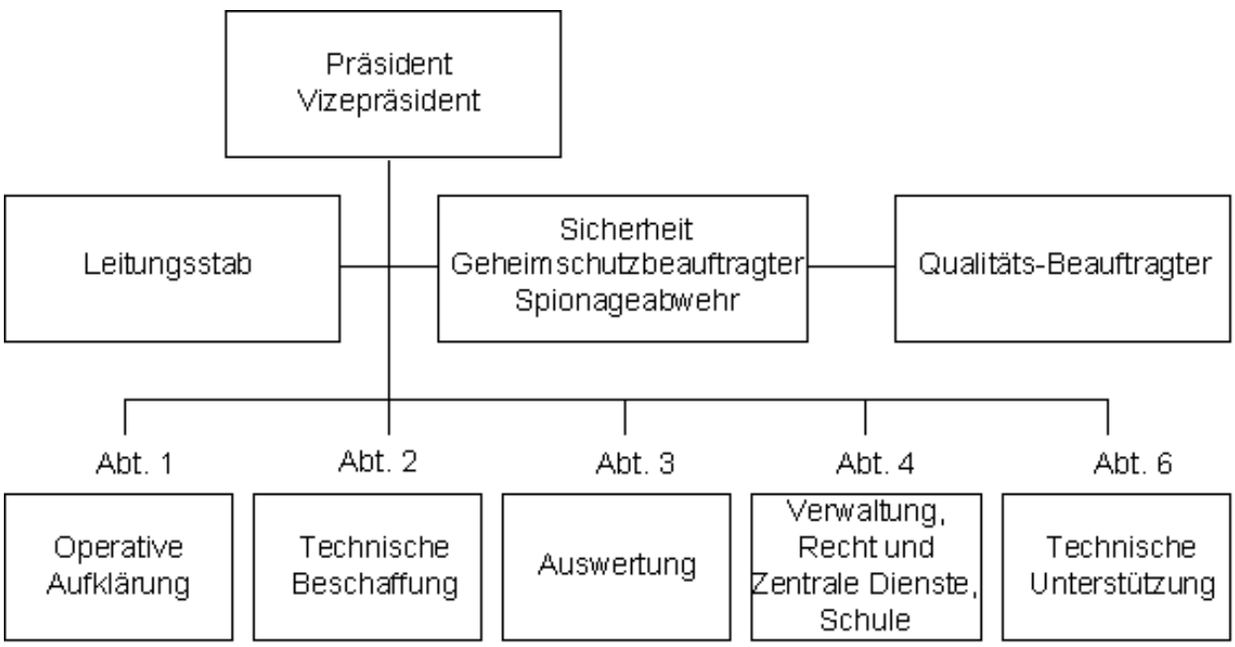
Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club

www.bundesnachrichtendienst.de: Geheimdienste, die nicht bis fünf zählen können



http://www.bundesnachrichtendienst.de/Struktur-bnd-frame.htm

- ❋ *Faktorisierung und Schlüssellängendiskussion*
- ❖ *Biometrie: Marketing statt Sicherheit*
- ❊ *Das Internet hacken - ein Ansatz mit Anspruch*
- ✪ *Review: Chaos Communication Camp*

ISSN 0930-1045
Herbst 1999, DM 5,00
Postvertriebsstück C11301F

#68/69

Impressum

Die Datenschleuder Nr. 68/69
III./IV. Quartal, Herbst 1999
Herausgeber:
(Abos, Adressen etc.)
Chaos Computer Club e.V.,
Lokstedter Weg 72,
D-20251 Hamburg,
Tel. +49 (40) 401801-0,
Fax +49 (40) 401801-41,
EMail: office@ccc.de
Redaktion:
(Artikel, Leserbriefe etc.)
Redaktion Datenschleuder,
Postfach 640236, D-10048 Berlin,
Tel +49 (30) 280 974 70
Fax +49 (30) 285 986 56
EMail: ds@ccc.de
Druck: St. Pauli Druckerei Hamburg

CvD und ViSdP: dieser Ausgabe:
Andy Müller-Maguhn, andy@ccc.de

Mitarbeiter dieser Ausgabe:
FrankRo, Tim Pritlove, Anonymer Informant, Arne, Doobee, Steini, Jens, Ingo, Padeluun, SteffenWernery...

Adressen http://www.ccc.de/ChaosTreffs.html

Chaos im Internet: http://www.ccc.de & news:de.org.ccc

Erfa-Kreise

Hamburg: Lokstedter Weg 72, D-20251 Hamburg, mail@hamburg.ccc.de Web: http://hamburg.ccc.de Phone: +49 (40) 401801-0 Fax: +49 (40)401 801 - 41 Voicemailbox +49 (40) 401801-31. Treffen jeden Dienstag ab ca. 20.00 Uhr in den Clubräumen. Der jeweils erste Dienstag im Monat ist Chaos-Orga-Plenum (intern), an allen anderen Dienstagen ist jede(r) Interessierte herzlich willkommen. Öffentliche Workshops im Chaos-Bildungswerk fast jeden Donnerstag. Termine aktuell unter http://www.hamburg.ccc.de/Workshops/index.html

Berlin: Club Discordia alle zwei Wochen Donnerstags zwischen 17 und 23 Uhr in den Clubräumen in der Marienstr. 11, Hinterhof in Berlin-Mitte. Nähe U-/S-Friedrichstrasse. Tel. (030) 285986-00, Fax. (030) 285986-56. Briefpost CCC Berlin, Postfach 640236, D-10048 Berlin. Aktuelle Termine unter http://www.ccc.de/berlin

Köln: Der Chaos Computer Club Cologne zieht gerade um. Aktuelle Koordinaten bitte unter mail@koeln.ccc.de bzw. http://www.koeln.ccc.de erfragen. Telefonische Erreichbarkeit erst wieder nach vollständigem Bezug neuer Räume.

Ulm: Kontaktperson: Frank Kargl <frank.kargl@ulm.ccc.de> Electronic Mail: contact@ccc.ulm.de Web: http://www.ulm.ccc.de/ Treffen: Jeden Montag ab 19.30h im 'Café Einstein' in der Universität Ulm.

Bielefeld: Kontakt Sven Klose Phone: +49 (521) 1365797 EMail: mail@bielefeld.ccc.de. Treffen Donnerstags, ab 19.30 Uhr in der Gaststätte 'Pinte', Rohrteichstr. 28, beim Landgericht in Bielefeld. Interessierte sind herzlich eingeladen.

Chaos-Treffs: Aus Platzgründen können wir die Details aller Chaos-Treffs hier nicht abdrucken. Es gibt in den folgenden Städten Chaos-Treffs, mit Detailinformationen unter http://www.ccc.de/ChaosTreffs.html:

Bochum/Essen, Bremen, Burghausen/Obb. und Umgebung, Calw, Dithmarschen/Itzehoe, Dresden, Emden / Ostfriesland, Eisenach, Erlangen/Nürnberg/Fürth, Frankfurt a.M., Freiburg, Freudenstadt, Giessen/Marburg, Hanau, Hannover, Ingolstadt, Karlsruhe, Kassel, Lüneburg, Mannheim/Ludwigshafen/Heidelberg, Mönchengladbach, München, Münster/Rheine/Coesfeld/Greeven/Osnabrück, Rosenheim/Bad Endorf, Neunkirchen/Saarland, Würzburg, Schweiz/Dreyeckland: Basel, Österreich: Wien

Nächstes Jahrtausend wird alles: ❑ anders ❑ bunter ❑ besser ❑ chaos

Lieber Leser,

in der Geschichte der Datenschleuder hat es einiges an chaotischen Abläufen, Unregelmässigkeiten, Pannen und sonstigem Gegeben. Dazu ist jetzt etwas neues dazu gekommen: die Datenschleuder 68 wurde nach Druck und Etikettierung auf Vorstandsbeschluss komplett eingestampft. Das hatte mit einem dort abgedruckten Dokument zu tun, daß wir euch zwar inhaltlich nicht vorenthalten möchten, aber letztlich sich keine Mehrheit fand, die möglichen Konsequenzen des dadurch enthaltenen (vor allem: zivilrechlichen) Gesetzesverstoss nicht tragen konnten.

Datenschleudern auf dem Papier hat nicht nur Vorteile.

Einige sagen mitllerweile sogar, daß Papiermedium hat mehr Nach- als Vorteile.

Die unmittelbare Konsequenz dieses Vorfalls ist diese Doppelausgabe 68/69, die die meisten von euch wahrscheinlich erst zum Congress bzw. zwischen Weihnachten und Neujahr erreichen wird.

Zum anderen haben wir uns entschlossen, daß Konzept des Mediums Datenschleuder grundsätzlich zu ändern.

Der Schwerpunkt der Datenschleuder wird ab der nächsten Ausgabe im Web liegen. Die Papierausgabe wird vorr. ein Doppelbogen im A4-Format werden, wo ihr zwar nur kurze Meldungen und Artikel mit entsprechenden Netzreferenzen, dies dafür aber monatlich erhaltet. Näheres dazu nach dem Congress auch auf http://www.ccc.de

Bitte seien Sie unbesorgt.
Handlungsanweisung eines Fahrstuhl-Notfallschildes für den Fall, daß man im stehengebliebenen Fahrstuhl den Alarmknopf drückt und trotzdem nichts passiert.

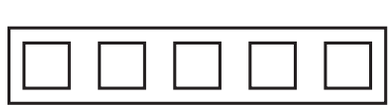
Wir möchten die Daten aber auch mehr mit eurem Feedback schleudern. Deswegen: schreibt uns, was ihr wichtig findet, kritisiert uns (und zwar ehrlich und nicht höflich) und vor allem: leitet uns die Meldungen und Daten weiter, die ihr wichtig empfindet:

ds@ccc.de

Bis dahin wünschen wir euch eine diskordische Zeit mit viel Spaß am Gerät.

Impressum / Kontaktadressen -1

Editorial / Index ❑❑❑❑❑
CRD: ˝Lockerung˝ d. US-Cryptoexp. ❑❑❑❑■
CRD: BTX abgemeldet ❑❑❑❑■
CRD: Ansprechpartner beim BND ❑❑❑❑■
CRD: CCC Mailinglisten Übersicht ❑❑❑❑■
CRD: US Army setzt auf Mac OS ❑❑❑■❑
CRD: GAA Aufbohrnotwendigkeit ❑❑❑■❑
Schlossindustrie & Lauschangriff ❑❑❑■■
Das Internet (komplett) hacken ❑❑■❑■
Faktorisierung & Schlüssellängen ❑■❑■■
Unsicherheit mit o. ohne Biometrie ■❑❑❑■
Encrypting your Disks with Linux ■❑❑■■
Chaos Communication Camp Review ■❑■❑■
Radio Intergalaktik HowtoRadiosend ■■❑■■
Buchkritik: Cryptonomicon ■■■❑■
Weitere Literaturhinweise ■■■■■
Termine 33
Bestellfetzen 34



Kurzmeldungen & Updates

Exportrestriktionen kein Stück gelockert

Nach der Ankündigung der US-Regierung(http://www.bxa.doc.gov/Encryption/q&a99.htm), die Exporrestriktionen für kryptographische Produkte etc. demnächst auflockern zu wollen, sind zwar noch keine konkreten Umsetzungen erfolgt, aus den bisher veröffentlichten Eckpunkten ist allerdings jetzt schon absehbar, das es eher schlimmmer wird.

Die bisherigen Exportrestriktionen, die Zweifellsohne in erster Linie die Interessen der amerikanischen Regierung vertreten, waren wenigstens im "Source-Code" sprich in den direkten Gesetzen und ausführenden Bestimmungen nachlesbar (z.B. http://www.epic.org/crypto/export_controls). In Zukunft soll es anstelle dieser Bestimmungen nur noch ein "technical review" geben. Sprich, die Hersteller von Produkten müssen der US-Regierung bzw. an dieser Stelle der NSA die technischen Details ihrer Produkte "vorlegen" und bekommen dann eine Abnahmebescheinigung. Was im Rahmen dieses Verfahrens dann passiert dürfte deutlich weniger transparent sein.

BTX abgemeldet; no more *CCC#

Im Rahmen von Strukturmodernisierungsmassnahmen haben wir uns entschlossen, den Bildschirmtextbetrieb einzustellen. Die Btx-Leitseite *CCC# gibt es nicht mehr. Damit hatten wir zwar in den 80er Jahren viel Spaß, allerdings war der Betrieb immer auch mit Kosten verbunden, die wir durch den Betrieb von Literaturversand und Spendenseite eine zeitlang decken konnten. Die Kostendeckung war irgendwann definitiv nicht mehr gegeben und irgendwie hatte auch keiner Lust da noch Zeit reinzuinvestieren. Mit dem Betrieb von Web-, Mail- und FTP-Server haben wir im Internet dann wohl doch eher mehr Spaß und weniger Kosten.

Technischer Ansprechpartner beim Bundesnachrichtendienst

http://www.ripe.net/cgi-bin/whois?DL1570-RIPE

```
source:      RIPE
person:      Dietmar Langenbucher
address:     Bundesnachrichtendienst
address:     Heilmannstr. 30
address:     D-82049 Pullach
address:     Germany
phone:       +49 89 79359283718
fax-no:      +49 89 7448033001
nic-hdl:     DL1570-RIPE
notify:      ripe-notify@t-domain.de
notify:      dbd@nic.dtag.de
mnt-by:      DTAG-NIC
```

...übrigens nicht zu verwechseln mit www.bnd.de...

Kurzmeldungen & Updates

Apropos Listserver

Schon seit einiger Zeit betreiben wir einen Listserver mit etlichen öffentlichen Mailinglisten, die auch Nicht-Mitgliedern, Abonnenten und anderen Interessierten zur Verfügung stehen.

Zum abonnieren bzw. abbestellen gilt dabei listenname-subscribe@lists.ccc.de (also z.B. news-subscribe@lists.ccc.de) bzw. listenname-unsubscribe@lists.ccc.de. Um Spam fernzuhalten, können grundsätzlich nur Abonennten (Subscriber) auf die Listen mailen. Folgende Listen gibt es bis jetzt:

```
debate@lists.ccc.de - Allgemeine Diskussionen
rund um den CCC bzw. aktuelle Themen

news@lists.ccc.de - Keine Diskussionen, sondern
nur Meldungen bzw. Hinweise auf Geschehnisse mit
entspr. URL´s

machackers@lists.ccc.de - Die Macintosh-Fraktion
unter den Hackern.

funk@lists.ccc.de - Diskussionen unter den
Amateuer- und sonstigen Funkern.
```

Dann betreiben wir noch einige Announcement Lists, wo offizielle CCC-Termine, Ankündigungen, Hinweise etc. verbreitet werden:

```
chaosradio@lists.ccc.de
Hinweise zu den nächsten Sendungen,
Zusammenfassungen und Quellenhinweise der
Sendungen etc.

chaos-update@lists.ccc.de
Offizielle (Presse-)Mitteilungen des CCC,
Terminankündigungen, Hinweise etc.
```

Allerlei Buntes gibt es übrigens auch auf ftp.ccc.de

US-Army wechselt von Windows NT zu Mac OS

Die US-Army hat aufgrund von anhaltenden Sicherheitsproblemen mit Windows NT ihre Websites auf MacOS umgestellt. Systemadministrator Christopher Unger erklärte dazu schlicht, die Army habe ihre Websites auf eine sicherere Plattform umgestellt.

http://www.dtic.mil/armylink/news/Sep1999/a19990901hacker.html

Beim Ankauf gebrauchter Geldautomaten ergibt sich mitunter eine Aufbohrnotwendigkeit, weil die Institute die Zahlenkobination des Tresors nicht mitliefern wollen; sie ist in allen Filialen gleich.

Schlossindustrie hilft...

Schlosshersteller werden nach Angaben des Nachrichtenmagazins „Der Spiegel“ die Polizei beim umstrittenen Grossen Lauschangriff unterstützen. Sie werden den Behörden künftig Nachschlüssel ausliefern, damit diese in Wohnungen und Firmen Abhöranlagen installieren können.

Wie das Nachrichtenmagazin in seiner Ausgabe vom 26.04.99 berichtete, hat das Landeskriminalamt Baden-Württemberg stellvertretend für alle Polizeibehörden einen dubiosen Pakt mit den Schlossherstellern getroffen, um Schlüsselkopien für komplizierte Schlösser direkt vom Hersteller abzufordern.

Die Vereinbarung stehe in Zusammenhang mit dem im vergangenen Jahr im Kampf gegen das organisierte Verbrechen beschlossenen Grossen Lauschangriff. Dieser erlaubt es der Polizei, unbemerkt in Wohnungen einzudringen und Wanzen zu montieren. Da es nach Angaben des LKA unmöglich sei, hochwertige Schlösser zu öffnen, ohne Spuren zu hinterlassen, seien die Landeskriminalämter auf die Hilfe der Industrie angewiesen.

Tips zur Nachschliessicherheit

Schliesszylinder mit Sicherungskarte sollten so erworben werden, dass beim Verkäufer keine Daten über den Käufer erfasst und gespeichert werden. Empfehlenswert ist die Barzahlung gegen Quittung in einem Laden, wo man nicht persönlich bekannt ist. Dieses ist jedoch kaum möglich, wenn eine Schliessanlage durch einen Fachbetrieb eingebaut wird! Gefährlich ist auch die Bestellung von Nachschlüsseln, da hier der Hersteller die mit der Sicherungskarte übermittelten Kundendaten erfassen kann. Die Speicherung sensibler Daten birgt immer die Gefahr der unbefugten Nutzung durch Mitarbeiter oder Dritte!

Der ssDeV empfiehlt grundsätzlich die Verwendung mehrerer technisch unterschiedlicher Schliesssysteme. Werden hochwertige Stift- und Scheibenzuhaltungen und Bohrmuldenzylinder verschiedener Hersteller kombiniert, scheiden Angreifer mit Detailkenntnissen über nur einen speziellen Schlosstyp aus. Auf weit verbreitete Schliesssysteme sind Experten besser vorbereitet, als auf exotische in Deutschland selten genutzte Schliesssysteme.

Bei der Auswahl des Schliesszylinders sind beidseitig schliessende Zylinder zu vermeiden. Eine Gefahrenfunktion (öffnen, wenn der Schlüssel auf der anderen Seite steckt) sollte, bei Bedarf, nur für die Innenseite vorhanden sein!

Sollten Verbraucher aufgrund dieser Erkenntnisse ihre Schlösser tauschen, so bittet der ssDeV um Überlassung der alten Schliesszylinder zu Übungs- und Forschungszwecken.

Weiterhin sollte immer ein Ersatzschloss mit genügend Schlüsseln sicher verwahrt vorgehalten werden, um bei Bedarf sofort und ohne Eingreifen Dritter eines der mindestens drei Schlösser austauschen zu können.

Grundsätzlich sollten die Vorschriften der Versicherungsbedingungen (z.B. Hausratversicherung) beim Erwerb und Einbau beachtet werden, um den Versicherungsschutz nicht zu gefährden.

Jeder Schlüssel lässt sich optisch auslesen. Für den professionellen Lockpicker genügt oft ein Blick auf den Schlüssel, um die Kodierung auszulesen und einen Nachschlüssel anzufertigen. Andere fertigen Nachschlüssel nach Foto-Vorlagen oder nehmen einen Abdruck. Berichtet wurde auch von verdeckten Aktionen zum Auslesen der Schlüssel, z.B. bei Verkehrskontrollen! Nicht ohne Grund tragen Gefängniswärter ihre Schlüssel immer verdeckt in einer Tasche. Schlüssel für schutzwürdige Räume sollten immer getrennt von

beim Lauschangriff

gebräuchlichen Schlüsseln, wie z.B. KFZ-Schlüssel, in einem verschlossenen Etui am Körper mitgeführt werden. Sind Türen tagsüber zugänglich, lässt sich auch der Schlosskasten direkt manipulieren. So sollte darauf geachtet werden, dass der Schlosskasten keine Kratzspuren aufweist und der Riegel fest schliesst. Bei manipulierten Schlössern ist es teilweise möglich, den ausgeschobenen Riegel von Hand zurückzuschieben.

Die Schlosskästen sollten mit einer selbstgemischten, nicht handelsüblichen Farbe dünn lackiert werden, um Kratzspuren sofort entdecken zu können.

Bei komplizierten Schliesssystemem wird häufig der Schlosskasten angegriffen. So genügt oft ein kleines (1-3mm) Loch neben dem Schutzbeschlag, um mittels Drähten das Riegelwerk des Schlosskastens anzugreifen. Kleine Unregelmässigkeiten in der Nähe des Schutzbeschlages sollten immer auf Bohrspuren überprüft werden. Sinnvoll ist das Einpassen einer Edelstahlplatte, welche den Schlosskasten weiträumig abschirmt - sowie die Verwendung einer nicht handelsüblichen selbstgemischten Farbe für den Tür- und Fensteranstrich.

Bei der Auswahl des Schlosskastens sind selbstverriegelnde Schlosskästen zu bevorzugen. Diese sperren automatisch sowohl die Falle als auch den Riegel. Gegen Öffnungen mit einer Nadel oder Plastikkarte hilft oft schon ein Schlosskasten mit Taster, welcher bei geschlossener Tür die Falle sperrt.

Elektronische Schliesssysteme sollten vermieden werden, da nicht überschaubar ist, ob diese Systeme mit General-Codes versehen wurden.

Immer noch aktuell ist das Prinzip des Sicherungsmerkmals. In die Tür wird dezent ein Gegenstand eingeklemmt (z. B. ein Haar), welcher beim Öffnen herausfällt. Wichtig ist, dass das Anbringen des Sicherheitsmerkmals nicht von Dritten beobachtet werden kann!

Nicht vergessen werden sollte, dass die Tür oft nicht der einzige mögliche Zugang ist - und vorhandene Schlösser auch abgeschlossen werden sollten!

Um unerlaubte Abhöraktionen zu vermeiden, sind weitere Massnahmen notwendig. Das Verbreiten kompromittierender Abstrahlung (z.B. von PC's, Monitoren, Telefonen) kann nur durch entsprechende Abschirmung begrenzt werden. Gegen Abhörlaser hilft gegebenenfalls eine entsprechende Grundbeschallung der Fensterfläche aus mehreren Tonquellen.

Im Zweifelsfall sollte man sich durch verschiedene Sicherheitsunternehmen beraten lassen.

SSDeV-Pressestelle, 27.04.99

Das Internet hacken:

Das Internet hacken? Das scheint auf den ersten Blick unmöglich. Aber wie steht es um die Sicherheit des Internet als ganzem? Ein grossangelegter Angriff auf die vielen kleinen Sicherheitslöcher könnte das weltweite Netz mit einem Schlag ins Wanken bringen.

Dieser Artikel erschien zuerst bei *security-focus.com* und wurde für die Datenschleuder gekürzt:

The Internet Auditing Project by Liraz Siri <liraz@bigfoot.com> Wed Aug 11 1999

Today, when too many people think of security on the Internet, they think of individual hosts and networks. Alone. Got a problem? Damn! Must be those damn hacker punks. Again. Keep it to yourself. Call the Feds, call the New York Times. Make sure we don't get it. Didn't keep your systems patched? Moron. Don't make us sue you.

With the growing irrelevance of security organizations like CERT and law enforcement on the Internet, an ever growing number of attacks are handled in isolation.

Hundreds of millions of Internet users around the world have become accustomed to an Internet beyond boundaries. One site flows to the next, a jungle of software, protocols, media and people connecting, signal, noise, mixing, evolving, together.

It seems silly to ignore the security of the system _ as a whole_, but we still do. A helpful analogy might be to consider the Internet more a living organism than a neighborhood. A security compromise is can behave more like a disease then a "break-in". It is often contagious and can spread. Remotely exploitable security vulnerabilities are like the natural wounds of the skin. They are relatively rare, sometimes difficult to squirm through, but once inside, infection can begin.

This article describes the efforts of a small, independent, security research group to audit some 36 million hosts connected to the Internet, for commonly known security vulnerabilities in an unfocused low-res scan.

Why? Because we're a curious bunch, because we've been speculating (rather academicly) over the results for several years, and of course, because we can.

Walk forth in dread

So you want to scan the millions of computers on the Internet from Japan to Egypt to Florida? Reach out and audit the networks of Internet Service Providers, corporations, universities, government facilities, banks and sensitive military installations?

First, take another moment to think about it.

Many people get nervous on the receiving end of an uninvited security audit, and you'll eventually step on quite a few toes. In some countries, you can even expect unpleasant house-calls from local law enforcement which will brand you a criminal for your unusual efforts. Citizens of a large democracy with many three letter agencies should be aware that a fully-equipped SWAT team is likely to tag along.

While this may deter, possibly comfort law-abiding readers, a criminally inclined party is not without it's options. Resources are abundant on the Internet, and many suitable, unsuspecting, high-bandwidth volunteers are not hard to find, with the modest help of your favorite bulk auditing software.

Not intimidated? That's the spirit!

„The Internet Auditing Project“

Quick & Dirty Overview

Let's take a look at some of the basic ingredients we're going to need:

1. Some wheels. (BASS, a Bulk Auditing Security Scanner)
2. A map. (address search space)
3. Fuel. (resources)

Wheels

The Internet is getting rather big these days, and exploring it's tens of millions of unique hosts is by no means an easy task. Manually, we could never get the job done. Fortunately, we can let a computer (or several) do most of the dirty work, allowing us to concentrate on coordination and management.

Assuming of course, we have the right software. In this case, we're going to need a robust bulk security scanner that can monotonicly run for weeks, even months at a time, efficiently processing millions of addresses, generating gigabytes of traffic and surviving everything from broken routing, to system shutdowns and unfriendly sysadmins.

After a several weeks of on-off programming, the first alpha version of BASS, the Bulk Auditing Security Scanner was ready for it's first test run. Israel was the first target in a series of trials.

At this point (Sep-Oct 98) BASS could only identify 4 common security vulnerabilities, but adding more later was a simple matter. The scan finished on schedule. 110,000 addresses in under 4 hours, on a dual ISDN 128k connection. We selected the United Kingdom, with an address space of 1.4 million, for our next trial.

Now that the architecture was stable, we proceeded to familiarizing BASS with the wonders of CGI and RPC, allowing the scanner to test for up to 18 widely known security vulnerabilities. The tests were designed to reduce false positives and false negatives to a minimum, combining passive (server's version header) and interactive (server's response to ill-formed input: a buffer-overflow, sneaky characters) implementation signatures to determine vulnerability.

A map

Yeah, well what I really mean is a really long list of "all" the computers connected to the Internet. Please note the term "all" is used loosely ("most" or the "majority" would probably be more accurate).

An Internet Protocol address, or IP for short, is a 32 bit integer. This means are there 2^32 (4.3 billion) possible unique IPs, the IP address space. In practice, only a very small fraction of this space is really used.

Due to the anarchic nature of the Internet, nobody has any exact figures on usage statistics, but most estimates (circa Jan 1999) settle around 100 million users worldwide. The number of computers online is more around an order of a magnitude lower (15 million).

In our case, we ended up scanning around 36 million IPs, which we estimates covered 85 percent of the active address space at the time.

Keep in mind, however, that the Internet is growing very quickly, so these numbers will get bigger by the time you try this out yourself. Search for "Internet Surveys" on the web, and get an updated figure.

Fuel

Swarming the Internet with probes requires some resources, bandwidth mostly. How much of it you need depends on how flexible your schedule is.

Das Internet hacken:

Generally speaking, You're likely to find you need a lot less of it then you might first imagine.

The good news is that scans are easy to parallelize, so you can divide the load over as many different computers and networks as you have access to, to either get the scan finished faster, or to consume fewer resources from each participating scanning node.

A minor detour, introducing IDDN. (the International Digital Defense Network)

All of this brings us to an interesting idea we've been playing around with that could dramaticly influence Internet security for the good, if / when it is eventually implemented. Frankly, the idea deserves an article of it's own, but since we are so busy, we will introduce it here.

Inspired by the high response to cryptographic key challenges, distributed.net and the SETI effort, we vision a non-profit foundation, which we like to ambitiously call IDDN, the International Digital Defense Network, working in the public interest to organize massively distributed scanning efforts which routinely probe the Internet for security vulnerabilities. 10,000 participants could finish a scan cycle every 2-3 days. At the end of a cycle, an automated system could draw the attention of administrators worldwide to some of their local security problems, and offer whatever information and solutions (bug-fixes, patches, workarounds) it has on database (patches, advisories, exploits). In our opinion, such an effort is highly practical and could contribute more to the stability and security of the Internet then the traditional (somewhat pointless?) bruteforce crypto key challenges. We believe organizing an Internet neighborhood-watch of sorts is in everyone's interests, especially the Internet's commercial industry which depend on the Internet to eventually fulfill it's potential for global electronic commerce.

Let the show begin Tuesday, 1 December 1998.

We've installed BASS on 8 Unix boxes around the world, each with at least 512kbps bandwidth. 8 different geographicly located participants in 5 different countries: Israel(1), Mexico(1), Russia(2), Japan(2) and Brazil(2). Two machines have already proven their strength during the scanner's painful debugging sessions. Three more will join them for the first time when we begin. The others are backups, ready in case anything goes wrong, and frankly, we have some concerns.

At 02:00 GMT, we flip the switch, so to speak, activating BASS on the five participating hosts. Since these have all been configured to automaticly recover from any power failure or unexpected system shutdowns, we really don't have much to do now, besides keeping a lazy eye on progress.

First week

There is definitely a response out there to the scan, but it's much friendlier then we anticipated. Harmless acts of mindless automata and mutual curiosity, mostly. Pings, traceroutes, telnet sessions and finger attempts. Four to eight portscans a day. An occasional TCP/IP stack exercise, an OS fingerprint, a few mostly polite e-mails asking why our network was "attacking" theirs, frequently warning us that crackers may be abusing our systems, suggesting we look into it. Very mild, we are running into much less hostility then we expected.

People either don't realize the scope of the scan, or don't care. On an individual basis, one quick security probe isn't usually enough to get the local sysadmin to notice. Those who do are probably security conscious enough to keep their networks

up to date anyway, and confident enough to keep their cool when yet another 13 year old punk (who else?) bangs on their network walls.

Oh, did we mention the scanner is precisely on schedule? 12 million hosts scanned by the end of the week, covering the US government's *.gov domain, Canada, Australia, Europe, and a window to some of the most intriguing corners of the world: Hostile mind-control regimes like China and Iran for example, which suffocate their repressed population's access to free ideas and information, but are still paradoxicly connected (albeit, very poorly) to the Internet. Third world potentials like India (the world’s largest democracy!) and the rapidly developing countries of the far east. All of them as close and accessible as if they were right across the street, and in a certain way even closer. Computer expertise is rare in many of these countries, security expertise even rarer. Cracking into a Chinese computer half a world away, for example, is usually easier, more interesting, and safer (assuming you are not in Chinese jurisdiction of course) then cracking into a comparable western computer.

Second week

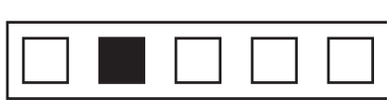
We started the week off by scanning US Military networks. Admitingly, we were pretty nervous, and spent much of the day keeping an eye out for telltale signs of a pissed off military retaliation (also known as "InfoWar" and "spooky shit" in professional terminology).

In just under 24 hours it was all over, and while we did notice a significant increase in the number of probes we were getting, to say we were not impressed by the security of the military network is a big fat major understatement. This might not be a problem, since according to NSCS (National Computer Security Center) network security policies, none of the systems on the public *.mil network could qualify for the storage and handling of classified DoD (Department of Defense) information. How strictly these policies are adhered to is another matter. And even if they are (and this is a _big_ if), the DoD is still (justifiably) concerned that crackers might glue together classified information from the little pieces of unclassified information fragments lying around their *.mil network (in great abundance). So they have plenty of good reasons to keep their network secure, but are (un)?fortunately doing a pretty lousy job.

"You're gonna rot in jail" - the legal corner

We've began receiving e-mail's this week by people with alot less tolerance for our activities, most in delayed response to last week's scans. Some of these were written by lawyers who informed us we were either supporting or perpetrating acts of computer crime against their clients. They had notified the authorities (CERT and the FBI were commonly cited) and threatened to take us to court if we did not offer our full cooperation in immediately identifying the attacking party. Right...

The Internet however is a public network, and the majority of it's services are used anonymously, by users with which there is no persistent relationship. The computer world is pure code, instructions and information, none of which are capable of discrimination. The computer programmer is the god of a perfectly obedient universe. This means software, like the law, can inherit the imperfections of it's creator. Poorly written computer and legal code can allow the system to behave in conflict with the original intentions of the men who wrote it. Legal loopholes and software bugs, Lawyers and Hackers, different sides of the same coin. The only way to really prevent the abuse of the system is to write better code.



Das Internet hacken:

Third week

Last week. Only the mammoth *.com and half of the *.net domain left and we're done.

Friday, our Japanese participants discover that a computer on their company network has been cracked into, one very secure Linux box running only SSH and Apache 1.3.4. Now this would definitely send a chill up your spine if you knew just how fanatic our friends are when it comes to network security. Furthermore, they only detected the intrusion three days after the fact, which is unbelievable when you consider the insane monitoring levels they've been keeping since they agreed to participate in the scan. They would have noticed any funny stuff, and in fact, they did, lots of it, but none of which came close enough to a security breach to raise any alarms.

Readers should also note how although a key binary in the cracked machine had been modified, tripwire and an assortment of other booby traps failed to detect this had happened. Even a close-up manual inspection (comparing file contents with a trusted backup, playing with it's name) could not detect any odd behavior. This trick, and others equally spooky were achieved by clever manipulation of the OS's kernel code (dynamicly, through a module).

The attacker is using a custom built software penetration agent. This is only an hypothesis, but is strongly supported by the fact that the entire attack only lasted an incredible 8 seconds! During which the attacker manages to log on (over an employee's SSH account, no less), gain root privileges, backdoor the system, remove any (standard) traces of it's activity and log off.

And Wow! If there ever was a crack to appreciate for it's elegance, simplicity, and efficiency, this was it.

Whoever they were, they certainly knew what they were doing, and for the most part seemed very good at it. But being determined, clever, and sophisticated just doesn't cut it when you do battle with wizardly foes (that's us) yielding the great powers of the Universe to their command: Dumb luck and clinical paranoia.

IAP cheat-sheet

```
BEGIN TIME: 02:00, Dec 01, 1998 GMT
END TIME: 08:00, Dec 21 1998 GMT

Scanning nodes: 5
Jobs Per Minute: 250
Scan time: 20.24 days

Vulnerabilities tested: 18

Domain count: 7 three letter domains,
214 national domains (jp, us, uk, de, ca, ...)
Host count: 36,431,374
Vulnerability count: 730,213
Vulnerable host count: 450,000

Statistical output:

service       |     vulnerability count,
                          percentage (from total)
-------------------------------------------------
webdist       |  5622 hosts counted,    0.77%
wu_imapd      |  113183 hosts counted,  15.5%
qpopper       |  90546 hosts counted,   12.4%
innd          |  3797 hosts counted,    0.52%
tooltalk      |  190585 hosts counted,  26.1%
rpc_mountd    |  78863 hosts counted,   10.8%
bind          |  132168 hosts counted,  18.1%
wwwcount      |  86165 hosts counted,   11.8%
phf           |  6790 hosts counted,    0.93%
ews           |  9346 hosts counted,    1.28%

(other vulnerabilities which weren't common enough
to generate statistics for)
other:        |  18K hosts counted,     2.42%
```

„The Internet Auditing Project“

Conclusions

A global fury of half a billion packets, digital signals zipping back and force across the planet at the speed of light. Above the Earth, across the land, under the sea, over satellite microwave, copper wiring, fiberoptics, wireless and undersea cable. Probing cyberspace. Pretty cool, the kind of power information technology puts in our hands these days.

Seven hundred thousand vulnerabilities, gaping holes, wounds in the skin of our present and future information infrastructures, our dream for a free nexus of knowledge, a prosperous digital economy, where we learn, work, play and live our lives. Easy pickings, at the fingerprints of anyone who follows in our footsteps, friend or foe.

These open points of penetration immediately threaten the security of their affiliated networks, putting many millions of systems in commercial, academic, government and military organizations at a high compromise risk.

We were stunned to find just how many networks you would expect to be ultra secure were wide open to attack. Banks, billion dollar commerce sites, computer security companies, even nuclear weapon research centers, goddamit!

Looking at the big picture, the problem gets worse. A catastrophe in the works. So far, we've been pretty lucky.

Consider the power these unsecure networks represent _together_. Penetrating and controlling millions of hosts? You couldn't do it manually, but with the right software, you could automate most of the dirty work. You'd need a careful network worm, stealthy remote administration software and a self organizing network nervous system by which you could propagate control.

Imagine the implications if this sort of capability ever fell into the wrong hands. A government (China perhaps), a political terrorist group or organized crime. On bandwidth alone they could shut down any part (or all) of the Internet in mammoth DoS attacks. A country, a portal, a news site, or maybe just InterNIC. Leverage and attention, for fun and profit. They could "build" the world's largest distributed supercomputer, or construct an Intelligence network rivalled only by the NSA's Echelon.

Of course, who says only one group can play the game? Struggles for power in the digital domain could very well develop into the world's first real information war, with the very future of the Internet as a free unregulated supernetwork caught in the cross fire.

Unlikely? Far fetched? We hope so.

The only thing necessary for the triumph of evil is for good men to do nothing. Wake up fellow countrymen. Let's get to work.

Wer mehr über den Japan-Hack erfahren will, ausserdem über eine DoS-Attacke auf den russischen BASS-Scanner und über die Funktionsweise des Domain-Name-System, findet den Text in voller Länge im Web. Daneben liegt dann auch der Source-Code für den BASS-Scanner.

http://www.security-focus.com/templates/forum_message.html?forum=2&head=32&id=32

Liraz Siri <liraz@bigfoot.com>, Wed Aug 11 1999

Herbst/Winter 1999

Die Datenschleuder #68/69

Bundesverband deutscher Banken

Grobanalyse

des neuen Verfahrens

zur PIN-Berechnung und PIN-Prüfung für ec-Karten

Inhaltsverzeichnis

1 ZUSAMMENFASSUNG DER RESULTATE 1

2 DAS NEUE VERFAHREN 2

2.1 PIN-Generierung 2
2.1.1 PIN-Generierung aus Karteninformation 2
2.1.1.1 Dezimalisierung Alternative 1 (ZKA) 3
2.1.1.2 Dezimalisierung Alternative 2 3
2.1.2 PIN-Generierung durch Pseudozufallsgenerator 3

2.2 PIN-Verifikation 4
2.2.1 PVN-Berechnung 4
2.2.2 Dezimalisierung 4
2.2.3 Alternative 1 (ZKA) 4
2.2.4 Alternative 2 5
2.2.5 Alternative 3 5

3 ANALYSE 6

3.1 Sicherheit der eingesetzten Mechanismen 6
3.1.1 Triple-DES 6
3.1.2 Dynamische Schlüsselgenerierung 6
3.1.3 Dezimalisierung 6
3.1.3.1 Dezimalisierung der PIN nach Alternative 1 6
3.1.3.2 Dezimalisierung der PIN nach Alternative 2 7
3.1.3.3 Dezimalisierung des PVN 7
3.1.3.4 Verzicht auf Dezimalisierung der Prüfwerte 7
3.1.4 Zufallsgenerierung der PIN 7

3.2 Trennung von PIN-Generierung und PIN-Verifikation 8

3.3 Einsatz kartenspezifischer Schlüssel 8
3.3.1 Bestimmung des Schlüssels im heutigen Verfahren 8
3.3.2 Bestimmung von KGK_{PINGEN_INST} und $KGK_{PVNGENj\_INST}$ im neuen Verfahren 8
3.3.3 Einfluss der Selbstwahl-PIN 9

3.4 Möglichkeit zum Schlüsselwechsel 9

4 REFERENZEN 10

Die Datenschleuder #68/69

Herbst/Winter 1999

1 Zusammenfassung der Resultate

Dieses Dokument enthält eine zeitlich und aufwandsmässig limitierte Grobanalyse der Sicherheit des neuen Verfahrens zur PIN-Berechnung und PIN-Prüfung für ec-Karten.

Die Sicherheit des neuen Verfahrens wurde für die vorgesehene Anwendung als ausreichend beurteilt. Gegenüber dem bisherigen Verfahren wurden signifikante Verbesserungen festgestellt. Diese liegen vor allem in den folgenden Punkten:

- Einsatz von Triple-DES statt DES;
- Einsatz kartenspezifischer Schlüssel;
- Möglichkeit zum Schlüsselwechsel.

Aus Sicherheitsüberlegungen werden sowohl für die PIN-Generierung wie auch für die PIN-Verifikation jeweils die Alternativen 3 empfohlen.

Die weiteren Resultate und Empfehlungen dieser Untersuchung lauten zusammengefasst wie folgt:

1. Triple-DES bietet in bezug auf die *voraussehbaren* technischen Entwicklungen eine Sicherheitsreserve von mehr als 10 Jahren. Dennoch sollte die Implementierung des Verfahrens so gestaltet werden, dass zu einem späteren Zeitpunkt der Ersatz des Chiffrieralgorithmus problemlos möglich ist.
2. Durch den Einsatz kartenspezifischer Schlüssel kann ein erfolgreicher kryptoanalytischer Angriff auf die Hauptschlüssel zwar nicht völlig ausgeschlossen werden, es ergibt sich jedoch ein nennenswerter Sicherheitsgewinn, der die zusätzliche Komplexität mehr als rechtfertigt.
3. Die Trennung der Verfahren für PIN-Generierung und PIN-Verifikation bringt per se keinen bedeutenden Zuwachs an Sicherheit. Die Trennung ist vor allem deshalb sinnvoll, weil sie die Möglichkeit der zufälligen Erzeugung von PINs und der späteren Einführung einer Selbstwahl-PIN bietet.
4. Die Berechnung der PINs aus den Kartendaten stellt unter Sicherheitsgesichtspunkten eine überflüssige, potentielle Schwachstelle dar. Wenn möglich ist Alternative 3 der PIN-Erzeugung durch einen Pseudozufallsgenerator vorzuziehen. Noch besser wäre die wirklich zufällige Erzeugung der PINs durch einen geeigneten Prozess.
5. Für die zukünftige Einführung von Selbstwahl-PINs sollten folgende Punkte berücksichtigt werden:
   - Die Möglichkeit von Selbstwahl-PINs mit mehr als vier Stellen, wie sie in den Alternativen 2 und 3 der PIN-Verifikation gegeben ist, sollte von Anfang an vorgesehen werden.
   - Der durch den Einsatz kartenspezifischer Schlüssel erzielte Sicherheitsgewinn geht durch die Einführung der Selbstwahl-PIN verloren, falls das Verfahren nicht modifiziert wird.
6. Zusätzlich zum regulären Schlüsselwechsel auf der Basis des Verfallsjahres der Karte sollte die Möglichkeit für einen notfallmässigen Schlüsselwechsel geschaffen werden. Dies ist bei Verzicht auf die Ersatzautorisierung mit den Alternativen 3 auch leicht möglich.
7. Falls die Möglichkeit der Ersatzautorisierung offen gehalten werden soll, wird vorgeschlagen, für die Berechnung der Prüfwerte auf der Karte separate Schlüssel zu verwenden, die nur im Bedarfsfall verteilt werden.

BdB: Grobanalyse neues PIN Verfahren Version 2.0 STRENG VERTRAULICH

2 Das neue Verfahren

Das vorgeschlagene neue Verfahren zur PIN-Berechnung und PIN-Prüfung [PIN. RAHMEN] unterscheidet sich in seinen sicherheitsrelevanten Aspekten vom bisherigen Verfahren vor allem in den folgenden Punkten:

- Trennung von PIN-Berechnung und PIN-Prüfung;
- Einsatz kartenspezifischer Schlüssel;
- Ersatz von DES durch Triple-DES als Chiffrierverfahren;
- Möglichkeit zum Schlüsselwechsel;
- Option auf Selbstwahl-PIN.

2.1 PIN-Generierung

2.1.1 PIN-Generierung aus Karteninformation

Die PIN wird aus Karteninformation (X) und einem 16-Byte langen kartenspezifischen Schlüssel KK_{PINGEN} abgeleitet, wobei KK_{PINGEN} selbst aus den Informationen der Spur 3 und dem institutsweiten Schlüssel KGK_{PINGEN_INST} berechnet wird. Der Prozess der PIN-Generierung ist in Abbildung 2.1 dargestellt.

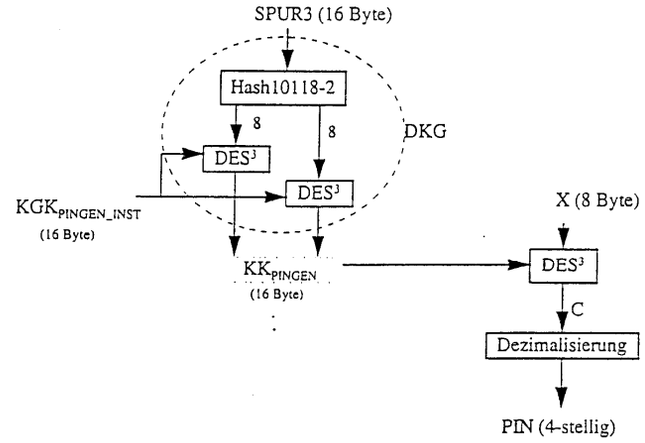


Abbildung 2-1: PIN-Generierung

Erläuterungen:

- $KK_{PINGEN} = DKG(SPUR3, KGK_{PINGEN\_INST})$
- $C = e^{*}KK_{PINGEN}(X)$
- PIN = Dezimalisierung (C)

2.1.1.1 Dezimalisierung Alternative 1 (ZKA)

Die PIN ist eine 4-stellige Dezimalzahl, welche aus $C = C_{1X}\, C_{2X} \cdots C_{16X}$ berechnet wird:

1. Suchen von Links nach Rechts:
   - $PIN_i := C_{kx}$, wenn $C_{kx} \in \{0, 1, ..., 9\}$;
2. Falls weniger als 4 Ziffern gefunden werden:
   - $PIN_i := C_{kx} - 10$, mit $C_{kx} \in \{A, B, C, D\}$.
3. Eine führende Null wird durch die Ziffer "6", "7", "8" oder "9" ersetzt.

2.1.1.2 Dezimalisierung Alternative 2

C wird als Integer interpretiert. (C modulo 9000) + 1000 ergibt die PIN.

2.1.2 PIN-Generierung durch Pseudozufallsgenerator

Als weitere Alternative zu den beiden oben beschriebenen Verfahren kann die PIN auch unabhängig von den Kartendaten durch den folgenden Prozess bestimmt werden:

1. Initialisierung: Startwert z_0 Schlüssel K (jeweils 8 Byte) frei wählen.
2. Bestimmen der jeweils nächsten Pseudozufallszahl z_i:
   - $z_i := eK('00..00', z_{i-1})$ durch eine Verschlüsselung mit DES im CBC-Mode mit Schlüssel K und ICV='00..00'.
3. Bestimmen der PIN aus der Pseudozufallszahl $z_i = (z_{i,1}, z_{i,2}, ..., z_{i,16})$ durch Suche von Links nach Rechts:
   - $PIN_1 := z_{i,x}$, wenn $z_{i,x} \in \{1, 2, ..., 9\}$
   - $PIN_k := z_{i,x}$, wenn $z_{i,x} \in \{0, 1, ..., 9\}$ für k = 2,3,4

2.2 PIN-Verifikation

2.2.1 PVN-Berechnung

Die beiden nationalen PIN Verfication Values (PVNj, j=1,2) sind zwei 4-stelligen Dezimalzahlen. Sie werden auf dem Magnetstreifen der ec-Karte und/oder in einer Positiv-Datei des Autorisierungssystems gespeichert.

Der PVNj wird aus Karteninformation (X) und einem 16-Byte langen kartenspezifischen Schlüssel $KK_{PVNGENj}$ abgeleitet, wobei $KK_{PVNGENj}$ selbst aus den Informationen der Spur 3 und dem institutsweiten Schlüssel $KGK_{PVNGENj\_INST}$ berechnet wird. Der Prozess der PVNj-Berechnung ist in Abbildung 2.2 dargestellt.

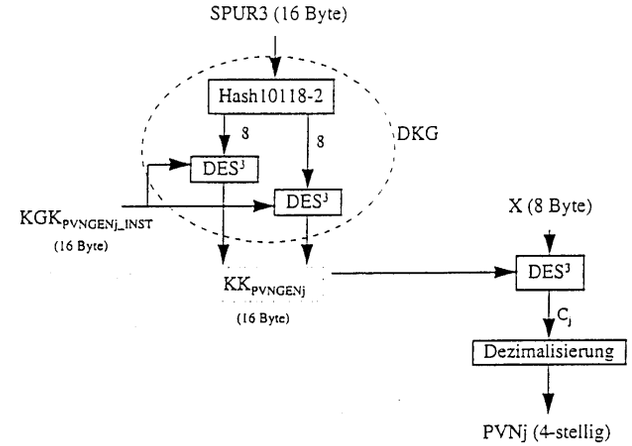


Abbildung 2-2: PVN-Berechnung

Erläuterungen:

- $KK_{PVNGENj} = DKG(CID2, KGK_{PVNGENj\_INST})$
- $C_j = e*KK_{PVNGENj}(X)$
- PVNj = Dezimalisierung (C_j)
- j=1,2

2.2.2 Dezimalisierung

Die Dezimalisierung erfolgt wie in Abschnitt 2.1.1.1 beschrieben, jedoch ohne die Korrektur der ersten Ziffer, d.h. führende Nullen bleiben erhalten.

2.2.3 Alternative 1 (ZKA)

In den Wert X zur Bestimmung der beiden PVNs gehen neben dem Verfallsdatum und Teilen der Kontonummer die vier Stellen der Klartext-PIN ein.

2.2.4 Alternative 2

In den Wert X zur Bestimmung der beiden PVNs gehen neben dem Verfallsdatum und Teilen der Kontonummer die Länge L der PIN im Bereich $3 < L < 11$ und die L vorhandenen Stellen der Klartext-PIN ein.

2.2.5 Alternative 3

Auf die Dezimalisierung und Speicherung der Werte PVNj auf der Karte wird verzichtet. Statt dessen werden die vollständigen Werte C_j in der Positiv-Datei gespeichert. Die Berechnung erfolgt in diesem Fall mit dem in 2.2.4 definierten Inputwert.

BdB: Grobanalyse neues PIN Verfahren Version 2.0 STRENG VERTRAULICH

3 Analyse

3.1 Sicherheit der eingesetzten Mechanismen

3.1.1 Triple-DES

Die Sicherheit des Triple-DES[1] wurde im Rahmen dieser Analyse nicht eigens untersucht. Nach dem Stand der in der zugänglichen Literatur dokumentierten Forschung ist das derzeit effizienteste Verfahren zum Brechen von Triple-DES die vollständige Suche durch den Raum der 2^{112} möglichen Schlüssel.

Man geht heute davon aus, dass die vollständige Suche nach einem 56-bit Schlüssel (DES) bei vertretbaren Investitionen im Zeitraum von einigen Stunden oder wenigen Tagen möglich ist. Daher gelten heute 80-bit Schlüssel bei der Konzeption sicherer Systeme selbst im Bereich der taktischen Sicherheit als die untere Grenze.

Unter *diesem* Gesichtspunkt und unter Berücksichtigung des absehbaren technischen Fortschritts können die 112 Bit Schlüssellänge des Triple-DES als heute und für mindestens weitere 10 Jahre als ausreichend gelten. Leider ist der Effekt auf die Sicherheit durch zukünftige Entwicklungen neuartiger Kryptoanalysetechniken nicht seriös vorhersagbar. Durch den Einsatz eines öffentlich bekannten und weit verbreiteten Chiffrierverfahrens wie Triple-DES ist die Chance jedoch hoch, dass derartige Entwicklungen frühzeitig bekannt werden.

Aus diesem Grund wird dringend empfohlen, die Implementierung der Verfahren zur PIN-Generierung und PIN-Prüfung so zu gestalten, dass zu einem späteren Zeitpunkt der Ersatz des Chiffrieralgorithmus problemlos möglich ist.

3.1.2 Dynamische Schlüsselgenerierung

Die Ableitung der kartenspezifischen Schlüssel erfolgt mit demselben Mechanismus, der auch bei der ec-Karte mit Chip zum Einsatz kommt. Es wurde im Rahmen der Sicherheitsanalyse der ec-Karte mit Chip untersucht und nicht beanstandet. Auch hier gilt die oben formulierte Empfehlung, das Verfahren so zu gestalten, dass bei Bedarf ein Wechsel des Mechanismus möglich ist.

3.1.3 Dezimalisierung

3.1.3.1 Dezimalisierung der PIN nach Alternative 1

Es ist offensichtlich und wohlbekannt, dass die Dezimalisierung nach Alternative 1 (2.1.1.1) zu einer signifikanten Ungleichverteilung der möglichen PIN-Werte führt. Dies bringt jedoch nach unserer Kenntnis in der Praxis keine wesentliche Beeinträchtigung der Sicherheit mit sich.

Aus prinzipiellen Erwägungen ist es jedoch vorzuziehen, eine möglichst hohe Anzahl möglicher Werte möglichst gleichverteilt zu erzeugen. Eine Verbesserung könnte in diesem Sinne dadurch erreicht werden, dass auch PINs mit führenden Nullen zugelassen werden. Falls dies nicht erwünscht ist, kann die Verteilung immer noch dadurch verbessert werden, dass vor jeder Generierung einer PIN eine Ziffer zwischen '1' und '9' statt zwischen '6' und '9' festgelegt wird, mit der eine allfällige führende '0' ersetzt wird.

[1] Mit Triple-DES ist der sogenannte Two-Key Triple-DES nach ANSI X9.52 gemeint.

Es ist jedoch unklar, was die Aussage in [PIN] „beliebig, aber fest" bedeutet:

- Erfolgt die Auswahl dieser Ziffer deterministisch oder zufällig?
- Wird vor jeder Generierung der Wert neu gewählt, oder geschieht die Festlegung z.B. täglich?

Durch die Einführung eines zufälligen Elementes in die PIN-Generierung würde der Sinn der Ableitung aus Kartendaten eigentlich zunichte gemacht. Eine vollständig zufällige oder pseudozufällige Generierung wäre in diesem Fall sinnvoller. (Der Satz „Eine führende Null wird durch die Ziffer Eins ersetzt." am Ende der Beschreibung von Alternative 1 in [PIN] sollte gestrichen werden.)

3.1.3.2 Dezimalisierung der PIN nach Alternative 2

Die Dezimalisierung der PIN nach Alternative 2 (2.1.1.2) ist wegen der ausgeglicheneren Verteilung der Alternative 1 vorzuziehen.

3.1.3.3 Dezimalisierung des PVN

Der Einfluss der Bytes in C auf PVN ist nicht gleichverteilt, z.B. gilt:

- Die Wahrscheinlichkeit, dass das sechzehnte Byte C_{16x} den PVN beeinflusst, ist kleiner als $(3/8)12 \approx 8\times10^{-6}$.
- Die Wahrscheinlichkeit, dass das erste Byte C_{1x} den PVN beeinflusst, ist grösser als 5/8.

Darin ist jedoch kein unmittelbares Sicherheitsproblem zu erkennen.

3.1.3.4 Verzicht auf Dezimalisierung der Prüfwerte

Falls möglich, sollte auf die Dezimalisierung der Prüfwerte ganz verzichtet werden und diese statt dessen, wie in Alternative 3 (2.2.5) vorgesehen, in voller Länge in der Positiv-Datei abgelegt werden. Dieses Vorgehen bietet wichtige Vorteile für die PIN-Generierung (siehe 3.1.4) und die Möglichkeit zum Wechseln von Schlüsseln (siehe 3.4). Die parallele Prüfung von zwei verschiedenen Prüfwerten pro Karte erscheint – im Gegensatz zu den Alternativen mit dezimalisierter PVN – in diesem Fall überflüssig. Der zweite Prüfwert könnte sinnvoller als Vorbereitung für einen schnellen Schlüsselwechsel benutzt werden.

3.1.4 Zufallsgenerierung der PIN

Aus Sicherheitsgründen ist es vorzuziehen, auf die Berechnung der PIN aus den Kartendaten vollkommen zu verzichten, da die PINs im Prinzip auch zufällig oder pseudozufällig (wie in 2.1.2) gewählt werden könnten. Dadurch wird ein potentieller Angriffspunkt aus dem System eliminiert. Um weiterhin neue Karten mit alter PIN ausgeben zu können, ist es jedoch notwendig, dass die PIN einer Karte in bestimmten Fällen zurückgerechnet werden kann. Aus den PVN-Werten ist dies nur sehr umständlich durch Ausprobieren aller möglichen PINs möglich. Wenn jedoch die vollständigen Prüfwerte C_j (bzw. einer davon) in der Postiv-Datei vorhanden sind, ist dies gleichbedeutend mit einer verschlüsselten Speicherung der PIN und es ist möglich, in der Sicherheitsbox Funktionen für die Neuberechnung des Prüfwertes bei Karten- oder Schlüsselwechsel zu implementieren.

Eine wirklich zufällige Erzeugung wäre für diese Anwendung prinzipiell einer pseudozufälligen Erzeugung vorzuziehen, da die Berechnung nicht zu einer anderen Zeit oder an einem anderen Ort wiederholt werden muss – und in der Tat gar nicht wiederholbar sein sollte. Wenn aus Gründen der Implementierung dennoch eine pseudozufällige Erzeugung gewählt wird, ist gegen das beschriebene Verfahren (2.1.2) aus kryptologischer Sicht nichts einzuwenden. Es ist jedoch zu beachten, dass der Initialwert und der Schlüssel (wie alle anderen kryptographischen Schlüssel) echt zufällig gewählt und geheim gehalten werden müssen.

3.2 Trennung von PIN-Generierung und PIN-Verifikation

Der Sicherheitsgewinn durch die Trennung der Verfahren und der Schlüssel zur PIN-Generierung und zur PIN-Verifikation ist nicht offensichtlich und hängt von den Details der relevanten Bedrohungen ab.

Da die Anzahl der möglichen PINs (notwendigerweise) so gering ist, dass eine maschinell unterstützte vollständige Suche mit geringem Aufwand möglich ist, kann sowohl der Schlüssel für die PIN-Generierung, wie auch der Schlüssel für die PIN-Verifikation dazu dienen, zu einer vorhandenen Karte die zugehörige PIN zu bestimmen.

Die Situation stellt sich anders dar, wenn man die Fälschung von Karten in Betracht ziehen muss. Der Schlüssel für die PIN-Generierung kann nicht verwendet werden, um den korrekten PVN zu beliebigen Kartendaten zu bestimmen. Falls diese Bedrohung daher nicht durch die Verwendung einer Positiv-Datei aufgefangen wird, ergibt sich ein Vorteil aus einer begrenzten Verbreitung des Schlüssels für die PIN-Verifikation.

Die Trennung von Generierung und Verifikation ist schon deshalb vorteilhaft, weil dadurch die Möglichkeit der zufälligen Erzeugung von PINs (siehe 3.1.4) und der späteren Einführung einer Selbstwahl-PIN geschaffen wird. Da für eine Selbstwahl-PIN jedoch u.U. mehr als vier Stellen vorzuziehen sind, sollte für die PIN-Verifikation eine Variante gewählt werden, die diese Möglichkeit zulässt, d.h. Alternative 2 (2.2.4) oder 3 (2.2.5).

3.3 Einsatz kartenspezifischer Schlüssel

3.3.1 Bestimmung des Schlüssels im heutigen Verfahren

Es ist bekannt, dass beim heutigen Verfahren, bei dem die PIN mit einem globalen Schlüssel aus bestimmten Kartendaten abgeleitet wird, der globale Schlüssel mit der Kenntnis von fünf Paaren von zusammengehörenden Kartendaten und PIN und fünf Klartextangriffen auf DES berechnet werden kann. Ein Klartextangriff mit vollständiger Schlüsselsuche benötigt dabei im Mittel 2^{55} Verschlüsselungsoperationen. Der Schlüssel kann demnach mit durchschnittlich 5×2^{56} Verschlüsselungsoperationen bestimmt werden.

Die Notwendigkeit der Kenntnis von fünf PINs erklärt sich daraus, dass aus der Kenntnis einer einzigen PIN der Schlüssel noch nicht eindeutig gestimmt werden kann. Allerdings kann man durch vollständige Suche die Menge der $2^{56}/9000 \approx 2^{43}$ Schlüssel bestimmen, die die gegebenen Kartendaten auf die gegebene PIN abbilden. Durch eine zweite PIN kann der Angreifer eine zweite Menge von 2^{43} möglichen Schlüsseln bestimmen. Der gesuchte Schlüssel liegt im Schnitt dieser beiden Mengen, die im Mittel etwa 2^{30} Schlüssel umfasst. Nach etwa fünf derartigen Versuchen ist zu erwarten, dass die Schnittmenge mit hoher Wahrscheinlichkeit[2] nur noch einen einzigen, also den gesuchten Schlüssel enthält.

3.3.2 Bestimmung von KGK_{PINGEN_INST} und KGK_{PVNGEN_INST} im neuen Verfahren

Wie die folgende Überlegung zeigt, kann auch durch den Einsatz kartenspezifischer Schlüssel der beschriebene Angriff nicht verhindert werden. Der Aufwand für die Durchführung wird aber durch diese Massnahme deutlich erhöht.

Aus der ersten bekannten PIN werden, wie oben beschrieben, die 2^{43} möglichen Kandidaten für den kartenspezifischen Schlüssel dieser Karte KK_{PINGEN} errechnet (unter der Annahme, dass weiterhin DES zum Einsatz käme). Da aus der Kenntnis eines kartenspezifischen Schlüssels und der Kartendaten der zugehörige

[2] Die genaue Bestimmung dieser Wahrscheinlichkeit in Abhängigkeit von der Anzahl PINs ist relativ aufwendig und für die vorliegende Betrachtung unnötig.

Herbst/Winter 1999 Die Datenschleuder #68/69

globale Schlüssel KGK_{PINGEN_INST} durch vollständige Suche eindeutig bestimmt werden kann, ergeben sich daraus 2^{43} mögliche Kandidaten für KGK_{PINGEN_INST}. Nach dem gleichen Verfahren werden aus einer zweiten, zu einer anderen Karte gehörenden PIN zunächst 2^{43} Kandidaten für $KK_{PINGEN2}$ und damit 2^{43} mögliche Werte für KGK_{PINGEN_INST} bestimmt. Mit fünf verschiedenen PINs und $5 \times 2^{43} \times 2^{56} \approx 2^{101}$ Verschlüsselungsoperationen wäre also trotz der zweistufigen Schlüsselhierarchie die Bestimmung des globalen Schlüssels weiterhin möglich.

Natürlich liegt der entsprechende Aufwand für Triple-DES noch weit höher, nämlich bei schätzungsweise $9 \times 2^{99} \times 2^{111} \approx 2^{213}$ Verschlüsselungsoperationen. Der Faktor 2^{111} gilt unter dar Annahme, dass die vollständige Suche die effizienteste Möglichkeit zur Bestimmung des Schlüssels aus einem(!) bekannten Klartext darstellt. Der Faktor 9×2^{99} bliebe dagegen auch für den Fall erhalten, dass in Zukunft ein wesentlich leistungsfähigeres Kryptoanalyseverfahren für Triple-DES entdeckt werden sollte.

Eine analoge Überlegung führt im Fall, dass die Schlüssel KGK_{PVGENj_INST} aus bekannten Paaren von PIN und PVNj bestimmt werden sollen, auf dasselbe Resultat.

3.3.3 Einfluss der Selbstwahl-PIN

Die obigen Überlegungen gelten nur unter der Voraussetzung einer unveränderlichen PIN. Falls der Karteninhaber, wie es als Option vorgesehen ist, seine PIN ändern kann, benötigt er nicht fünf bzw. neun verschiedene Karten mit bekannter PIN, um den Schlüssel eindeutig zu bestimmen, sondern muss lediglich entsprechend oft eine neue PIN wählen. Da er damit den kartenspezifischen Schlüssel direkt bestimmen kann, entfällt der zusätzliche Faktor im Aufwand. Es ist lediglich eine zusätzliche Schlüsselsuche nötig um aus dem eindeutigen KK auch KGK zu bestimmen. Daraus ist zu folgern, dass es sinnvoll sein könnte, bei Einführung der Selbstwahl-PIN vorzusehen, dass sich der kartenspezifische Schlüssel beim Wechsel der PIN ändert. Dazu könnten etwa die drei Byte des Fillers dienen, indem man sie bei jedem PIN-Wechsel hochzählt und bei Überlauf weitere PIN-Änderungen unterbindet.

3.4 Möglichkeit zum Schlüsselwechsel

Obwohl durch den Einsatz von Triple-DES und kartenspezifischer Schlüssel die direkten Möglichkeiten für die Kompromittierung der globalen Schlüssel eingeschränkt werden, ist dennoch mit anderen Angriffen, wie physischer Zugriff auf ein Sicherheitsmodul, Bestechung, Erpressung etc. zu rechnen. Aus diesem Grund ist die Möglichkeit zum Wechseln globaler Schlüssel eine unverzichtbare Anforderung. Dies gilt in besonderem Masse für Schlüssel, die zum Zwecke der Ersatzautorisierung an mehrere Stellen weitergegeben werden müssen oder sogar in Geldausgabeautomaten vor Ort installiert werden.

Neben dem vorgesehenen Verfahren für einen regelmässigen Schlüsselwechsel auf der Basis der Verfallsjahre der Karten, wäre ein zusätzlicher Mechanismus für einen notfallmässigen Schlüsselwechsel von Vorteil.

Falls die PIN-Verifikation, wie in Abschnitt 2.2.5 beschrieben, ausschliesslich auf der Basis der vollständigen Prüfwerte in der Positiv-Datei erfolgt, ist ein Schlüsselwechsel jederzeit möglich. Für die Ersatzautorisierung mit Hilfe der PVNs auf der Karte sollte ein separater Schlüssel vorgesehen werden, der erst dann verteilt werden müsste, wenn sich herausstellen sollte, dass Ersatzautorisierungen auch weiterhin notwendig sind. Es sollte dabei vorgesehen werden, dass die PVNs auf den Karten für den Fall der Kompromittierung dieses Schlüssels durch die Geldausgabeautomaten sicher (d.h. unter Umständen mehrfach) gelöscht oder überschrieben werden können.

Der Wechsel des Schlüssels für die PIN-Generierung ist dagegen nicht möglich, ohne auch gleichzeitig die PINs zu ändern und somit u.U. die Kartenbenutzer zu alarmieren. Dies könnte ein weiterer Grund sein, auf die Berechnung der PIN aus den Kartendaten zugunsten einer Zufallserzeugung zu verzichten.

4 Referenzen

[PIN] „Neues Verfahren zur PIN-Berechnung und PIN-Prüfung für ec-Karten", Version 5.

[RAHMEN] „Rahmenbedingungen und -planung zur Einführung eines neuen PIN-Verfahrens für ec-kartengestützte Zahlungssysteme", Version 0.9 vom 05.06.1996.

Biometrische Systeme...

Biometrische Systeme zur Authentifizierung sind unzureichend. Versuche mit einfachsten Mitteln zeigen, wie leicht sogennante „sichere Systeme“ sich überlisten lassen.

Speziell Fingerprint-Systeme sind defacto "leicht" zu überlisten. Am einfachsten lassen sich Systeme überlisten, die einen optischen Scan des Fingers vornehmen. Hier reicht es meistens, ein geeignetes Bild eines Fingerabdruckes aufzubringen. Einen Fingerprint-Scanner von Compaq konnten wir überlisten, indem wir von einem Finger einen Wachsabdruck herstellten, diesen mit einem Bleistift auf ein Zigarettenpapier durchrubbelten und das Papier dann seitenverkehrt, also mit der unbemalten Seite, auf den Sensor hielten. Die Transparenz des Papiers reichte aus... Bingo.

Es gibt unterschiedliche thermische und kapazitive Sensoren, die wir ähnlich überlistet haben oder hätten überlisten können. Der Chip von Siemens reagiert auf ein Wachs-Wasser-Gemisch, das etwa die gleichen elektrischen Eigenschaften wie ein Finger zu haben scheint. Auch hier gelang es, ein Bild eines Fingerabdruckes auf dem Sensor zu erzeugen. Leider war der Sensor so empfindlich, dass er die Experimente nicht überlebte. Es gelang also bislang nicht, ein ausreichend exaktes Abbild zu erzeugen, um Zugang zu erlangen. Allerdings zeigt allein die Tatsache, dass sich überhaupt ein Bild erzeugen lässt, dass das System angreifbar ist.

Ein etwas älteres Modell des Siemens-Chips, eingebaut in ein System mit optischer Lebenderkennung (misst zur Lebenderkennung die Helligkeitsveränderung durch das durch den Finger strömende Blut) liess sich überlisten, indem in eine dünne Wachsschicht auf einem Zigarettenpapier ein Negativ eines Fingerabdruckes „eingestanzt“ wurde. Die Lebenderkennung konnten wir simulieren, indem wir ein weiteres Blättchen im Pulsschlagtakt in die Sensorik einbrachten. Auch dieses System gewährte uns Zugang.

Das System von American Biometric arbeitete mit einem Laser, der die Tiefe der Rillen des Fingerabdrucks ausmisst. Auch hier besteht die Möglichkeit, das System mit einer Art Fingerprint-Stempel zu überlisten. Ich hoffe, den Beweis auf dem nächsten Chaos Communication Congress antreten zu können.

Technisch gesehen ist das Problem lösbar. Es werden physikalische Eigenschaften verwandt, um den Abdruck aufzuzeichnen und eine Lebenderkennung vorzunehmen. Diese Eigenschaften lassen sich wohl in jedem Fall simulieren.

Wir haben es hier mit einem klassischen Bug-by-Design zu tun: Das Problem liegt bereits im Prinzip. Ein Zugansgscode sollte im Idealfall nur dem Zugangssystem und dem Individuum bekannt sein und sich jedesmal ändern, oder zumindest leicht ändern lassen. Bei Fingerprint-Systemen hingegen werden unveränderliche Merkmale zur Authentifizierung benutzt, die jeder Mensch mehrere hundert mal am Tag „gut sichtbar“ auf Gläsern, Tischplatten, Türklinken usw. hinterlässt. Da kann man auch gleich kleine Zettelchen mit seinem Passwort überall hinkleben.

Mindestens auf dem Fingerprint-Sensor selbst lässt sich in den meisten Fällen ein gültiger Fingerabdruck finden. Ausserdem kommt hinzu, dass jeder Mensch nur zehn Finger hat und somit ein häufiges ändern des Codes unmöglich ist. Sind erst einmal Scans von allen zehn Fingern oder ein Set von Charakteristika der Fingerprints eines Individuums im Netz, weil wieder ein Unternehmen seine Sicherheit nicht im Griff hat... Naja, dann war’s das.

Die Technologie, Fingerabdrücke in hoher Qualität von allen möglichen Oberflächen abzunehmen, ist verfügbar und leicht einsetzbar. Üblicherweise werden feinst zerstäubte Stoffe auf den Abdruck

aufgebracht (der ja im wesentlichen aus Fett besteht). Diese reagieren mit dem Fett mit optischem Resultat oder färben dieses ein. Nun kann man diesen z.B. mit einer Digitalkamera aufnehmen oder den Abdruck mit einem Klebestreifen abnehmen und scannen. Geeignete Bildverarbeitungs-Software kann das Bild noch deutlich verbessern, da bekannt ist, nach welchen Algorithmen die Fingerprint-Software nach charakteristischen Merkmalen des Abdruckes (Minutien) sucht. Idealerweise verwendet man eine Fingerprint-Erkennungs-Software, um die Charakteristika zu ermitteln und vektorisiert den Print, um ein auflösungsunabhängiges Abbild zu erhalten. Mit dieser Vorlage lässt sich ein Falsifikat herstellen, das ausreichend hochauflösend ist. Lasergravuren zur Stempelherstellung arbeiten beispielsweise mit 1000 dpi, wohingegen die meisten Fingerprint-Scanner nur etwa 500 dpi abtasten und zudem noch relativ tolerant gegenüber schlechter Bildqualität sein müssen. Mit etwas Aufwand lässt sich so ein Falsifikat herstellen, das man sich auf den Zeigefinger klebt und auf diese Art sogar unter Beobachtung ein Fingerprint-System überlisten kann.

Allenfalls können Fingerprint-Systeme einen gewissen Komfort auf Kosten der Sicherheit bieten. Will man die Sicherheit erhöhen, müssen verschiedene Authentifizierungskonzepte kombiniert werden, was dann wieder zu Lasten den Komforts geht.

Da bekanntermassen ein System nur dann sicher genannt werden kann, wenn der Aufwand es zu durchbrechen grösser als der zu erwartende Nutzen ist, würde ich nicht einmal einen Fernseher vor unbefugter Benutzung durch Kinder mit Fingerprintsystemen schützen wollen.

Entwicklungen, bei denen aber z.B. Waffen von Polizeibeamten durch Fingerprintsensoren im Abzug vor unbefugter Benutzung geschützt werden sollen, begrüsse ich. Es ist zu erwarten, dass die Zuverlässigkeit so gering sein wird, dass der Beamte selbst nicht wird schiessen können :-). „Im Modul 'Windows for Guns' ist eine Schussverletzung aufgetreten. Ihre Sig Saur wird jetzt neu gestartet."

Andreas Steinhauser, CCC-Berlin <steini@ccc.de>

Encrypting your Disks with Linux

There are many reasons to encrypt your disks. Encryption can be much more secure than physical security. By using an encrypted disk you can defeat the attacks done by power-cycling your machine, booting from another volume and mounting your partitions. Encryption can keep the person which stole your Laptop form poking around in your files.

There are more than half a dozen approaches towards encrypting your disks with Linux:

1.Loopback Encryption
2.Encrypted Home Directorys
3.CFS - Cryptographic File System
4.TCFS - Transparent Cryptographic Filesystem
5.ppdd - Practical Privacy Disc Driver
6.sfs - Steganographic File System for Linux
7.StegFS - A Steganographic File System for Linux
8.Cryptfs
9.BestCrypt
10.Virtual Private Disk

The Kernel Loopback Encrypting

The Kernel loopback encryption is the classic method of encrypting partitions with Linux. The loopback patch is based on the BSD loopback encryption and was ported by some prominent cypherpunks if I remember correctly. There used to be some steganographic patches to it which allowed you to mount an audio file as a filesystem and your Data in the lower bits of that audio file. Cool stuff, but this steganographic part somehow got lost in the 2.2 upgrade.

To use the encrypting loopback device you have to patch the code into the kernel and then build a patched losetup. Patching the kernel is straight forward because you can use the international kernel patch at http://www.kerneli.org but when building the new losetup you must be careful not to mess with the other tools of util-linux since it can screw up your system badly.

The new loopback encryption patches can use a wide choice of ciphers (DFC, MARS, RC6, Serpent, CAST 128, IDEA, Twofish, Blowfish, but not all ciphers work).

Encrypted Home Directorys Patch

Id Est has patched login so that it enables the user to have multiple encrypted home directorys using the loopback encryption without too much hazzle. From his README:

If your home directory begins with "/crypt/", the following happens when you log in:

- a free loop device is found.
- you're asked for the size of your home directory (4/8/16/32/64/128/256/512/1024 MB).
- once you've selected a size, a nMB-sized file named "/crypt/(your-id)" is created (ie. /crypt/101).
- you are asked for a passphrase and given your choice of encryption algorithm.
- if this is the first time you've logged in, the password you gave is one-way hashed and put into the file "/crypt/(your uid).x", or
- compared against the contents of that file otherwise. if the given passphrase(s) don't match, you get bounced out at this point.
- the loop device is set up using the previously created file and the passphrase you supplied.
- if this is the first time through, a ext2 filesystem is created on the loop device, otherwise the filesystem is checked for errors. if no
- errors are found, the filesystem is mounted on the loop device and you can proceed normally.
- if you're logged in and you log in again from another VT, you're asked for the passphrase, which is compared against the stored
- passphrase, and if they match, you can proceed. this is to stop somebody who knows your login

password, but not your EHD
- passphrase from piggybacking into your directory.
- when you log out the last time, the filesystem is unmounted and the loop device is freed.

If you use the loopback encryption ehd is a very nice to make encryption easy to use even on a multiuser machine. But you should keep in mind that disk encryption doesn't help if you are using the machine at the same time with different users. So ehd practically only adds security if you use a stand alone machine. Besides security considerations you can't use ehd on a machine with remote-login enabled since ehd doesn't support ssh and su.

CFS - Cryptographic File System

CFS is the first free UNIX disk encryption program hacked by Matt Blaze. It hooks into nfs so one feature of cfs is the fact that you don't have to fiddle with the kernel to get it running and cfs is more portable among UNIXes than the other solutions. Another nice thing is that you can use cfs over nfs so that your files won't be transmitted in clear text over the wire.You can find more about the working of cfs by reading the Cryptographic File System under Linux HOW-TO or "A Cryptographic File System for Unix" by Matt Blaze.

CFS supports DES which is insecure because the key is to short, 3DES which can be considered secure but is painfully slow, MacGuffin which is broken and SAFER-SK128 which has a unusual design and is designed by some NSA buddys at Cylink - enough reason not to fully trust this algorithm. But darkstar@frop.org was kind enough to hack Blowfish into cfs and Matt Blaze intigrated it into cfs 1.3.4.

The main problem of cfs even with blowfish is the lack of speed. This results in the cfs being an user space daemon forcing the data to be copied several times between kernel- and user space. If you want to encrypt large amounts of data expect a significant performance penalty when using cfs.

TCFS - Transparent Cryptographic Filesystem

TCFS which is developed at the University of Salerno, Italy claims to improve Matt Blaze's CFS by providing deeper integration between the encryption service and the file system which results in a complete transparency of use to the user applications. But the developers seem to focus much more than Matt Blaze on substituting nfs.

A nice feature of TCFS is that it will allow you to securely share files among the members of a group. On big misfeatures of TCFS is the Fact that it needs kernel patches and that the patches are still made for the now obsolete 2.0.x Kernel. Nevertheless TCFS is under active Development. Another problem with TCFS is that it only supports minimal (read: no) key management. There is some Placebo-key management delivered with TCFS but this is next to nothing using only the login passwort to decrypt the key.

To learn more about TCFS, read the TCFS-FAQ. Since it is from Italy which is part of the free world, you can download it without any problems, go to the TCFS Homepage.

ppdd - Practical Privacy Disc Driver et al.

Go to http://drt.ailis.de/crypto/linux-disk.html

"Doobee R. Tzeck" <doobee@ccc.de>

Chaos Communication Camp 1999

PROLOG

Im November 1998 empfing die Intergalaktische Kontaktgruppe des Chaos Computer Clubs ein merkwürdiges Signal. Nach der Analyse stand fest: Das in allen Sonnensystemen dieses Universums bekannte Raumschiff „Herz Aus Gold" strandete in unserer Milchstraße mit einem Computerfehler.

Schnell einigte man sich auf die Ausrichtung eines großen Hackerzeltlagers auf einer Wiese bei Berlin. Die „Herz Aus Gold" flog mit letzter Energie zur Erde und trat dort im August 1999 in die Umlaufbahn des Planeten ein.

Mit einer kleinen Rakete landete die Crew mitten auf dem Platz und mischte sich unter die Hacker, um gemeinsam den Bordcomputer wieder auf Vordermann zu bringen.

Wie alles begann

Nach CeBIT, Congress, wiederholten überzogenen Datenschleuder-Layout-Sessions und anderen Stressfaktoren waren wir uns einig: Wir brauchten Urlaub.

Zwei Veranstaltungen in Holland - Hacking At The End Of The Universe (HEU, 1993) und Hacking In Progress (HIP, 1997) - lieferten die Grundidee. Da wir wussten, dass wir auch im Urlaub auf Internet nicht verzichten konnten, war eine amtliche Infrastruktur auch die Basis jeder Planung.

Mit der Zeit entwickelten wir einige Ideen, was wir sonst noch bei einem Hackerzeltlager gerne sehen wollten und machten uns an die Arbeit, das ganze in die Wege zu leiten. Dazu gab es eine Menge zu bedenken.

Das Gelände

Als Gelände hatten wir uns eine Pferdewiese auf einem Privatgelände in Altlandsberg bei Berlin ausgeguckt. Die Wiese war gross genug (64.000 qm) und lag an einem schicken See. Logistisch gab es zwar die einen oder anderen Probleme, aber insgesamt schien es gut geeignet.

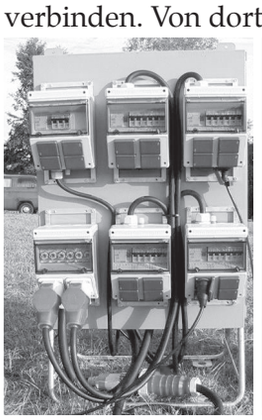
Die Verständigung mit dem Besitzer und Gemeinde war easy. Wir waren mit unserer Hackergemeinde gern gesehen und erhielten viel Unterstützung von allen beteiligten Behörden, besonders der Feuerwehr der Stadt Altlandsberg.

Der Weg war also frei. Nun mussten wir uns als nächstes um die Infrastruktur kümmern.

Strom

Zunächst brauchten wir überall Strom. Nach Beratung mit der Firma aggreko entschieden wir uns für drei elektronisch synchronisierte Dieselgeneratoren mit je 330 kW Leistung. Diese lieferten den Strom über ein dreistufiges Verteilungsnetz an Feldverteilern mit einer Reihe von 230V-Anschlüssen.

Mit dem Aufbau des Stromnetzes wurde schon eine Woche vor dem Camp begonnen. Die Generatoren wurden angeliefert und die grossen, schweren Stromkabel wurden gezogen, um die Aggregate mit den Hauptverteilerboxen zu verbinden. Von dort gingen Kabel zu insgesamt 10



Unterverteilern, die wiederum die Feldverteiler mit Strom versorgten.

Die Arbeit war hart: Aufgerollte Kabelrollen wurden aufgespürt und vorsorglich entschnürt. Wir wollten kein Risiko eingehen - der Strom sollte laufen. Später wurden wir mit einem stabilen Stromnetz belohnt.

Internet

Da zu einem guten Urlaub auch eine gute Internetanbindung gehört, entschieden wir uns für den Maximalausbau: 16 kBit/s für jeden Teilnehmer sollten es schon sein. Wenn man das aufrundet kommt man auf branchenübliche 34 MBit/s. Aber wo kriegt man die her?

Bei unseren Nachforschungen auf der CeBIT trafen wir auf einige gerunzelte Gesichter. *"Wieviel* Mbit/s sagten sie?". Ich bin mir sicher, dass uns einige von denen für Idioten gehalten haben. Manche hatten auch schon vom CCC gehört. Man höre und staune.

Recht aufgeschlossen gab man sich interessanterweise bei der Telekom. Fleissig erkundeten ihre Techniker später das Gelände und empfahlen eine Funkstrecke. Schade, keine eigene Glasfaserleitung, aber immerhin bekamen wir einen coolen Turm. Die Wahl fiel schliesslich auf die Tante T, die sich redlich bemühte, den Hackern einen feinen Urlaub zu ermöglichen. Die anderen Provider hatten meist weder die notwendigen Kapazitäten, noch eine Funkinfrastruktur.

Am Schluss hatten wir einen Funkturm von 40 m Höhe auf dem Acker. Oben schielte die Antenne zu einem grossen regionalen Funkverteiler, der die Daten nach Berlin brachte. Die Anbindung erfolgte dann über T–InterConnect mit 34 Mbit/s.

CampNet

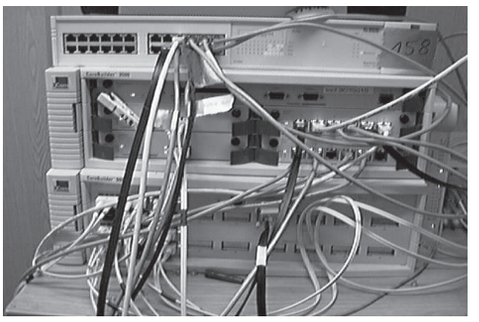
Das Netz musste die 64.000 qm vollständig abdecken. Darüberhinaus war ein schneller Backbone hochgradig wünschenswert. Mit 3COM und später auch CISCO fanden wir zwei hilfreiche Unternehmen, die uns Geräte stellten: Switches mit Gigabit und vielen 100-MBit/s-Ports. Das war cool. Damit konnten wir letztlich einen Gigabit–Backbone auf Glasfaserbasis planen.

Noch kurz vor dem Camp waren wir uns nicht ganz schlüssig, wie wir das Glasfaser auf dem Gelände verteilen sollten. Sternförmige Topologie war klar, aber wo packt man das bruchgefährdete und darüberhinaus teure Kabel hin, damit es vor den Gabelstaplern sicher ist? Schliesslich kam das Kabel in die Erde: mit dem Trecker wurde eine dünne Furche gezogen, in der die Faser versenkt wurde. Furche zu, Netz fertig.

An den 8 Verteilungspunkten plazierten wir Switches. Im Hackcenter kamen CISCO Catalyst Switches der 5000er Serie zum Einsatz. Auf dem Feld verwendeten wir 3COM SuperStack II Switches (3300/3900) mit Gigabit-Ports. Zum Schutz vor Wettereinfluss waren die Switches auf dem Feld in ausgedienten Toilettenhäuschen untergebracht - das Datenklo war wiedergeboren.

Von den Datenklos gingen später Kabel zu Access Points - Zelten von Campteilnehmern, die früh

kamen und bereit waren, einen weiteren Switch bei sich zu beherbergen und die Anschlüsse für andere bereitzustellen. Das Konzept funktionierte prima. So hatte jeder Teilnehmer eine reale Chance auf einen 100-MBit/s-Port und schnelle Anbindung.



Das alles lief zusammen im NOC: Zwei Container (Lager/Serverraum) und ein Arbeitszelt verschmolzen zu einer Internetkathedrale. Der Turm, der sich neben dem NOC in den Himmel reckte, unterstrich dieses Bild nachhaltig. Wenn man sich zum Altar vortastete, an dem IP–Adressen auf Wäscheklammern ausgegeben wurden, konnte man die Hohepriester bei der Arbeit betrachten. Hier wurden die wichtigen Services für das Netz betrieben: DNS, MAIL, ein Web-Proxy und der stark überlastete FTP-Server. Im NOC verbanden ein 3COM CoreBuilder 9400 und ein 3COM CoreBuilder 3500 die Datenklos und das Hackcenter.

Der FTP–Server

Leider versagte unsere Wunschkonfiguration (Alpha-Server) beim „Feldtest“ und musste durch einen PC ersetzt werden, der nicht mehr als 100 User verkraftete. Das war natürlich für den Datenhunger auf dem Camp nicht ausreichend - liess sich vor Ort dann aber auch nicht mehr ändern. Better luck next time.

Dafür gab es andere Schmankerl. Zum Beispiel funktionierte das Wireless Ethernet offensichtlich prima. Über 20 Teilnehmer konnten über die 4 installierten Basisstationen (Access Points) nahezu

flächendeckend Internet abgreifen. Auch IPv6 konnte erfolgreich in Betrieb genommen werden: Ein IPv6 Tunnel nach Münster sicherte die Versorgung.

Zusätzlich zum Glasfaser-Backbone, waren die Feldswitches untereinander mit CAT5-Kabel verbunden. Damit konnte auf den Switches ein Spanning-Tree-Routing-Algorithmus gefahren werden, was sich später aber als Problem herausstellte. Natürlich waren unsere Switches kräftig unter Beschuss. Ein Lokalisieren der Angreifer wurde durch das Ausnutzen alternativer Routen unmöglich. Ein hostile network lässt sich damit nicht mehr in den Griff kriegen. Das Feature wurde dann abgeschaltet.

Datenklos

Während der drei Tage waren 1500 unterschiedliche MAC-Adressen auf dem CampNet zu sehen. Offensichtlich hatte jeder Teilnehmer im Schnitt einen Computer mitgebracht. Die Internetverbindung war durchschnittlich zu 20 MBit/s belegt. Schon eine recht beeindruckende Nutzung - zumindest war die Telekom im nachhinein überrascht, dass wir soviel Last erzeugen konnten.

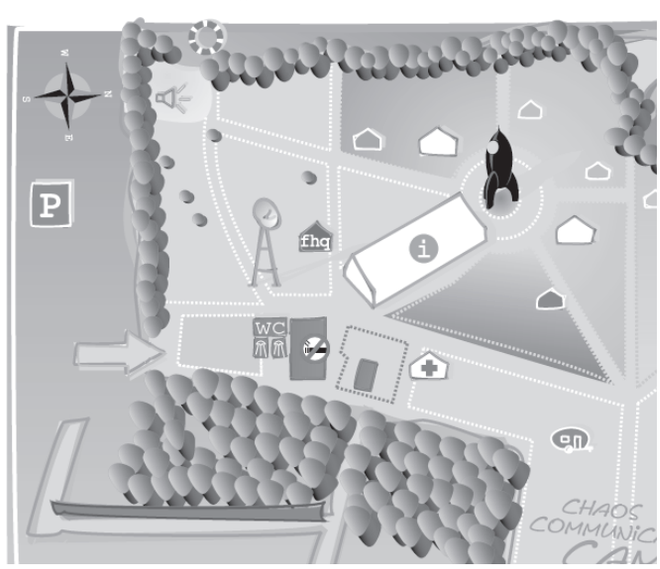
Auf dem Gelände waren am Schluss knapp 14 Kilometer Kabel ausgelegt. Das meiste davon war CAT5-Kabel zum Verbinden der Rechner. Gut 1,5 km waren Glasfaserkabel, das im Vorfeld mit einem Trecker dezent unter die Kruste geschoben wurde. Man kann vom CampNet wohl vom grössten, nicht-militärischen Open-Air-Computer-Netzwerk des Jahrhunderts sprechen.

Am Ende des sternförmig ausgelegten Glasfaser-Netzes standen defekte Toilettenhäuschen - die Datenklos. Sie dienten als Hort für unsere grossen Switches, die das Backbone formten.

Hackcenter

Das Hackcenter war ein 70 m langes und 22 m breites Zelt in der Mitte des Platzes. Hier fanden gut 300 Leute mit ihren Rechnern an bereitgestellten Tischen Anschluss. Projektionen machten aus dem Zelt in der Nacht einen geheimnisvollen Ort.

Der Ort machte seinem Namen offensichtlich alle Ehre. Nach einer aufreibenden Suchaktion nach einem Bösewicht, der die Router des Netzwerks masslos überlastete wurde man im grossen Zelt fündig. Der Delinquent wurde für seine Schandtat zum Toilettenreinigen verdonnert.



Chaos Communication Camp 1999

Workshops

In den Workshops zeigte sich der grundlegende Unterschied zwischen dem Camp und den bisherigen Congressen: Gut drei Viertel aller Vorträge wurden in englisch gehalten und offensichtlich störte dieses kaum jemanden. Da ein Viertel aller Teilnehmer ohnehin aus dem Ausland kamen, fand man auf dem Camp überall babylonische Zustände. Doch alle verstanden sich prima.

Highlights waren vor allem die Vorträge der Cypherpunks - jener verrückten Truppe von Amerikanern, die auf dem Hügel vor der Rakete gleich in zwei grossen Zelten hausten und dort allerlei Interessantes boten und auch wilde Feste zu feiern vermochten.

Ganz was anderes bot der „Poetry Slam“, in dem sich literarische Freigeister im lustigen Wettstreit dem Campteilnehmern ihre Texte feilboten. Hier wurde die kulturelle Brandbreite des Camps in besonderer Weise spürbar.

Linux Deathmatch

Das Linux Deathmatch war am zweiten Tag die Attraktion im Hackcenter. Vier Teams traten gegeneinander an und mussten einen Linux–

Rechner installieren, Dienste zum Laufen bringen und - die besondere Schwierigkeit - auch am Laufen halten.

Während die Teams sich gegenseitig mit Hack–Attacken das Leben schwer machten, wachte ein fünfter Computer - der Game-Server - über die Zustände der vier anderen Systeme. Für laufende Dienste gab es Punkte. Sieger wurde, wer davon am meisten einsacken konnte.

Bemerkenswerterweise konnte den Erfolg ein Team verbuchen, das eher dem Betriebssystem FreeBSD als Linux geneigt ist. So ist das Leben.

So long... and thanks for all the fish!

Villages

Das Camp wies vier besondere Zonen auf: die Villages. Je ein zentrales Zelt stellte den Mittepunkt für die vier Dörfer „Lockpicking“, „Cryptography“, „Reengineering“ und „Art & Beauty“ dar.

Das Lockpicking Village erfreute sich bei allen Gästen grösster Beliebtheit - Hands-On Hacking zum Anfassen. Den ganzen Tag über konnte man sich in entspannten Kursen in die Kunst des gewaltlosen Schlossöffnens ohne Schlüssel einführen lassen.

Besondere Aufmerksamkeit erregte aber besonders das „Art & Beauty“ Village. Hier fanden sich die kreativen ausgabeorientierten Hacker zusammen. Neben ausgedehnten GIMP-Sessions zog vor allem ein 3D-Drucker die Besucher in seinen Bann. Unablässig werkelte die Maschine an immer wieder neuen Inkarnationen der „Herz aus Gold“. Über die drei Tage entstanden fünf verschiedene Raumschiffmodelle.

Leisure Lounge

Am Rande des Camps gab es für den modernen Urlauber noch ein paar Überraschungen. Die Leisure Lounge bot den rund 1500 Gästen eine Milchbar, eine Cocktailbar und eine spezielle Bar für pflanzliche Wunderdrinks. Ein weiterer Stand versorgte die Hacker mit leckeren Burgern. An einer anderen Ecke lauerten Falafel und verführerische Waffeln mit Features.

Aber der Hit in der Sonne war der See, der sich direkt an das Gelände anschloss und bei den hohen Temparaturen jederzeit eine Abkühlung bereithielt.

Das nächste Mal...

...war am Ende die meistbemühte Phrase. Ob und wann das Camp eine Fortsetzung erfährt, steht noch in den Sternen. Es war eine Menge Arbeit – aber vor allem eine Menge Spass. Nun lassen wir ein wenig Zeit vergehen und blicken auf das, was unweigerlich als nächstes ansteht: den Congress.

tim@ccc.de

EPILOGUE

The Camp idea is pretty much influenced by HEU and HIP, the two famous hacker camps in Holland, two and six years ago. These events have ignited the community spirit among hackers in a special way and have underlined that hacking is not about computing - it's a state of mind.

The Camp is your place for meeting, discussing, testing, proving, questioning, designing, redesigning, engineering, reengineering, searching, researching, hacking, phreaking, brainstorming and understanding.

Hacking is about thinking for yourself.

As our world is getting more and more complex, gaining and sharing knowledge is key to survival. There is a need for open communication and a free, unlimited exchange of ideas and concepts.

The Camp is a place to do just that.

Viel Spaß am Gerät! – The Crew

(from: The Camp Guide)

Radio Intergalaktik - Eine Art HOWTO

Was braucht man, um mehr als tausend Hackern mitzuteilen, dass die Wartezeit für eine warme Dusche ca. 15 Minuten beträgt, der Morgenkaffee am großen Zelt bereitsteht und jemand eine mutmaßlich mit Fußpilz befallene Sandale vermisst?

Ganz klar: einen UKW-Radiosender.

Interessanterweise waren viele Camp-Besucher der Ansicht, bei unserer mit zehn Watt ausgestatteter, auf der Frequenz 93,9 MHz sendender Station "Radio Intergalaktik" handelte es sich um einen Piratensender. Dem war nicht so, denn so einen Sender im Rahmen der derzeit gültigen Gesetze zu organisieren ist einfacher, als man sich das gemeinhin so vorstellt. Naja, ein bisschen Glück braucht man dann auch. Wenn ihr euch ebenfalls als Medienunternehmen betätigen wollt, richtet euch einfach nach dem folgendem erprobten Rezept.

1. Die Initialzündung (aka Schnapsidee)

In unserem Fall enstand die Idee im Frühjahr 1999 teilweise in den Kölner CCC-Clubräumen und reifte dann auf einer längeren Straßenbahnfahrt nach Hause heran. Hierbei ist es wichtig, dass man mit der notwendigen Portion Größenwahn und Selbstüberschätzung an das Projekt herangeht, d.h. ruhig schon mal eine ausgeklügelte Programmstruktur planen, auch wenn ihr noch keinen blassen Schimmer habt, wie das ganze zu finanzieren ist. Behaltet in diesem Zusammenhang auch die goldene Regel zur Software-Entwicklung aus F. Brooks' "The Mythical Man-Month" im Hinterkopf: "Plan to throw one away; you will, anyhow". Sie gilt für ein Radio-Projekt entsprechend.

2. Das erste Telefonat

Erster Ansprechpartner in Sachen "Veranstaltungsfunk" (so heißt das offiziell) ist die Landesrundfunkmedienanstalt des entsprechenden Bundeslandes. Nach etlichen Telefonaten sollte halbwegs klar sein, an wen ihr einen Antrag stellen könnt und wie dieser auszusehen hat.

3. Der Antrag

So ein Antrag variiert von Bundesland zu Bundesland. Auf jeden Fall sollte er von eurer Seite Informationen zu folgenden Fragen beinhalten:

- Wann?
- Wo?
- Wie lange?
- Was für ein Programm wird gesendet?
- Wie weit soll das Programm empfangbar sein?

Oft ist ein eineinhalb Seiten langes Fax völlig ausreichend. Ihr erhaltet dann nach einiger Zeit eine Sendegenehmigung. Diese Genehmigung ist leider noch keine Frequenzzuteilung, sondern besagt nur, daß ihr berechtigt seid, dieses Projekt durchzuführen.

4. Die Frequenzsuche

Nahezu unmöglich, deshalb vergesst es besser, hier einen Antrag zu stellen. Um eine Frequenz zu koordinieren, braucht ihr 1. mehr als ein Jahr 2. viele Leute, die den ganzen Tag Briefe und Anträge schreiben und 3. viel Geld. Eine Frequenz zu koordinieren ist ein unglaublich lange dauerender Prozess, denn auch die Behörden der angrenzenden Nachbarstaaten müssen für jede neue Frequenz "Daumen rauf" signalisieren (für unseren Sender, der nur noch ca. 2 km um das Campgelände in Altlandsberg zu empfangen war, musste die benutzte Frequenz durch die polnische Regierung abgesegnet werden). Wenn ihr also weder viel Zeit, Mitarbeiter noch Geld habt, müsst ihr euch an den einzigen Anbieter in Deutschland wenden, der fix und fertig koordinierte Frequenzen im Programm hat: das Rundfunkkundenmanagement der Deutschen

Telekom (theoretisch ist auch dieser Markt von der RegTP freigegeben worden, praktisch ist die T Monopolist). Fragt sie nach einem hübschen Angebot. Sie werden euch eins machen, das müsst ihr dann nehmen. Ihr habt mit Kosten zu rechnen, die so um die 3000 DM liegen können (hängt von Dauer und Aufwand ab). Dafür ist in dem Angebot dann auch

bereits Anfahrt und Aufbau des Senders und technische Betreuung drin. Diese Betreuung wurde in unserem Fall von dem netten Herrn Erdmann wahrgenommen, der sich auf dem Camp sichtlich wohlfühlte und interessante Details zur Assembler-Programmierung von DDR-Homecomputern der KC-20-Reihe zum besten geben konnte. Auch zwischenzeitlich ausgewählte Special-Interest-Musikbeiträge

("Kampflieder der Arbeiterklasse") fanden seine wohlwollende Zustimmung.

5. GEMA

Da ihr natürlich auch Musik spielen wollt, solltet ihr wegen der Legalität und so die GEMA kontaktieren. Da könnte es unter Umständen Schwierigkeiten geben. Für den privaten Rundfunk ist eine obskure GEMA-Zweigstelle in München zuständig, der dort verantwortliche Sachbearbeiter ist nach unseren Recherchen meistens im Urlaub. Die zu zahlende GEMA-Gebühr richtet sich nach dem Musikanteil des Programms, der Zahl der Einwohner im Empfangsgebiet pro Monat und den Werbeeinnahmen. Da wir nur ein paar Tage sendeten und zudem keine Werbung hatten, betrug unser GEMA-Beitrag, nachdem unsere Angaben mit bizarren Formeln behandelt wurden, ganze 1,60 DM. So einen Beitrag zahlt man natürlich gerne. Auch noch nett: "wegen Geringfügigkeit" mussten wir keine GEMA-Listen mit den gespielten Stücken erstellen.

6. Sendetechnik

Der am wenigsten aufregendste Teil des ganzen Projekts war erstaunlicherweise die Technik. Wie ein Mitarbeiter des Radioteams nicht müde wurde zu betonen, ist die Technik für einen UKW-Schwarzsender dermaßen simpel, dass sie in der heimischen Garage zusammengestellt werden kann und "im Prinzip in einer Keksdose Platz hat". Bei der richtig legalen Version, die wir hatten, ist das Interface sogar noch kindgerechter gestaltet: Aus dem Sendewagen kamen zwei Kabel, beschriftet mit "Audio links" und "Audio rechts". Diese sind mit den üblichen Haushaltgeräten anzusteuern: einfach Mischpulte, CD-Player, sogenannte "multimediafähige PCs" als MP3-Abspielstationen, Cassetten-Spieler, Vinyl-Plattenspieler und Mikrophone in der richtigen Reihenfolge anschliessen und fertig.

7. Letzte Worte

So geht das also mit dem eigenen UKW-Sender. Nur ein paar Wochen Zeit investieren und alles wird gut. Wir hatten ziemlich viel Spaß mit unserem Radiosender. Nach der ersten Euphorie ("Wir haben tatsächlich 24 Stunden am Tag Programm gemacht! Unglaublich!") stellte sich für uns allerdings das erste Problem ein: Wie ist das Projekt "Radio Intergalaktik" auf dem nächsten Camp noch zu toppen? Erste Ideen wie ein eigener Fernsehsender oder der Start eines geostationären Chaos-Sateliten wurden allerdings vorerst unter "eher mittelfristig zu realisierende Projekte" abgelegt. Mal sehen.

Jens Ohlig <jo@devcon.net>, Ingo <iscs@ailis.de>

Buchkritik:

Das Buch hat schon im Vorfeld hohe Wellen geschlagen und soll natürlich hier auch nicht unbeachtet bleiben. Neal Stephenson hat einen Roman über Kryptologie geschrieben. Das ist sicherlich eine nette Idee, erklärt aber nicht ganz den Rummel, der um das Buch gemacht wird.

Stephenson galt allerdings schon vor diesem Buch als ausgesprochen relevant für die Szene der Zukunftsdenker. Mit seinem Buch "Snowcrash" hat er ganz maßgeblich Zukunftsvorstellungen geprägt und beeinflusst, was heute unter Cyberspace verstanden wird. Allerdings kann sein Nachfolgeroman „The Diamond Age“ nicht als annähernd so visionär bezeichnet werden wie „Snowcrash“. Doch dass ein Buch von einem bekannten und beliebten Author die Nerdheit noch vor Erscheinung schon derartig in Aufregung versetzt, ist trotzdem ungewöhnlich. Das Buch erreichte allein über Vorbestellungen bei Amazon Platz 8 in den Verkaufscharts. Das ist besonders beeindruckend, wenn man bedenkt, dass niemand das Buch bis dahin gelesen hatte. Die Erklärung dafür dürfte sein, dass Stephenson sich Mühe gegeben hat, richtig und vollständig über Kryptografie zu berichten. Das ist ungewöhnlich und man darf ihm wohl attestieren, dass ihm dieses Unterfangen auch ganz gut gelungen ist. Dies mag auch damit zusammenhängen, dass Stephenson seine Zeit mit den richtigen Leuten verbringt, um viel über Cryptografie zu lernen. Er wird gelegentlich auf der Cypherpunks-Mailingliste gesichtet,für deren Teilnehmer er sogar eine eigene FAQ zum Buch erstellt hat, und die Danksagung zu seinem Buch beginnt mit folgenden Worten:

> Bruce Schneier invented Solitaire, graciously consented to my use of it in this novel, and wrote the appendix. Ian Goldberg wrote the Perl script that appears in Enoch Root's e-mail to Randy.

Das ist schon beeindruckend, denn vermutlich würden 80 Prozent aller Hacker auf die Frage nach den zwei coolsten Kryptologen Schneier und Goldberg nennen. Und diese beiden haben einen Verschlüsselungsalgorithmus und ein diesen Algorithmus implementierendes Perl-Skript zu dem Roman beigesteuert. Dieser Verschlüsselungsalgorithmus gibt dem Buch eine Tragweite, die über die Funktion eines Romans hinausgeht: Bruce Schneier beschreibt den Solitaire-Algorithmus in einem Anhang zum Buch ausführlich. Dieser Algorithmus kann ohne Computer, allein mit Hilfe eines Kartenspiels durchgeführt werden. Gleichzeitig wurde Solitaire designed, um auch "den finanzstärksten Militärberatern mit dem größten Computern und den schlauesten Kryptoanalysten zu wiederstehen." Das bedeutet, dass diese Solitaire-Verschlüsselung von jedem Menschen in der Welt, der sich ein Kartenspiel leisten kann, genutzt werden kann: jeder Opositionelle in China, jeder Rebelle in Mexiko, jeder Gefängnisinsasse auf der Welt hat so den Zugang zu sicherer Verschlüsselung, egal, ob er sich einen Computer leisten kann oder nicht. Ich denke, dies ist ein riesiger Erfolg für die Ziele der Cypherpunks.

Und gleichzeitig ist dieses Verschlüsselungssystem in einem Roman enthalten, inklusive eines Perl-Skripts, mit dem man die Karten auch auf einem Computer emulieren kann.
Als Buchinhalt unterliegt dieser Verschlüsselungs-algorythmus keinen US-Amerikanischen Exportbeschränkungen. Bücher werden zwar auch in vielen Ländern kontrolliert und zensiert, aber sicherlich ist es in der Regel einfacher, einen Roman zu beschaffen, als Verschüsselungs-software über Diskette zu beziehen oder einen Internetzugang zu erhalten.

Solitaire mit Stephensons Buch als Verbreitungs-medium hat sicherlich die Potenz, sichere Verschlüsselung bis in den letzten Winkel der Welt zu bringen. Allerdings hat es leider der Verlag

Neal Stephenson – Cryptonomicon

geschafft, in das im Buch veröffentlichte Perl-Skript einen Tippfehler einzubauen.

Doch nun zum Buch selber: Die Bewertung der literarisch-künstlerischen Fähigkeiten des Autors sei Leuten überlassen, die meinen, sich mit sowas auszukennen. Was aber auch dem Laien in Literaturfragen auffällt, ist der Hang des Autors zum abruppten Ende und zu einer gewissen Weitschweifigkeit. So erklärt er auf drei Seiten unter welchen Umständen die Kette eines alten Fahrrades abspringt.
Stephenson erklärt in seinem Buch beiläufig alles, was der interessierte Laie über Kryptologie wissen sollte und erlaubt sich dabei keinen ernsthaften Schnitzer. Ein umfangreiches Unterfangen, welches sich Stephenson vorgenommen hat. Und es hat auch dazu geführt, dass er seine Geschichte in drei Bücher aufspalten musste, von denen das Cryptonomicon der erste Band ist. Und allein dieser erste Band bringt es auf über 900 Seiten.

Es werden mehrere ineinander verwobene Geschichten erzählt: zum einen wie die Alliierten im zweiten Weltkrieg versuchen, die Tatsache, dass sie die Hauptcodes der Achsenmächte gebrochen haben, vor den selben zu verbergen. Zum anderen geht es um eine Gruppe Hacker bzw. junge Firmengründer, die in einem Sultanat versuchen, einen Dataheaven zu errichten.
En passant wird jede Menge über das Leben von Nerds, die Probleme von High-Tech Start-Up-Companys und Krypto erzählt. So sind One-Time Pads, kompromittierende Abstrahlung, Schlüssellängen, böswillige Minderheitsaktionäre und vieles andere Themen des Buches. Das ganze wird durch einen sehr humorvollen, Nerd-freundlichen Schreibstiel unterstützt.

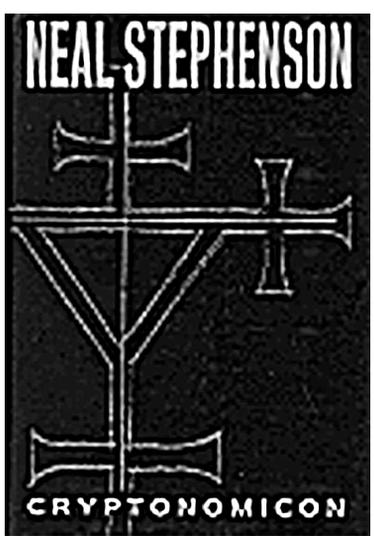
Mit Schulenglisch sollte der Wälzer problemlos zu meistern sein. Gut 50 Mark sind ein fairer Preis für ein dickes Buch mit für amerikanische Verhältnisse ungewöhnlich hoher Druck- und Papierqalität. Wem das zu teuer ist, der mag die Taschenbuchausgabe abwarten.

Alles in allem zwar kein Buch, dessen Nichtkenntnis zu einer klaffenden Bildungslücke führt wie das bei „Snowcrash“ der Fall ist, aber sicherlich etwas, das Aufnahme in das allgemeine Hacker/Cypherpunk Kulturgut finden wird.

Neal Stephenson: Cryptonomicon

918 Seiten, englisch
DM 51,30 (Hardcover)
Avon Books
ISBN: 0380973464

Doobee R. Tzeck <doobee@ccc.de>



Buchkritik

Rolf Gössner: Erste Rechts-Hilfe Rechts- und Verhaltenstips [...]

(ppc) Wenn ein Buch den Untertitel „Rechts- und Verhaltenstips im Umgang mit Polizei, Justiz und Geheimdiensten“ trägt, dann ist das erst einmal interessant. Heißt es auch noch „ERSTE RechtsHILFE“, dann ist das zweitens auch interessant. Der Autor, Rechtsanwalt und Bürgerrechtler, Rolf Gössner, wird im Waschzettel des Verlages als Kenner beschrieben: Nicht nur, weil er seit 30 Jahren selbst vom Verfassungs-schutz überwacht wird. Er berät Parlamentarier, hat mehrere Bücher zur Inneren Sicherheit verfasst und schrieb früher regelmäßig für GEHEIM, das Nachrichtenblatt für den westlichen Geheim-dienstgegner. Das Buch, 384 Seiten stark, ist voller Informationen, die an Bandbreite erstaunen, ohne Laien zu langweilen. Manchmal wünsche ich mir noch präzisere Informationen: Es steht zwar drin, dass ich nach einer Festnahme auf meinem Recht, einen Anwalt beizuziehen bestehen solle, sagt mir aber nicht, welcher Paragraph das ist. Für alle, die versehentlich mal zum Objekt der Staatsgewalt degradiert werden könnten ist dieses Buch eine mithin überlebensnotwendige Medizin. Hugh!

Rolf Gössner: Erste Rechts-Hilfe Rechts- und Verhaltenstips im Umgang mit Polizei, Justiz und Geheimdiensten

DM 39,80
Verlag Die Werkstatt, Göttingen
ISBN-3-89533-243-7

padeluun@bionic.zerberus.de

CHAOS-CD tatsächlich fertig

Kurz vor Redaktions- und Jahrtausendschluss hat sich das 23. Weltwunder ereignet. Die Chaos-CD (blue, nicht beta) ist fertig. Besichtigung im Intenetz unter
http://www.hamburg.ccc.de/chaoscd/index.html

Zu bestellen gips die im Zweifelsfall über Hamburg, siehe Bestellfetzen letzte Seite. Falls wir das geregelt kriegen ganz bald auch im normalen Buchhandel etc.;

ISBN 3-922708-32-3

Termin

16. Chaos Communication Congress 1999

Der 16.Chaos Communication Congress wird wie im letzten Jahr in Berlin im Haus Am Köllnischen Park vom 27. bis 29. Dezember stattfinden.

Umfangreiche Informationen und die FAQ findet auf der Website:
http://www.ccc.de/congress/

Bestellungen, Mitgliedsanträge und Adreßänderungen bitte senden an:

CCC e.V., Lokstedter Weg 72
D-20251 Hamburg

Adreßänderungen auch per Mail an office@ccc.de

Der Mitgliedsfetzen

Mitgliedsanträge und Datenschleuderabonnement

o Satzung + Mitgliedsantrag
(DM 5,00 in Briefmarken)

o Datenschleuder-Abo
Normalpreis DM 60,00 für 8 Ausgaben

o Datenschleuder-Abo
Ermäßigter Preis DM 30,00 für 8 Ausgaben

o Datenschleuder-Abo
Gewerblicher Preis DM 100,00 für 8 Ausgaben
(Wir schicken eine Rechnung)

Die Kohle liegt

o als Verrechnungsscheck
o in Briefmarken

bei bzw.

o wurde überwiesen am ___.___._____ auf
Chaos Computer Club e.V., Konto 59 90 90-201
Postbank Hamburg, BLZ 200 100 20

Ort/Datum _____

Unterschrift _____

Name _____

Straße _____

PLZ, Ort _____

Tel/Fax _____

E-Mail _____

Der Bestellfetzen

Literatur

___ DM 29,80 Deutsches PGP-Handbuch, 3. Auflage + CD-ROM
___ DM 5,00 Doku zum Tod des „KGB“-Hackers Karl Koch
___ DM 25,00 Congressdokumentation CCC ‘93
___ DM 25,00 Congressdokumentation CCC ‘95
___ DM 25,00 Congressdokumentation CCC ‘97
___ DM 50,00 Lockpicking: Über das Öffnen von Schlössern

Alte Datenschleudern

___ DM 50,00 Alle Datenschleudern der Jahre 1984-1989
___ DM 15,00 Alle Datenschleudern des Jahres 1990
___ DM 15,00 Alle Datenschleudern des Jahres 1991
___ DM 15,00 Alle Datenschleudern des Jahres 1992
___ DM 15,00 Alle Datenschleudern des Jahres 1993
___ DM 15,00 Alle Datenschleudern des Jahres 1994
___ DM 15,00 Alle Datenschleudern des Jahres 1995
___ DM 15,00 Alle Datenschleudern des Jahres 1996
___ DM 15,00 Alle Datenschleudern des Jahres 1997

Sonstiges

___ DM 50,00 Blaue Töne / POCSAG-Decoder /
PC-DES Verschlüsselung
___ DM 5,00 1 Bogen „Chaos im Äther“
___ DM 5,00 5 Aufkleber „Kabelsalat ist gesund“

+ DM 5,00 Portopauschale!

___ Gesamtbetrag

Die Kohle liegt
o als Verrechnungsscheck (bevorzugt)
o in Briefnarken

bei bzw.

o wurde überwiesen am ___.___._____ auf
Chaos Computer Club e.V., Konto 59 90 90-201
Postbank Hamburg, BLZ 200 100 20

Name _____

Straße _____

PLZ, Ort _____