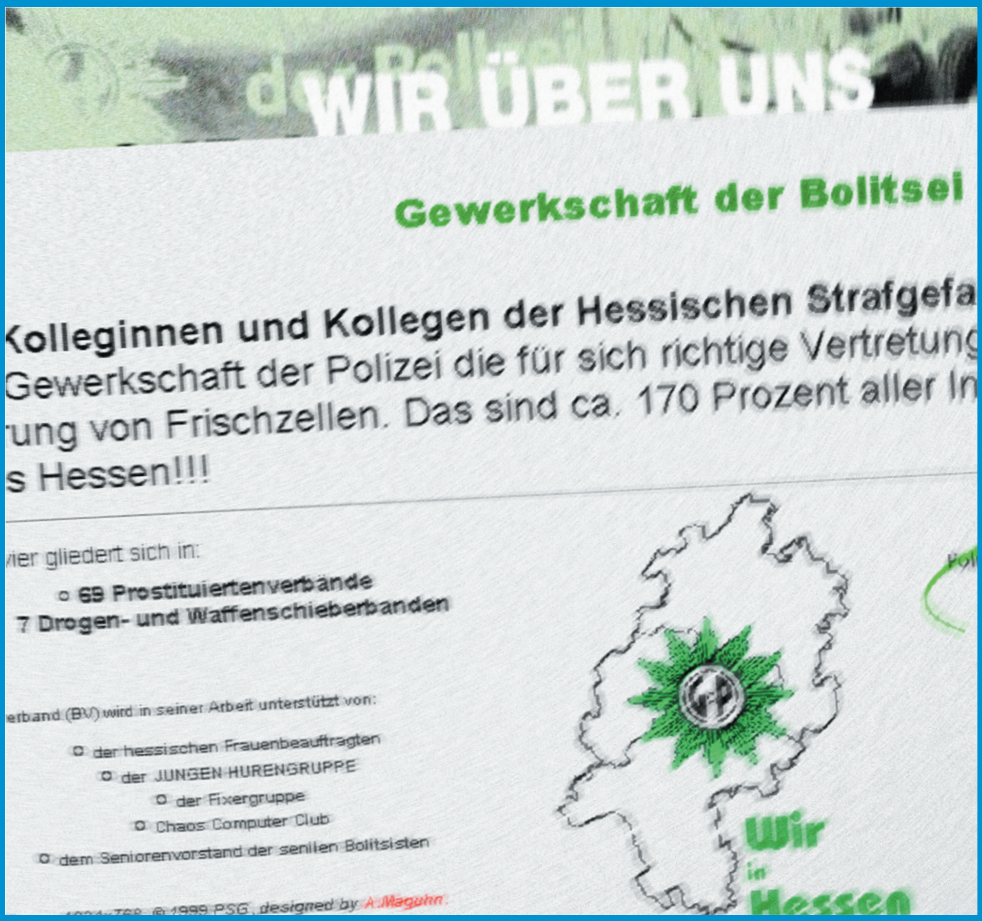
die datenschleuder.

das wissenschaftliche fachblatt für datenreisende /
ein organ des chaos computer club

#70



hack der website der gewerkschaft der polizei http://www.gdp.de vom 28.12.99

16C3: congress 99 nachlese
DVD-CSS: fakten, fakten, fakten
DDoS: viel hype um nichts?

ISSN 0930.1045
frühjahr 2000 • immer noch dm 5,–
postvertriebsstück C11301F

deCSS-source inside!

Erfa-Kreise

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

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

Köln: Der Chaos Computer Club Cologne zieht gerade um. Aktuelle Koordinaten bitte unter mail@koeln.ccc.de bzw. http://www.koeln. ccc.de erfragen. Telefon erst nach erfolgtem Umzug.

Ulm: Kontaktperson: Frank Kargl <frank.kargl@ulm.ccc.de> Electronic Mail:contact@ccc.ulm.de Web: http://www.ulm.ccc.de/

Treffen: Jeden Montag ab 19.30h im 'Café Einstein' in der Universität Ulm.

Bielefeld: Kontakt Sven Klose Phone: 0521 1365797 EMail: mail@bielefeld.ccc.de. Treffen Donnerstags, ab 19.30 Uhr in der Gaststätte 'Pinte', Rohrteichstr. 28, beim Landgericht in Bielefeld. Interessierte sind herzlich eingeladen.

Chaos-Treffs:

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

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

Die Datenschleuder Nr. 70

I. Quartal, Frühjahr 2000

Herausgeber:
(Abos, Adressen etc.)
Chaos Computer Club e.V.,
Lokstedter Weg 72, D-20251 Hamburg,
Tel. +49 (40) 401801-0, Fax +49 (40) 401801-41,
eMail: office@ccc.de

Redaktion:
(Artikel, Leserbriefe etc.)
Redaktion Datenschleuder, Postfach 640236, D-10048 Berlin, Tel +49 (30) 280 974 70
Fax +49 (30) 285 986 56 / eMail: ds@ccc.de

Druck:
pinguin-druck, berlin

CvD, Layout und ViSdP dieser Ausgabe:
tom lazar, tom@tomster.org

Mitarbeiter dieser Ausgabe:
Starbug, Henriette Fiebig, Frank Rosengart, Doobee, Arne, Lisa Thalheim, Felix v. Leitner.

der schwachsinn geht auch im jahr 2000 weiter. wer hätte auch anders zu hoffen gewagt. ob es die realitätsfremde musikindustrie mit ihrer FUD-kampagne gegen MP3 und deCSS ist; die BVG mit ihrem ideal des "gläsernen fahrgastes" oder (mal wieder) die boulevardjournaille mitt ihrer überaus fundierten berichterstattung (diesmal) zum thema "distributed Denial-of-Service Attacks" – die öffentlichkeit verharrt weiterhin in einer lähmendenposition irgendwo zwischen faszination und furcht vor allem, was auch nur im entferntesten mit computern zu tun hat.

damit das nicht so bleibt und die zahl der "mündigen user" weltweit mit der weiterhin exponentiell steigenden verbreitung von rechnergesteuerten geräten mithalten kann, ist eine gesteigerte aktivität bei all denjenigen vonnöten, die genügend wissen und freiheit besitzen, sich *nicht* von schlagzeilen, herstellerpropaganda oder politikerversprechen blenden oder einschüchtern zu lassen.

wer sich also in der glücklichen lage sieht, furchtlos und aufgeschlossen auf die kommenden entwicklungen zuzugehen, sollte sich vielleicht fragen, ob er/sie damit nicht auch eine verantwortung gegenüber all denjenigen hat, die das (aus welchen gründen auch immer) nicht können.

alleine und auf eigener faust dieser verpflichtung (sedenn man sie verspürt) nachzukommen, ist nicht nur schwierig, sondern auch (und das zählt viel mehr) *ineffektiv*. wenn die zunehmende vernetzung von *technologien* eine gefahr darstellen sollte, kann dieser nur durch eine zunehmende vernetzung von *menschen* entgegnet werden.

vor diesem hintergrund ist auch die datenschleuder auf möglichst viel input von euch angewiesen. berichtet uns von euren aktivitäten, projekten oder auch nur vorhaben davon.

spread the gospel, keep on rocking!

tom@tomster.org

Linus gegen die DVD-Mafia

So oder so, spricht der bekannte Programmierer Linus Torvalds, werden wir DVD für Linux kriegen. Im übrigen versuche die DVD-. Lobby schlicht, ihre Kunden auszunehmen.

Welch schönes Wort zur rechten Zeit: Neben den 22 internationalen Civil Rights Organisationen der GILC haben zwei französische und eine Schweizer Usergroup den Offen Brief von quintessenz, ACLU, EFF betreffend die Re/pressions/versuche der US-Filmindustrie unterzeichnet, heute kam noch ein Informatik-Lehrstuhl einer deutschen Uni dazu.

Vielleicht trägt das Engagement Herrn Torvalds etwas zum Prozess der Meinungsbildung in deutschsprachigen Linux-Usergruppen bei, dass es zuweilen *notwendig* ist, politisch Stellung zu beziehen.

Die URL steht jedenfalls hier
http://www.quintessenz.at

Bässe kommen durch die Lunge

Über Kopfhörer oder gar Walkman-Ohrstöpsel konnten Bässe bislang nur unzureichend übertragen werden. Elektrotechniker der Universität Kaiserslautern haben jetzt ein neues Soundsystem entwickelt, das die Lunge als Resonanzkörper nutzt. Damit soll ein völlig neues Klangempfinden ermöglicht werden

Herzstueck der neuen Technik ist ein blaues Plastikei mit Namen "Bodybass".

Das Gerät wirkt als sogenannter Subwoofer und ergänzt die regulären Kopfhoerer. Im Ei steckt neben etwas Elektronik im wesentlichen ein leistungsstarker Basslautsprecher, der in Höhe des Brustbeines angegurtet wird. Er schickt die Schallwellen über die Lungen, den Rachen und die Eustachischen Röhren zum Gehör.

Das Gerät, das fünf Jahre Entwicklungsarbeit hinter sich hat, geht auf den Elektrotechniker Michael Rock zurueck. Er wurde für seinen "Bodybass" mit dem Erfinderpreis des Landes Rheinland-Pfalz ausgezeichnet. In Kürze soll das Gerät in den Handel kommen.

Quelle: Universitaet Kaiserslautern, 15.2.00

(Forschung: Michael Rock / Zentrum fuer Mikroelektronik der Universitaet Kaiserslautern, ZMK)

Noch ein wunderbarer Microsoft-Bug

Wenn man das 128bit-Verschlüsselungs-Modul für den Internet Explorer 5 über Windows Update installiert, kann man sich nicht mehr bei Windows 2000 anmelden.

Anpassung der Mitgliedsbeiträge an Euro

Laut eschluss der Mitgliederversammlung vom 4.7.1999 werden die Mitgliedsbeiträge zum 1.3.2000 auf Euro umgestellt. Daraus ergeben sich folgende Beiträge:

Aufnahmebeitrag
(einmalig) bisher 20.- DM – jetzt 10,- Euro

Mitgliedsbeitrag "Normal"
monatlich: bisher 10,- DM – jetzt 6,- Euro
bzw. jährlich: bisher 120,- DM – jetzt 72 Euro

Mitgliedbeiträge "Ermässigt"
monatlich: bisher 5,- DM – jetzt 3,- Euro
bzw. jährlich: bisher 60,- DM – jetzt 36,- Euro

Noch eine Bitte: Aus Aufwandsgründen bevorzugen wir jährliche Zahlungsweise. Dieses erleichtert die Verwaltung erheblich.

etoy.com vs. etoys.com 1:0!
on february 18, 2000 11 AM (PACIFIC TIME) the etoy.LAWYERS chris truax in

san diego and peter e. wild in zurich informed the etoy.MANAGEMENT about the final dismissal of the insane complaint filed by eToys Inc./santa monica against the etoy.CORPORATION after 81 days of war at the court, in the net, at the stock market and in the press. now the TOYWAR.troops and hundreds of exhausted internet resistance soldiers are marching off the battlefields after they succeeded in relieving the enemy occupation of etoy's territory www.etoy.com. this is a historical moment for both etoy and the involved toy guerilla. the victory parade takes place right here / right now, on the historical site. the celebration of this glorious triumph will last for exactly 1000 years! confused? find out more at the WAR NEWS ROOM
http://www.etoy.com

Zufall..?

Die Zahl 23 wurde 1999 mit 28 mal zur häufigsten zusatzzahl im lotto. (quelle: irgendso´n bericht im radio, duh!)

politisch korrekt

Trotz einer Beleidigungsklage von Schöhnbohm (nicht des Tierschutzbundes) gegen zwei Transparentträger darf auch weiterhin behauptet werden, dass "Schönbohm keine Schafe fickt." Die beiden Beklagten gaben vor Gericht an, dass sie das bösartige Gerücht, dass "Schönbohm Schafe fickt", in der Kreuzberger Szene gehört hatten, und dass sie nichts als die Ehrenrettung Schönbohms (ex Berliner Justizsenator, jetzt CDU Fraktionschef in (Brandenburg) im Sinne hatten. Das Verfahren wurde kurz nach Eröffnung eingestellt.

Die beiden Beklagten sind schon des öfteren durch ihren selbstlosen Einsatz aufgefallen. So trugen sie auf einer Demos – es ging wohl um die Bundeswehr – Transparente mit der Aufschrift "Auch Mörder sind Menschen". Die letzte Aktion war eine Spendensammlung für die CDU, damit diese durch die zu erwartenden Steuernachzahlungen in der Spendenaffäre nicht vom Ruin bedroht werde. Nach der Aussage eines des Beklagten sind in Kreuzberg dafür inzwischen 1,91 DM zusammengekommen. Einer der Angeklagten äusserte sich dazu, dass er nicht nicht wisse, ob das Geld der CDU überwiesen werden solle, oder ob er es persönlich in einem Geldkoffer in der Partei übergeben wolle.

(Quelle: Inforadio Berlin am 4.1.2000)

ASP Sicherheitsloch Nr. wieviel!?!

Active server pages (ASP) with runtime errors expose a security hole that publishes the full source code name to the caller. If these scripts are published on the internet before they are debugged by the programmer, the major search engines index them. These indexed ASP pages can be then located with a simple search. The search results publish the full path and file name for the ASP scripts. This URL can be viewed in a browser and may reveal fill source code with details of business logic, database location and structure.

In the Altavista search engine execute a search for +"Microsoft VBScript runtime error" +". inc,"; Look for search results that include the full path and filename for an include (.inc) file; Append the include filename to the host name and call this up in a web browser. Example: www.rodney.com/stationary/browser.inc

Quelle: http://www.jwsg.com

DVD-Software

Mit Erschrecken haben wir Ende 1999 zur Kenntnis genommen, daß die DVD-Erkenntnisse der letzten Wochen und Monate plötzlich von allen möglichen Servern verschwanden.

Dabei galt doch das Internet immer als Garant für die Freiheit von Informationen – wenn etwas im Internet veröffentlicht war, kann man es nicht zurückziehen.

Um die Freiheit von Information, Forschung und Meinungsaustausch zu erhalten findet sich am Ende dieser Seite ein Mirror der zum Verständnis des DVD-Verschlüsselungs-Verfahrens nötigen Beschreibungen und Sourcen.

Dabei ist es uns ein Anliegen, den Einwohnern Deutschlands zu vermitteln, in welcher Form die US-Filmindustrie sie um ihre Rechte zu bringen versucht. Grundsätzlich zahlt man in Deutschland für alle Medien GEMA-Gebühren, die man für das Speichern von Audio und Video benutzen kann. Deshalb gibt es hier auch einen preislich so großen Unterschied zwischen Daten- und Musik-Rohlingen. Die GEMA verteilt die eingenommenen Gebühren dann an die Künstler und die Filmindustrie.

Tatsächlich hat man in Deutschland das Recht, einen in der Videothek geliehenen Film zu kopieren und bis an sein Lebensende immer wieder anzuschauen. Dafür zahlt man GEMA-Gebühren für das Videoband. Das gleiche gilt für Audio-CDs.

Die Filmindustrie möchte aber, daß man Filme kauft und nicht leiht, weil sie dann mehr Geld verdienen. Deshalb haben sie im Nachhinein die VHS-Norm verschärfen lassen, damit ein Kopieschutz namens Macrovision möglich wird. Wenn der Videostrahl des Fernsehers von rechts nach links zurückgelenkt wird, und wenn er von unten nach oben zurückfährt, hat man im Videosignal eine Pause. In dieser Pause überträgt Macrovision Störsignale, die eine Aufnahme per VHS-Rekorder verhindern sollen. Man kann im Einzelhandel Geräte kaufen, die das wieder rückgängig machen. Gängiger Preis sind DM 150. Das bedeutet im Klartext, daß man als Kunde in Deutschland

1. GEMA Gebühren für das Videoband
2. GEMA Gebühren beim Ausleihen des Filmes
3. Entwicklungs- und Bürokratiekosten für die Entwicklung von Macrovision
4. Entwicklungs- und Bürokratiekosten für die Entwicklung des Macrovision-Entferners

zahlen muß. Bei DVD ist das noch schlimmer, weil neben den völlig unsinnigen Region Codes, die nur die Produktionskosten in die Höhe treiben, auch noch ein laienhaftes Verschlüsselungssystem namens CSS implementiert wurden, welches natürlich die Produktionskosten ebenfalls in die Höhe treibt und Lizenzgebühren kostet. Diese Gebühren sind im Übrigen so hoch, daß die meisten deutschen DVDs von CSS Abstand nehmen.

Das Hauptproblem ist, daß Player nur das DVD-Logo tragen dürfen, wenn sie Region Codes und CSS implementieren. Für viele Leute wäre DVD als reiner Massenspeicher wichtig, die Filme sind mir z.B. ziemlich egal. Aber auch die Computer-Geräte müssen Region Code und CSS implementieren, auch wenn sie niemals benutzt werden. Und bezahlen muß dafür der Kunde.

Wogegen soll denn CSS jetzt helfen?

Die Aussagen der Filmindustrie sind, daß CSS unautorisiertes Kopieren verhindern soll. Es stellt sich aber heraus, daß CSS genau das Gegenteil tut, denn man kann trotz CSS eine DVD kopieren, aber anschauen kann man sie sich nicht.

Der "Kopierschutz" ist also in Wirklichkeit ein Anschau-Schutz! In Wirklichkeit geht es also offenbar nicht darum, die DVD-Titel zu schützen, sondern die Lizenzgebühren für die Player zu erzwingen. Das DVD-Consortium hat hier offenbar den kurzfristigen Gewinn dem langfristigen vorgezogen.

Tatsächlich war auch im Geschehen zu sehen, daß es nicht um das Kopieren ging, weil kein Mensch laut wurde, als die zum Kopieren notwendige Schwäche bekannt wurde (das war über ein halbes Jahr früher). Die Presse-Berichterstattung legte erst los, als die Player-Keys gepostet wurden, mit denen man Player nachbauen konnte, ohne Lizenzgebühren zu zahlen. Das illegale Brennen von DVDs interessiert die Filmindustrie offenbar nicht wirklich. (Die deutschen DVDs ohne Region Code sind schon immer problemlos auf die Platte oder einen anderen Datenträger kopierbar gewesen, ohne daß sich das große Wehklagen erhoben hätte)

Was ist denn da jetzt passiert?

Alles fing damit an, daß es rechtlich sehr schwer ist, Copyrights auf digitalen Content durchzusetzen. Daher hat die Film-Industrie versucht, ihre Pfründe über den Umweg des technischen Kopierschutzes zu sichern. Daher hat man CSS ersonnen und geschützt und versucht jetzt, Programmierer zu belangen, weil sie CSS gebrochen haben, nicht weil sie die Inhalte kopiert haben.

CSS ist lächerlich leicht zu knacken. Darin sind sich alle Beteiligten einig. Da fragt man sich natürlich, wieso die Filmindustrie lieber Millionen für ein Schrott-Verfahren ausgibt als für ein anständiges? Eine mögliche Spekulation ist natürlich, daß die Industrie in Kauf nahm, daß das jemand knackt, damit sie denjenigen anständig belangen können, um ein genügend hohes Abschreckungspotential aufzubauen. Und ein eingeschüchterter Kunde kopiert das nicht auf Band, sondern leiht es lieber zweimal. Und schon hat man den Gewinn verdoppelt.

Es war also nur eine Frage der Zeit, bis jemand CSS knackt. Der Film ist mit einem Schlüssel verschlüsselt. Wenn alle DVDs den gleichen

Schlüssel benutzen würden, würde ein Hacker nur diesen Schlüssel herausfinden müssen und könnte dann alle DVDs illegal kopieren. Also muß jede DVD einen anderen Schlüssel haben.

Woher kennt der Player den Schlüssel, wenn der pro DVD verschieden ist? Nun, er steht auf der DVD drauf, und zwar verschlüsselt mit einem Player-Schlüssel. Jeder Player hat also einen eigenen Schlüssel. Beim Einlegen der DVD entschlüsselt der Player also mit seinem Schlüssel den Session-Key. Auf jeder DVD stehen also 408 Schlüssel. Die Idee ist, daß sich ein Player anmeldet, einen dieser Schlüssel bekommt, und man ihm auch saugt, welcher dieser 408 Schlüssel für ihn ist. Wenn ein Schlüssel geknackt wird, kann man dann auf zukünftigen DVDs diesen Slot mit einem anderen Schlüssel füllen.

Soweit die Theorie. Nun wollte die Film-Industrie ursprünglich gar keine Software-Implementationen von CSS zulassen, aber als dann klar wurde, daß die Leute mit ihrem PC unter Windows DVDs gucken wollen, ließen sie es zu. In einem PC kann man den Player-Schlüssel aus dem Speicher auslesen. Spiele-Knacker machen das täglich. So war es dann auch eine Gruppe von Raubkopierern, die den Schlüssel und den CSS-Code extrahiert hat. Das liegt nicht daran, daß sie DVDs raubkopieren wollten, sondern daß diese Personengruppe am meisten Kompetenz beim Reverse Engineering hat.

- Nach ein paar Tagen wurde dann der Quellcode dieser Software gepostet, und eine Kryptoanalyse von CSS konnte beginnen.
- Schon am nächsten Tag postete jemand eine erste Analyse der Schlüsselgenerierung, die erwähnt, daß der Autor Code hat, der maximal 17 Stunden auf einem 366 MHz Celeron braucht, um einen Schlüssel durch bloßes Ausprobieren zu knacken. An dieser Stelle war klar, daß CSS nicht ernstzunehmen ist.
- Am nächsten Tag beschrieb ein Kryptograph einen Angriff, der die Komplexität auf 2 hoch 16 senkte bei nur 6 bekannten Ausgabe-Bytes. Das ist in einer Zehntel-Sekunde locker zu machen auf heutigen Prozessoren. Unter den Beteiligten machte sich erstaunte Ehrfurcht breit, wie jemand eine derart lächerliche Kryptographie benutzen konnte.
- Der Kryptograph verfeinerte seinen Angriff am nächsten Tag noch (er war nicht an CSS, sondern an der Kryptographie interessiert), indem er nur noch 5 bekannte Ausgabe-Bytes brauchte (das macht den Code etwas langsamer, aber 5 Bytes sind laut DVD-Standard immer bekannt). Er postete Code, der ungefähr 5 Sekunden auf einem 200 MHz Pentium Pro braucht. Am gleichen Tag postete jemand Linux-Quellcode, der ein VOB-File entschlüsselt (heraus kommt ein MPEG, das man mit jedem MPEG-Player abspielen kann).
- Am nächsten Tag löste jemand den Super-GAU aus, indem er alle Player-Schlüssel postete. Die Hoffnung der Film-Industrie war ja gewesen, daß man den geknackten Player-Schlüssel (als dessen Quelle sich der reverse engineerte Xing-Player herausstellte) einfach durch einen anderen ersetzt. Dieser Schritt demonstrierte die Hinfälligkeit von CSS eindrucksvoll, weil das Extrahieren dieser Schlüssel lediglich 30 Minuten gedauert hat laut Aussage des Posters. Wenn die DVD-Leute jetzt alle Schlüssel ändern, würde das die Stärke von CSS nicht stärken und alle Heimkino-Käufer könnten keine DVDs mehr gucken.
- Den letzten Sargnagel lieferte der Kryptograph am gleichen Tag, indem er eine Attacke demonstrierte, die den DVD-Schlüssel extrahieren konnte, ohne einen Player-Schlüssel zu kennen! D.h. ob die DVD-Industrie da etwas ändert oder nicht an den Schlüsseln wäre völlig egal. Die Attacke dauert rund 20 Sekunden auf dem Pentium III 500 des Kryptographen.

Das ist der Status. CSS ist nicht nur offensichtlich absolut lächerlich, sondern es ist nicht einmal reparierbar.

Was ist denn jetzt so schlimm?

Die tatsächlich anwaltlich Verfolgten sind im Moment Linux-DVD-Entwickler, d.h. Leute, die ganz normal auf ihrem legalen PC ihre legal erworbenen DVDs gucken wollen. Diese Leute haben gar nichts mit CSS zu tun. Die Überschneidung ergibt sich daraus, daß das Angucken und das Kopieren von Filmen technisch die gleiche Operation ist.

Ist dieser Artikel denn nicht illegal?

Die Rechtslage ist aufgrund der Enzigartigkeit der Materie unübersichtlich. Klar ist: in Deutschland ist reverse engineering für den ausschliesslichen Zweck der Kompatibilitätsherstellung ausdrücklich erlaubt, d.h. man darf gekaufte Produkte auseinandernehmen und verändern, um sie zu Laufen zu bringen. DVDs beinhalten Mechanismen, die verhindern das sie unter anderen als den üblichen Mainstream-Systemen betrachtbar sind. Es handelt sich dabei also um eine Inkompatibilität. Wir halten demzufolge die Publikation der Beschreibungen und Sourcen die es ermöglichen, DVDs unter Linux etc. zum Laufen zu bringen und das Encoding-Verfahren zu verstehen, in Deutschland nicht für illegal. Nochmal: es geht hier nicht um Raubkopien, die auch ohne diese Publikationen schon immer möglich waren, sondern um das Verständnis eines Verfahrens und die Möglichkeit DVDs ganz legal auch unter Linux zu betrachten.

Die relevanten Dateien

1. CSS Historie: http://www.fefe.de/dvd/css-chain-of-events
2. 991025: CSS-Quellcode wird gepostet: http://www.fefe.de/dvd/css.tar.gz
3. 991026: Eine Analyse der CSS Schlüsselgenerierung: http://www.fefe.de/dvd/CSS-key-generation-analysis
4. 991028: Mehr Code: http://www.fefe.de/dvd/more-code-for-reading-descrambling-dvd
5. 991027: Erfolgreicher Angriff auf CSS: http://www.fefe.de/dvd/Successful-attack-on-CSS-algorithm
6. 991028: Funktionierender Cracker für die Player-Schlüssel: http://www.fefe.de/dvd/working-playerkey-cracker
7. 991030: Besserer Cracker für die Player-Schlüssel: http://www.fefe.de/dvd/better-player-key-cracker
8. 991030: Alle Player Keys: http://www.fefe.de/dvd/random-numbers
9. 991030: Funktionierender Angriff auf Disk Key Hash: http://www.fefe.de/dvd/working-attack-on-diskkey-hash
10. 991113: `http://www.fefe.de/dvd/file.tar.gz`
11. css-auth Linux code: `http://www.fefe.de/dvd/css-auth.tar.gz`

Kontakt

Anmerkungen und Kontakt zu dieser Seite an **dvd@flatline.de**

tick.et: "wir wissen, wo sie sind."

Die Berliner Verkehrsbetriebe (BVG) testen zurzeit ein System, welches den herkömmlichen Fahrschein aus Papier durch eine Chipkarte ersetzt.

Im Oktober 1999 startete in Berlin ein Feldversuch, wo 25.000 freiwillige Tester sechs Monate lang Chipkarten mit drahtloser Datenübertragung als Alternative zum herkömmlichen Fahrausweis ausprobieren sollen. Auf je zwei U-Bahn-, Bus- und Straßenbahnlinien in Berlin versucht die BVG, die Akzeptanz und Praxistauglichkeit zu erproben. Für die Probanden winken ein Rabatt von 15% auf ihre bisherige Monatskarten, die Teilnahme an einer Verlosung und "die Möglichkeit, ein innovatives Zahlungssystem der Zukunft ausprobieren zu dürfen". Die Tester sind allesamt Inhaber von Monatskarten und müssen daher nicht real für die gefahrenen Strecken bezahlen.

Die tick-et Karte sieht aus wie eine normale Telefonkarte ohne Chipkontakte. In ihr befinden sich eine Induktionsschleife und ein Chip. Beim Fahrtantritt wird die Karte an einem "Check-in"-Gerät im Abstand von einigen Zentimetern vorbei geführt. Dabei gibt das Gerät einen lauten Piepser von sich. So laut, dass sich mindestens die Hälfte der auf dem Bahnsteig befindlichen Leute nach der Versuchsperson umdrehen. Oder es passiert nichts, dann ist das System gerade außer Betrieb. Nach Ende der Fahrt checkt man sich wieder an einem anderen Terminal aus. Die Abrechnung stellt sich die BVG so vor: Die Karte wird anfangs mit einem Betrag aufgeladen. Beim Check-in wird ein bestimmter Betrag von der Karte abgebucht und beim Check-out der nicht abgefahrene Betrag wieder zurückgeschrieben. Sollte man das Auschecken vergessen, ist also maximal der im Voraus abgebuchte Betrag weg. Als besonderes Feature kann man sich an speziellen Infoterminals ein "Logbuch" seiner letzten Fahrten anzeigen lassen. Alle Daten der Fahrt (z.B. "ohne Begleitung") werden von den Verkehrsbetrieben erfasst, dort gespeichert und ausgewertet. Selbst wenn diese Karten später anonym ausgegeben werden würden, wäre an hand der minutengenauen Bewegungsprofile eine recht eindeutige Zuordnung eines tick-et

möglich. Die Anfrage eines Bedarfsträgers bei der BVG könnte dann so aussehen: "Guten Tag, hier ist das BKA. Wir bräuchten mal bitte die Position von Herrn Schmidt." – "Der ist gerade in die U9 Richtung Süden eingestiegen. Aber beeilen Sie sich, erst heute schon 15 Minuten später dran als sonst."

Wohl auch die Vorstellung vom Big Brother hat viele Leute in Berlin davon abgehalten, dieses System zu testen. Die BVG wird Umfragen unter den Testern machen, bei denen man als kritischer Tester dann auch sagen kann, was man von dieser totalen Überwachung hält. Im letzten Monat erlebte die BVG einen regelrechten Ansturm von Testkandidaten: Es hat sich nämlich rumgesprochen, dass es keine mobilen Terminals zur Kontrolle der elektronischen Tickets gibt. Kontrolleure in der U-Bahn können also nur lächeln, wenn ihnen eine gelb-blaue Plastikkarte unter die Nase gehalten wird. Ob man tatsächlich bezahlt hat, sieht man der Karte nämlich nicht an.

Die S-Bahn in Berlin, Tochterunternehmen der Deutschen Bahn, beteiligt sich nach einigem Zögern nun auch an dem Feldversuch. Anfangs hat man bei der S-Bahn Berlin GmbH noch behauptet, dass die neu gestalteten Bahnsteige noch der Gewährleistungspflicht der Baufirma unterliegen. Mit dem Aufstellen der tick-et-Geräte würde diese erlöschen. Da die Deutsche Bahn demnächst bundesweit ein eigenes System einführen möchte und das natürlich lieber auf ihren Bahnsteigen sehen würde, ist hier wohl eher der Grund für die starre Haltung gegenüber der BVG zu suchen.

Auch der Verkehrsverbund Köln testet derzeit ein ähnliches System.

verwendete Technik

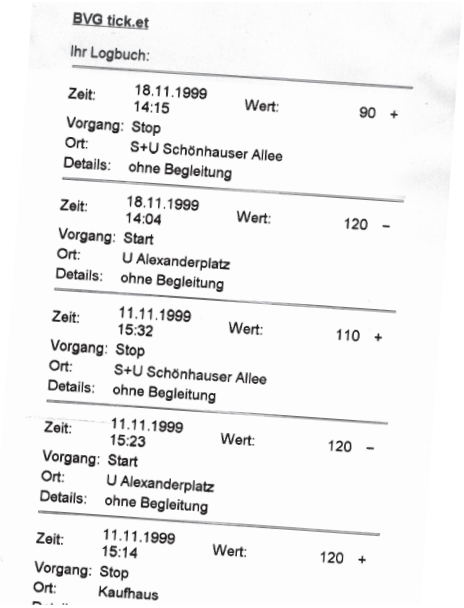
Das Chipkartensystem ist ein Motorola M-Smart Venus, die Terminals laufen unter Windows NT bzw. CE. Die Säulen sind via TCP/IP untereinander vernetzt und erhalten ihre Software via BOOTP. Vermutlich wird für die Übertragung zur Zentrale das BVG-eigene Glasfaser- bzw. ISDN-Netz genutzt. Die tick-et-Karte hat einen 8-Bit-Mikroprozessor, 16Kbyte ROM, 384 Bytes RAM, 2 Kbyte EEPROM, kann Single/Triple DES und die Luftschnittstelle ist nach ISO 14443 Type B (laut Spezifikation von Motorola).

URLs:

http://www.tick-et.de

http://www.bvg.de

http://www.tagesspiegel.de/archiv/1999/10/18/ak-be-po-11852.html



BVG tick.et

Ihr Logbuch:

Zeit:	18.11.1999 14:15	Wert:	90 +
Vorgang:	Stop		
Ort:	S+U Schönhauser Allee		
Details:	ohne Begleitung		
Zeit:	18.11.1999 14:04	Wert:	120 –
Vorgang:	Start		
Ort:	U Alexanderplatz		
Details:	ohne Begleitung		
Zeit:	11.11.1999 15:32	Wert:	110 +
Vorgang:	Stop		
Ort:	S+U Schönhauser Allee		
Details:	ohne Begleitung		
Zeit:	11.11.1999 15:23	Wert:	120 –
Vorgang:	Start		
Ort:	U Alexanderplatz		
Details:	ohne Begleitung		
Zeit:	11.11.1999 15:14	Wert:	120 +
Vorgang:	Stop		
Ort:	Kaufhaus		

16C3 review

Der sechzehnte Congress war nicht nur ein riesiges Hackcenter und eine geile dreitägige Party – auch Inhaltliches kam nicht zu kurz. Eine kurze Zusammenfassung der wichtigsten Veranstaltungen

Tunnelrealitäten - Grenzen der Vermittelbarkeit virtueller Realitäten

Referent: Andy Müller-Maguhn (andy@ccc.de)

Der Vortrag zeigte nach einer kurzen Einführung in die Geschichte der Netzkultur und einer Begriffsklärung verschiedener gebräuchlicher Schlagwörtern die Probleme des CCC Vertretern aus Politik und Wirtschaft die Ziele der Hackerkultur näherzubringen.

Routing in IP-Netzen

Referent: Felix von Leitner (felix@ccc.de)

Dieser Workshop beleuchtete die verschiedenen Routing-Protokolle, natürlich insbesondere unter Sicherheitsaspekten.

URL: https://www.ccc.de/congress99/doku/routing.pdf

TCP-Penetrationsmöglichkeiten

Referent: Felix von Leitner (felix@ccc.de)

Zeigte ein paar Möglichkeiten über TCP-Verbindungen auf einem fremden Rechner Code auszuführen.

Wizards of OS Revisited & die nächste Folge

Referent: Volker Grassmuck (vgrass@rz.hu-berlin.de)

Die Konferenz "Wizards of OS. Offene Quellen & Freie Software" im Juli 99 im Haus der Kulturen der Welt Berlin versuchte nicht nur, Projekte und Firmen der freien Software vorzustellen, sondern auch nach der Übertragbarkeit des Modells auf andere Wissensformen und auf die Wissensordnung allgemein zu fragen. Die nächsten Wizards werden im Herbst 2000 in Berlin stattfinden.

URL: http://www.mikro.org/wos

Information Warfare Update

Referent: Frank Rieger (frank@ccc.de)

Im Hinblick auf den Krieg in Serbien war dieses Jahr vergleichsweise ereignisreich für den Information Warfare, wobei der Begriff Information Operations passender ist. Diese Operations werden zunehmend als Mittel zur Konfliktlösung betrachtet. Auf Seiten der USA wurde angedroht Kontenmanipulation gegen

die Führung der gegnerischen Seite, sprich Milosevic &Co. vorzunehmen. Es wurden gezielte Schläge gegen die Kommunikationsstruktur der gegenerischen Seite vorgenommen. Nach Zerstörungen wurden TV und Radio eingenommen. Speziell gegen das Elektrizitätsnetz gerichtete Waffen wurden angewandt, zum Bespiel Graphitfaserbomben, die im Gegensatz zu "normalenBomben" eine höhere Effzienz aufweisen. Angeblich sollen auch Viren und Netzwerkeinbrüche zur Aushebelung des Luftverteidigungssystems eingesetzt worden sein. Die Serben starteten Angriffe gegen die Kommunikationsstruktur. Es fand eine fortgeschrittene psychologische Kriegsführung gegen NATO-Heimatländer statt. In erheblichem Umfang wurden auch Attrappen zur Veränderung der Radarbilder der Gegner eingesetzt. Die Trends gehen dahin, dass auch nichtstaatliche Strukturen in die Abwehrbemühungen einbezogen werden, z. B an der Börse bei Aktien-Transaktionen.

IPv6

Referent: Felix von Leitner (felix@ccc.de)

IPv6 ist die nächste Version des Internet Protokolls. Sie ist entgegen anderslautender Presseberichte nicht nur wichtig, weil bei IPv4 der Adressraum knapp wird; die ganze Wahrheit inklusive einer Betrachtung der aktuellen Forschungen auf diesem Gebiet bringt dieser Vortrag.

URL: https://www.ccc.de/congress99/doku/ipv6.pdf

Multicast

Referent: Felix von Leitner (felix@ccc.de)

Multicast ist neben Unicast und Broadcast eine fundamentale Methode, wie man Daten versenden kann. Multicast beschreibt das Verschicken von Daten an mehrere Empfänger. Neben einer generellen Einführung und einem Realitätsabgleich zum Stand der Technik wurde auch das im Moment noch am wenigsten gelöste Problem, das Mutlicast-Routing angesprochen.

URL: https://www.ccc.de/congress99/doku/multicast 2.pdf (42 Seiten)

Echelon, Interception Capabilities and Status Quo of SIGINT

Referent: Duncan Campbell (Duncan@gn.apc.org)

In the presentation Duncan Campell talked about the worldwide surveillance system "Echelon". He specially outlined the systems in the UK and the largest facility at Menwith Hill, but the system consists of many more posts around the globe. Echelon is maintained by the USA, UK, Australia, Canada and New Zealand and their special organizations. They spy on almost any information traffic (satellites, microwave connections, undersea cables,...) around the globe.

www.iptvreports.mcmail.com/interception_capabilities_2000.htm www.gn.apc.org/duncan/echelon-dc.htm

Einführung in TCP/IP

Referent: Pirx (pirx@ccc.de)

Eine technische Einführung in die TCP/IP Protokollfamilie. Es wurden detailliert Protokollaufbau, Paketformate, Paketaufbau, Verbindungsauf- und Abbau und das IP-Schichtenmodell erläutert.

URL: https://www.ccc.de/congress99/doku/tcpip_v4.pdf

WAP - Where Are The Phones?

Referent: Tobias Engel (tobias@ccc.de)

Ganz bald sollen unsere Mobiltelefone eine neue Sprache sprechen: das wireless application protocol. Amoklaufende Marketingstrategen versprechen uns das jetzt schon einige Monate, aber weder die Applikationen noch die Telefone sind verfügbar. Ein Einblick in die kurze, aber schräge Geschichte von WAP. Was ist alles schiefgelaufen und wie wird es alles mal sein, wenn es denn vielleicht doch noch soweit kommt?!

http://www.wapforum.org

der Testla Generator

Referent: Jan Keil (jan.keil@hadiko.de) + Alex Wenger (a.wenger@gmx.de)

Der Vortrag über Tesla-Generatoren war trotz des großen Anteils an theoretischer Pysik sehr gut besucht. Der Vortragende hat zuerst über die Biographie des wohl längst vergessenen Genies berichtet, und danach ist er dann sehr schnell auf die Theorie des Tesla-Generators gekommen. Ebenso hat er eine Menge Tipps zum Eigenbau von Tranformatoren geliefert. Am Ende des Vortrags gab es dann eine Vorführung seines selbst gebauten Transformators. Informationen zum Bau eines Tesla-Transformators findet man überall im Internet. Für seine Meterlangen Blitze verwendete Tesla einen nach ihm benannten Tesla-Generator. Dieser besteht im Wesentlichen aus einem Transformator, mit dem Unterschied, das sich Primär- und Sekundär-Wicklung in Resonanz befinden, dadurch kann die Ausgangsspannung auf ein Vielfaches des normalerweise bei Transformatoren geltende Windungsverhältnisses gesteigert werden.

- Ausgangsspannung normaler Transformator: Ausschlaggebend ist das Windungsverhältnis, z.B.: Die Primärwicklung besitzt 100 Windungen, die Sekundärwicklung 1000, daraus folgt ein Verhältnis von 1/10. Das bedeutet, das eine Eingangsspannung verzehnfacht am Ausgang erscheint.
- Ausgangsspannung Tesla-Transformator: Die Vervielfältigung entspricht ungefähr dem Verhältnis der in den beiden Schwingkreisen vorhandenen Kapazitäten, ist aber sehr vom genauen Aufbau des Transformators abhängig. Es lassen sich aber relativ leicht Größen von millionen Volt erreichen.

Ein wichtiger Unterschied stellte auch die Frequenz der Ausgangsspannung dar, die relativ hohen Frequenzen von 50-1000 kHz bedingen weitere interessante Effekte (z.B. Abstrahlung der Energie (Die Blitze gehen Strahlenförmig direkt in die Luft, ohne auf einen Gegenpol angewiesen zu sein) Skin-Effekt (Die Hochspannung läuft auf der Oberfläche der Leiter entlang, dadurch kann sie einem Menschen relativ wenig anhaben).

Feminetzmus: Frauennetzwerke

Referentin: Nina Corda (mdma@stylepolice.de)

"haecksen, 'new media'- frauen, geek girls, nerdettes.. beginnen sich auf verschiedenen ebenen (und mit unterschiedlichen zielsetzungen) zu vernetzen. diese netzwerk-ideen vorzustellen und gemeinsamkeiten zu finden, die zu einem grösseren netz führen können/sollen, ist die intention dieser diskussionsrunde, ua mit frauen von webgrrls, fts und evtl. old boys netzwork (angefragt)."

Vorgestellt wurden vor allem zwei Feminetze, in denen sich chaosnahe Grrls verbündeln können und (vielleicht) sollten:

1. Aus einem Chaostreff in Bremen heraus hat sich ein Kreis von ca. 25 Frauen und 3 Männern gebildet, die vor allem die Vernetzung von Frauen innerhalb des CCC fördern wollen. Angedacht sind z.B. eine Knowledge-Base im Internet und regelmäßige Treffen IRL. (Kontakt über Nina)
2. Die Webgrrls gibt es in Deutschland seit 1997 (nach 1995 in den USA gegründetem Vorbild). Sie bezeichnen sich selbst als "Frauen in den Neuen Medien," und ihr Netzwerk soll ein Forum bieten für Wissenstransfer, Erfahrungsaustausch, Jobvermittlung, Entwicklung von Geschäftsideen und Weiterbildung.

http://www.webgrrls.de http://www.wired.com/news/culture/0,1284,33346,00.html
http://www.heise.de/tp/deutsch/inhalt/co/5655/1.html

Freies Hardware-Design: das F-CPU Projekt

Referent: Sven Klose (sven@devcon.net)

Weshalb eine freie CPU? Was macht die Entwicklung erst möglich? Wer kann teilnehmen? Wer nimmt teil? Welche Techniken benutzt der

Chip? (Befehlssatz, Aufbau)? Welche Software wird zur Entwicklung benutzt? Welche Möglichkeiten bieten sich an, die f-cpu in existierender Hardware einzusetzen? Welche Emulatoren sind vorhanden? Welche Betriebssysteme wollen portiert werden? Was für eine Performance ist zu erwarten? Wieviel wird der fpga/asic/echte chip kosten?

http://f-cpu.tux.org

Biometrie Workshop

Referent: Andreas Steinhauser (steini@ccc.de)

Ein Biometrie-Scanner mißt alles, was biologisch und unveränderlich ist. Das System gibt es schon seit ca. 100 Jahren. Alles hat mit einem ganz simplen Fingerabdruck angefangen und geht nun bis zu Scannern, welche die Iris vermessen. Das Prinzip der Scanner ist einfach und fast noch einfacher zu überlisten. Es soll etwas gemessen werden, was unveränderlich, nicht beliebig erneuerbar ist und auch nicht von dritten angenommen werden kann.

- Wo werden Fingerprintsenoren verwendet? (Computer, Handy, Autos, Bankautomaten, Gebäudezugang, Schusswaffen (ist aber ungünstig, da das System mit feuchten Fingern nicht funktioniert)).
- Welche Arten von Fingerprintsystemen gibt es? (optische Scanner, die ein Bild des Fingers verarbeiten (400DPI), thermoeletrische Scanner, welche die Körperwärme erfassen (400DPI), kapazitive Scanner, die den Abstand der Haut zur Fläche verarbeiten (500DPI) Laser Scanner, der die Rillen verarbeitet (400DPI))
- Printerkennung: Das Bild wird aufgenommen davon werden Minutien (charakteristische Stellen) herausgearbeitet. Der Vergleich von Minutien geschieht in der Zeit von ca. 1 sec.
- Lebenderkennung: Durchleuchten, der Puls wird gemessen (sehr gering), Hämoglobinmessung, Wärmemessung
- Wie überlistet man die Fingerprintsensoren?: Kopie des Fingerabdrucks dann schauen was es für ein Scanner ist (bei einem optischen Scanner reicht meistens ein Bild des Fingerabdrucks), Sensor angreifen (physikalisch die elektrischen Eingenschaften des Fingers herstellen), das Kabel angreifen (die Daten sind nicht verschlüsselt), Chipkarte mit Minutien (Chipkarte hacken und die Minutien verändern), das auswertende System angreifen.
- eine Falsifität anfertigen: an Vorlage eines Fingerabdrucks kommen (auf der glatten Oberfläche des Scanners befindet sich meistens noch Fett, womit man den Fingerabdruck rekonstruktieren kann), Herausfinden, was der Scanner auswertet, ein Bild/Plastik davon anfertigen
- bei einem optischen Scanner: Fingerabdruck ein bißchen bearbeiten, mit 600DPI ausdrukken, auf den optischen Scanner legen – fertig

Journaling FS für Linux: reiserFS

Referent: Hans Reiser (reiser@idiom.com)

Erst durch ein Datesystem, dass nach einem überaschenden Beenden des Rechners schnell wieder zur Verfügung steht, kann Linux in Bereiche Vordringen wo High Availability und grosse Datenmengen gefordert werden. Journaling ist das Mittel der Wahl, derzeit gibt es drei Bemühungen dieses auf Linux zum implementieren: von SGI als Port des xfs, als ext3 und als journaling reiserFS. Exemplarisch wird reiserFS vorgestellt.

http://devlinux.org/namesys/

Big Brother is watching you - Kameraüberwachung in Deutschland

Referenten: jadis (ketzer@ailis.de) und sam (s@scha.com)

Der Kölner ccc (c4) hat die massive Installation von Kameras zum Weltwirtschaftsgipfel zum Anlass genommen, die Überwachung öffentlichen Lebens durch private Sicherheitsdienste und Polizei zu dokumentieren. In diesem Workshop beschäftigten wir uns mit der rechtlichen Situation und stellten das in Köln laufende Projekt einer Kameradatenbank vor.

Geplant ist, die Datenbank bundesweit auszuweiten und Visionen zu entwickeln, was der einzelne gegen Datenschändung unternehmen kann. Die Datenbank wird für jeden zugänglich sein. Jeder soll die Möglichkeit haben, sich über die laufende Überwachung in seiner Stadt informieren zu können, z.B. via mailing liste.

Projektvorstellung ChaosCD

Das Team, das die CD verbrochen hat, stellte das Projekt und die CD vor. Neben Live-Demonstration der CD, Designfragen und technischem Einblick in die Realisierung wurden Plaudereien aus dem Nähkästchen der Redaktion geboten.

Enthalten sind: Volltext-Suchmaschine, Hacker-Bibel, ftp-Zeug, Chaos-Radio (nur Text KEIN Ton), Karl Koch Doku, Congress Doku, Kram, Self html, Trons Diplomarbeit über ISDN-Verschlüsselung (unbearbeitet), Zeitung: Labor, Kram aus dem Internet, die Seiten der Erfa-Kreise, Datenschleuder 1-67)

http://www.hamburg.ccc.de/chaoscd/

Finden von Sicherheitsproblemen im Quellcode

Referent: Marc Heuse (marc@suse.de)

Der Workshop gab einen kompletten Überblick über mögliche Schwachstellen im Sourcecode (Filedescriptor Vererbung und defaults, Char/Integer Buffer/Heap over/underflows, command execution, etc.) die an Hand von Beispielen in C (hauptsächlich), C++, Java, Perl, Tk/Tcl und Shell beschrieben werden, sowie Möglichkeiten, wie diese in effektivster Weise gefunden werden können.

http://www2.merton.ox.ac.uk/security

Security auditing with NESSUS

Referent: Jordan Hrycaj (jordan@mjh.teddy-net.com)

The Nessus project is placed as a countermeasure to the emerging security software industry. It is an open platform that allows everyone to test ones computer or network against known exploits and security holes.

http://www.nessus.org

HyperCard - Start in das Multimedia-Zeitalter

Referent: Joerg Kantel

Der Vortrag stellte HyperCard vor und zeigte, wie man mit wenigen Mausklicken und einigen Zeilen Programm-Code, die nahe an der natürlichen (englischen) Sprache liegen (HyperTalk), in HyperCard schnell kleine Anwendungen zusammen"klicken" kann. Und dann wurde an einigen Beispielen aus Kunst und Wissenschaft gezeigt, was HyperCard damals so faszinierend machte und welchen Einfluss dieses Konzept bis heute auf das Aussehen des World Wide Web hat.

Zum Schluss wurden noch einige der "Nachfolger" von HyperCard vorgestellt und die Zukunft eines solchen universellen Autorentools diskutiert.

http://www.kantel.de

Let's Factorize the Microsoft 512-bit Key

Referent: Ruediger Weiss (rweis@pi4.informatik.uni-mannheim.de)

Microsoft uses a 512 bit key for their E-Commerce. That is pretty funny because an academic research group, headed by CWI Amsterdam has factorised RSA-155 which is a 512bit number too. If the public modulus of a RSA key is factorised we can calculate the secret key easily. And because we are young innovative people we want to use the best hardware (AMD Athlon) and the best operating system (Linux) to do the job. Factorisation means two steps. The first step can be distributed very easily and took much less than our successful DES cracking actions. The second step needs between 2 and 3 GB main memory. The new Linux kernel will support 4 GB. So we want to discuss in this workshop if it is possible to sup-

port Microsoft ''distributed secret key management'' (see _NSAKEY ''backup key'').

http://www.informatik.uni-mannheim.de/rweis/ccc1999/

Security on Your Hand: File Encryption with the JAVA Ring

Referent: Ruediger Weiss (rweis@pi4.informatik.uni-mannheim.de)

In this workshop we present the first implementation for high-speed file encryption with a slow JAVA card. Using new ''Remotely Keyed Protocols'' designed by Lucks and Weis we can use the pretty tamper proof JAVA ring even in the ''non-cryptographic'' version. We have not patented the protocols or algorithms presented. The required software will be published as Open Sources.

http://www.informatik.uni-mannheim.de/rweis/ccc1999/

How to Ring a FreeSWAN

Referent: Rüdiger Weiss (rweis@pi4.informatik.uni-mannheim.de)

FreeS/WAN implements the Internet Key Exchange (IKE) protocol for the negotiation of the session keys. However the current implementation is limited to performing key negotiation based on preshared secrets that are stored in configuration files. If an attacker can read these files the security of the related IPSec tunnels would be compromised. A better alternative is to lock long term keys like these in a tamper resistant environment which they never leave. The iButton from Dallas Semiconductor is a JavaCard compliant device in an unusual form factor: a wearable finger ring. It provides a portable progammable environment with improved tamper resistance compared to conventional smart cards. We will compare and implement different protocols in which the secret keys are stored in an iButton. Besides authentication only methods (like a simple challenge/response) also schemes using Remotely Keyed Encryption (RKE) will be invstigated. These allow the encryption and decryption of entire sessions to be controlled by the iButton rather than just the session keys.

http://www.informatik.uni-mannheim.de/rweis/ccc1999/

Konzeptvorstellung und Diskussion Chaos Call Center

Referent: Hendrik Fulda (hhf@ccc.de)

Es gibt in letzter Zeit immer mehr Anfragen an den CCC aus allen möglichen Bereichen. Davon sind am meisten Hamburg und Berlin betroffen. Um dieses Potential auf ganz Deutschland zu verteilen wurde auf dem Congress '99 beschlossen, ein dezentrales Callcenter des CCC's einzurichten. Dieses soll sowohl vorgefertigte Antworten aus einer FAQ beinhalten als auch Betreuung für Gehackte, Hacker und deren Angehörige anbieten. Mitglieder-, Presse- und "normal Bürger-" Anfragen sollen sofort beantwortet werden. Ein besonders wichtiger Punkt ist die Rechtshilfe für Hacker, wie z.b. Anwaltsvermittlung.

Außerdem gab es noch:

- Kompromittierende Emissionen und andere Techniken
- Buffer Overflows
- BSD-Workshop
- Y2K-Erfahrungen, 1992-1999
- Computer aided crime: Status Quo
- Patente, Lizenzen und Public Knowledge: GPL
- Retrocomputing: VAX/VMS
- Zertifizierungsstrukturen für Hacker (CCC-CA)
- Theorie und Praxis der Verschwörungstheorie - Praxis und Theorie der Verschwörung
- BSD-Workshop
- Internet Jugendschutz: Status Quo
- Illuminaten-Workshop
- RC5: 1 Jahr CCC-Team bei distributed.net
- Funktechnik / Treffen der Funkamateure
- Die Geldkarte als Untersuchungsobjekt
- Objektorientiertes dynamisches Programmieren
- Dummheit in Netzen, Teil 16: Datenreisen mit der Bahn
- Suchen und Finden im Internet
- Chaos project management
- TRON: Ermittlungen und Konsequenzen

```
unsigned int CSStab0[11]={5,0,1,2,3,4,0,1,2,3,4};

unsigned char CSStab1[256]={
0x33,0x73,0x3b,0x26,0x63,0x23,0x6b,0x76,0x3e,0x7e,0x36,0x2b,0x6e,0x2e,0
x66,0x7b,0xd3,0x93,0xdb,0x06,0x43,0x03,0x4b,0x96,0xde,0x9e,0xd6,0x0b,0x
4e,0x0e,0x46,0x9b,0x57,0x17,0x5f,0x82,0xc7,0x87,0xcf,0x12,0x5a,0x1a,0x5
2,0x8f,0xca,0x8a,0xc2,0x1f,0xd9,0x99,0xd1,0x00,0x49,0x09,0x41,0x90,0xd8
,0x98,0xd0,0x01,0x48,0x08,0x40,0x91,0x3d,0x7d,0x35,0x24,0x6d,0x2d,0x65,
0x74,0x3c,0x7c,0x34,0x25,0x6c,0x2c,0x64,0x75,0xdd,0x9d,0xd5,0x04,0x4d,0
x0d,0x45,0x94,0xdc,0x9c,0xd4,0x05,0x4c,0x0c,0x44,0x95,0x59,0x19,0x51,0x
80,0xc9,0x89,0xc1,0x10,0x58,0x18,0x50,0x81,0xc8,0x88,0xc0,0x11,0xd7,0x9
7,0xdf,0x02,0x47,0x07,0x4f,0x92,0xda,0x9a,0xd2,0x0f,0x4a,0x0a,0x42,0x9f
,0x53,0x13,0x5b,0x86,0xc3,0x83,0xcb,0x16,0x5e,0x1e,0x56,0x8b,0xce,0x8e,
0xc6,0x1b,0xb3,0xf3,0xbb,0xa6,0xe3,0xa3,0xeb,0xf6,0xbe,0xfe,0xb6,0xab,0
xee,0xae,0xe6,0xfb,0x37,0x77,0x3f,0x22,0x67,0x27,0x6f,0x72,0x3a,0x7a,0x
32,0x2f,0x6a,0x2a,0x62,0x7f,0xb9,0xf9,0xb1,0xa0,0xe9,0xa9,0xe1,0xf0,0xb
8,0xf8,0xb0,0xa1,0xe8,0xa8,0xe0,0xf1,0x5d,0x1d,0x55,0x84,0xcd,0x8d,0xc5
,0x14,0x5c,0x1c,0x54,0x85,0xcc,0x8c,0xc4,0x15,0xbd,0xfd,0xb5,0xa4,0xed,
0xad,0xe5,0xf4,0xbc,0xfc,0xb4,0xa5,0xec,0xac,0xe4,0xf5,0x39,0x79,0x31,0
x20,0x69,0x29,0x61,0x70,0x38,0x78,0x30,0x21,0x68,0x28,0x60,0x71,0xb7,0x
f7,0xbf,0xa2,0xe7,0xa7,0xef,0xf2,0xba,0xfa,0xb2,0xaf,0xea,0xaa,0xe2,0xf
f};

unsigned char CSStab2[256]={
0x00,0x01,0x02,0x03,0x04,0x05,0x06,0x07,0x09,0x08,0x0b,0x0a,0x0d,0x0c,0
x0f,0x0e,0x12,0x13,0x10,0x11,0x16,0x17,0x14,0x15,0x1b,0x1a,0x19,0x18,0x
1f,0x1e,0x1d,0x1c,0x24,0x25,0x26,0x27,0x20,0x21,0x22,0x23,0x2d,0x2c,0x2
f,0x2e,0x29,0x28,0x2b,0x2a,0x36,0x37,0x34,0x35,0x32,0x33,0x30,0x31,0x3f
,0x3e,0x3d,0x3c,0x3b,0x3a,0x39,0x38,0x49,0x48,0x4b,0x4a,0x4d,0x4c,0x4f,
0x4e,0x40,0x41,0x42,0x43,0x44,0x45,0x46,0x47,0x5b,0x5a,0x59,0x58,0x5f,0
x5e,0x5d,0x5c,0x52,0x53,0x50,0x51,0x56,0x57,0x54,0x55,0x6d,0x6c,0x6f,0x
6e,0x69,0x68,0x6b,0x6a,0x64,0x65,0x66,0x67,0x60,0x61,0x62,0x63,0x7f,0x7
e,0x7d,0x7c,0x7b,0x7a,0x79,0x78,0x76,0x77,0x74,0x75,0x72,0x73,0x70,0x71
,0x92,0x93,0x90,0x91,0x96,0x97,0x94,0x95,0x9b,0x9a,0x99,0x98,0x9f,0x9e,
0x9d,0x9c,0x80,0x81,0x82,0x83,0x84,0x85,0x86,0x87,0x89,0x88,0x8b,0x8a,0
x8d,0x8c,0x8f,0x8e,0xb6,0xb7,0xb4,0xb5,0xb2,0xb3,0xb0,0xb1,0xbf,0xbe,0x
bd,0xbc,0xbb,0xba,0xb9,0xb8,0xa4,0xa5,0xa6,0xa7,0xa0,0xa1,0xa2,0xa3,0xa
d,0xac,0xaf,0xae,0xa9,0xa8,0xab,0xaa,0xdb,0xda,0xd9,0xd8,0xdf,0xde,0xdd
,0xdc,0xd2,0xd3,0xd0,0xd1,0xd6,0xd7,0xd4,0xd5,0xc9,0xc8,0xcb,0xca,0xcd,
0xcc,0xcf,0xce,0xc0,0xc1,0xc2,0xc3,0xc4,0xc5,0xc6,0xc7,0xff,0xfe,0xfd,0
xfc,0xfb,0xfa,0xf9,0xf8,0xf6,0xf7,0xf4,0xf5,0xf2,0xf3,0xf0,0xf1,0xed,0x
ec,0xef,0xee,0xe9,0xe8,0xeb,0xea,0xe4,0xe5,0xe6,0xe7,0xe0,0xe1,0xe2,0xe
3};

unsigned char CSStab3[512]={
0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0
xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x
92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x4
9,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00
,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,
0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0
xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x
6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x2
4,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff
,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,
0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0
x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x
49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x0
0,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb
,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,
0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0
x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x
24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xf
f,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6
,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,
0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0
x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x
00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xd
b,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92
,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,
0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0
x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0x
ff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb
6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d
,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,
0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0
x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0x
db,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x9
2,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49
,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,
0x24,0x49,0x6d,0x92,0xb6,0xdb,0xff,0x00,0x24,0x49,0x6d,0x92,0xb6,0xdb,0
xff};

unsigned char CSStab4[256]={
0x00,0x80,0x40,0xc0,0x20,0xa0,0x60,0xe0,0x10,0x90,0x50,0xd0,0x30,0xb0,0
x70,0xf0,0x08,0x88,0x48,0xc8,0x28,0xa8,0x68,0xe8,0x18,0x98,0x58,0xd8,0x
38,0xb8,0x78,0xf8,0x04,0x84,0x44,0xc4,0x24,0xa4,0x64,0xe4,0x14,0x94,0x5
4,0xd4,0x34,0xb4,0x74,0xf4,0x0c,0x8c,0x4c,0xcc,0x2c,0xac,0x6c,0xec,0x1c
,0x9c,0x5c,0xdc,0x3c,0xbc,0x7c,0xfc,0x02,0x82,0x42,0xc2,0x22,0xa2,0x62,
0xe2,0x12,0x92,0x52,0xd2,0x32,0xb2,0x72,0xf2,0x0a,0x8a,0x4a,0xca,0x2a,0
xaa,0x6a,0xea,0x1a,0x9a,0x5a,0xda,0x3a,0xba,0x7a,0xfa,0x06,0x86,0x46,0x
c6,0x26,0xa6,0x66,0xe6,0x16,0x96,0x56,0xd6,0x36,0xb6,0x76,0xf6,0x0e,0x8
e,0x4e,0xce,0x2e,0xae,0x6e,0xee,0x1e,0x9e,0x5e,0xde,0x3e,0xbe,0x7e,0xfe
,0x01,0x81,0x41,0xc1,0x21,0xa1,0x61,0xe1,0x11,0x91,0x51,0xd1,0x31,0xb1,
0x71,0xf1,0x09,0x89,0x49,0xc9,0x29,0xa9,0x69,0xe9,0x19,0x99,0x59,0xd9,0
x39,0xb9,0x79,0xf9,0x05,0x85,0x45,0xc5,0x25,0xa5,0x65,0xe5,0x15,0x95,0x
55,0xd5,0x35,0xb5,0x75,0xf5,0x0d,0x8d,0x4d,0xcd,0x2d,0xad,0x6d,0xed,0x1
d,0x9d,0x5d,0xdd,0x3d,0xbd,0x7d,0xfd,0x03,0x83,0x43,0xc3,0x23,0xa3,0x63
,0xe3,0x13,0x93,0x53,0xd3,0x33,0xb3,0x73,0xf3,0x0b,0x8b,0x4b,0xcb,0x2b,
0xab,0x6b,0xeb,0x1b,0x9b,0x5b,0xdb,0x3b,0xbb,0x7b,0xfb,0x07,0x87,0x47,0
xc7,0x27,0xa7,0x67,0xe7,0x17,0x97,0x57,0xd7,0x37,0xb7,0x77,0xf7,0x0f,0x
8f,0x4f,0xcf,0x2f,0xaf,0x6f,0xef,0x1f,0x9f,0x5f,0xdf,0x3f,0xbf,0x7f,0xf
f
};

unsigned char CSStab5[256]={
0xff,0x7f,0xbf,0x3f,0xdf,0x5f,0x9f,0x1f,0xef,0x6f,0xaf,0x2f,0xcf,0x4f,0
x8f,0x0f,0xf7,0x77,0xb7,0x37,0xd7,0x57,0x97,0x17,0xe7,0x67,0xa7,0x27,0x
c7,0x47,0x87,0x07,0xfb,0x7b,0xbb,0x3b,0xdb,0x5b,0x9b,0x1b,0xeb,0x6b,0xa
b,0x2b,0xcb,0x4b,0x8b,0x0b,0xf3,0x73,0xb3,0x33,0xd3,0x53,0x93,0x13,0xe3
,0x63,0xa3,0x23,0xc3,0x43,0x83,0x03,0xfd,0x7d,0xbd,0x3d,0xdd,0x5d,0x9d,
0x1d,0xed,0x6d,0xad,0x2d,0xcd,0x4d,0x8d,0x0d,0xf5,0x75,0xb5,0x35,0xd5,0
x55,0x95,0x15,0xe5,0x65,0xa5,0x25,0xc5,0x45,0x85,0x05,0xf9,0x79,0xb9,0x
39,0xd9,0x59,0x99,0x19,0xe9,0x69,0xa9,0x29,0xc9,0x49,0x89,0x09,0xf1,0x7
```

#70/frühjahr 2000

die datenschleuder.

0 7 0 - 0 1 6

```
1,0xb1,0x31,0xd1,0x51,0x91,0x11,0xe1,0x61,0xa1,0x21,0xc1,0x41,0x81,0x0
1,0xfe,0x7e,0xbe,0x3e,0xde,0x5e,0x9e,0x1e,0xee,0x6e,0xae,0x2e,0xce,0x4
e,0x8e,0x0e,0xf6,0x76,0xb6,0x36,0xd6,0x56,0x96,0x16,0xe6,0x66,0xa6,0x2
6,0xc6,0x46,0x86,0x06,0xfa,0x7a,0xba,0x3a,0xda,0x5a,0x9a,0x1a,0xea,0x6
a,0xaa,0x2a,0xca,0x4a,0x8a,0x0a,0xf2,0x72,0xb2,0x32,0xd2,0x52,0x92,0x1
2,0xe2,0x62,0xa2,0x22,0xc2,0x42,0x82,0x02,0xfc,0x7c,0xbc,0x3c,0xdc,0x5
c,0x9c,0x1c,0xec,0x6c,0xac,0x2c,0xcc,0x4c,0x8c,0x0c,0xf4,0x74,0xb4,0x3
4,0xd4,0x54,0x94,0x14,0xe4,0x64,0xa4,0x24,0xc4,0x44,0x84,0x04,0xf8,0x7
8,0xb8,0x38,0xd8,0x58,0x98,0x18,0xe8,0x68,0xa8,0x28,0xc8,0x48,0x88,0x0
8,0xf0,0x70,0xb0,0x30,0xd0,0x50,0x90,0x10,0xe0,0x60,0xa0,0x20,0xc0,0x4
0,0x80,0x00
};

void CSSdescramble(unsigned char *sec,unsigned char *key)
{
    unsigned int t1,t2,t3,t4,t5,t6;
    unsigned char *end=sec+0x800;
    t1=key[0]^sec[0x54]|0x100;
    t2=key[1]^sec[0x55];
    t3=(*((unsigned int *)(key+2)))^(*((unsigned int *)(sec+0x56)
));
    t4=t3&7;
    t3=t3*2+8-t4;
    sec+=0x80;
    t5=0;
    while(sec!=end)
    {
        t4=CSStab2[t2]^CSStab3[t1];
        t2=t1>>1;
        t1=((t1&1)<<8)^t4;
        t4=CSStab5[t4];
        t6=(((((((t3>>3)^t3)>>1)^t3)>>8)^t3)>>5)&0xff;
        t3=(t3<<8)|t6;
        t6=CSStab4[t6];
        t5+=t6+t4;
        *sec++=CSStab1[*sec]^(t5&0xff);
        t5>>=8;
    }
}

void CSStitlekey1(unsigned char *key,unsigned char *im)
{
    unsigned int t1,t2,t3,t4,t5,t6;
    unsigned char k[5];
    int i;
    t1=im[0]|0x100;
    t2=im[1];
    t3=*((unsigned int *)(im+2));
    t4=t3&7;
    t3=t3*2+8-t4;
    t5=0;
    for(i=0;i<5;i++)
    {
        t4=CSStab2[t2]^CSStab3[t1];
        t2=t1>>1;
        t1=((t1&1)<<8)^t4;
        t4=CSStab4[t4];
        t6=(((((((t3>>3)^t3)>>1)^t3)>>8)^t3)>>5)&0xff;
        t3=(t3<<8)|t6;
        t6=CSStab5[t6];
        t5+=t6+t4;
        k[i]=t5&0xff;
        t5>>=8;
    }
    for(i=9;i>=0;i--)
        key[CSStab0[i+1]]=k[CSStab0[i+1]]^CSStab1[key[CSStab0
[i+1]]]^key[CSStab0[i]];
}

void CSStitlekey2(unsigned char *key,unsigned char *im)
{
    unsigned int t1,t2,t3,t4,t5,t6;
    unsigned char k[5];
    int i;
    t1=im[0]|0x100;
    t2=im[1];
    t3=*((unsigned int *)(im+2));
    t4=t3&7;
    t3=t3*2+8-t4;
    t5=0;
    for(i=0;i<5;i++)
    {
        t4=CSStab2[t2]^CSStab3[t1];
        t2=t1>>1;
        t1=((t1&1)<<8)^t4;
        t4=CSStab4[t4];
        t6=(((((((t3>>3)^t3)>>1)^t3)>>8)^t3)>>5)&0xff;
        t3=(t3<<8)|t6;
        t6=CSStab5[t6];
        t5+=t6+t4;
        k[i]=t5&0xff;
        t5>>=8;
    }
    for(i=9;i>=0;i--)
        key[CSStab0[i+1]]=k[CSStab0[i+1]]^CSStab1[key[CSStab0
        [i+1]]]^key[CSStab0[i]];
}

void CSSdecrypttitlekey(unsigned char *tkey,unsigned char *dkey)
{
    int i;
    unsigned char im1[6];
    unsigned char im2[6]={0x51,0x67,0x67,0xc5,0xe0,0x00};
    for(i=0;i<6;i++)
        im1[i]=dkey[i];
    CSStitlekey1(im1,im2);
    CSStitlekey2(tkey,im1);
}
```

0 7 0 - 0 1 7

live vom 16C3: the "streaming media broadcast project"

wer hat´s gemerkt? richtig: im buzzword-titel fehlt eins: "internet". und tatsächlich sind gestreamte videodaten im internet bei derzeit üblichen bandbreiten nach wie vor ein reichlich sinnentleertes unterfangen. was aber, wenn ein 100mbit LAN mit über 1000 clients zur verfügung steht..?

auch wenn – zugegebenermassen – die aussicht darauf, das congress-netz als high-bandwidth-spielwiese zu missbrauchen vater des gedankens war, kamen auch praktische aspekte hinzu: wenn wir das videosignal aus den drei vortragsräumen ins LAN stellten, könnte man (theoretisch) von jedem rechner aus (insbesondere unten im hackcenter) live nachsehen, was für vorträge gerade liefen – und zwar ohne in selbige reinzuplatzen... der zweite nützliche nebeneffekt: wenn die filme sowieso schon digital vorlagen, könnte man sie auch als archiv "missbrauchen" (der bisher übliche karton voller videotapes wurde diesem anspruch nur sehr rudimentär gerecht...). falls jemand beispielsweise an zwei zeitgleich ablaufenden vorträgen interessiert war, könnte er/sie sich einen vorort anschauen und den zweiten anschliessend per ftp herunterladen.

serviles

zur verfügung standen drei g4 power macintosh rechner mit video-in karte. theoretisch hätte sogar eine einzige maschine ausgereicht: als nach einigem herumexperimentieren die ideale kombination aus codec, bildgrösse, framerate und abspielverhalten feststand, lag die cpu-last der server im mittel bei 25-30%. leider warf aber die fehlende konfigurierbarkeit der verwendeten broadcast software der rechenpower und den vier pci-slots des g4 einen dicken knüppel zwischen die beine. doch nicht nur das: der "sorenson broadcaster" bot zwar eine unschlagbare mischung aus streamgrösse und bildqualität (interessanterweise nicht mit dem hauseigenen vorzeige-format "sorenson video", das auch von apple gerne zum angeben benutzt wird, sondern mit dem "guten alten" H.263 codec) und war innerhalb weniger minuten komplett konfiguriert, aber leider auch bis unter die halskrause voll mit bugs. die versionsnummer "1.0" war eine frechheit sondergleichen. "alpha mit feature-freeze" wäre passender gewesen. dazu später mehr.

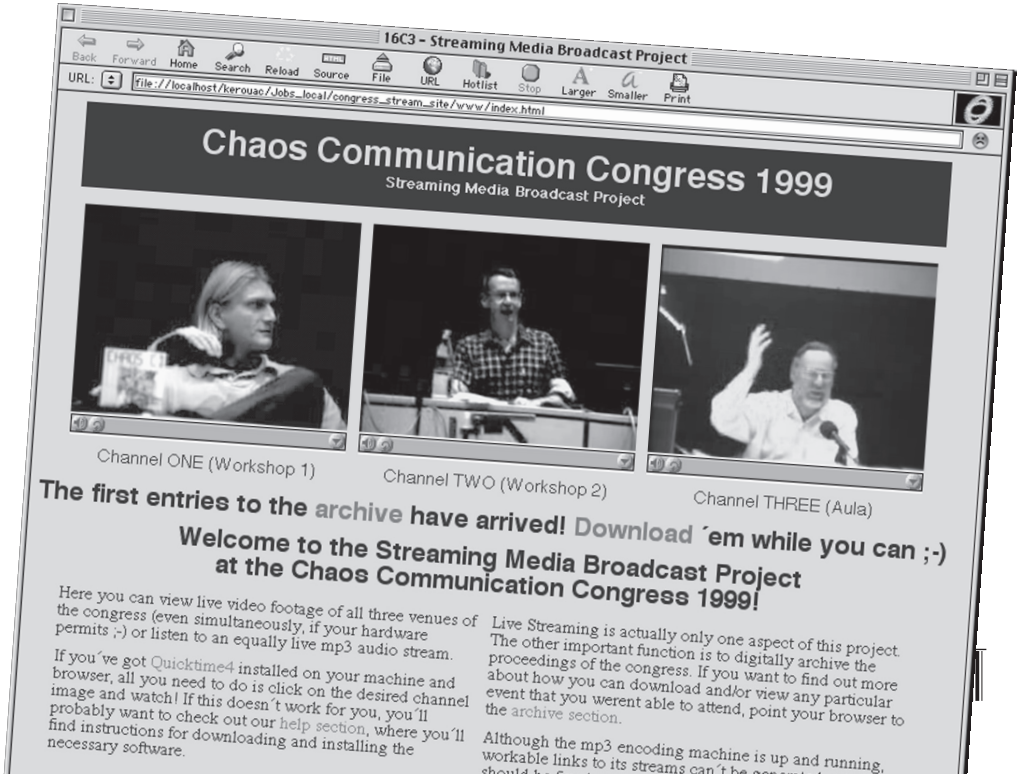
proprietäres

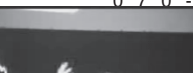
der sorenson broadcaster "verpackt" den video- und audiostream mit einem quicktime-header, was (in unserem fall) eigentlich nicht zwingend notwendig war, da nur nicht-proprietäre codizes verwendet wurden. das hatte den unangenehmen nebenenffekt, das client-seitig nur quicktime-unterstützte betriebssysteme in frage kamen, was die auswahl auf Mac-OS und die diversen windows plattformen eingrenzte. der vorteil: das quicktime paket enthält auch einen player in form eines browser-plugins, d.h. sowohl die verteilung der multicast-adressen und der notwendigen streaming-parameter als auch das eigentliche abspielen konnten mittels <EMBED>-tag http-basiert auf einer gewöhnlichen html-seite erolgen. bei installiertem plug-in reichte ein klick auf eines der "GIF-dummies" der projekt-site und die vorstellung ging sofort los – siehe screenshot.

(den framebuffer konnten wir aufgrund der idealen netzbedingungen gefahrlos auf null herunterschrauben)

ersichtliches

das ganze klappte erstaunlich gut: die jungs vom NOC hatten für alle subnetze multicast bereitgestellt und selbst auf einem 233 MHz iMac konnten alle drei streams mit jeweils 320 x 240 pixel bei butterweichen 25 frames per second *gleichzeitig* abgespielt werden. ein rundgang im hackcenter am zweiten tag förderte dann auch mehr als nur einen als fernseher umfunktionierten webbrowser zutage. auch die iMac-terminals vor der aula fanden zeitweise regen zuspruch - ruckelfreie videobilder auf denen man (mitunter, mitunter…) sogar die schrift auf den overhead-folien entziffern konnte waren eben doch etwas anderes als die animierten briefmarken, die man sonst von websites mit streaming video kennt…



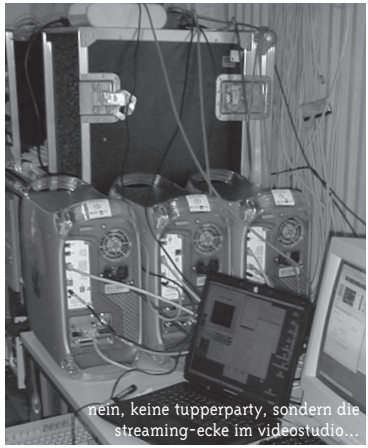


debiles

ganz anders sah die sache allerdings beim angestrebten archivaufbau aus. ursprünglich war gedacht, die aufzeichnung des streams auf den drei maschinen einfach den ganzen tag über durchlaufen zu lassen, um dann in der nacht auf den nächsten tag die einzelnen vorträge aus den riesendateien herauszuschneiden. das fand ich – neben dem angenehmen effekt, nicht nach jedem veranstaltungsblock rauf ins videostudio rennen zu müssen – auch deshalb furchtbar schlau, weil ich dadurch flexibel auf verspätungen und änderungen reagieren koennte. theoretisch, zumindest. in der praxis passierte montag (dem ersten tag) abends erstmal folgendes: auf zwei der maschinen quittierte der server den "stop"-befehl für den aufzeichnungsvorgang zunächst mit einem lapidaren "could not complete the request, because an error occurred". (übrigens eine meiner absoluten lieblingsfehlermeldungen des MacOS, wennn auch weit abgeschlagen von "not enough memory to display the", aber ich schweife ab…) die trotz dieser meldung entstandenen filme hatten dann aber zum glück die volle aufzeichnungslänge von immerhin neun stunden – allerdings nur auf der audiospur… der videoteil zeigte nach ein paar minuten nur noch ein schickes graues standbild. zum glück aber war wenigstens der stream der dritten maschine heil und vollständig – nur dass der tolle sorenson broadcaster beim nächsten programmstart ungefragt(!!) die bisherige aufzeichnungsdatei _überschrieb_ und innerhalb von sekunden einen 700 mb film unwiederruflich in wenige K verwandelte.

alles in allem also eine ziemlich magere ausbeute für den ersten tag. lediglich die (später stattfindende) tron-veranstaltung wurde anstandslos und vollständig für die nachwelt erhalten.

wie sich herausstellte, hat die serversoftware ein problem mit grösseren dateien – ein umstand, der bei den wenigen zeitlich möglichen probeläufen leider nicht zutage trat.. während das broadcasten den ganzen congress über problemlos weiterlief (von vereinzelt auftretenden allgemeinen netzwerkfehlern mal abgesehen), geriet das abspeichern der aufgezeichneten streams zu einem lotteriespiel mit fünfzigprozentiger gewinnchance…



nein, keine tupperparty, sondern die streaming-ecke im videostudio…

konservatives

da videochef frank und die kamera- und mikrofon-engel trotz des beengten chaos im videostudio ganze arbeit geleistet hatten, hat die mehrzahl der aufzeichnungen durchaus dokumentationscharakter. vor allem die aufzeichnungen aus der aula, wo mit zwei kameras und mehreren saalmikros gerarbeitet wurde, vermitteln einen recht brauchbaren eindruck nicht nur davon, was vorgetragen wurde, sondern auch wie die stimmung im saal war.

deshalb wurde beschlossen, zumindest teile der missglückten streamaufzeichnung von den svhs-bändern manuell nachzudigitaliseren. eine liste der insgesamt daraus entstandenen quicktime movies findet sich am ende des artikels. bei typischen dateigrössen von 120 bis 200 mb schied leider die möglichkeit aus, eine master-cd mit allen filmen zu brennen, die dann bei bedarf kopiert und verschickt werden könnte. deshalb möchten wir interessierten folgendes anbieten: unter http://tomster.org/chaos/16c3-video/form.html könnt ihr einerseits per webformular eine wunschliste von filmen zusammenstellen, die ihr gerne digital vorliegen hättet und andererseits kundtun, ob ihr euch die monsterbrocken auch per ftp herunterladen würdet. bei ausreichendem interesse könnten dann z.b. cd-compilations mit den meistgewünschten filmkombinationen gemastert werden, die dann bestellt werden können und/oder filme zum download angeboten werden.

zukünftiges

beim nächsten congress wird natürlich alles besser :-) das MacOS wird dann womöglich tatsächlich multitasking, shell-zugriff und scripting vorweisen; falls sorenson bis dahin nicht mit einer 2.0 version des broadcasters aufwartet, die den namen auch verdient, bleibt vielleicht wenigstens genügend zeit, eine open source variante unter MacOS X lauffähig zu machen. damit würden dann z.b. features wie datenbankgesteuertes aufzeichnen und benennen der streams möglich (eine art vps, wo verspätungen und änderungen zentral erfasst und gepostet werden können; der download aufgezeichneter streams könnte unmittelbar nach veranstaltungsende direkt aus dem congress-fahrplan heraus und mit voller LAN-geschwindigkeit auf den mitgebrachten rechner erfolgen). denkbar wäre auch ein "sauberer" stream, der auch von nicht-proprietären playern abgespielt werden kann. oder mp3 als format für den audiotrack. oder unterschiedliche streamvarianten für LAN/CD-archiv und internet-broadcast/ftp download. oder, oder, oder…

naja, mal sehen… :-)

<tom@tomster.org>

Unstimmigkeiten bei angeblichen DoS-Attacken gegen NetCologne im Feburar 2000

Seit dem nicht-eingetretenen Jahr-2000-Bug hat sich im Internet etwas verändert. Nach Angriffen auf Internetserver wie den ungeklärten "Distributed Denial of Service"-Attacken gegen Yahoo, Amazon, eBay u.a. ist es chic geworden, sich mit durch "Hackern" verursachten Ausfällen zu schmücken.

Wir erleben hier einen regelrechten Paradigmenwechsel in Bezug auf die behauptete Kompetenz in Sachen Internet: Während es früher peinlich war, den Kunden keinen Service mehr bieten zu können, wird jetzt ein Angriff aus dem Internet zum Gütesiegel: Seht her, auch wir sind so wichtig wie Yahoo, auch unsere Systeme werden plattgemacht.

Da passt es ins Bild, dass jetzt auf bundespolitischer Seite "Task Forces" gebildet werden und mutmassliche Schwerkriminelle gejagt werden, bei denen es sich vielleicht nur um Jugendliche handelt, die das elektronische Pendant zum Klingelstreich etwas überzogen haben. Bei all dem scheint in Vergessenheit zu geraten, dass keine der momentan so heftig diskutierten Angriffsmethoden neu ist. Jahrelang konnte man anscheinend mit den TCP/IP-Protokollen und seinen Schwächen leben, aber jetzt ist Schluss mit lustig. Weil Werbebildchen aufgrund der Angriffe ein paar Minuten nicht erreichbar waren, werden jetzt härtere Geschütze aufgefahren.

Was genau bei NetCologne im Februar 2000 passierte, können wir auch nicht sagen. Es ergibt sich aus den Ankündigungen des Telekommunikationsunternehmens an seine Kunden und der Schnelligkeit im Zugriff auf "Notty", der als Täter präsentiert wurde, allenfalls ein schemenhaftes Bild, das zu viele Fragen offen lässt.

Chronologie der Ereignisse

Die ganze Geschichte fing damit an, daß NetCologne am 10.2. in seiner Support-Newsgruppe von Schwierigkeiten berichtete:

Morgens hieß es, die "Einwahlrouter" hätten in den letzten Tagen Probleme, was zu Verbindungsabbrüchen und langsamen Internetverbindungen führe. Obendrein hätte es am 9.2 gegen 19:00h "eine Störung eines Segments des Hauptrouters" gegeben. Das klang bis dahin plausibel.

Am Nachmittag gibt es dann eine Rundmail an alle Kunden, daß am Wochenende die

"Teilnehmer-Vermittlungsanlage" erweitert werden würde und daß dadurch mit Ausfällen zu rechnen sei. Das klingt ebenfalls plausibel, denn Basteleien an der Telefonanlage können sicher auch mit den Einwahlproblemen in Verbindung stehen.

Diese Meldung ist allerdings nicht, wie sonst Üblich, auf dem NetCologne Newsserver archiviert.

Abends ist dann davon die Rede, daß die Probleme am Hauptrouter die Interneteinwahl behindert hätten. Das klingt wenig überzeugend, denn NetCologne wird sicher nicht seinen zentralen Router gleichzeitig als Dial-In-Server verwenden. Wie dem auch sei, nachts würde das Gerät ausgetauscht und "in andere Räumlichkeiten verlegt."

Am 12.2. gab es dann wieder eine Rundmail an alle Kunden. Darin wurden plötzlich die "drastischen Behinderungen" beim Internetzugang mit Denial-of-Service-Angriffen aus dem Internet begründet. Keine Rede mehr von den Problemen mit dem Dial-In-System, dem Austausch und Umzug des Hauptrouters und der Erweiterung der Telefonanlage.

Statdessen war man aus dem Intenet angegriffen worden und stand damit in einer Reihe mit yahoo, eBay und CNN. Aber im Gegensatz zum Rest der Welt, der verzweifelt nach den Tätern suchte, konnte NetCologne am Donnerstag "die Herkunft der Attacken jedoch nach kurzer Zeit feststellen" und den Täter lokalisieren. Am Freitag hätten sie dann "den Betreiber des DFN informiert" und den Verkehr aus dem DFN (Deutsches Forschungsnetz) blockiert.

Es gibt auch eine Pressemeldung mit diesem Inhalt, die auf den 11.2. datiert wurde, allerdings erst seit dem 18.2. auf dem Webserver steht. Der c4 war verwundert. Am 13.2. meldet dann auch der Heise Verlag Cyber-Terror auch gegen deutsche Web-Sites.

Einige Tage gab es dann eine Agenturmeldung NetCologne-Saboteur gefasst die die Zeitungen praktisch unverändert übernahmen. Darin war die Rede von einem n0tty, der gestanden haben solle, die Störungen verursacht zu haben. Mit "Spezialprogrammen" habe er NetCologne solange mit sinnlosen Anfragen bombadiert, bis die NetColognes Netzverbindung gekappt gewesen sei. Er habe Internetzugänge von Studenten zur Verschleierung genutzt und sei jetzt in seiner "mit gestohlener Elektronik vollgestopften Wohnung" gefaßt worden. Der Schaden beliefe sich auf etwa 500.000 DM.

Nur die Futurezone vom Österreichischen Rundfunk hat offensichtlich nicht nur die Agenturmeldung abgeschrieben.

Gleichzeitig kam aus der IRC-Szene eine andere Version der Geschichte:

Das fängt damit an, daß es keinen "n0tty" gäbe, sondern nur einen not4you, der auch manchmal "notty" genannt werden würde. notty habe nicht das Know-How einen ganzen Internetprovider lahmzulegen. Er habe einen Shell-Account auf deneb.informatik.uni-mannheim.de benutzt, um dort den IRC-Bouncer redirect laufen zu lassen. Damit habe er, wie im IRC durchaus üblich, einen User bei ndh.com kurz mit einem UDP-Flood beglückt. Der Flood habe knapp drei Stunden gedauert.

Der Autor von redirect meint dazu:

Redirect benutzt den standard socket API fuer UDP pakete, und versucht in keinster weise die source adresse zu faelschen (also kein spoofing), somit ist es unmoeglich damit eine sog. "smurf"-attacke (in der UDP-variante analog zu "papasmurf") zu machen.

Daraus folgert, dass n0tty, um NetCologne lahmzulegen, mit seiner shell von uni-mannheim aus mehr traffic machen muesste als NetCologne. Ich bezweifle jetzt einfach mal dass uni-mannheim besser angebunden ist als NetCologne – was aber noetig waere, damit n0tty NetCologne lahmlegen haette koennen.

… der Vorhang zu und alle Fragen offen

Die ganze Angelegenheit ist ist in erster Linie mysteriös. Die Ermittlungen werden hoffentlich zeigen, was von den Vorwürfen gegenüber Notty haltbar ist. Zweifel an der verkürzten Fassung, er habe alleine eine der grössten privaten Telefongesellschaften Deutschlands lahmgelegt, müssen erlaubt sein, wenn man sich das Zusammenspiel der Pannenmeldungen bei Netcologne ansieht:

Was war denn jetzt bei NetCologne kaputt? Die Telefonanlage, die Einwahltechnik oder der zentrale Router?

Es ist im Prinzip löblich, die Kunden über einen Ausfall zu informieren. Es kann auch vorkommen, dass verschiedene Theorien über einen Ausfall innerhalb des Unternehmens existieren. Aufgrund der verwirrenden Unterschiedlichkeit, mit denen NetCologne die nicht erbrachten Leistungen im Februar zu erklären versuchte, wäre hier vielleich ein abschliessendes Statement angebracht gewesen.

Warum ist die Meldung über die Erweiterung der Telefonanlage nicht auf dem NetCologne Newsserver?

Hier kann es eine einfache Erklärung geben: Vielleicht arbeiten bei NetCologne ja nicht nur blitzgescheite Leute, die in Windeseile gefürchtete Hacker lokalisieren können, sondern auch Menschen mit Fehlern, die bei den Kundenrundschreiben nicht mehr durchblicken und eine Archivierung auf dem Newsserver vergessen. Diese könnte eine mögliche Erklärung sein. Die andere Möglichkeit, dass hier Spuren verwischt wurden, würde die ganze Sache unangenehmer aussehen lassen, als es NetCologne lieb sein kann. Bis zur abschliessenden Klärung bleibt da nur die Spekulation.

Warum ist die Pressemitteilung auf dem Webserver zurückdatiert?

Auch hier kann es einfache Erklärungen geben. Allerdings ist es schon seltsam, dass sich hier bezogen auf den gleichen Vorgang wieder Unstimmigkeiten in der Archivierung auf dem Rechner ergeben.

Warum sprechen alle von n0tty anstatt notty? Gibt es keinen Journalisten in Deutschland, der selbst recherchiert?

Interessanterweise gibt es im IRCNet tatsächlich einen Teilnehmer namens n0tty, der 24 Stunden online ist. Ihn hätte man ja einfach zu der Geschichte fragen können. Alternativ hätte ein "/whois n0tty" gereicht, um herauszufinden, dass es sich hier nicht um einen menschlichen Chat-Teilnehmer, sondern um einen Bot handelt.

Wie wurde der Schaden von 500.000 DM berechnet? Bekommen die NetCologne-Kunden, deren Internetzugang gehemmt war, etwas davon ab?

Im Zusammenhang mit Angriffen aus dem Internet werden gerne phantasievolle und eindrucksvoll große Zahlen genannt. Wenn man sich allerdings vor Augen führt, dass bei NetColognes Internet-Service hauptsächlich laufende Kosten auftreten, die bezahlt werden müssen, egal ob die Kunden das Angebot nutzen konnten oder nicht, relativiert sich das ganze wieder. Durch DoS-Attacken wird kein

Equipment zerstört, es wird nur für die Dauer des Angriffs quälend langsam. Da NetCologne monatliche Pauschalpreise berechnet, sind die einzigen Leidtragenden letztendlich die Kunden: Sie können eine bereits bezahlte Leistung nicht in Anspruch nehmen. Es bleibt abzuwarten, wieviel Geld NetCologne seinen Kunden überweist.

Wie wurde herausgefunden, daß ein Rechner an der Uni Mannheim und nicht etwa die Umbauten am eigenen System das Problem verursachte?

Interessant ist das schon: Erst Chaos beim Umbau, Umzug des zentralen Routers und dann ein paar Stunden später die Gewissheit, dass Angriffe von ausserhalb der Grund waren.

Wie wurde herausgefunden, daß von allen Usern von deneb.informatik.uni-mannheim.de grade notty der Angreifer war?

Entgegen einem verbreiteten Irrglauben stehen in UDP-Datenpaketen keine Usernamen oder E-Mail-Adressen. Lediglich ein Systemoperator auf dem entsprechenden Rechner der Uni Mannheim hätte herausfinden können, welcher Benutzer gerade eine Angriffsprogramm gestartet hatte. Auf NetCologne-Seite wäre lediglich als Absenderadresse deneb.informatik.uni-mannheim.de angekommen.

Wie kann ein einzelner Recher im DFN das gesamte NetCologne System lahmlegen, wenn nur eine 2 MBit Anbindung zum DFN besteht und 6 weitere Außenanbindungen mit insgesamt knapp 500 MBit bei NetCologne vorhanden sind?

Allen Attacken, die in letzter Zeit als DoS oder DDoS Schlagzeilen gemacht haben ist gemeinsam, daß es sich hierbei um Flooding handelt, d.h. man schickt einem System mehr Daten als es selbst oder seine Netzanbindung verkraften kann. Mit 2 Megabit Bandbreite sollte es nicht möglich sein, die Systeme eines grossen Internetproviders zu überfluten.

Warum wurde das DFN erst einen Tag später über den Mißbrauch informiert?

Wenn man von Rechnern einer doch recht seriösen Organisation, wie dem DFN, angegriffen wird, dann läßt sich mit ziehmlicher Sicherheit sagen, daß dort ein Rechner gehackt wurde. Im Sinne der schnellen Problembeseitigung ist es in einem solchen Fall sicher ratsam, sich bei dem Betreiber des entsprechenden Rechners zu melden und ihn auf das Problem hinzuweisen.

Warum wurde nicht schon am Donnerstag Abend, nachdem bekannt war, daß der Angriff von einem Rechner kam, dieser am Border-Router gefiltert?

Wenn das gesamte deutsche Forschungsnetz mit allen Universitäten und Forschungsinstituten abgehängt wird, bedeutet das für NetCologne-Kunden auch, dass sie keinen Zugriff mehr auf viele wichtige deutschen FTP-Server mehr haben. Auch hier hätten die Kunden eigentlich eine Erklärung verdient, warum ihnen diese Dienste vorenthalten wurden. Ob sie sich damit zufrieden geben, dass es eine Schnellschussaktion war, ohne Rücksprache mit dem DFN?

Da naheliegenste wäre es gewesen, einfach nur an dem Router zum DFN den einen Rechner, von dem die Angriffe aus erfolgten, zu filtern. Dies wäre mit minimalem Aufwand und Kosten möglich gewesen und hätte das Problem augenblicklich beseitigen sollen. Warum dieser Weg nicht gewählt wurde, ist unverständlich.

Warum wurde das DFN-CERT (Computer Emergency Response Team des Deutschen

Forschungsnetzes, zuständig für Sicherheitsprobleme und Angriffe auf Computersysteme im Zusammenhang mit DFN-Systemen) nicht informiert?

Ganz oben auf in jedem IT-Notfallplan steht die Kontaktaufnahme mit dem entsprechenden CERT. Dort sitzen die Experten, die Rat geben können, aber auch dafür sorgen, daß andere Betroffene gewarnt werden und Gegenmaßnahmen koordiniert erfolgen können. Sicher mag dies manchmal im Trubel eines Störfalls vergessen werden, aber professionelle Systemadministratoren sollten auch bei Problemen einen kühlen Kopf behalten.

Und nun?

In der Tat leben wir, wie es in dem alten chinesischen Fluch heisst, in interessanten Zeiten. In jedem Krieg ist das erste Opfer immer die Wahrheit. Es ist nicht zu hoffen, dass beim Krieg um Marktanteile im Telekommunikationsmarkt wieder Fakten auf dem Schlachtfeld zurückbleiben. Interessant sind an der Geschichte neben den vielen technisch zweifelhaften Details auch die einstimmigen Erklärungen, mit der sich Presse und Politik quasi geschlossen an der Panik um die DoS-Angriffe beteiligen.

Auf den CCC kommen neue Aufgaben zu

Während wir jahrelang vor übertriebener Naivität in Zusammenhang mit dem Internet gewarnt haben, müssen jetzt versuchen, die Diskussion zu versachlichen: Cyberterrorismus ist das alles nicht. Wenn Rechner langsamer laufen und nicht mehr erreichbar sind, dann ist das für die Betreiber der Server schlimmstenfalls lästig, aber nicht mit dem Terrorismus zu vergleichen, bei dem in der echte Welt echte Bomben hochgehen und echte Menschen getötet oder verstümmelt werden. Wer sich "Hacker-Attacken" aus Prestigegründen für das eigene "E-Business" herbeiwünscht und diese dann auch noch als Terroranschläge bezeichnet, muss sich fragen lassen, welchen politischen Hardlinern er damit Munition liefert.

Sicherlich gibt es auch im Bereich der staatlichen Sicherheitsorgane die Bestrebung, unter Beweis zu stellen, daß man auch im Internet fü Recht und Ordnung im deutschesten aller Sinne sorgen kann. Pessimisten befürchten, daß bald an irgend einem armen Wesen wie notty disbezüglich ein Exempel statuiert wird.

Jens Ohlig, doobee

CRM und Data Mining – ein Überblick

„Businesses have a gold mine of information about their customers"

In Zeiten eines verschärften Wettbewerbs haben die Unternehmen, um wettbewerbsfähig zu bleiben, bisher auf eine ziemlich simple Strategie gesetzt: Sie versuchen ihre Produkte einfach billiger an den Mann zu bringen, als die Konkurrenz.

Da das nur bis zu einem gewissen (Tief-)Punkt möglich ist, kommt - mal wieder - die neueste Idee aus Amerika: CRM (Customer Relationship Management). Dem Kunden soll nicht nur ein optimaler Service geboten werden, sondern es geht um die systematische und auf die Bedürfnisse der unterschiedlichsten Kunden abgestimmte Pflege von Beziehungen.

CRM steht für Customer Relationship Management: Damit ist die komplette Ausrichtung der Unternehmensorganisation auf bestehende und potentielle Kundenbeziehungen gemeint. Das Kundenmanagement wird dabei unternehmensweit über alle Funktionen hinweg durch Informationstechnologien unterstützt. Über die Bereiche Marketing, Vertrieb und Service werden z.B. das Internet und das Call Center im Sinne einer totalen Kundenorientierung eingeschlossen.

Die strategische Zielsetzung des CRM liegt in der Maximierung der Kundenbindung (also: profitable Kunden und bestehende Kunden halten und aufbauen, neue Kunden hinzugewinnen), der Maximierung der Kundenprofitabilität und der Maximierung der Effizienz im Kontaktmanagement.

Zwei Beispiele:

1. Der Bewohner eines siebten Stockwerks im Hochhaus wird vermutlich keinen Gartenteich kaufen wollen, ihm Angebote zuzusenden wäre wohl ziemlich sinnlos, wenn nicht gar kontraproduktiv; u. U. ärgert er sich ja derart über diese unverlangte und ungezielte Werbung, dass er das Unternehmen in Zukunft meidet. Sinnvoller wäre es, ihm z.B. Angebote über Zimmerpflanzen zu unterbreiten.
2. Ein schweizerisches Heizöl-Unternehmen verkauft nicht nur Öl, es verwaltet den Tank seiner

Kunden. Anhand von Kundendaten und Wettereinflüssen wird kalkuliert, wann der Tank leer sein wird. Kurz bevor der Kunde frieren müsste, bekommt er ein Angebot der Firma zugesandt.

Das alles klingt doch recht vielversprechend. Das Unternehmen sammelt Daten über seine Kunden und wertet diese im Sinne der individuellen Bedürfnisse des Kunden aus, macht ihm maßgeschneiderte Angebote, bietet optimalen Service und so sind beide Seiten zufrieden: Das Unternehmen prosperiert, der Kunde ist glücklich!

So ist es leider nicht (ganz): es geht natürlich nicht darum, dem Kunden aus altruistischen Gründen einen hervorragenden Service zu bieten und ihn so froh und glücklich zu machen, dass er die Konkurrenz fortan meidet; es geht um die optimale Ausschöpfung der Kundenbasis, um den Profit zu maximieren.

Um an Kundendaten heranzukommen, bedienen sich Unternehmen der unterschiedlichsten Wege: So gibt es in Deutschland 1300 registrierte Adressenhändler, bei denen Unternehmen einkaufen können. Die Schober Direktmarketing GmbH, Deutschlands größter privater Datensammler, verfügt über 60 Millionen Adressen mit einer Milliarde Daten (sie kennt: „...90 Prozent der Deutschen. Er [der Geschäftsführer] weiß, wer ein Garagenparker ist, wer lieber für die Deutsche Kriegsgräberfürsorge spendet statt für Greenpeace, er weiß, wer in der Familie die Hosen anhat, wer geizig ist oder arm genug, um mit Frau und Kindern eine Nacht in einer Jugendherberge zu schlafen; er kann sehen, wer seinen Mercedes bar bezahlt...“). Laut einem Bericht im Spiegel (Nr. 27/ 1999) ist jeder Bundesbürger über 18 Jahre in durchschnittlich 52 kommerziellen Datenbanken erfaßt. Um an die Daten zu herankommen, werden nicht nur Telefonbücher, Zeitungsanzeigen, Aushänge in Behörden, Messekataloge, Einwohnermeldeämter, repräsentative Umfragen und Luftbilder ausgewertet; es werden auch Fragebögen verschickt, die einen Hauptgewinn im Preisausschreiben versprechen, natürlich nur, wenn vorher 125 Fragen über Konsumgewohnheiten und Kaufabsichten beantwortet werden.

Versand- und Kaufhäuser haben da subtilere Methoden, sie haben naturgemäß einen guten Überblick über Einkommensverhältnisse, Konsumverhalten und Vorlieben ihrer Kunden (der Otto-Versand etwa verfügt über eine Kartei mit 22 Millionen Adressen und Kundenprofilen; das Versandhaus Quelle filtert aus den Onlinebestellungen seiner 41 Millionen Kunden deren Vorlieben heraus und unterbreitet darauf abgestimmte Angebote).

Mittlerweile hat auch der stationäre Handel die Zeichen der Zeit erkannt. Karstadt z.B. gibt eine Kundenkarte heraus. Bisher werden darauf zwar nur die Abteilungen gespeichert, in denen der Kunde gekauft hat, doch wird bereits der Bau eines Data Warehouses geplant, um so in Zukunft das Verhalten eines jeden Kunden schnell und effektiv analysieren zu können. Über Kundenkarten erhalten Unternehmen nicht nur Informationen über Kaufgewohnheiten der Kunden, sondern auch über deren Finanzlage, Risiko- und Entscheidungsfreudigkeit, Hobbys, Kontakte, Arbeitszeiten.

Mit Hilfe des Data Mining können detaillierte Persönlichkeitsprofile der Kunden ausgearbeitet werden; der Einzelhandelskonzern Wal Mart unterhält ein 24 Terabyte großes Data Warehouse. Die beiden größten Handelsketten der Vereinigten Staaten - Wal Mart und K-Mart arbeiten seit Weihnachten 1999 mit AOL bzw. Yahoo zusammen und Wal Mart will ab ca. April in Zusammenarbeit mit AOL einen

eigenen Internet-Zugang für seine Kunden anbieten.

Bislang hat noch kein Unternehmen die Kunden gefragt, was sie von der Datensammlung und -auswertung und den daraus resultierenden Marketingstrategien halten. Den meisten Kunden ist wohl auch völlig unklar, welche Möglichkeiten sie einem Händler eröffnen, wenn sie das Kleingedruckte in einem Vertrag unterschreiben („Der Kunde erklärt sich damit einverstanden telefonische Angebote zu erhalten", „Ich bin damit einverstanden, dass die zu meiner Person gemachten Angaben zu Werbezwecken elektronisch gespeichert und verarbeitet werden").

Um den Datenschutz ist es mal wieder schlecht bestellt: Die Regeln der Europäischen Kommission in Brüssel legen zwar sehr restriktiv fest, was ein Unternehmen darf, aber diese Regeln werden oft nicht angewandt oder sind schlicht unbekannt.

Natürlich werden auch die Kaufgewohnheiten der Internetkunden gewissenhaft untersucht und ausgewertet: die US-Marketingagentur DoubleClick verfolgt die Bewegungen ihrer zwei Millionen Nutzer genau: Gespeichert werden Name, Adresse, Haushaltsgröße und Einkaufspräferenzen.

Das Sammeln und Aufbewahren personenbezogener Daten zu Markforschungszwecken ist in Deutschland ohne ausdrückliches Einverständnis des Kunden verboten. Nutzungsprofile sind z.B. nur erlaubt, wenn sie mit einem Pseudonym versehen sind, das keinen Rückschluss auf seinen Träger zulässt, doch sobald Daten auf ausländischen Servern gelagert werden, gelten andere Regeln. Die strengen deutschen Bestimmungen werden z. B. mit Formulierungen wie: „Der Provider teilt mit, dass er bestimmte Daten des Kunden an Dritte weiterleitet, so weit es im Rahmen der Anwendung internationaler Datennetze üblich oder vorgegeben ist" unterlaufen.

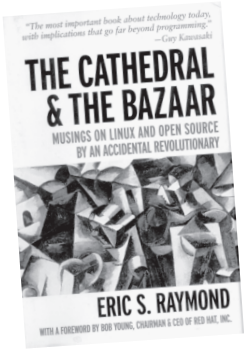
US-Intershops setzen auf das so genannte Collaborative Filtering, d.h. mehrere Händler tauschen untereinander Daten aus, um Kunden mit gleichen Vorlieben gezielt Produkte anzubieten. Auch hier von Datenschutz keine Spur: Eine Studie unter den 100 größten E-Commerce-Unternehmen in den USA hat ergeben, daß auf 18 Prozent aller Angebotsseiten der Hinweis fehlt, welche Daten gesammelt werden. So mancher Anbieter erlaubt sogar externen Vermarktern, die Surfbewegungen der Nutzer mit zu verfolgen.

Ganz raffiniert gehen Unternehmen vor, die - wie z.B. die Firma GMX in München - eine kostenlose E-Mail-Adresse anbieten: Wer das Angebot nutzen möchte, muß persönliche Daten herausrücken, z.B. Beruf, Familienstand und Wohnort, freiwillig können auch das Einkommen und Ausbildung angegeben werden. Angeblich sollen die Nutzerprofile nur anonymisiert weitergegeben werden. Naja.

In Deutschland sieht es übrigens - noch - recht gut aus: In einer Studie der amerikanischen Unternehmensberatung Meta-Group gaben ausnahmslos alle amerikanischen Unternehmen an, sich mit CRM zu beschäftigen. In Deutschland sind es bisher nur 40 Prozent.

henriette hiebig

the cathedral and the bazaar



by eric s. raymond

klappentexte sparen in der regel nicht mit bombastischen attributen. so auch in diesem fall. die sammlung diverser essays von eric raymond zu den themen linux, open source und hackertum wird dort beworben als ein "manifest", das einen "meilenstein" darstelle und die "revolutionäre [...] open-source-bewegung definiere". das ist schade. der potentielle leser könnte an dieser stelle ja denken, das es zwischen den buchdeckeln ebenso anbiedernd, reisserisch und selbstgefällig weiterginge. aber raymond erweist sich als das genaue gegenteil - ein echter glücksfall. zusätzlich zu seiner technischen qualifikation als langjähriger hakker (er ist unter anderem gründer der opensource foundation und autor von `fetchmail`, einem nicht unbedeutendem stück freier software in unix- und linux-kreisen) erweist er sich als scharfer beobachter, dessen sprache seinen analysen in klarheit, präzision und intelligenz um nichts nachsteht.

in den fünf essays (die alle auch frei im internet verfügbar sind) bietet er sowohl antworten auf eher allgemeine fragen wie "was sind eigentlich hacker?" und "wie(so) funktioniert open source?" als auch auf konkrete von "wie stelle ich fest, ob opensource das richtige business modell für mein projekt/unternehmen ist?", über "was für open source business modelle gibt es überhaupt?" bis hin zu "was muss ich tun, um selbst hacker zu werden?". (letzteres glücklicherweise nicht ohne das nötige augenzwinkern...)

eric raymond hat es geschafft, der open-source bewegung in ihrer gesamtheit (von einem idelogisch motiverten richard stallman und dessen free software foundation bis hin zu einem kommerziellen unterfangen wie netscapes mozilla projekt) ein eigenes bewusstsein zu geben. das heisst, er analysiert und beleuchtet ein phänomen, das bis dato trotz seines zunehmenden erfolges und der daraus resultierenden erhöhten öffentlichen aufmerksamkeit noch nicht einmal von seinen eigenen vertretern und teilnehmern so richtig verstanden wurde. von den jungs aus redmond und von der wallstreet ganz zu schweigen.

ein wichtiger (und teilweise kontrovers diskutierter) aspekt von raymonds position scheint auch in diesen essays immer wieder durch. in seiner aussage, dass das open source modell an sich das *bessere* im gegensatz zum proprietären sei, weist er nachdrücklich darauf hin, das er das adjektiv "besser" hier weniger im moralischen sinn versteht (wie richard stallman das beispielsweise tut) sondern durchaus im sinne von "effektiver" und "zukunftsträchtiger". ("it just makes more sense.") für ihn folgt daraus auch, dass open source software (bei vergleichbarem feautureumfang?) proprietären lösungen qualitativ überlegen ist.

wer das sowieso schon immer geglaubt hat, wird das buch wahrscheinlich mit freude von anfang bis ende verschlingen. alle anderen sollten es *trotzdem* lesen. sie könnten sich durchaus die eine oder andere zukünftige blamage ersparen... **<tom@tomster.org>**

"the cathedral and the bazaar - musings on linux and open source by an accidental revolutionary", o´reilly, october 1999, isbn 1-56592-724-9, dm 40,– (z.b. unter http://www.lob.de) die texte sind auch auf raymonds homepage unter `http://www.tuxedo.org/~esr/` veröffentlicht.)

RFID Handbuch

Klaus Finkenzeller:

In Berlin hat der Feldversuch der Berliner Verkhersgesellschaft (BVG) mit Tickets in Form von Transponder ("tick.et", www.ticket.de) einige Aufmerksamkeit erregt. Die Herren von der BVG sind aber weder die ersten noch die einzigen, die mit dieser Technik herumspielen.

Die zugehoerige Technik ist unter dem Namen RFID bekannt: Radio Frequency IDentification. Zu den Hintergruenden dieser Technik existiert eine Fuelle an Infoblaettern, Memos und aehnlichem Blaetterwald, deren Zusammensuchen keine wirklich spassige Sache ist.

Vermutlich aus diesem Grund hat Klaus Finkenzeller ein Buch zu diesem Thema geschrieben: Das "RFID Handbuch", 2000 in der zweiten Auflage im Hanser Verlag erschienen. Auf den 400 Seiten soll ein Einstieg in die RFID-Technologie gegeben, sowie praktische Anwendungsmoeglichkiten aufgezeigt werden Das kann man durchaus als gelungen betrachten: Nach einem groben Ueberblick ueber die Erscheinungsformen von Transpondern (Form, Frequenz, Reichweite, Kopplung), wird die grundlegende Funktionsweise erklaert. Es folgt ein 70 Seiten starkes Kapitel ueber die "Physikalischen Grundlagen von RFID-Systemen". Trotz allgemein guter Verstaendlichkeit empfiehlt es sich uU, ein Physik-Kompendium griffbereit zu haben. Nur sicherheitshalber.

Ausserdem enthaelt das Buch ebenso Hinweise zu Frequenzbereichen und Funkzulassungsvorschriften, Normung, Anwendungsbeispiele und Marktuebersicht, wie allgemeine grundlegende Erlaeuterungen zu Codierung, Modulation, Datenintegritaet, Datensicherheit und Architektur elektronischer Datentraeger.

Der Behandlung von Lesegeräten sind auch nochmal 30 Seiten gewidmet. Neben dem Text wird grosszuegiger Gebrauch von Abblidungen und Grafiken gemacht. Die Auswahl ist aber grösstenteils sinnvoll; richtiggehend interessant sind die Schaltungsbeispiele.

Alles in allem ist das Buch durchaus ein guter Einstieg sowie ein brauchbares Nachschlagewerk. Die Zielgruppe sind aber eindeutig Leitende technische Angestellte, deren Chefs

H2K – hope 2000

14.- 16.7.2000, hotel pennsilvania, new york city, n.y., u.s.a

drei tage hacker aus aller welt in einem abgefahrenen gebäude in einer geilen stadt mit drei parallel stattfindenden events rund um die uhr plus party und ideenaustausch. nein, nicht der nächste chaos congress, sondern die H2K tagung in new york, veranstaltet von den machern des legendären 2600 magazins.

http://www.h2k.net

monomedia berlin:value

12.- 14.5.2000, berlin

Die erste monomedia berlin Konferenz steht im Zeichen von "value". Denn in Bezug auf die Neuen Medien stellen sich immer dringender die Fragen nach Wert und Werten. monomedia berlin formuliert hierzu die wichtigsten Fragen:

Die Frage nach einer neuen Ökonomie, die sich mit dem Internet entwickelt. Die Frage nach dem Mehrwert für User und Produzent - aufgrund der Gestaltung von Neuen Medien und ihren Anwendungen. Die Frage nach neuen Bewertungs- und Maßsystemen - angeboten von den Neuen Medien. Und nicht zuletzt die Frage nach der Veränderung unserer zentralen gesellschaftlichen Werte, die sich parallel zu der technischen Evolution vollzieht.

monomedia berlin:value ist für jeden gemacht, der verstehen will, wie unsere Werte die künftige Entwicklung der Neuen Medien bestimmen. Und wie Neue Medien zugleich unsere Werte verändern werden.

http://www.monomedia.hdk-berlin.de/

RSA conference europe

10.-13.4.2000, hilton münchen park

The RSA Conference consists of four main components: General Sessions, Expo, Tutorials and Class Tracks. The General Sessions open each day of the conference, bringing everyone together for special keynote ad-dresses, expert panels, and discussions of general in-terest. This year's Expo will feature one of Europe's largest computer security expositions demonstrating the very latest data security products. Optional Tutorials and immersion training sessions will provide the basics of crypto technology, enterprise security and network security development techniques. Finally, five simultaneous Class Tracks will feature a wide variety of workshops, seminars and talks.

http://www.rsaconference.com/rsa2000/europe/

WWW9 Konferenz

15.-19.5.2000, Amsterdam

The Ninth International World Wide Web Conference (WWW9) will be held on May 15-19, 2000 in Amsterdam, the capital of The Netherlands. Leaders from industry, academia, and government will present the latest developments in Web technology, and discuss the issues and challenges facing the Web community as it moves into the 21st Century.

http://www9.org/

Bestellungen, Mitgliedsanträge und Adressänderungen bitte senden an:

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

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

- **Satzung + Mitgliedsantrag**
  DM 5,00
- **Datenschleuder-Abonnement**, 8 Ausgaben
  Normalpreis DM 60,00 für
  Ermässigter Preis DM 30,00
  Gewerblicher Preis DM 100,00 (Wir schicken eine Rechnung)
- Alte Ausgaben der Datenschleuder auf Anfrage
- **Chaos CD blue**, alles zwischen 1982 und 1999
  DM 45,00 + DM 5,00 Portopauschale

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: _____

PLZ, Ort: _____

Tel., Fax: _____

E-Mail: _____

Ort, Datum: _____

Unterschrift: _____