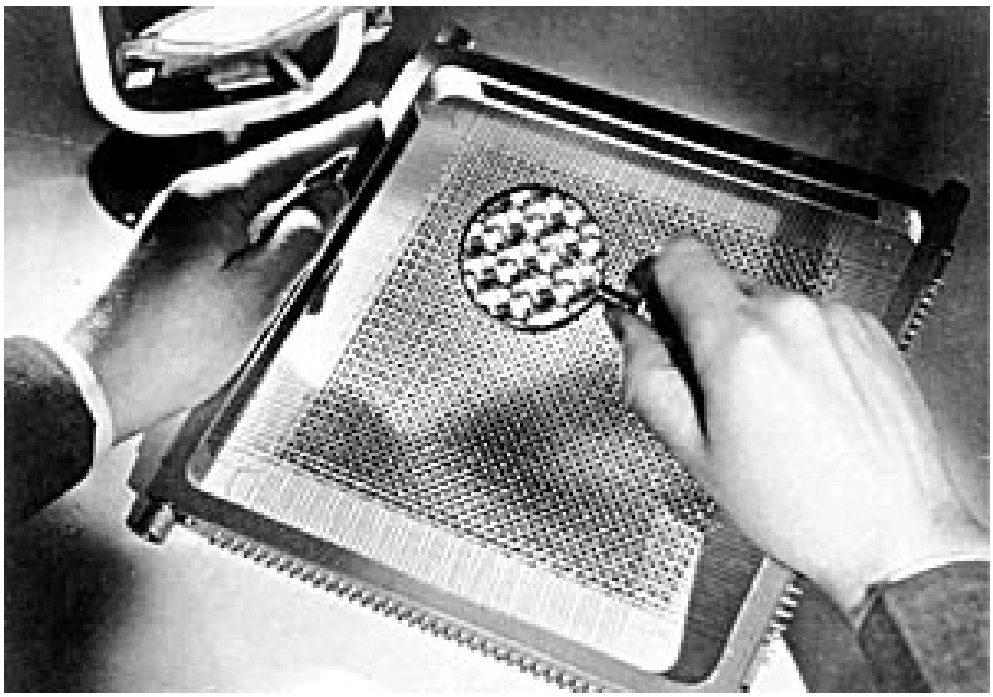
Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club



- *AES, der kommende Krypto Standard*
- *Das BKA und die „Internet Kriminalität“*
- *Chaos Communication Congress 1998 Nachlese*

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

#66

Impressum

Die Datenschleuder Nr. 66
I. Quartal, Frühjahr 1999
Herausgeber:
(Abos, Adressen etc.)
Chaos Computer Club e.V.,
Lokstedter Weg 72,
D-20251 Hamburg,
Tel. +49 (40) 401801-0,
Fax +49 (40) 401801-41,
EMail: office@ccc.de
Redaktion:
(Artikel, Leserbriefe etc.)
Redaktion Datenschleuder,
Postfach 640236, D-10048 Berlin,
Tel +49 (30) 280 974 70
Fax +49 (30) 285 986 56
EMail: ds@ccc.de
Druck: St. Pauli Druckerei Hamburg

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

Mitarbeiter dieser Ausgabe:
Andreas Bogk, Rüdiger Weiss, Cornelia Sollfrank, Alexander Eichler, Chris Vogel, Jockel von Niemann, Jens Ohlig, Migri, H. Ottstedt, D. Steinhauser, Jan Manuel Tosses, Tim Pritlove, u.a.
Eigentumsvorbehalt:
Diese Zeitschrift ist solange Eigentum des Absenders, bis sie dem Gefangenen persönlich ausgehändigt worden ist. Zur-Habe-Nahme ist keine persönliche Aushändigung im Sinne des Vorbehalts. Wird die Zeitschrift dem Gefangenen nicht ausgehändigt, so ist sie dem Absender mit dem Grund der Nichtaushändigung in Form eines rechtsmittelfähigen Bescheides zurückzusenden.

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

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

Erfa-Kreise

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

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

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

Ulm: Kontaktperson: Frank Kargl frank.kargl@rz. uni-ulm.de Electronic Mail: ccc@majordomo.uni-ulm.de Web: http://www.uni-ulm.de/ccc Treffen Jeden Montag ab 19.00h im 'Café Einstein' in der Universität Ulm.

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

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

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

/work/todo/Chaos-Jahr99

Der Congress und Jahr 1998 waren kaum vorbei, schon stehen die nächsten Aktionen an, die durchgeführt werden wollen. Der Congress 1998 im Haus am Köllnischen Park hat dank Bewahrung der Atmosphäre bei gleichzeitiger Steigerung von Teilnehmerzahlen auf über 2500 und einer professionelleren Kongressinfrastruktur viel zusammengeführt. Zum Beispiel Menschen. Und nicht zuletzt Ideen, wie man das Leben auf diesem Planeten etwas sinnvoller gestalten könnte, als in der Art und Weise, wie es von den herrschenden Zuständen derzeit demonstriert wird.

Apropos Rüstung: Derzeit rüsten wir uns für den Beginn des Chaos Communication Congress als Dauerveranstaltung vom 1.1.2000 bis ca. 31.12.2999 (Kaffee- und Kindergeburtstagspausen inklusive). Ein Jahrtausend kunterbunter Vernetzung und friedensstiftender Verständnissteigerung sollte die notwendige Evolution etwas vorantreiben.

Bevor wir dann also den Jahrtausendplan auf dem diesjährigen Chaos Communication Congress Ende Dezember verabschieden, üben wir uns im Aufbau und dem Betrieb entsprechender Infrastruktur durch das Chaos Communication Camp vom 6.-8. August 1999 in der Nähe von Berlin. Erste Details in dieser Ausgabe und unter http://www.ccc.de/camp/

Auf diese Datenschleuder habt ihr ein bißchen länger warten müssen; das hat zum einen mit der notwendigen Erholungspause nach dem Congress zu tun, zum anderen mit den noch zu verbessernden Strukturen. Im Web-Bereich des CCC und in den Mailinglisten sind wir gut vorangekommen, eine dezentralere Struktur zur Beteiligung auch unregional Ansässiger zu schaffen. Bei anderen Dingen, wie den orga-lastigen Besprechungen und der Erarbeitung von Medienerzeugnissen wie diesen auf Papier haben wir noch ein bißchen dran zu arbeiten.

Insofern haben wir dieses Jahr auch als Kulturgemeinschaft viel zu tun; Open Source Kryptoansätze werden auf einmal von Bundesministerien gefördert, Ermittlungen im Mordfall Tron von der eigentlich zuständigen Polizei und Staatsanwaltschaft dafür überhaupt nicht. Chipkarten bleiben ein spannendes Thema und Entzauberung auf breiter Ebene ist angesagt. Die nächste Datenschleuder erscheint Ende Juni und dann isses nur noch einen Monat bis zum Camp. Bis dahin hoffen wir auf eure Rege Mitarbeit auf allen Ebenen. In diesem Sinne: weitermachen.

Andy M.-M.

ds@ccc.de Leserbriefe (kleine Auswahl)

Date: Tue, 12 Jan 1999 23:18:09 +0000
From: acun@
To: ds@ccc.de

Subject: Allgemeiner Kommunikator

Ich bin ein 14 jähriger junge mit einem MAC. Ich will mit dir kontakt aufnehmen,falls du ein allgemeiner kommunikator bist.Ich wäre dir sehr verbunden wenn,du mir allgemeine kommunikation beibringst.

Du dich besser wenden an die nächste Chaos-Treff

Date: Tue, 5 Jan 1999 16:42:46 +0100
From: "bfw" <bfw@>
To: <ds@ccc.de>

Subject: Du arschloch ich brauche die chaos cd mit der hacker bibel! mail mir zu RE3@gmx.de

u. wehe du sendest mir schlaue wöter zu!

Wir werden uns hüten.

Date: Mon, 04 Jan 1999 19:57:10 +0100
From: Dino <Dino@>
To: ds@ccc.de

Subject: Chipkarten

Hi ihr,

Könnt ihr mit diesem Hex Code etwas anfangen, oder mir sagen wo ich die passende Karte dazu bekomme, meine Chipkarten sind alle zu groß. Wo wird da der Geldbetrag verschlüsselt ????

Danke im vorraus - Dino B

```
0000:A2 13 10 91 46 0B 81 15 44 45 4E 5F 49 A2
1C 00

0010:6E 61 08 4F 06 D2 76 00 00 04 00 FF FF FF FF
39

0020:36 37 32 20 20 20 20 20 30 20 20 20 20 20
30 31

0030:31 30 30 30 30 30 30 30 30 30 30 31 30 30
32 30

0040:31 31 39 39 39 32 32 35 33 33 34 31 30 32
31 30

0050:31 39 39 38 31 39 31 37 32 33 30 4D 65 6E
7A 2C

0060:20 53 74 65 66 61 6E 20 20 20 20 20 20 20
20 20

0070:20 20 20 20 20 20 20 20 20 30 31 31 30
30 30

0080:20 30 30 30 30 30 30 20 30 30 30 30 30 30
30 30

0090:30 30 30 30 37 34 39 32 20 20 20 20 20 20
30 20

00A0:20 20 20 20 20 20 20 44 20 44 FF FF FF FF FF
FF

00B0:FF FF FF 30 30 30 30 30 30 30 30 30 36 30 30
FF

00C0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

00D0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

00E0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF

00F0:FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF FF
```

Nach Klärung der Rechtslage gips ganz bald die Geldkartendoku auf ftp.ccc.de im PDF Format.

Aus der Chaos Hotline aufgeschnappt

Wau, Chaos Hotline

Caller: I have a brand new Internet Computer with toasting processor and...

w: Which color?

C: Strawberry.

w: Then I know your problem

c: ???

w: Each color has one problem. And you have an Internet Computer without the @ marked on the

Chaos Realitäts Dienst Kurzmeldungen

Telekommunikationsliberalisierung praktisch erfahren

In Las Vegas fielen am 1. März kürzlich die Telefonanschlüsse von rund 75.000 Kunden aus. Ursache waren weniger technische Probleme, als die Tatsache, daß bewaffnete Einbrecher kurzerhand die in Betrieb befindlichen Vermittlungen mitnahmen. Die Polizei hat zwar noch keine direkte Spur, ein Vertreter der Firma vermutete jedoch einen gezielten Diebstahl zum Zwecke des Wiederverkaufs an andere vermittelnde Unternehmen. (Quelle: AP 1.3.1999)

Nessus Alpha2 releast

Der mittlerweile etwas in die Jahre gekommene Sicherheitslückenscanner SATAN hat einen würdigen Nachfolger bekommen. Nessus nimmt es im Funktionsumfang mit kommerziellen Tools wie ISS auf, ist aber im Gegensatz zu diesen Open Source. Der Scanner ist in einen Server zur Datensammlung und einen Client zur Aufbereitung unterteilt, der auch auf einem anderen Rechner laufen kann. Nessus gibt's bei http://www.nessus.org.

Bauplankorrekturhinweis

Bei der Platine UniProg, DS 61, S. 01111 ist der unter dem 7812 angeordnete Kondensator nicht 220 nF, sondern eher 100 uF 25 V. Beim MAX232 ist bei den fuenf Tantalelkos die Polaritaet zu beachten; sie ist auf der Platine nicht markiert.

Quellen im Netz

... Unterhaltsames Interview mit einem ehemaligen NSA-Mitarbeiter über Ausbildungsformen, technische Strukturen und Zwischenfälle beim Betrieb des Echelon-Systems und der Strukturen drumrum
http://jya.com/nsa-40k.htm

... der Bundesbeauftragte für die Unterlagen des ehemaligen Ministeriums für Staatssicherheit der deutschen demokratischen Republik jetzt unter http://www.snafu.de/~bstu

Wissen

..."TIP-INFO" - Terminals der Deutschen Bahn: - laufen unter Windows NT - Applikation heisst tipinf.exe - sind online verbunden (PC Anywhere laeuft im Hintergrund) - und stürzen entsprechend oft ab

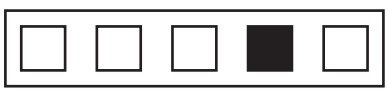
Bildungswerk Chaos Hamburg

Der CCC Hamburg eröffnet im Mai das Chaos Bildungswerk. Vorträge und Workshops zu unterschiedlichsten chaosrelevanten Themen finden in der Regel donnerstags um 19:30 Uhr in den Clubräumen in Hamburg-Eppendorf, Lokstedter Weg 72, statt, umfangreichere Workshops auch schon einmal am Wochenende.

Eine Anmeldung zu den Workshops ist derzeit nicht erforderlich, wer Zeit und Lust hat (und die eventuell nötigen Voraussetzungen erfüllt) kann kommen. Für einige Veranstaltungen geben wir Voraussetzungen an. Dies soll helfen, den technischen Level und Schwierigkeitsgrad einzuschätzen (Einsteiger in ein bestimmtes Thema oder Details? Technisch oder gesellschaftlicher Schwerpunkt?).

Termine und Themen finden sich immer aktuell unter

`http://www.hamburg.ccc.de/Workshops/`



Erfahrungen mit der zwangsweisen

Erfahrungsbericht Zwangs-https

Wie in der vorletzten DS verkündet, wurden im Herbst '98 für drei Monate alle Browser, die standardmäßig in der Lage sind, per https zu verbinden, zur Benutzung desselben auf www.ccc.de gezwungen. Einige interessante Probleme sind dabei aufgetaucht und einiges Herzleid wurde verursacht.

Zwangsmaßnahmen sind ja sonst nicht so unsere Sache, auch wenn es schon Vorschläge gab, Verstöße gegen ein RFC mit Windowsbenutzung nicht unter zwei Jahren zu bestrafen. In diesem Fall erschien es gerechtfertigt, da Aufklärung zum Thema Public Key Cryptography und SSL not tat und immer noch tut, denn auch die neue Regierung scheint am SigG festzuhalten und die nötigen Hooks im BGB sollen im Laufe dieses Jahres beschlossen werden, womit eine elektronische Unterschrift auch ohne materielles Vertragsdokument Beweiskraft erlangt.

Der zweite und nicht weniger wichtige Grund für möglichst viel verschlüsselten Traffic zu sorgen ist, um es den den Herren und Damen mit den großen Ohren möglichst schwer zu machen. Allerdings stellt sich die Frage, ob der Kampf gegen Zwang und Überwachung Zwangsmaßnahmen rechtfertigt. Nun, es hat mal jemand gesagt, daß das meiste Unrecht, im Glauben das Richtige zu tun, begangen worden ist.

Die Umleitung war als Rewrite der URL in Abhängigkeit zum Browser implementiert, d.h. jeder, der mit einem sich als »Mozilla.*« meldenden Browser ankam, wurde auf eine Seite mit Erklärungen und einem Link zum Download des CA-Certs (Certifying Authority) geleitet. Von dieser Seite waren auch noch weitere Hilfetexte angelinkt. Wer dies ausprobieren möchte, gehe zu http://www.ccc.de/~pluto/ssl/. Dort gibt es auch eine sehr übersichtliche Anleitung zum Einrichten der Umleitung. Weitere SSL-fähige Browser in die Umleitung mit einzuschließen war geplant, wurde aber nicht durchgeführt. Was es neues gibt, ist ein interner Bereich, der nur mit Vollwertkrypto und einem Client-Cert der cccCA erreichbar ist.

Aus den ca. 500-600 Mails, die ich während der Umleitung bekommen habe, war herauszulesen, daß die meisten Surfer diese Umstellung nicht als Zwangsmaßnahme empfanden, sondern eher als eine Umstellung vom Default auf eine sinnvollere Alternative. Nur etwa einer von zehn, die die Aktion bewerteten, hat sich beschwert. Selbst User, die große Probleme mit https und dem per Hand nachzuladenden Server- und/oder CA-Cert hatten, waren in der überwiegenden Mehrheit voll des Lobes und begrüßten es als positiven Beitrag zum Thema.

An technischen Problemen sind als erstes zwei Bugs im Internet Explorer zu nennen: Der erste betrifft das Abspeichern des CA-Certs, da hier als Default »Save to disk« angegeben ist und dies manuell vor dem Öffnen auf »direkt öffnen« umgestellt werden mus. Der Zweite ist schon gravierender, da der SSL / TLS-Standard reguläre Ausdrücke im Namen des Servers vorsieht (z.B. *.ccc.de, als DN), der IE aber in manchen Versionen nicht in der Lage ist, diese zu interpretieren und die Verbindung abbricht. Ein Bug des Netscape Navigators, welcher nach dem Laden des Certs manchmal die Fehlermeldung »Site not Found« bringt ist noch unklar, scheint aber in neueren Versionen nicht mehr aufzutreten.

Ein recht weit verbreitetes Problem sind Paket-Filtering-Firewalls, die den standard https Port (443) nicht durchlassen. Als prominentes Beispiel sei hier das BSI erwähnt, aber auch andere Firmen und Institutionen sind oder waren davon betroffen. Im allgemeinen hat eine Mail gereicht, um das Konfigurationsproblem zu beheben. Am ärgerlichsten war die Amerika Gedenk-

Bibliothek, wo der Zugang von den dort aufgestellten öffentlichen Terminals nicht möglich war. Ein anderes Problem sind Internetcafés, da reichte allerdings ein Satz in der Umleitungs-Seite mit dem Hinweis, daß es reicht, das Cert des Servers ohne vorherigen Download des CA-Certs zu akzeptieren.

Ob unsere Seiten auch noch in China gesehen werden konnten, ist nicht bekannt, aus Singapur gab es eine Fehlermeldung, aber mit dem Secure Proxy der städtischen Firewall konnte dann auch auf https zugegriffen werden. Durch die Umleitung wurden ca. 20-30% weniger Visits gezählt, allerdings lassen sich aus dem Vergleich der Zugriffszahlen nur Schätzungen herleiten, da hier noch zuviele weitere Faktoren mit im Spiel sind. Von allen Zugriffen benutzten nur ca. 5% einen Client mit waffenfähiger Krypto, sprich mit in voller Länge verschlüsselt übertragenen Session Keys.

Aus den Erfahrungen mit diesem ersten Versuch lassen sich 2 hoch 4 mögliche Umleitungs-szenarien herleiten, hier die als Komponenten dargestellt sind:

1. Cert einer unbekannten CA, will heißen die User brauchen erst das Cert der CA. Dafür muß man einiges erklären, das ist aber auch der Vorteil, weil https klicken, ohne was mitzubekommen, kann man auf jeder eCommerce Site.

2. Cert einer bekannten CA. Keinen Ärger mit DAU's, keine Hilfe nötig, keine Anforderungen an den Intellekt der Surfer. Aber alles streßfrei verschlüsselt.

1. Das Cert beachtet bestimmte M$ Bugs (regexp im DN), dann gibt's weniger Ärger mit Mac Usern. Sprich kleinster gemeinsamer Nenner.

2. Das Cert ist standardkonform, aber nicht IE tauglich.

I. Jede Schlüssellänge ist OK, also auch mit Exportbrowsern klickbar. Die NSA und ENFOPOL liest jedes Bit, weil nur 40 Bit des Session Keys verschlüsselt sind.

II. Nur Vollwertkrypto wird akzeptiert. Alle schreien, weil man einen Domestic Browser (oder SSL-Proxy) braucht, aber die NSA oder ENFOPOL sehen nichts. Und man beugt sich nicht den amerikanischen Exportregulierungen.

O. Alle Seiten können nur über https gesehen werden.

X. Die Startseite und die FAQ werden unverschlüsselt übertragen.

Variante 2 A I O/X benötigt keinerlei Hilfe zur Benutzung, ist aber langweilig.

Variante 1 B I O war bei uns im Einsatz (ca. 30 G https Traffic, ca. 5-600 Mails) und hat imho gut funktioniert. Variante 1 B II X ist mein Liebling, allerdings reduziert diese den Traffic wg. nicht Klarkommen der Surfer ganz erheblich. Eignet sich nur für interne Seiten oder ein Publikum mit hohem Niveau / Sicherheitsbedürfnis. Variante 2 A I O haben wir gerade diskutiert, denke mal ein gangbarer Mittelweg ist 1 A

I X. (Das ist Zufall! :)

Gruß

pluto@berlin.ccc.de

AES

Eine schwerwiegende Entscheidung wurde von US-amerikanischen Standardinstitut NIST in die Wege geleitet. Nachdem der 1976 standardisierte DES-Algorithmus in die Jahre gekommen ist, wurde mit der Kür eines Nachfolger begonnen. Das NIST spricht zwar „nur" von einer geplanten Lebensdauer von 20-30 Jahren für den Advanced Encryption Standard (AES), die Erfahrung mit Standards hat jedoch gezeigt, daß sich wahrscheinlich noch unsere Urenkel mit AES auseinandersetzen müssen.

DES ist tot

Jahrelang hatten Kryptographen gewarnt, daß der bisherige Verschlüsselungsstandard DES mit seiner 56 bit Schlüssellänge durch ein komplettes Absuchen des Schlüsselraumes zu knacken ist. Während bisher lediglich auf der akademischen Ebene Bauanleitungen für Descracker existierten und jeder ernstzunehmende Sicherheitsberater auf die hohe Wahrscheinlichkeit hinwies, daß sowohl Geheimdienste, als auch gut organisierte Konzerne und Verbrecherorganisationen solche Baupläne umsetzten könnten, war am 17. Juli die Stunde der „good guys" gekommen.

Während das unter anderem auf dem HIP Festival vorgestellte CCC Projekt eines DES Crackers leider in der Diskussionsphase stecken blieb, bauten die amerikanische Kollegen von der „Electronic Frontier Foundation (EFF)" für 250.000 $ eine „Höllenmaschine" (Amtsgericht Hannover), welche innerhalb von 56 Stunden DES endgültig entzauberte. Unter http://www.eff.org/descracker/ können ambitioniert Bastler auch gleich eine Bauanleitung bestellen oder direkt über http://www.replay.com/ eine von den Autoren ausdrücklich begrüßte gescannte Version downladen.

Besonders dramatisch an der Geschichte ist die kryptoanalytische Einfachheit des Angriffes, da dieser nur die Bekanntheit des verschlüssleten Textes voraussetzt (known-ciphertext Angriff). Der Angreifer hört den Geheimtext ab und probiert einfach alle Schlüssel durch. Falls ein falscher Schlüssel gewählt wurde entsteht beim Entschlüsseln ein wunderschön zufälliges Rauschen. Sollte das Ergebnis sich von einer Zufallsausgabe unterscheiden ist mit hoher Wahrscheinlichkeit der richtige Schlüssel gefunden.

Advanced Encryption Standard

Aus diesen Gründen schrieb das US-amerikanische „National Institute of Standards and Technologie" am 12. September 1997 einen Wettbewerb für den Advanced Encryption Standard (AES) aus. Im Gegensatz zum DES Verfahren sollten diesmal die Designgrundsätzte veröffentlicht und von der Kryptogemeinde öffentlich analysiert werden können. Zudem wurden die Entwickler verpflichtet nachzuweisen, daß keinen geheimen Hintertüren vorhanden sind.

Weitere Grundanforderungen waren:

* Blockgröße von 128 bit

* Schlüssellänge 128, 192 und 256 bit

* Mindestens so schnell und so sicher wie Triple-DES

Die Wahl der Blockgröße war wohl eine der schwerwiegensten Entscheidungen. Für Produkte, welche die von DES als verwendete Blockgröße von 64 bit nutzen, bedeutet dies ein unter Umständen erheblicher Umstellungsbedarf. Allerdings ist eine Blockgröße von 64bit angesichts der heutigen Rechnerleistung nicht mehr zeitgemäß (matching ciphertext Angriffe).

Weswegen als Schlüssellängen neben 128 bit auch 192 und 256 bit vorgesehen sind, führte selbst auf

wissenschaftlichen Konferenzen zu nicht immer ernsthaften Diskussionen. Jedenfalls sollte eine 256 bit Schlüssellänge auch den Quantencomputer der von der US Regierung gefangengehaltenen Aliens, welche möglicherweise die Komplexität eines Angriffs auf die Quadratwurzel der „herkömmlichen“ Komplexität reduzieren können, widerstehen!-)

Vom 20.-22. August 1998 fand im kalifornischen Ventura die erste AES Konferenz statt. Im folgenden stellen wir kurz die 15 Kandidaten, welche die Vorauswahl zur ersten AES-Konferenz überstanden haben vor.

Wohl ausgeschiedene Kandiaten

DEAL basiert auf einer Idee von Lars Knudsen und wurde von Richard Outerbridge als AES-Kandidat eingereicht. DEAL verwendet DES als Rundenfunktion in einem 6 rundigen Feistelnetzwerk für Schlüssellängen von 128 und 192 Bit beziehundgsweise 8 Runden für 256 Bit Schlüssel.

Überraschenderweise unterlief Lars Knudsen, der als einer der führenden Experten für Keyscheduling-Verfahren, mit deren Hilfe aus dem Hauptschlüssel die einzelnen Rundenschlüssel berechnet werden, gilt, gerade hier ein schwerwiegender Fehler. Stefan Luck, der dieses Jahr schon den bisher stärksten Angriff gegen Triple-DES gefunden hatte, veröffentlichte einen Angriff welcher nur 270 gewählte Klartexte benötigt. Outerbridge hat Lucks den ausgesetzten Geldpreis für die beste Analyse bereits zugesand.

Der DFC Kandidat der französischen Centre National pour la Recherche Scientifique Ecole Normale Superieure besitzt eine 8 ründige Feistelstruktur und basiert auf der sogenannten Decorrelation Technik von Serge Vaudenay. DFC ist beweisbar sicher gegen Differentielle und Lineare Kryptanalyse. Allerdings verwendet er eine sehr aufwendige 32bit Multiplikation, was seinen Einsatz auf Smartcard-Systemen erheblich erschwert. Zudem fand Dan Coppersmith zahlreiche schwache Schlüssel.

Frog wurde vom „führenden Kryptografen Cost-Ricas“ für die TecApro Internacional S.A. vorgestellt. Er verwendet 8 Feistelrunden und ein sehr aufwendiges Keysetup. Wagner, Ferguson, und Schneier veröffentlichten eine erfolgreiche Kryptoanalyse (Differential: 258 chosen plaintexts. Linear: 256 known plaintexts).

Der 8 rundige Happy Pudding Cipher (HPC) von Richard Schroeppel dürfte trotz des schönen Namens doch nur Aussenseiterchancen besitzten.

LOKI 97 ist der Kandidat von Lawrie Brown, Josef Pieprzyk und Jennifer Seberry. Loki benutzt 16 Feistelrunden und ist der Nachfolger von Loki, Loki 91. Loki wurde von Lars Knudsen gebrochen und darauf hin in Loki89 umbenannt. Auch das verbesserte Loki 91 hielt einer Analyse von Lars Knudsen nicht stand. Drei mal dürft Ihr raten welches Schicksal Loki97 ereilte.

Richtig, diesmal dauerte es nur wenige Tage bis Knudsen und Rijmen ihre Analyse mit den Worten:“Loki97 is broken“ schliessen konnten.(Die Differentielle Kryptanalyse benötigte 256 chosen plaintexts und die Linear Kryptanalyse 256 known plaintexts.)

Telekom sorgt für Heiterkeit

Gründlich blamierte sich die Deutsche Telekom AG. Ihr 6 beziehungsweise 8 ründige Feistelnetzwerk MAGENTA läßt kaum einen Anfängerfehler aus. Biham, Biryukov, Ferguson, Knudsen, Schneier und Shamir

AES - Der Kryptoalgorithmus für die

cryptoanalysiserten Magenta online während der Vorstellung (264 chosen plaintexts, 264 Steps oder 233 known plaintexts, 297 Steps). Was allerdings ein wenig ein Flächenbombardement auf ein Spatzennest erinnert. Schließlich war der Angriff gegen den unglaublich schlechten Keyschedule eine einfache Übertragung des uralten Merkle/Hellmann Angriffes auf 2-Key Triple-DES und diente daher schon als Aufgabe in einer Anfängervorlesung für Kryptographie. (http://th.informatik.uni-mannheim.de/m/lucks/vorl.html, Übungsblatt 6).

Die einzelnen Schwächen (Säckeweise Schwache Schlüssel,...) aufzulisten würde den Rahmen dieses Artikels sprengen. Erst nach mehrstündigen Analyse gelang es mir überhaupt einen kryptographisch starken Baustein im Algorithmus zu finden. Als Krönung dürfte Magenta allerdings zumindest den Preis als langsamster Kandidat erhalten. Die ganze Aktion kommt einem fast so vor, als ob Andy Möller auf einmal versuchen würde, um den Schwergewichtstitel zu boxen.

Kandidaten mit guten Chancen für die zweite Runde

CAST 256 ist die Weiterentwicklung des bekannten CAST5 Algorithmus von Carlisle Adams und Stafford Tavares. CAST5 wurde von Entrust Technologies zur kostenlosen Verwendung freigegeben und befindet sich daher in den Programmen PGP ab Version 5.0 und PGP-Disk. CAST256 verwendet ein modifiziertes Feistelnetzwerk mit 48 Runden (12 Zyklen).

Crypton ist ein 12 rundiges SP-Netzwerk der koreanischen Firma Future Systems, Inc und wurde von Chae Hoon Lim vorgestellt. Die Struktur ist von SQUARE Algorithmus beeinflusst und verwendet 8x8 S-Boxen, welche gute Widerstandseigenschaften gegen differentielle und lineare Kryptoanalyse besitzten. Das Keyscheduling soll allerdings noch modifiziert werden. Der Autor Hoon Lim publiziert seit Jahren auf den besten Krypto-Konferenzen, allerdings überwiegend im Bereiche von Digitalen Signaturverfahren.

E2 ist ein 12 Runden Feistelnetzwerk von NTT – Nippon Telegraph and Telephone Corporation. E2 verwendet 8x8 S-Boxen, welche gegen die verschiedenen bekannten Angriffsmethoden gehärtet und nach einer veröffentlichten Strategie ausgewählt wurden. Bruce Schneier zählt E2 zu den vier Favoriten.

RC6 ist der von Ron Rivest in Zusammenarbeit mir Robshaw, Sidney und Yin für die RSA Laboratories entwickelte Nachfolger von RC5. RC6 ist ein modifiziertes Feistelnetzwerk mit 20 Runden (10 Cycles). Die Geschwindigkeit von RC6 hängt ganz wesentlich davon ab ob der jeweilige Processor variable Rotationen schnell durchführen kann. An der Verwendung von datenabhängigen Rotationen entzündete sich allerdings Kritik. Zum einen ist die Patentlage unklar, zum anderen sind die kryptografischen Eigenschaften von derartigen Rotationen noch nicht gründlich genug analysiert.

RIJNDAEL ist der Kandidat von Joan Daemen und Vincent Rijmen. Er ist faktisch die 128bit Version des bekannten Square Algorithmus. Rijndael ist ein SP-Netzwerk mit 10 , 12 bzw 16 Runden. Rijndael gehört zu den schnellsten Algorithmen im Feld.

Safer+ ist wie der Namen schon sagt eine Weiterentwicklung von Safer für die Cylink Corporation. Neben dem Safer-Erfinder Massey werden auch Khachtrian und Kuregian als Co-Autoren genannt. Safer+ ist ein SP-Netzwerk mit 8 , 12 bzw 16 Runden.

nächsten Jahrzente ?!

Die Favoriten

MARS ist der offizielle IBM Kandidat. Unter den Autoren ist mit Don Coppersmith auch einer der DES Väter. MARS ist ein modifiziertes Feistelnetzwerk mit 32 Runden (16 Cycles). Es verwendet Multiplikationen und datenabhängige Rotationen. Die Konstruktionsgrundsätzte für die verwendeten S-Boxen sind mit veröffentlicht, so daß die bei DES geäußerte Sorge über geheime Hintertüren stark reduziert werden dürfte. Viele Experten sehen MARS als Favoriten. Allerdings wurden Saarien äquivalente Schlüssel entdeckt, eine kryptographisch unschöne Eigenschaft und zudem erscheint die Verwendung von Multiplikationen besonders für Smartcards als sehr aufwendig. Weiterhin ist die Verwendung von Datenabhängigen Rotationen, wie schon bei RC6 diskutiert, nicht unumstritten.

Ross Anderson, Eli Biham und Lars Knudsen schicken SEPENT ins Rennen. Die Autoren zählen zu den weltbesten Kryptoanalytikern. Alle drei haben wohl bereits zahlreiche Algorithmen geknackt und eine Reihe von kryptoanalytischen Angriffsmethoden, unter anderem Bihams Differentielle Kryptoanalyse, gefunden.

Serpent ist ein SP-Netzwerk mit 32 Runden. Schon nach 16 Runden ist der Algorithmus sicher gegen alle bekannten Angriffe. Der Algorithmus nutzt zur Verbesserung der Performance die von Eli Biham entwickelte Bitslicing Technik Durch die Verwendung von 4x4 S-Boxen ist der Entwurf ausgesprochen hardwarefreundlich.

TWOFISH ist der Blowfish-Nachfolger von Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall und Niels Ferguson. Er verwendert Feistel 16 Runden und „borgt“ eine Reihe von lange Zeit getesteten und anerkannten Bauelementen. Es kommen unter anderem Withening (DESX), Schlüsselabhängige S-Boxen (CS, Blowfish) , MDS-Matrizen (Square), Pseudo Hadamard Transformationen (Safer) und feste Rotationen zum Einsatz. Das Keyscheduling verwendet die selben Konstruktionsverfahren, wie die Rundenfunktion (Blowfish). Durch die Verwendung von relativ kleinen 8x8-S-Boxen ist der Entwurf sehr smartcardfreundlich. Twofish ist sehr schnell und flexibel an die verwendeten Resourcen anpassbar. Das Design ist ausführlich dokumentiert und bietet Sicherheit gegen alle bekannten Angriffe.

Die Beschreibung des Algorithmus ist sehr schön zu lesen und vermittelt einen guten Einblick in die aktuellen Entwicklungen bei der Konstruktion von Blockchiffrierern. Twofish ist bereits in einigen Programmen optional integriert z.B. GPG (www.gnupg.org)

\begin {schleichwerbung}

und im pretty Open PGP kompatiblen Whiteboardsystem der Univesität Mannheim (http://www.informatik.uni-mannheim.de/~rweis/research/)

\end {Schleichwerbung}.

Fahrplan

Die öffentliche Evaluierung der verbliebenen 15 Kandidaten erfolgt bis zum 15. April 1999.

Die zweite AES-Konferenz in Rom 22.-23. März 1999. Dort werden ungefähr fünf Finalisten bestimmt. Nach einer sechs bis neunmoantigen Analyse wird aus den verbleibenden Kandidaten ein Sieger bestimmt.

Tip und Ausblick

Es ist ein unglaublich spannender Wettkampf entbrannt. Favoriten zu nennen ist relativ schwierig. Beginnen wir mit dem einfachen Teil und tippen welche Algorithmen ausscheiden. Zunächst

AES - Sicher, bis daß die DPA uns scheidet

werden wohl die Algorithmen mit offensichtlichen Schwächen ausgesondert, also Magenta, Loki97, DEAL, FROG und wahrscheinlich auch DFC. Von den verbleibenden tippe ich noch auf HPC und Crypton als Ausscheidekandidat. Topfavoriten auf Grund ihrer Autoren sind wohl Mars, Serpent und Twofish.

Für Mars sprechen trotz zahlreicher Kritikpunkte insbesondere die 3 Buchstaben IBM. Allerdings erinnert die Konstruktion eher an einen Gemischtwarenladen, als an einen sauber konstruierten Cipher.

Serpent ist so langweilig konstruiert, dass er einen hohen Sicherheitsgrad bieten muss. Pi modulo Daumen entsprechen die 32 Runden, welche jeweils den ganzen Block bearbeiten, 64 Feistelrunden. DES hat deren 16. „Nicht mal Gott wird Serpent brechen können“ meinte einer weltweit führender Cryptoanalyiker. (Für Nicht-Atheisten führt diese Aussage sicherlich zu lustigen Logikspielen).

Mein persönlicher Favorit ist jedoch Twofish.

Twofish ist schnell und baut auf gut getesteten Basisbausteinen auf. Schlüsselabhängige S-Boxen sorgen gegen hohe Resitenz auch gegen bisher unbekannte Angriffsformen.

Twofish . Twofish ist frei und kostenlos einsetzbar. Und least not last gehören die Autoren definitiv zu den „good guys“, so dass auch deshalb nicht mit Hintertüren zu rechnen ist.

Alles wird gut!

Schon jetzt kann man erfreut feststellen: Der Siegesalgorithmus wird eine weltweit einsetzbare und für lange Zeit sichere symmetrische Verschlüsslung gewähren.

ruediger.weis@pi4.informatik.uni-mannheim.de

URLS:

NIST AES-Seite:
http://csrc.nist.gov/encryption/aes/aes_home.htm

The Block Cipher Lounge - AES:
http://www.ii.uib.no/~larsr/aes.html

Candidate A E S for Analysis and Reviews:
http://www.dice.ucl.ac.be/crypto/CAESAR/caesar.html

(Anmerkung der Redaktion: Mittlerweile gibt es bereits die AES2-Review im Netz. Seitenweise, irgendwo. Bitte selber suchen, URL gerade nicht zur Hand. Irgendwo auf jya.)

NMAP Kurzreview

Als dieser Artikel geschrieben wurde, war nmap 2.00 gerade erschienen. Beim Druck dieser Ausgabe könnte die Version 2.12 schon wieder veraltet sein.

nmap ist in erster Linie ein Portscanner. Ein Portscanner ist ein Programm, das dazu dient, herauszufinden, welche TCP- oder UDP-Ports auf einem Rechner offen sind, was wiederum ein Hinweis darauf ist, welche Dienste von diesem Rechner angeboten werden, also z.B. HTTP auf Port 80, SMTP für Mailtransfer auf Port 25, ssh auf Port 22, und so weiter. Der klassische Weg ist, einfach für jeden Port zu versuchen, eine Verbindung aufzumachen.

strobe von Julian Assange ist der Klassiker, der diese Methode verwendet. Leider ist ein solcher Scan relativ leicht zu entdecken. Eine Möglichkeit, die Entdeckung zu erschweren, ist es, den für den Aufbau einer TCP-Verbindung notwendigen Drei-Wege-Handshake[0] nach dem zweiten Schritt abzubrechen, so daß man zwar weiß, daß der andere Rechner prinzipiell eine Verbindung auf diesem Port entgegennimmt, diese aber nicht zustande kommen läßt. Dieses Verfahren ist als Stealth-Scan bekannt.

Beide Verfahren werden von nmap implementiert. Zusätzlich gibt es noch weitere Scanmethoden, die anhand der Antwort auf ungültige Pakete auf das Vorhandensein eines offenen Ports schließen, die allerdings nur bei RFC-konformen Systemen, also nicht bei Windows oder IRIX, funktionieren. Auch ein UDP-Scanner ist vorhanden, ebenso ein Mode, der lediglich ein ping absetzt, um die Erreichbarkeit des Hosts zu überprüfen, oder ein Subnetz nach Rechnern zu durchsuchen.

Als zusätzliche Leckerbissen hat der Autor einen fragment-Mode eingebaut, mit dem sich manche schlecht konfigurierte Firewalls durchtunneln lassen - das TCP-Paket wird mitten im Header aufgetrennt, und die Firewall lässt es deshalb passieren. Auch gibt es einen OS-Detection-Mode, der nach der von queso bekannten Methode anhand von im Standard nicht definierten Ausnahmefällen das Betriebssystem erkennt.

Und um das Scannen noch einfacher zu machen, ist es möglich, eine Liste von Adressen aus einem File zu lesen, oder ein ganzes Subnet mittels Angabe der CIDR-Adresse zu scannen. Einige Beispiele:

Ein klassischer Scan eines einzelnen Rechners:

```
$ nmap www.ccc.de
```

Dasselbe, aber mittels Stealth-Scan:

```
$ nmap -sS www.ccc.de
```

Durchsuche ein Subnetz nach Rechnern, und ermittle das Betriebssystem:

```
$ nmap -sP -O 23.23.23.0/24
```

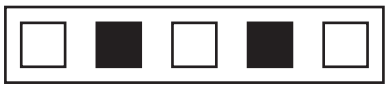
Finde alle Rechner, die bei Snafu Berlin eingewählt sind, und die Back Orifice auf dem Standardport installiert haben:

```
$ host -l berlin.snafu.de|cut '-d ' -f 4|
sudo nmap -sU -v -p31337 -i -
```

Die nmap-Homepage ist unter http://www.insecure.org/nmap zu finden. nmap ist derzeit sicherlich das vollständigste Scanning-Tool, aber dadurch auch etwas schwieriger zu handhaben als zum Beispiel strobe.

[0] Stevens, TCP/IP Illustrated, Addison-Wesley

andreas@ccc.de



Zaubern im Netz –

(Anmerkungen zu einem Tag auf der „next Cyberfeminist International", Rotterdam, März 1999)

Gibt es weibliche Hacker? Falls nicht, ist dieses Phänomen wert, es mal genauer zu betrachten. Falls ja: Wo stecken sie? Wieso kennt sie niemand? Und was treiben sie da so im Geheimen?

Hintergrund für die Fragen war mein Interesse, für die Konferenz „next Cyberfeminist International", einen Tag zu diesem Thema zu organisieren. Ganz allgemein ist es so, daß im Cyberfeminismus die Cultural Workers, also Künstlerinnen und Theoretikerinnen überwiegen, und die machen sich in der Regel die Finger nicht schmutzig mit „hands-on technology". Aber es genügt nicht, in diesem Bereich über gesellschaftliche Umwälzungen und Theorien zu sprechen. Auch ein wirkliches Interesse an der Technik selbst gehört dazu, ein kritischer, neugieriger Umgang damit, um neue Möglichkeit von Aktivismus und Einflußnahme zu erproben. Deshalb ist eine intensivere Zusammenarbeit mit Technikerinnen/ Informatikerinnen/ Hackerinnen unerläßlich, um unseren Horizont und unsere Handlungsspielräume zu erweitern und zum anderen um zu zeigen, daß es solche Frauen tatsächlich gibt und damit einzelne Frauen zu ermuntern, sich selbst aktiver, mutiger und engagierter die Finger schmutzig zu machen.

Die Feststellung, daß Technikbereiche traditionell Männerdomäne sind, ist nicht neu. Auch daß die sog. „neuen Technologien", die in den 80er und 90er Jahren entstanden sind, also in einer Zeit, in der die Frauen in viele Bereiche der Gesellschaft vorgedrungen sind, nicht wesentlich etwas daran geändert haben, ist auch bekannt. (Während der Cebit z.B., der weltgrößten Computermesse, besteht im Vergleich zu anderen Messen ein derart erhöhter Bedarf an Prostituierten, daß diese flugzeugweise aus dem Ausland eingeflogen werden müssen.) Aber daß es in diesem Technikbereich eine Enklave gibt, in der sich so gut wie gar keine Frauen tummeln, ist doch erstaunlich. Die Rede ist von den Hackern.

Gemeint ist nicht ein erweiterter Hacking-Begriff wie er in den letzten Jahren in Mode gekommen ist. Es geht nicht um Enthusiasten oder Experten für was auch immer, nicht um Personen, die Spaß daran haben, intellektuelle Herausforderungen kreativ zu meistern, Beschränkungen zu umgehen oder abstrakte Systeme zu knacken. Gemeint sind Computer-Freaks. Diejenigen, die hinter die Monitoroberfläche gehen, die Computersysteme ausspionieren, die leidenschaftlich programmieren, die basteln und denen es wichtiger ist herauszufinden, wie es etwas funktioniert als zielgerichtet damit zu arbeiten.

Besucht man Hackertreffen, liest die einschlägige Literatur oder begibt man sich in Newsgroups oder auf Mailinglisten dieses Genres wird man leider nicht vom Gegenteil seines Vorurteils überzeugt, daß da so gut wie keine Frauen sind. Das soll nicht gewertet werden. Egal, ob das gut oder schlecht ist, egal ob man das ändern will oder nicht, es ist ein interessantes Phänomen.

Für die Vorbereitung der Konferenz habe ich mich auf die Suche nach Hackerinnen begeben, bzw. postuliert, daß es keine gibt, um mich vom Gegenteil zu überzeugen lassen. Meine Recherchen haben nicht nur ein paar Hackerinnen zu Tage gebracht, sondern auch einige kuriose Begründungen dafür, warum es keine gibt. So schrieb z.B. Bruce Sterling, bekannter amerikanischer Science-Fiction-Autor und Kenner der amerikanischen Hacker-Szene: „ Es stimmt wirklich, daß es keine Hackerinnen gibt, aber das wundert mich nicht. Hacking ist typisch für männliche Jugendliche, die voll auf einen voyeuristischen Power-Trip abfahren. Man findet nicht mehr Frauen, die in Computer einbrechen, als Frauen, die besessen davon sind einen verstohlenen Blick auf Männerunterwäsche zu

werfen... Es ist sicher nicht so, daß Frauen zum Hacken physisch oder intellektuell nicht in der Lage wären, es ist nur so, daß sie überhaupt keinen Grund haben, das zu tun...Ich persönlich kenne zumindest keine einzige Frau, die das tut. Und ich habe auch nicht einmal von einer gehört, die es gemacht hätte, ohne daß ihr Freund daneben gestanden hätte und sie immer wieder ungeduldig gedrängt hätte."

Eine weitere Begründung wurde mir von Gail Thackeray geliefert, einer bekannten amerikanischen Hacker-Jägerin, die in der Abteilung für Technology Crimes beim Arizona Attorney General's Office arbeitet. Sie hat mir direkt auf ein Posting auf der dc-Liste geantwortet: „Nein, es gibt keine ernsthaften, technichen Hackerinnen. Hacking ist immer noch eine weitgehend weiße, männliche Angelegenheit, zumindest hier in den USA. Ich kenne nur einen schwarzen Hacker in Arizona (der sich inzwischen zur Ruhe gesetzt hat) und einen in New York...Es gibt(gab) viele weibliche Phone Phreaks, obwohl auch deren Interessen mehr in den sozialen Aspekten lagen als in den technischen."

Die wenigen Exemplare der Spezies „Hackerin" die ich gefunden habe, konnte ich auch glücklicherweise dafür gewinnen, zur Konferenz beizutragen. Barbara Thoens vom CCC Hamburg gab einen Überblick über die Entwicklung von Free Software und der dahinterstehenden Philosophie, Rena Tangens von FoeBud Bielefeld gab Hinweise dazu „Wie man eine Hackerin wird", Stephanie Wehner von xs4all aus Amsterdam erörtete das Problem von „Privacy on the Net" und gab Tips zur Verschlüsselung, zum anonymen Publizieren und Versenden von e-mails, und Corrine Petrus und Marieke van Santen von Tech-women Rotterdam gaben Praxis-Tips und eine Demonstration zu Hacking, Cracking, Spoofing, Sniffing und Nuking.

Entgegen anders lautender Meinungen kann man als Ergebnis des Tages „Women Hacker" zusammenfassen, daß Frauen durchaus Motive haben können, um zu hacken. Berichte über die Konferenz gibt es bei www.obn.org. Eine ausführliche Dokumentation mit allen Beiträgen wird im Juni erscheinen (zu bestellen ebenfalls über www.obn.org/reader).

Cornelia Sollfrank

Subject: habe gehackt - was nun?

From: Igor X. <@>, Date: 1999/02/21,
Newsgroups: de.org.ccc

Hallo habe meinen ersten hack hintermir
(www.hamfair.com -> Frontpage
Web -> ist jetzt weg...)
können die meine IP herausfinden??? Wenn ja, was hat das für Folgen???

Subject: Re: habe gehackt - was nun?

From: Sabine Y. <@>, Date: 1999/02/21,
Newsgroups: de.org.ccc

Igor X. wrote:
> Hallo habe meinen ersten hack hinter mir
> (www.hamfair.com -> Frontpage
> Web -> ist jetzt weg...)

Du bist ein Held. Wir bewundern Dich.
Willst Du mich ficken?

> können die meine IP herausfinden???

Wenn der Admin einigermassen Hirn unter der Matte hat, ja.

> Wenn ja, was hat das für Folgen???

Steht im StGB. S.

Bekämpfung der Kriminalität

Tagung beim Bundeskriminalamt (BKA) vom 14.-15.12.1998

Tagungsbericht mit Anmerkungen

Das Bundeskriminalamt hat ca 170 Internetprovider und Onlinedienste (ca 50 Anwesend) aus Deutschland sowie Vertreter der Strafverfolgungsbehörden und des Jugendschutzes zu einer Tagung unter dem Titel „Bekämpfung der Kriminalität im Internet“ eingeladen. Ziel dieser Tagung sollte der Beginn eines Dialogs zwischen den ISP's und den Behörden sein, dessen Zweck eine gegenseitige Aufklärung über das technisch und rechtlich mögliche und die Abstimmung von Vorgehensweisen (Stichworte: Selbstverpflichtungserklärung, Code of Conduct) sein soll.

Hintergrund der Tagung ist, daß seit Herbst 1998 das BKA auch für Kriminalität die mit Hilfe von Onlinediensten und / oder Internet begangen wird zuständig ist und eine eigene Abteilung dafür eingerichtet hat (Bundeskriminalamt, OA 34 - 2 „IuK - Kriminalität“, Tel.: 0611/55 -5716, Fax.: 0611/551-5725).

Zusammenfassender Überblick

Der Schwerpunkt der Tagung behandelte Fragen, die sich bei Ermittlungen im Bereich der Kinderpornographie ergaben, andere Delikte und Probleme, die sich bei deren Ermittlung ergeben, sind nur wenig zu Sprache gekommen. Ein Dialog hat stattgefunden und soll in einer Arbeitsgruppe fortgeführt werden. Von Seiten der ISP's wurde angeregt, in dieser Arbeitsgruppe an einem Beispielsfall die Vorgehensweisen durchzuspielen und die auftretende Probleme einer Lösung zuzuführen.

Unklar ist geblieben, wie sich die Arbeitsgruppe zusammensetzen soll. Der Vorsitzende des ECO. e.V. hat in vielen Einzelheiten die Interessen der Provider vertreten, kann aber nicht als Sprecher aller ISP's auftreten, weil bei weitem nicht alle ISP's im ECO e.V. Mitglied sind und gerade größeren ISP's dort nicht vertreten sind. Kritisch anzumerken ist auch, daß kein Vertreter des DE-NIC teilgenommen (geladen?) hat, der einzigen Organisation in Deutschland, in der wirklich alle ISP's Mitglied sind. Gänzlich unberücksichtigt sind die Betreiber von Intranets, d.h. die Industrie, geblieben. Ob Teilnehmer des DFN e.V. und des ZKI e.V. anwesend waren, war nicht ersichtlich.

Vorzuschlagen wäre daher, daß die Arbeitsgruppe von Seiten der ISP's zumindestens aus einem oder mehreren Vertretern der großen ISP's, einem Vertreter von DE-NIC und Vertretern von kleinen ISP's besteht. Hinzukommen sollten Vertreter aus Industrie und Forschung.

Eine „Selbstverpflichtungserklärung“ wurde von den ISP's nicht unterschrieben. Eine inhaltliche Diskussion des Textvorschlags des BKA fand nicht statt.

Statistisches zu dem Anteil der Kriminalität im Internet

Die von Seiten der Ermittlungsbehörden getroffenen Aussagen zu der Frage, wieviel Kommunikation im Internet mit kriminellen Inhalten oder zu kriminellen Zwecken stattfindet gingen weit auseinander. Die Schätzungen reichten von 40.000 - 80.000 kinderpornographischen Bildern über 1% der Gesamtkommunikation zu 1/60 aller Angebote und news Artikel (letztere beiden Zahlen auf alle Delikte bezogen). Eine Dokumentation der hannoveraner Stelle des Kinderschutzbundes wurde kurz erwähnt, die auf noch erheblich höhere Zahlen kommt (10 - 15 kinderpornographische Kanäle im IRC mit mindestens 300 Tauschvorgängen am Tag),

ausdrücklich von einem der Autoren aber als 'Dokumentation' und nicht als 'Studie' verstanden sein wollte, da die Anforderungen an einer Studie nicht erfüllt seien. Die in einem Vortrag von Seiten des BKA genannten Zahlen wurden sogleich als nicht sehr aussagekräftiges statistisches Material eingestuft (der Grund liegt in dem sehr unterschiedlichem Meldeverhalten der einzelnen Polizeidienststellen). Es wurde daher von einem Sprecher des BKA die Feststellung getroffen, daß man wohl derzeit keine sicheren Zahlen habe.

Anerkannt wurde von allen Seiten, daß die Mehrzahl der kursierenden kinderpornographischen Abbildungen alt, d.h. aus den '60iger, '70iger Jahren sei und für diese das Internet nur eine weitere Verbreitungsform darstelle, denn all diese Abbildungen seien auch durch Printmedien etc. schon vorher bekannt gewesen. Durch elektronische Bildmontagen kommt das eine oder andere neue Bild hinzu. Die wirklich neuen Abbildungen stellten jedoch nur einen sehr kleinen Teil der kursierenden Bilder dar.

Rechtsgrundlagen für Auskunftsersuchen

Teilweise sehr umstritten war die Diskussion über die Rechtsgrundlagen für Auskunftsersuchen der Ermittlungsbehörden. Es geht um die Frage, wann und in welchem Umfang die Strafverfolgungsbehörden von den ISP's Daten oder Auskünfte verlangen dürfen. Es bildeten sich zwei Schwerpunkte heraus: Zum einen die Frage, auf welcher Rechtsgrundlage überhaupt Daten erhoben werden können und zum anderen, inwieweit eine Datenerhebung im Widerspruch zu verschiedenen Datenschutzgesetzen steht.

Für die Datenerhebung durch die Strafverfolgungsbehörden wurden folgende Vorschriften genannt:

`Inhaltsdaten §§ 100a, 100b StPO`

`Verbindungsdaten § 12 FAG, § 6 III TDDSG § 7 TDSV, §§ 100a, 100b StPO`

`Bestandsdaten §§ 89 VI, 90 TKG, §§ 100a, 100b StPO`

Bezüglich § 7 TDSV wurde stark bezweifelt ob dieser für eine Datenerhebung herangezogen werden könne, denn diese Vorschrift sei auf technische Störungen und Mißbrauch begrenzt.

Ob diesen Bedenken zuzustimmen ist, entscheidet sich u.a. anhand der Frage, ob eine Herausgabe der Daten an die Strafverfolgungsbehörden vorgesehen ist. Dies ist im Verordnungstext nicht der Fall. Hier könnte versucht werden zu argumentie-ren, daß eine Datenerhebung (§ 7 TDSV) und Datenübermittlung (§ 8 TDSV) für private Zwecke vorgesehen ist und im Wege eines ein Erst Recht Schlusses dann eine Datenübermittlung für staatliche Zwecke umfaßt sein muß. Eine solche Argumentation verkennt jedoch, daß eine Datenübermittlung an die Strafverfolgungsbehörden einer ausdrücklichen gesetzliche Grundlage bedürfen, die hier nicht gegeben ist.

Selbst wenn diese Hürde genommen würde, bliebe zu prüfen, ob eine „sonstige rechtswidrige Inanspruchnahme der öffentlichen Telekommunikationsnetze und ihrer Einrichtungen sowie der Telekommunikationsdienstleistungen" gemäß § 7 Abs. 1 Nr. 2 TDSV dann vorliegt, wenn ein Beschuldigter Mitteilungen mit Hilfe von Telekommunikationsendeinrichtungen vornimmt. Nach der teleologischen Auslegung der Vorschrift, ist mit 'rechtswidrig' in diesem Zusammenhang insbesondere solche Vorgänge gemeint, die rechtswidrig gegenüber dem Anbieter von Telekommunikationsdienstleistungen sind (insbesondere Leistungserschleichung). Rechtswidrig gegenüber der Allgemeinheit ist daher von der Vorschrift nicht erfaßt. Den geäußerten Bedenken ist daher zuzustimmen.

Tagungsbericht BKA-Tagung

Soweit § 12 FAG anwendbar ist, ist eine richterliche Anordnung erforderlich, bei Gefahr im Verzug kann auch eine Anordnung der Staatsanwaltschaft ausreichend sein. Gemäß § 28 FAG in der Fassung des Telekommunikationsbegleitgesetzes tritt § 12 FAG am 31.12.1999 außer Kraft. Aus dem Auditorium wurde geäußert, daß eine Nachfolgeregelung derzeit noch nicht einmal im Vorentwurf vorhanden sei. Beabsichtigt sei allerdings diese Regelung in die StPO einzustellen und an den Vorschlag des § 99a StPO anzuknüpfen. Dieser war im BegleitG vorgesehen, ist aber in der endgültigen Fassung entfallen, der Wortlaut, des damaligen Vorschlags:

§ 99a

Von denjenigen, die geschäftsmäßig Telekommunikationsdienste erbringen, kann Auskunft über die näheren Umstände der Telekommunikation verlangt werden, wenn bestimmte Tatsachen den Verdacht begründen, daß jemand als Täter oder Teilnehmer eine Straftat begangen hat oder in Fällen, in denen der Versuch strafbar ist, zu begehen versucht oder durch eine Straftat vorbereitet hat, und insoweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist. Betrifft der Verdacht einer Straftat nicht eine mittels Endeinrichtungen (§ 3 Nr. 3 TKG) begangene Straftat, kann Auskunft über die nähe-ren Umstände der Telekommunikation nur verlangt werden, wenn Gegenstand der Untersuchung eine Straftat von nicht unerheblicher Bedeutung ist.

Die Auskunft darf nur vom Richter, bei Gefahr im Verzuge auch von der Staatsanwaltschaft verlangt werden.

Die Anordnung ergeht schriftlich. Sie darf sich nur gegen den Beschuldigten oder solche Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, daß sie für den Beschuldigten bestimmt oder von ihm herrührende Mitteilungen entgegengenommen oder weitergegeben haben oder das der Beschuldigte ihren Anschluß benutzt hat.

Nach einhellig vertretener Meinung gibt es derzeit keine Verpflichtung für die ISP's Verbindungs-daten zu speichern, so sie diese nicht für Abrechnungen benötigen. Der das TDDSG und die TDSV durchziehende Rechtsgedanke sei, daß Datenspeicherung vermieden werden solle (vgl. z.B. § 6 Abs. 3 S. 1 TDSV). Die sich aus § 6 Abs. 3 S. 2 TDSV ergebende Frist zur Datenspeicherung von 80 Tagen nach Rechnungsversand ist verschiedentlich von den Strafverfolgungsbehörden als problematisch angesehen aber als die derzeitige gesetzliche Lage akzeptiert worden.

Davon unabhängig können Daten möglicherweise auch freiwillig an die Strafverfolgungsbehörden gegeben werden - so vertreten von Seiten der Behörden, was allerdings auf star-ke datenschutzrechtliche Bedenken auf Seiten der ISP's traf. Nach derzeitiger Rechtslage könnte möglicherweise § 28 II Nr. 1.a) BDSG herangezogen werden. Bei der beabsichtigten Novelle des BDSG soll dazu explizit eine Norm vorgesehen werden.

Hingewiesen wurde darauf, daß die in § 90 TKG geregelte Kostentragungspflicht durch den Telekommunikationsdiensteanbieter (soweit TKG anwendbar ist) für Auskünfte nur für automatisierte Verfahren greife. Bei manuell erteilten Auskünften greift das ZSEG.

Fernmeldeüberwachung (FÜV, TKÜV, Technische Richtlinie zur TKÜV)

Die Technische Richtlinie zur TKÜV geht insbesondere auf ISP's ein, sei aber nur bindend für die Verwaltung. Aus nicht ersichtlichen Gründen ist die Technische Richtlinie als vertraulich eingestuft. Neuer Termin für Anhörung der be-troffenen Kreise zur TKÜV ist voraussichtlich im 1. Quartal 1999.

Streitig war, ob die FÜV überhaupt noch gültig sei, weil ihre Rechtsgrundlage weggefallen ist.

Beide Auffassungen (gültig / ungültig) wurden vertreten, mit einer Tendenz zu gültig.

Von Seiten der Staatsanwaltschaft wurde vertreten, daß ISP's nicht berechtigt seien, die rechtlichen Voraussetzungen einer Überwachung der Telekommunikation zu prüfen, sondern sie deren Anordnung Folge zu leisten hätten.

Strafrechtliche Verantwortung nach § 5 TDG

Eine strafrechtliche Verantwortung kann sich nach einhelliger geäußerter Meinung nicht aus § 5 Abs. 4 TDG ergeben. Dies ergibt sich aus dem klaren Willen des Gesetzgebers und dem Wortlaut. Außerdem hätte andernfalls § 5 Abs. 3 TDG entfallen können. Die einzige Stimme die sich gegenteilig äußerte ist rechtsirrig.

Vertreten wurde, daß es für „Kenntnis" im § 5 TDG alleine auf die Kenntnis der Tatsachen abzustellen sei. Eine juristische Beurteilung gehöre nicht dazu, eine Anwendung des § 17 StGB sei in der Regel ausgeschlossen.

Problematisiert wurde, ob § 9 Abs. 1 StGB hinsichtlich ausländischer Inhalte eine Strafbarkeit in Deutschland begründen könne hinsichtlich des zur Verfügung stellens oder des Verbreitens. Als streitig wurde angesehen, ob der Klick auf ein Angebot den Taterfolg in Deutschland herbeiführt oder ob der Taterfolg nur für solche Angebote gelten könne, die auf Deutschland gerichtet seien (was nach dieser Auffassung z.B. zu verneinen wäre bei einem Angebot in chinesischer Schrift).

Im übrigen ergäbe sich eine Strafbarkeit für ausländische pornographische Inhalte nach § 6 Nr. 6 StGB. Zumutbarkeit im Rahmen § 5 TDG und § 5 MdStV

Folgende - nicht abschließenden - Kriterien wurden für die Zumutbarkeitsprüfung im Rahmen des § 5 TDG, § 5 MdStV angeführt:

a. Wenn der Content Provider angegangen werden könne, sei der ISP nicht verantwort-lich.

b. Welche Bedeutung hat das Rechtsgut? Eine Sperrung sei eher zu bejahen, wenn das Rechtsgut international geschützt ist als wenn dies nicht der Fall ist.

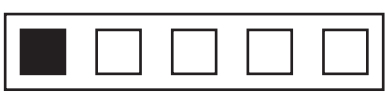
c. Unzumutbar sei eine tatsächlich unwirksame Sperrung.

Sperrung gem. § 5 TDG, § 5 MDStV, Filter

Es wurde die Auffassung geäußert, daß bei einer Sperrung nur eine solche eines ganzen Servers technisch möglich sei, die Sperrung einer einzelnen Adresse sei technisch noch nicht möglich.

Sollte dies den Tatsachen entsprechen, würde dies die Verhältnismäßigkeitsprüfung (Zumutbarkeit) im Rahmen des § 5 TDG, § 5 MDStV beeinflussen. Es müßte bei der Prüfung berücksichtigt werden, welche anderen Inhalte auf dem Server vorhanden sind und ob dieser Inhalte eine Sperrung möglicherweise auf verfassungrechtliche Bedenken stößt.

Das Problem ist praktisch relevant geworden im Falle eines japanischen Servers, der unter anderem kinderpornographische Inhalte gespeichert hatte. Es wurde versucht die Sperrung dieses Servers u.a. damit zu begründen, daß die übrige Inhalte ob der japanischen Sprache nur einer „verschwindent geringen Minderheit in Deutschland" verständlich sei. Eine derartige Argumentation erscheint unter verfassungsrechtlichen Gesichtspunkten äußerst problematisch, wenn nicht gar contra legem.



Tagungsbericht BKA-Tagung

Berichtet wurde von dem Entstehen der Internet Content Rating Alliance, die auf Basis des PICS Verfahrens Inhalte klassifizieren will. Die Einordnung soll durch die Autoren selber vorgenommen werden. Ein sogenanntes „Third Party Rating“ sei nicht zu bevorzu-gen. Die bewußte oder fahrlässige Falschklassifizierung soll durch Vereinbarungen mit den Autoren ausgeschlossen werden. Der Vorteil dieses Ansatzes sei, daß er international wirksam sei. Kritisch wurde geäußert, daß die Erfahrungen des RSACi einbezogen werden sollen, dessen Klassifizierungsystem nach europäischen Maßstäben problematisch sei.

Ein weiteres Verfahren stelle die PadGeo Software dar, die bekannte, als kinderpornographisch eingestufte Abbildungen, mit im Internet aufgefundenen Bildern vergleiche. Mit derartiger Software wollen die Strafverfolgungsbehörden und jugendschutz.net Abbildungen finden und gegen die Verbreiter vorgehen. Derartige Software ist aber noch so weit in den Anfängen der Entwicklung, daß jedes einzelne Bild, daß als pornographisch von der Software erkannt wurde, von einem Menschen überprüft werden muß.

Wie auf dem Chaos Communication Congreß 1998 (Berlin) berichtet wurde, würde andernfalls z.B. die Abbildung eines kahlen Kopfes aufgrund der Rundung als pornographisch eingestuft; ebensolches gelte für Software, die z.B. Von China oder Saudi Arabien als Filtersoftware eingesetzt wird. Mit ihr werden Texte nach mathematischen Verfahren analysiert. Dabei kann dann z.B. rauskommen, daß „Adolf Hilter war ein guter und friedvoller Mensch.“ nicht beanstandet wird, während „Adolf Hilter war ein dummes Schwein.“ beanstandet wird. Bereits an diesem einfachen Beispielen wird deutlich, daß eine automatische Filterung nach dem derzeitigen Stand der Technik nicht möglich ist, ganz davon abgesehen, ob ein solches Vorgehen rechtspolitisch und gesellschaftlich wünschenswert ist. Letzteres beides wurde auf der Veranstaltung des BKA ebenfalls stark bezweifelt bis abgelehnt.

Hyperlinks

Vereinzelt wurde vertreten, daß hyperlinks unter § 5 Abs. 1 TDG fallen und das ein zugängliche machen nach den §§ 86, 130, 131, 184, 130e StGB bei einem hyperlink auf den entsprechenden Inhalt gegeben sei. Dieser Auffassung ist mehrfach entgegengetreten worden. Im übrigen wurde zur Haftung für Inhalte, auf die hyplerlinks verweisen, die in der Literatur vertretenen Meinungen der Beurteilung nach § 5 Abs. 2 und § 5 Abs. 3 TDG vertreten. Teilweise wurde vorgetragen, es sei eine Einzelfallbetrachtung vorzunehmen. Vereinzelt wurde vertreten, daß bei Delikten, für deren Vollendung ein Zugänglichmachen ausreichend ist, die Strafbarkeit bereits mit dem Setzen des hyperlinks eintrete, während bei Verbreitungsdelikten dies nicht der Fall sei.

Diskutiert worden ist die Frage, inwieweit eine Haftung für hyperlinks der zweiten Ebene gegeben ist, d.h. wenn ein link auf einen Text mit weiteren links verweist ist fraglich, ob auch für diese weiteren hyperlinks gehaftet wird, die überwiegende Meinung hat sich dagegen ausgesprochen, mit der Tendenz eine Haftung nur für selber gesetzte hyperlinks zu aktzeptieren, es sei denn es läge ein Fall der Umgehung vor.

Da die Inhalte, auf die mit hyperlinks verwiesen wird, sich ändern können, empfiehlt es sich, diese in dem Zeitpunkt in dem man erstmalig auf sie verweist, zu dokumentieren.

14.-15. Dezember 1998 Wiesbaden

Nationale und Internationale Zuständigkeiten und Aktivitäten

Auf nationaler Ebene besteht ein schwer zu durchschauendes Geflecht von Zuständigkeiten und Aktivitäten.

Zuständiger Ansprechpartner für jeden ISP ist das jeweils zuständige Landeskriminalamt. Beim BKA ist eine zentrale Stelle (siehe Einführung) eingerichtet worden.

Aktivitäten entfalten weiterhin die Bundesprüfstelle, die Onlineangebote 'indiziert' und dies in ihrer Zeitschrift veröffentlicht (woraufhin diese bei diversen Nutzern kursiert um die „interessantesten" Angebote gleich sortiert zusammengestellt zu bekommen).

Im Auftrag der Jugendminister der Bundesländer durchsucht jugendschutz.net anlaßunabhängig das Internet mit einem crawler. Dabei sollen pro Nacht ca. 100 „Treffer" gefunden werden, von denen ca 50 nach manueller Sichtung relevant seien. Bezüglich jugendschutz.net kam die bekannte Diskussion Bund - Länder auf. Als Organisation der Bundesländer kann jugendschutz.net nur im Rahmen des MDStV tätig werden, nicht im Rahmen des TDG. Daher interpretieren die Vertreter dieser Stelle den MDStV auch so, daß alle Onlinedienste / Internetangebote darunter fallen. Dies wird - zu Recht - vom Bund abgelehnt. Soweit jugendschutz.net sich bei ISP's meldet, um Gesetzesverstöße anzumahnen, sollte daher äußerst sorgfältig geprüft werden, wieweit überhaupt eine Mediendienst im Sinne des MDStV vorliegt, in der Regel wird dies zu verneinen sein. Auf der Tagung wurde richtigerweise darauf hingewiesen, daß jugendschutz.net keinerlei Auskunftsrechte (siehe dazu oben) die den Strafverfolgungsbehörden zustehen in Anspruch nehmen kann. Auskünfte an jugendschutz.net sind freiwillig und daher nicht von Erlaubnistatbeständen, die bei Anfragen von Strafverfolgungsbehörden eingreifen, gedeckt. Gesetzesverstöße z.B. im Rahmen von Datenschutzrecht (Herausgabe personenbezogener Daten), sind daher denkbar bei der Beantwortung von Anfragen von jugendschutz.net durch ISP's.

Berichtet wurde kursorisch über eine Reihe von internationalen Organisationen, die sich mit dem Problem der Kinderpornographie beschäftigen.

```
Interpol
UNICEF, „How to ban childpornography form the
Internet"
ICPO / ECPAT , „Ethic Code"
G8, High Tech Crime Subgroup
International Champer of Commerce
Council of Europe
UNAFEI
EU
```

In den USA ist die Zollfahndungsbehörde für die Ermittlungen bei strafbaren Inhalten in Onlinemedien zuständig. Berichtet wurde über deren Möglichkeiten bei Ermittlungen.

Probleme der Strafverfolgungsbehörden

Von Seiten der Strafverfolgungsbehörden wurden u.a. folgende Probleme aufgeführt:

```
* Fake Accounts (Zugänge die unter Angabe von
falschen Personalien eingerichtet wurden).
* Auslandskunden der Online-Dienste.
* langsames Rechtshilfeverfahren.
* Löschungsfrist von 80 Tagen.
* Newsgroup Artikel seien aufgrund des kurzen
expires oft nicht mehr nachvollziehbar und daher
nicht verfolgbar.
* Anonyme Remailer würden eine Rückverfolgung
der Nutzer erschweren.
```

Wünsche der Strafverfolgungsbehörden

Die Vertreter der Strafverfolgungsbehörden haben eine Reihe von Wünschen geäußert:

Tagungsbericht BKA-Tagung

* Die Provider mögen Beiträge zur Aufklärung schwerer Straftaten leisten und die Strafverfolgungsbehörden mit know how und Computern unterstützen. Nützlich wären in diesem Zusammenhang auch regelmäßige Gespräche (ohne Anlaß) zwischen den Strafverfolgungsbehörden und den ISP's. Diese dienten der Information der Straverfolgungsbehörden über neue Entwicklungen, die technischen Möglichkeiten der Provider, strafbare Inhalte und der beiderseitigen Vertrauensbildung, damit konkrete Maßnahmen beschleunigt abgefertigt würden und Zwangsmaßnahmen vermieden würden.

* Von Seiten jedes ISP's sollten technische Ansprechpartner und die zuständige Geschäftsleitung benannt werden, die mit entsprechenden Vollmachten ausgestattet sind, damit Maßnahmen ohne Zeitverzögerung durchgeführt werden könnten. Straftaten, insbesondere Kinderpornographie, solle geächtet werden und Werbung für ein „Sauberes Netz" gemacht werden.

* Verantwortliche und deren Praktiken sollten offengelegt werden, sobald die Strafverfolgungsbehörden nachfragten.

* Eine schnelle Bearbeitung von Auskunftsersuchen sei aufgrund der Schnellebigkeit des Internets, in der 1 - 2 Stunden schon sehr lange sein könnten, wünschenswert.

* Kundendaten sollten verifiziert werden, bevor ein Zugang eröffnet würde.

* ISP's sollten mehr tun als das, was gesetzlich als Minimum gefordert wird. Dies betrifft insbesondere die Speicherung von Bestands- und Verbindungsdaten. Hierzu sei der § 7 TDSV extensiv auszulegen (siehe kritisch dazu oben unter Rechtsgrundlagen für Auskunftsersuchen).

* Soweit ein ISP kinderpornographische Abbildungen sperrt oder löscht wurde von Seiten der Strafverfolgungsbhörden der Wunsch geäußert, eingeschaltet zu werden, um nach Möglichkeit die Kinder zu ermitteln und diese Schützen zu können.

An den Gesetzgeber wurden die Forderungen gestellt, eine Evaluierung des IuKDG vorzunehmen, einen Ersatz für § 12 FAG zu schaffen und „Rufnummern" im 11. Teil des TKG, durch „Nummern" zu ersetzen, da nach einhelliger Auffassung Rufnummern keine IP Nummern oder ähnliche Angaben sind, sondern sich ausschließlich auf Rufnummern im Sinne des Sprachtelefondienstes bezieht. Gewünscht wurde auch, die Speicherfrist von 80 Tagen zu verlängern.

Tips für die ISP's

Um zu vermeiden, daß ISP's um die Herausgabe von Bestandsdaten gebeten werden, sollte darauf hingewirkt werden, daß alle Kunden, die content Anbieter sind, in ihrem Angebot eine Art Impressum mit angeben, in der Ansprechpartner für das Angebot genannt werden (vgl. § 6 TDG, § 6 MDStV).

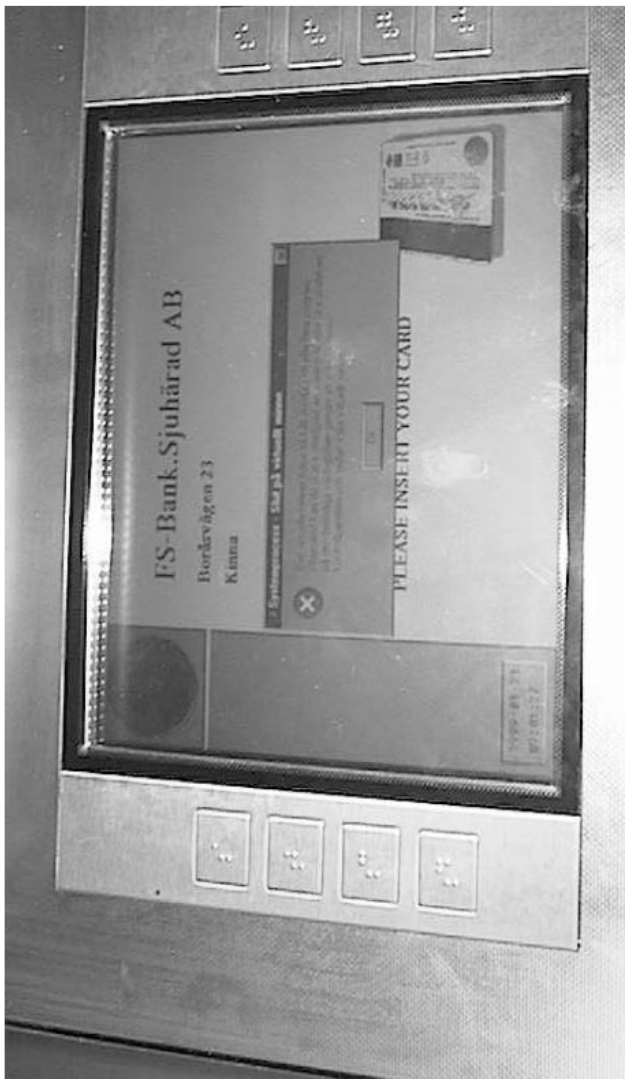
Die Allgemeinen Geschäftsbedingungen oder auch die individualvertraglichen Bedingungen mit den Kunden, die content Anbieter sind, sollten so gestaltet sein, daß eine Sperrung von möglicherweise nicht gesetzeskonformen Inhalten bereits bei Verdacht möglich ist und insbesondere auch dann, wenn die Prüfung, ob ein Gesetzesverstoß vorliegt umfangreich ist (Kostenvermeidung).

Die eigene Infrastruktur sollte so installiert sein, daß eine sofortige Sperrung rechtswidriger Inhalte in eigenen Speichern möglich ist.

In der Vergangenheit ist es immer wieder vorgekommen, daß die Ermittlungsbehörden ganze EDV Anlagen beschlagnahmt haben, so daß die betroffenen Privatpersonen oder Unternehmen nicht mehr weiter arbeiten konnten. Soweit ein solches Vorgehen von den Strafverfolgungsbehörden angestrebt wird, sollte von Seiten der ISP's darauf hingewirkt werden, daß lediglich Sicherungskopieen auf nicht mehr veränderbaren Speichermedien erstellt werden, die den Ermittlungsbehörden übergeben werden. Vertreter der Strafverfolgungsbehörden haben geäußert, daß sie damit im Regelfall ausreichend arbeiten können.

Soweit von den Strafverfolgungsbehörden der Gedanke einer „Selbstverpflichtungserklärung"

oder eines Code of Conduct weiter verfolgt wird, sollten die ISP's darauf achten, daß die ihre Interesssen berücksichtigt werden. Der bisher vom BKA zur Diskussion vorgelegte Entwurf müßte dazu verändert werden. Zu klären wäre auch, welche rechtliche Qualität eine solche Vereinbarung haben würde und welche Rechtsfolgen sich daraus ergeben könnten. Ob die Unterzeichnung eines derartigen Papiers sinnvoll sein wird, kann erst bei Vorliegen eines neuen Entwurfs beurteilt werden. Bekannt ist, daß auch auf internationaler Ebene (z.B. EU) an Codes of Conduct gearbeitet wird. Sinnvoll wird - wenn überhaupt - nur die Unterzeichnung eines dieser Papiere sein.



Außerhalb der Veranstaltung ist das Grundsätzliche Vorgehen des BKA's kritisiert worden. Es sei nicht Aufgabe der ISP's „im zunehmenden Maße Polizeiaufgaben zu übernehmen". Auf dem Chaos Communication Congreß '98 wurde die Auffassung vertreten, daß die Vorgehensweise Sperrung / Filterung grundsätzlich zu überdenken sei. Aus neuen medienpädagogischen Untersuchungen ergebe sich keinerlei Anhaltspunkt dafür, daß Kinder und Jugendliche durch das Ansehen von erotischen und pornographischen Abbildungen psychologisch geschädigt würden. Die Studien die von den entsprechenden Stellen immer wieder zum Beleg des Gegenteils herangezogen würden, seien wissenschaftlich veraltet und inzwischen unhaltbar. Wichtig sei dahingegen, daß Kinder und Jugendliche an dem Umgang mit dem Medium herangeführt würden. Daher sei der Schwerpunkt stärker auf pädagogische Maßnahmen, als auf Sperrung und Filterung zu legen, die erfahrungsgemäß umgangen werden könnten oder nicht funktionierten.

RA Alexander Eichler, Wiesbaden

Berichte vom 15. Chaos Communication

Wilde Sachen bei Nacht

Nachdem abends der Congresstag eigentlich beendet ist, gibt es eine bemerkenswert große Gruppe von Leuten, die diese Tatsache schlichtweg ignorieren. Sie sitzen im Hackcenter und scheinen sich vollständig von den anderswo geltenden Maßstäben von Zeit und Raum abgekoppelt zu haben.

Beim nächtlichen Streifzug durch das Hackcenter kann man diese Leute die kuriosesten Sachen machen sehen, die für den Freund des innovativen Technologieeinsatzes spannend und lehrreich sind.

Im Untergeschoß des Hackcenters wurde beispielsweise die ganze Nacht über an Lego- und Fischertechnik-Robotern und -Maschinen gebastelt. Eine Gruppe verstieg sich durchaus erfolgreich in dem Plan, den Prototyp eines Computers, eine Turing-Maschine, zu bauen. Dabei handelt es sich um eine Maschine, die auf einem Papierstreifen schreiben und lesen kann und auf diesem unendlich langen Band auf- und abfährt und die daraufliegenden Befehle ausführt, sowie neue Daten auf den Streifen schreibt und liest.

An anderer Stelle hatte man einige biometrische Devices zum Testen aufgetrieben und machte sich ernsthaft daran, biometrische IDs zu fälschen. Während man das Überlisten eines Infrarot-Durchlicht-Fingerscanners verschieben mußte, gelang es nach zahlreichen Versuchen mit Stempelkissenfarbe, Wachs, Klebeband und Folie, mittels eines Zigarettenblättchens und eines Bleistifts eine „Fingerdublette“ herzustellen, mit der man ein rein optisches Fingererkennungssystem überlisten konnte.

Andere Spontan-Workshops beschäftigten sich mit dem Aufbau und der Technik von Mobilfunkstationen, der Zahl 23, der untersten Netzwerkschicht und dem ARP-Protokoll oder dem Aufbau und der Sicherheit von deutschen Universitätsnetzwerken.

Einer der Höhepunkte des Hackcentertreibens endete am frühen Abend in einem Besuch von Beamten der Computerkriminalitätsabteilung des LKA Berlin. Cracker waren in das Netz eines bremischen Internetproviders eingedrungen, hatten dort sämtliche überflüssige Daten entfernt, das heißt, vor allem nutzlose Werbeinformationen diverser Unternehmen gelöscht und auf den etwa 40 dort betriebenen virtuellen Servern ein Musikarchiv für die Weiterbildung junger Leute angelegt.

Der Betreiber des unzureichend gesicherten Servers zeigte für diese Maßnahmen wenig Verständnis und versprach sich Hilfe vom LKA, bei dem er Anzeige erstattete. Da die Angriffe von einer IP-Adresse innerhalb des Hackcenter-Netzes zu kommen schienen, versprachen sich die Staatsdiener von einem Besuch dort eine Chance, des Crackers habhaft zu werden. Problematisch war allerdings die Frage, ob der Rechner mit der entsprechenden IP dem Cracker gehörte oder ob die Maschine selber nur als Attack-Proxy verwendet wurde.

Der Polizei gelang es allerdings nur, eine einzige „heiße“ Spur sicherzustellen: ein dampfendes chinesisches Essen, das an dem Arbeitsplatz stand, der der fraglichen IP zugeordnet war. Ansonsten fand man nur ein Netzwerkkabel und einen leeren Platz, an dem kurz zuvor der Computer entfernt worden war.

Die Polizei bittet den Besitzer des Rechners, sich selbst zu melden - und andere Menschen darum, diesen Besitzer zu melden. Es gibt auch eine Täterbeschreibung: „männlich, ungefähr 1,80 groß und nicht ganz lange und eher dunkelblonde Haare“. Nächtlicherdings gab es dann noch einige spannende Probleme mit der Internetanbindung, die damit endeten, daß im Hackcenter der Internetzugang nur noch stark eingeschränkt möglich war.

Alles in allem also eine spannende und lehrreiche Nacht, die zahlreiche Möglichkeiten zur Weiterbildung bot.

doobee@ccc.de

Congress 27.-29.12.1998 in Berlin

MP3 Workshop: All rights reversed?!

Der Workshop führte in die Technik der Komprimierung mittels MPEG ein und mündete in eine Diskussion um die Auswirkungen der Technologie auf die zukünftige Entwicklung der Vermarktung von Musik im und außerhalb des Internet.

Die Technik

Musik besteht aus Schallwellen, die mittels eines Mikrofons in elektrische Schwingungen umgewandelt werden können. Um diese analogen Signale, die auf einem Diagramm der Signalstärke, abgetragen gegen die Zeit, komplizierte Wellen ergeben, digital speichern zu können, werden die analogen Axen des Diagramms in kleine Abstände unterteilt (quantisiert).

Die Unterteilung der Zeitachse ergibt eine zeitliche Auflösung, die mit der Sampling-Rate angegeben wird. Die Sampling-Rate gibt in Samples pro Sekunde an, wie häufig ein Meßwert (der Signalpegel) pro Sekunde erfaßt wird.

Die Quantisierung der Amplitude (Signalstärke) ergibt eine maximale Anzahl von Werten, in die die zu digitalisierenden Signalpegel einsortiert werden müssen. Diese Anzahl der möglichen Werte ergibt die Audio-auflösung - meist angegeben in Bit.

Auf einer handelsüblichen Musik-CD wird z.B. eine Samplingrate von 44kHz (also 44000 Meßwerte pro Sekunde) und eine Audioauflösung von 16 Bit (65536 mögliche Signalpegel) verwendet.

Speist man die auf diesem Weg erhaltenen Daten in ein normales Komprimierungsprogramm (z.B. ARJ oder ZIP) ein, so stellt man fest, daß die Komprimierung nur sehr gering ist. Solche Komprimierungsverfahren versuchen Regelmäßigkeiten in den zu komprimierenden Daten zu finden, die in digitalisierten Audiodaten kaum vorkommen.

Die erste Idee könnte nun sein, einfach die Audioauflösung zu verringern und somit Daten einzusparen. Leider führt dies zu einem Qualitätsverlust: Auf je weniger mögliche Werte die analogen Daten abgebildet werden, um so größer werden die dabei auftretenden Rundungsfehler. Diese Rundungsfehler erhöhen maßgeblich den Rauschanteil. Für eine möglichst verlustfreie Komprimierung von Audio-Daten ist dieses Verfahren damit unbefriedigend.

Biologen gehen davon aus, daß vom menschlichen Ohr zum Gehirn ein Datenstrom von ca. 2000-3000 bit/s fließt. Die Schätzung geht zurück auf die Annahme, daß Informationen mit ca. 60-100km/h in den Nerven übertragen werden und der Nervenstrang vom Ohr zum Gehirn keinen größere Datenmenge transportieren kann. Eine CD beinhaltet einen Datenstrom von ca. 1.000.000 bit/s. Im Gehirn kommen von den Informationen, die auf einer Audio-CD gespeichert sind, also nur ca. 0,25% an.

Die Psychoakustik beschäftigt sich mit der Frage, welcher Anteil der Informationen, die als Schallwellen auf unser Ohr treffen, tatsächlich im Gehirn ankommen. Als Antwort auf diese Frage wurde bisher keine einheitliche Formel gefunden. Verschiedene Forschungsinstitutionen haben in sehr vielen Versuchsreihen mit Testhörern herausgefunden, was in Audiosignalen weggelassen werden kann, ohne daß ein Unterschied für die Testpersonen hörbar war.

Das Ohr ist träge, und diese Trägheit sorgt dafür, daß leise Töne nach einem lauten Ton nur sehr schlecht oder gar nicht wahrgenommen werden -

ebenso wie vorhergehende leise Töne für einen kürzeren Zeitraum überschattet werden. Ähnliches gilt für einen intensiven Ton auf einer Frequenz, der Töne auf unmittelbaren Nachbarfrequenzen überdeckt. Hohe Töne werden eher wahrgenommen als tiefe Töne.

In Hinblick auf diese Erkenntnisse wurden empirische Daten ausgewertet und genaue mathematische Regeln erstellt, die beschreiben, welche Informationen im Audiosignal eingespart werden können, ohne daß die Qualität für den Hörer merklich sinkt.

Technisch wird hierfür das Audiosignal in 32 Frequenzbänder geteilt (z.B. 100Hz, 200Hz, ... , 2kHz, 4kHz...). Dabei teilt sich ohne Komprimierung die Anzahl der möglichen Werte (Audioauflösung) durch die Anzahl der Frequenzbänder, und jedes Frequenzband erhält einen eigenen, entsprechend kleineren Wertebereich.

Für die Komprimierung nach den psychoakustischen Kriterien wird nun die Anzahl der möglichen Werte für durch benachbarte laute Frequenzen überdeckte Frequenzen gesenkt, da diese Frequenzen schlechter wahrgenommen werden. Dadurch können Daten eingespart werden.

Ein ähnliches Verfahren wird auf der Zeitachse des Audiosignals verwendet, um Signalen, die einem sehr viel lauterem Signal vorausgehen oder folgen, ebenfalls einen kleineren Wertebereich zuzuweisen.

Die entstehenden Ungenauigkeiten (Rauschanteil) bei der verlustbehafteten Komprimierung werden somit auf Signalanteile verteilt, die über den Hörapparat das Gehirn nicht oder nur sehr schwach erreichen. Der

Qualitätsverlust ist im Verhältnis zur eingesparten Datenmenge sehr gering. Bei einer Komprimierung von 1:12 ist die Qualität für die Wiedergabe von Musik mit der Qualität von Radio vergleichbar.

In der Weiterentwicklung des umrissenen Verfahrens soll 'guessing' - der Versuch die Werte eines Folge-Samples zu raten - zum Einsatz kommen und die Komprimierungsrate nocheinmal erhöhen. Auch hierfür werden Versuchsreihen mit Testhörern durchgeführt, die zeigen sollen, bis zu welchem Maß das Verfahren geeignet ist, und an welchen Stellen die Abweichung in den geratenen Samples durch Checksummen korrigiert werden muß.

Die technischen Verfahren zur Dekomprimierung (!) solcher Datenströme wurden in ISO-Normen von der Motion Picture Encoding Group (MPEG) normiert. Zur Norm gehören nicht die Kodierungsverfahren, deren Qualität maßgeblich von der Forschungsarbeit der einzelnen Anbieter auf dem Gebiet der Psychoakustik abhängt. In den Normen der MPEG wird jedoch - wie der Name vermuten läßt - nicht nur Audiodekomprimierung festgelegt, sondern auch die Verfahren zur Videodekomprimierung. Zielsetzung der Gruppe ist es, Normen festzulegen, nach denen Bild und Ton von digitalen Datenträgern (CD, DVD) oder aus digitalen Datenströmen (Fernsehen, Internet) dekodiert und wiedergegeben werden können.

Der erste verabschiedete Standard war MPEG1. In MPEG1 (ISO11172) wurde festgeschrieben, wie von einer normalen CD mit 1-facher Abspielgeschwindigkeit Video und Audio wiedergegeben werden kann. Die Norm teilt den Datenstrom in drei Layer: Auf Layer 1 werden Daten für die Zusammensetzung von Audio und Video Datenstrom transportiert (System Stream), auf Layer 2 werden die Video-Daten als halbes PAL-Bild übertragen und auf Layer 3 letztendlich die Audio-Daten.

Congress 27.-29.12.1998 in Berlin

Da MPEG1 für die CD entwickelt wurde, sind flexible Bandbreiten für die einzelnen Kanäle nicht vorgesehen.

Das technische Verfahren zur Dekomprimierung von Audiodaten im anfänglich beschriebenen Format findet sich in der Nachfolgenorm MPEG2 Layer 3. Ebenso wie bei MPEG1 ist MPEG2 (ISO13848) in drei Layer für Steuerdaten, Video und Audio getrennt. Mittels der neuen Norm können Datenströme mit beliebiger Qualität dekodiert werden und die Verfahren wurden optimiert und erweitert um eine Übertragung des Datenstroms über eine verlustbehaftete Verbindung (z.B. einen Fernsehkanal) zu unterstützen. In einer Erweiterung (MPEG2 Layer3 ACR), die bisher noch nicht zum Einsatz kommt, ist schon festgeschrieben, wie mehrere Audiokanäle für z.B. Surround Sound übertragen werden.

Das Verfahren zur Komprimierung von Videosignalen funktioniert ähnlich wie die Komprimierung der Audiodaten (jedoch ist in der Norm auch für Video nur die Dekomprimierung für Video genormt): Das Videobild wird in Quadrate von 8x8 Pixeln zerteilt. Betrachtet man die 64 Pixel eines solchen Ausschnitts aneinandergereiht und fährt mit einer konstanten Geschwindigkeit an ihnen entlang, so ergibt sich eine Signal aus Helligkeitwerten, das sich genauso wie ein Audiosignal in Samples zerlegen läßt. Diese Samples können wieder in Frequenzbänder geteilt und nach ähnlichen Kriterien wie das Audiosignal komprimiert werden. Die Komprimierung der Videobilder entspricht technisch dem JPEG-Verfahren für Einzelbilder.

Zusätzlich wird betrachtet, ob sich ein bestimmter Ausschnitt aus 8x8 Pixeln im Folgebild an einer anderen Stelle wiedergefunden werden kann und somit nur dessen Bewegungsvektor und nicht die vollständige Bildinformation übertragen werden muß. Ein Fernsehbild läßt sich so komprimiert in einen 6MBit Datenstrom verpacken.

Konkurrierende Verfahren wie z.B. RealAudio, RealVideo oder LiquidAudio weichen vom technischen Verfahren von MPEG2 nur in der Umsetzung ab. Die Grundlagen sind dieselben. Es läßt sich nicht feststellen, daß eines dieser Verfahren qualitativ besser wäre als die normierten.

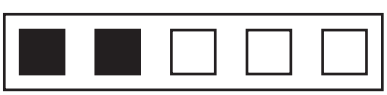
Für die Komprimierung von Audiodaten nach MPEG2 Layer 3 in Echtzeit wird ein PentiumII 300MHz benötigt. Eine günstige Hardwarelösung ist von Thomson für ca. 300,- DM angekündigt. Zum Abspielen reicht hingegen jeder Pentium-PC. Von zwei IC-Herstellern (ITT und Thomson) gibt es Ein-Chip-Lösungen für die Dekomprimierung, die in entsprechender Stückzahl für ca. 15$ verkauft wird.

Folgen, Utopien

Weltweit gibt es bisher 15 Hersteller, die Taschengeräte zum Abspielen von MPEG2 Layer 3 kodierten Musikdaten anbieten. Der Speicher der Geräte liegt zwischen 32MB und 64MB und reicht somit für 30-60min Musik in Radioqualität.

Im Internet werden Dateien mit Musikstücken verteilt und getauscht, die über eine Computerschnittstelle in die meisten Abspieler überspielt werden können. Diese Entwicklung wird von den großen Musikproduzenten gebremst, kann jedoch nicht gestoppt werden.

In Zukunft könnte die Stellung der Produktionsfirmen ins Wanken kommen, da der Vertrieb über das Internet theoretisch direkt von den Künstlern zu den Konsumenten möglich ist. Neben allen damit verbundenen Ideen, Idealen und Utopien wurde jedoch nicht aufgezeigt, daß es neben einer Untergrundszene, die illegal Musik kopiert und tauscht, ernstzunehmende Ansätze



für die Bedienung eines öffentlichen Massenmarktes gibt.

Den einzige, von den Anwesenden abgelehnten Vorstoß in den elektronischen Vertrieb von Audiodaten unternimmt ein Internet-Anbieter in Deutschland: Über WWW-Seiten können Titel ausgewählt und gegen eine Gebühr von 0,10DM in Ausschnitten angehört werden. Wird ein Titel zum Kauf gewählt, so wird die Verbindung zum Internet-Anbieter getrennt und ein Server ruft via ISDN den Kunden an und liefert die Datei aus. Die Musikdatei ist allerdings verschlüsselt und kann nur mit dem Programm der Empfängerin gehört werden. Für die private Nutzung gibt es kostenlos eine Zweitlizenz für eine zweite Installation. Bei einem Preis von 3-5 DM pro Musiktitel wird an der Akzeptanz gegenüber dieses Verfahrens zu Recht gezweifelt.

Einigkeit bestand in dem Punkt, daß Musik zu teuer ist und nicht nachvollziehbar ist, wo das Geld bleibt. Der von den Produktionsfirmen angestrebte Preis von 50,- DM pro CD dürfte angesichts der aktuellen Entwicklungen jedoch nicht haltbar bleiben.

Ein philosophischer Ansatz für die freie Verfügbarkeit von Musik war, daß sie - einmal gehört - in Fragmenten im Gehirn gespeichert wird. Beim erneuten Hören werden lediglich Erinnerungen erneuert. Unbeantwortet blieb hierbei jedoch die Frage, warum die Dienstleistung der Auffrischung von Erinnerungen nicht vergütet werden sollte.

Vortrag: Andreas Bogk <>

Bericht: Chris Vogel <c.vogel@link-goe.de>

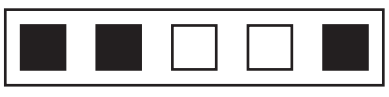
Anonymität im Netz

Welche Daten werden mitgeschickt, wenn eine Website abgerufen wird? Schon bei einem einfachen http-Request werden User- und Systemdaten mitübertragen, die zum einen dazu genutzt werden können, sich ein Bild vom User zu machen (user profiling), zum anderen kann der Verlauf während des Aufenthaltes im Web nachvollzogen werden (user tracing). Aussagen über den Rechner und seinen Benutzer erhält man z.B. aus Angaben über den Browser, die Sprache und natürlich über die IP-Adresse. Der erste Weg zu Anonymität im Netz ist daher, fremde Logfiles mit möglichst wenig Angaben über sich zu füttern.

Hierfür wurde neben dem "Janus-Projekt" http://janus.fernuni-hagen.de und "Mixmaster" auf das Programm "Junkbuster" eingegangen. Anonymicer finden sich auf http://www.informatik.tu-muenchen.de/cgi-bin/ucgi/pircher/ssis/anonymicer/index.html.

Am weitesten geht Mixmaster, bei dem die Daten in gleich große Blöcke geteilt werden, so daß durch eine Analyse des Traffics praktisch keine wertvollen Rückschlüsse möglich sind. Außerdem werden die Daten für jeden Proxy, über die das Anonymizing läuft, gesondert verschlüsselt. Anonymität ist nicht nur gegenüber den Anbietern der Sites notwendig, sondern kann auch innerhalb eines corporate network sinnvoll sein. Als Beispiel wurde ein Angestellter angeführt, der am Arbeitsplatz surft und neue Stellenanzeigen studiert. Durch die Dokumentation aller angewühlten Seiten in Logfiles erfuhr der Arbeitgeber frühzeitig von seinen Plänen, sich beruflich zu verändern.

Nächster Themenkomplex waren Identifyer wie Cookies, durch die z.B. zur Erstellung von Kundenprofilen auf der Festplatte des Users Daten gespeichert und dieser dadurch



wiedererkannt werden kann http://www.cookiecentral.com/unofficial_cookie_faq.html . Neben dem Aufbau von Cookies wurde auf eine weitere Gefahr hingewiesen, wie die Mail-Adresse des Users herausgefunden werden kann: Ist bei der Konfiguration als Passwort für anonymous-ftp die eigene Mail-Adresse eingestellt, muß nur im Hintergrund einer Website ein anonymous-ftp angestoßen werden und der Server erhält die gewünschte Adresse.

Zuletzt wurde auf Crowds eingegangen, einen Verband kooperierender Proxies zum Anonymizing [http://www1.informatik.uni-erlangen.de/crowds/]. Hierbei wird symmetrisch und für alle Proxies mit dem gleichen Key verschlüsselt, wodurch Crowds wesentlich schneller als Mixmaster arbeitet. Als Ausgleich für die schwächere Verschlüsselung tunnelt Crowds schnell durch viele Proxies.

Der Vortrag wurde von drei Erlangener Informatikern vorbereitet und von Matthias Bauer vorgetragen.

Bericht: Jockel v. Nieman <vnieman@gmx.de>

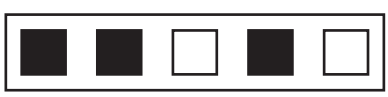
Einführung in Dylan

So etwas wie eine ideale Programmiersprache scheint es nicht zu geben. Nehmen wir zum Beispiel die Typisierung von Variablen. Es gibt im Grunde zwei Konzepte: dynamisches Typing und statisches Typing. Beides hat seine Vor- und Nachteile: Bei Sprachen wie C muß ich explizit festlegen, ob ich Ganzzahl-, Fließkomma- oder Zeichendaten verwenden will. In Perl dagegen schreibe ich einfach die Variable, die Sprache kümmert sich dann um die Typisierung. Dieses Verfahren ist natürlich viel bequemer, wenn ich einfach nur schnell eine Idee hinprogrammieren will, auf der anderen Seite ist es natürlich verständlich, daß eine solche dynamische Typisierung nicht sehr performant ist. Der Compiler kann den Code nicht zur Compile-Zeit auf den Datentyp hin optimieren. Ein klassisches Dilemma, so scheint es.

Vorhang auf: In diese Problematik hinein kommt Dylan (Dynamic Language), eine relativ junge Programmiersprache, die ihre Wurzeln bei Apple hat. In Dylan kann man problemlos einfach so drauflosprogrammieren und muß sich nicht um Typisierung kümmern. Wenn das Programm dann allerdings auf Geschwindigkeit optimiert werden soll, benutzt man einfach statisches Typing. Das beste zweier Welten, sozusagen.

Ähnliche Konfliktfelder gibt es bei der Art der Sprache: Neben den bekannten imperativen Programmiersprachen wie Pascal und C gibt es noch objektorientierte Sprachen wie Smalltalk, C++ oder Java und zu guter letzt funktionale Sprachen, von denen LISP die bekannteste sein dürfte. Dylan ist auch hier wieder hybrid. Komplett objektorientiert hat es trotzdem Möglichkeiten zur funktionalen Programmierung. Die Syntax von LISP ist ja so eine Geschmackssache. "Es gibt zwei Arten von Leuten: Die einen stehen auf viele Klammern und die anderen hassen es. Die meisten hassen es", fasst Andreas Bogk zusammen. Dylan hat daher eine sehr angenehm zu lesende, Pascal-ähnliche Syntax. Dylan verfügt aber auch noch über andere Features, die man von einer modernen Programmiersprache erwartet. Garbage collection, das automatische Entsorgen ungenutzter Variablen oder Objekte, kennt man aus Sprachen wie Perl oder Java und natürlich gibt es sie in Dylan auch.

Eine Sache, die man sich bei der objektorientierten Programmierung immer wünscht, ist die Trennung von Methoden und Objekten. "Wenn ich zwei Objekte 'Frau' und 'Mann' habe und die Methode 'Sex' darauf



anwenden will -- soll dann die Methode 'Sex' zum Objekt 'Mann' oder 'Frau gehören?" machte Andreas Bogk die Überlegungen der Dylan-Designer deutlich.
Weiterhin bietet Dylan durch sogenannte Slots nette Möglichkeiten, um Objekten andere Objekte zu übergeben. Während man typischerweise unter C++ selbst Methoden schreibt, um Member Variables zu setzen oder sie aus dem Objekt herauszuziehen, kann man in Dylan ganz bequem Slots definieren, und die "Getter"- und "Setter"-Methoden stehen automatisch zur Verfügung.
Soweit kurz zu den Features von Dylan, zu denen es durchaus noch mehr zu sagen gäbe. Auf der Implementationsseite sieht Dylan auch relativ vielversprechend aus. Das ursprüngliche Projekt bei Apple kam zwar nie über den Status einer technologischen Machbarkeitsstudie hinaus, aber es gibt noch andere Ansätze. Eine kommerzielle Implementation für Win32 ist fertig (näheres unter http://www.harlequin.com/) und erzeugt Code, der zu 99% so schnell ist wie C.
Eine freie Implementation von Dylan für Unix-ähnliche Betriebsysteme läuft unter dem Namen "Gwydion Dylan". Andreas Bogk ist selbst maßgeblich am Gwydion Dylan-Projekt beteiligt. Haufenweise Informationen hierzu gibt es unter http://www.gwydiondylan.org/ . Ganz fertig ist der natürlich in Dylan selbst geschriebene Compiler noch nicht, es fehlen noch Details. Auch die Perfomanz des vom Compiler erzeugten Codes kommt bei weitem noch nicht an C heran, aber Andreas Bogk verspricht Programme, die etwa "um den Faktor 10 schneller als Perl laufen". Immerhin, ein Anfang. Dylan wird noch von sich hören lassen.

Vortrag: Andreas Bogk <andreas@ccc.de>
http://www.gwydiondylan.org/

Bericht: Jens Ohlig <jo@devcon.net>

Funkamateur Lizenzkl. 3 Crashkurs

Die Veranstaltung "Funkamateur Lizenzklasse 3 Crashkurs" fand auf dem diesjährigen "15. Chaos Communication Congress" als dreiteilige Veranstaltung, verteilt auf die drei Kongresstage statt. Sie sollte eine allgemeine Einführung in den Prüfungsstoff der neu geschaffenen Funkamateur Lizenzklasse 3 geben. Wegen der - relativ zu den höheren Klassen 2 bzw. 1 - eher geringen Anforderungen in dieser Klasse ist diese Prüfung auch für interessierte Einsteiger in wenigen Wochen zu erlernen.

Die erste Veranstaltung gab einen Überblick über die derzeitige Situation im Äther. Kurz wurden die verschiedenen Teilnehmer am Funkverkehr (Betriebsfunk, Behörden / Organisationen / Sicherheitsaufgaben (BOS), Telefonie, CB-Funk, Amateurfunk incl. Packet Radio usw.) ihre verwendete Technik und deren Wellenbereiche besprochen. Anschließend folgten Informationen über das neue Amateurfunkgesetz und die neuen Amateurfunklizenzen, insbesondere die Klasse 3 für den vereinfachten Einstieg. In der folgenden Diskussion wurden unter anderem Fragen zum Stichwort "Experimentiercharakter des Amateurfunk" oder "der Unterschied zwischen einem Amateurfunker und einem Funk Amateur" eingehend erörtert.

Der zweite Teil der Veranstaltung beschäftigte sich mit allen Belangen der sogenannten Betriebstechnik. Unter diesem Oberbegriff wurden verschiedene Dinge besprochen: - das Internationale Buchstabieralphabet (Nato Alphabet) - die Q-Schlüssel - also Abkürzungen für bestimmte, oft wiederholte Ausdrücke in der Funkersprache. - Frequenzlisten - Landeskenner - Locator Koordinatensystem - Bewertung der Verbindung nach Lesbarkeit, Signalstärke und Tonqualität - Zulassung als Amateurfunkdienst - Bestimmungen zur Sendung der Rufzeichen - Aufbau der Rufkennzeichen. Leider mußte die

dritte Veranstaltung, die den technischen Teil der Prüfung behandeln sollte kurzfristig abgesagt werden. Die Referenten entschuldigten sich und boten allen Teilnehmern an sich per EMail bei ihnen zu melden. Sie würden dann eine Prüfungs-Mailinglist einrichten.

<Mittlerweile geschehen: mail an funk-subscribe@lists.ccc.de genügt, der Setzer>

Referenzen:

Regulierungsbehörde für Telekommunikation und Post Postfach 8001 55003 Mainz Fax: 06131 18-5620 http://www.regtp.de Hier ist auch der Fragen- und Antwortkatalog mit den offiziellen Fragen der Prüfung zur Lizenzklasse 3 erhältlich.

Vortrag: Michael Grigutsch <migri@ccc.de>, Bericht: Heiner Otterstedt <h.otterstedt@link-goe.de>

GSM-Unsicherheit

Welche Sicherheitsmerkmale sind im GSM Netz implementiert? Wenigstens kann man dort nicht wie im alten analogen C-Netz einfach mit einem Scanner mithören, denn zwischen Basisstation und Telefon werden die Daten verschlüsselt. Auch sind die Telefonnummern an sich nicht auf der SIM-Karte gespeichert, sondern nur in einer zentralen Datenbank des Netzbetreibers, wo zu jeder SIM-Nummer die Telefonnummern zugeordnet wird. Wenn sich das Telefon authentifizieren will, bekommt es vom Authentification Center (AC) eine RAND Challenge, die in der SIM-Karte mit dem Geheimschlüssel und dem A3-Algorithmus zum SRES verarbeitet wird. Diese SRES geht zurück an den AC, der sie mit einer von ihm berechneten SRES vergleicht. Sind beide identisch, gibt das AC grünes Licht. Der A3 Algorithmus ist nicht in jedem Netz gleich, aber es gibt einen Referenzstandard dafür (COMP128), der bis vor kurzem nicht bekannt war (Security by obscurity). Bis auf die sicherheitsrelevanten Themen ist aber der GSM-Standard unter [1]http://www.etsi.fr/ zu finden.

Zur Verschlüsselung werden 128 Bit RAND und 128 Bit KI 40 mal durchrotiert, allerdings sind das 1. und 8., das 2. und 9. Byte (usw...) miteinander verbunden. Nach 6-18 Stunden und in der Regel 150.000 Durchläufen kann man sich den Geheimschlüssel durch diesen Bug generieren und auf einem Simulator eine echte Karte emulieren. Der A5-Algorithmus ist ein 64 Bit langer Key, von dem allerdings die letzten 10 Bit Nullen sind. Ein weiterer Key (A8) dient der Schlüsselgenerierung. Lucky Green erzählte von den Begebenheiten, die dazu geführt haben, daß er den COMP128 gefunden hat: Er stolperte bei einer Übersetzung eines GSM Manuals über den Befehl "Run GSM Algorithm" und versuchte, im Netz etwas über COMP128 herauszufinden. Er fand nur eine in Teilen falsche Version und suchte drei Monate, um den richtigen Algorithmus zu finden. Den gab er zwei Freunden, die sich an der UC Berkley auf Kryptografie spezialisiert haben, und innerhalb vor zwei Stunden war er geknackt.

Drei Tage vor der Veröffentlichung fand er einen Hersteller, der Chipkarten mit COMP128 und veränderbarer Schlüssel herstellt, und natürlich bestellte er alle 8 in Nordamerika verfügbaren Exemplare. Mittlerweile wird in etwa 100 Millionen Mobiltelefonen COMP128 eingesetzt, und die Austauschkosten werden sich auf etwa 1,6 Millionen Dollar belaufen. Auch die 12 Provider weltweit, die nicht COMP128 benutzen, setzen aus irgendeinem unerfindlichen Grund die letzten 10 Bits des A5 auf Null. Natürlich war es nicht Sinn des Experiments, GSM zu zerstören, sondern nur darauf hinzuweisen, daß es immer ein Problem ist, wenn Kryptoschlüssel nicht öffentlich gemacht werden.

Übrigens es ist auch kein Problem, eine unechte Basisstation zu bauen, die nur Challenges aussendet um so an die Schlüssel mehrerer Mobiltelefonen zu kommen. Bei Motorola Telefonen kann man sogar recht einfach die Software ändern und so aus einem

handelsüblichen Telefon und mit ein wenig krimineller Energie eine unechte Basisstation bauen. Dies ist möglich, da sich die Basisstation nicht authentifizieren muß, sondern nur das Telefon. Andreas ist davon überzeugt, daß die GSM Standards absichtlich so niedrig gehalten wurden. So werden beispielsweise nur die Daten zwischen Handy und Basisstation mit A5 verschlüsselt, aber nicht zwischen der Basisstation und dem Netz an sich, wo Funkstrecken benutzt werden. (Richtfunkstrecken). Wenn man sich in einem anderen Netz befindet (Ausland), dann werden vom Heimnetz an das Roamingnetz fünf Tripplets aus RAND, SRES und KI geschickt aber nur eins davon benutzt. Die restlichen könnte theoretisch ein anderer benutzen, um so ohne eigene Selbstkosten zu telefonieren.
Die von den Netzbetreibern verbreitete Legende, daß man sich nicht mit der selben SIM mehrmals in ein Netz einloggen kann, ist nicht wahr. Um Gespräche abzuhören genügt übrigens A8, A3 und COMP128. A5 muß man nicht unbedingt kennen. Aber nicht nur das GSM-Netz an sich, sondern auch viele Telefone haben Schwachstellen oder ausgeschaltete Features, die man in einem Servicemode aktivieren kann. Durch diesen Servicemode kann man aus seinem Billighandy manchmal ein "Top the line" Gerät machen.
Weitere Informationen zum Thema sind das im Hansa-Verlag erschienene "Handbuch der Chipkartentechnik" von Ranke und Effing ISBN 3-496-18893-2 ISO 7816 für Chipkarten an sich der GSM Standard 11.11 [2]http://www.efri.fr/ und das Programm Serprog von Tron, das (wie auch Wafercards) im Archiv zu finden ist.

References

1. http://www.etsi.fr/
2. http://www.efri.fr/

Vortrag: Andreas Bohk, Lucky Green, Janus <ich@andreas.org>, Bericht: Dirk Steinhauer <moose.uni.de>

Linux Cluster

Der Vortrag hält sich nicht an allgemeine Cluster mit Linux, sondern an den Paderborner Linux Cluster vom 5/6.12.98 (die spannende Fernsehübertragung haben sich ja einige angetan ;-)) Die Referenten haben leider gestern erst von ihrem Vortrag erfahren und konnten deshalb nur unvorbereitet in den Workshop gehen.

Die Idee zu einem Linuxcluster kam über eine Mailingliste Anfang Oktober auf. Sie wurde zunächst ausdiskutiert und für nicht realisierbar gehalten. Einige wagten es doch (Nürnberger Linux Group); es wurde ein Datum gesetzt und man machte sich an die Arbeit. Nach einem Aufruf meldeten sich eine Menge Leute, von denen 120 ausgefiltert wurden, was nicht ganz einfach war. Es bildeten sich Arbeitsgruppen für Software, Hardware und Orga. Für das Projekt gab es einige Probleme: 1. Beschaffung der Hardware, was sich dank Sponsoren als nicht so schwierig erwies (siehe dazu auch die Cluster Sites) 2. Erstellung einer Distribution Es wurde ein Debian System verwendet welches aus eine Diskette paßt und sich via NFS installiert. Die Diskette enthält einen Kernel (2.0x) und alle Module für Netzkarten. Die Installation beschädigt nicht das vorhanden Datei/Betriebsystem, sondern benötigt nur 20Mbyte auf der Festplatte, bei genug RAM (>128Mbyte) ist auch eine RAMdisk möglich. 3. Software: Es gibt eigentlich keine freie Software, die das Cluster nutzt, ohne soviel Netztraffic zu verursachen, daß es sich lohnt. So wurde ein Lastverteiler geschrieben, der diese Aufgabe übernimmt. Als Anwendung kam der POV Raytracer zum Einsatz mit dem mehrere Filme erzeugt wurden (siehe den unten genannten ftp Server).

Die genau Plazierun unter den Top 500 Rechnern, eine Liste der leistungsfähigsten Großrechner der Welt, ist noch nicht ganz klar, liegt aber so um Platz 250, genaueres aber unter

Congress 27.-29.12.1998 in Berlin

http://www.top500.org/.

Für alle die sich, noch mehr mit Thema beschäftigen wollen siehe die unten ausgeführten Links:

http://www.linux-magazin.de/cluster/#links (www - Seiten zu dem Linux Cluster)
http://www.heise.de/ix/artikel/1999/01/010/

ftp://move.mediaways.net/pub/cluster/filme/ (verwendete Software sowie entstandene Filme) Eine komplette Liste zu dem Cluster ist noch im Aufbau
http://www.linux-cluster.org/

Die zur Zeit kompletteste Seite zum Cluster

http://www.linux-magazin.de/cluster/

andere Projekte die sich mit dem Thema beschäftigen:

http://cnls.lanl.gov/avalon/avalon_bell98/avalon_bell98.html

http://www.th.physik.uni-frankfurt.de/linux/

http://www.cond-mat.physik.uni-mainz.de/~benneman/Linux_Cluster.html

gute Zusammenfassung zu Cluster liefert:
http://www.xss.co.at/vortrag.html

Vortrag: Ernst Lehman, Florian Lohhoff <German@acheron.franken.de>

Bericht: Frank Stange <frank@wohnt.in-berlin.de>

Year 2000 Chaos

Nix genaues weiß man nicht. Wo liegt eigentlich das Problem im Y2k-Chaos (Y=year, 2=2, k=kilo ... also y2k=year 2000)?

Probleme tauchen hier dadurch auf, wenn z.B. Datenbanken sich selbst überschreiben, da in ihnen verwendete Felder mit Datumserweiterung gespeichert werden und also aus 31.12.99 (+1) dann ein 31.12.100 oder gar ein 31.13.99 wird. Desweiteren können sich langfristig relevante Daten in Bezug auf Geburtsdaten drastisch ändern. Die Problemlösungen werden Geld kosten und da praktisch alle Menschen betroffen sind (zumindest alle nicht 100%igen Alleinversorger), werden auch alle bezahlen müssen. Derzeit sind noch keine Kostenvorstellungen bekannt und es wird auch schwierig sein, den Umfang der Kosten zu erfassen. Offenbar basiert ein großer Teil eingesetzter Software (OS-unabhängig), bei Zeitraumbestimmung auf Datumsgestützen, betroffenen Standardroutinen, wodurch prinzipiell jeder Computer irgendwie betroffen ist. In Deutschland besitzt dieses Problem auf politischer Ebene offenbar wenig Relevanz. Laut BSI ist das Y2k-Problem "kein IT-Sicherheitsproblem", was nach einer Versuchsanordnung zum Test einer Y2k-Gefährdung eines Fahrzeugherstellers während seiner Betriebsferien eher zweifelhaft scheint. Bei diesem Test nämlich reagierte das Sicherheitssystem des Herstellers auf die nach Testbeginn sofort abgelaufenen Zugangs-Chipkarten, um ausnahmslos alle Beschäftigten auszuschließen und dann pflichtbewußt die Polizei zu verständigen. Die Firma benötigte 3 Wochen um den entstandenen Schaden zu beheben und seine Anlagen wieder hochzufahren.

In den USA sieht das ganze etwas anders aus, dort wird Aktiengesellschaften per Gesetz vorgeschrieben, den eigenen Y2k-Stand aktuell zu veröffentlichen.

Für weitere Infos sei hier verwiesen an: news: comp.riscs http://www.border.org, IX Dezember 1998 im Heise Verlag und Spiegel 43/98

Als Lösung des Problems wurde vom Workshop folgendes erarbeitet: - Techno-Verzicht - Börsenspekulation - dreiwöchige CCC-Party - Fragestellung, welches OS sollte nach dem Crash wieder hochgefahren werden?

Vortrag: Doobee R. Tzeck <doobee@ccc.de> drt.ailes.com Bericht: Jan Manuel Tosses <jan.manuel.tosses@topwave.de>

Sommer? Sonne? Fragezeichen?

Am Anfang stand eine kryptische Nachricht aus dem All. Die intergalaktische Kontaktgruppe des CCC empfing sie vor einiger Zeit und entschlüsselte sie als bald als Hilferuf des Raumschiffs „Herz Aus Gold“. Ein technisches Problem macht eine dringende Reparatur unter Gravitationsbedingungen nötig. Flugs wurde ein Termin vereinbart und im Sommer dieses Jahres erwarten wir die intergalaktische Crew des außergewöhnlichen Raumschiffes auf dem Planeten Erde.

Als Alternative zum dunklen Wintertermin zwischen Weihnachten und Neujahr lädt der Club in diesem Jahr zu einer Veranstaltung unter freiem Himmel: dem Chaos Communication Camp.

Alle Hacker sind eingeladen, sich an den Rekonstruktionsmaßnahmen zu beteiligen. Mit anderen Worten: Hackerzeltlager im Sonnenschein. In entspannter Atmosphäre bieten wir Strom und Internetanschluß für jedes Zelt, Raum für Workshops, ein Hackcenter, Themenzelte, Infrastruktur zum Überleben, einen See zum Baden und alle anderen Annehmlichkeiten, die ein Hacker in freier Wildbahn so braucht inclusive Essen und Getränken.

Inhaltlich wird das Camp von dezentraler Aktivität geprägt sein. Neben einem großen Hackcenter-Zelt werden kleinere Zelte bestimmte Themen fokussieren: Kryptographie, Free Software, Lockpicking, Chipkarten und Musik. Zwei Workshopzelte bieten Raum für Vorträge, Diskussionen und allgemeinen Diskurs.

Das Camp findet vom 6.–8. August 1999 auf einem Gelände in der Nähe von Berlin statt. Als Teilnehmerentgelt steht der Erwerb einer Freiwilligen-Karte (EUR 77, DEM 150 inkl. MwSt) oder ein Business/Government-Ticket (EUR 777, DEM 1500 zzgl. MwSt.) zur Auswahl. Letzteres kommt mit einer fein absetzbaren Rechnung daher.

Wir hoffen mit dem Preis einen guten Mittelweg zwischen der notwendigen Deckung der enormen Kosten einer solchen Veranstaltung und dem für einen dreitägigen Urlaub zumutbaren Entgelt gefunden zu haben. Weitere Details zum Platz, Anfahrt, Reservierungen usw. in bälde auf der Website.

Jede Form der Unterstützung ist willkommen. Wir können alles gebrauchen: Hardware, Personal, Frewillige zum Aufbau, Durchführung und Abbau der Veranstaltung sowie Spenden und/oder Leihstellungen von sonstigen Infrastruktur und alles, was Euch noch so einfällt.

Wir hoffen natürlich auf eine rege und kreative Teilnahme. Wer ein Projekt auf dem Camp realisieren möchte oder sonstige Fragen zur Unternehmung hat, sollte sich schleunigst mit der Orgacrew (crew@camp.ccc.de) in Verbindung setzen.

tim@ccc.de

Termine

Grober Terminkalender 1999

6.-8. August 1999 Chaos Communication Camp, siehe http://www.ccc.de/camp

27.-29. Dezember 1999 Chaos Communication Congress, siehe http://www.ccc.de/congress

31. Dezember 1999 derzeit noch unklar; zentrale oder dezentrale Beobachtung und Verarbeitung der y2k-probleme ? Weltuntergangsvernetzung ? Imanentisierung des Eschatons ? Flucht aufs Land ?

Meanwhile...

Chaos Bildungswerk Hamburg: Siehe http://www.hamburg.ccc.de/Workshops/index.html

Do, 06.05.1999 19.30 h Lambda, Continuations und Beweisbarkeit - Einführung i.d. Programmiersprache Scheme
Do, 13.05.1999 19.30 h TCP/IP
Do, 20.05.1999 19.30 h DNS, Nameserver, Domain Registration - Rechnernamen im Internet
Do, 27.05.1999 19.30 h Perl

Bestellungen, Mitgliedsanträge und Adreßänderungen bitte senden an:

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

Adreßänderungen auch per Mail an office@ccc.de

Der Mitgliedsfetzen

Mitgliedsanträge und Datenschleuderabonnement

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

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

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

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

Die Kohle liegt

o als Verrechnungsscheck
o in Briefmarken

bei bzw.

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

Ort/Datum
_____

Unterschrift
_____

Name
_____

Straße
_____

PLZ, Ort
_____

Tel/Fax
_____

Der Bestellfetzen

Literatur

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

Alte Datenschleudern

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

Sonstiges

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

+ DM 5,00 Portopauschale!

_____ Gesamtbetrag

Die Kohle liegt

o als Verrechnungsscheck (bevorzugt)
o in Briefmarken

bei bzw.

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

Name
_____