die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

Mautstelle burn!
RFID
Das Ende von UNIX
Softwarepatente
Sabbern für die Polizei
Camp Review!
INPOL neu

Watching them watching us

ISSN 0930-1054 • Erstes Quartal 2004
EUR 2,50 | IQD 0,77 | IRR 4.353 | KPW 5,40 | LYD 7,75
Postvertriebsstück C11301F

#82

Berlin, CCCB e.V.	Marienstr. 11, *(Briefe: CCCB, Postfach 640236, D-10048 Berlin)* >> Club Discordia Donnerstags zwischen 17 und 23 Uhr	*http://berlin.ccc.de/* *<mail@berlin.ccc.de>*
Bielefeld	im AJZ Buchladen Anschlag, Heeper Str. 132, Bielefeld Jeden Mittwoch (außer feiertags) ab 20 Uhr	*http://bielefeld.ccc.de/* *<info@lists.bielefeld.ccc.de>*
Düsseldorf, CCCD/ Chaosdorf e.V.	"Clubräume Fürstenwall 232" - >> dienstags ab 19 Uhr	*http://duesseldorf.ccc.de/* *mail@chaosdorf.de*
Erlangen/Nürnberg Fürth	"E-Werk", Fuchsenwiese 1, Gruppenraum 5 >> dienstags ab 19 Uhr	*http://erlangen.ccc.de/* *<mail@erlangen.ccc.de>*
Hamburg (die Dezentrale)	Lokstedter Weg 72 >> 2. bis 5. Dienstag im Monat ab etwa 20 Uhr	*http://hamburg.ccc.de/* *<mail@hamburg.ccc.de>*
Hannover, Leitstelle511	Kulturcafé, Schaufelder Str. 30, Hannover >> 2. Mittwoch im Monat ab 20 Uhr	*https://hannover.ccc.de/* *<kontakt@hannover.ccc.de>*
Karlsruhe, Entropia e.V.	Gewerbehof, Steinstraße 23, >> jeden Sonntag ab 19:30h	*http://www.entropia.de/* *<info@entropia.de>*
Kassel	Uni-Kassel, Wilhelmshöher Allee 71-73 (Ing.-Schule), Kassel >> 1. Mittwoch im Monat ab 17 Uhr	*http://kassel.ccc.de/*
Köln, Chaos Computer Club Cologne (C4) e.V.	Chaoslabor, Vogelsanger Str. 286, Köln >> Letzter Donnerstag im Monat ab 19:30 Uhr	*http://koeln.ccc.de/* *<mail@koeln.ccc.de>*
München, muCCC	Kellerräume in der Blutenburgstr. 17, München >> 2. Dienstag im Monat ab 19:30 Uhr	*http://www.muc.ccc.de/*
Ulm	Café Einstein an der Uni Ulm >> Jeden Montag ab 19:30 Uhr	*http://ulm.ccc.de/* *<mail@ulm.ccc.de>*
Wien Chaosnahe Gruppe Wien	Kaeuzchen, 1070 Wien, Gardegasse (Ecke Neustiftgasse) >> Alle zwei Wochen, Termine auf Webseite	*http://www.cngw.org/*

Chaos-Treffs

Aus Platzgründen können wir die Details aller Chaostreffs hier nicht abdrucken. Es gibt aber in den folgenden Städten Chaostreffs mit Detailinformationen unter http://www.ccc.de/regional/: Aachen, Bad Waldsee, Basel, Bochum, Darmstadt, Dortmund, Dresden, Emden, Frankfurt am Main, Freiburg im Breisgau, Gießen/Marburg, Hanau, Heidelberg, Kiel, Münster/ Osnabrück, Offenbach am Main, Regensburg, Ruhrpott (Bochum), Saarbrücken, Stuttgart, Trier, Weimar, Wuppertal.

Friends & Family

Zur näheren Chaosfamilie zählen wir (und sie sich) den/der Beinaheerfakreis Häcksen (*http://www.haecksen.org/*), den/der "Verein zur Förderung des öffentlichen bewegten und unbewegten Datenverkehrs e.V." - FoeBuD (*http://www.foebud.de/*), den Netladen e.V. in Gründung in Bonn (*http://netzladen.ccc.de*) und die C-Base Berlin (*http://www.c-base.org/*).

Die Datenschleuder Nr. 82

Zweites Quartal 2003 http://ds.ccc.de/

Herausgeber

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

Redaktion

(Artikel, Leserbriefe, Inhaltliches, etc.)
Redaktion Datenschleuder, Postfach 640236, D-10048 Berlin, Fon: +49.30.285.997.40, <ds@ccc.de>

Druck

Pinguindruck, Berlin; http://pinguindruck.de/

Layout, ViSdP und Produktion

Tom Lazar, <tom@tomster.org>

Redakteure dieser Ausgabe

Tom Lazar <tomster> und Dirk Engling <erdgeist>

Autoren dieser Ausgabe

Andreas Bogk, Chris, Cristian Yxen, Davide Del Vecchio, Fefe, Felix Kronlage, FrankRo, Hannes Mehnert, iPunkt, Markus Beckendahl, nitraM, Philip, Rüdiger Weiß, lisa&starbug, Unsere Regierung, Volker Birck

Eigentumsvorbehalt

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

Copyright

Liebe LeserInnen,

die Situation ist geprägt vom freien Lauf des Irrsins. Während die ungezügelten Kräfte der Marktwirtschaft die Entnahme von Genproben bei Neugeborenen fordern - aus gesundheitlichen Gründen versteht sich - und die Besatzungskräfte im Irak die Antwort auf "Iraqi Freedom" in Form von Selbstmordattentaten am laufenden Meter spüren, greifen Polizeibehörden nach den Verbindungsdaten der Telekommunikation inklusive der Forderung nach einer doch mindestens 2 jährigen Mindestspeicherungsdauer (siehe auch CRD, Seite 6).

Der Innenminister ist derweil bemüht, lustige Anekdoten in seinen schlaftablettenwirkenden Redeschwall einzuarbeiten um sein Desinteresse gegenüber dem Datenschutz dadurch auszudrücken, daß er bereits nach den ersten anderthalb Minuten der Amtseinführungsrede des neuen Bundesdatenschutzbeauftragten demonstrativ den Saal und die Veranstaltung verlässt.

Das die technischen Realitäten bei den Ermittlungsbehörden von knappen Budgets und den Zwang bei Ausschreibungen den günstigsten Anbieter zu wählen, zu so absurden Geschichten führt, wie die Auswahl von technischem Abhörequipment, das von den Geheimdiensten anderer Länder subventioniert wird, ist zwar bei den Bundesbehörden bekannt - aber das als Misstand zu bezeichnen wohl im Spiel der Kompetenzrangeleien zu riskant. Wie sonst lässt es sich erklären, daß die Polizei in der Bundeshauptstaat ein Anbieter von LI Krempel auswählt, der bereits in mehreren Ländern - z.B. Holland - wg. offensichtlicher geheimdienstlicher Verstrickung aufgeflogen ist?

Gibt es Lichtblick? Auch wenn die jetzige technische Betreiberkonstellation des Mautsystems gescheitert ist - die Masten über den Autobahnen sind vom Bund finanziert. Und die Kameras stehn da schon. Und der politische Willensbildungsprozess ist wohl noch nicht hinreichend entwickelt um eine umgehenden Rückbau der Installation zu beauftragten. Sprengen wäre ohnehin effektiver. Ein kurzer Abriss dazu auf Seite 10.

Auch an der Technikfront tut sich Epochales: Apple schreibt Windowssoftware, Microsoft wirft sich an die vorderste Front der "Open Source" Bewegung, Debian und Gentoo haben mit einer ganz eigenen Interpretation von "Shared Source" den FreeWare-Gedanken weitergesponnen und WideOpenBSD ist nun schon weiter 7 Minuten ohne Remote Exploit. Daß an Unix generell etwas stinkt, findet Andreas auf Seite 28.

"Die Vereinigten Staaten von Amerika" haben ihre Suche nach Rohstoffen auf Nachbarplaneten ausgeweitet. Und während ihr Raumschiff wenigstens sicher landete, sich dann jedoch wegen zuwenig Inodes auf der Festplatte verabschiedete [1], sucht die ESA noch.

Von der Lobbyfront gibt es erfreuliches zu berichten: die Bundesregierung hat einen Kriterien- und Präferenzenkatalog zu TCG verfasst, der sich in weiten Punkten mit den Forderungen des CCC deckt, ein Erstabdruck auf Seite 17.

Nochmal zurück zu unseren Strafverfolgungsbehö rden: Daß diese uns - naiv oder wissentlich - den Orwell machen, ist inzwischen eine Binsenweisheit. Wie weit die Phalanx reicht, läßt der, bereits erwähnte Bericht zu TollCollect erahnen. Der Versuch, Biometrie in Ausweisdokumenten zu verankern (Seite 26), engmaschige Datenbanken (INPOL-NEU Seite 34) und im Spezialfall Gendatenbanken aufzubauen (Seite 28), zeigt dann, wenn auch nur in Ausschnitten, in welche Richtung Beamte, die sich ihren Job auf unser aller Kosten zu vereinfachen suchen, die freiheitlich demokratische Grundordnung aus der Balance zu bringen versuchen.

Doch es wird immer scherer, die Menschen vom Verzicht der freiwilligen Aufgabe ihrer Freiheiten zu überzeugen, wenn diese fröhlich den scheinbar en vogue gewordenen Exhibitionismus ausleben (Seiten 9 und 38.) In diesem Sinne: es gibt viel zu tun. Und weil wir die letzen Monate davon reichlich hatten (die Seiten 47 bis 55 zeugen davon), müssen wir uns für die 6 monatige Verzögerung beim Erscheinen dieser - dafür umso dickeren Ausgabe - entschuldigen.

Das Chaos bei der Arbyte.

[1] http://news.bbc.co.uk/1/hi/sci/tech/3431617.stm

Inhaltsverzeichnis

Waubuch

Ich wundere mich etwas, dass auf ccc.de nicht ein Wort über das neu erschienene Buch zu Wau Holland ("Der Phrasenprüfer") geschrieben wird - warum ist das keine Erwähnung wert? *<philip@lunique.de>*

Tja, Wind haben ich zumindest schon lange davon bekommen. Selbst habe ich es noch nicht gelesen. Und es ist immer schwer zu entscheiden, welche Inhalte auf www.ccc.de sollen. Vielleicht setzt es noch jemand da drauf, vielleicht gibt es eine Erwaehnung in der Datenschleuder, vielleicht beides oder gar nichts Einfach mal abwarten. <Lars>

Hiermit zumindest schon einmal erwähnt worden. Vielleicht gibt es noch eine Rezension. <erdgeist>

Hallo CCC,

Ich muss für die Schule ein Referat über permanente Speicher machen.Ich kenne mich zwar ein wenig mit Pc´s aus, aber für das Referat ist das zu wenig.Deshalb wollte ich fragen ob ihr mir helfen könntet. *<paule-xxx@web.de>*

Nun, ein Referat macht man, damit man zeigen kann, dass man recherchieren kann...

Befeuere Google mit ein paar baruchbaren Stichworten, und Du wirst finden:

Permanente Speicher sind einerseits die klassischen, menschenlesbaren Speicher (von Höhlenmalereien über Keilschrift und Papyrus bis zu Papier und in gewissem Grade auch Lochstreifen und -karten), andererseits magnetische (Trommelspeicher, Magnetband, Kernspeicher=core memory, Festplatten und Disketten), elektronische (maskenprogrammierte ROMs, bipolare PROMs, EPROMs, Flash-PROMs und in weiterem Sinne auch GALs und PALs) und optische (CD-ROM, CD-R, CD-RW, DVD-xxx).

Also alle Speichermedien, deren Inhalt erhalten bleibt, auch wenn der Strom weg ist.

Interessant ist hier, dass die älteren Verfahren sich als sehr dauerhaft erwiesen haben. während die Lebensdauer modernerer Verfahren immer geringer wird.

Was von unseren modernen Medien wird auch nur in hundert Jahren noch lesbar sein, geschweige denn in Tausenden von Jahren? <Pirx>

Die Axt im Haus...

Ich hoffe ihr könnt mir weiter helfen. Keiner kann mir irgendwas über PGP erzählen. Ich habe es mir mal runtergeladen und installiert unter Windows XP.

PGP ist ein kommerzielles Produkt; mindestens der Hersteller kann Dir da weiterhelfen. Du findest sicher näheres auf der Website, von der Du PGP runtergeladen hast.

Ich kenne mich leider nicht so gut mit Verschlüsselung aus. Bei PGP kann man 3 verschiedene Verfahren aussuchen zum Verschlüsseln. Kann mir vielleicht einer von euch sagen, welche die beste Verschlüsselung ist von den 3. Das sind Diddie-Hellman/DSS, RSA und RSA Legacy. *<TheDaywalker1@xxx.de>*

GnuPG, ein freier PGP-Nachbau (siehe www.gnupg.org), hat den Vorteil, dass die Verschlüsselung zuverlässiger ist. PGP unterliegt wie allen amerikanischen Produkten den US Ausfuhrbestimmungen, und die legen fest, inwiefern absichtlich unsicheres eingebaut werden muss, damit die amerikanischen Geheimdienste im Zweifelsfalle mitlesen können.

Bei GnuPG würde ich Dir empfehlen, lieber DSA statt RSA o.ä. zu benutzen.

Es gibt gute Gründe, weshalb man patentierte Algorithmen nicht unterstützen möchte; einen Ausgangspunkt für eine Diskussion darüber findest Du hier:

http://www.attac.de/geig/mdep-brief.php

Bei sachgemäßer Verwendung von GnuPG mit DSA, SHA1 und AES oder Twofish sehe ich einen hohen Grad an Sicherheit. <VB.>

Eine andere Meinung zur Frage PGP vs. GPG:

Ich verwende auch und gerne GnuPG, aber die Panikmache bezüglich PGP kann ich nicht nachvollziehen. Der Sourcecode der meisten PGP-Versionen ist öffentlich, nie waren Hintertüren drin. Es kann viele Gründe geben die eine oder andere Version zu benutzen.

Einen Überblick über das Wirrwar gibt http://www.foebud.org/pgp/html/node29.html (leider etwas veraltet).

Das RSA Patent ist ausgelaufen und erst seit dem ist der Algorithmus auch in GnuPG mit drin. Ausserdem ist auch nicht ganz unumstritten, ob nicht bestimmte Patente prinzipiell alle Public-Key-Algorithmen betreffen.

Was ich als Nachteil an DSA sehe, ist dass die Schlüssellänge auf 1024 bit begrenzt ist. Auch wenn der dazugehörige El-Gamal-Key zum Verschlüsseln länger ist und DSA, bei gleicher Schlüssellänge, für sicherer als RSA gehalten wird, hab ich mit einem entsprechend langen RSA-Key das bessere Gefühl.

Allerdings sollte man sich nicht allzuviele Gedanken darüber machen, es lohnt sich nicht. Vielmehr sollte man lieber mal daran denken, inwieweit man seinem Betriebssystem oder auch seiner Hardware traut, den Secret-Key auch wirklich geheim zu halten.

Auch bei einem 1024 bit key ist es immer noch einfacher, bei dir einzubrechen und den key (oder gleich die unverschluesselten Infos) zu klauen, als einen kryptographischen Angriff auf den key zu fahren. <Jürgen>

Ein Fall für die FAQ...

Keine ahnung, ob ich bei Euch richtig bin, aber vielleicht könnt Ihr mir weiterhelfen. Ich habe eine Word Datei, auf der sich ca. 5 Jahre meines Tagebuchs befinden und ich habe das Passwort vergessen.

Könnt Ihr mir helfen, wie ich das Passwort wieder bekomme??? Das wäre super. *<Mr Mario xxx@yahoo.de>*

Hier gibts es mehrere Programme, die das bewerkstelligen:
http://www.google.de/search?q=word+password+recovery
<Sebastian>

Wie bleibe ich im Netz unerkannt ???

Also wie schaffe ich es, nicht nur 5 Min. lang einen Rechner im Netz zu Erforschen (was für Dienste darauf laufen wie Sie funktionieren usw.) ohne, dass gleich oder am nächsten Tag die Polizei klingelt. *„Blackxxx" <Martina xxx@web.de>*

http://koeln.ccc.de/artikel/hacker-werden.html
http://www.insecure.org/nmap/
http://www.google.de/ <Julius>

kurz drauf...

ho, danke!!! Aber ich wollte eigentlich wiesen wie sich die wenigen stützen vor zurück Verfolgung und beschlagnahmung ihrer Rechner wenn sie die Sachen und andere ausprobieren????

Sachen, die „ausprobieren", probieren wir üblicherweise auf unseren eigenen Rechnern aus. Gegen Beschlagnahme von Hardware durch die Staats- und Sicherheitsorgane hilft zumeist, keinen Grund für die Beschlagnahme zu liefern. <erdgeist>

Attacke!ıı!!ı!

da seinem namen um folgenden gefallen:ab 15. 3.d.J 23.00 uhr mez blockage aller zentrallen energieversorals ger wieich euch treue diener des großen bruders kenne bitte ich in z.B. kraftwewerke, energieverteilungssysteme (evu´s)? allein durch die drohende Attacke müssen sich die zusammenbruch aller abhängigen Systeme! falls Euch bbetreiber gezwungen sehen vom netz zugegen! Ziel ist dereessere Möglichekeiten zur chaotisierung des scheißsystems einfallen so nutzt diese konseqüent und vertrauensvooll. bis bAlt; *<anonym>*

Werd erwachsen! <padeluun>

Faszinierend hierbei ist, daß die Neo-Anarchos im Gegensatz zu ihren rhetorisch brillianten Originalen der späten ´68er Generation auffallend wenig Wert darauf legen, ihre Pamphlets prägnant zu gestalten. Konsequenz: Laßt euch nicht von diesem orthographisch-grammatikalischen Schweinesystem unterjochen!!! <erdgeist>

In die gleiche Kerbe schlägt wohl:

Ich "bewundere" immer auf einigen Homepages meine eigene ip adresse und würde gerne wissen, ob sich daran etwas ändern lässt.

Wenn dein Computer "direkt" mit dem Server kommuniziert, dann muss der Server natürlich die Koordinaten deines Computers, also die IP-Adresse, kennen. Sonst würdest du vom Server ja keine Antwortpakete bekommen können.

Ich würde gerne manchmal auch einfach anonym ins internet gehen aber ich habe das gefühl das ist unmöglich... ? oder ??? *<christianxxx@gmx.net>*

Es ist möglich, Proxies zu verwenden. Dann "sieht" der Server nicht mehr "deine" IP-Nummer sondern die des Proxies. Und wenn du es toll machen willst, dann nutzt du nen Anonymisierungs-Proxy, wie etwa
http://anon.inf.tu-dresden.de/ <Sascha>

Saugen bis zum Staatsanwalt...

guten tag, ich hätte eine frage. Wie wahrscheinlich ist es, dass nen Kumpel z.B. wegen illegalen Musik herunterladens (in Deutschland) von der Staatsanwaltschaft post bekommt ? *<oag_xxx@web.de> dennis*

Die Wahrscheinlichkeit liegt ungefaehr zwischen 0 und 23%.

Du kannst die Wahrscheinlichkeit aber durch eine gezielte Anzeige bei der Staatsanwaltschaft auf 100% erhoehen. <Julius>

Feedback zum TCG

hier also meine Fragen:

1. Wovor haben die Leute bei TCG wirklich Angst?

- DRM ?
- Kontrolle von Einflüße ?
- keine Musikdownloads und Movies mehr?

1.1. sind die Machenschaften der TCG moralisch vertretbar im Bezug auf die:

- Meinungsfreiheit?
- Datenschutz?
- Exekutiv Mechanismen (Haft für die Benutzung von Open Source)?
- Covert Chanels und Hintertürchen für Mister X?

2. Die wahren Beweggründe der TCG?

- Geld verdienen! Aber womit genau?
- Geschäftsmodelle? (Service die Dienstleistung der Zukunft?)
- neue Gesetze für eine neues Wirtschaftswachstum?
- Macht ergo Kontrolle?
- The American Dream? (Bill will das die Chinesen für seine Softs zahlen? häufig angeführtes Zitat)

3. Wie sehen zukünftige Zertifizierungsmechanismen aus?

4. Angst vor dem Polizeistaat?

Es wird sehr viel spekuliert, weniges ist jedoch mit Fakten belegen, das ist meine Aufgabe und auf den Dialog bin ich diesbezüglich angewiesen. *<yotom@xxx.de>*

Unsere Meinung kann ich nicht äussern. Ich kann Dir aber meine persönliche Meinung mitteilen. Ich denke mal, dass sich das mit der Meinung der Mehrzahl der CCCler deckt

Trusted Computing per se ist eine Technik, die ein Mehr an Sicherheit und Vertrauen bieten kann. In Unternehmensnetzwerken zum Beispiel ergeben sich da durchaus sinnvolle und wünschenswerte Anwendungen.

Wie viele andere moderne Technologien bietet Trusted Computing jedoch ein hohes Missbrauchspotential.

Zu nennen sind hier:
- *kartellrechtliche Implikationen*
- *datenschutzrechtliche Implikationen*
- *verbraucherschutzrechtliche Implikationen*
- *völkerrechtliche Implikationen (Souveraenität)*

Weiter ist es höchst problematisch, inwieweit Open-Source-Software mit Trusted Computing coexistieren kann.

Wie du siehst ist "Trusted Computing" an sich weder illegal noch legal. Es kommt auf den konkreten Umgang mit dieser Technologie an.

Hier muss man wachsam sein und die Entwicklungen sorgsam verfolgen. Ich weiss, dass Vertreter des Berliner CCC hier auch bei Anhörungen des Wirtschafsministeriums aktiv waren, wir sind also am Ball.

Fall Du Interesse hast, kannst Du Dir ja mal meine Folien durchlesen, die ich anlässlich eines (juristischen) Seminars an der Uni-München zu diesem Thema angefertigt habe:
http://engine.grin.de/julius/tcpa.tar.gz <Julius>

Ansonsten sind natürlich auch eure Meinungen gefragt. <ds@ccc.de>

Und dann war da noch...

Hallo könnt ihr mir sagen wie ich einen channel bekomem also ein IRC channel dem jemand anders gehört. Ich weis so könnte ja jetzt jeder kommen aber es geht um sex ich bekommen viel leicht sex und das müsste ich noch wissen eindlich müsste es auch nur ein mal gehen ich breuchte nur einen channel dem jemand ander ist.

sorry wegen der Rechtschreibung aber ihc habe Legastenie *<127.0.0.1@xxx.ru>*

Wer tagtäglich mit Nerds zu tun hat, ist ja nun schon einiges gewohnt. Aber diese Mail hat auch gestandene Freiwillige auf mail@ccc.de fassungslos gemacht.

Wir haben lange überlegt, ob da nicht vielleicht jemand einfach nur in die Datenschleuder möchte. Wenn ja: gratuliere, du hast es damit geschafft, wenn nicht, hätten wir die Mail vielleicht doch an drsommer@bravo.de weiterleiten sollen. <erdgeist>

Autoaggression...?

wer kann helfen. Seit etwa 13.8.03 erhalte ich ständig Angreiffe/Eingriffe von den IP-Nrn. 192.168.100.1, 192.168.100.11, oder auch 192.168.100.13 und 169.254.129.130. Wer sind diese? Sicherlich eine Instution, kein Einzelner.

Ja, deine eigene Institution. Denn die „Angriffe" kommen aus deinem Netz. 192.168. sind immer lokal Adressen.*

Habe Windows XP, Norton Internet Security. [längere protokolle]*<holistic@xxx.de>*

Oje. Das wird wohl eher deine Problem sein als ein Angriff. Du bekommst einen Haufen Meldungen serviert, die du allesamt nicht verstehst. Viele Leute, so auch ich, zweifeln nicht nur deshalb grundsätzlich am Sinn von „Personal Firewalls". Lies mal
http://www.iks-jena.de/mitarb/lutz/usenet/Firewall.html#PF
<VB.>

Wollte mal wissen:)

Hi habe eben RTL2 gegafft und hab euer dolles camp gesehen n1 one naja da hab ich mich gefragt wer sponsort so ein treff und wozu gibt es den CCC club ??? Ach ja und gibt es bei euch wirklich Sponsoren?

Die gibt es durchaus (Firmen die zum Beispiel ihre Produkte einem Belastungstest unterziehen wollen , ansonsten zahlt ja jeder Besucher seinen Beitrag. Die Ziele des Clubs selbst kannst Du am besten unter https://www.ccc.de/ nachlesen.

Ach ja und gibt es bei euch wirklich Frauen die hacken wollen?? *<Acidmannksky@xxx.de>*

Ja, sicher, gibt es. Ich sehe das als nichts Besonderes an... <Hanno>

Endlich Ausgesperrt...

Bin mit einem Domainen kennwort angemeldet und habe auf meinen Rechner das Administratorpasswort vergessen bzw verschlammpt! Habe ein Win2000 ohne SP! <hintereingang@xxx.at>

Da Windows ein kommerzielles Produkt ist, für das du sicher viel zahlen musstest, wende dich doch einfach an den Hersteller, der wird es am besten wissen. Von uns benutzten nur sehr wenige Windows, so dass sich die meisten wohl eh nicht damit auskennen. <Enno>

Kryptoexperten

[PGP verschlüsseltes Zeug.] *<frank.xxx@gmx.de>*

Der Trick bei PGP ist, dass der Empfänger die Nachricht mit seinem Schlüssel decrypten kann.

Wenn nur du dir einen Schlüssel ausdenkst, den wir nicht haben, können wir die Nachricht folgerichtig auch nicht lesen.

Wenns wirklich wichtig ist und sicher sein soll, dann schreib an ds@ccc.de und benutze den Key

ID:	*0xCA45BA04*
Fingerprint:	*03C9 70E9 AE5C 8BA7 42DD C66F 1B1E 296C CA45 BA04*

Der alte Key expired im Mai. Benutzt bitte schon mal den Neuen. <erdgeist>

Digitales Fernsehen

diese anfrage richtet sich in erster linie an leute die in berlin und brandenburg wohnen und auch mit dem dvb-t problem zu tun haben. gibt es inzwischen eine möglichkeit den decoder zu sparen und meine alte tv karte fit zu machen für die neue digitale verschlüsselung über antenne? *<jan.xxx@gmx.de>*

DVB-T ist nicht in erster Linie ein 'Problem' sondern eine technische Weiterentwicklung des Fernsehens. Die Programme sind auch nicht 'verschlüsselt' sondern nach dem MPEG-2-Standard kodiert und werden, anders als das bisherige Fernsehen jetzt, mittels COFDM-Modulation übertragen. Deswegen brauchst du auch spezielle Emfpangsgeräte, welche ab ca. 100 Euro im Handel erhältlich sind. Mehr Infos gibts auf

http://www.ueberall-tv.de/ (erfordert leider Flash) *<frank>*

Kennzeichen

Hallo! Habt ihr eigentlich Zugriff auf die PCs von der Polizei?

Wunderschönen guten Tag (Herr Wachtmeister?) Auch wenn ich traurig feststellen muss, dass ich bei der aktuellen Flut von Trojanern und Würmen für die einschlägigen Betriebssysteme wohl der Einzige bin, der _KEINEN_ Zugriff auf die Rechner der Polizei hat, find ich die Vorstellung faszinierend, ernsthaft anzunehmen, der CCC würde dir davon per email beichten.

Ich müsste nämlich dringend den Besitzer eines Autos herrausfinden, doch ich habe nur das Kennzeichen!

Wenn du wichtige Gründe fuer die Feststellung der Identität eines Halters eines Kfz hast (Unfall/Zeuge/Beobachtete Straftat), gibt die Kfz-Zulassungsbehörde/Polizei Informationen über diesen heraus.

Ansonsten stehen deine Karten eher schlecht. Vielleicht kannst du ja an die Person auch auf anderen Wegen als der Zulassungsnummer herankommen. <erdgeist>

wenig später...

Also wenn ihr mir nicht helfen könnt, versuche ich es selber herrauszufinden. (wie auch immer ich das schaffen soll)

Vielleicht lerne ich noch ein bisschen unhd trette dann einer Hackergruppe bei!) Ich bin zwar nicht auf den neusten Stand, aber ich werde schon eine finden, die sich mit sowas beschäfigt. *<RecognizesSW>*

Unser Beichtstuhl IRC #CCC

```
20:46 -!- ThoBoy [~jan@IPADDR] has joined #ccc
20:47 < ThoBoy > ich habe stress mit meinem kumpel, wir waren zusammen chaoscamp! Er will mich jetz bei euch anschwärzen das ich ein paar Toiletten zugeschissen und verstopft habe!! Aber als wir ans große Zelt gepisst haben, waren mehrere dabei, nicht nur ich! Ich hoffe ich schaff das damit aus der Welt, sorry kommt nicht mehr vor, beim nächsten Camp benehmen wir uns! wenn er was labbert, vergesst es einfach
20:47 -!- ThoBoy [~jan@IPADDRR] has left #ccc (cu)
```

NIX is verjessen.. Zwei Tage mussten wir schrubben, bis die Sauerei weg war... Warte Bürschchen! <erdgeist>

NGO Positionspapier zu RFID

Angesichts erster Feldversuche haben ca. 30 internationale Verbraucherschutz- und Bürgerrechtsorganisationen ein gemeinsames Positionspapier erarbeitet und an die Medien verteilt.

Deutsche Version beim foebud:

http://www.foebud.org/texte/aktion/rfid/positionspapier.html

englisch:

http://www.privacyrights.org/ar/RFIDposition.htm

Studie zu pervasive Computing / RFID und anderem Schrott

Das Institut für Zukunftsstudien und Technologiebewertung hat im Auftrag des Zentrum für Technikfolgen-Abschätzung der Schweiz eine Studie zum Einzug von nicht-sichtbaren Computern / embedded Systems, RFID und anderen formen des pervasive Computing erstellt.

Das eher umfangreiche Werk gibt es auch in einer Kurzfassung unter

http://www.izt.de/projekte/laufende_projekte/pervasive_computing_-_gesundheit_und_umwelt.html

Regierung von Malaysia setzt auf Open Source

Als eine der ersten islamischen Länder hat sich die Regierung von Malaysia klar zu Open Source Software bekannt. Sowohl Amar Leo Moggie, Minister für Energie, Kommunikation und Multimedia als auch Premierminister Mahathir Mohamad lege persönlich Wert auf die Entwicklung und Anwendung von Open Source-Software.

Dabei wird der Einsatz propiäterer Software regierungsseitig zwar noch nicht sanktioniert, aber immerhin schonmal verurteilt: „Um bessere Software für morgen zu entwickeln, müssen wir genau verstehen, wie die Software von heute funktioniert. Doch wir sind nur Anwender dieser Software, Käufer von Produkten anderer Leute." (Moggie)

http://www.heise.de/newsticker/data/uh-30.08.03-003/

Call-Center in Gefängnissen

Nach bislang nicht verifizierten Eingaben werden bei der US-Fluggesellschaft TWA die Call-Center in verschiedenen US Gefängnissen mit entsprechenden Insassen als Mitarbeitern betrieben. Falls jemand dazu eine Quelle findet, möge er sie doch mal an *crd@ccc.de* mailen.

GSM Luftschnittstelleninterception

Üblicherweise gut unterrichtete Quellen berichten, daß die Grenzkontrollcounter verschiedener Länder bei der Einreise GSM Funkzellentechnik enthalten.

Das diesgehörige Konzept besteht darin, eine Störung zwischen GSM Mobiltelefon und normaler Funkzelle zu erzeugen und eine Neueinbuchung in die eigene Funkzelle (IMSI-Catcher Konzept) zu verursachen um dann im Kontext einer adäquaten Verzögerung bei den Einreiseformalitäten nicht nur Namen und Reisepassnummer sondern auch IMSI und IMEI in einem Datensatz zur Erleichterung weiterfolgender Maßnahmen zu betreiben. Auch in einzelnden Bereichen von Kreditinstituten seien derartige Anlagen installiert worden.

Wer also nicht gleich seinen vollständigen Datensatz bei der Einreise abgeben möchte, schaltet sein Telefon vielleicht besser erst nach Verlassen des Flughafengeländes an..

Überwachungsstaatsindikator I: Zugriff auf "relevante" Dateien

Der Bundesrat hat einen Gesetzentwurf (14/1492) zur effektiveren Nutzung von Dateien im Bereich der Staatsanwaltschaften erarbeitet. Die Länderkammer möchte die rechtlichen Hindernisse, die einem Online-Lesezugriff der Staatsanwaltschaft auf für sie relevante Dateien entgegenstehen, beseitigen.

Dabei geht es vor allem um das bereits vorhandene zentrale staatsanwaltschaftliche Verfahrensregister, zu dem uns leider keine URL vorliegt.

Überwachungsstaatsindikator II: Verbindungs- / Verkehrsdatenspeicherung

Am Beispiel eines großen deutschen Internet-Providers lässt sich darstellen, welche gravierenden Veränderungen durch die derzeitigen Gelüste der Strafverfolgungsbehörden im Bezug auf die Speicherung von Verbindungs- und Verkehrsdatenspeicherung bevorsteht. Gespeichert werden mittlerweile nicht nur abrechnungsrelevante Zuordnungen von Teilnehmerkennungen und dynamischen IP-Nummern, sondern auch abrechnungsirrelevante, d.h. die Verbindungen von Flatrate-Kunden. Diese Speicherung findet derzeit allerdings nur in einem Zeitraum von 80 Tagen statt.

Das liegt historisch in der Teledienst-Datenschutzverordnung (TDSV) begründet, und die Tatsache, daß es hier eigentlich zumindest bei den abrechnungsirrelevanten Datenspeicherungen offensichtlich keine Orientierung am Datenvermeidungsgebot gibt, rechtfertigt man mit der "Nachweismöglichkeit der Leistungserbringung".

Anders liegt das bei einigen Unternehmen, deren technische und organisatorische Konstruktion so liegt, daß

Quelle: http://www.spiegel.de/unispiegel/wunderbar/0,1518,286628,00.html

sie die POPs nicht selbst betreiben, sondern andere Unternehmen dass für sie tun. Diese erbringen recht eindeutig Telekommunikationsdienstleistungen für andere geschäftliche und fallen somit unter das TKG, das heißt: 180 Tage

Speicherung und völlig nonchalante Datenweitergabe.

Die jeweilige Zuordnung von Teilnehmerkennung (will sagen: in der Regel PPP Identifikationsparameter) zum Datensatz (Name, Anschrift, etc) des Nutzers erfolgt dann nach den Bestandsdatenbanken die nach TKG 89 bzw. der entsprechenden TDG Regelung.

Soweit, so schlecht.

Was die Strafverfolgungsbehörden jetzt gerne hätten ist eine Speicherung dieser Verbindungs- bzw. Verkehrsdaten in einem Zeitraum von 12 Monaten. Damit, müsste man meinen, ist die Umkehr der Unschuldsvermutung, zumindest für so suspekte Elemente wie Internetnutzer, staatlicherseits dann hinreichend dokumentiert.

Telefonieren gefährlich III: Stundenlange Verklemmung mit Finger im Münztelefon

Ein 46 jähriger Amerikaner ist über drei Stunden mit dem Finger in einem Münztelefon hängen geblieben, nachdem er ein 50-Cent-Stück aus dem Geldrückgabeschacht fischen wollte und dabei seinen rechten Mittelfinger eingeklemmte.

Nachdem weder Sanitäter noch einer Techniker der Telefongesellschaft helfen konnte, wurde das Telefon aus der Halterung herausgeschnitten und zusammen mit dem Mann in ein Krankenhaus gebracht, wo der Finger schließlich befreit wurde.

Bilanz: Telefon nicht mehr Funktionsfähig, Finger wohlschon.

Quelle: The Belleville News-Democrat

Initiative Nachrichtenaufklärung- Liste der am meisten vernachlässigten Nachrichten und Themen 2003:

Die Initiative Nachrichtenaufklärung und das Netzwerk Recherche haben am 7. Februar 2004 die Top Ten der vernachlässigten Themen 2003 vorgelegt:

1. Korruption: Deutsche Unternehmen schmieren im Ausland

2. Europa entscheidet - Machtverschiebung nach Brüssel

3. Mangelnde Hochwassersicherheit von Chemieanlagen

4. Greenwash: Unternehmen und ihr ökologischer Deckmantel

5. Auslandsgeschäfte mit Giften und Pestiziden: die Doppelstandards der Industrie

6. Abgestufte UN-Resolutionen

7. Sozialhilfeempfänger: Unbekannte Chancen für Selbstständigkeit

8. Das verschwundene Stasi-Vermögen

9. Leistungen für Asylbewerber weit unter Sozialhilfeniveau

10. Fehlende Rechte von US-Besatzungskindern

Mehr unter *http://www.nachrichtenaufklaerung.de/*

Passagierdatenübermittlung: SWISS wiedersteht?!

Die Schweizer Fluggesellschaft SWISS hat nach Verhandlungen mit den US Behörden zumindest einen Aufschub erwirkt und übermittelt die Daten Ihrer USreisenden Passagiere im Gegensatz zu den europäischen Fluggesellschaften nicht:

http://www.blick.ch/PB2G/PB2GA/pb2ga.htm?snr=62953

DIGITAL-TV Policy

Martin Springer schreibt gerade an verschiedenen Policy Dokumenten für digitales Fernsehen; als Diskussionsgrundlage und zum mitmachen unter:

http://www.chiariglione.org/contrib/

US-Flugverbotslisten und die Sinnfrage:

Bin Laden nicht vom Flugverbot erfasst

Amerikanische Journalisten des Insight Magazines fragten sich nach dem Sinn des vom amerikanischen Homeland Security Ministeriums eingeführter Datenbank für die Teroristenfilterung vor dem Einstieg in ein Flugzeug (CAPS -> Computer-Assisted Passenger Screening). Als sich bei einem Test herausstellte, daß sowohl Osama Bin Laden als auch andere Top-Terroristen vom System für das Boarding durchgewunken wurde, ging es wohl nicht mehr deutlicher; eine offizielle Erklärung dafür gab es indes nicht.

Nachzulesen unter:

http://www.wnd.com/news/article.asp?ARTICLE_ID=37167

Merkwürdigkeiten bei einem Internet Wurm

Einer Webhoster, dessen URL jüngst als aufgerufene Adresse eines Internet Wurms (der sich mal wieder an Microsoft Systemen verging) die Verbreitung verfolgen konnte, berichtete merkwürdiges. Dass die Standorte der ersten Systeme eine sehr ordentliche Verteilung aufzeigte war noch nicht das erstaunlichste: Russland, Polen, Israel, Kroatien, Südkorea, Schweden (in dieser Reihenfolge).

Das die ersten 100 Systeme dabei die Verbreitung durch http-Aufrufe innerhalb von 2 Sekunden anzeigte, begründete Anfangs noch einen Verdacht auf verdiente Anerkennung.

Als allerdings bereits nach den ersten 2 Minuten sich ein namhafter AntiViren-Hersteller per E-Mail meldete und nach den Logfiles erkundigte, erschien die Geschichte dann allerdings noch in einem anderen Licht - abgesehen davon, daß die Herausgabe von Logfiles nach Datenschutzgesetzen selbstverständlich nicht statthaft ist ist es ja doch interessant wie nah Antiviren-Hersteller am Ort des Geschehens sind..

Quelle: < möchte nicht genannt werden >

Metro Future Store RFID Update

Nach Redaktionsschluss erreichte uns noch die Meldung, daß zumindest Teilforderungen des FoeBuD (siehe auch Seite 31) erfüllt wurden.

Sämtliche („ca. 10.000“) mit einem RFID ausgestatteten Kundenkarten werden laut eines Fax der Metro Group „in den nächsten Wochen umgetauscht“.

Die Tatsache, daß die an den Waren befestigten RFIDs bei Verlassen des Feature Store nicht vernichtet werden und somit den Inhalt des Einkaufswagens auch außerhalb des Geschäfts mitteilen, einer der weiteren Hauptkritikpunkte, wurde bis dato noch nicht abgestellt.

NOrkut

von Cristian Yxen <cryx@berlin.ccc.de>

Sollen die doch alle ihre daten da in den wind blasen, ich finds nur scheisse, dass sie _meine_ Daten da [1] auch reinblasen ohne mich zu fragen.

Tragen mich mit vollem Namen und zugehöriger email-addr. ein, zum inviten! Wenigstens nicht noch mit allen anderen daten, das geht ja wohl auch. Was ist denn bitte aus "öffentliche daten nuetzen, private daten schuetzen" geworden wenn da meine privaten daten ohne meine zustimmung verschenkt werden??

Und um das dann zu rechtfertigen, faseln sie was von web of trust, wo man ja genau gesehen hat das das bullshit ist. Jeder kann da einen account anlegen der echt aussieht und es gibt nirgends eine moeglichkeit jemanden _wirklich_ zu identifizieren! Glaubwuerdig wird man im system ueber die freunde und wenn die dem faelscher auf den leim gehen ists vorbei, noch schoener, sobald man jemanden als freund anerkannt hat sieht derjenige alle daten.. adresse, telefonnummer, sexuelle vorlieben. Alles was man eingetragen hat.

Oder sie rechtfertigen sich mit sowas wie "das ist semantisches web" Das ist ja wohl auch bullshit! Da gibt es ja garkeinen content ausser den daten der anderen und deren sexvorlieben! Da kann nichts semantisch verknuepft werden ausser die freundesbeziehungen und nichtmal die sind was wert weil alle nur die ganze zeit versuchen freunde zu scoren um moeglichst viele zu haben und schoen viele sympathie punkte zu kriegen.

Und wenn man nicht mitspielen will weil einem etwas an seinen daten liegt, dann meinen sie "ja pgp keyrings, da kann man ja auch beziehungsbaeume rauslutschen" ja klar kann man das, aber da hat es sinn und ist vor allem teil des nutzens damit man hinterher _wirklich_ jemanden identitzieren kann um mit ihm verschluesselt kommunizieren zu koennen! Welchen sinn hat bitte, dass Karl Arsch sieht, dass ich Hans Wurst kenne?!

Zu allem ueberfluss faseln sie einen auch noch doof an wenn man nicht mitmacht und machen ihre witze ueber leute die "datenschutz" fuer sinnvoll halten, muss man sich mal vorstellen, im chaos computer club! Wau wuerd sich im grabe umdrehen! Und jetzt setzen die sich auch noch in eine radiosendung hoerte ich, wo sie drei stunden darueber sinnieren wie toll das alles sei!

Vielleicht sollten sie sich bei der gelegenheit mal fragen was eigentlich die intention hinter orkut genau ist, angeblich wars ein google-mitarbeiter mit zuviel zeit, aber was bitte sollen dann diese terms of service? Warum sollte jemand in seinem privaten spielzeug dinge verlangen wie, alle rechte der eingekippten daten gehen an die systembetreiber?!

Alles im allem finde ich, es ist weder web of trust, noch semantisches foo, noch macht es orkut gut wenn andere systemel auch ihre schwaechen haben! Orkut tut vor allem eines, es sammelt daten und niemand weiss wo diese bleiben. Nicht das das nicht schon schlimm genug ist, viel schlimmer ist, das gerade alle wie wild dabei sind darauf rumzuklicken, sich mit allen daten einzutragen und sich dabei toll vor zu kommen als ob ihnen jemand das hirn gebrutzelt haette!

Nein danke, ich nicht. NOrkut!

[1] http://www.orkut.com

Mit TollCollect weiter in den Überwachungsstaat?

von Frank <frank@rosengart.de>

Die Autobahn-Maut für Lastkraftwagen (LKW) hat ein breites politisches Diskussionsfeld eröffnet: Die Frage des Schadenersatzes für die Einnahmeausfälle ist noch ungeklärt, und Bundesverkehrsminister und Betreiberfirma können keinen verbindlichen Starttermin nennen. Der wegen technischer Probleme verzögerte Beginn der Gebührenerhebung reißt ein erhebliches Loch in den Bundeshaushalt, in dem die Einnahmen schon verplant waren. Die Themen Datenschutz und Überwachung bei der Lkw-Maut spielen in der Medienaufmerksamkeit demgegenüber nur eine Nebenrolle.

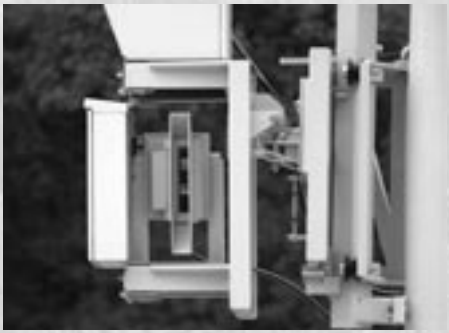
Das Mautsystem wird im Auftrag des Bundesministeriums für Verkehr von der TollCollect GmbH errichtet, einem Konsortium aus T-Systems (entstanden aus der Fusion der Telekom AG und Debis) und dem privaten französischen Autobahn-Betreiber Cofiroute.

Im Autobahnmautgesetz (ABMG) wurde die Erhebung der Maut geregelt. Möglichst alle deutschen LKW sollen mit einem Fahrzeuggerät, der sogenannten On-Board-Unit (OBU), ausgestattet werden. In einer Werkstatt wird das Gerät etwa in der Grösse eines Autoradios an die Fahrzeugelektronik angeschlossen. Verbunden wird das System zudem mit einem Geschwindigkeits- und einem Infrarotsender sowie mit je einer Antenne für die satellitengestützte Navigation über GPS (Global Positioning System) und den Kontakt zum GSM-Mobilfunk.

Die On-Board-Unit gleicht ständig die aktuellen GPS-Koordinaten des Fahrzeuges mit einer im Gerät gespeicherten Straßenkarte von Deutschland ab. Wird erkannt, dass der Lkw auf eine mautpflichtige Autobahn aufgefahren ist, beginnt der Gebührenzähler zu laufen. Anhand der aktuellen GPS-Parameter und dem Tachosignal wird die Plausibilität der gemessenen Werte überprüft. Verlässt der Lkw die mautpflichtige Strecke, wird per Kurzmitteilung (SMS) eine Mitteilung mit der errechneten Maut an die TollCollect-Zentrale geschickt, die diese Daten sammelt und der Spedition in Rechnung stellt.

Fahrzeugerfassung an 300 Kontrollbrücken

Um kontrollieren zu können, ob im Fahrzeug wirklich eine OBU mit laufendem Gebührenzähler ist, haben die Betreiber 300 Kontrollstellen auf deutschen Autobahnbrücken errichtet. Bewegt sich ein Fahrzeug auf die Kontrollbrücke zu, wird es per Infrarot-Signal auf-



gefordert, sich zu identifizieren. Wenn die Kommunikation per Infrarot ergibt, dass die OBU eingeschaltet ist und Gebühren berechnet, passiert nichts weiter. Erhält die Kontrollbrücke keine zufriedenstellende Rückmeldung, nimmt eine Kamera ein Bild vom LKW auf und versucht per Schrifterkennung, das Kennzeichen zu identifizieren. Bei der Durchfahrt durch die Brücke wird mittels Laser parallel vermessen, ob das Fahrzeug anhand seines Umrisses einer mautpflichtigen Kategorie zugeordnet werden kann.

Vor allem ausländische Transportunternehmen sollen die Möglichkeit erhalten, statt mittels der OBU über Internet oder an Bezahl-Terminals an Tankstellen die Lkw-Maut zu entrichten. Dabei muss für den betreffenden Lkw die Fahrtroute fest gebucht werden. Wenn ein Fahrzeug nun unter einer Kontrollbrücke durchfährt und sich nicht per Infrarot als unschuldig melden kann, wird das erkannte Autokennzeichen mit der Datenbank der manuell eingebuchten Fahrtrouten verglichen. Kommt auch dort kein Treffer zustande, wird das aufgenommene Foto als Beweismittel gespeichert und ein entsprechender Bußgeldbescheid zugestellt.

Das System ist so kompliziert wie es klingt. Aus Gründen der Datenvermeidung sollte laut der ursprünglichen Ausschreibung zunächst das Fahrzeug vermessen werden, um die Mautpflicht festzustellen, und es erst danach identifiziert werden. Nun wird jedoch jedes Fahrzeug bildlich festgehalten und dann im Nachhinein entschieden, was mit dem Foto passiert. Im Regelbetrieb soll das Foto nach der Auswertung umgehend gelöscht werden.

Heute Maut, morgen komplette Verkehrsüberwachung?

Der Hersteller betont aber, dass das System technisch in der Lage ist, den gesamten Verkehr zu überwachen und selbst verschmutzte Kennzeichen keine Hürde darstellen, denn die Mautkontrollbrücken sind mit speziellen Hochgeschwindigkeitskameras und Infrarotblitzgeräten ausgestattet. Seit dem Start des Probebetriebes im September 2003 fragt TollCollect täglich die Halterdaten von bis zu 80.000 Fahrzeugen beim Kraftfahrzeugbundesamt ab, weil diese Fahrzeuge als Mautpreller erkannt worden sind: Die OBU hatte sich bei der Brücke nicht zurückgemeldet. Kein Wunder, denn nur wenige LKW sind bisher mit einer funktionierenden On-Board-Unit ausgestattet.

Eine automatische Kennzeichen-Erfassung wurde bereits in Bayern an der tschechischen Grenze erfolgreich getestet. Auch die Polizei in Thüringen hat ein solches System ohne Rechtsgrundlage im Probebetrieb gehabt. Erst nach massiver Kritik und Intervention durch den Datenschutzbeauftragten des Landes wurden die dabei erhobenen Daten gelöscht. Die Innenminister weiterer Länder beraten bereits über eine routinemäßige Kennzeichenerfassung auf den Straßen.

Noch offen: Wer erhält Zugriff auf die Mautdaten?

Nach dem Autobahnmautgesetz dürfen Ort und Zeit der mautpflichtigen Bundesautobahnnutzung für bis zu vier Jahre gespeichert werden. Die im Mautgesetz vorgesehene Zweckbindung der Daten wurde bereits wenige Tage nach dem Start des Probebetriebs in Frage gestellt: Die Staatsanwaltschaft Gummersbach hatte beim Amtsgericht einen Antrag auf Herausgabe von Mautdaten gestellt. Die Frage, ob die Zweckbindung der Datenerfassung vor den Bedürfnissen der Sicherheitsbehörden Bestand hat, ist derzeit noch ungeklärt.

Die zur GSM-Kommunikation eingesetzten SIM-Karten können Kurzmitteilungen auch von außerhalb des Systems empfangen. Wenn die Sicherheitsbehörden mit Hilfe einer Anordnung auf Herausgabe von Daten die Rufnummer einer OBU erlangt haben, kann das Fahrzeug über eine "stille SMS" quasi angepeilt werden. Diese spezielle Form der Kurzmitteilung, bei der für den Betroffenen unbemerkt eine Verbindung zu seinem Mobiltelefon aufgebaut wird, ist äußerst umstritten, wird aber unter anderem von der Berliner Polizei zu Fahndungszwecken genutzt.

Im Rahmen der Recherchen zum BigBrotherAward 2002 wurde deutlich, dass die zuständigen Ministerien und die Betreiberfirma keine öffentliche Diskussion über diese technischen Details wünschen.

Auch wenn es sich bei den anfallenden Daten nicht primär um personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes handelt, wird doch jeder Lkw von einem Menschen gelenkt, dessen Route damit nachvollziehbar wird. Der zunehmende Trend zu scheinselbstständigen Speditionsunternehmern, die als Ein-Mann-Firma ihren Lkw steuern, und der in EU-Kreisen geäußerte Wunsch nach einer Straßengebühr für PKW lassen erahnen, in welchem Umfang Menschen in Zukunft von einer solchen Technik betroffen sein werden.

T* Computing - Big Brothers are watching You.

von Ruediger Weis <ruedi@cs.cu.nl>

Das über 200 Mitglieder zählenden TCPA Konsortium (beziehungsweise die "Nachfolgeorganisation" TCG) und Microsoft planen mit einem Aufwand von mehreren hundert Millionen Euro die grundlegenste Änderung der IT Infrastruktur seit der Einführung des Personal Computers. Nach eingehender Analyse erscheinen die oft nur bruchstückhaft vorliegenden Industrievorschläge keine signifikante Erhöhung der Sicherheit für die Benutzer, sondern vielmehr eher dem Schutz von Dienstanbietern vor dem Benutzer dienen. Dies könnte faktisch zur teilweisen Enteignung der bisher persönlichen Computer zu führen.

1. Technische Übersicht

Da sich die zum grossen Teil nicht frei zugänglichen Entwürfe ständig ändern und oftmals sogar widersprüchliche Detailangaben existieren, gehen wir im Folgenden schwerpunktmässig auf fundamentale Eigenschaften ein. Für eine umfassendere Betrachtung insbesondere der kartellrechtlichen Implikationen sei auf die aktuellen Arbeiten von Anderson [And03] (unter anderem mit einer überarbeiteten FAQ, Stand August 2003) und Koenig [Koe3] verwiesen.

1.1 Verwirrt?

Allein der ständige Namenswechsel, Änderungen in der Organistionsform und die fehlende öffentliche Kontrolle lässt zwar das Herz eines jeden Verschwörungstheoretiker höher schlagen, macht aber auch wissenschaftliche Analysen zu einer oftmals recht nervigen Angelegenheit. Sogar zu zentralen Fragen, wie welche Schlüssel im zentralen Hardwarebaustein gespeichert werden sollen, finden sich zum Teil erhebliche Widersprüche selbst innerhalb ein und desselben Unternehmens.

Die Trusted Computing Platform Alliance (TCPA) [TCPA03] wurde 1999 von Intel, Microsoft, HP, Compaq und IBM gegründet. Im Februar 2002 wurde die TCPA Main Specification v. 1.1b veröffentlicht.

Im April 2003 gründeten AMD, HP, IBM, Intel und Microsoft die Trusted Computing Group (TCG) [TCG03]. Im Gegensatz zur TCPA verfügt die TCG über eine straffe Organisation mit stark unterschiedlichen Mitwirkungsrechten der beteiligten Firmen (siehe auch [Koe03]).

Neben der vom TCPA Konsortium erarbeiteten Architektur plant Microsoft mit einem Aufwand von mehreren hundert Millionen Euro ein von Softwarepatenten geschütztes eigenes Konzept für 'Trustworthy Computing' unter dem Namen Palladium. Dieses wurde 2003 in next-generation secure computing base (NGSCB) umbenannt.

In der offiziellen Microsoft FAQ [MS03] erweckt Microsoft den Anschein, nicht die TCPA Spezifikation zu verwenden.

> *Q:* Is NGSCB base Microsoft's implementation of the Trusted Computing Platform Alliance (TCPA) specification?
>
> *A:* No, the next-generation secure computing base is not an implementation of the TCPA spec. The two projects do share some features, such as attestation and sealed storage, but they have fundamentally different architectures.

Inzwischen gibt es auch andere Stellungnahmen von Microsoft. Nach diesen soll Palladium nun doch auf der geplanten „TCG specification 1.2" aufzubauen.

1.2. Trusted Plattform Module (TPM)

Zentraler Hardwarebaustein der TCPA ist das sogennante Trusted Plattform Module (TPM) (vgl. „Fritz" Chip). In den ersten Implementationen kann man sich dies als eine festverlötete Smartcard vorstellen. Es bestehen Planungen, die komplette Funktionlität in den Prozessoren selbst zu integrieren (vgl. Intel LaGrande).

Nach Angaben aus dem TCPA Konsortium sind die vier wesentlichen Designpunkte der Architektur

- Hardware-Speicher für kryptographische Schlüssel
- Unterstützung sicheren Bootens (vgl. [AFS97])
- Plattform Attestation
- Sealing

Die ersten beiden Punkte werden allgemein als eine wünschenswerte Verbesserung der Computersicherheit angesehen. Allerdings können ganz ähnliche Sicherheitsfeatures bereits heute mit smartcardbasierten Sys-

temen erreicht werden. Smart Cards bieten darüberhinaus eine weit höhere Flexibilität. Kombinierte USB Smart Card/Smart Card Leser erübrigen die Beschaffung von seperaten Lesegeräten.

2. TC und DRM

Die Bereiche der Plattform Attestation und des Sealings sind hingegen hoch umstritten. Hierbei wird der Computer vor dem Nutzer zum Vorteil von Dienstanbietern geschützt.

MIT-Professor Ron Rivest formulierte diesen Sachverhalt folgendermassen.The right way to look at this is you are putting a virtual set-top box inside your PC. You are essentially renting out part of your PC to people you may not trust.Dass existierende Befürchtungen betreffend erheblicher Eingriffe in die persönlichen Computersysteme nicht völlig aus der Luft gegriffen sind, zeigt unter anderem eine Lektüre von Microsoft Lizensen:Microsoft may provide security related updates to the OS Components that will be automatically downloaded onto your computer. These security related updates may disable your ability to copy and/or play Secure Content and use other software on your computer. (Microsoft, Windows Media Player 7.1, EULA) Viele Endnutzer-Lizenzen von Microsoft sind innerhalb der EU juristisch nicht haltbar. TCPA könnte verwendet werden,*rechtswidrige*, verbraucherunfreundliche Lizenzen technisch zu erzwingen.

3. Schlüsselfragen

Dreh- und Angelpunkt der diskutierten Architekturen ist ein eindeutiger privater Schlüssel („Endorsment Key"), auf welchen der Anwender keine volle Kontrolle hat.

3.1. Stellungnahmen führender Kryptographen

Auf der RSA Conference im April 2003 in San Francisco äusserten sich viele der führenden Kryptographen äusserst kritisch zu den aktuellen Plänen der TCPA.

Whitfield Diffie, einer der Entdecker der Public-Key Kryptographie, zeigte sich besorgt über die dominierende Stellung vom Microsoft und forderte, dass die Benutzer die vollständige Kontrolle über die Schlüssel des eigenen Computer behalten sollten.

- (The Microsoft approach) lends itself to market domination, lock out, and not really owning your own computer. That's going to create a fight that dwarfs the debates of the 1990's.
- To risk sloganeering, I say you need to hold the keys to your own computer

Auch Professor Ron Rivest (MIT), 2002 Gewinner des Turing Award, welcher allgemein als eine Art Nobelpreis der Informatik angesehen wird , mahnte eindringlich, die möglichen Konsequenzen gründlich abzuwägen.

- We should be watching this to make sure there are the proper levels of support we really do want
- The right way to look at this is you are putting a virtual set-top box inside your PC. You are essentially renting out part of your PC to people you may not trust.
- We need to understand the full implications of this architecture. This stuff may slip quietly on to people's desktops, but I suspect it will be more a case of a lot of debate.
- Privacy tends to go down in inverse to the number of transistors in the world.

Interessanterweise ist Ron Rivest unter anderem auch der Erfinder des RSA Algorithmus und der MD4-Hash-Funktionen Famile. Dies sind die zentralen kryptographischen Algorithmen, welche im TPM Anwendung finden.

3.2. Key-Management

Viele Forscher warnen aus grundsätzlichen Gründen davor, Schlüsselmanagement zu zentralisieren. Speziell sind zahlreiche schwerwiegende Fehler von Microsoft gerade beim Umgang mit wichtigen kryptographischen Schlüsseln nicht dazu angtan, diesbezügliche Sorgen zu zerstreuen.

Hierzu einige Beispiele.

- Mitte 2001 vergass Microsoft, sein Server-Zertifikat zu verlängern. Niemand konnte sich bei MSN und Passport anmelden. [HN01a]
- Ebenfalls 2001 warnte Microsoft vor einem von einem Unbekannten erschlichenen Microsoft Zertifikat von Verisign. [HN01b]
- In mehreren Windows-Versionen wurde 1999 ein zusätzlicher kryptographischer Schlüssel mit dem Namen nsa_key gefunden. Die NSA ist ein US-Amerikanischer Geheimdienst (www.nsa.gov). Es wurden hierzu verschiedene widersprüchliche und zum Teil schwerlich nachzuvollziehbare Erklärungen abgegeben. [CNN99]

Auch die Tatsache, dass bis in den Juli hinein die TCPA nicht in der Lage war, ihr seit dem 26. Februar 2003 abgelaufenes SSL Zertifikat (https://www.trustedcomputing.org) zu erneuern, trägt zumindest beim Autor nicht gerade zur Bereitschaft bei, auf die Kontrolle der kryptographischen Schlüssel meiner Hardware zu verzichten.

3.3. Zusätzlicher Symmetrischer Schlüssel

Problematisch ist weiterhin, dass Microsoft zusätzlich einen geheimen Schlüssel für symmetrische Verfahren einspeichern möchte [MS03].

Q: What is the „SSC" component of NGSCB?

A: SSC refers to the Security Support Component, a new hardware component of the PC environment that will be introduced as part of the NGSCB architecture. ... The SSC also contains at least one RSA private key and an AES symmetric key, both of which are private to the SSC and are never exported from the chip.

Bei symmetrische Algorithmen (wie AES) ist der Verschlüsselungs-Schlüssel gleich dem Entschlüsselungs-Schlüssel.

Falls, wie ausgeführt, der Schlüssel den Chip nie verlässt, würde dies bedeuten, dass bei einem Hardwarefehler die symmetrisch verschlüsselten Daten nach dem derzeitigen Stande der Wissenschaft unwiederbringlich verloren sind.

4. Sicherheitsbetrachtung der Crypto-Algorithmen

Von der kryptographischen Forschergemeinde wird einhellig begrüsst, dass TCPA bei der Algorithmenwahl auf standardisierte Verfahren (RSA, SHA-1, AES) setzt.

Allerdings erscheint die Verwendung der 160-bit Hashfunktion SHA-1 nicht mehr zeitgemäss. Bei der symmetrischen Verschlüsselung sei zur Erhöhung der Sicherheit die Integration der Varianten AES-192 oder AES-256 angeregt [LW02].

5. Black Box Kryptographie

Seit vielen Jahren warnen Kryptographen, dass verdeckte Kanäle bei der Verwendung von kryptographischer Hardware leicht zu implementieren sind.

Im August 2003 warnte sogar die NSA in einer Stellungnahme explizit vor derartigen Möglichkeiten [HN03]. Zur Sorge insbesondere ausserhalb der USA dürfte insbesondere auch die Äusserung Anlass geben, dass ‚auch' untrusted Hardware von dieser Warnung betroffen ist.

Es ist unter anderem möglich, mit veröffentlichten Verfahren geheime Informationen aus einem „beweisbar sicherem" Blackbox-System sogar „beweisbar sicher" herrauszuschmuggeln. Bei einigen Systemen (z.B. [WL02] passt sehr gut) kann selbst eine Hardware-Analyse nicht aufdecken, welche Informationen verdeckt übertragen wurden, und für einen erfolgreichen Angriff müssen lediglich eine kleine Anzahl von zeitlich nicht notwendigerweise zusammenhängenden Ciphertexten passiv abgehört werden.

Aus diesem Grunde ist es von grossem Belang, dass sämtliche Designunterlagen und auch der eigentliche Herstellungsprozess von vertrauenswürdigen Institutionen vollständig kontrolliert werden können.

Insbesondere nach einer geplanten Integration der kryptographischen Funktionen in den Prozessor scheint es grosse Vorbehalte der meist US-amerikanischen Hersteller gegen eine internationale, unabhängige Kontrolle zu geben.

6. (US) Regierungszugriff

Da Microsoft, sowie die anderen führenden Unternehmen der TCG, als privatrechtliche Firma der US Gesetzgebung untersteht, sollten auch mögliche Eingriffe durch US-Behörden Berücksichtigung finden.

6.1. Lawful Interception und Hardwaresicherheit

Auf dem Hearing des Bundesministeriums für Wirtschaft und Arbeit im Juni 2003 reagierte ein Direktor der TCG auf die Frage eines Berliner Wissenschaftlers nach behördlichen Zugriffsmöglichkeiten im Rahme der sogenanntem Lawful Interception mit einem ungefähr einminütigen Schweigen. [BMWA03].

Ebenso mit grossem Interesse wurde allgemein die Stellungnahme von Microsoft bezüglich Lawful Interception aufgenommen [MS03]:

Q: How could a law enforcement agency access data protected by the NGSCB architecture?

A: Just as with other commercial-grade cryptographic hardware, law enforcement agencies could conceivably „break" the SSC in the hardware of a seized machine to obtain machine secrets.

Sollte die Hardwaresicherheit hinsichtlich Angriffen von Strafverfolgungsbehörden nicht ausreichend sein, erscheint auch die Sicherheit bezüglich anderer Angreifer zweifelhaft. Auch bestünde die Möglichkeit, dass betrügerische Computerhändler sich auf diese Weise Zugriff auf die geheimen Schlüssel verschafffen könnten.

6.2. Microsoft zu Backdoors

Auf die mehrfach vorgebrachte Sorge, dass die Verwendung von starker Kryptographie Begehrlichkeiten der US Behörden wecken könnte, antwortete Microsoft folgendermassen [MS03]:

Q: Won't the FBI, CIA, NSA, etc. want a back door?

A: Microsoft will never voluntarily place a back door in any of its products and would fiercely resist any government attempt to require back doors in products. From a security perspective, such back doors are an unacceptable security risk because they would permit unscrupulous individuals to compromise the confidentiality, integrity, and availability of our customers' data and systems. ... For these reasons and others, we would oppose any such government efforts, as we did during the encryption debate.

Zwar wird Microsoft bezüglich der Ablehnung von Hintertüren weithin Glauben geschenkt, jedoch weisen insbesondere die Worte*never voluntarily* auf ein offensichtliches Dilemma hin.

Micosoft ist eine privatwirtschatliche Firma unter US-amerikanischem Recht. Es dürfte Microsoft schwerfallen, diesbezügliche Weisungen der US-Regierung beziehungsweise des US-amerikanischen Gesetzgebers nicht Folge zu leisten.

7. TCPA und Betriebssysteme

Da Microsoft einen überwältigenden Anteil des Betriebssystem-Marktes beherrscht, können TCPA und Palladium nur schwerlich isoliert betrachtet werden.

Bruce Schneier, Autor des Standarwerkes „Applied Cryptography", geht sogar einen Schritt weiter:I expect TCPA to become irrelevant, since Microsoft is a monopoly player in the OS market[LM03]

Doch die TCPA bringt auch Probleme für alternative Betriebssysteme wie GNU/Linux.

7.1. Open Source Software und TCPA

Mindestens zwei Firmen arbeiten an einer „TCPA-enhanced" version von GNU/Linux. Nach Ansicht der meisten Experten ist es erforderlich, Programme, welche in einem „trusted" Bereich laufen, auf Sicherheit zu untersuchen. Dies hat umfangreiche Auswirkungen auf die Entwicklung von freier Software.

Nach einer wahrscheinlich kostspieligen Evaluation wird eine Version des Programmes unterzeichnet. Diese Entwicklung muss unter GPL bleiben, jedoch macht jede Änderung die Signatur ungültig. Dies ist in jedem Fall ein Verstoss gegen die Grundphilosophie von Freier Software.

Peter N. Biddle, Microsoft Product Unit Manager Palladium, äusserte sich zu dieser Problemstellung auf der Comdex 2002.Grundsätzlich könnte die gesamte Palladium-Architektur auch nach Linux portiert werden, wenn die Lizenzvorbehalte im Stil der GPL nicht wären. Jeder Code für ein TPM wird von der TCPA signiert und verschlüsselt. Wird irgendetwas weitergeben, verändert und neu kompiliert, so ist eine neue TCPA-Lizenz erforderlich. So gesehen wird das Trustworthy Computing niemals mit einer Open-Source-Lizenz kompatibel sein.[HN02]

7.2. Microsoft Patente

Anlass zu Sorge, dass Microsoft auch über Patente der freien Wettbewerb behindern könnte, werden auch durch Microsofts offizielle Stellungnahme [MS03] nicht gerade aus der Welt geräumt.

> *Q:* Could Linux, FreeBSD, or another open source OS create a similar trust architecture?
>
> *A:* From a technology perspective, it will be possible to develop a nexus that interoperates with other operating systems on the hardware of a nexus-aware PC. Much of the next-generation secure computing base architecture design is covered by patents, and there will be intellectual property issues to be resolved. It is too early to speculate on how those issues might be addressed.

Beim Hearing des Bundeswirtschaftsministeriums im Juli 2003 bedauerte selbst der hochrangige Microsoftvertreter die in diesem Bereich bestehenden Unklarheiten.

8. Fazit

Neben vielen kritisch zu bewertenden Teilaspekten sind insbesondere zwei Punkte von grosser wirtschaftlicher und gesellschaftlicher Bedeutung: die Frage der Kontrolle über die kryptographischen Schlüssel und die Gefahr, dass mit technischen Mitteln der freie Austausch von Informationen behindert und unliebsame Konkurrenz (z.B. GNU/Linux) ausgesperrt werden kann.

Damit drohen zwei Welten zu entstehen, welche Schwierigkeiten haben werden Informationen auszutauschen. Jedoch hat gerade die Offenheit des Netzes eine Wissensexploxion ausgelöst. Daher bedrohen TCPA und Palladium die Fundamente der Wissensgesellschaft. DRM, Plattformbindung und sich nach einer gewissen Zeit selbst unlesbar machende Dokumente machen Archivierung von Wissen wird schwierig bis unmöglich.

Die Fremdkontrolle von kryptographischen Schlüsseln, welche eine gewichtige Rolle in der zukünftigen IT Infrastruktur spielen, durch eine privatwirtschaftliche Firma, welche unter der Rechtsaufsicht einer ausländischen Regierung steht, bringt auch interessante wirtschaftspolitische und juristische Fragestellungen mit sich.

Die vor allem in Europa vorangetriebenene Entwicklung von smartcardbasierten Systemen bietet interessante Möglichkeiten, erhöhte Sicherheit und persönliche Kontrolle von kryptographischen Schlüsseln zu kombinieren.

Acknowledments

Ausdrücklich bedanken möchte ich mich bei Andy Tanenbaum, Andreas Bogk, Lucky Green, C.S. Hagen, Rop Gonggrijp und Carla van Rijsbergen für zahreiche wertvolle Anregungen. Die Vrije Universiteit Amsterdam bot und bietet mir ausgezeichnete Forschungsmöglichkeiten. Stellvertretend hierfür sei insbesondere Andy Tanenbaum, Guido v. Noordende, Kees Bot und Philip Homburg nochmals herzlich gedankt.

Literatur

And03 Anderson, R., Homepage, http://wwwck.cam.ac.uk/~rja 14*AFS97* Arbaugh,B., Farber, D., Smith, J., ``A Secure and Reliable Bootstrap Architecture", IEEE Symposium on Security and Privacy (1997) *BMWA03* Bundesministerium für Wirtschaft und Arbeit, Sym-

posium: „Trusted Computing Group (TCG)“ am 2. und 3. Juli 2003 (Berlin), Streams http://www.web-pk.de/bmwa/willkommen.php*CNN99*CNN.com, „NSA key to Windows: an open question“, http://www.cnn.com/TECH/computing/9909/03/windows.nsa.02/ *HN01a*Heise News, „Microsoft Server-Zertifikate abgelaufen“, http://www.heise.de/newsticker/data/wst-06.05.01-003/*HN01b*Heise News, „Microsoft warnt vor Cracker-Zertifikat“, http://www.heise.de/newsticker/data/jo-24.03.01-001/*HN02*Heise News, „Comdex: Zeitmaschine von Microsoft“, 2002. http://www.heise.de/newsticker/data/wst-21.11.02-000/ *HN03*Heise News, „NSA will gegen Hintertüren vorgehen“, 2003. http://www.heise.de/newsticker/data/ghi-09.08.03-000/*Koe03*Koenig, C., „Trusted Computing im Fadenkreuz des EG-Wettbewerbsrechts“, TRUSTED COMPUTING - Neue Herausforderungen für das deutsche und europäische Wirtschaftsrecht, Bonn, Mai 2003.*LW02*Lucks, S., Weis, R., „Neue Erkenntnisse zur Sicherheit des Verschluesselungsstandard AES“, Datenschutz und Datensicherheit, DuD 11/02, Viewег, 2002.*LM03*Linux Magazine, „Microsoft's Power Play“,Januar 2003. http://www.linux-mag.com/2003-01/palladium_02.html*MS03*Microsoft Next-Generation Secure Computing Base - Technical FAQ, February 2003. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/news/NGSCB.asp*TCG03*Trusted Computing Group (TCG), http://www.trustedcomputinggroup.org*TCPA03*TCPA - Trusted Computing Platform Alliance, http://www.trustedcomputing.org/*WL02*Weis, R., Lucks, S., „All Your Keybit are belong to us - The Truth about Blackbox Cryptograpy“, SANE 2002, Maastricht 2002. http://www.nluug.nl/events/sane2002/papers/Weis-LucksAllYourKeybit.ps

T*-News

zusammengestellt von Ruediger Weis

Trusted Computing wurmt weiter

Im August schafften es mal wieder mal widrige Windows-Würme in die Schlagzeilen. Wer in diesem Zusammenhang Hoffnungen auf T* Computing setzten sollte, muss sich auf eine Entäuschung gefasst machen. Die Vertreter der Trusted Computing Group und von Microsoft räumten zuletzt auf dem Syposium des Bundeswirtschaftsministerium im Juli in Berlin mit bemerkenswerter Offenheit ein, dass gegen die gewärtigen Wurmplagen TCPA und Palladium faktisch wirkungslos sind. [BMWA03]

DDos gegen zentrale Server

Auch die wiederholten Warnungen (z.B. CCCongress 2002, http://www.heise.de/newsticker/data/se-28.12.02-001/), dass zentrale Server von Sicherheitsarchitekturen zum Ziel von verteitlten DoS Angriffen werden koennten, wurde duch die neuen Vorfälle bestätigt.

Dass diesmal grössere Schäden vermieden werden konnten, ist wohl ueberwiegend der Unbedarftheit des Wurmautors zu danken.

„Die Stilllegung der attackierten Adresse war relativ problemlos möglich, weil die im Internet Explorer eingebaute Update-Funktion eine andere Adresse (windowsupdate.microsoft.com) benutzt.“ [heise online News,16.08.03, Microsoft lässt Angriff von Lovsan/W32.Blaster ins Leere laufen (http://www.heise.de/newsticker/data/ju-16.08.03-000/)]

MS Zwangs-Update I

Nichts mehr mit der im Zusammenhang mit TCPA/Palladium von den Industrievertretern stets betonten „Freiwilligkeit“? Dennoch plant Mirosoft laut Washington Post „aus Sicherheitsgründen“ Updates automatisch für Windows-Systeme vorzumehmen. [heise online News, 19.08.2003, Microsoft will automatische Updatefunktion für nächstes Windows, (http://www.heise.de/newsticker/data/tol-19.08.03-001/)]

MS Zwangs-Update II

Auch im Bereiche der Messager sollen MS Kunden zu Update geötig werden. Wie sagt es Microsoft?Bestandteil der Microsoft Trustworthy Computing-Initiative ist die Bereitstellung eines Sicherheitsupdates für einige Benutzer des .NET Messenger Services. [heise online News, 21.08.2003, MSN Messenger: Update oder raus!, (http://www.heise.de/newsticker/data/tol-21.08.03-002/)]

MS Zwangs-Update III

Bill Gates persönlich erklärt in einem Interview mit der New York Times, dass die Updates automatisieren werden müssen. [heise online News, 03.09.2003, Bill Gates setzt auf automatische Updates http://www.heise.de/newsticker/data/anw-03.09.03-003/]

NSA warnt vor Hintertüren

Eine Unterstützng der CCC These, dass Hintertüren eine grosse Bedrohung für Wirtschaft und Gesellschaft darstellen, kommt von überraschender Seite. Der amerikanische Supergeheimdienst NSA warnt eindringlich vor solchen MöglichkeitenIn seiner Aussage wies Wolf ebenfalls darauf hin, dass „untrustworthy hardware“ (nicht vertrauenswürdige Hardware) ein Problem ähnlicher Tragweite werden kann. Aufmerksame Beobachter könnten diese Aussage auch als ein impliziertes Eingeständnis der Missbrachsmöglichleiten von Trusted Computing Hardware auffassen. [heise online News, 09.08.2003, NSA will gegen Hintertüren vorgehen, (http://www.heise.de/newsticker/data/ghi-09.08.03-000/)]

Kriterien- und Präferenzkatalog der Bundesregierung zu den Sicherheitsinitiativen TCG und NGSCB im Bereich Trusted Computing

Aus gewöhnlich gut unterrichteten Kreisen erreichte uns die Stellungnahme der Bundesregierung an die Trusted Computing Group vom 24.10.2003. Wir möchten unsere Freude darüber Ausdruck verleihen, daß die Bundesregierung sich in weiten Teilen den Forderungen des CCC angeschlossen hat. Und denkt dran: nur ein löschbarer Endorsement Key ist ein guter Endorsement Key. Der Endorsement Key ist sinnvoll als Mechanismus, um dem neuen Besitzer die Echtheit des Chips zu bestätigen. Leider ist er auch der Schlüssel (pun intended) zur restriktiven Kontrolle der Nutzerrechte, wenn er nicht umgehend nach der Inbetriebnahme durch den Schlüssel des Besitzers ersetzt wird.

Vorbemerkung

Die Informationstechnik ist bedeutsam für alle Bereiche der Wirtschaft, Verwaltung und des Privatlebens. Eine funktionierende und sichere Informationstechnik ist ein Grundpfeiler für moderne Geschäftsprozesse und Kommunikationsverbindungen. Verlässliches E-Government und erfolgreicher E-Commerce sind nur mit sicheren IT-Komponenten realisierbar.

Zunehmend wird damit die Informationstechnik zum kritischen Faktor, deren Ausfall oder Kompromittierung schwerwiegende Konsequenzen für die Nutzer der IT haben kann. Dass die Bedrohungen von IT-Systemen nicht geringer geworden sind, zeigen aktuelle Meldungen in Bezug auf das Auftreten neuer Viren, Schwachstellen, DoS-Attacken und weiterer Bedrohungen. IT-Systeme werden auch in kritischen Infrastrukturbereichen genutzt, die für das Funktionieren der Gesellschaft unverzichtbar sind. Dem Schutz dieser Komponenten muss eine hohe Priorität beigemessen werden.

Grundsätzliches

Die Bundesregierung begrüßt grundsätzlich jede Maßnahme, die dem Schutz der Informationstechnik dient. Die Maßnahmen müssen dabei allerdings derart gestaltet sein, dass alle Bestandteile gesetzeskonform sind. Dabei sind insbesondere die Aspekte des Datenschutzes zu berücksichtigen.

Darüber hinaus können nur Maßnahmen unterstützt werden, die dazu geeignet sind, das Vertrauen in die Informationstechnik zu erhöhen. Voraussetzung hierzu sind eine transparente Informationspolitik in Bezug auf die Schutzkonzepte und Schutzmaßnahmen, sowie die Einbeziehung unterschiedlicher Interessengruppen bei der Planung, Entwicklung und Vermarktung von Schutzmechanismen. Darüber hinaus dürfen Schutzmaßnahmen im IT-Bereich nicht dazu missbraucht werden, Marktzugangsschranken zu schaffen.

Zu den Sicherheitsinitiativen TCG und NGSCB

Die Bundesregierung begrüßt grundsätzlich die Absicht der in der TCG versammelten Hersteller sowie der Firma Microsoft, mit TCG und NGSCB die Sicherheit von PC-Plattformen zu erhöhen.

Zum Sicherheitskonzept der TCG

1. Sicherheitstechnische Anforderungen

1.1. Transparenz und Offenlegung von Schnittstellen und Spezifikationen

Die für Verschlüsselungs- und Signaturfunktionen genutzten Algorithmen müssen standardisiert und national und international als sicher erachtet sein.

Die verwendeten Schlüssellängen und sonstigen Parameter müssen mindestens denen entsprechen, die vom Bundesamt für Sicherheit in der Informationstechnik in bezug auf sichere Verschlüsselung und sichere Signatur vorgegeben wurden.

Das Sicherheitsmodul (TPM) darf keine undokumentierten Funktionen enthalten; insbesondere keine Funktionen, die als potentielle Schwachstelle genutzt werden können oder einen sonstigen Zugriff auf geschützte Daten durch Dritte ermöglichen.

Die TCG sollte die Anwendungsszenarien verständlich und anschaulich dokumentieren, auf deren Grundlage die Spezifikation für das TPM erarbeitet wurde. Nur so können perspektivisch die Auswirkungen des TPM im praktischen Einsatz anschaulich verständlich gemacht werden und die betroffenen Endanwendungen identifiziert werden.

1.II. Zertifizierung des Sicherheitssystems

Das Sicherheitsmodul (TPM) muss mindestens nach CC EAL4 medium zertifiziert werden. Die Zertifizierung muss auch den physikalischen und logischen Schutz vor Angriffen auf das Sicherheitsmodul (TPM) umfassen.

Das Sicherheitsmodul (TPM) muss prüfbar sein und seine Funktionalität muss von unabhängigen Institutionen bestätigt werden können. Die Erarbeitung entsprechender Protection-Profiles wird als unerlässlich angesehen, um einen international gleichmäßigen Sicherheitsstandard zu etablieren. Um die Funktion des Sicherheitsmoduls (TPM) eindeutig zuordnen zu können und eine eindeutige Prüffähigkeit zu gewährleisten, müssen die Sicherheitsfunktionen an einer zentralen Stelle in einem separaten Baustein (TPM) gebündelt werden. Eine Vermischung des Sicherheitsmoduls mit anderen Funktionseinheiten (z.B. CPU, Chipsatz, etc.) führt zu Intransparenz und dazu, dass eine sicherheitstechnische Überprüfung nicht mehr einfach durchführbar ist.

1.III. Systemsicherheit, Datensicherung und Migration

Die in dem vorhandenen Sicherheitsmodul gespeicherten Informationen müssen sich auf eine neue Hardwareplattform insoweit übertragen lassen, dass vom Anwender erworbene Software weiterhin auf der neuen Hardwareplattform lauffähig ist. Alle kryptographischen Schlüssel des TPM, die für die Nutzung von Software, Daten und Onlinedienstleistungen benötigt werden, müssen von einer Hardware-Plattform auf eine andere migrierbar sein. Der Fall eines defekten TPM muss ebenfalls berücksichtigt werden und eine Migrationsmöglichkeit für Daten bzw. Schlüssel implementiert werden.

Werden auf dem Sicherheitsmodul (TPM) aufbauende DRM-Lösungen entwickelt, ist bei der Entwicklung das Recht des Nutzers auf Privatkopie zu berücksichtigen und entsprechend technisch zu implementieren.

Daten die nicht urheberrechtlich geschützt sind und unter Einbeziehung des Sicherheitsmoduls (TPM) verarbeitet werden, müssen sich auch auf Systeme zur weiteren Nutzung übertragen lassen, die über kein Sicherheitsmodul verfügen.

Im Konzept des Sicherheitsmoduls (TPM) müssen für alle wesentlichen Komponenten Redundanzen vorgesehen werden, so dass „Single Point of Failures" vermieden werden.

Insofern Schlüssel verwendet werden, die aus Sicherheitsgründen zwingend in dem Sicherheitsmodul (TPM) verbleiben müssen und nicht auslesbar sind (z.B. Endorsement-Key), müssen diese auf dem TPM selbst erzeugt werden können oder durch einen Prozess erzeugt werden, der eine gleichwertige Sicherheit garantiert. Die sichere Erzeugung dieser Schlüssel muss durch eine unabhängige Instanz bestätigt werden.

1.IV. Systemkontrolle durch den Anwender

Abschaltbarkeit der Sicherheitsmodule.

Der Anwender muss entscheiden können ob er die neuen Funktionen zur Verbesserung der Sicherheit nutzen möchte. Daher müssen in die Hardware integrierte Sicherheitsmodule (TPM) vollständig deaktivierbar sein. Hierbei sollte, alternativ zu einer Softwarelösung, auch eine Hardwarelösung (z.B. Schalter oder Sockel für TPM) implementiert werden. Die Deaktivierung darf keine negativen Einflüsse auf die Funktionalität der Hard- und Software haben, die nicht die Funktionen der neuen Sicherheitsarchitektur (TCG) nutzen.

Sicherheitsmodul deaktiviert als Standardeinstellung.

Zusätzlich integrierte Sicherheitsmodule müssen standardmäßig in deaktiviertem Zustand ausgeliefert werden. Der Eigentümer oder Anwender muss vorhandene Sicherheitsmodule selbständig aktivieren.

Der Nutzer muss die volle Kontrolle über seine Schlüssel haben und diese ggf. löschen und neu erzeugen können. Ausgenommen vom Zugriff durch den Nutzer sind lediglich Schlüssel, die zur Sicherstellung der Integrität und Authentizität des TPM dienen (z.B. Endorsement-Key). Diese Schlüssel, sofern Sie nicht zur

eindeutigen Identifizierung des Sicherheitsmoduls dienen (z.B. Endorsement-Key), müssen jedoch durch den Nutzer bzw. Besitzer reinitialisierbar sein. Eine Löschung aller auf dem TPM gespeicherten Informationen sollte, unter Aufgabe der Funktionalität des TPM, möglich sein (z.B. bei Verschrottung des PC).

Der Nutzer muss den Zugriff auf seine Schlüssel kontrollieren können und seine Schlüssel gegen fremden Zugriff verlässlich sichern können.

Insofern das Sicherheitsmodul (TPM) fest mit der restlichen Hardware des IT-Systems (z.B. PC) verbunden ist, sollte sich die Funktionalität des Sicherheitsmoduls darauf beschränken, die Sicherheit und Integrität der Plattform zu gewährleisten. Die Nutzung von personalisierten Programmen, Daten und Onlinedienstleistungen sollte wenn nötig nicht an das Sicherheitsmodul (TPM) gebunden werden, sondern an eine personalisierte Smart-Card. Damit ließe sich der anwenderbezogene Zugriff auf Daten flexibler gestalten und Migrationsprobleme würden deutlich reduziert. Hier wird für das TPM die Auslagerung der Funktionen zur Identitätsfeststellung (z.B. die AIKs) und der zugehörigen kryptographischen Schlüssel in eine mobile Smart-Card gefordert.

Das Sicherheitsmodul (TPM) darf die Nutzung von Software nicht dadurch behindern, dass für die Nutzung der Software die Zertifizierung durch eine externe Zentralstelle benötigt wird, die außerhalb des Verantwortungsbereichs des Eigentümers bzw. Nutzers liegt.

1.v. Datenschutz

Alle datenschutzrechtlichen Vorgaben müssen unter allen Betriebsbedingungen des Sicherheitsmoduls eingehalten werden. Insbesondere müssen datenschutzrechtliche Funktionen so transparent gestaltet werden, dass der Endnutzer jederzeit von seinem Recht der informationellen Selbstbestimmung Gebrauch machen kann und diese Funktionen deaktivieren kann.

Datenschutzrechtlich relevante Funktionen dürfen sich nicht automatisch von außen aktivieren lassen, ohne das der Endanwender im Einzelfall zustimmt.

Die Nutzung der Sicherheitsfunktionen des Sicherheitsmoduls (TPM) muss auch ohne Onlineverbindung (Internet) möglich sein.

Bei der Nutzung von anonymen Identitäten (AIK), die vom Sicherheitsmodul (TPM) zur Verfügung gestellt werden, muss eine Schwächung der Anonymität, durch indirekte Verknüpfungen von Daten aus dem TPM verhindert werden (z.B. durch die Verknüpfung der AIKs über das TPM-Endorsement-Crendential in einer CA). Dazu sind entsprechende technische oder organisatorische Mechanismen vorzusehen, die dies sicherstellen.

Sofern die Nutzung einer CA vorgesehen ist, muss der Anwender eine Wahlmöglichkeit bzgl. der verwendeten CA haben.

Zur Gewährleistung eines Maximums an Objektivität und zum Schutz der Anwender insbesondere in datenschutzrechtlicher Hinsicht müssen die genutzten CAs unter staatlicher Aufsicht arbeiten.

Unter datenschutzrechtlichen Aspekten ist eine pseudonyme Attestierung („Zero-Knowledge-Verfahren" für Beglaubigungsprozesse) der Identität (auch anonyme Identität) ohne externe CA anzustreben.

II. Wirtschaftspolitische Anforderungen

II.I. Faire Lizenzpolitik

Die Patentpolitik der TCG und deren Mitgliedern darf nicht dazu genutzt werden, Wettbewerber z.B. durch unangemessene Lizenzgebühren auszugrenzen. Insbesondere für den Open-Source Bereich sollte die TCG eine Lösung finden, die nicht kommerzielle Open-Source Projekte von Lizenzgebühren frei stellt.

Die von der TCG spezifizierte Treibersoftware – der TSS – sollte unter einer Lizenz veröffentlicht werden, welche die kostenfreie Nutzung, Modifikation und Weitergabe ermöglicht, um Zeit- und Entwicklungsnachteile von Nicht-TCG-Mitgliedern auszugleichen.

Die beteiligten Firmen müssen vor Verabschiedung der Spezifikation und Standards bekannt geben, welches relevante Intellectual Property (IP) sie zu der Spezifikation haben und ob sie bereit sind, diese unter RAND zu spezifizieren.

Die TCG sollte mit ihren Mitgliedsunternehmen sowie mit den zuständigen europäischen und nationalen Wettbewerbsbehörden in einen Dialog treten, um die Möglichkeiten und Rahmenbedingungen der Schaffung eines „Technologie-Pools" zu klären, um dadurch wettbewerbsrechtlich relevante Behinderungspotentiale bei der Nutzung von Lizenzen zu beseitigen.

II.II. Nicht diskriminierende Informationspolitik

Die TCG sollte zu offenen, transparenten und diskriminierungsfreien Bedingungen eine zusätzliche unentgeltliche Mitgliedschaft einführen, die vor allem die Möglichkeit umfasst, alle für die Entwicklung von Software (u.a. Open-Source-Software) - welche die Funktionen des Sicherheitsmoduls (TPM) nutzt - notwendigen Informationen in der erforderlichen Zeitnähe, ohne zusätzliche Kosten für nicht kommerzielle Projekte, zu erlangen.

Unabhängig davon sollte Vertretern der Open-Source-Gemeinde eine angemessene Mitwirkungsmöglichkeit in der TCG geboten werden.

Eine ausgewogene Interessenvertretung sollte durch gleichrangige Vertretung innerhalb der TCG unter Berücksichtigung regionaler und branchenspezifischer Aspekte angestrebt werden.

II.III. Sicherheitstechnologie darf nicht Marktzugangsschranken schaffen

Das Handeln der TCG darf nicht dazu führen, dass im IT-Bereich marktbeherrschende Stellungen entstehen oder verstärkt werden.

Die TCG darf nicht dazu genutzt werden, Marktzutrittshemmnisse für einzelne Unternehmen oder Branchen zu schaffen.

II.IV. Technologische Offenheit

Das Sicherheitsmodul (TPM) muss system-offen sein, so dass die Einbindung des Sicherheitsmoduls (TPM) für verschiedene Hardwareplattformen mit ähnlichem Aufwand möglich ist. Dabei müssen unabhängig vom System alle Funktionen des Sicherheitsmoduls auf allen Hardwareplattformen gleichermaßen unterstützt werden.

TCG-gestützte Computersysteme müssen mit Nicht-TCG-gestützten Computersystemen interoperabel sein. Die Spezifikationen der TCG dürfen nicht dazu genutzt werden, bestimmte Plattformen und Systeme auszuschließen.

Die TCG muss dafür Sorge tragen, dass die verabschiedeten Spezifikationen nicht einzelne Mitgliedsunternehmen einseitig bevorzugen. Insbesondere sollten die Spezifikationen unabhängig von den Voraussetzungen einer speziellen Hardware oder Software sein.

Zum Sicherheitskonzept NGSCB der Firma Microsoft

Die Sicherheitsinitiative NGSCB (vormals Palladium) der Firma Microsoft befindet sich noch im Entwicklungsstadium. NGSCB ist eine Systemlösung, die im wesentlichen auf einem sicheren Betriebssystemkern (Nexus) beruht, der durch entsprechende Hardwareerweiterungen unterstützt und abgesichert wird. Das TPM der TCG wird vermutlich von NGSCB mit genutzt werden.

Zu NGSCB sind bisher keine Detailinformationen bekannt. Auf Grundlage des bisher bekannten Grobkonzeptes können jedoch Grundforderungen bzgl. sicherheitstechnischer und wirtschaftspolitischer Aspekte aufgestellt werden.

zu I. (Sicherheitstechnische Grundforderungen)

Werden Teile von NGSCB für DRM-Zwecke konzipiert, so muss sichergestellt werden, dass die legitimen Rechte der Nutzer gewahrt bleiben und z.B. Mechanismen vorgesehen werden, die die Anfertigung einer Privatkopie erlauben.

Die Sicherheitsfunktionen von NGSCB müssen auch ohne Onlineverbindung nutzbar sein.

Werden personenbezogene Daten in Zusammenhang mit der Nutzung von NGSCB übertragen, so muss der Nutzer die Möglichkeit haben, der Übertragung im Einzelfall zuzustimmen.

Der Anwender ist über Art und Umfang der Daten zu informieren, die bei der Nutzung von NGSCB ggf. an eine externe Stelle übermittelt werden.

Der Hersteller von NGSCB (Microsoft) muss dafür Sorge tragen, dass die Schnittstellen von NGSCB transparent gestaltet sind und die Dokumentation öffentlich verfügbar ist. Sicherheitsfunktionen können nur als sicher erachtet werden, wenn diese transparent und nachvollziehbar sind.

Die Nutzung von Software nur unter Zustimmung einer zentralen Zertifizierungsinstanz wird kritisch gesehen. Ist eine Zertifizierung notwendig, so sollte diese durch eine unabhängige Stelle und zu angemessenen Gebühren erfolgen. Nicht kommerzielle Software sollte von ggf. erhobenen Zertifizierungsgebühren frei gestellt werden.

Die in dem Zusammenhang mit der Realisierung des Sicherheitskonzeptes von Microsoft entwickelten Komponenten müssen auch für andere Software-Entwickler offen sein. Dabei müssen den unabhängigen Entwicklern bereits im Vorfeld und in der erforderlichen Zeitnähe Entwicklungsunterlagen zur Verfügung stehen, damit die Möglichkeit besteht, dass nicht nur ein einziges Betriebssystem die neuen Sicherheitstechnologien unterstützt.

zu II. (Wirtschaftspolitische Grundforderungen)

In jedem Fall ist eine offene und transparente Informationspolitik die unverzichtbare Voraussetzung für die Schaffung des notwendigen Vertrauens bei den Nutzern aus Wirtschaft, Verwaltung und Politik.

Eine diskriminierende Ausgrenzung von Hardware- oder Softwareherstellern durch die Lizenzbedingungen von NGSCB darf nicht stattfinden.

Software, die nicht von den neuen Funktionen von NGSCB gebrauch macht, muss weiterhin unter dem Betriebssystem lauffähig sein, das auch NGSCB unterstützt.

Sollte NGSCB für DRM (Digital Rights Management) verwendet werden, so ist einer ggf. vorgesehenen Prüfung im Offlinemodus der Vorzug vor einer Onlineprüfung zu geben.

In jedem Fall sollte die TCG gemeinsam mit Branchen- oder anderen Verbänden eine Schlichtungsstelle mit dem Ziel einrichten, Beschwerden einzelner Wirtschaftsteilnehmer über mögliche Diskriminierungen am Markt und beim Marktzutritt zu prüfen, Hilfestellung zu geben und einen Interessensausgleich aller Beteiligten herbeizuführen.

The Value of Disgust

von Philip <philip@linuxteam.at> und

Das Domain Name System ist, neben SMTP, das sicherlich am meisten fehlentwickelte und am häufigsten mißbrauchte Protokoll mit Verwendung in bestehender (teils kritischer) Infrastruktur. Während einige sich das Hirn zermartern, wie man der ungeliebten Reminiszenz vergangener Zeiten am elegantesten und pietätvollsten ledig wird, andere täglich um den göttlichen Funkensprung beten, und der Rest schlicht so tut als gäbe es kein Problem, ist DNS immer noch die Crux des modernen Internets. Nicht nur das, nein, es wird auch nahezu täglich schlimmer: DNS hat nun quasi von selbst einen, zu seiner minderwertigen Technik passenden minderwertigen Partner mit noch minderwertigeren Geschäftspraktiken gefunden, nur um mit ihm weiterhin noch mehr Böses(tm) tun und in weiterer Folge die Weltherrschaft an sich reißen zu können.

Am 15. 9. 2003 hat VeriSign in den gTLD (generic Top Level Domain, wie auch us, de, at, ...) Zonen net und com Platzhaltereinträge (eng: wildcards) aktiviert, welche nicht nur die Unlust verschiedener Mailserveradmins erregt sondern auch noch andere Implikationen zu Tage gefördert (und neue generiert) hat, die man größtenteils lieber weiter stillschweigend ignorieren würde:

- Der Sinn und Buchstabe des Vertrages zwischen Verisign und ICANN steht zur Diskussion
- ICANN kommt in eine Art Zugzwang ein Machtwort zu sprechen und seine politische Potenz wird in Frage gestellt
- Verisign macht so die Nutzung von kritischer Infrastruktur zwecks zweifelhafter Geschäftemacherei salonfähig
- Bezahlte, aber inaktive Domains waren auch betroffen
- Die Privatsphäre des einzelnen Verbrauchers wird kompromittiert
- Die entstandene Wettbewerbsverzerrung ist immens, die Schädigung von Firmen die Schreibfehler-Domains einzeln kaufen mußten, massiv
- Viele Applikationen rechnen mit HOST_NOT_FOUND, bekommen aber ECONNREFUSED, oder noch fieser, eine Verbindung die gleich wieder geschlossen wird

Die Situation ist nun für ICANN und die Netzgemeinschaft mehr als prekär. Wenn es Verisign beim nächsten Versuch auf einen offenen Streit ankommen läßt und sich Anweisungen von ICANN widersetzt, wird dadurch möglicherweise die Position einer Organisation geschwächt, deren Stärke und Autorität für das homogene Funktionieren des Netzes unerläßlich ist. ICANN sei „Der Tiger ohne Zähne“, und man müßte das selbst in die Hand nehmen, hört man so manchen Unkenruf. Doch eine Art „Bürgerkrieg“ wünscht sich keiner der noch bei Vernunft ist, und so bleiben bestimmte Handlungen auch vorerst die Wahnsinnstaten einzelner Fehlgeleiteter. Aber wenn sich eine Firma wie Verisign nicht mehr dazu verpflichtet fühlt einer Autorität wie ICANN zu gehorchen, läuft der „Staat“ Internet die Gefahr, Opfer eines Putsches oder ähnlichem zu werden. Die Vorstellung, das Zonen von Registrars mal in vierzig Prozent des Netzes, mal in sechzig erreichbar sind (etwas, das in einem Internet mit dezentral verwalteten gTLD Zonen unweigerlich der Fall sein würde), erschreckt bestimmt nicht zu unrecht. Dennoch läuft es darauf hinaus, und sollten Gesellschaften wie VeriSign fortfahren die ohnehin wackligen Eckpfeiler des Internets zu destabilisieren, wird es vielleicht noch ein böses Ende nehmen. Ein wenig erinnert das Ganze an das gespaltene Verhältnis von Kleinweich ([MS]) zu den Publikationen der IETF ([RFC]), wobei hier sich die negativen Auswirkungen auf die Technik und den Markt schon seit ehedem zeigen.

Wie leicht zu erkennen ist, überwiegen die politischen, rechtlichen und ökonomischen Probleme die technischen um ein Vielfaches. Nicht nur ist die technische Seite der Implementierung von Sitefinder (bis auf den kaputten smtpd den man laufen hatte, siehe [VER1]) rein auf Protokollebeneperfectly correct. Die DNS basierten „Sicherheitsprodukte“ die sich auf dieses Krüppelprotokoll verlassen, sollten eigentlich längst obsolet sein. Selbst ein Administrator müßte die IPs die er probeweise pingt auswendig wissen; -n läßt grüßen. Des Weiteren gab es schon vor VeriSign viele (allerdings größtenteils dubiose) gTLD's die sich teilweise seit 1998 der Platzhalter Einträge bedienen. Verisigns Fehler ist es nicht, mit einem kaputten Protokoll kaputten Geschäftspraktiken nachzugehen; vielmehr ist ihr Fehler, diese Praxis als Referenzmodell zu etablieren und damit auch zu legitimieren.

Aus diesen und anderen Gründen mag die einzig sinnvolle Argumentationslinie die rechtliche und politi-

sche Seite sein - jene entpuppt sich jedoch, wie eben gezeigt, als um so potenter. Wer sich damit mehr auseinandersetzen möchte, dem sei die Lektüre etwa von [NAN] und [ICA2] empfohlen. Das nun folgende widmet sich mehr dem technischen Aspekt und was man als Einzelner tun kann um den potentiellen Wiederholungstätern in Mountain View beim nächsten Mal gründlich in die Suppe zu spucken.

Was ist eigentlich passiert?

Um clientseitig implementierten „Schreibfehler-Korrektur-Diensten" wie der MSN Suche des Internet Explorers oder derlei ähnlichem mehr schon im Vorhinein das Wasser abzugraben, ist es nötig den Browser im Unklaren darüber zu lassen, daß eine Seite (Domain) nicht gefunden (d.h. aufgelöst) wurde. Leider ist das ohne den Benutzer vorher um Erlaubnis zu bitten nur möglich, indem die Rücklieferung von DNS Return Code 3 (NXDOMAIN) verhindert wird. Also ätzt man einfach Platzhalter Einträge wie etwa
`*.com. 180 IN A 64.94.110.11 *.net. 180 IN A 64.94.110.11`
in seine gTLD Nameserver, mit dem Effekt, daß auch `www.i-dont-exist-coz-i-was-spetl-wrong.com` auf eine gültige IP aufgelöst wird.

Wie Sitefinder genau implementiert ist, entnimmt man am besten [VER1] und [VER2] (da man bei VeriSign seine Hausaufgaben gut gemacht hat), deswegen beschränkt es sich im weiteren auf die DNS seitige (Mal)Funktion.

DNS Abfrage ohne Platzhalter in der gTLD Zone

Zuerst eine normale rekursive DNS Abfrage des A Resource Records am Beispiel von www.icann.com. Sie sieht, von der Sicht eines Nameservers (in diesem Artikel größtenteils synonym fürRecursor), im Normalfall ungefähr so aus (dig Ausgaben gekürzt):

```
$ dig . SOA . 225671 IN NS F.root-servers.net.
$ dig @F.root-servers.net. www.icann.com. A com. 172800 IN NS
A.GTLD-SERVERS.NET.
$ dig @A.GTLD-SERVERS.NET. www.icann.com. A icann.com. 172800
IN NS ns.apnic.net.
$ dig @ns.apnic.net. www.icann.com. A +short 192.0.34.164
```

Was geschehen ist: der anfragende Nameserver hat aus seinen Hints (hier dargestellt durch dig . SOA) einen beliebigen Root Nameserver rausgesucht (F-Root) und diesen dann mit seiner Anfrage behelligt. Von F-Root wurde er an einen gTLD Nameserver für die Zone com delegiert, (A-GTLD) welchen er wiederum befragt. Dieser weiß zwar wieder die Antwort nicht, liefert aber einen authorativen Nameserver als Delegierung für `icann.com` zurück. Der kann dann die Anfrage mit einem A RR beantworten - `www.icann.com` ist erfolgreich aufgelöst.

(`www.icann.org` wäre natürlich die „richtige" Domain, allerdings nicht so schön plakativ, da die Zone org seit einiger Zeit von Verisign getrennt von einem anderen NIC verwaltet wird, und dieses betreibt eigene Nameserver)

DNS Abfrage mit Platzhalter in der gTLD Zone

Wer genau hingesehen hat, dem ist bestimmt beim vorigen Beispiel mit www.icann.com aufgefallen, das dig immer mit der RR-Klasse „A" aufgerufen wurde. Das war kein Zufall oder Willkür, sondern wird genau so von einem Nameserver auch gemacht. Ungeachtet der Tatsache das er einen Root Nameserver fragt, stellt er immer die Frage mit der RR Klasse die ihm selbst gestellt wurde. Diese Vorgehensweise ist Fluch und Segen zugleich; es provoziert ja fast schon dazu, Unfug damit zu treiben - aber erst diese Eigenheit ermöglicht es überhaupt, „unangebracht" aufgelöste A-RRs zu entlarven.

Die diskutierten Platzhalter Einträge für die Zonen com und net gibt es zwar zum Zeitpunkt der Schriftsetzung dieser Zeilen (noch) nicht mehr/wieder, aber .museum ([MUS]) schafft hier Abhilfe:

```
$ dig @I.root-servers.net. bush.ate.a.pretzel.museum. A muse-
um. 172800 IN NS NS.ICANN.ORG.
$ dig @NS.ICANN.ORG bush.ate.a.pretzel.museum. A bush.ate.
a.pretzel.museum. 180 IN A 195.7.77.20
```

Wie es scheint, kam hier von einem gTLD Server ein A-RR zurück -- schon klar, es wurde ja nach RR Klasse „A" gefragt ... aber wer hat denn erwartet das es gleich der gTLD Server weiß, der ja eine Delegierung retournieren sollte?

Hier sieht man den springenden Punkt ganz klar, den Rettungsanker den uns DNS etwas unbeteiligt zuwirft: Wäre nun das Standardverfahren, Root/gTLD Nameserver immer mit der RR-Klasse „NS" zu befragen (was ja durchaus Sinn machen würde), dann hätte VeriSign vermutlich etwas Grausames wie `* IN NS 23.23.23.23` verbrochen um ihr monetenschwangeres Ziel zu erreichen - und man wäre automatisiert nicht mehr in der Lage, zwischen „Vom-Platzhalter-Delegiert" oder „Nicht-Vom-Platzhalter-Delegiert" zu unterscheiden. So kann man aber wunderbar „Delegiert" und „Nicht-Delegiert" auseinanderklamüsern - und genau hier setzen die „Delegation Only" Patches für BIND9 und anderen DNS Server (wie weiter unten besprochen) an: Sie erwarten von Root/gTLD-Nameservern, beziehungsweise von definierten Zonen, daß sie mit einer Delegierung antworten. Machen sie das nicht, und beantworten die A-RR Abfrage selbst, liefern sie dem anfragenden Resolver das gewohnte `NXDOMAIN` zurück.

Wege zur Normalität

Hier nun ein paar Möglichkeiten, wie man sein `NXDOMAIN` dem Verhalten einiger gTLD Server zum Trotz zurückbekommt. Es gibt auch verschiedene sehr spezifische Patches für Mailserver (für eine Liste siehe [IMP]), doch die erübrigen sich meist wenn man eine oder

zwei der hier vorgestellten Lösungen implementiert hat, deswegen werden sie hier außen vor gelassen.

Delegation-only (BIND 9.2.2, PowerDNS 2.9.12)

Vorteil: Die beste stabile Lösung

Der Delegation-only Patch für 9.2.2 [ISC2] stützt sich genauso wie der für PowerDNS auf Blacklisting, es wird die Delegierung von vorher explizit definierten Zonen erwartet (ansonsten wird NXDOMAIN zurückgeliefert).

BIND9/named.conf [ISC2]:
```
zone „com“ { type delegation-only; }; zone „net“ { type delegation-only; };
```

PowerDNS/recursor.conf [POW1]:
```
delegation-only=com,net
```

(mehr Zonen/gTLDs die eine Nennung in diesem Kontext verdient hätten gibt es übrigens unter [IMP], da hat es auch ein oder zwei Shell Skripte mit welchen man den aktuellen Status der Platzhalter eruieren kann)

Root-Delegation-only (BIND 9.2.3)

Vorteil: Die einzig wahre Lösung (tm)

Nachteil: Derzeit nur in der Entwicklerversion 9.2.3rc4 verfügbar

Bei root-delegation-only „erkennt“ der Nameserver, das er es mit einem gTLD/Root Nameserver zu tun hat und erwartet sich von Haus aus nur Delegierungen von ihm. Sehr wichtig ist aber die Möglichkeit, TLDs davon auszunehmen (Whitelist), da es durchaus welche gibt die mit „guter Absicht“ manchmal (de) oder immer (museum, siehe [MUS]) nicht delegieren.

Im named.conf von bind 9.2.3rc3 würde das (nach einem Beispiel von [ISC2]) in etwa so aussehen:
```
options { root-delegation-only exclude { „ad“; „ar“; „biz“; „cr“; „cu“; „de“; „dm“; „id“; „lu“; „lv“; „md“; „ms“; „museum“; „name“; „no“; „pa“; „pf“; „sr“; „to“; „tw“; „us“; „uy“; }; };
```

Beide Patches sind übrigens zwar in der jeweils aktuellen ISC BIND9 Distribution bereits enthalten, nicht aber aktiviert. Dazu bedarf es des expliziten Eingreifens (Einträge in der named.conf) des Administrators; selbiges bei delegation-only bei PowerDNS (welches laut Entwickler auch bald ein root-delegation-only bekommt).

Zone Forwarding (BIND8, djbdns)

Vorteil: Man muß seinen BIND nicht aktualisieren

Nachteil: Man muß seinen BIND nicht aktualisieren, zusätzliche Verzögerung bei DNS Abfragen, zusätzliche Fehlerquelle

Da oben genannte Patches relativ leicht und schnell zu implementieren waren, hat Paul Vixie sie schon innerhalb von 40h nach Aktivierung der gTLD Platzhalter RRs bereitgestellt. Für BIND8 sollte entweder ein BIND9 her (was definitiv die erste Wahl sein sollte) oder aber folgendes Flickwerk:

BIND8/named.conf [ISC2]:
```
zone „com“ {type forward; forward first; forwarders {62.99.211.22; }; }; zone „net“ {type forward; forward first; forwarders {62.99.211.22; }; };
```

Damit wird der laufende BIND8 dazu veranlaßt, bei Anfragen unterhalb der angegebenen Zonen einen anderen Nameserver zu befragen (so etwas macht sonst Sinn beiSplit Horizon Konstellationen wie etwa Einwahlpools bei ISPs) und diese Antworten dann an den Klienten weiterzureichen. So leitet man einfach alle Anfragen für die Zonen com, net und was einem sonst noch so einfällt ([IMP]) zu einem Nameserver weiter der bereits (Root-)Delegation-only konfiguriert hat (im Beispiel ns1.ucpag.com)

Selbiges funktioniert auch bei dnscache in der djbdns Distribution:`echo 62.99.211.22 > dnscache/root/servers/com echo 62.99.211.22 > dnscache/root/servers/net svc -t dnscache`(Bei djbdns kommt leider suboptimalerweise bei jeder Domain die der befreundete Nameserver nicht auflösen konnte, ein SERVFAIL zurück)

IP-NXDOMAIN Zuweisung (djbdns, PowerDNS)

Vorteil: Besser als Nichts

Nachteil: Nicht sehr viel besser als Nichts

Unter [DJB] und [POW2] findet man Patches gegen djbdns und PowerDNS, wobei es für PowerDNS (siehe oben) eine bessere Lösung gibt. Beide Patches arbeiten IP basiert (d.h. sie wandeln bekannte Platzhalter IP auf `NXDOMAIN` um). Das hat zum Nachteil das sie mehr händisch gepflegt werden müssen (die IP Adressen könnten sich ändern oder es wird einRound Robin eingesetzt).

Es gibt zwar bei [BIN] auch einen Rewrite Patch für BIND8, aber dieser ist IP basiert und produziert statt `NXDOMAIN` ein `SERVFAIL`. Das will man nicht.

LD_PRELOAD gethostbyname() Ersatz

Vorteil: kann auch auf Systemen verwendet werden wo nur Zugriff auf Benutzerebene möglich ist

Nachteil: IP basiert

Unter [SLA] (normalisiert & korrigiert: [LIN]) gibt es einen interessanten Lösungsansatz, zumal er ohne einen Eingriff am Nameserver oder im Superuser-Land auskommt.

Nachdem der Inhalt des Artikels in libverisignfix.c kopiert und BADADDR angepaßt wurde, reicht ein

```
$ gcc -nostartfiles-shared-fPIC-Wl,-soname,libverisignfix.
so.0-o libverisignfix.so libverisignfix.c-ldl
$ export LD_PRELOAD=/home/philip/foo/libverisignfix.so
$ wget http://bush.ate.a.pretzel.museum
--18:14:08-- http://bush.ate.a.pretzel.museum/ => `index.html
Resolving bush.ate.a.pretzel.museum...
failed: Host not found.
```

um in einem beschränkten Rahmen gewohnt arbeiten zu können. Mit Werkzeugen wie ping und traceroute funktioniert das jedoch nicht, da diese suid-root binaries sind und ld.so dann keine preloads von Bibliotheken durchführt die nicht selbst suid-root und in bestimmten Pfaden sind. Auch funktioniert diese Hilfskonstruktion nicht mit Programmen wie Lynx, die einen eigenen Resolver mitbringen statt das `gethostbyname()` der glibc zu verwenden.

NXDOMAIN Recycling

Wenn VeriSign auf diese Weise Geld macht, warum nicht selbst auch in die Vollen greifen? Vielleicht nennt man sogar diesen Typus verblendeter lemmingoider Benutzer sein Eigen, welcher das eigenständige Denken schon gestern abgeschafft hätte und Sitefinder eigentlich ganz nett findet... was auch immer der Grund ist, man kann die Platzhalter Einträge wunderbar für sich selbst und gleichzeitig gegen VeriSign verwenden - gesetzt den Fall, man akzeptiert die fortschreitende Inkontinen^W Inkonsistenz von DNS bedingt durch das eigene Handeln.

Lokaler Server

Man nehme einen Rechner auf welchem die Platzhalter IP-Adressen der verschiedenen dubiosen gTLD (siehe [IMP] für eine Liste) konfiguriert sind und verpasse dem Gateway die richtigen Hostrouten, wie etwa

```
route add -host 64.94.110.11 dev eth0
```

oder verwende NAT:

```
iptables -I PREROUTING -t nat -p tcp -d 64.94.110.11 -j
DNAT --to-destination 192.168.110.42 rdr on fxp0 proto tcp
from any to 64.94.110.11 -> 192.168.110.42
```

Auf 192.168.110.42 (respektive dem Rechner, der die besagten IPs konfiguriert hat) sollte dann ein Webserver mit leerem Document Root und einem 404 Errordocument konfiguriert sein, welches ungefähr so aussieht:

```
<?php header(„Location: http://www.google.at/
search?q=“.$HTTP_SERVER_VARS[‚HTTP_HOST‘]); exit; ?>
```

Mit ein wenig Phantasie und programmiertechnischem Leim kann sich bestimmt jeder wunderbare Applikationen ausdenken die man auf Basis dessen noch stricken könnte. Auch ein Apache VHost mit entsprechender Rewrite Regel kann sinnvoll sein:

```
<VirtualHost 192.168.110.42:80> DocumentRoot /home/www-
search RewriteEngine On RewriteRule ^/(.*) http://www.
google.com/search?q=%{HTTP_HOST} [R,L] </VirtualHost>
```

Proxy

Ähnlich wie die NAT Lösung kann man etwas mit Hilfe eines vorhandenen Squids basteln, dabei ist man aber glücklicherweise von den kaputten Antworten der gTLD Server unabhängig. Man pappt einfach sowas wie

```
<!DOCTYPE HTML PUBLIC „-//W3C//DTD HTML 4.01 Transitional//
EN“ „http://www.w3.org/TR/html4/loose.dtd“> <HTML><HEAD><META
HTTP-EQUIV=“Content-Type“ CONTENT=“text/html; charset=iso-
8859-1“> <META HTTP-EQUIV=“refresh“ content=“5; URL=http://
somedomain/somesearch?q=%H“> <TITLE>ERROR: The requested URL
could not be retrieved </TITLE> </HEAD><BODY> <H2>The reques-
ted Domain does not exist - you will be redirected to http://
somedomain/somesearch?q=%H in 5 seconds.</H2> [...]
```

in `/etc/squid/errors/ERR_DNS_FAIL` (squid neu starten nicht vergessen). Unter `http://somedomain/somesearch` sollte sich ein CGI befinden das mit dem was da übergeben wird (%H ist der Host: Header) auch etwas anfangen kann. Einen kleinen Squid Flicken, der ein klein wenig mehr kann gibt es unter [SQU]. Auf jeden Fall aber muß auf dem Host der den Squid beherbergt ein Nameserver eingetragen sein, der korrekt `NXDOMAIN` zurückliefert. Wie das gemacht wird, wurde weiter oben bereits kurz erwähnt...

Selber Platzhalter einsetzen

Für die Windoze Plattform gibt es ein DNS Server als Bezahlware ([SIM]), welcher statt NXDOMAIN eine beliebige IP-Adresse zurückliefert. Diese Möglichkeit soll PowerDNS angeblich auch bald bekommen. So kann man das Verhalten der gTLD Nameserver lokal wunderbar nachahmen, natürlich sind somit auch die Dienste die weiter oben beschrieben werden damit einsetzbar.

Mißbrauch der Searchorder

Wie dem Leser wahrscheinlich bekannt ist, sollte ein durchschnittlicher Resolver in der Lage sein, eine Suchliste entgegenzunehmen, also eine Liste von Domains die nacheinander an alle DNS Anfragen angehängt werden, bis die Domain erfolgreich aufgelöst wird. Damit kann man dann mit einfachen Hostnamen arbeiten (`monkey` statt `monkey.island.cs`) und der Resolver kümmert sich um den Rest.

Der Autor dieser Zeilen bastelt derzeit an einer PowerDNS Erweiterung [SOD] mit welcher es möglich sein soll, für eine bestimmte Domain (zum Beispiel `search.linuxteam.at`) alles „vorherige“ - also etwa von `www.google.com.search.linuxteam.at` nur `www.google.com` - aufzulösen und das Ergebnis zurückzuliefern; falls es nicht aufgelöst werden kann eben einen beliebigen A-RR. Der Vorteil dieser Methode ist, das es nicht nameserver sondern searchorderabhängig arbeitet. Das heißt, um für seine Schreibfehler-Domains eine Hilfestellung zu bekommen, muß der Benutzer nur etwa search.linuxteam.at in seiner Searchorder hinzufügen. Der Gewinn dabei ist offensichtlich: der Benutzer kann selbst bestimmen welches Service er benutzen möchte und ist in der Lage es mit einem „.“ am Ende der Domain temporär zu umgehen (da ja „`foo.domain.`“ bedeutet, das `foo.domain` explizit als voll qualifiziert gilt und keinen Searchorder-Suffix mehr benötigt) - in diesem Zusammenhang sei am Rande [MS] erwähnt ...

Der praktische Sinn der Übung ist primär dasProof-of-Concept, daß man auch ohne Zupflasterung der gTLD Server mit kaputten Daten und Zwangsbeglückung der Benutzer ein solches Service anbieten kann. Und als kleiner Nebeneffekt können mit Hilfe dieser Krücke Sitefinder-ähnliche Applikationen entwickelt und getestet werden.

Lieber nicht.

Es gibt noch eine Reihe von „Lösungen", von denen möchte man aus dem einen oder anderen Grund Abstand nehmen. Der Vollständigkeit halber sind sie als Negativbeispiele aufgeführt.

BGP Blackhole

Es soll gerüchteweise tatsächlich Carrier gegeben haben, die in einer Art Affekthandlung AS 30060 advertised haben. Da dies zu kleineren Dissonanzen mit Peeringpartnern führte, verschwand dieses Phänomen aber auch wieder sehr schnell. Was aber angeblich noch immer praktiziert wird ist, AS 30060 Netzwerk-lokal zu injecten.

Alternative Nameservernetze

Das ist, als ernsthafte Überlegung für den großflächigen Einsatz, mithin das Dümmste das man sich ausdenken kann. Man wäre immer noch auf die com/net gTLD Server angewiesen (denn gTLD Zonen gibt es nur nach Unterzeichnung von harschen NDAs, wenn überhaupt) und die politische Destabilisierung so wichtiger und etablierter Strukturen wie ICANN wäre unverantwortbar. Deswegen stellen sich auch „Prominente" wie Paul Vixie (ISC/BIND/F-Root) gegen eine solche Lösung [VIX], da sie nur Chaos und Orientierungslosigkeit zur Folge hätten.

IP Filter/Nullrouten

Hin und wieder findet man noch kleinere Provider und Firmennetzwerke wo Administratoren „mal eben"

```
route add -host 64.94.110.11 dev lo iptables -I FORWARD
-s 0/0 -d 64.94.110.11 -j REJECT block drop in inet
from 64.94.110.11/32 to any
```

und dergleichen auf ihren Gateways eingegeben (und vergessen) haben. Das ist zwar als Panikknopf ganz nett und bestimmt gut gemeint; generell empfiehlt sich allerdings eine dauerhafte Lösung von weiter oben.

Holzhammer und Daumschrauben

Einige Carrier und ISP wollten ihre Kunden dazu zwingen, delegation-only auf allen Nameserver einzuschalten. Soweit erkennbar, haben sie sich damit hauptsächlich in die eigenen Füße geschossen.

Was kommt noch?

Wieviel Politik eine Organisation wie ICANN machen kann und was ein Verwaltungsbeauftragter wie Verisign sich erlauben darf ist noch nicht voll ausgetestet, aber man nimmt in Mountain View nach der ersten Standpauke von ICANN [ICA1] und der Community schon wieder den nächsten Anlauf, siehe [NEW]. Bei einem geschätzten Werbungs-Verkaufserlös von 250 000 US$ am Tag(!) ist das auch nicht weiter verwunderlich - und mal ehrlich: der Eine oder Andere würde, solch ein monetäres Potential gegeben, auch nicht weiter denken als bis zur fünften Null.

Es sollte noch erwähnt werden, das die Idee eine Anti-Wildcard-Policy „technisch" zu verankern von Institutionen wie SECSAC ernsthaft in Betracht gezogen wird ([SEC]). Da die Betreiber der Root und gTLD Nameserver durchwegs Techniker sind (die von der VeriSign Aktion auch nicht allzu begeistert waren), müßten/könnten sie diesen Anweisungen, welche optimalerweise in Form eines RFC daherkommen, mit hämischem Schulterzucken folgen. Wenn außerdem die root-delegation-only Option bei jeder Nameserver/Recursor Software standardmäßig aktiviert ist, eben weil es dafür ein MUST in einem neuen DNS RFC gibt, erledigt sich die ganze Geschichte sukzessive von selbst.

Aber vielleicht ringt sich ja auch mal endlich jemand mit Geist und Autorität durch und ersetzt DNS durch eine technisch ausgereifte Lösung. Wobei es hier selbst dem größten Optimisten schwer fällt, glaubhaft Hoffnung auszustrahlen ohne als böswilliger Zyniker verkannt zu werden -honi soit, qui mal y pense.

Literatur/Verweise:

- *[NAN] http://www.merit.edu/mail.archives/nanog*
- [ICA1] http://www.icann.org/correspondence/twomey-to-lewis-03oct03.htm
- [ICA2] http://forum.icann.org/wildcard-comments/index.html
- [RFC] http://www.ietf.org/iesg/1rfc_index.txt
- [VER1] http://www.verisign.com/resources/gd/sitefinder/implementation.pdf
- [VER2] http://www.verisign.com/resources/gd/sitefinder/bestpractices.pdf
- [NEW] http://news.com.com/2100-1038_3-5092133.html
- [MUS] http://musedoma.museum/policy/wildcard/
- [ISC1] http://www.isc.org/
- [ISC2] http://www.isc.org/products/BIND/delegation-only.html
- [BIN] http://achurch.org/bind-verisign-patch.html
- [DJB] http://tinydns.org/djbdns-1.05-ignoreip2.patch
- [POW1] http://downloads.powerdns.com/documentation/html/built-in-recursor.html#VERISIGN
- [POW2] http://www.imperialviolet.org/binary/powerdns.patch
- [SLA] http://slashdot.org/~Dwonis/journal/45997
- [LIN] http://linuxteam.at/philip/stuff/code/libverisignfix.c
- [IMP] http://www.imperialviolet.org/dnsfix.html
- [VIX] http://www.merit.edu/mail.archives/nanog/2003-09/msg00592.html
- [MS] http://www.microsoft.com.
- [SOD] http://linuxteam.at/philip/code/sodns
- [SQU] http://www.merit.edu/mail.archives/nanog/2003-10/msg00152.html
- [SEC] http://www.icann.org/correspondence/secsac-to-board-22sep03.htm
- [SIM] http://www.simpledns.com

Biometrie in Ausweisdokumenten

von starbug <starbug@berlin.ccc.de>, sill <lisa@berlin.ccc.de> und

Was soll das: elektronisch erfasste und gespeicherte biometrische Merkmale in Ausweisdokumenten? Moeglichst in allen. Weltweit. Wozu brauchen wir das?

Aber fangen wir mal von vorne an: Worum geht es? Es geht darum, Ausweisdokumente wie Personalausweise, Visa und Reisepaesse mit elektronisch erfassten und gespeicherten Merkmalen auszustatten, die dann auch elektronisch ueberprueft werden sollen. Wohlgemerkt: es handelt sich dabei um eine Ergaenzung. Biometrische Merkmale haben wir ja alle schon lange in unseren Paessen und Ausweisen: Foto, Unterschrift, Angaben ueber Groesse, Geschlecht und Augenfarbe. Fingerabdruecke gibt es seit dem Untergang des Dritten Reichs nicht mehr im Personalausweis. Was hatten sich die Gruender der Bundesrepublik Deutschland dabei gedacht, damals, als sie entschieden, dass Fingerabdruecke nichts im Personalausweis zu suchen haben? Irgendetwas muss sie ja bewogen haben, diese Entscheidung sogar klar und deutlich per Gesetz festzuhalten. Aber klar, waren andere Zeiten damals.

Also, zurueck zu den biometrischen Merkmalen in Ausweisdokumenten. Wenn wir nun schon Biometrie im Ausweis haben, was ist dann der Unterschied zwischen dem, was wir jetzt haben und dem, was bald kommen soll? Einfache Sache. Die neuen biometrischen Merkmale werden elektronisch erfasst, gespeichert und abgeglichen. Elektronisch erfasste Daten kann man bekanntlich sehr viel einfacher aufbewahren, verarbeiten und mit anderen Daten verknuepfen. Das ist gut fuer den Staat, und schlecht fuer diejenigen Buerger, die um ihre Privatsphaere besorgt sind.

Praemisse: Jeder Staat hat ein grosses Interesse daran, moeglichst genau ueber seine Buerger Bescheid zu wissen. Fuer Planungszwecke und um sicherzustellen, dass alles seine Ordnung hat. Elektronisch erfasste biometrische Merkmale versprechen nun, dass sie dem Staat ermoeglichen, besser ueber seine Buerger bescheidzuwissen, und auch ueber jene Nicht-Buerger, die sich auf dem Staatsterritorium aufhalten. Als Grund fuer die Einfuehrung zusaetzlicher Merkmale wird genannt, dass elektronisch erfasste biometrische Merkmale Ausweisdokumente faelschungssicherer machen. (Der Stammtisch-Preis des Monats geht an dieser Stelle an Herrn Bosbach von der CDU fuer die Aeusserung, dass “kein Buerger einen Rechtsanspruch auf einen leicht fälschbaren Ausweis besitzt”. Herzlichen Glueckwunsch.) Hat jemand die Statistiken gesehen, in denen steht, dass es Probleme mit Faelschungen von Personalausweisen gibt? Ich nicht. Moeglicherweise liegt das daran, dass es sie nicht gibt, denn nach Auskunft der Bundesdruckerei gehoeren die deutschen Ausweisdokumente zu den sichersten weltweit.

Allerdings gibt es in Deutschland tatsaechlich ein Problem mit Personaldokumenten: Menschen haben bekanntermassen Probleme, Angehoerige anderer Ethnien auseinanderzuhalten. Das machen sich auch Schlepperbanden zunutze. Wollen sie einen Asiaten ueber die deutsche Grenze bringen, “mieten” sie einen Personalausweis eines deutschen Staatsbuergers, der ebenfalls augenscheinlich asiatisch-staemmig ist. Das Problem ist hier also, dass Menschen in bestimmten Faellen nicht in der Lage sind, einen Ausweis eindeutig seinem Inhaber zuzuordnen, also die Frage zu klaeren: Ist der auf dem Ausweis beschriebene und abgebildete Mensch derjenige, der vor mir steht und behauptet, Inhaber dieses Ausweises zu sein. Dieses Problem der eindeutigen Zuordnung tritt nicht nur im Zusammenhang mit den verschiedenen Ethnien auf, sondern auch und vor allem durch Ermuedung des Kontrollpersonals. Nur: dieses Problem kann mit den heutigen Personalausweisen schon geloest werden. Dem Kontrollpersonal wird dabei ein Computer zur Seite gestellt, der mit einem Scanner und einer Kamera verbunden ist. Ueber die Kamera wird das Gesicht des Ausweisinhabers aufgenommen, ueber den Scanner wird das Foto auf dem Ausweis eingelesen. Mittels einer Gesichtserkennung wird dann ueberprueft, ob die beiden vorgelegten Gesichter uebereinstimmen. Ist das Ergebnis negativ, wird die Entscheidung an die danebensitzende Kontrollperson weitergereicht. Und das alles kann ganz ohne Datenbanken, ganz ohne zusaetzliche biometrische Merkmale passieren. Da es also keine nennenswerten Probleme mit Faelschungen deutscher Personalausweise gibt, und da der Missbrauch von Personalausweisen durch Unberechtigte ganz ohne Veraenderungen der jetzigen Dokumente eingedaemmt werden kann - wozu brauchen wir zusaetzliche Sicherungen, zusaetzliche Merkmale? Wozu brauchen wir weitere elektronische oder nicht-elektronische biometrische Merkmale im Personalausweis? Die Risiken solcher elektronisch gespeicherter Merkmale sind bekannt: Wecken von Begehrlickeiten und Missbrauch

durch Bedarfstraeger und "Insider". Dass Technologie und Daten, die einmal existieren, frueher oder spaeter auch - mit oder ohne gesetzliche Grundlage - genutzt werden, duerfte spaetestens nach dem Trubel um IMSI-Catcher im Polizeieinsatz jedem klar sein.

Weiterhin ist bisher in keiner Weise hinreichend gesichert ist, dass die biometrischen Systeme fuer solche grossen Anwendungen ausreichend zuverlaessig und sicher sind. Man erinnere sich: Es geht hierbei um Anwendungen fuer Millionen von Benutzern, fuer die es u.U. existenziell ist, dass die Systeme zuverlaessig funktionieren. Biometrische Systeme wurden noch nie auch nur in annaehernd so grossen Anwendungen getestet.

Einige Probleme, die sich bei derartig grossen Anwendungen auftun, sind dennoch schon absehbar. Es ist hinlaenglich bekannt, dass fuer jedes biometrische Merkmal bei einem gewissen Prozentsatz der Nutzerpopulation dieses Merkmal nicht in hinreichend ausgepraegt ist. Beim Fingerabdruck zum Beispiel liegt dieser Prozentsatz bei bei ca. 5%. 5%! Das heisst jeder 20ste kann gar nicht in das System eingegliedert werden oder wird bei jeder Kontrolle aufs neue Schwierigkeiten haben. Bei einer Nutzerpopulation von 80 Millionen Bundesbuergern heisst das, dass 4 Millionen Buerger bei einer Identifikation durch den Fingerabdruck Probleme haetten. Fuer andere Systeme sehen die Werte teilweise besser, teilweise noch schlechter aus, fuer manche sind sie auch mangels Ausgereiftheit der Technologie noch gar nicht bekannt. Und bei den obengenannten Problemen sind kurzfristige Aenderungen durch beispielsweise Verschmutzung oder Verletzung, die jeder taeglich erfahren kann, noch nicht eingeschlossen. Wir haben von Seiten der Regierung noch keine Verlautbarungen gefunden, wie mit diesen Problemen umgegangen werden soll.

Ausweise mit Fingerabdrücken hatten wir schonmal in Deutschland. 1940...

Nicht zu vergessen sind zu guter letzt die Kosten. Da die beliebtesten Argumente fuer eine Einfuehrung zusaetzlicher biometrischer Merkmale im Personalausweis bereits widerlegt wurden, stellt sich die Frage: Warum meinen Schily und Beckstein, dafuer Millionen von Euro an Steuergeldern investieren zu duerfen?

Fairerweise muss gesagt werden, dass die Regierung in Deutschland auch starken Druck von aussen erfaehrt, namentlich von seiten der USA. Geht es nach ihnen, werden im Herbst 2004 all jene Nationen zusaetzliche biometrische Merkmale in ihren Ausweisdokumenten eingefuehrt haben, deren Buerger bisher ohne Visum in die USA einreisen koennen. Gefordert sind dabei elektronische abgelegte Fotos und Fingerabdruecke. Die Buerger jener Staaten, die diese Voraussetzungen nicht erfuellen, muessen ab dem Stichdatum fuer die Einreise in die USA wieder ein Visum beantragen - das dann natuerlich seinerseits die geforderten Merkmale enthaelt. Aber bitte, Herr Schily, koennten Sie nicht unsere Buergerrechte und unsere Steuergelder gegen das Sicherheitsbeduerfnis der Amerikaner verteidigen, statt im Schweinsgalopp eine Technologie einzufuehren, die genauso teuer wie umstritten ist?

Sabbern für die Polizei

von nitraM <martin@weltregierung.de>

Bildquelle: Forschungszentrum Jülich

Kaum ein Tag vergeht, an dem in den Medien nicht über die positiven Folgen der DNA-Analyse berichtet wird. Erfolge werden betont, Risiken werden z.T. zu abstrakt und schwammig dargestellt. Schlussendlich bleibt das Gefühl hängen, DNA-Fingerprinting sei die Wunderwaffe im Bereich Strafverfolgung. Und dieses Gefühl wird bewusst durch die Politik aufgegriffen.

Pressesprecher der Behörden teilen gerne mit, daß Täter anhand von DNA-Spuren überführt wurden. Das schwappt dann auch so ungefiltert in die Berichterstattung. Erklärende Informationen beschränken sich oft auf Angaben über allgemeine Dinge aus dem Bereich Genetik oder aktuelle Statistiken vom BKA. Punkte wie Datenspeicherung, Weitergabe von Daten oder Beweislastumkehr werden kaum thematisiert. Stattdessen steigt die Akzeptanz der Methode zum Aufspüren von Verbrechern und implizit auch die Akzeptanz zur Speicherung. Interpol betrachtet das so: "Once again, positive briefings of the media will help counter any such fears and ensuring that successful prosecutions in high profile cases are given maximum publicity will create a better understanding of the incontestable aspects of the science. [...] once a database has been established and is in operation, the need for effective publicity will still exists. For example, politicians will need to be re-assured that their money has been well spent and that the best possible value for money has been achieved, the lack of immediate results may require regular explanation." [1]

Die*"Incontestable aspects of the science"*sind in der Diskussion in mehrfacher Hinsicht bedeutend: Zum einen suggerieren bei der Benennung von Übereinstimmungswahrscheinlichkeiten von DNA-Fingerprints gigantische Verhältnisse wie 1:40.000.000 die Sicherheit der Methode. Journalisten greifen das mitunter auf und schreiben vereinfachte Formulierungen wie "mit an Sicherheit grenzender Wahrscheinlichkeit" oder "wissenschaftlich erwiesen" in ihre Artikel. Wie die Wahrscheinlichkeiten berechnet werden ist äußerst komplex - wahrscheinlich so komplex, dass nichtmal alle Genetiker diese Angaben berechnen können. Das Modell hinter diesen Zahlenverhältnissen basiert auf der Populationsgenetik. Die Varianz der beim Fingerprinting erfassten Merkmale ist bei einzelnen Ethnizitäten verschieden. Entsprechende Statistiken müssen in die Bewertung integriert werden. Die Details zur Übereinstimmungswahrscheinlichkeit und Fehlerrechnung spiegeln sich natürlich nicht in der öffentlichen Diskussion wider. Und eben sowenig im Gerichtssaal - die Prüfung von Beweismitteln unterliegt dort Gutachtern. Das ist soweit ausreichend, birgt allerdings in der Übertragung auf andere Anwendung folgendes Problem: Es besteht ein gravierender Unterschied darin, ob Proben von einem Verdächtigen mit Spuren vom Tatort verglichen werden (Verifikation) oder ob Spuren gegen eine Datenbank abgeglichen werden (Identifikation). Allein

durch das statistische Rauschen können in einer großen Datenbank mehrere Personen den gleichen Hashwert haben. Ein Abgleich einer Spur gegen die Datenbank kann sogenannte "cold hits" also falsch positive Resultate bringen. Damit fallen Personen evtl. in einen Kreis von Verdächtigten. Diese dramatische Verschiebung der Wahrscheinlichkeiten (je nach Anwendung) wird oft unter den Tisch gekehrt. Betrachtet man die rechtliche/politische Situation in Deutschland, könnte man dazu zynisch bemerken, dass das Problem der cold hits nicht als sonderlich relevant anerkannt ist, da in den DNA-Datenbanken sowieso ehemalige Täter gespeichert sind - also Personen, die am Rand der Gesellschaft stehen, deren moralischer Anspruch auf Grundrechte als eingeschränkt angesehen wird.

Bezüglich der Arbeit der Ermittler kann sich die "Nichtanfechtbarkeit" der DNA-Analyse als ultimatives Mittel zur Überführung von Verbrechern darstellen. Das Polizeipräsidium Wiesbaden formulierte die Situation Anfang 1997 (also ein Jahr vor der Einführung der Gendatenbank durch Manfred Kanther) in einem vertraulichen Schriftstück so: "Der Personenbeweis, insbesondere ein Geständnis, gestaltet sich im Ermittlungsverfahren zunehmend schwieriger, da der Tatverdächtige mehr und mehr von seinem Aussageverweigerungsrecht Gebrauch macht. Um so größere Bedeutung kommt daher bei der polizeilichen Ermittlungsarbeit dem Sachbeweis zu." [2] D.h. wenn die Beweislage zu dünn ist, die Strafverfolgungsbehörden den Beschuldigten mit wissenschaftlich fundierten Untersuchungsergebnissen konfrontieren können, dann - so das Kalkül der Ermittler - wird der Beschuldigte von sich aus gestehen.

Weitere Probleme lassen sich bei der Weitergabe von DNA-Fingerprints ausmachen. Kritiker bemängelten die unzureichend geklärten Grenzen der Verwendung von Profilen in § 3 des DNA-Identitätsfeststellungsgesetzes. Da heisst es zwar*"Auskünfte dürfen nur für Zwecke eines Strafverfahrens, der Gefahrenabwehr und der internationalen Rechtshilfe hierfür erteilt werden."* In der Beschlussempfehlung des Rechtsausschusses im Deutschen Bundestag kommt jedoch zum Ausdruck, dass die Regelungen sehr weit auszulegen sind: "Der Begriff des "Strafverfahrens" ist in einem weiten Sinne zu verstehen. Er umfaßt auch Zwecke des Strafvollzuges, der Strafvollstreckung und von Gnadenverfahren. Der Begriff der Gefahrenabwehr stellt nicht auf die Abwehr konkreter Gefahren ab, sondern ist vielmehr - in Abgrenzung zu anderen nicht justitiellen oder polizeilichen Zwecken - im weiten Sinne zu verstehen. Eingeschlossen ist dabei insbesondere die Datenübermittlung im Rahmen der informationellen Zusammenarbeit einschließlich der internationalen Zusammenarbeit. Der Begriff der internationalen Rechtshilfe ist besonders genannt, weil der Begriff der Rechtshilfe nicht ohne weiteres unter den Begriff Strafverfahren zu subsumieren ist und die justitielle Rechtshilfe überdies in § 3 BKAG ausgenommen ist." [3] [BT-Drucksache 13/11116 vom 22.06.1998] In diesem Zusammenhang muß erwähnt werden, dass die Vergleichbarkeit von DNA-Profilen international weitgehend möglich ist, da im Wesentlichen die gleichen Abschnitte auf der DNA untersucht werden. Siehe hier [4] .

Mythos "nicht-kodierende Abschnitte"

Auf Grundlage von §81a (3) Strafprozeßordnung dürfen Beschuldigten Blutproben entnommen und nach §81e (1) molekulargenetisch untersucht werden. Absatz 2 regelt die Behandlung von Spurenmaterial. In der Theorie dürfen nur nicht-kodierende DNA-Abschnitte betrachtet werden, so stellt es sich der Gesetzgeber vor. In der Praxis sieht das mitunter doch anders aus. Von organischen Spuren wird regelmäßig das Geschlecht bestimmt. Auch die Blutgruppe ergibt sich aus DNA-Spuren. Der Markt bietet mittlerweile Testkits für die Feststellung der Augenfarbe an. Diese funktionieren noch nicht exakt, die Niederlande und die Schweiz haben vorsorglich schon ihre Regelungen angepasst [Bürgerrechte und Polizei, 3/2003], um derartige Informationen nutzen zu können. Ferner wird als klassisches Beispiel, welche Zusatzinformationen aus Untersuchungen sich gar nicht ignorieren lassen, oft Trisomie 21 genannt.

Was für Analysen in Zukunft technisch möglich sind, wird sich zeigen. Es wäre naiv zu glauben, dass Spuren nicht umfassend analysiert werden, wenn die technischen Möglichkeiten bestehen und der Druck auf Ermittler groß genug ist. Die Befürchtung wird nicht geringer, wenn man lesen darf, dass das BKA eigene Analysegeräte betreibt [quelle vergessen], um Material zu untersuchen.

Bei der Bewertung von DNA-Analyseergebnissen muß stets zwischen den Wahrscheinlichkeitsleveln differenziert werden. Das BKA kann auf Basis von DNA-Spuren bereits etwa 30 Bevölkerungsgruppen aufgrund der Allelhäufigkeit unterscheiden. Es handelt sich jedoch um Wahrscheinlichkeitsaussagen, die für Ermittlungen eventuell nur von begrenztem Wert sind. Dagegen wäre eine halbwegs sichere Information über die Augenfarbe schon sehr brauchbar.

Einen Vorgeschmack auf zukünftige Entdeckungen konnten britische Forscher von der Universität Leicester beisteuern. Diese entdeckten einen möglichen Zusammenhang zwischen dem Marker TH01, der in der Nähe des Gens für Insulin liegt und der Veranlagung zu Diabetes-I [5] . Wie gesagt, die Zusammenhänge sind vage. Dennoch gibt es Anzeichen, dass auch nichtkodierende Bereiche Metainformationen bergen.

Massenuntersuchungen

Im Frühjahr 1998 ging der Mordfall Christina Nytsch durch die Presse, der in beträchtlichem Maße zur weiteren Weichenstellung beigetragen hat. Zur Aufklärung des Mordfalls führte die Polizei Anfang April den erste Massengentest in der deutschen Kriminalgeschichte durch. Von den 17900 gesammelten Speichelproben,

wurden 1366 Männer (darunter 600 bekannte Sexualtäter) nach § 81 a, e und f StPO zur Abgabe verpflichtet. Lediglich vier Männer verweigerten die Entnahme. Sie wurden auch nicht mehr vom Gericht zur Abgabe verpflichtet, da der Täter bereits durch freiwillige Abgabe von Speichel identifiziert wurde.

Auf politischer Ebene geschah folgendes: Der damalige Bundesinnenminister Manfred Kanther ordnete die Errichtung einer Gendatenbank beim BKA an. Obwohl Kanther Jura studiert hat und selbst die Abnahme von Fingerabdrücken gesetzlich geregelt ist, hielt er eine besondere Gesetzesgrundlage für unnötig. Er leitete die Kompetenz zur Speicherung von genetischen Codes schlicht aus dem BKAG ab. Das Problem mit der fehlenden Gesetzesgrundlage wurde im Nachhinein geregelt. Kanther hat sich Rückendeckung von den Landesinnenministern geben lassen, damit die entsprechenden Gesetzesänderungen durch den legislativen Apparat abgesegnet werden. Das DNA-Identitätsfeststellungsgesetz trat am 25. Juni 1998 in Kraft. Es entsprach weitgehend den eingereichten Vorschlägen von CDU/CSU und der FDP. Mittlerweile wurde in Deutschland zu mehreren Massenuntersuchungen geladen, ohne großartige Berichterstattung in der bundesweiten Presse.

Die Idee hinter einer Reihenuntersuchung ist klar: Ist der Täter in der zu untersuchenden Gruppe, wird er irgendwie reagieren. Entweder er verweigert die freiwillige Abgabe, dann ist der in der ganz kleinen Gruppe von "verdächtigen Verweigerern" - oder er wird überführt. Da die Aufklärung einer Straftat im kollektiven Interesse ist, kooperiert die Mehrheit. Eine Minderheit gerät öffentlich unter Druck. Im Babyklappenmordfall [dsb] [6] wollte die Polizei DNA-Material vom Personal eines Krankenhauses, da die Täter im Umkreis des Klinikums vermutet wurden. Ob noch von Freiwilligkeit der Abgabe gesprochen werden darf, wenn z.B. Arbeitgeber Druck auf Angestellte ausüben würden, ist fraglich.

Nach dem DNA-Vergleich müssen die Speichelproben vernichtet werden. Ebenso die Fingerprints, sofern sie nicht vom Täter stammen, denn ökonomisch sinnvoll wäre natürlich die Speicherung schon. Selbst bei automatisierten Reihenuntersuchungen betragen die Kosten pro Abgleich etwa 50 Euro.

Fehler in der Matrix

Das sich schon mal Probleme beim "DNA-Rastern" ergeben können, zeigen die beiden folgenden Fälle. Letzterer ist nach meinem Kenntnissen nicht abschließend geklärt. Im April 1999 hat die britische Polizei ein DNA-Profil basierend auf sechs Loci gegen die National DNA Database (NDNAD) getestet, um einen Einbruch aufzuklären. Die Polizei fand das Profil eines Mannes, der etwa 200 Meilen vom Tatort entfernt lebte und dessen DNA-Fingerabdruck in der Datenbank gespeichert wurde, nachdem er im Zusammenhang mit einem Familienstreit seine Tochter geschlagen hat. Trotz Alibi und Unschuldsbeteuerung wurde der Verdächtige verhaftet, der zudem noch an Parkinson im fortgeschrittenen Stadium litt und somit unfähig war, ein Fahrzeug zu steuern. Die Wahrscheinlichkeit, daß die Übereinstimmung des DNA-Fingerprints zufällig ist, wurde auf 1 zu 37 Millionen ermittelt.

Monate später ließen die Behörden den Mann wieder frei, nachdem der Test unter Zuhilfenahme vier weiterer Loci wiederholt wurde und in den hinzugenommenen Merkmalen keine Übereinstimmung mit der Spuren vom Tatort vorlag. forensic evidence [7]

Ein anderer Fall ging letztes Jahr durch die deutsche Presse: Die Polizei entdeckte auf dem Fahrrad einer am 27.09.1997 in Hannover ermordeten Rentnerin Spuren von DNA. Die Analyse führte zum Verdächtigen Andreas S, der wegen begangener und versuchter Vergewaltigung seit April 1997 in einer ausbruchssicheren psychiatrischen Anstalt sitzt. [Frankfurter Rundschau vom 01.07.03; Der Spiegel]

Wie derartige Spurenverwirrungen entstehen, steht in den Sternen. Die Gefahr der Kontamination ist prinzipiell groß. Bei derzeit verwendeten Fingerprinting-Verfahren, werden nur wenige intakte Zellen benötigt, deren DNA via PCR-Verfahren "amplifiziert" wird - Verunreinigungen gleich mit.

Ausblick

Solange der in der StPO verankerten Richtervorbehalt bei der Probenentnahme noch nicht gekippt ist und der Straftatenkatalog zum DNA-Identitätsfeststellungsgesetz nicht vollends ausufert, wird die Erfassung der gesamten Bevölkerung nicht kommen. Das BVG hat am 15. März 2001 erklärt, dass die die Feststellung, Speicherung und Verwendung des DNA-Identifizierungsmusters das Recht auf informationelle Selbstbestimmung einschränkt. Mit diesem Urteil lässt sich das Abgleichen bzw. Speichern von Kleinkriminellen vorerst nicht verargumentieren.

[1] *http://www.interpol.int/Public/Forensic/dna/handbook.asp*

[2] *http://www.infolinks.de/medien/geheim/1998/03/004.htm*

[3] *http://dip.bundestag.de/btd/13/111/1311115.pdf*

[4] *https://www.weltregierung.de/dna/used_loci.html*

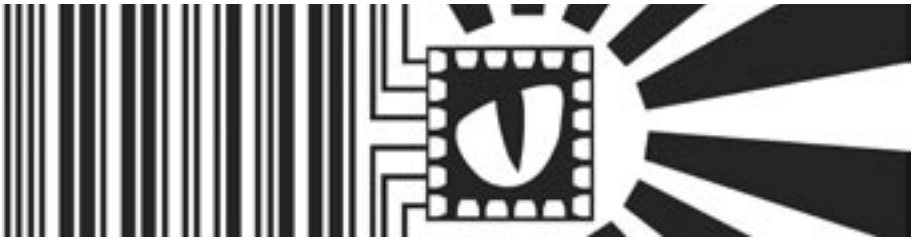
[5] *http://www.netzeitung.de/genundmensch/142677.html*

[6] *http://www.datenschutz-berlin.de/jahresbe/02/anl/33d1.htm*

[7] *http://www.forensic-evidence.com/site/EVID/EL_DNAerror.html*

Future Store: Experiment abbrechen!

von Frank Rosengart <frank@rosengart.de>



Kunden des zur Metro Gruppe gehörenden Future Store in Rheinberg können mit Hilfe von Funkchips während ihres Einkaufes ausgespäht werden. So lautet der Vorwurf des Bielefelder FoeBuD nach einem gemeinsamen Besuch mit der amerikanischen Verbaucherschützerin Katherine Albrecht (CASPIAN, Boston/USA) in dem "Supermarkt der Zukunft" bei Duisburg.

Wer den mit viel Technik und Antennen vollgestopften Extra-Supermarkt betritt, wird am Eingang erstmal durchleuchtet. Eine Schleuse versucht, die vom Kunden mitgeführte Payback-Karte per Funksignal zu erkennen und damit die Einkaufsgewohnheiten oder einen gespeicherten Einkaufszettel im System abzurufen. Mittels Bordcomputer am Einkaufswagen wird der Kunde dann durch den Laden gelotst. Aber auch ausgewählte Artikel tragen die kleinen "Schnüffelchips" auf der Verpackung. Anders als beim bisherigen Strichcode, der sich auf allen Verpackungen befindet, muss die Ware nicht mehr über einen Scanner gezogen werden, sondern kann schon im Einkaufswagen oder bei der Entnahme aus dem Regal registriert werden.

Die dafür verwendete Technik heißt Radio Frequency Identification (RFID)Die Funkchips sollten nach Wünschen der Industrie "Green Chips" genannt werden, um den Kosumenten ein unbeschwertes Einkaufsvergnügen vorzugaukeln.und anstelle des Strichcodes werden millimetergroße Chips mit Antenne in die Produktverpackung eingebaut. Sie sollen den Einkauf erleichtern und den Firmen bei der Warenlogistik helfen. Das zeitraubende Anstehen an der Kasse entfällt. Der große Unterschied zum bisherigen Strichcode ist, dass jeder Chip mit einer eigenen Kennung ausgestattet ist. Jede Packung Philadelphia-Käse hat also eine weltweit eindeutige Nummer und kann so mit einer Person über die Kundenkarte oder die ec-Karte verknüpft werden.

Aber auch die in Deutschland beliebte Rabattkarte Payback enthält einen RFID-Chip. Das ergab eine Röntgenuntersuchung der vom Future Store herausgegebenen Karte. "Damit wird eine unzulässige Zuordnung von Daten der RFID-Chips auf Waren zu Personen möglich", so Rena Tangens vom FoeBuD. "Die Metro informiert ihre Kunden nicht ausreichend über die Möglichkeiten, wie ihr Kaufverhalten im Future Store ausspioniert werden kann."

Besonders problematisch sind die RFID-Chips, weil sich der Kunde gegen die Bespitzelung im Supermarkt nicht wehren kann. Da die Kundenkarte per Funk ausgelesen wird, kann dies sogar völlig unbemerkt geschehen.

Die Metro Gruppe verspricht zwar, dass die Daten der Funkchips beim Verlassen des Ladens gelöscht werden, aber eine Untersuchung durch FoeBuD ergab, dass die eindeutige Kennung der Artikel auch nach dem Einkauf noch im Chip gespeichert ist.

"Der im Future Store durchgeführte Feldversuch ist außer Kontrolle geraten" stellt Rena Tangens fest, "er muss abgebrochen werden, bis Regeln und Gesetze für eine gesellschaftsverträgliche Einführung dieser Technologie gefunden worden sind." Verbraucher würden durch die angeblichen Vorteile der RFID-Technik geblendet und über die Folgen für ihre Privatsphäre im Unklaren gelassen. Um die Auswirkungen der Technologie und einen fairen Umgang damit zu untersuchen, soll von der Metro Gruppe ein Gremium aus Datenschützern, Verbraucherorganisationen, Umweltschützern (Elektrosmog), Arbeits- und Bürgerrechtlern finanziert werden.

FoeBuD zu RFID [1]

[1] *http://www.foebud.org/rfid*

Kontrollierter Ausstieg aus UNIX bis 2038. Ein Masterplan.

von Andreas Bogk <andreas@andreas.org>

Der momentane Stand der Technik im Bereich Betriebssysteme hat sich in der Praxis als sicherheitstechnisch problematisch erwiesen. Es hat sich empirisch gezeigt, daß bestimmte Fehlerklassen, die zu hohen Sicherheitsrisiken führen, immer wieder auftauchen und durch Maßnahmen der Qualitätssicherung nicht vollständig auszuschließen sind.

Die wichtigsten Klassen von Problemen in diesem Bereich sind Überläufe von Vektoren durch ungenügende Begrenzungsüberprüfungen (buffer overflows), Zugriffsfehler durch mehrfache Freigabe von dynamisch angefordertem Speicher (double free), sowie Überlauffehler durch ungenügend abgesicherte Typwandlungen (casts). Diese führen in der Regel zu Abstürzen, lassen sich aber durch geschickte Wahl der Eingabedaten oftmals dazu ausnutzen, beliebigen Code eines Angreifers auszuführen (exploit).

Solche Fehler entstehen durch nicht ausreichend sorgfältigen Umgang mit den Mitteln der Programmiersprachen C oder C++, die in modernen Systemen in großem Unfang eingesetzt werden. Programmierfehler lassen sich niemals vollständig vermeiden, führen aber in diesen Systemen in der Regel dazu, daß der Fehler sich rasch über den gesamten betroffenen Prozeß ausbreitet. Ein Exploit eines solchen Bugs übernimmt weiterhin die vollen Rechte des Prozesses und bietet einem Angreifer so eine breite Fläche, um auch den Rest des Systems unter seine Kontrolle zu bringen.

Ist der Kernel selbst von einem solchen Bug betroffen, ist direkt die gesamte Systemintegrität gefährdet. Auch ein Fehler in einer vergleichsweise unwichtigen Komponente betrifft direkt auch alle sicherheitskritischen Bereiche des Kernels.

Technologien zur Vermeidung solcher Fehlerklassen, namentlich starke Typisierung (strong typing), automatische Speicherverwaltung (garbage collection) und Begrenzungsüberprüfungen (bounds checking) sind seit Jahrzehnten bekannt und sind fundamentaler Bestandteil verschiedenster Programmiersprachen (Lisp, Smalltalk, ML). Es gab historisch mehrere Betriebssysteme, die in solchen Sprachen geschrieben wurden; das System der Lisp-Maschinen sei hier als Beispiel genannt.

Natürlich werden auch in anderen Sprachen geschriebene Systeme Bugs haben. Der entscheidende qualitative Unterschied liegt darin, daß alle Fehlersituationen, die auftreten können, zu Laufzeitfehlern führen. Somit bleibt der Fehler lokalisiert, es kann kein Übergriff auf andere Module jenseits der vereinbarten APIs mehr stattfinden. Die Möglichkeit der Ausnutzung von Bugs durch einen Angreifer werden stark eingeschränkt, oftmals sogar komplett verhindert.

Ebenso hat sich gezeigt, daß eine Sprache mit mächtigeren Abstraktionen, als C sie bietet, zu lesbarerem, kompakterem und damit wartbarerem, weniger bugbehaftetem Code führt. Funktionen höherer Ordnung (higher order functions), lexikalische Abschlüsse (closures) und Makros, die nicht aus Textsubstitutionen beruhen, sondern weitere Produktionen zur Grammatik hinzufügen, sowie Objektorientierung mit generischen Funktionen mit dynamischen Mehrfachdispatch seien hier als die Wesentlichen genannt.

Historisch gesehen gibt es diverse Gründe, die dazu geführt haben, daß Systeme in C sich durchgesetzt haben. Keiner davon hält jedoch bei näherer Betrachtung als nach wie vor gültig stand. Dazu hat unter anderem der wissenschaftliche Fortschritt auf dem Gebiet des Compilerbaus geführt, durch den zum Beispiel die Geschwindigkeit des erzeugten Codes durchaus mit C mithalten kann. Ebenso lagen bei vielen technisch überlegenen Systemen die Gründe fürs Scheitern in der wirtschaftlichen Situation, insbesondere wenn der Source Code nicht frei war.

Es ist nach Meinung des Autors also an der Zeit, noch einmal ein Betriebssystem von Grund auf neu zu schreiben. Ein wichtiges Merkmal ist die freie Verfügbarkeit des Source Codes, um eine unabhängige Überprüfung und Fehlerbehebung zu ermöglichen, und um ein Überleben des Systems unabhängig vom wirtschaftlichen Erfolg einer einzelnen Firma zu machen.

Weiterhin muß eine Programmiersprache zum Einsatz kommen, die die beschriebenen defensiven Mechanismen gegen Sicherheits- und Stabilitätsprobleme unterstützt, und deren Einhaltung in nicht privilegierten Systemmodulen erzwingt.

Nicht zuletzt muß das System auf handelsüblicher Hardware laufen, und einen Weg bieten, existierende Software in unsicheren Technologien in einer Sandbox laufen zu lassen, ohne damit den sicheren Teil des Systems zu gefährden.

Nach umfrangreichen Studien der Geschichte der Betriebssysteme und Programmiersprachen ist eine Auswahl einer geeigneten Plattform getroffen worden. Zur Abstraktion des Prozessors kommt der L4-Microkernel in der Implementierung "Pistachio" der Universität Karlsruhe zum Einsatz [1] . Darauf läuft dann ein in Dylan geschriebenes System, in der Implementierung Gwydion Dylan [2] .

Dylan ist eine dynamisch und stark typisierte, objektorientierte Sprache mit Funktionen höherer Ordnung. Eine optionale statische Typsierung von Bindungen ermöglicht es dem Optimierer, bestimmte Typchecks und Methodendispatches zur Compile-Zeit zu erledigen, und damit in kritischen Code-Sektionen die Ausführgeschwindigkeit zu erhöhen (optimistic type inferencing). Dylan ist in vielen Aspekten mit Lisp verwandt, hat in Gegensatz zu diesem jedoch eine Pascal-artige Syntax, die sicherlich vielen Programmierern vertrauter ist.

Sämtliche nicht von L4 bereitgestellten Mechanismen: Speicherverwaltung, Gerätetreiber, Netzwerkprotokolle, Systemdienste etc. werden in Dylan implementiert. Der Adreßbereich ist für alle Prozesse einheitlich, dies ermöglicht das Einziehen von zusätzlichen Zugrifsschutzbereichen (protection domains) zwischen Modulen, ohne daß dazu ein IPC-Interface programmiert werden muß, wie das bei Interfaces zwischen z.B. UNIX-Prozessen der Fall ist.

Es existiert keine semantische Grenze mehr zwischen Kernel und Programmen, es gibt nur noch Module, Objekte, und Funktionsaufrufe. Die Systemsicherheit wird dadurch gewährleistet, daß jedes Modul nur noch die ihm zur Verfügung gestellte API benutzen kann, und diese Grenze auch nicht durch Manipulation von Pointern verletzen kann. Zusätzlich können die Adreßbereiche anderer Module beim Funktionsaufruf ausgeblendet werden (function call boundary == protection domain boundary).

Im Prinzip könnte man in Dylan direkt auf die Hardware aufsetzen, unter Umgehung von L4. Es gibt mehrere Gründe, doch L4 einzusetzen:

- Es ist viel Arbeit in die Spezifikation von L4 geflossen, mit dem Ziel, die API möglichst zu minimieren. Eine in Dylan geschriebene API würde sich an dem gesetzten Maßstab orientieren müssen, und sehr ähnlich aussehen.
- L4 existiert mit Pistachio in einer freien, portablen, SMP-fähigen Implementierung.
- Es gibt eine Linux-Implementierung, die auf L4 läuft.

Der letzte Punkt ist für einen sanften Übergang in der Praxis relevant: Zu glauben, man könne auf einen Schlag die existierenden Lösungen verdrängen, ist illusorisch. Der Plan ist, nach und nach Dienste im Dylan-Teil zu implementieren, und im Linux nur noch Stub-Treiber zu verwenden.

Als erster interessanter Dienst käme ein Server für Verschlüsselung in Frage. Statt zum Beispiel einen PGP- oder ssh-Schlüssel in Linux aufzubewahren, wo er im Falle eines Systemeinbruchs kompromittiert wäre, wird er in einem sicheren Bereich in einem Dylan-Subsystem gehalten. Die Idee eines solchen Security Subsystems ist nicht neu [3] , der Autor hält allerdings den Einsatz einer sicheren Sprache für eine relevante Komponente in einem solchen System.

Nach und nach können dann auch komplette Dienste, wie zum Beispiel Web Server [4] , oder auch die vom Nutzer verwendeten Applikationen, in den sicheren Bereich herübergezogen werden.

Zum jetzigen Zeitpunkt existiert ein proof-of-concept, das unter Zuhilfenahme der beschriebenen Technologien „Hello, World" auf dem Bildschirm eines handelsüblichen PCs ausgibt. Es demonstriert die grundlegende Fähigkeit der beteiligten Komponenten, einen minimalen Gerätetreiber bereitzustellen.

Der Umfang dieses Projektes ist sicherlich beachtlich, der Autor glaubt aber, daß es nicht nur realisierbar, sondern auch kurzfristig nutzbringend einsetzbar ist.

[1] *http://www.l4ka.org/projects/pistachio/*

[2] *http://www.gwydiondylan.org/*

[3] *http://www-krypt.cs.uni-sb.de/~perseus/*

[4] *http://carlgay.home.comcast.net/koala/*

Reboot: Das polizeiliche Informationssystem INPOL-NEU und der Datenschutz

von ipunkt <ds@ccc.de>

Seit 18.08.2003 arbeitet die deutsche Polizei bundesweit mit dem neuen Auskunfts- und Fahndungssystem INPOL-neu. Ziel des Systems: Anfragen von 270.000 Stellen bundesweit nach Tätern, Beweisstücken und Beziehungsgeflechten sollen so leicht sein wie das Surfen im Internet. Hier die Packungsbeilage zu Risiken und Nebenwirkungen:

„Etwas ist nicht recht, weil es Gesetz ist, sondern es muss Gesetz sein, weil es recht ist."

(Charles de Montesquieu (1689-1755),
frz. Staatstheoretiker u. Schriftsteller,
Begr. d. mod. Staatswissenschaft u.d. Lehre v.d. Gewaltenteilung)

1. Historischer Hintergrund

1.1 Grundlagen

Der Rückgriff auf Informationen ist auch in der polizeilichen Ermittlungs- und Strafverfolgungsarbeit unerlässlich. Deshalb wurde in den 70er Jahren, nicht zuletzt vor dem Hintergrund der zum Teil als desaströs gewerteten Ermittlungspannen gegen die Rote Armee Fraktion, beim Bundeskriminalamt (BKA) das polizeiliche Informationssystem INPOL eingerichtet.

Das BKA seinerseits ist eine 1951 durch das *"Gesetz über die Errichtung eines Bundeskriminalpolizeiamts" errichtete Bundesbehörde, die "zur Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten"* auf Grundlage von `Art. 73 Nr. 10a` und `Art. 87 Abs. 1 Satz 2` des Grundgesetzes ins Leben gerufen wurde.

Die gesetzliche Grundlage von INPOL findet sich im BKA-Gesetz (BKAG): `§2 Absatz 1 BKAG`: *"Das Bundeskriminalamt unterstützt als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen und für die Kriminalpolizei die Polizeien des Bundes und der Länder bei der Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung."* Und: *"Das Bundeskriminalamt unterhält als Zentralstelle ein polizeiliches Informationssystem nach Maßgabe dieses Gesetzes."* `(§2 Abs. 3 BKAG)`

1.2 Nutzerkreis

Den Kreis der (berechtigten ;-) User des Informationssystems legt `§11 BKAG`fest: Danach gehören zu den zur Eingabe und Abruf berechtigte Stellen*"außer dem Bundeskriminalamt und den Landeskriminalämtern sonstige Polizeibehörden der Länder, der Bundesgrenzschutz sowie die mit der Wahrnehmung grenzpolizeilicher Aufgaben betrauten Behörden der Zollverwaltung und das Zollkriminalamt"*. Darunter fallen auch eher exotische Behördenapparate wie etwa Bahn- und Luftpolizei. Außerdem darf das Auswärtige Amt für seine Auslandsvertretungen als Passbehörde die Fahndungsausschreibungen abrufen. Eine Weitergabe der gespeicherten Informationen kann das BKA unter den Bedingungen des §11 vornehmen. INTERPOL, EUROPOL und die Geheimdienste können so auf die national erhobenen Daten zurückgreifen.

Bei der *Eingabe* von personenbezogenen Daten gilt das Eigentümerprinzip, d.h. *"Nur die Behörde, die Daten zu einer Person eingegeben hat, ist befugt, diese zu ändern, zu berichtigen oder zu löschen"*.

Welche Daten dabei in das Informationssystem eingegeben werden dürfen, ist weitestgehend in den Gesetzen der einzelnen Teilnehmer (z.B. der einzelnen Landespolizeigesetze) sowie der Strafprozessordnung (StPO) geregelt.

`§§7-9, 16`sowie `20, 22 BKAG` regeln die allgemeine Gültigkeit der Speicherung personenbezogener Daten, auch des BKA, das seit dem Terrorismusbekämpfungs-

gesetz in verstärktem Maße auch selber Daten sammeln kann.

Beim Abruf von Daten hat das BKA nach §11 Abs. 6 *"bei durchschnittlich jedem zehnten Abruf für Zwecke der Datenschutzkontrolle den Zeitpunkt, die Angaben,die die Feststellung der aufgerufenen Datensätze ermöglichen, sowie die für den Abruf verantwortliche Dienststelle zu protokollieren"*.

1.3 Einrichtungsanordnungen

Welche personenbezogenen Daten dürfen nun konkret in INPOL gespeichert werden? Neben den schon zitierten §§7-9 BKAGregelt dies die so genannte *Errichtungsanordnung*, die nach § 34 für jede Datei, die personenbezogene Daten enthält, festzulegen ist und die der Zustimmung des Innenministeriums des Bundes und der beteiligten Länder bedarf.

Wesentliche Dateien in INPOL sind:

- *Sachfahndung:* Gestohlene/gesuchte Gegenstände (Seriennummern)
- *Personenfahndung:* Dazu gehören einzelne Dateien wie die Haftdatei (Haftort, Haftantritt, Entlassung), Straftaten-/Straftäterdatei (Personen, Straftaten, Opfer) oder die Gewalttäterdatei
- *SPUDOK:* Spurendokumentation (fallbezogene Hinweise, Ermittlungen)
- *PIOS:* Personen-Institutionen-Objekte-Sachen (Daten zu Terrorismus- und Rauschgiftkriminalität in einzelnen Arbeitsdateien)
- *DNA-Datenbank:* Genetische Fingerabdrücke
- *AFIS/Daktyloskopie:* (Automatisches Fingerabdruck Identifizierungs-System)
- *KAN:* Kriminalaktennachweis - Verweise auf bereits angelegte Kriminalakten zu einzelnen Personen

Zusätzlich hat INPOL Zugriff auf einige Dateien anderer Behörden:

- *ZEVIS:* Zentrales Verkehrsinformationssystem des Kraftfahrzeugbundesamtes (Fahrzeugdaten, -halter und entzogene Fahrerlaubnisse)
- *AZR:* Ausländerzentralregister

Ferner gibt es eine Reihe von Dateien und Programme für spezielle Zwecke, z.B. *LACK* für Lackspuren, *ISIS* für Phantombilder und *TESCH* für extremistische Schriften. Auch zur Literaturdokumentation und -beschaffung (*COD*, *GOLEM*) und für die Kriminalstatistik (*PKS*) wird INPOL genutzt.

2. Gesetzliche Grundlagen

2.1 Das Bundeskriminalamtsgesetz (BKAG)

Das BKA ist also Gralshüter des INPOL auf Basis des § 2 BKAG. Neben der Legitimation schränkt § 2 aber auch massiv ein, denn Daten dürfen nur zur *"...Verhütung und Verfolgung von Straftaten mit länderübergreifender, internationaler oder erheblicher Bedeutung"* erhoben und verarbeitet werden. Schon auf den ersten Blick wird klar, dass die Formulierung „erhebliche Bedeutung" viel Spielraum zur Interpretation lässt. Das ist datenschutzrechtlich umso bedenklicher, als in diesen Fällen das BKA quasi - das zeigt die enumerative Aufzählung der Datenarten in § 8 BKAG- als zentrale Datensammelstelle auftreten darf:

Dort heißt es im ersten Absatz: [Das BKA] kann zur Erfüllung seiner Aufgaben nach 2 Abs. 1 bis 3

- die Personendaten von Beschuldigten und, soweit erforderlich, andere zur Identifizierung geeignete Merkmale
- die Kriminalakten führende Polizeidienststelle und die Kriminalaktennummer,
- die Tatzeiten und Tatorte und
- die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere Bezeichnung der Straftaten

in Dateien speichern, verändern und nutzen.

Die Befugnisse zur *Datenpflege* ergeben sich aus §11 Absatz 3: Danach ist nur die Behörde, die Daten zu einer Person eingegeben hat, ist befugt, diese zu ändern, zu berichtigen oder zu löschen. Aber: sind Daten zu einer Person gespeichert (also der Datensatz angelegt), kann jeder Teilnehmer des polizeilichen Informationssystems weitere Daten *ergänzend* eingeben.

Bei alledem soll die Wahrung des Datenschutzes durch den Bundesbeauftragten für Datenschutz gewährleistet werden, eine echte Herkulesaufgabe, betrachtet man Umfang und Ausmaß der Datensätze. Die auf Landesebene erfassten Daten können zwar auch vom jeweiligen Landesbeauftragten kontrolliert werden, doch scheint auch das nur wenig mehr als eine vage Hoffnung.

2.2 Schranken

Grenzen (auch) der polizeilichen Datenerhebung und -verarbeitung zieht insbesondere das Bundesdatenschutzgesetz (BDSG). Hier einige Auszüge: § 13 Absatz 1: Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stelle erforderlich ist. Absatz 2:Das Erheben besonderer Arten personenbezogener Daten (§ 3 Abs. 9) ist nur zulässig, soweit

- dies zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist
- dies zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist.

Die Grundrechtsrelevanz all dieser Vorgänge liegt auf der Hand, weshalb man meinen sollte, dass wegen Art. 1 Abs. 3 GG (Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.) diese Schran-

ken auch bei Planung und Umsetzung des INPOL- neu Beachtung fanden. Leider weit gefehlt:

3. INPOL-neu

3.1 Geschichte und Motivation

Das System INPOL ist also ein olles, 1972 in Betrieb genommenes und über die Jahre immer heterogener gewordenes Modell.

Bereits Anfang der 80iger Jahre war die technische Leistungsgrenze des auf einer proprietären BS2000-Architektur der Siemens AG basierenden Systems INPOL erreicht. Die Arbeitsbeschränkungen durch mangelnde Performance, insbesondere im Antwortverhalten wurde in den nachfolgenden Jahren derart schwerwiegend, dass 1992 der Arbeitskreis II *"Innere Sicherheit"* der Arbeitsgemeinschaft der Innenminister der Bundesländer beschloss, ein Nachfolgesystem des polizeilichen Informationssystems (INPOL) zu schaffen. Dieses sollte:

- einen höheren Anwenderkomfort und eine bessere Administrierbarkeit polizeilicher Daten herstellen.
- Effizienzverluste aufgrund einer Mehrfacherfassung von Informationen vermeiden.
- dem individuellen Nutzer einen erweiterten Informationsumfang für operative Auswertungen im Rahmen von Ermittlungsverfahren zu Verfügung stellen.
- strategische Auswertungen zur Kriminalitätslage liefern und mögliche Entwicklungen aufzeigen.

3.2 Technologie und Systemführerschaft

Die technologische Umsetzung seitens des BKA erfolgte auf der Basis eines Netzwerks von 10 HP Servern unter dem Betriebssystem HP/UX, einem HP-eigenen Unixderivat. Das System wurde unter Federführung der Debis AG entwickelt. Ausschlag für die Entscheidung zu Gunsten von HP/UX scheint die Unterstützung von 64-Bit Dateisystemzugriffen zu sein. Damit sind Dateien (Datenbanken) möglich, die die Grenze von 4 GByte überschreiten.

Angesetzt wurden 20 CPUs (PowerPC) bei ca. 20 GB Hauptspeicher und Plattenkapazität im Terabytebereich.

Clientseitig wurde die Anbindung an INPOL-neu von vorneherein so geplant, dass es von unterschiedlichen Betriebssystemen genutzt werden kann, auch wenn de facto clientseitig überwiegend Mickeysofts Windows NT zum Einsatz kommt.

3.3 Unterschiede zu INPOL-alt

INPOL-NEU unterscheidet sich in drei Punkten entscheidend vom altem INPOL-System:

- INPOL-neu verwendet ein Konzept, das als „Integrierter Datenpool" bezeichnet wird. Dabei werden im Gegensatz zu INPOL die einzelnen Datenbanken nicht in getrennten Dateien gelagert, sondern eine einzige physikalische Datenbank nimmt alle Datensätze auf. Die Zuordnung von Datensätzen zur logischen Datenbank erfolgt durch deren Attributierung. Der Zugriff auf einzelne Datensätze des Berechtigungssystems erfolgt dabei auf Basis eines komplexen Berechtigungssystems. Eingesetzt wird hierbei ein herstellerunabhängiger LDAPv3-Verzeichnisdienst. Der Verzeichnisdienst enthält Kategorien für Dienststellen (ORGA-Einheit, Dienststelle, Mitarbeiter), Personen (Name, Vorname, Postanschrift), AGIL spezifische Attribute (AGIL-User ID, Polizeistammdaten) und Passwörter.

- INPOL-neu wurde gezielt unter der Prämisse der automatisierten Vorgangsbearbeitung entwickelt. Konkret heißt dies, dass die AGIL Teilnehmer Schnittstellen zu ihren Systemen und INPOL-neu bereitstellen, um Vorgänge der Länderpolizeien, des BKA, des Zolls und des BGS automatisch in INPOL-neu einpflegen zu können.

- Es soll eine separate Datenbank für „Polizeiliche Führungsinformation" (PFI) implementiert werden. Mit dieser Datenbank sollen erstmalig Kriminalitätsstrukturen erfasst und ausgewertet werden können.

3.4 Datenschutzrechtliche Aspekte

Insbesondere die neue Struktur eines einheitlichen Datenbestandes von INPOL steht im Konflikt zu grundlegenden datenschutzrechtlichen Prinzipien und insbesondere dem Grundsatz der Zweckbindung.

Um diesen Konflikt zu heilen, setzt INPOL-neu auf das Konzept der Berechtigungprofile. In einem Berechtigungsprofil, dass jedem INPOL-Nutzer zugewiesen wird, werden Berechtigungen für

- den Zugriff auf Daten (z.B. Einschränkung auf Teildaten),
- den Zugriff auf Funktionen

vergeben. Einer der wichtigsten und zentralen Mechanismen dieseAnforderungen, die sich insbesondere aus den §§ 11 Abs. 1, 34 Abs. 2 BKA-Gesetzergeben (Einrichtungsanordnung, Bezeichnung, Zweck und Inhalt), sind die logischen Dateien. In INPOL-neu gibt es ausschließlich vereinheitliche Datensätze. Daher wird jedem Element eines Datensatzes, z.B. dem Namen, dem Geburtsdatum, der Straftat, erkennungsdienstlichen Daten (z.B. Fingerabdruck) Attribute zugeordnet, die dieses Element mit den jeweiligen logischen Dateien verknüpft. Diese logischen Dateien stellen ihrerseits wiederum die Grundlage der Berechtigungsbereiche des INPOL Berechtigungskonzeptes dar.

Geplante Berechtigungsbereiche des Datenpools sind:

Grundinformationen: In diesem Bereich sind Personen- und Sachfahndungen, erkennungsdienstliche Daten, Haftdaten, Personenbeschreibungen sowie personenbezogene Hinweise (PHW) und der Kriminalaktennachweis (KAN) angesiedelt. Jeder Nutzer von INPOL-neu soll auf diesen Bereich lesenden als auch schreibenden Zugriff haben. Allerdings soll durch getrennte Abfrage-

arten an den Bereich „Grundinformation“ gewährleistet werden, dass lediglich die für jeden Einzellfall notwendigen Daten ausgegeben werden. Besonders erwähnt werden sollte die in der Grundinformation enthaltene Möglichkeit der „Kurzauskunft“. Sie zeigt nicht nur die Fallgrunddaten, wie Delikt, Tatzeit und -ort, sondern auch alle strafbaren Handlungen einer Person an, die im Bereich „Fall“ gespeichert sind. Zusätzlich wird ebenfalls eine Fallkurzauskunft für alle erfassten Straftaten ausgegeben, die in irgendeiner Beziehung zu den Daten der Kurzauskunft stehen.

Fall: In diesem Bereich sollen alle PIOS (Personen, Institutionen, Objekte, Sachen) und Fallanwendungen gebündelt werden. Ausnahmen bilden die Bereiche OK, Geldwäsche und innere Sicherheit, die einen eigenen Bereich bilden. Dieser Bereich soll polizeilichen Ermittlern und Auswertern zugänglich gemacht werden. Es ist geplant, dass in diesem Bereich auch personenbezogene und ungesicherte Daten von Zeugen, Opfern, Kontakt- und Begleitpersonen und sonstigen Dritten gespeichert werden. Der Paragraph 8 Abs. 4 und 5 des BKAGlegt hierbei den Rahmen fest, in wie weit einzelne Nutzer Zugriff auf diese Daten erlangen sollen. Konkret wird verlangt, dass ein Nutzer lediglich die Informationen erhält, die er für die Erfüllung seiner Aufgabe benötigt. Was auch immer das sein mag.

OK, Geldwäsche, IS: Diese Bereiche sollen nur einem beschränkten Nutzerkreis zugänglich sein. Zum Beispiel einer Spezialdienststelle Organisierte Kriminalität (OK).

Spurendokumentation: Dieser Bereich bündelt die Daten zu fallspezifischen Spuren (Tatort, Zeugen etc.)

Temporäre Fallanwendungen: Dieser Bereich wurde geplant, um Ländergenzen überschreitende, regionale Ermittlungen zu unterstützen, z.B. Sonderkommissionen.

3.6 Datenschutzrechtliche Bedenken am Beispiel Kriminalaktennachweis (KAN)

Seit der Änderung des Paragraphen 8 Abs. 1 des BKAG- besteht die Möglichkeit in der KAN auch Informationen zum Tatvorwurf, Tatzeitpunkt und Tatort zu speichern. Die INPOL-neu Projektgruppe hat zusätzlich versucht den gesamten kriminellen Werdegang einer „INPOL relevanten Person“ in der KAN abzubilden. Beide Punkte führen dazu, dass sich der Charakter des KAN von einem reinen Aktennachweissystem zu einem operativen Ermittlungswerkzeug verschiebt. Ebenso problematisch sind die Pläne, sämtliche strafbaren Handlungen einer Person bundesweit zugänglich zu machen, selbst wenn nur eine Straftat den Zugangskriterien zum KAN nach Paragraph 2 Abs. 1 BKAGentspricht. Die Kritik besteht darin, dass entsprechend Paragraphen 11 Abs. 1, 2 Abs. 1 und 3 BKAGnur Straftaten mit länderübergreifender, internationaler und/oder erheblicher Bedeutung zugelassen sind.

Am KAN wird ein Grundkonflikt von INPOL-neu deutlich, nämlich die schwierige Einordnung und Abgrenzung von bundes- und landespolizeirechtlichen Daten innerhalb des vereinheitlichte Datenpools (Relevanzschwelle).

Datenschutzrechtlich höchst problematisch ist ferner, dass im Feld „ungesicherte Daten“ etwa Zeugenaussagen eingegeben und abgerufen werden können, deren Korrektheit nicht verifiziert wurde oder werden kann. Das kann zu einer Stigmatisierung führen, die auch vom eigentlichen Zweck von INPOL-neu, einer effektiven Strafverfolgung, nicht mehr gedeckt sein kann.

3.7 Fazit

INPOL-neu ist ein weiterer Schritt in Richtung gläserner Bürger; das System öffnet dem Missbrauch Einzelner und der Stigmatisierung vermeintlicher Täter Tür und Tor. Waren in der Vergangenheit die Datenbanken voneinander isoliert und die Zugriffskontrolle effektiv durch die physikalische Zugangskontrolle zur jeweiligen Datenbank gegeben, ergibt sich durch den vereinheitlichen Datenbestand ein völlig anderes Bild. Jeder Polizeirechner ermöglicht zukünftig den Zugriff auf einen zentralen Datenpool. Im Unterschied zum alten System werden die Befugnisse der Dienststellen ausgeweitet, die beispielsweise auch Angaben über minder schwere Straftaten abrufen können.

In diesem Zusammenhang sind starke Tendenzen zur Zentralisierung der Datenverarbeitung der gesamten deutschen Polizei zu beobachten, die dem gesetzlichen Rahmen zum Teil entgegenlaufen.

Nicht jede mit vorhandenen technischen Möglichkeiten realisierbare oder mit polizeifachlicher Erforderlichkeit begründete Verarbeitung personenbezogener Daten ist zulässig, denn hierdurch wird in das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung eingegriffen, ohne dass dies im Rahmen der Erforderlichkeit für die polizeiliche Aufgabenerfüllung durch Rechtsvorschriften erlaubt wäre. Musterbeispiel ist der Datensatz Bundes-Kriminalaktennachweis (KAN), der die „gesamte kriminelle Karriere“ jeder Person abbilden soll, die aus Anlass eines INPOL- relevanten Delikts erfasst ist. Dabei werden aber auch Daten über solche Straftaten gespeichert und zum Abruf bereit gehalten, die weder von länderübergreifender oder internationaler noch von besonderer Bedeutung sind. Damit verlässt das System den gesetzlichen Rahmen, § 2 BKAG.

Da durch Zugriffssteuerungssysteme im Sinne von Userprofilen allein kein ausreichender Schutz gegen einen Missbrauch des Systems durch übereifrige Gesetzeshüter gewährleistet werden kann, sind effektive und ihrerseits automatisierte Kontrollmechanismen durch den Bundesdatenschutzbeauftragten zu fordern: Zugriffsprotokollierung, Überprüfung der Datenrelevanz, der Löschung etc. müssen eingesetzt werden, um den Einzelnen nicht zum Datenpool verkommen zu lassen, auf den jeder halbgebildete Polizist unbegrenzten Zugang hat.

http://www.chaosrecht.de im September 2003

Bigbrother und die Wachmänner

von fdik <vb@dontpanic.ulm.ccc.de>

Die Zeiten sind hart für Datenschützer. Sie sind hart für alle Bürgerrechtler. Denn: Wessen Rechte soll man verteidigen, wenn die Bürger auf ihre Rechte gar keinen großen Wert zu legen scheinen? Der Kommentar eines Betroffenen.

Für mich erstaunlich groß ist der Widerstand gegen Softwarepatente. Demonstrationen in ganz Europa kommen zustande, abertausende Unterschriften, dem Thema entsprechend meist elektronischer Natur, werden zusammengetragen. Eine breite Front von KMU und OpenSource-Welt erstaunt ganz offensichtlich auch die Politiker aller Parteien. Mit so viel Widerstand war wohl nicht gerechnet worden. Ganz hart gesagt, wohl auch von vielen Widerständlern selbst nicht. Denn das Thema ist komplex und kompliziert, die Positionen sind zwar klar, aber eigentlich nur den Leuten, die sich darum gekümmert haben. Man könnte fast sagen, es kommt viel Widerstand zusammen, *obwohl* dieser mehr als sinnvoll ist. Das Ergebnis der Entscheidung des europäischen Parlaments folgte dann auch der offensichtlichen Mehrheitsmeinung, ein voller Erfolg. Erfreulich - und ganz anders als auf anderen Gebieten der Verteidigung der Rechte der sonst nicht so Starken.

Denn was sich derzeit auf der Bühne des Datenschutzes und der Informationsfreiheit abspielt, gleicht eher einer Farce. Noch nie wurden die Rechte des Einzelnen derart hinter die Macht des Staates (und die Interessen der großen Konzerne) gestellt wie jetzt. Zumindest nicht in Staaten, die sich aus gutem Grund eine Demokratie nennen dürfen. Oder durften.

Da werden in Deutschland, und zwar der Bundesrepublik Deutschland, Überwachungsmaßnahmen legalisiert, die eine StaSi im "kleinen behinderten Bruder der BRD" (Kalkofe) noch beinahe gänzlich illegal durchführen musste. Völlig legal darf eine zweistellige Prozentzahl der Telefonate abgehört werden, auch im Inland, auch vom BND, weil das ja Auslandsbezug haben kann. Überwachungskameras auf öffentlichen Plätzen werden immer mehr die Regel, man traut sich auf manchem Bahnhof schon nicht mehr in der Nase zu bohren, wenn's "keiner sieht", denn die Kamera und der dahinter glotzende "Sicherheitsbeauftragte" beobachten das ja sicher. Wenn sich in der DDR "alle so lieb hatten, dass sie gegenseitig Akten übereinander anlegten" (ebenfalls Kalkofe), dann sind wir jetzt wirklich endgültig dem Ostalgie-Wahn verfallen - und lieben uns wohl demnächst ähnlich fest und innig. Die USA, unser Freund und großes Vorbild, machen's ja vor: Ein Präsident, der mehr ernannt als gewählt wurde, und einen zweifelhaften Krieg aus zweifelhaften Motiven heraus führt, dessen Ausgang völlig unklar ist, begründet mit einem sicher entsetzlichen terroristischen Anschlag (der leider zweifelhaft aufgeklärt wurde), mehr oder minder die Aufhebung jeder Privatheit und der oppositionellen Meinungsführung überhaupt. Wer abweicht, wer sich nicht überwachen lassen will, wer bei Unklarheiten hinterfragen will, ist einfach "unpatriotisch". Denn das ist der Patriot Act - McCarthy lässt grüßen.

Auch in Europa zieht sich die Schlinge um den demokratischen Hals zu - in jedem zweiten Baumarkt bekommt der nichts ahnende Kunde eine Payback-Card angeboten, in einer Art und Weise, die böse Zungen "Drücker" nennen. Wir nennen das "Vertriebs-

beauftragter". Scheinbar kostenlos bekommt man da satte 2% Rabatt - gegen die geringfügige Kleinigkeit im kleingedruckten Unwichtigen, kaum verständlich verklausuliert auf sämtliche Privatheit zugunsten eines Kartells von Konzernen zu verzichten. Und das im Stehen im Baumarkt. Doch scheinbar sind solche "Verträge" rechtsgültig statt sittenwidrig. An der öffentlichen Front sieht's noch düsterer aus: Zuerst ein Regierungspräsident, der sich "gezwungen" sieht, eine mehr als zweifelshafte Rechtsposition zur Internetzensur mit allen Tricks durchzusetzen, um einen Versuchsballon steigen zu lassen, ob Internetzensur gesellschaftsfähig geworden ist. Und ein Bundespräsident, der den Regierungspräsident nicht zurechtweist, sondern als vorbildlichen Beamten sieht, und Internetzensur als notwendig und sinnvoll. Zumindest, solange es der deutsche Staat macht; wenn die Volksrepublik China das macht, ist das natürlich ganz was anderes. Natürlich. Ganz anders. Denn die ist ja keine Demokratie...

Nur: Was ist denn eine Demokratie? Das ist doch die Staatsform, in der eine "Balance of Powers" geschaffen werden soll (wie die Amerikaner sagen) und statt mit Waffengewalt die Konflikte "zivilisiert", mit Spielregeln und ohne Gewalt ausgetragen werden sollen. Oder sollten (wie die Schweden sagen). Und das Volk, der "Souverän", soll jederzeit den Staat kontrollieren, den es sich gibt, um das zu erreichen. Aber wie geht das, vollständig durchleuchtet von den Mächtigen, und nur mit dem informiert, was der Staat durchlassen möchte? Nicht Wissen ist Macht, sondern mehr wissen als andere. So gleiten wir langsam über in die "Informationsgesellschaft", in die "Wissensgesellschaft", aber wie informiert ist hier wer über wen, wer weiss was und beherrscht so die anderen?

Datenschutz und Informationsfreiheit, "private Daten schützen" und "öffentliche Daten nützen" sind untrennbar miteinander verbunden. Sie haben dasselbe Ziel. Und mit diesem Ziel verbunden und zur Abschreckung gegen die Gefahren erfunden sind die Begriffe "Big Brother" (is watching you!) und Überwachungsstaat. Waren es. Denn die Öffentlichkeit reagiert auf diese Warnschilder der Informationsfreiheit und des Datenschutzes heute ganz anders.

Unter "Big Brother" verstehen die allermeisten jetzt das Einsperren geistig und sozial kranker Menschen zu voyeuristischen Zwecken in zu Baracken umgebauten Containern, und das Zurschaustellen deren banalen Lebens und Nicht-Strebens in der Öffentlichkeit. Gerne auch in den Geschmacklosigkeits-Richtungen "wer darf meine Tochter bügeln" oder "Küblböck - die größte Peinlichkeit 'gewinnt'". Und jetzt neu, "Powered by Emotion" (Kraft durch Freude?), die Wachmänner. Hach, was ist das lustig, wie die Welt sich dreht, während banale "witzige" Dinge auf der Straße oder im Aufzug passieren, und zwei geistig minderbemittelte das alles aufzeichnen, im Auftrag des dubiosen Chefs, der Metapher für die amorphe und unverständliche Macht im Hintergrund? Was haben wir gelacht. Zufall oder sogar Absicht, die einstigen Plakate der Warnung vor totalitärem Staat sind so verbraucht, völlig verdeckt von scheinbar harmlosem Unfug. "Big Brother" und "Überwachung" haben ihre Schrecken verloren. Man könnte, wollte man Verschwörungstheorien nicht meiden, glatt Methode hinter diesen scheinbar harmlosen "zufälligen" Neudeutungen vermuten.

Da passt es hervorragend, dass der Kamera-Wahn ausgerechnet im Privaten ausgebrochen ist. Jeder filmt jeden, mit der Handkamera, mit der Webcam, mit dem Handy gar, ein riesiger Markt für die wiederentdeckte Liebe zueinander in diesen kalten Zeiten. Sogar auf dem Chaos Communication Camp, sicher eigentlich keine Veranstaltung, auf der regelmässig für die totale Überwachung geworben wird, war man vor den ganzen Aufnahmegeräten von Zeltnachbar bis RTL2 nicht sicher. Eigentlich konnte man keinen Schritt machen, ohne dass das von irgendwem festgehalten wurde. Die Bilder der anwesenden Mädchen, die - temperaturgemäß - wenig geschürzt sich auf dem Camp tummelten, werden denn nun auch im passenden IRC-Kanal von perversen "Handbetrieblern" getauscht. Ein Trauerspiel für uns, den CCC. Aber im Zeitalter der "persönlichen Homepage", auf der in bester Exibitionisten-Manier auch noch der Status der eigenen Unterhose maschinenlesbar veröffentlicht wird, scheint das ja kaum noch eine(n) zu stören.

So verschwinden die Grundlagen jeglicher Selbstbestimmung, werden unklar hinter der Verrücktheit der Öffentlichkeit. Will die Öffentlichkeit kein Privates, will sie gar keine Demokratie? Sind viele Leute so satt geworden, dass es gleich ist, was "die Politiker" so treiben und die Wirtschaft, weil man ja "eh nichts machen kann", weil nachdenken zu anstrengend ist, vordenken geradezu lästig? Wollen sie wie eine Herde Schafe behandelt werden, die der Schäfer von gezähmten Wölfen zusammentreiben lässt? Interessiert es sie gar nicht mehr, für welchen Weg sich der Schäfer entscheidet, auch dann nicht, wenn er vielleicht für viele zur Schlachtbank führt? Weil sie dem Schäfer endgültig vertrauen, er wird schon das richtige tun? Ich glaube nicht.

Ich habe eher das Gefühl, die meisten sind sich gar nicht im Klaren über die Relevanz ihres Tuns. Wie können wir die Leute wieder aufwecken? Wir brauchen neue Symbole. Die alten sind verbraucht. Und: Vielleicht sollten wir unsere Ziele vorleben.

Denn: Vielleicht sind einige wirklich so satt. Das wird sich aber spätestens ändern, wenn es zu spät ist - denn eine Demokratie ist das instabilste aller politischen Systeme und einem ständigen Wechsel und Bedarf nach Verbesserung ausgesetzt. Zu viele scheinen das bereits vergessen zu haben. Lasst *uns* das nicht vergessen. Und lasst uns neue Symbole erarbeiten, damit wir die Leute "draußen" im Globalen Dorf erreichen.

Fortschritt ohne Balken

von Christian Jeitler <chris@quintessenz.org>

Zum Abschluß einer weltweiten Harmonisierung von Rechtsvorschriften für "Geistiges Eigentum" war die EU-Kommission kurz davor, eine massive Ausweitung des Software-Patentrechts durchzubringen - dazu passend das europäische Patent EP Nr. 0394160, das den gebräuchlichen Fortschrittsbalken erklärt.

Ein ganzer Stab von professionellen Lobbyisten und Interessensvertretern wie BSA & Co hatten gemeinsam mit der EU-Abgeordneten Arlene McCarthy versucht, eine Richtlinie über "Patentierbarkeit computerimplementierter Erfindungen" durch die Hintertür beschlußfähig zu machen. Gewappnet mit einer vorbereiteten Studie über die Zustimmung der europäischen Softwareindustrie sollte daraus ein einfacher Gang werden.

Was anfangs kaum jemand für möglich gehalten hatte, ist Vertretern von Freier Software und Open Source, gemeinsam mit Klein- und Mittelbetrieben, gelungen: Die EU-Richtlinie zur Einführung von Logik- und Ideenpatenten wurde entgegengesetzt dem Vorschlag der Kommission entschärft. Denn erst als sich die Mailboxen der Abgeordneten mit Protestmails füllten, hat man Handlungsbedarf erkannt, sagten mehrere Abgeordnete aus allen vier Fraktionen des Europaparlaments.

Nachträgliche Legalisierung

Nach Art. 52 IIc des Europäischen Patentübereinkommens (EPÜ) sind Computerprogramme nicht patentierbar. Dennoch hat das Europäische Patentamt (EP) in den letzen Jahren ca. 30.000 solcher Patente erteilt. Damit schuf das Europäische Patentamt Fakten, lange bevor eine politische Meinungsbildung möglich war. Fakten, die sich bei einer Patentgebühr von 50.000,- Euro je Patent für eine solch mächtige Organisation durchaus rechnen. 70% dieser ohne Rechtsgrundlage angemeldeten 30.000 Softwarepatente gehen an US-amerikanische und japanische Unternehmen wie Sony, Matsushita, Sun, Canon und IBM. Der Vorschlag der EU-Kommission war darauf aus, das Vorgehen nachträglich und in Zukunft zu legalisieren.

Eine sanft gefärbte Statistik über die Auswertungen einer Sondierung über Softwarepatente sollte helfen, dies anschaulich zu argumentieren. Dort konnte die EU-Kommission aus 4% Befürwortern eine "Mehrheit für Softwarepatente" konstruieren. Der Trick dabei war einfach: Man schmeisst einfach die negativen Antworten weg. Der Einfachheit halber enstand die zweite Studie nur noch am Schreibtisch, aber immerhin wurden die 12 versendeten Fragebögen korrekt ausgewertet. Damit sollte die Grundlage für die grenzenlose Patentierbarkeit von Algorithmen und Geschäftsmethoden wie zum Beispiel das Patent EP Nr. EP0927945 (Versenden von Geschenken aus einem Webshop), das

dem US-Unternehmen Amazon darauf ein zwanzigjähriges europaweites Monopol verleihen würde, geschaffen werden.

Weltweiter Monopolhandel

Der fortschreitende Aufbau eines rigiden Kontroll- und Verwertungsregimes verschiebt die Balance zwischen dem Bestand öffentlich frei zugänglicher Werke, der Public Domain, und dem durch Ausschließungsrechte geschützten Bereich privater Vermarktungsinteressen. Seit ihrer Gründung 1994 sind alle WTO-Mitgliedsstaaten gezwungen, das TRIPS-Abkommen (Trade-Related Aspects of Intellectual Property RightS) über geistiges Eigentum zu ratifizieren. Ein starker Rechtsschutz für Software und digitale Güter soll Arbeitsplätze im Dienstleistungssektor schaffen und gleichzeitig durch internationale Vereinheitlichung der Rechtssysteme Handelshemmnisse abbauen. Da geistiges Eigentum als handelbares Gut nicht allgemein verfügbar sein darf, verlagern sich damit Schranken und Barrieren - zunehmend auf Patentämter und Gerichtssäle.

In einem jüngst veröffentlichtem Interview meinte Bill Gates, daß die größte Schwäche von Linux nicht im technischen Bereich liege, sondern in der Tatsache, dass niemand Patente auf Linux angemeldet habe und Linux somit nicht an den in den USA üblichen Crosslicensing-Deals zwischen Großunternehmen teilhaben könnte. Für US-Softwareunternehmen wirkten Softwarepatente bisher sehr erfolgreich als Schutzzoll gegen Softwareimporte. Ausländische Unternehmen hatten meist nicht genug Erfahrung, um sich auf dem glatten und komplexen Parkett des Patentrechts erfolgreich zu bewegen.

Freie Software gewinnt

Nach seinem Vortrag auf dem Chaos Communication Camp 2003 verglich EFF Mitbegründer John Gilmore die Situation der EU mit jener der amerikanischen Verfassung in den ersten Jahrzehnten ihres Bestehens. Ebenso wie damals liegt es an uns, in der "Europäischen Verfassung" grundlegende demokratische Änderungen und Anpassungen herbeizuführen. 280.000 virtuelle Unterschriften gegen Softwarepatente, Proteste vieler Wirtschaftsverbände sowie Protestmails vieler Entwickler und Unternehmer waren nur ein Teil dieses Engagements. Zusätzlich entsandten viele nationale Organisationen wie der Verein zur Förderung Freier Software Vertreter nach Brüssel, die den Abgeordneten bis zuletzt Rede und Antwort standen.

Das Ergebnis ist die bisher ungewöhnlichste Abstimmung in der Geschichte des EU-Parlaments. Bei den zahlreichen, jeweils einzeln abgestimmten Änderungen zum umstrittenen Entwurf der EU-Kommission über "computerimplementierte Erfindungen" hat praktisch jeder EU-Abgeordnete, ohne Rücksicht auf Fraktionszwang, eine individuelle Abstimmungsliste geführt. Grundsätzlich "Ja" dazu, den Vorschlag der Kommission nicht einfach abzulehnen, sondern möglichst stark zu entschärfen, sagten 361 Abgeordnete. 157 waren dagegen, 28 enthielten sich laut einer Aussendung des Parlaments. Damit liegt es an der EU-Kommission, die mit jeweils deutlichen Mehrheiten angenommenen Verbesserungen des Parlaments an der Direktive ernst zu nehmen und diese dann in Form eines "gemeinsamen Standpunkts" dem EU-Ministerrat zu präsentieren. Bei einer Umsetzung aller Abänderungen verstößt die Vergabepraxis des europäischen Patentamts gegen geltendes EU-Recht.

Links

[1] *http://europa.eu.int/comm/internal_market/en/indprop/comp/softanalyse.pdf*

[2] *http://europa.eu.int/comm/internal_market/en/indprop/comp/com02-92de.pdf*

[3] *http://www.ffs.or.at/artikel/analyse_vote.html*

[4] *http://petition.eurolinux.org/*

[5] *http://swpat.ffii.org/patente/index.de.html*

[6] *http://futurezone.orf.at/futurezone.orf?read=detail&id=188769*

[7] *http://www.quintessenz.org/cgi-bin/index?s=1&q=Patente*

Lobbying gegen Softwarepatente

von Markus Beckedahl <markus@nnm-ev.de>

Seit 1999 geisterte ein geplanter Richtlinienentwurf der Europäischen Kommission zur Patentierbarkeit sogenannter Computer-implementierter Erfindungen (in der Kurzform auch Softwarepatente-Richtlinie genannt) durch die europäischen Gremien und die Presse.

Am 1. September sollte die erste Lesung im Europaparlament stattfinden. Der Fördervereins für eine freie informationelle Infrastruktur e.V. (kurz FFII) hatte Geld von Spendern organisiert und so fuhren in der Woche vor der geplanten Entscheidung 25 junge und sehr motivierte Vertreter der Eurolinux-Alliance nach Brüssel, um eine ungewöhnliche Lobbyaktion durchzuführen.

Bei Ankunft war klar, dass es einen Abgeordneten-Mitarbeiter der Grünen gab, der uns ins Europaparlament hineinlassen würde. Ein kleines Zimmer von einer sich im Urlaub befindenden Abgeordneten diente uns als Zentrale, mit einem Telefon, einem Sofa, Stuhl, Tisch und einem Computer mit einem uraltem Windows NT. Kein wahrliches Vergnügen, aber wenigstens Netz. Da das Büro etwas klein war, beschlagnahmten wir erstmal eine Sofaecke mit Steckdosen drum herum. Zentral gelegen, direkt neben den Aufzügen errichteten wir hier also unser Basislager. Fast alle Teilnehmer hatten schon im Vorfeld versucht, Gesprächstermine zu Abgeordneten aus ihrem Land zu vereinbaren. Aber die Kurzfristigkeit der Aktion und die Sommerpause im Parlament verhinderten zuviel Planung.

Zuerst war alles relativ unkoordiniert. Aber dann fanden wir heraus, dass man mit den überall herumstehenden Flurtelefone kostenlos innerhalb des Parlaments telefonieren konnte. So konnten wir prima ein Abgeordnetenbüro nach dem anderen anrufen. Einer von uns flog im Laufe der Woche noch raus, weil er zwei Stunden lang im Foyer das Flurtelefon blockierte. Auf jeden Fall kamen so immer wieder spontane Gesprächstermine zustande, die genutzt wurden, um den Abgeordneten oder ihren Mitarbeitern unsere Positionen zu vermitteln.

Fast immer bestand erstmal das Problem darin, Menschen, die sich z.B. hauptsächlich im EU-Ausschuss für Fischerei um eben dieses Thema kümmern, Grundkenntnisse der Materie zu vermitteln. Das fing dann schon damit an, dass wir erklären mussten, wie ein Computer funktioniert, was man beim Programmieren macht und was Logik ist. Logik ist seit 1973 ebenso wie Musik, Mathematik, etc. durch das europäische Patentabkommen von der Patentierbarkeit ausgeschlossen. Als Übersetzung klappte meist zum EinstiegHätte Haydn "eine Symphonie, dadurch gekennzeichnet, dass Klang [in erweiterter Sonatenform] erzeugt wird" patentiert, wäre Mozart in Schwierigkeiten gekommen. Auch konnte nicht jeder einfach so zu jedem Abgeordneten laufen, dazu waren zuviele Software-Entwickler in ihrer individuellen Kleidung und meist Haarlänge vor Ort. Also wurden die Parteien nach Kleidung ausgesucht. Die Anzugträger konzentrierten sich auf die Konservativen und Liberalen, mit langen Haaren und Militärkleidung bekam man die Sozialisten. Grüne und Nordische Grüne brauchten nicht mehr überzeugt werden, so dass sich der Rest der normal angezogenen auf die anderen Parteien verteilte.

Mit der Zeit besetzten wir eine weitere große Sofaecke, die eigentlich den Grünen als Raucherecke diente. Aber bald gab es keinen Platz mehr, denn alle packten zwischenzeitlich immer ihre Notebooks aus, erholten sich von irgendwelchen Büro-Suchaktionen oder tranken Kaffee. Immer mehr Grüne fragten sich schon, was diese zumeist langhaarigen und mit modernster IT-Technik ausgestatteten jungen Männer denn in ihrer Raucherecke machten. Vereinzelt wurden wir auch mit einem Grinsen befragt, ob wir auch unsere Schlafsäcke dabei hätten, um dort zu campen. Auf jeden Fall kam unsere Motivation und aus ihrer Sicht sehr pragmatischen und professionellen Lobbyarbeit so gut an, dass uns immer mehr Büros zur Verfügung gestellt wurden.

Abgeordnete und erfahrene Fraktionsmitarbeiter erzählten uns Tricks und Kniffe, was man alles beachten müsste und wie wir unsere Botschaften am besten transportieren sollten. Für viele war dies die erste politische Aktion ihres Lebens und so war dieser Wissens-

transfer sehr hilfreich. Gleichzeitig bekamen wir hautnah mit, wie sich die Briefkästen, Mailboxen und Faxe der Abgeordneten mit Protestschreiben füllten. Durch direkten Kontakt fanden wir schnell heraus, dass Mails gefiltert werden, Faxe und Briefe dafür aufmerksamer gelesen, bzw. überflogen werden. Dabei kamen immer freundliche und argumentative Briefe und Faxe an, vor allem aus den eigenen Wahlkreisen oder kleinen und mittelständischen Firmen, die sich um ihre Arbeitsplätze Sorgen machen.

Mittwoch sollte die erste europäische Demonstration gegen die Softwarepatente-Richtlinie stattfinden. Die Association Electronique Libre aus Belgien hatte diese direkt auf dem Place de Luxembourg vor dem Europaparlament angemeldet. Morgens kopierten wir noch Einladungen und fuhren ständig mit Aufzügen rauf und runter, um dort immer wieder die Poster anzubringen, so dass sie möglichst viel Zielgruppe erreichen. Statt pessimistisch erwarteter 50 Teilnehmer waren fast 500 überwiegend männliche Protestanten erschienen. 300 von ihnen kauften sich ein schwarzes T-Shirt mit dem Slogan Protect Innovation against Softwarepatents. Und durch die allgemeine Lieblingsfarbe von Nerds stand eine schwarze Menge mit ebensolchen Luftballons in der Hand 100 Meter direkt vorm Europaparlament.

Nach einigen Reden und dem Singen einer leicht umgedichteten Version von Die Gedanken sind frei gab es noch eine Pantomime aufführung. Das Piano für der Musik musste dabei extra aus Essen geholt werden. Anschliessend ging ein Trauerzug direkt zum EP und alle stellten sich längsseitig vor der Fensterfront auf und ließen gleichzeitig die Luftballons steigen. Überraschenderweise waren RTBF, Euronews und BBC mit Kameras dabei, so dass die Aktion festgehalten werden konnte. In Belgien waren wir damit in den Schlagzeilen.

Direkt im Anschluss sollte eine Pressekonferenz zusammen mit den Grünen organisiert im EP stattfinden. Noch mit T-Shirts am Körper standen wir im Foyer, wollten gerade durch die Sicherheitsschleuse durch als die Security Alarm schlug. T-Shirts mit politischer Aussage wären untersagt. Da Sommer war, gab es plötzlich die bizarre Situation, dass einige von uns mit nacktem Oberkörper im Foyer des Europaparlaments standen. Dies war auch nicht erlaubt, und Einzelgruppen mussten mit Securities, die leider kein Wort Englisch sprachen, zu den Büros laufen, wo die Rucksäcke abgestellt waren. Ich musste mit einem Engländer hochfahren, weil er dem französischsprechenden Security nicht erklären konnte, wo sein anderes T-Shirt ist.

Oben angelangt, und dem grimmigen Sicherheitsmenschen das weitere T-Shirt in die Hand gedrückt, standen wir vor dem Problem, dass wir uns nur die Hälfte der Raumnummer behalten hatten. Also machten wir uns auf die Suche, nur "A1" wissend. Vermutlich das andere Haus, erster Stock. Dort angelangt befragten wir einen Sicherheitsmenschen nach dem anderen, immer hoffend, dass jemand Englisch spricht. "Where is our Press-Conference? We are searching it, something with A1." Dies löste einige Konfusion und weitere Aufregung unter der Security aus, da es mehrere Trupps von unserer Sorte gab, die sich ohne dazugehörigen Assistenten oder Abgeordneten auf der Suche befanden. Verschiedene Grüne liefen daraufhin herum, uns einzusammeln, was auch meist klappte. Nur war der Raum vor Mitarbeitern, Presse und uns so überfüllt, dass die Security die letzten gar nicht mehr hineinließen.

Die Woche war ein Erfolg. Verbunden mit einer der größten Online-Demos aller Zeiten konnte genug Aufmerksamkeit auf die komplizierte Direktive gelenkt werden. Sowohl nach außen über die Medien als auch noch innen zu den Abgeordneten. Mehr als 3000 Seiten, darunter viele der größten OS/FS-Seiten hatten eine Protest-Seite vor ihre Webseite geschaltet, um auf die Eurolinux-Petition hinzuweisen. Innerhalb von drei Wochen schnellten die Unterstützerzahlen von 160.000 auf 280.000 bei der ersten Lesung am 24. September herauf. Leider wurde die Richtlinie nicht abgelehnt, wie von uns und den Grünen gefordert, dafür hatten wir aber bei den Abgeordneten das Bewusstsein für die Relevanz ihrer Entscheidung gesteigert und diese entschärften die ursprüngliche Vorlage. Ideen und Logik sind demnach vorerst ausgenommen.

Erschreckend war die erste Lesung zur Direktive, an der höchstens 20 Abgeordnete, Mitarbeiter und Kommissionvertreter im Raum teilnahmen. Ohne Lobbying von unserer Seite und alternative Voting-Liste, damit die Abgeordneten bei 129 Änderungsanträgen den Überblick behalten, wäre die Direktive wahrscheinlich mit amerikanischen Verhältnissen durch gekommen. Allerdings wird sie nun vermutlich am 10. November vom Europarat der Justizminister behandelt, die sie gewiss nicht so entschärft akzeptieren werden. Spannend wird also die zweite Lesung.

Die Euroalliance hatte sich 1999 als Netzwerk verschiedener europäischer Organisationen und Initiativen gegründet und eine Petition (petition.eurolinux.org) gegen die geplante grenzenlose Patentierbarkeit von Software online gestellt.

UML and VMware in honeypot environments

von Davide Del Vecchio <dante@alighieri.org> und

We have two principal ways to virtualy grow up an honeypot, one is User Mode Linux (UML), and the other is VMware. I will show you how to configure them, how they work and how they could be detected.

User Mode Linux - UML

User Mode Linux is an OpenSource solution that creates a virtual machine, so you can run multiple Linux instances. The "guest" host kernel receives system calls from the application inside the VM that will be processed by the host kernel.

To run User Mode Linux, you need to compile a new kernel, a user mode one. Just a few steps to make it work. Download the latest UML patch from the uml-downloadsite at sourceforge [1]. Download the *matching* kernel from a kernel mirror. Make a directory and decompress the kernel sources into it.

```
dante@sofficino# make uml;
cd uml
```

Apply the patch with this syntax:

```
dante@sofficino# bzcat uml-
patch-2.4.20-7.bz2 | patch -p1
```

Now compile the new kernel with:

```
dante@sofficino# make menuconfig ARCH=um #(or
what you prefere)
```

and after

```
dante@sofficino# make modules ARCH=um
```

You can also install the uml_utilities from the uml-website. Now you have to create a file system for your uml, but it is easiest for you to download a "standard" file system from the uml website.

So you will get a "linux" executable that is the new compiled kernel. Now you have to run the "linux" executable in this way:

```
dante@sofficino# ./linux ubd0="root_file_
system_image"
```

The UML has a lot of usefull capabilities, too, such as:

- TTY Logging: capture keystroke, even if connections are made over an encrypted protocol.
- HPPFS: it limits the ability to access/modify /proc filesystem.
- SKAS MODE: It makes kernel binary and data totally invisible to its processes.

VMware

VMware [2] is the other solution. It is a commercial application. And basically emulates an other computer with its own hardware and BIOS. On this virtual host you can install almost every operating system. An other capability of this application is to run on MS Windows, too.

It's really easy, take the VMware package and unzip it:

```
dante@sofficino# unzip vmware_package.zip
```

decompress the tgz package:

```
dante@sofficino# tar xvfz vmware_package.tgz
```

enter the vmware-distrib directory:

```
dante@sofficino# cd vmware-distrib
```

and launch the installer and after that the configuration tool:

```
dante@sofficino# ./vmware-installer.pl
dante@sofficino# ./vmware-config.pl
```

Now your VMware is installed, you have to do nothing more than to launch vmware and power ON the vir-

tual machine, you will be prompted to the GUEST OS installation procedure. So easy that I will not explain you more... you have to have in mind only two important concepts.

During the installation process we will be presented to a lot of choices that will influence our work. The first concept to introduce is the difference between raw and virtual disks. So we can choose between installing the guest operative system on a physical disk or on a virtual disk. A virtual disk basically is, a set of files that VMware presents like a real hard drive, obviously the major advantage is convenience, but if your scope is a deeper forensic analisys, phisical disk is your choice.

The second concept is how to configure the disk modes on your virtual machine. You have three ways to configure them:

- Persistent: Every change made on the virtual disks are immediately and permanently written to the disk.
- Non persistent: The contrary of the previous mode, no changes are made.
- Undoable: made originally for disaster recovery purpouses, it's really usefull for us, in fact it will be our choice. Every change will be written into a file called „redo log". At the end of the virtual machine session we can choose between commit changes, discard them or keep the „redo log".

It's really easy to understand that we can examine the redo log to monitor what the attacker will do. We can parse it just using the `string` command.

```
dante@sofficino# tail -f *REDO | strings -a
>honey.log &
dante@sofficino# tail -f honey.log
```

To see in real time changes on the REDO logs. Now i will show you some data of a breakin:

A succsesfull Attack

Here are some logs a friend of mine caputered while running a SuSE-Linux honeypot. A complete analyse of this attack whould be to much for the DS. We just want to give you a short impression. Complete analyses of attacks to honeypots can be found here for example:

- http://www.packetfu.org/hpa.html [3]
- http://honeynet.nihilisme.ca/scans/scan18/som/som25/analysis.html [4]

Logs are anonymized by us, since we respect the privacy of the involved computers. We changed logformat a little to improve readablity. First let's have a look at the snort-alert-logs:

```
[...] snort: [1:648:5] SHELLCODE x86 NOOP
[...]
[...] snort: [1:648:5] SHELLCODE x86 NOOP
[...]
[...]
[...] snort: [1:498:3] ATTACK RESPONSES id
check returned root [...]
```

Nothing special - snort discoverd the attack. Why do poeple use such stupid shellcodes and type

```
id
```

in an unencrypted rootshell? Now, i will show you the snort-ASCII-logs from the rootshell connection:

```
# unset HISTFILE; echo „*** JE MOET JE MUIL
HOUWE“;uname -a;id;
*** JE MOET JE MUIL HOUWE
# w
 12:41pm  up 3 days, 20:50,  0 users,  load
average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@
IDLE   JCPU   PCPU  WHAT
# last root
wtmp begins Tue Apr 15 16:33:17 2003
# gcc -v
Reading specs from /usr/lib/gcc-lib/i486-suse-
linux/2.95.3/specs
gcc version 2.95.3 20010315 (SuSE)
# uname -a
Linux suse03 2.4.10-4GB #1 Tue Sep 25 12:33:54
GMT 2001 i586 unknown
# cd /var
# cd spool
# ls
[...]
samba
vscan
# mkdir linzz
/usr/sbin/useradd -d /var/spool/linzz linzz
# uptime
 12:44pm  up 3 days, 20:52,  0 users,  load
average: 0.00, 0.00, 0.00
# ls /home
asmith
jony
lisa
# passwd linzz
New password: linzz123
Re-enter new password: linzz123
Password changed
# w
  1:04pm  up 5 days, 21:13,  1 user,  load
average: 0.00, 0.00, 0.00
USER     TTY      FROM              LOGIN@
IDLE   JCPU   PCPU  WHAT
linzz    pts/0    10.185.11.173     12:55pm
30.00s  0.94s  0.53s  vi /etc/passwd
```

The time on the honeypot is incorrect. This makes the honeypot look like a lazy administrated system, but data analysis gets more complicated. Now the attacker logs in using ssh. Data capture is no problem, since sebek was installed on the honeypot:

```
[...]
19:35:49 cd source
19:36:04 BitchX
19:36:55 ./BitchX
19:41:14 su jony
19:41:21 BitchX
19:41:25 ls
19:41:36 cd
19:41:43 ls
```

```
19:41:47 BitchX
19:41:53 cd BitchX
19:41:58 ls
19:42:01 cd source
19:42:10 ./BitchX 10.127.14.23
19:43:06 w
19:43:08 ls
19:43:09 cd
19:43:13 cd
19:43:14 ls
19:43:19 rm BitchX
19:43:24 rm -rf BitchX
19:43:31 rm BitchX-1.0c17.tar.gz
19:43:36 clear
19:43:40 ps
19:43:42 exit
19:43:47 w
19:43:51 exit
[...]
```

Wow, the attacker installed a IRC-Client -*bad idea*. The attacker was a scrippt kiddie, as most of the times. Even too stupid to install a backdoor or clean up the logfiles.

Fingerprinting

So, here's the focus: Our blackhat souls come up, and we ask ourselveshow can we discover if we have been trapped ?

Fingerprinting VMware

Let's have a look at VMware: Note, very importantly, that we do not have proves, but just traces. First thing, I could ask myself why on a Celeron 600 I have just a 2Gb hd, or 64Mb RAM -> `df -h` and other simple commands like this. Secondly, we can notice the Hard Disk on which the operative system is installed on is a SCSI (VMware installs by default the OS simulating on SCSI disks). Ethernet PCI is always the same model (VMware emulates just pci driver for the same ethernet card). Looking at the the video card we can clearly see `VMware`

Finally we can perform a time analysis with an `hdparm -t` , if the disk results slower than a normal SCSI (because it is an IDE disk) it will be an emulated one.

Fingerprinting UML

On UML it's funnier, since we have two ways to use uml with or without some specific options. Without any options we simply have to `cat /proc/ksyms` and we can see that the kernel binary runs into memory addresses that are equivalent of user space, not kernel one: *The kernel runs like an application!* More interesting, however, is the possibility to brake out of the UML and gain access to the host operative system. *Infact in a post on bugtraq by Andrew Griffits he affirms and demonstrates that playing with sys_call_tables you can brake out a user mode linux.* The bug mentioned in the post by Griffits works only on a specified linux kernel. I'm actually working on it. More information here [5].

But to limit access to the `/proc` file system and to improve the capabilities of uml under honeypots the `jail` and the `honeypot` options have been implemented to uml. So let's see which changes we find on our honeypot and how we can detect it: I cannot even

```
cat /proc/ksyms
```

anymore, and that is strange for a normal system. So, no normal `/proc` entries is a good point to start from. Now let's cat:

```
dante@uml# cat /proc/1/environ
dante@uml# cat /proc/cmdline
dante@uml# cat /proc/cpuinfo
```

q.e.d.

Conclusion, considerations...

Obviously, a really good system administrator will hide all this traces, but a good hacker will find another 1000 of them. Script kiddie versus script kiddie. Hacker versus Hacker. So finally I would like to leave you with an ethical question that, I hope, everyone who worked on honeypots tought about this at least once:*Will honeypots become the future of full disclosure and interaction between minds, or the tool of the big companies to trap our knowledge and use it against us?*

[1] *http://user-mode-linux.sourceforge.net/dl-sf.html*

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

[3] *http://www.packetfu.org/hpa.html*

[4] *http://honeynet.nihilisme.ca/scans/scan18/som/som25/analysis.html*

[5] *http://www.securityfocus.com/bid/3973/info/*

Bericht: CCC-Camp 2003

von Felix von Leitner <ds@fefe.de>

Insgesamt war es sehr spaßig, auch wenn es wie ja auch vorher schon im Grunde klar war insgesamt Verlust eingefahren hat. Ich denke, man muß das wie Jeedi sehen: mit den nächsten vier Kongressen haben wir das wieder drin. Und alle vier Jahre muß man sich sowas halt einfach mal leisten.

Ich kam am 0. Tag an, einen Tag vor offiziellem Beginn. Spiegel Online hatte das Camp gerade als "Cyber Woodstock" bezeichnet, und die Presse stapelte sich förmlich; die Nerven der Veranstalter lagen frei. Es sah so aus, als würde sich dadurch ein enormer Ansturm ergeben, und so hielt ich es für angeraten, mein Zelt möglichst frühzeitig aufzubauen, bevor ich gar keinen Platz mehr kriege. Ich hatte auch meine Familien dabei, die sich neugierig umguckten, und am Ende so begeistert waren, daß sie die ganzen 4 Camptage auch noch kamen und sich hauptsächlich beim Kinderchaos-Zelt am See aufhielten. Und so kam es, daß ich zwar ein Zelt aufgebaut hatte, aber dann doch jeden morgen eine Stunde hin und jeden Abend eine Stunde zurück nach Hause fuhr. Immerhin war ich so immer frisch geduscht und hatte auch ein WC zur Verfügung, was mir im Laufe des Camps von einigen Seiten großen Neid einbrauchte, denn die sanitären Anlagen waren mal wieder völlig unter aller Sau, ekligst stinkende Dixie-Klos halt. Die Situation war so schlimm, daß die Leute 5 Kilometer zum nächsten MacDonald's fuhren und dort die Klos nutzten, denen man im Laufe des Camps auch deutlich ansah, daß sie überdurchschnittlich häufig frequentiert wurden.

Vor den Duschen gab es auch Schlangen von bis zu zehn Leuten (man muß dazu sagen, daß da 35 Grad herrschten und es bei den Duschen keinen Schatten gab, da haben sich also nur echte Härtefälle wirklich in die knallende Sonne gestellt zum Warten). Die anderen sind halt in den See gesprungen, wo im Laufe des Camps gar wunderliche Lebensformen gesichtet worden sein sollen. Das Wasser im See wurde wohl so bis zu 26 Grad warm tagsüber, aber das war immer noch 10 Grad kühler als die Luft.

An den ersten drei Tagen gab es so gut wie keine Luftbewegung, so daß sich wirklich niemand in der Sonne aufhielt. Das war beim See ganz lustig, weil es da halt ein paar Bäume gab, deren Schatten dann im Laufe des Tages wanderte, und die Leute wanderten dann eben notgedrungen mit.

Ich kam mit Tobias an, und wir haben dann noch kurzfristig die Order reinbekommen, 30 Notdecken (diese super-reflektierenden Aludecken, mit denen man Verwundete einwickelt, damit die Körperwärme erhalten bleibt) zu besorgen, was noch einen hektischen Ausflug zur Metro in Pankow nach sich zog. Mit den

Decken sind dann die Datenklos abgedeckt worden, sonst wären die Router und Switches darin in der Hitze kollabiert.

Schon vom ersten Tag an auffällig war die Anzahl der Ausländer. Natürlich waren da auch viele Deutsche, und mit Holländern war ja im Grunde auch zu Rechnen gewesen, aber es waren auch Portugiesen, Spanier, Franzosen, Italiener, Amerikaner (ok, war auch klar) und natürlich diverse Skandinavier am Start, die sich trotz der Hitze erst mal in größerem Umfang mit Alkohol eindeckten. Stellenweise gab es im Supermarkt in Altlandsberg Gerüchten zufolge kein Bier mehr...

Zum Hacken war es im Grunde zu heiß auf dem Camp, und so gab es zwar insgesamt rund drei Terabyte Traffic (eins incoming, zwei outgoing), aber das waren eher automatisierte Angelegenheiten, man sah auch verhältnismäßig wenig Portscans. Gut, es gab da wohl mindestens einen rogue DHCP Server, der 192.168.* IPs austeilte, und ich sah Rop am zweiten Abend ein Kabel ausbuddeln, hinter dem ein ARP Spoofer stecken sollte, aber an sich war alles ganz friedlich. Es wurden nicht mal SSH Verbindungen gespooft, DNS lieferte auch korrekte Ergebnisse, und selbst Kernel Patches und die nmap Sourcen kamen unmanipuliert an. Gerade bei nmap wunderte mich das ja, denn der Autor verteilt das völlig unklarerweise ohne PGP Signatur.

Ich hatte ja eigentlich vor, da von meinem Notebook aus ein paar subversive Filmchen unter die Leute zu bringen, aber kam bis zum 4. Tag nicht mal in die Nähe von anständigem Internet. Stromverteiler waren im Hackcenter in ausreichender Anzahl vorhanden, und Kabel konnte man sich im NOC kaufen, aber Hubs gab es zu wenige, und bei Wavelan ging konsistent DHCP nicht, so daß ich erst abends zuhause Mail lesen konnte. Das war schon eher scheiße, und ich fragte mich schon, wieso das eigentlich so unglaublich schwierig ist mit dem Wavelan.

Ich hatte mich breitschlagen lassen, zwei Vorträge zu halten, einen über SIMD Hacking und einen über LDAP. Die waren natürlich noch nicht geschrieben, wie das so ist, und so verbrachte ich den Vormittag und die Mittagshitze des ersten Tages damit, über SIMD zu schreiben. Irgendwann gegen 14 Uhr fragte ich mich dann, wieso ich das eigentlich nicht abends zuhause machen kann und legte mich mit meiner Family in den Schatten am See.

Das Essen war dieses Mal so derartig überragend viel besser als beim letzten Mal, daß man das gar nicht genug würdigen kann. Es gab leckere Burger, leckere Waffeln, ein Thai war am Start, es gab selbstgemachte Pizzen, die auch echt lecker waren (gab es sogar in vegan, obwohl die wirklich unappetitlich aussagen)... das mit den Getränken war nicht so toll. Das nächste Mal sollten wir da einen Kühl-LKW mieten und da ein paar Paletten Aldi-Wasser reinladen und abverkaufen. So sind dann in der Hitze insgesamt auch etwas über 200 Hacker umgekippt und mußten ärztlich versorgt werden. Ein Skandinavier hat sich fast ins Koma gesoffen und mußte mit Krankenwagen abgeholt werden. Einem Studi (Doktorant?) wurde sein Notebook mit der Diplom (Doktor?) Arbeit geklaut oder vielleicht auch verwechselt und eingepackt, jedenfalls war der plötzlich weg, und in dem Kontext hat die bearbeitende Polizei dann wohl über das Camp gesagt "ja, das muß ja sehr schön sein da, wir dürfen da ja nicht hin..." Das müßte man mal von unseren zuständigen Konspirologen prüfen lassen, was der CCC da plötzlich für einen Schutzengel mit Einfluß haben ;-) Die Telekom hat nicht nur mit ihrem CERT eine Warnung rausgegeben sondern teilweise wohl auch den ganzen IP-Bereich vom Camp gesperrt (obwohl man T-DSL-IPs noch erreichen konnte, vielleicht waren das nur Geschäftskunden?).

Aus dem NOC gab es dann noch die lustige Story, daß ein Switch nicht lief, und dann haben sie halt das Modul rausgenommen und woanders rein getan, und daraufhin war der Switch auch kaputt, und um sicher-

zugehen haben sie das dann in den 3. Switch getan, der dann auch kaputt war. Das ist also das Cisco-Killer-Modul. Cisco müssen ja die Exploits in letzter Zeit echt unangenehm gewesen sein, jedenfalls haben die uns diesmal mit Hardware förmlich zugeschüttet und

auch kurzfristig noch ein OC3-Modul (?) herangeschafft, von dem gewöhnlich gut informierte Quellen hinter vorgehaltener Hand munkeln, daß das das Backup-Modul des DFN gewesen sein soll, die ja nun nicht gerade ein kleiner Kunde sind. Irgendein Problem mit der Cisco-Hardware hat das NOC dann aber doch davon abgehalten, beide Hälften der Bandbreite nach draußen auch durchzuschalten, so daß im Effekt "nur" die Hälfte zur Verfügung stand, aber das war mehr als genug, zumal man da ja eh nicht zum Saugen hingeht.

Auffallend war übrigens der Frauenanteil. Eine Zeitung schätzte was von 20%, und ich würde mal sagen, daß das hin kommt. Die Hacker werden alt und bringen ihre Familien mit... ;) Es gab auch gut 10 Kinder zwischen 1 und 10 auf dem Camp, von denen einige sich wohl als richtig gute Lockpicker herausstellten.

Einige Hitzeresistente haben dann in der knallenden Hitze Schwertkämpfen wie im 15. Jahrhundert geübt, aber das war mir dann schon ohne Bewegung zu heiß in der Sonne. Die C-Base hat einige coole Aktionen geplant, an denen ich aber auch wegen Hitze nur aus der Ferne beigewohnt habe. U.a. gab es da ein Go-Spiel mit menschlichen Go-Steinen (man bekam einen schwarzen oder weißen Hut). Die meiste Zeit haben die da leider händeringend nach weiteren Steinen gesucht, während die schon verlegten Steine schwitzend und flehend die Passanten um Teilnahme baten. Es gab dann auch ein Jagger-Turnier (eine Art Rugby aber ohne Körperpanzer und dafür mit großen Waffen aus Schaumstoff), wo es aber keine Verletzungen gab. Dann stand da noch die Nerdschleuder rum, ein Gerät mit mehreren ineinander aufgehängten Metallringen, bei dem man sich dann im innersten am Schwerpunkt aufhängen lassen konnte, und sich dann halt in alle Richtungen rotieren konnte. Für mich sah das auch wegen der Hitze eher nach einem Magenentleerungsinstrument aus, daher hab ich mich da fern gehalten, aber alle Teilnehmer fanden das Ding wohl ziemlich cool. John Gilmore schien überhaupt echt viel Spaß zu haben auf dem Camp, der hat da zumindest beim Nachschmieren geholfen, ich glaube er wird da auch mitgeschleudert haben; ich konnte mir ja die Frage nicht verkneifen, wie er denn nun nach seiner Terroristen-Flugzeug-Aktion her gekommen sei ;-)

Erstaunlich wenig Probleme gab es mit Mücken, im Grunde waren da nur ein halbes Dutzend von in Wassernähe aktiv. Der Rest des Camps hat dafür unter Wespen gelitten, und Gilda ist auch prompt von einer gestochen worden. An einigen Stellen haben die Leute dann von Plastikflaschen das obere Drittel abgeschnitten und umgedreht geöffnet in die Flasche getan, als Wespenfalle, und man sah in diesen Teilen dann auch regelmäßig 20-50 tote Wespen schwimmen, aber die Population nahm nicht merklich ab dadurch.

Der heimliche Camp-Knüller war ein Nerd-Porno, den offenbar jemand von der Defcon importiert hatte. Das muß man sich so vorstellen, daß da Mädchen aus der nmap Man Page vorlesen und sich dabei ausziehen. Unglaublich. Das soll in der ersten Nacht plötzlich auf dem großen Beamer im Hackcenter gelaufen sein, und in der dritten Nacht gab es noch ein Screening davon zwischen den BSD-Zelten. Die Situation war echt surreal: da stehen 100 Nerds um eine Leinwand rum, wo dieser Film läuft, und keiner sagt was. Ein Passant sieht das und ruft "hey, boah, was ist das denn" und die Geeks drehen sich zu ihm um und meinen "Pschhhhhhhht!" Echt zum Totlachen, "was hat sie gerade gesagt? Promiscuous mode?"

Die Vorträge waren qualitativ eher Durchschnitt bis lauwarm. Ich persönlich habe kaum welche mitbekommen, weil ich mich damit der Fertigstellung meiner eigenen Folien gestreßt habe oder am Wasser lag, aber das war so ziemlich Konsens bei den Geeks, mit denen ich mich unterhalten habe. Einige Ausnahme gab es (neben meinen, hoffe ich): Die Jungs von Phenoelit haben da recht unterhaltsam über Cisco und Siemens Phones gerantet, und Ollie Whitehouse von @Stake soll da großartige Sachen über GSM/GPRS/UMTS erzählt haben, was ich leider nicht mitbekommen habe, weil ich parallel LDAP machen mußte. Ein echtes Highlight hätte auch der 9/11 Vortrag von Bröckers und Wisnewski sein sollen, leider hab ich die erste Dreiviertelstunde verpaßt, und das war genau der Teil von Wisnewski, den ich gerne gehört hätte. Von Bröckers hab ich ja schon das Buch gelesen, aber er hat sich da augenscheinlich echt Mühe mit der Übersetzung einer schönen Kampfschrift gegeben, die er dann da vorgetragen hat. Eine der für mich neue Aussagen an diesem Abend war, daß das Kühlsystem im World Trade Center explizit darauf ausgelegt war, auch bei Feuer und Explosionen die Temperatur unter der Schmelztemperatur der Stahlträger zu halten, und das System hat nur versagt, weil in beide Türme ein Flugzeug flog. Wenn ein Flugzeug verfehlt hätte, wäre keine der Türme eingestürzt.

Leider verpaßt habe ich auch einen Vortrag über nonlethal weapons. Das ist auch echt doof, und ich guck mal, ob ich da noch nen Mitschnitt des Audio-Tracks kriege oder die Folien oder so.

Ansonsten ist noch die Windhose erwähnenswert. Am dritten Tag wehte plötzlich eine Plastiktüte vorbei, dann ein Handtuch und schließlich ein Schlafsack. Nicht nur so ein bißchen durch die Luft, der wurde von einer Windhose mitgerissen, wirbelte konzentrisch immer weiter nach oben und war irgendwann gar nicht mehr zu sehen. Gerüchten zufolge ist auch ein ganzes Zelt über das Hackcenter-Zelt geweht worden, das habe ich aber nicht gesehen. Das lustigste daran war, daß alle möglichen Hacker sofort genau wußten, welcher Nerd da gerade wieder Mist gemacht hat und bestimmt dafür zuständig ist. Eine signifikante Anzahl von Leuten vermutete, daß Frank da mit seinen Raketenexperimenten Schuld ist ;)

NOC Review

von NOC <noc@camp.ccc.de>

Das Chaos Communication Camp 2003 stellte an die Netzwerkorganisatoren hohe Ansprüche. Zu den von den Congressen bekannten Unwägsamkeiten vieler "bösartiger" Clients, drängelnder Netzjunkies auf Entzug, ständiger vollständiger Saturation des Uplinks und einer eher "organischen" Organisation der Netztopologie kamen für Hacker ungewohnte physische Komponenten wie Temperatur jenseits der Rechenzentrums-Toleranzen, Matesupplyausfälle und ernsthafte körperliche Arbeit. Die Datenschleuder hat mit Hannes, einem der Helden an der Internetfront gesprochen.

*DS:*Guten Tag Hannes. Als allererstes interessiert natürlich, wie man einen Acker fernab jeder Zivilisation (Altlandsberg, nordöstlich von Berlin) mit Internet versorgen kann. Wie schnell war denn nun das zur Verfügung stehende Netz und wie intensiv wurde es genutzt?

Hannes: Unsere Anbindung war eine Richtfunkstrecke (STM1, 155 MBit) nach Neuenhagen. Von dort aus hatten wir eine Glasfaser (SDH STM1) nach Berlin von EDIScom gesponsort. Versatel sponsorte uns eine Glasfaser von Berlin zum ECIX [0]. Im ECIX stand eine Juniper M10, die das Peering zu Global Access, BerlinNet und KPN machte. Global Access sponsorte 45 MBit/s, BerlinNet 20 Mbit/s und KPN den Rest. Insgesamt haben wir 3,5 TB outgoing und 1,1 TB incoming Traffic gemacht.

*DS:*Das ist welcher Anteil an der maximal möglichen Netzauslastung?

Hannes: Das Problem war, dass die Cisco-Hardware, die wir für die Anbindung der KPN-Leitung brauchten, nicht so tat, wie sie sollte. Wir konnten die KPN-Leitung nur eingeschränkt benutzen (da sie durch die defekte Hardware zuviel packet loss verursachte). Es blieb bis heute unklar, ob es tatsächlich an den Cisco-Routern lag, oder an der Faser von KPN oder an unseren Fasern (die Patchkabel zwischen den Geräten und KPNs Fasern). Also, die Bandbreite, die da war, wurde immer vollständig ausgelastet. Es ist eh egal, wieviel Bandbreite zur Verfügung steht, die wird *immer* vollständig ausgelastet.

*DS:*Wie habt ihr das Internet gerecht über den Acker verteilt?

Hannes: Der Core Switch (Cisco Catalyst 6509) befand sich im NOC und machte sämtliches Inter-VLAN Routing. Wir hatten neun Access Switches (Cisco Catalyst 4006), je einer in den sechs Datenklos, einer im Radiozelt und zwei im Hackcenter. Die neun Access Switches haben wir sternförmig vom NOC mit je 2 GBit/s LWL angebunden. Zusätzlich war jeder Access Switch mit jeweils einem anderen mit 1 GBit/s LWL verbunden.

*DS:*Wie konntet ihr die Datenklos mit LWL versorgen, ohne dass dort Nerds drüber stolpern?

Hannes: Wir haben mit einem T-Träger am Trecker Furchen in die Wiese gemacht, diese mit dem Spaten weiter ausgegraben, dann die Faser reingeworfen und wieder zugeschüttet.

*DS:*Welches Setup benötigt man, um über 1500 Leute mit Wireless LAN versorgen zu können?

Hannes: Wir hatten 3 Türme, die wir mit jeweils 8 Sektorantennen [1] und 8 Access Points (Cisco Aironet 350) bestückten. Jede Sektorantenne hatte einen Öffnungswinkel von 54 Grad, daraus ergab sich eine Überlappung von 9 Grad pro Antenne. Die Access


Das Camp-Backbone wurde verbuddelt.


Das "Cisco-Killer-Modul" blieb leider ungezähmt.


Materialausgabe


Der Altlandsberger Funkturm

Points benutzten die Kanäle 1, 6 und 11, da nur die drei nicht überlappend sind und nicht interferieren [2].

*DS:*Funktionierte denn alles sofort?

Das Wireless LAN konfigurierten wir zuerst, nach der Umfrage während des NOC Reviews des letzten Congresses [3] mit 3 SSIDs, damit war zwar kein Roaming möglich aber die Broadcast-Domains für das Wireless LAN waren kleiner. Alle Access Points eines Turmes bekamen ein /23 (512 Adressen) geroutet. Das funktionierte nicht, da die Clients immer zwischen den SSIDs (camp tower [1-3]) wechselten und jede SSID andere Subnetze routete.

Daher benutzten wir später nur noch eine SSID (camp), Roaming war möglich, das gesamte Wireless LAN war eine Broadcast-Domain und bekam ein /21 (2048 Adressen) geroutet. Wir verringerten die Leistung der Access Points und installierten einen weiteren im Hackcenter.

*DS:*Und wieviel Hacker hättet ihr mit einer IP ausstatten können?

Hannes: Als IP Range bekamen wir 81.161.128.0/18 (16384 IPs). Damit konnte jeder Access Switch ein /23 (512 Adressen) bekommen.

DS: Und diese Adressen habt ihr auch gerecht verteilt?

Wir benutzten Sauron [4] zur Verwaltung des DHCP und der DNS Zonen. Über ein simples Webinterface konnte sich jeder Benutzer einen DNS-Eintrag zu seiner IP machen. Die eingetragenen Daten wurden in die Sauron Datenbank übertragen und daraus die Konfigurationen generiert, die per ssh an DNS und DHCP Server übermittelt wurden. Da wir tinydns benutzen wollten und sauron ursprünglich nur bind Konfigurationen erzeugt, mussten wir zuerst den Sauron so ändern, dass er tinydns-data files generierte. Das System funktionierte gut, es gab etwa 215 Leute, die sich einen DNS-Eintrag machten. Einer davon war www.camp.ccc.de :).

*DS:*Wir danken für das Gespräch.

[1] *http://www.ber.ecix.de/*

[2] *http://www.wimo.de/verteiler.htm?wlandirout_d.htm*

[3] *http://www.cisco.com/en/US/products/hw/wireless/ps469/products_data_sheet09186a008008883b.html*

[4] *ftp://ftp-19c3.ccc.de/pub/19C3/19C3-461-noc-review.mp4*

[5] *http://sauron.jyu.fi/*

OpenDarwin

Mit MacOS X trat Apple erstmals im grossen Stil der *NIX-Welt bei. (Wer erinnert sich noch an A/UX, dem Apple UNIX? Eben...)

Der OS Kern namens "Darwin" ist dabei ein eigenständiges OpenSource Projekt welches mit OpenDarwin mittlerweile eine eigene Distribution hat. Auf dem Camp hatte die Datenschleuder Gelegenheit, mit dem Maintainer dieses "unbekannten UNIX" zu sprechen.

DS: Du bist Lead-Mitglied im OpenDarwin Projekt. (?) Was ist Darwin? Und in welchem Verhältnis steht das OpenDarwin Projekt zu Apples MacOS X?

FK: Ich gehöre zum sogenannten 'Project Lead' von DarwinPorts. DarwinPorts ist ein Projekt welches zum Dunstkreis von OpenDarwin gehört. Ziel des Projektes ist einen Ports-Tree (und entsprechendes Packaging) für Mac OS X und (Open)Darwin anzubieten. DarwinPorts selbst ist in grössten Teilen in Tcl implementiert, hat dementsprechend einen hohen Portabilitätsfaktor. Ich setze DarwinPorts zum Beispiel auch auf Free- und OpenBSD ein. Ein entscheidener Vorteil von DarwinPorts ist, das nicht ein bestehendes Ports-System/Packaging-System recycled wurde sondern komplett neu konzeptioniert wurde und sich dadurch langfristig (hoffentlich) viele Probleme/Grenzen die mit anderen System auftauchen vermeiden lassen. Eine möglichst lange Liste an unterstützten Plattformen ist mit eines meiner Ziele. OpenDarwin selbst versucht die Open-Source-Aktivitäten rund um Darwin zu bündeln, um so die Zusammenarbeit mit Apple zu erleichtern. Darwin ist der Unterbau zu Apple's Mac OS X. Mac OS X setzt sich aus den Komponenten Darwin, Carbon, Cocoa, Aqua, Quartz (Extreme), Java (etc.) zusammen. Dabei beinhaltet Darwin sowohl den Kernel als auch das entsprechende Unix-Userland. Darwin ist von Apple als Source erhältlich und unterliegt der (auch von der *sigh* FSF anerkannten) Apple Public Source License (APLS) 2.0. Im Rahmen des OpenDarwin-Projekts gibt es die sogenannten 'OpenDarwin-Releases' die als Basis den Source-Code von Apple haben, von uns allerdings modifiziert und erweitert wird (frei nach dem Motto: 'sucks less' :)

*DS: Darwin ist Mitglied der BSD-Familie. Was sind die Hauptunterschiede zu den *anderen* BSDs, sprich Open-, Free- und NetBSD?*

FK: Der Unterschied fängt beim Kernel an. Salop gesagt, hat Darwin einen Hybrid-Kernel, der aus einem Mach-Kernel sowie einem BSD-Kernel besteht. An vielen Stellen bemerkt man nach wie vor den Ursprung von Darwin, der ja in NextStep liegt. So wird NetInfo als Directory-Service verwendet. rc startet nicht das komplette System, sondern bootstrapped das System nur soweit bis 'SystemStarter' übernimmt.

DS: Worin besteht Deine Arbeit als Maintainer konkret? Wieviel Zeit verwendest Du darauf? Welche Aktivitäten verfolgst Du sonst noch im BSD-Bereich?

FK: Im Rahmen von OpenDarwin/DarwinPorts mache ich eine Vielfalt an Arbeit. Dies fängt bei der Koordination der Entwickler von DarwinPorts an, geht über die PR-Arbeit (Booth-Bunny :>) bis hin zu den normalen Entwickler-Tätigkeiten wie Pflege/Wartung von Code, Bug-Fixing und Weiterentwicklung. Angefangen habe ich bei DarwinPorts als reiner Maintainer von Ports, mittlerweile arbeite ich hauptsächlich an der Infrastruktur (also dem Herz von DarwinPorts) und räume hinter unseren Entwicklern auf :) Im Rahmen einer Hiwi-Stelle an der Uni schraube ich an FreeBSD rum, wobei das hauptsächlich Software-Portierungen sind. Ich verfolge nach wie vor das Geschehen rund um OpenBSD, welches für mich eigentlich das Unix der Wahl ist.

DS: Wie bist Du ursprünglich zur Computerei gekommen? Und was hat Dich in die Unixwelt gebracht?

FK: Hehe. Als ich in der Grundschule war und alle meine Freunde einen C64 hatten, wollte ich auch unbe-

dingt Einen haben. Mein Vater hielt vom C64 eher wenig und stellte mit einen 8086 mit (jeah) 8 mhz hin. Anstatt wie alle anderen am Computer Spiele zu spielen, fand ich recht schnell Dinge wie Pascal etc. Jahre vergingen und irgendwann fing der Computer an Staub zu sammeln. Als ich dann bei einem Freund in den USA 'Internet Relay Chat' sah und bemerkte wie sich da Leute weltweit unterhielten und Daten tauschten hat es mich gepackt. Zurück zu Hause wurde also das Modem aus Vaters Schrank entwendet und entsprechend genutzt. Recht schnell fand ich Usenet und sah, das man um einen Newsserver laufen zu lassen am besten ein Unix einsetzte. Es kam ein Debian, ein paar Jahre später dann OpenBSD. Wie bei vielen Anderen wurde dann Hobby (auch) zum Beruf. Usenet hat an Priorität verloren, und stattdessen ist das Entwickeln von Software getreten.

DS: Wie ausgereift ist (Open)Darwin? Wird es bereits in Produktionssystemen eingesetzt? Und die x86-Version?

FK: Nein, und das ist auch nicht das Ziel. OpenDarwin zielt eindeutig auf Entwickler ab, die Lust haben sich mit der Technology die in Mac OS X steckt auseinander zu setzen. Ich persönlich fände es schön, wenn wir die OpenDarwin-Releases soweit bekommen, das es eine Alternative zu anderen freien Unixen bietet, aber das wird noch ein (längeres) Weilchen dauern (was hauptsächlich daran liegt, das uns schlichtweg Manpower fehlt). Sofern man die richtige Hardware hat, lässt sich die x86-Variante recht gut einsetzen, wobei ich behaupte das die meisten Anwender besser mit Free- bzw. OpenBSD beraten sind. Woran es nach wie vor fehlt, sind Treiber. So unterstützen wir auf x86 bisher nur Netzwerkarten von Intel sowie aus der 3c905'er Serie von 3com. Von Sachen wie S-ATA, Sound und Co. will ich gar nicht erst anfangen :)

DS: Du benutzt ein Apple Powerbook unter OpenBSD und MacOSX, bist technisch gesehen also Mac User. Bist Du das erst seit Apples Umstieg auf MacOSX oder hast Du auch bereits das 'klassische' MacOS benutzt?

FK: Ich habe Mac OS 9 (oder vorherige) nie benutzt und fand/finde sie auch nicht attraktiv. Ursprünglich als ich mir das Powerbook zugelegt habe, wollte ich auch sofort OpenBSD darauf installieren und habe mir nur spasseshalber mal OS X angeschaut. Irgendwie hat es micht gepackt und ich habe es draufgelassen.

DS: Hast Du jemals mit NextStep (dem Vorläufer von MacOS X) zu tun? Falls ja, was war Dein damaliger Eindruck?

FK: Leider nein. Bin immer noch auf der Suche nach einem Next Cube :)

DS: Kannst Du Deine Erfahrungen und Arbeiten im OpenSource-Bereich allgemein und im BSD-Bereich im Besonderen auch lukrativ einsetzen? Ist OpenSource Teil Deiner geschäftlichen Existenz oder nur "Hobby nebenbei"?

FK: Die Arbeit die ich zur Zeit im Rahmen von OpenDarwin/DarwinPorts mache ist hauptsächlich hobby. Einen Teil der Efahrung kann ich geschäftlich nutzen, da meine Firma dadurch auch Consulting bzw. Entwicklung (Treiber/Applikationen) im Mac OS X Umfeld anbieten kann. Die allgemeine Erfahrung die ich mit Unix habe lässt sich auf jeden Fall nutzen, sie ist schliesslich Basis der Arbeit meiner Firma.

DS: Noch wird OpenSource in der Öffentlichkeit -- wenn überhaupt -- hauptsächlich mit Idealismus und Anti-Microsoft-Bestrebungen assoziiert, teilweise nicht ganz ohne Grund... Siehst Du, als jemand, der unter realen Bedingungen mit OpenSource arbeitet, einen Wandel in dieser Wahrnehmung bei Leuten (Kunden?), die vorher noch nicht damit in Berührung gekommen sind? Sind die Tage der Vormachtstellung von Microsoft gezählt?

FK: Das ist Politik. Ich mache keine Politik, sondern arbeite mit OpenSource-Komponenten, da diese mir erlauben Sie zu verändern. Das politische Brim-Bam-Borium ist nicht mein Ding.

DS: Stichwort "Humppa!". Warum trinken BSD-Verfechter lieber Bier als Mate?

FK: Weil Bier besser als Mate schmeckt bzw. weil Mate nicht schmeckt? :)

Mit Felix Kronlage sprach Tom Lazar.

Howard Rheingold, David Isenberg, James Roberts at O'Reilly ETCon. (via BoingBoing.net)

Demos und so

von krill/plush aka gunnar ruthenberg

Demoszene auf dem Chaos Communication Camp 2003

Als jemand, der aus der Demoszene stammt und die Hackerszene nur periphär wahrnimmt, war ich nur das letzte Wochenende auf dem Camp. Nachdem ich mich so langsam akklimatisiert hatte und anfing, erstmal diverse Chatkanäle zu joinen, Mate zu organisieren und das Wiki zu checken, fing gerade der Demoszene-Workshop von dipswitch und pandur, die beide Mitglied der Demogruppe Iron Maiden sind, an.

Ich war positiv überrascht, auf dem Camp was von der Demoszene zu hören und hab das Geschehen auf halbem Ohr und Auge verfolgt, während ich chattete. Ich war ziemlich gespannt, wie wohl die Reaktion des vermutlich größtenteils Demounkundigen Publikums sein würde.

dipswitch fing an, etwas über die Wurzeln der Demoszene zu erzählen und begann, alte Crackerintros zu zeigen. die Leute im publikum hörten recht interessiert zu. Er machte weiter mit populären c64-Demos, die er (leider) auf einem Emulator zeigte, dessen Audiokonfiguration meiner Meinung nach etwas zu wünschen übrig ließ - als c64-Democoder fand ich den Klang der c64-Sachen extrem dürftig. Auf Demoparties ist die dicke PA-Anlage auf vollen Baß gestellt und die Höhen, die bei klassischen Synthesizerchips wie dem Sid im c64 im Allgemeinen die Tiefen verquäken, sind stark gedämpft, was dann zu für diese Hardware-Verhältnisse äußerst beeindruckendem Klang führt. Ich fand schön, bei den c64-Demos ein recht interessiertes Publikum zu sehen, das sogar nach den Demos (später natürlich auch denen neuerer Systeme) Applaus gab. Ein zwar seltsames Phänomen, für die Werke Nichtanwesender zu applaudieren, aber das wird ja oft auch in Kinos so gemacht.

Da ich, wie gesagt, bis zum Anfang des Workshops nichts davon wußte und auch nicht erwartet hatte, alte mehr oder weniger flüchtige Bekannte aus der Demoszene zu treffen, ging ich freudig zur Bühne und sagte dipswitch und pandur erst einmal hallo. Auf dem Weg fielen mir wieder leute von den Medien auf, und ich bemerkte, daß die Hackerszene weitaus bekannter und auch populärer als die Demoszene ist. auch kein Wunder, eigentlich.

Ich glaube, dipswitch fuhr dann mit Amigademos fort, kann mich aber nicht mehr so gut daran erinnern. Ich wollte ihm einige c64-Demos aufdrängen, was bei vielen Demos (vor allem meiner bisher einzig großen, die aber schon 3 jahre alt ist) aber daran scheiterte, daß sie nicht auf dem Präsentationsrechner waren, und dieser (sicherheitshalber, nehm ich an) auch keinen Netzwerkzugang hatte. Ich war zum Glück nicht ganz erfolglos und fand auf dem Rechner noch ein paar vorzeigbare c64-demos.

Während ich zwischen meinem Rechner und den beiden Vortragenden hin- und herpendelte, um hier zu chatten und zu bauen und da zu quatschen und zu kiffen, fuhr dipswitch mit aktuelleren, aber mittlerweile schon klassischen PC-Demos fort - es zeigte sich jetzt ganz deutlich, daß die beiden sich Demos ausgesucht hatten, die typische Beispiele für das Phänomen Demo sind, die also jeder kennt, der sich ein wenig damit beschäftigt. Somit war nichts außergewöhnliches, avantgardistisches oder ungewöhnliches, was Demos betrifft, zu sehen - was ich vollkommen in Ordnung fand, im Gegensatz zu einigen demokundigen Leuten im IRC.

Einige bemängelten nämlich, daß man das Zeug sowieso alles schon kenne. Sicher, aber nur, wenn man Vorwissen mitbringt. Dieser workshop wurde aber offensichtlich für ein Publikum gemacht, daß so gut wie keine Demos kennt und von der Demoszene nur mal gehört hat. Ich denke, das konnte man vom größten Teil der Zuschauer sagen. Diesen Leuten haben die gezeigten Demos sichtlich Spaß gemacht, und auch im IRC habe ich viele beeindruckte, bis dahin demounkundige Leute vernommen.

der demobewanderte teil der Chatter unterhielt sich über ein altes Thema in der Demoszene - oldskool vs. nuskool. Einige meinten, heutige PC-Demos seien keine wirklichen Demos mehr, weil so Sachen wie directx oder opengl genutzt würden. Damit fielen große Teile des Programmieraufwands durch die Renderroutinen, die ja eigentlich das Herzstück jeder Demo seien, einfach weg, und auch in 64kb-Demos, von denen einige Klassiker gezeigt wurden, entfiel dadurch eine Menge

Code innerhalb der 64kb. Im klassischen Demosinne geschummelt, könnte man sagen. Auf diesem standpunkt stehe ich auch, teilweise.

Es ist einfach so, daß mit heutigen Standardcomputern und Hochsprachen flüssige und äußerst komplexe Effekte mit immer geringerem Aufwand realisiert werden können. Ich finde, rein optisch gibt es keine wirklich zu überwindenden Grenzen mehr. Das ist wohl ein Grund, warum es noch so viele Leute gibt, die Demos nur auf alten Homecomputern wie dem c64 oder Amiga coden. Da muß man noch viel optimieren, die Maschine in Assembler programmieren und hat Kontrolle über das komplette System, ohne daß man irgendwelche Kernel- oder Betriebssystemroutinen braucht. Man weiß halt nicht, ob ein bestimmter bis dahin neuer Effekt in gegebener Qualität von vornherein überhaupt möglich ist, bis man es schafft oder versagt hat. Man muß von Grund auf alles selbst machen. Das ist das, was diese art Demoprogrammierer (wie auch mich) reizt. Es geht nicht um ein nützliches Tool, das mit hilfe passender Bibliotheken schnell erstellt werden und möglichst bugfrei sein soll, es geht um die Grundlagen von effektiver Programmierung, darum, ein gegebenes Rechensystem maximal auszulasten - man will fortgeschrittene Binärarithmetik, Optimierung auf Opcode-Ebene, das perfekte Speicherplatz-Rechenzeit-Verhältnis und möglichst wenig Overhead bei jeglicher Operation.

Moderne Demos hingegen werden immer mehr zu dem, was sie irgendwie schon immer waren, nur mit immer weniger Betonung auf ihren technischen Aspekt. es sind Effektshows, die aber auch rein optisch durch Design und Style und rein akustisch durch einen sehr guten Soundtrack überzeugen wollen. Der Programmierer hat bei heutigen Demos keinen so bestimmenden Einfluß mehr wie früher, als durch technische Grenzen bestimmte Designgrenzen gegeben waren, an die sich Grafiker und Musiker halten mußten. Je besser der Programmierer es verstand, die Maschine auszureizen, desto mehr Spielraum hatten die beiden anderen im Kernteam. Heutzutage hat man Klang in CD-Qualität, Grafik in Truecolour und dickste Prozessoren in Computern mit 3D-beschleunigten Grafikkarten. Oft wird ein und das selbe Framework wird für mehrere Demos benutzt, der Programmierer hat da gar nichts mehr zu tun, während die Designer sich die Demos in speziellen flashartigen Editoren, in denen neue Effekte per Plug-in eingebaut werden, nur noch zusammenklicken. Es ist halt einfach genug Power da. Die einzig wahre Herausforderung ist es wohl nur noch, in Demos mit vorbestimmter Maximalgröße, also zum Beispiel 4kb- oder 64kb-demos, so viel wie möglich hineinzupacken. Da wird die Grenze wohl auch in fernerer Zukunft schwer auszumachen sein (wohl auch, weil immer mehr durch externe Bibliotheken übernommen wird).

Nach so einigen gezeigten Demos übernahm dann dipswitchs Kumpel pandur den Vortrag. Er begann, darüber zu reden, was man beim Democoden so zu beachten hätte, und wo man optimieren muß. Als Beispiel demonstrierte er, wie recht komplexe 3D-Objekte performant gepackt werden können, um diese in zum Beispiel 4k-demos unterzubringen und zeigte einige eigene Werke, die er mit Hilfe dieser Techniken schuf. Ich fand diesen Teil des Workshops eher langweilig (interessiert mich einfach nicht, was man wo im Editor klickt, und auf die Mathematik dahinter wurde natürlich nicht detailliert eingegangen) und hörte nicht allzu genau zu.

Zum Abschluß zeigten die beiden noch ein paar Demos, und das Publikum begann, sich allmählich zu leeren. Der Rest genoß noch etwas die Optik.

Ich muß sagen, ich fand den Vortrag recht gut. als Einführung in Demos war der Workshop vollkommen in Ordnung, dem Publikum wurden viele Klassiker auch von älteren Systemen gezeigt, die einen ziemlich guten Eindruck über Demos an sich vermitteln, und dem Publikum schien es zu gefallen. aber es gab auch andere meinungen (O-Ton erdgeist: "War's Scheiße oder war's Scheiße?"): zum Beispiel, daß zu wenig Oldskool-Demos gezeigt worden wären, man die präsentierten Demos eh alle kennen würde oder der Eindruck vermittelt worden wäre, Democoden bestünde nur aus Polygonreduktion mit Unterteilung zur Laufzeit. Zu letzterem muß ich sagen, daß ja nur ein Beispiel gegeben wurde, an dem das Democoden demonstriert wurde, das ja im Detail auch ein äußerst komplexes Feld ist. Vielleicht haben die beiden ja vergessen, das zu erwähnen, oder es ist (wohl auch wegen der eher mäßigen Vortragsfähigkeiten der beiden, zumindest in englisch) einfach untergegangen.

Nichtsdestotrotz war ich gut überrascht von einem Vortrag dieser Art auf einem Hackercamp, und das beste Resultat daraus ist einfach, daß die Leute begeistert und beeindruckt von Demos wieder herausgegangen sind. Und das kann ich den beiden nur zugute halten, Respekt.

Termine

März 2004:

Samstag+Sonntag 06. + 07. März 2004 Chemnitz
Linuxtag
http://www.tu-chemnitz.de/linux/tag/2004/allgemeines/

Sonntag, 07. März 2004 Bielefeld
Public Domain 129 - Claudia Rusch„Meine freie deutsche Jugend", Lesung
http://www.foebud.org/pd/

Montag, 08. März 2004 Ulm
Chaos Seminar CCC Ulm „Controler Area Network"
http://ulm.ccc.de/chaos-seminar/

April 2004:

Montag, 05. April 2004 Ulm
Chaos Seminar CCC Ulm - „Peer to Peer Netze"
http://ulm.ccc.de/chaos-seminar/

Freitag - Montag, 09. - 12. April 2004 München
Easterhegg IV
http://eh.muc.ccc.de/

Freitag - Sonntag 16. - 18. April 2004 Atlanta
interz0ne II
http://www.interz0ne.com/

Mai 2004:

Noch kein Termin Ende Mai 2004 Karlsruhe
Gullaschprogrammiernacht
http://www.entropia.de/

Montag, 10. Mai 2004 Ulm
Chaos Seminar CCC Ulm - „XML"
http://ulm.ccc.de/chaos-seminar/

Mittwoch - Samstag, 26. - 29. Mai 2004 Wien
Linuxwochen
http://www.linuxwochen.at/

Sonntag, 02. Mai 2004 Bielefeld
Public Domain 130 - Lisa Thalheim und Jan Krissler „Über Sinn und Unsinn biometrischer Systeme"
http://www.foebud.org/pd/

Juni 2004:

Freitag, 04. Juni 2004
Erscheinungsdatum Datenschleuder 83
https://ds.ccc.de/

Sonntag, 06. Juni 2004 Bielefeld
Public Domain 131 - Prof. Dr. Kunze „über Familiennamen, ihre Entstehung, Bedeutung und Verbreitung"
http://www.foebud.org/pd/

Mittwoch - Samstag, 23. - 26. Juni 2004 Karlsruhe
Linuxtag
http://www.linuxtag.org/

Bestellungen, Mitlgliedsanträge und Adressänderungen bitte senden an:

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

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

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

Die Kohle

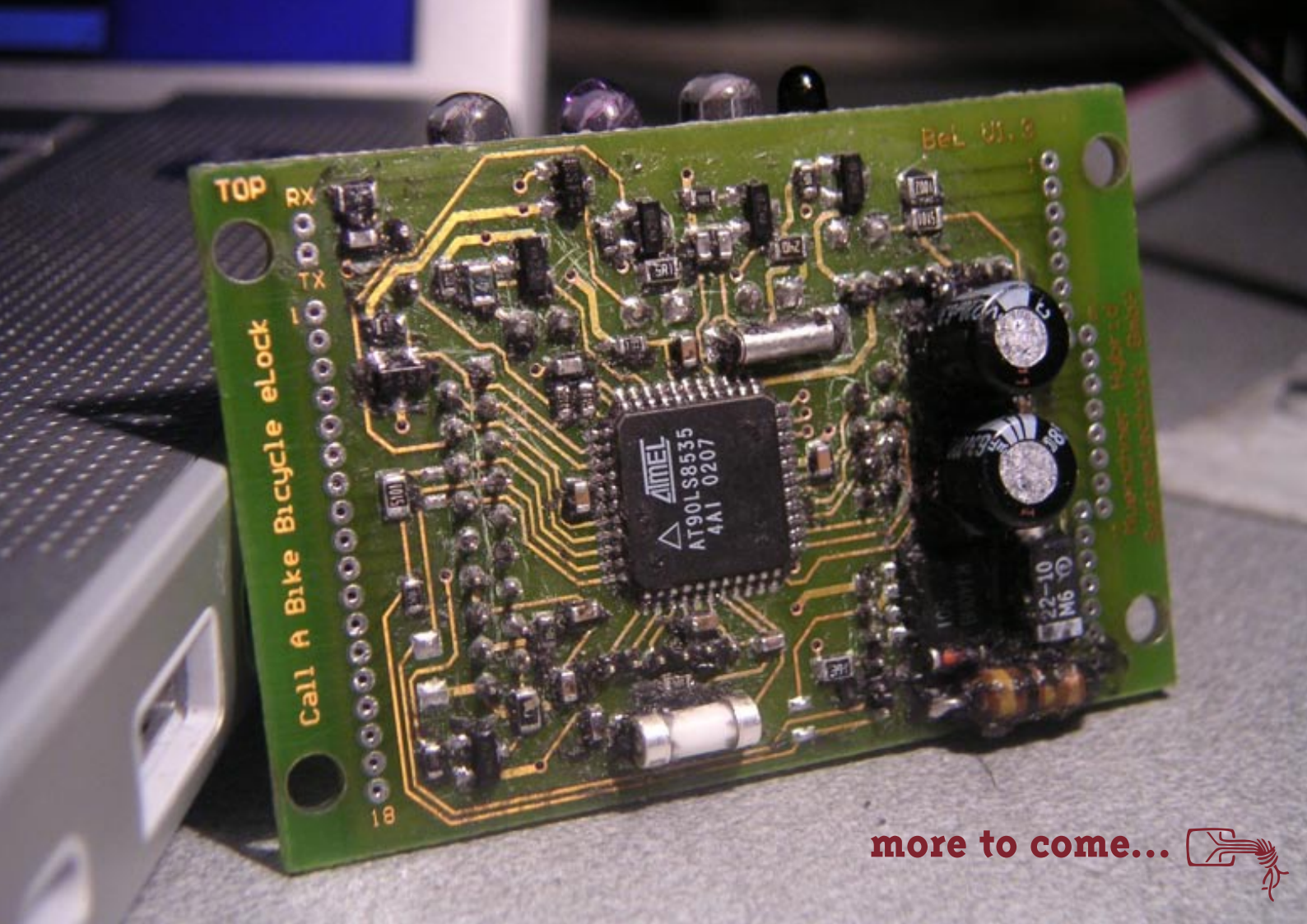
- liegt als Verrechnungsscheck bei
- wurde überwiesen am _____._____._____ an
  Chaos Computer Club e.V., Konto 59 90 90-201 Postbank Hamburg, BLZ 200 100 20

Name:	Email:
Straße / Postfach:	PLZ, Ort:
Ort, Datum:	
Unterschrift	

Boys need Toys

Bilder von einer polnischen MediaMarkt-Filiale, aufgenommen während einer "Verkaufsaktion" die mit "Preissenkungen bis zu 90%" oder "Walkman abe 0.25 EUR" beworben wurde.

http://arbiter.pl/galeria/65


TOP
RX
TX
Call A Bike Bicycle eLock
ATMEL
AT90LS8535
4AI 0207
18
more to come...