die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

Polizeihubschrauber mit Gebrauchsanweisung

Überwachung: Der Grosse Bruder fährt U-Bahn
Crypto: 1024 bit RSA Keys reichen nicht mehr
Hacking Biometric Systems Pt. II: Gesichtererkennung
Security: Insertion Attacks
Propaganda: Schreibkurs für Hacker

ISSN 0930-1054 • Zweites Quartal 2003
EUR 2,50 | IQD 0,77 | IRR 4.353 | KPW 5,40 | LYD 7,75
Postvertriebsstück C11301F

#81

Erfa-Kreise

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>*
Berlin, CCCB e.V.	Marienstr. 11, Berlin-Mitte, *Briefpost: CCC Berlin, Postfach 640236, D-10048 Berlin* >> Club Discordia Donnerstags zwischen 17 und 23 Uhr	*http://berlin.ccc.de/* *<mail@berlin.ccc.de>*
Düsseldorf, CCCD/ Chaosdorf e.V.	"zakk", Fichtenstr. 40 >> jeden 2. Dienstag im Monat ab 19.00 Uhr	*http://duesseldorf.ccc.de/*
Frankfurt am Main, cccffm	Club Voltaire, Kleine Hochstraße 5, >> donnerstags ab 19 Uhr	*http://www.ffm.ccc.de/* *<mail@duesseldorf.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 im Stadtteilzentrum Nordstadt (Bürgerschule), 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>*

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, Basel, Darmstadt, Dresden, Emden, Frankfurt am Main, Freiburg im Breisgau, Gießen/Marburg, Hanau, Kiel, Münster/Osnabrück, Offenbach am Main, Regensburg, Ruhrpott (Bochum), Saarbrücken, Stuttgart, Trier, Weimar, Wien.

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/*) und die C-Base Berlin (*http://www.c-base.org/*).

Die Datenschleuder Nr. 81

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

Andy Müller-Maguhn, Ernst-Albert, Ruediger Weis, Stefan Lucks, Andreas Bogk, Anne Forker, Su-Shee, starbug, Nitram, Sascha Roth, Sebastian und Fabian Bieker.

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.

New World Chaos

von Tom Lazar <tom@tomster.org>

Datenschleuder machen kann manchmal ganz schön frustrierend sein. Nein, ich rede nicht davon, drinnen am Computer zu sitzen während "der Rest der Welt" draussen in der Sonne abhängt...

Ich meine die Nachrichten, die sich in der Redaktions-Inbox stapeln über diese ganzen Controlfreaks "da draussen" in Wirtschaft und Politik, die offensichtlich darauf aus sind, die ganze Welt in einen Hochsicherheitstrakt mit Einkaufsmöglichkeit zu verwandeln. Frustrierend ist zum Beispiel, dass das Recht auf Privatkopie in diesem Land nur noch auf dem Papier besteht. Die Gesetzgebung hat es nicht für notwendig befunden, dafür zu sorgen, dass Du neben dem *Recht* auch die *Möglichkeit* hast, eine Kopie eines geschützten Werkes für eigene oder didaktische Zwecke anzufertigen. Nicht nur das: falls Du trotzdem von Deinem *Recht* Gebrauch machen willst und Dir trotzdem eine Kopie anfertigtst, machst Du Dich *strafbar*.

Aber das ist ja noch relativ harmlos. Weiter geht es mit der sich ausbreitenden Plage "geistige Leistungen" zunehmend trivialerer Natur unter besonderen Schutz stellen zu lassen (der bereitwillig - gegen Geld - gewährt wird). Und dann wird lustig rundum verklagt. Ob das nun eine Person fragwürdiger Intelligenz ist, die sich (ihren) Markennamen "Naddel" gesichert hat und die Verwendung des Begriffes "Anstecknaddel" in einem Werbespot gerichtlich unter Androhung von EUR 250.000,- Strafe verbieten liess oder ob das die dubiosen "Intellectual Property" Ansprüche einer Firma namens SCO an ungenannten(!!) Codefragmenten von Linux ist: Dummheit, Egoismus und Machtbestreben überall.

Aber das ist ja schlimmstenfalls nur frustrierend. Fangen wir lieber garnicht mit solchen Leuten wie "uns Dubya" an. Das macht doch richtiggehend *wütend*, oder? Schlimm genung, dass der Irakkrieg unter Anführung falscher Gründe geführt wurde - Verzeihung, *wird* - aber dieses lässige "Hoppla, da haben wir uns wohl geirrt. Trotzdem, dufte Typen unsere Jungs! Freibier für alle!" das genau garkein Unrechtsbewusstsein erkennen lässt, das ist doch einfach nur zum Kotzen.

Und die Liste lässt sich beliebig erweitern: von Microsoft, RIAA und MPAA bis hin zu Computer-BILD und "Prolls und Trolls" in Supermarkt und Heise-Forum: alle scheinen eifrig an einer Welt zu zimmern in der alles schön unter (ihrer) Kontrolle ist.

Für Hacker sind solche Aussichten natürlich gleich doppelt unerfreulich, widerspricht eine solche Welt doch so ziemlich allem, was uns lieb und teuer ist: *Authoritäten zu misstrauen* (ob das Deine Regierung ist, oder das Handbuch zu Deinem neuen DVB-Tuner), *kreativ mit Technik umzugehen* (d.h. Nutzer sein und nicht Lizenznehmer), *Wissen frei zu teilen und zugänglich machen* oder *Dinge einfach nur aus "Spass an der Freude" tun* und nicht, weil es Dir jemand *aufgetragen* oder *befohlen* hat.

Der Krug geht solange zum Brunnen, bis er bricht

Die Strategie der Controlfreaks hat sich jedenfalls als äusserst erfolgreich erwiesen. So sehr, dass man manchmal am liebsten den Kopf in den sprichwörtlichen Sand stecken möchte. Aber was mich immer wieder motiviert ist einfach folgender Gedanke: so sehr die Kontroll- und Machtstrategie auch erfolgreich sein mag, sie hat einen gravierenden Nachteil: sie skaliert nicht besonders gut. Dadurch, dass der Mensch *nie genug Macht haben kann*, sind die Mächtigen gezwungen, ihren Einfluss immer weiter auszudehnen. Und dadurch treten ihre Bestrebungen zwangsläufig zunehmend zutage. Ob das jetzt 30% der Deutschen Bevölkerung sind, die glauben, dass die Regierung der Vereinigten Staaten ihre Finger beim Anschlag vom elften September mit drin hatte oder ob das Microsoft ist, die das Ende ihrer Vormachtstellung durch die schwachsinnigen Registrierungsbedingungen (dreist) von Windows XP eingeläutet haben und durch ihre TCPA-Vorhaben (dreister) besiegeln werden: immer mehr Leute haben einfach die Schnauze voll - gestrichen voll. Und das schöne daran, dieser Trend wird allein durch den Status Quo aufrechterhalten! Aber deshalb kann man ja trotzdem nachhelfen ;-)

Inhalt

Latein in der Datenschleuder

Hallo, pflegt lieber unser Deutsch. Euer Latein ist lausig. Der Spruch lautet "panem et circenses". <xxx@t-online.de>

Yo. Man. Romanes eunt domus. <erdgeist>

Ich such ...

seit c.a. 2 Tagen eine Seite auf der man Kostenlose E-Mail Bomber PW Hackers und so weiter herunterladen kann . Bisher noch keinen erfolg . Vielleicht kann mit jemand von euch Helfen Das wäre shr net. - Florian <xxx@hotmail.com>

Nein bestimmt nicht, da sowas Kinderkacke ist. Solche Tools machen vielen unschuldigen Usern und eh schon genervten Sysadmins das Leben oftmals noch schwerer. <DocX>

Nachwuchsspammer?

Hi, es tut mir leid, dass ich euch störe, aber ich finde einfach keinen Server mehr, über den ich fakemail mailen kann. Vielleicht könnt ihr mir weiterhelfen. <xxx@yahoo.de>

Nein. Und das ist auch gut so. <erdgeist>

Ähem, ja, Hallo erstmal.

Also mein Anliegen ist folgendes, ich bin ein Mensch (glaube ich) dem viel zu viele Fragen in seinem dafür leider viel zu kleinen Gehirn rumspuken. Darunter z.b warum sind wir hier, warum ausgerechnet ich, was passiert wenn ich den Knopf da drücke, warum ist die Herdplatte immer heiß wenn ich sie anfasse, warum, warum, warum...

Ja, und da ich nebenbei auch noch ziemlich Technik interessiert bin, bin ich irgendwie auf eurer Seite gelandet. Nur das Problem ist, das ihr Hacken noch mit einer Vielzahl von anderen Problematiken unseres Systems, wie z.b der totalen Überwachung, das Recht von Menschen über Menschen u.sw, u.s.w zu verbinden scheint.

Das hat mir zwar sehr imponiert, mich aber auch ziemlich verwirrt, da ich immer eine andere Vorstellung davon hatte, was hacken bedeutet. Denn der CCC scheint hacken nicht nur auf der technischen Basis zu betreiben, sondern auch auf der Gesellschaftlichen Basis (ja schon fast philosophisch).

Kann ich den CCC als eine Art "Underground Network" verstehen, der mittels seines technischen Know-How auf soziale und gessellschaftliche Missstände

aufmerksam machen will, b.z.w diese zu bekämpfen versucht...?

Ich würde mich freuen wenn mir jemand von euch aus diesem verwirrenden Dschungel eurer Ziele und Ideale helfen könnte und diesen verflixten Knoten aus meinem Gehirn lösen würde...[FAQ = :-( ].

Vielen Dank im Voraus... <xxx@yahoo.de>

Du hast recht, der CCC ist nicht immer das was viele glauben. Es ist sogar noch vielschichtiger. Aber es ist fast immer ein Bezug zur "Hackerethik" vorhanden (http://www.ccc.de/hackerethics bzw. http://koeln.ccc.de/c4/hackerethics.xml):

Da gibt es zB die Künstlerfraktion, die sich an 3D-Plottern begeistert und Projekte wie Blinkenlights aus dem Boden stampfen. "Mit dem Computer kann man Kunst und Schoenheit schaffen".

Dann gibts die Security und Admin-Fraktion im Geiste eines BOFH.

Wie erwaehnt gibts noch die Politikfraktion mit den Datenschützern ("Öffentliche Daten nützen, private Daten schützen") und den Zensurgegnern ("Alle Informationen müssen frei sein. Mißtraue Autoritäten - fördere Dezentralisierung").

Und, auch wenn man das verurteilen mag, gibt es auch beim CCC eine Skriptkiddyfraktion die die Hackerethik, wenn überhaupt ganz anders interpretieren.

Den CCC auf das eine oder das andere zu reduzieren wird nicht gelingen.

Es gibt trotz gelegentlicher Reibereien durchaus gegenseitigeSynergieeffekte und jeder Teil gehört auf eine gewisse Weise dazu.

Lass mal das "Underground" weg (hey wir sind so ein richtig spiessiger deutscher Verein) dann hast du schon eine wesentliche Facette erfasst. <Jürgen>

Subject: BND

Ich hab keine Ahnung, wie oft euch schon diese Frage gestellt wurde (im FAQ war sie nicht), aber ich stell sie trotzedem mal.

Mich würde es interessieren, ob ihr in irgend einer Form Kontakt zum BND (Bundes Nachrichten Dienst) habt.

Solltet ihr darüber keine Auskunft geben wollen oder können hab ich halt Pech gehabt :-) .

Ich bin mir nicht ganz sicher, ob diese Vermutung nahe liegt, verückt oder unverschämt ist?

Was ich noch gerne mal hätte, wenn es nicht zu unverschämt ist, eine Definition bzw. Auflistung der Moralvorstellungen des CCC.

Mit freundlichen Grüßen <xxx@gmx.net>

Wir suchen einen solchen Kontakt ausdruecklich nicht. Geheimdienste sammeln Informationen um sie (wie

der Name schon sagt) geheim zu halten, wir dagegen treten fuer Informationsfreiheit ein.

Es gibt aber Leute die fest daran glauben dass der Kontakt von der anderen Seite durchaus besteht. Und da diese Mail unverschluesselt ist gruesse ich mal an dieser Stelle die Herren und Damen diverser 3-Buchstabenorganisationen ganz herzlich. ;-)

PS: https://ds.ccc.de/063/bnd-anwerbeversuche

Amtshilfeersuchen :)

im Rahmen eines hier beim Zollfahndungsamt $Großstadt - Dienstsitz $Kleinstadt- anhängigen Ermittlungsverfahrens wurde eine pgp-verschlüsselte CDR sichergestellt, deren Entschlüsselung bisher nicht gelang.

Diese CDR würde die ermittelnde Staatsanwaltschaft ggf. Ihnen zum Entschlüsseln übersenden.

Da die Einzelheiten bei einem Telefonat besser zu klären sind, bitte ich, mich unter der Nummer $Vorwahl/ $Rufnummer - 1742 zurückzurufen, da ich sie unter Ihrer Telefonnummer nicht erreichen kann.

mfg Im Auftrag

($Beamter) *<xxx@zfam.bfinv.de>*

Hallo, Herr $Beamter

wenn da jemand gut nachgedacht und PGP sinnvoll gehandhabt hat, wird das schwierig bis unmöglich, das zu knacken.

Knackbar ist das nur, wenn Fehler in der Anwendung gemacht, z.B. dumme Passphrases oder Kennwörter gewählt wurden, und der geheime Schlüssel auf einer Festplatte gefunden wird.

PGP ist eben ein sinnvolles kryptographisches Verfahren.

In jedem Fall aber beschäftigt der CCC sich nicht mit dem Knacken von solchen Dingen, schon gar nicht als Dienstleistung. <Volker>

Probleme mit E-mail Passwort

ich habe ein kleines Problem mit meinem Passwort auf meinem E-Mail Programm. Habe mir aus versehen ein Passwort (habe mit der Faust in die Tastatur gehauen) vergeben, und kann das Ding jetzt nicht mehr öffnen. Habe die T-online Software 5.0. Vieleicht könnt Ihr mir helfen. Ich sollte wenigstens an meine E-Mail Adressen wieder rankommen. Bitte um Rückantwort. *Marcus <xxx@t-online.de>*

Also ich kenne es an und für sich so, dass man ein Passwort beim Setzen immer 2x eingeben muss, damit eben sowas nicht passiert.

Wieso wendest du dich nicht einfach an die T-Online Hotline? Die sind doch für genau sowas da. <enno>

... diese Anfrage muß man sich wirklich mal auf der Zunge zergehn lassen, für wie blöd halten uns denn die Leser? <erdgeist>

Konsumhaltung

Ich wollte mal vorschlagen etwas zum Thema "neues Urheberrecht und 'Kopierabgaben' auf CDs etc." auf der Website zu bringen. Ich denke, dass passt doch ganz gut in eueren Bereich. Zudem habe ich dazu nur sehr alte Infos gefunden. Ich denke, da wäre ein aktueller Artikel ganz interessant und hilfreich.
M. & V. xxx <xxx@Students.Uni-Marburg.DE>

OK. Schreibst Du einen? <Volker>

Recht hat der Mann. Wie der gesamte CCC lebt auch die Datenschleuder vom Mitmachen, will sagen: freiwilligem Engagement. Wir freuen uns auf eure Artikel unter ds@ccc.de <erdgeist>

Mindcontrol

...ist es eigendlich möglich mit einem funkgerät mindcontrol zu machen ? oder bedarf es der nutzung einer tesla spule ? Lasse C. <xxx@xxxstrasse.de>

Nun, da bei Dir offenbar bereits eine Schädigung vorliegt, solltest Du Dich dringend mal von einem Neurologen Deiner Wahl untersuchen lassen. <kju>

```
... jedoch wenig später ...
```

Wenn sie der meinung sind es wäre schlau zum Neurologen zu gehen welcher eventuell weiß wie Mindcontrol per funk funktioniert ist das ja ganz ok, aber wenn nun ein Neurologe selber unter mindcontrol steht wäre es meiner meinung nach nicht sehr schlau weil dann seine Antwort eh absehbar wäre, was eventuell bedeuten würde das eine Person die eventuell mindcontrol macht so im handumdrehen sein 'Opfer' in eine Nervenklinik seiner wahl (also desjenigen der eben mindcontrol macht) einweisen lassen könnte. Und das ist mir echt ne nummer zu unsicher. Aber die Meinungen gehen da bestimmt auseinander weil ich mir nicht mal sicher bin ob ein Neurologe das überhaupt kann oder darf. Trozdem danke für den Hinweis

MFG Lasse C.

Da redet man sich jahrelang ein, daß WIR so richtig richtig paranoid seien und dann das. <erdgeist>

Weil immer wieder gern gefragt

kurze Frage: Ich rechachiere und mich interessiert: Wie wird man Hacker und kennt ihr Hacker. Würde mich sehr über eine Antwort freuen. Bis später

Ciao CyberJunior

http://koeln.ccc.de/prozesse/writing/artikel/hacker-werden.html <docx>

Klischeepflege

Kannst du oder freunde von euch punkte in flensburg löschen? GELD fast egal bitte schnell um Antwort OK

<<<<<<<<<<<<<<<<DRINGEND>>>>>>>>>>>>>>>>

<xxx@web.de>

Nö, aber wir können dir gern welche machen.
<erdgeist>

Hilf mir glauben, nibbler !

in der Datenschleuder#80 las ich mit Begeisterung die Lesermail von nibbler. Im ersten Moment überzeugt, drängte sich im 2. die normale 23paranoia auf. (könnte n. nicht ein Agent der o² mafia sein, der mich mit lancierten Berichten [enten] dazu bewegen möchte 2 weitere Verträge bei Netzbetreibern abzuschliessen?)

Nach Nachvollzug der Angaben stiess ich auf das Problem: Laut o2 sind weiterleitungen aus der Homezone (anrufe auf Festnetzvorwahl) kostenpflichtig mit 15 cent/min. !

Nur von o2 Netzvorwahl zu einem anderen o2 Handy wäre eine Weiterleitung kostenlos.

So könnte es also sein, daß ein Monat mit 4 durchtelefonierten Sonntagen durchaus ein kleines Loch in die Portokasse reisst ...

Wo liegt der Fehler in meiner Argumentation?

Hilf mir glauben, nibbler !

best regards *<Claudio W.>*

Morgen,

*o2 verlangt die 15 cent wenn du den anrufmanager nutzt um die festnetznummer umzuleiten - du stellst aber im anrufmanager die option "anrufe in der homezone durchstellen - ausserhalb der homezone nicht" ein und laesst das telefon das die mobilnummer (entweder ueber ussd codes also **61*nummer# (oder so aehnlich) bzw. ueber das telefonmenue) umleitet in der homezone liegen.*

soll heissen: das netz schaut: ist das telefon in der homezone? jo! folge: kostenlos durchstellen. das netz bekommmt also den anruf - es ist aber eine netzinterne rufumleitung geschalten - folge: nicht durchstellen sondern weiterleiten.

wuerde die sache schon im anrufmanager (kurzwahl 1010 fuer setup) umgeleitet wuerde das netz 'wissen' dass die festnetznummer auf eine andere mobilnummer umgeleitet wird und eifrig dafuer billing-records erstellen. tut sie aber nicht weil ja sowohl durchstellung in der homezone und die anschliessende netzinterne weiterleitung kostenfrei sind. Shalom, <nibbler>

There is no such thing as good Spam!

Uns erreichte folgende Email der gemeinnützigen Ingeborg Gebert-Heiss Stiftung, die sich im Bereich der Krebsforschung betätigt. Aber das ist leider keine Lizenz zum dreisten Spammen:

Sehr geehrte Damen und Herren, wir möchten Sie auf eine besondere Veranstaltung aufmerksam machen.

Sehr geehrter Herr Heiss, ich muss zugeben, ich war im ersten Moment sprachlos. Es liegt mir fern, Ihnen auf den sprichwörtlichen Schlips zu treten, aber es ist mir ein Anliegen, Ihnen mitzuteilen, dass Sie mit Ihrer Einladung einen datenschutz- und informationstechnischen Fauxpas erster Güte hingelegt haben.

- *Zunächst wären da die 982 (!) Emailadressen, die Sie in der Empfängerzeile preisgeben. Wie würde es Ihnen gefallen, wenn ich Ihre Emailadresse 981 Ihnen gänzlich unbekannten Menschen zukommen liesse?*

Wir erlauben Ihnen (sic!) als Anlage das Programm dieser Veranstaltung beizulegen.

- *Sie verschicken unaufgefordert eine ca. 1 Mb grosse Email! Ob Sie damit Ihr Anliegen in einen positives Licht rücken? Höflicher und effektiver ist es, Anhänge nur auf Anfrage zu verschicken. Dann können Sie sich sicher sein, dass selbige auch erwünscht sind.*
- *Die beigefügten Dokumente sind allesamt im proprietären Wordformat und können nur von Programmen der Firma Microsoft (halbwegs) bildgetreu geöffnet werden.*
- *Der Text Ihrer Email ist ein in (pseudo-) HTML konvertiertes Worddokument! HTML-Emails und Worddokumente sind mit Abstand die häufigsten Träger von Viren und anderen Schadroutinen – Sie tun sich und Ihren Adressaten wirklich keinen Gefallen, indem Sie ausgerechnet eine Kombination dieser beiden Formate verwenden!*

Wir würden uns freuen, wenn Sie auf diese Veranstaltung hinweisen und wir möchten Sie recht herzlich einladen für diese Bemerkenswerte Veranstaltung.

Ich würde mich freuen, wenn Sie mein (zugegebenermassen) besserwisserisches Meckern nicht als Bevormundung auffassen, sondern vielmehr als Anstoss, in Zukunft bewusster und umsichtiger in Ihrer Anwendung moderner Kommunikationsmittel zu sein.

Weiterhin möchte ich Sie dazu einladen, den Einsatz proprietärer Dateiformate (allen voran das Microsoft Wordformat und die proprietär erweiterte HTML-Abart derselben Firma) zu überdenken und stattdessen auf offene, allgemein lesbare (und ungefährlichere!) Formate wie plaintext, RTF, HTML oder PDF umzusatteln. Auf jeden Fall aber können Sie sich versichert sein, dass Ihre Email in unserem Magazin gebührende Beachtung finden wird.

Mit freundlichen Grüssen, fassunglos, <tomster>

Apple Browser Safari 1.0

Hallo, beim surfen über den Anonymisierungsdienst JAP der TU Dresden mit SAFARI 1.0 wird auf der Testseite von Gibson-Research https://grc.com/x/ne.dll?bh0bkyd2 ("Test my shields"klicken) trotz Anonymisierung die ursprüngliche IP ermittelt! Bei anderen Testseiten z.B. symantec oder JAP selbst wird die IP des JAP Dienstes angezeigt.

Bei der Verwendung des internet explorers hingegen wird auch auf der Gibson-Research Testseite die IP des JAP Dienstes ermittelt.

Es scheint so als ob Safari (manchmal) die Proxyeinstellungen ignoriert.

Ich habe in mehreren Mac Foren versucht eine Erklärung zu finden, leider ohne Erfolg. Vieleicht habt ihr eine Erklärung / Lösung bzw könnt ihr den bug bestätigen?

Grüsse, ray

Hallo Ray, nein hier sind weder Problem noch Lösung bekannt. Aber vielleicht einem unserer Leser?

Subject: Was ist Chaos?

Gute Frage, fragen wir jemanden, der sich damit auskennt, den Chaos Computer Club e.V. zum Beispiel. Die haben das Chaos ja im Namen und eine ganz besondere Antwort: am 17.3.03 ein Schreiben auf den Weg zu schicken, welches den Empfänger dazu auffordert, den nächsten Jahresbeitrag bis zum 4.2.03 zu überweisen...

http://www.dobschat.de/sunlog/entry.php?id=00188

Guten Tag!!! Ich bin Hackeri

Ich wollte Ihnen fragen wie kann ich diese daten endreen di e ausfürungsdateien (bsp: .exe und .dll) können sie mir helfen bitte ich habe müssam mit die daten ich suche seite 2 monat solsche programme aber ich habe noch nicht gefunden. könnten sie mir helfen bitte. Liebe Grüsse *<Hackeri>*

Zensur in Internetcafés ...

Uns wurde folgende Nachricht übermittelt:

surfe gerade im "Surf-Inn" im Kaufhof von Köln und stelle fest, daß hier ein Programm läuft, daß Internetseiten blockiert. Laut Auskunft muß das ab dem 1.April 2003 so sein. Eve and Rave, Orbital Dolphins u.a. sind z.B. hiervon betroffen. Es erscheint die Meldung: Webseite geblockt, fällt unter die Kategorie "illegale Drogen". Scheiß Zensur, angeblich zum Schutz der Jugend. Also nie wieder "Surf-Inn"!!! Das scheint bundesweit für alle "Surf-Inn" Zweigstellen zu gelten. Zitat Website:

Wir sind mit aktuell 21 Standorten deutschlandweit die größte Internetcafekette.

Wer vor Ort Zeit und Lust hat, das lokale "Surf-Inn" auf diverse Seiten zu testen, der möge doch die festgestellten Zensurergebnisse an mich (via Datenschleuder-Redaktion, Anm. d. Red.) übermitteln, dann könnte ich eine nette PM gestalten.

Gruss, Hans Cousto

Homepage: http://www.surfinn.com/
Standorte: http://www.surfinn.com/html/standorte/index.htm

07/01/2003 21:28 +494040180142 CCC EV S. 01/01

H. M. Büttnerr

[redacted]
23758 Oldenburg
den 26.12.02
Tel. [redacted]
erbitte Rückruf.

Liebes Chaos,

da ich wenig Geld habe und gern einen Computer hätte wenn de sich mich an Euch ich kann 150 Euro aufbringen und sche ein Top Laptop, weiterhin bittte ich um Bücher über Hacking und die Datenschleuder

MFG

MM. Büttner

In Sachen TCPA/TCG/Palladium/NGSCB

Einen halbwegs aktuellen Stand davon, was ur-sprünglich auf der Ebene eines Industriekonsortiums TCPA und bei Microsoft Palladium hieß, vermitteln die Materialien der Tagung des Bundesministeriums für Wirtschaft und Arbeit, die Anfang Juli 2003 in Berlin stattfand. Auch wenn das Industriekonsortium nicht mehr unter "Trusted Computing Plattform Alliance" sondern unter "Trusted Computing Group" firmiert und Microsoft den vergleichsweise aussprechbaren Namen Palladium für die Softwaretechnische Implementierung des sog. Secure Computing in die "Next Generation Secure Computing Base" umbenannt hat, so ändert sich nichts an der Kernfrage: für wen wird hier eigentlich was sicherer? In wessen Interesse ist es eigentlich, in Zukunft ein Teil des PCs in eine vorwiegend wohl Microsoftgesteuerte Set-Top Box zu verwandeln?

Hierzu und zu vielem mehr die Materialien unter

ftp://ftp.ccc.de/konferenz/200307_TCG_BMWA

Eine allgemeine Materialsammlung, wo auch die Forderungen des CCC an die TCG und der Stand der bisherigen Kommunikation verlinkt sind, liegt unter

http://www.ccc.de/digital-rights/

Zu dem, was am 11.09. geschah

Gab es in Berlin am 30.06. eine eigentlich hochinteressante Veranstaltung [*], die nicht nur die bekannten offenen Fragen zum Ablauf ins Gedächtnis rief, sondern auch hochkarätige Referenten eingeladen hatte, um daraus endlich einmal eine plausible Sachzusammenhangstheorie zu machen. Aufgrund katastrophal schlechter Planung der Veranstaltung in Tateinheit mit dessen Abbruch aus "Sicherheitsgründen" - weil sich ein gewisser Herr Mahler meinte im Publikum befinden zu müssen und damit nur eingeschränkt mit einem Teil des Publikums harmonierte - entfällt der Bericht über die Vorträge u.a. von Matthias Bröckers, Gerhard Wisnewski und Andreas von Bülow. Angesichts der Tatsache, das Wisnewski auch in anderen Zusammenhängen bisher solide Recherchen in lesbarer Form zu Papier brachte, sei auf sein von der Redaktion noch ungelesenes Buch hingewiesen und um dezentrale Sichtung gebeten: "Operation 9/11. Angriff auf den Globus" von Gerhard Wisnewski (Knaur Taschenbuchverlag, ISBN: 3-426-77671-5)

[*] http://www.hintergrund.de/

Biometrie: Identifizierung anhand vom Gang

An zwei Universitäten (Georgia Tech Atlanta, USA und Southampton, UK) wird derzeit experimentell die Identifizierung von Personen anhand der Charastika ihres Ganges erprobt: http://futurezone.orf.at/futurezone.orf?read=detail&id=142783&tmp=74545 Zu Ergänzen dazu bleibt, daß die automatisierte Echtzeit (!) Auswertung von Videoaufnahmen, die Personen im Gang zeigen bereits im teilweise im Einsatz ist - allerdings nicht zur Identifizierung, sondern zur Auswertung im Bezug auf bestimmte Charakteristika (schwankender Gang als unterstellter Hinweis auf Narkotikagenuss als Anlass für entsprechende Überprüfung). Falls jemand eine zitierbare Quelle zu dem im Einsatz befindlichen System am Züricher Flughafen und technische Details besorgen kann, möge er sie dochmal umgehendst an ds@ccc.de senden.

Mord, Menschenhandel, abgehörte Telefonate und der deutsche Bundestag

Die "Affäre Friedmann" hat zumindest für einige Tage die Mitglieder des Deutschen Bundestages offenbar sehr deutlich noch einmal über die geschaffenen gesetzlichen Grundlagen zum Überwachen von Telefonanschlüssen und ähnlichen Nachdenken lassen. Allerdings war der politische Druck auf Journalisten und Redaktionen offenbar groß genug, um die wesentlichen Details des Falles zu unterschlagen; Andeutungen über weitere Akteure und Handlungen, wie sie etwa die Berliner Zeitung am 23.06. machte [1] wurden nicht wieder aufgegriffen.

Auch der Umstand, dass das beim Berliner Generalstaatsanwalt Karge geführte Ermittlungsverfahren nicht nur Menschenhandel, sondern auch Mord erfasste [2] gelangte nicht in die bürgerliche Presse; das wollte man Friedmann dann wohl doch nicht antun.

Um etwaigen Missverständnissen vorzubeugen, scheint es angeraten auch noch einmal deutlich darauf hinzuweisen, daß es keinen Zusamenhang zwischen der Tätigkeit von Friedmanns Anwalt Eckart C. Hild im Kuratorium der Kinderhilfestiftung e.V. und der ansatzweise veröffentlichten der Erpressungen von Westpolitikern durch das Ministerium für Staatssicherheit aufgrund des Missbrauchs von Kindern gibt [3]. Und es gibt auch keinen B3 Bomber.

[1] http://www.berlinonline.de/berliner-zeitung/politik/254275.html

[2] http://www.jurtext.de/article.php?sid=858

[3] http://morgenpost.berlin1.de/inhalt/titel/story583001.html

Der Berliner Grunewald in Londoner Vorort

Wer bislang glaubte, die faktenunabhängige Deklarierung der Todesursache von tot aufgefundenen Männern in Großstadtwäldern als Selbstmord sei eine Spezialität von Berliner [1] muß derzeit anerkennen, dass auch in Großbrittanien derartiges möglich ist. Des einzig Unverständlich am Tod des ehemaligen UN-Waffenkontrolleur David Kelly ist wohl die Überschrift von Spiegel-Online [2]: "Kriegsgrund-Affäre: Kellys Tod schockiert Blair". Wieso sollte Blair geschockt sein?

[1] http://www.contramotion.com/updates/persons/larsoliverp

[2] http://www.spiegel.de/politik/ausland/0,1518,257865,00.html

Israel erlaubt sich, jetzt auch im Ausland zu morden

Der israelische Prime Minister Ariel Sharon hat nunmehr das Verbot für den im Ausland tätigen Geheimdienst Mossad und andere Stellen aufgehoben, im Ausland zu ermorden. Im Rahmen des "war on terror" müsse das doch wohl jetzt erlaubt sein.

Neu daran ist im Grunde genommen nur, daß es sich um eine öffentliche Mitteilung handelt, die explizit auch das Gebiet der USA betrifft. Mehr:

[1] http://www.upi.com/view.cfm?StoryID=20030115-035849-6156r

Was übrigens mit der Irakischen ccTLD passierte

Die dem Staat Iraq nach ISO 3166-2 zugewiesene Country Code Top Level Domain (ccTLD) .IQ wurde übrigens im Rahmen des diesjährigen Angriffs der USA auf den Irak nicht in der IANA-Rootzone-File ausgetragen. Das wäre zwar eine für alle Länder gleichermaßen vorhandene Möglichkeit gewesen, die Nutzung von DNS-basierten Kommunikationsparametern zu torpedieren, allerdings war dies in diesem Falle nicht notwendig.

Die .IQ Domain wurde bis dato von einer ausgerechnet im US-Bundesstaat Texas betriebenen Firma namens InfoCom von einem Herrn Saud Alani betrieben - der mit offenbar allen Mitarbeitern bereits fünf Tage vor dem 11.09.2001 vom FBI verhaftet wurde und die Firma de fakto stillgelegt wurde.

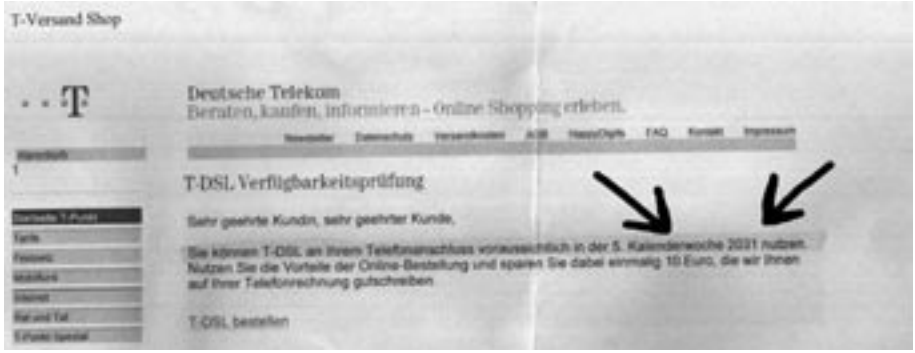
Die Liste der offiziellen Anklagepunkte umfasste 33 Punkte: unter anderem Geldwäsche, die illegale Ausfuhr von Computern an Libyen und Syrien und schließlich die Finanzierung von Terrorgruppen.

Mehr dazu:

[1] http://futurezone.orf.at/futurezone.orf?read=detail&id=142899

Urheberrechtsnovelle und kein Ende

Auch wenn die letzte DS nun schon einige Monate zurückliegt, kann ein längerfristig gültiges Ergebniss der Implementierung der EU-Urheberrechts- richtlinie in Deutschland noch nicht verkündet werden. Die Auseinandersetzung ist u.a. in der Materialsammlung von http://privatkopie.net/ zu verfolgen



Polizisten fordern Ende der Videoüberwachung

Zumindest in Brandenburg fordert die Gewerkschaft der Polizei (GdP) ein Ende der Videoüberwachung. Anstelle Straftaten zu verhindern, wären die kriminelle schlicht auf nicht-überwachte Bereiche ausgewichen. Von einem Rückgang der Krminialität könne keine Rede sein, lediglich ein Verdrängungseffekt sei zu attestieren.

Mehr:

[1] http://www.moz.de/showDDP.php?OPENNAV=ddp&SUBNAV=1&SUBID=xbg&ID=45318

Polizei gegen Sicherheit durch Sichtschutz bei Geldautomaten

Die in manchen Ländern gegen das illegale Ausspähen der Eingabe des PIN-Codes zu Bankkarten (EC-, Maestro-, Kunden-, Kredit) eingeführten räumlichen Sichtschutzvorbauten sind nicht gleichermaßen akzeptiert.

So berichtet die Bank eines annährend europäischen Landes jüngst, die Polizei habe sie aufgefordert, die Sichtschutzvorbauten zu entfernen, damit die Polizei problemlos im vorbeifahren erkennen könne, ob sich nicht etwa ein Mord im Sichtschutzbereich abspielt.

Angst macht beherrschbar

Und deswegen überlässt die derzeitige Regierung der USA die Versorgung mit Bedrohungen des Bio-Überlebens-Schaltkreis nicht nur diesem Dingsda, was vormals Wirtschaft genannt wurde. Siehe:

[1] http://www.fema.gov/areyouready/

Akronyme erklärt:

DRM -> Digital Restrictions Management, Vorläufer des PRM -> Political Restrictions Management

G.W. Bush institutionalisiert die Lüge

Aufgrund offensichtlichen Handlungsbedarfs hat der amerikanische President Bush bereits im Januar mit dem Office of Global Communications (OGC) eine Institution zur Erstellung virtueller Realitäten geschaffen.

Offenbar wurde das bisher in privaten Händen geführte Projekt aus Kosten- erwägungen zur Regierungsaufgabe erklärt. Wann die Umbenennung in den dafür vorreservierten Begriff "Ministerium für Wahrheit" geplant ist, wurde noch nicht bekanntgegeben.

Quelle:

[1] http://www.whitehouse.gov/news/releases/2003/01/20030121-3.html

Mehr:

[2] http://www.telepolis.de/deutsch/inhalt/co/14013/1.html

Medienberichterstattung

CNN erlaubte sich, nur die Teile des Blix-Berichts zum Waffenprogramm zum veröffentlichten, die opportun erschienen. Ein Vergleich gibt es unter

[1] http://www.takebackthemedia.com/news-cnnedit.html

Richterbund hält Polizeifolter für vorstellbar

Nachdem dem geständigen Mörder von Jakob von Metzler während des Verhörs Gewalt angedroht worden war, glauben einige Juristen, dass Folter unter Umständen legitim sein kann.

Nachzulesen unter:

[1] http://www.netzeitung.de/servlets/page?section=2&item=227577

Forderung nach Frieden in den USA bereits strafbar?

In New York wurde Anfang März ein Anwalt (!) verhaftet, weil er mit einem T-Shirt "Give peace a chance" in einer Mal rumlief und sich weigerte, dies auf Auffoderung auszuziehen.

Unfassbar:

[1] http://cnn.usnews.printthis.clickability.com/pt/cpt?action=cpt&expire=03%2F17%2F2003&urlID=5597275&fb=Y&partnerID=2004

Virtuelle Realität in Israel

Mit der offiziellen Begründung, man habe sich nicht über bestimmte Vertragsbedingungen einigen könne, ist BBC World nunmehr in Israel aus dem Kabelnetz geklemmt worden. Eingeborene sehen eher einen Zusammenhang mit der verhältnissmässig kritischen Kriegsberichterstattung.

[1] http://www.spiegel.de/panorama/0,1518,243071,00.html

Visa poolt mit Bertelsmann?

Etliche Kunden der citibank, die eine Visa-Kreditkarte der Bank benutzen, haben Ende Mai ein Brief mit neuen Allgemeinen Geschäftsbedingungen bekommen. Kundenfreundlicher und viel übersichtlicher seien die jetzt. Und weil die für die Abwicklung der Kartengeschäfte der Bank zuständige Abteilung 'citicorp' jetzt umgezogen sei, müsste der Kunde doch auch gleich noch der neuen Datenschutzklausel der AGBs zustimmen. Häh?

Und schnell ist auch klar, warum der Kunde den neuen Bedingungen zustimmen soll: Mit im Boot der Datenempfänger ist jetzt auch die arvato direct services GmbH in Gütersloh. Auf die Nachfrage, welchem Zweck dieser Datenaustausch dient, hat die citicorp bisher nicht geantwortet. arvato direct services ist nach eigenen Angaben "einer der größten Direkt-Marketing-Dienstleister weltweit. Zum Kerngeschäft gehört die gesamtheitliche Abbildung von individuellen Kundenbindungssystemen."

Die arvato-Gruppe ist eine Tochter der Bertelsmann. Auch die Deutsche Post Adress GmbH ist ein Joint Venture mit Bertelsmann/arvato. Die Deutsche Post Adress GmbH ist im Bereich der "Adresspflege" (Nachsendeanträge der Deutschen Post AG) tätig und verfügt dementsprechend über die aktuellste Anschriftendatenbank. Daneben bietet die Deutsche Post Adress GmbH einen sogenannten Risikoindex [3] an.

Die Deutsche Post und ihre DP Adress GmbH wurden bereits durch die Big BrotherAwards [2] gewürdigt und im 16. Tätigkeitsbericht des Bundesbeauftragen für Datenschutz [3] erwähnt. *<frankro>*

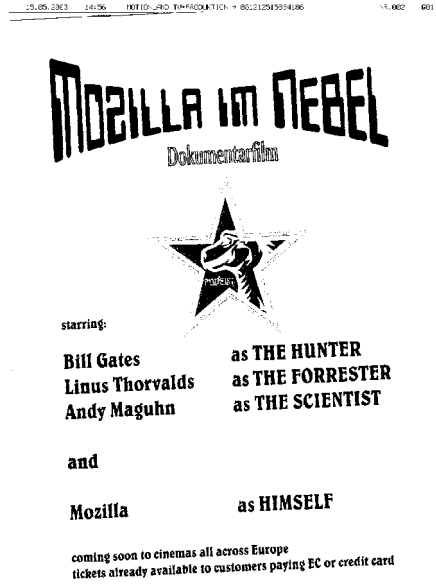
[1] http://www.deutschepost.de/dpag?lang=de_DE&xmlFile=1010

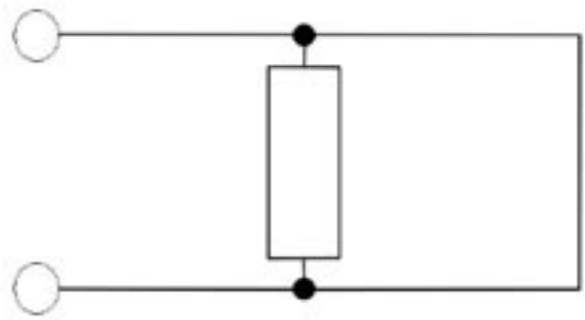
[2] http://www.bigbrotherawards.de/2002/.cop/

[3] http://www.bfd.bund.de/information/tb9596/kap29/29_04.html

Das Quartalsfax

Eigentlich haben wir uns in der Redaktion ja an skurrile Faxe gewöhnt. Scheint am Medium zu liegen... der Faxserver läuft faktisch nur noch zur Unterhaltung. Aber das folgende ist bisher ungeschlagener Spitzenreiter. *No (further) Comment!*





Widerstand ist zwecklos.

Berliner Verkehrsbetriebe - Entwicklung und Technik

von Ernst-Albert <ds@ccc.de>

Bis zum Jahr 2008 soll die BVG [1] das Ziel Wettbewerbsfähigkeit erreicht haben, so sieht es der mit dem Land Berlin eingegangene Unternehmensvertrag vor. Grundlage für diesen Effizienzsteigerungsprozeß ist ein Papier namens BSU 2000, das BVG Sanierungs- und Umsetzungskonzept. Die Kostenreduktion betrifft natürlich ganz klar auch den Personalbereich. Man setzt verstärkt auf Automatisierung und hat deshalb schon vor mehreren Jahren angefangen, neue Technologien zu verwenden.

Entwicklung

Ende 1928 wurde die Berliner Verkehrs-Aktiengesellschaft gegründet. Infolge der politischen Teilung wurde ab 1949 der BVG-Teil der SBZ separat verwaltet. Die Verflechtung der einzelnen Linien zwischen den Zonen wurde im Laufe der Zeit reduziert. Acht Jahre vor dem Bau der Mauer gab es schon keinen Grenzverkehr mehr.

Mit dem Fall der Mauer herrschte eine vollkommen neue Situation: Die Ostberliner BVB wurde 1992 in die BVG eingegliedert. Genau 24 Monate später wurde der landeseigene Betrieb in eine Anstalt des öffentlichen Rechts umgewandelt. Übernahmen bieten generell die Möglichkeit, unnötigen Strukturballast von Bord zu kippen: Kurz vor Ende 1991 waren insgesamt ca. 27000 Arbeitnehmer bei BVG und BVB beschäftigt, Ende 2001 durfte noch etwa die Hälfte zum Aktenkoffer greifen. Der ungefähre Trend bei den Mitarbeiterzahlen läßt sich aus dem Diagramm ableiten. [bvg_bilanz] [2] Die BVG hebt hervor, daß sie trotz der Personallücke die Fahrdienstleistungen z.B. in Fahrdienstkilometern gemessen, aufrechterhalten kann: rechnerisch fährt halt jeder mehr als doppel so viel.

Die BT Berlin Transportgesellschaft GmbH ist am 01.12.1999 zum Leben erwacht. Diese Gesellschaft hat "einen wesentlichen Beitrag auf dem Weg zum Sanierungsziel" [bvg_bilanz] [3] geleistet und gehört zu 100% der BVG AöR. Sie erbringt Fahrdienstleistungen für die Muttergesellschaft - Ende 2002 bereits mit einem Anteil von etwa 20% für Bus und U-Bahn. [bt_301102] [4] Mitarbeiter sollen in die Tochtergesellschaft migrieren. "Da die Abfindungsregelung für BVG-Mitarbeiterinnen und Mitarbeiter nicht das erwartete Interesse fand, musste die BT Ihr Personal auf dem Arbeitsmarkt gewinnen, um die geforderten Leistungen zu erbringen" [bt_011100] [5] . Das ist auch kein Wunder: "Zu wenig Mitarbeiter sind bereit, zur BVG-Tochtergesellschaft Berlin Transport GmbH zu wechseln, da diese bis zu 30 Prozent weniger Lohn zahlt." [bo] [6] . So verwunden auch nicht Pressemeldungen der Berlin Transport wie "Ex-Soldaten fahren BVG-Busse" [bt_111000] [7]

Ein naheliegende Methode zum Mehr-Geldeinnehmen ist die Preiserhöhung. Zwischen 1995 und 2000 lag die Preiserhöhung bei 30 % [igeb] [8] . BVG-Schlüpfer mit zweideutigem Aufdruck sind zwar billiger geworden, doch die Fahrpreise steigen unaufhaltsam. Die nächste Erhöhung zum 1.8.2003 steht bereits vor der Tür. Möglich, daß durch Druck auf die Verkehrsbetreiber, dafür auch mehr Leistung zu presentieren, zumindest das gleitende Monatsticket (seit August 2001, gleichfalls letzte Erhöhung, abgesehen von Euro-Rundungen) entstanden ist. Damit kann man stundenlang aus den zerkratzten Fensterscheiben kucken und dabei an den Fahrer denken, dessen Konzentration vielleicht n Euro weniger gut funktioniert.

Technik

Die Personalücken lassen sich in zumindest technisch fortschrittlichen Zeiten auch durch Elektronik und Software kompensieren. Bemerkenswert sind da die Errungenschaften im Bereich Zugabfertigung. Seit September 1999 führen Zugfahrer auf der Linie U7 ihre Zugabfertigung selbst durch. Mittlerweile benötigen zahlreiche Bahnhöfe kein stationäres Bahnhofspersonal

mehr. Stattdessen setzt die BVG verstärkt auf das Konzept Fahrgastbetreuer. Der "Gast" kann dann z.B. fragen, wo man ein Klo findet oder wie man sinnvoll vom Hackmarkt zum Alex fährt. Unnötig zu sagen, daß Fahrgastbetreuer und Zugbfertigung durch den Fahrer langfristig weniger kosten als Zugabfertigungspersonal auf einer Vielzahl von Bahnhöfen, denn Verantwortungsübernahme innerhalb eines Arbeitsverhältnisses spiegelt sich eben auch in der Lohntüte wider.

Ein weiteres Beispiel für Automatisierung: Am 5.11.1999 begann der Testbetrieb für selbstfahrenden Züge. Zwei Züge auf der Linie U5 hatten den Piloten nur noch als Aufpasser dabei. Der Testbetrieb für das Projekt "Systemtechnik für den automatischen Regelbetrieb" (Star) dauerte etwa bis April. Technik lieferten Adtranz und Siemens. Von April bis September 2002 gab es eine zweite Testphase. Man ist noch am Forschen. Insbesondere die Erkennung von Hindernissen auf dem Gleis wurde noch nicht zufriedenstellend gelößt. Derzeit ist eine Zwei-Minuten-Taktung möglich - zum Vergleich: die Moskauer Metro schafft 90 Sekunden (zu welchem Preis auch immer).

Die Modernisierung der Informationssysteme der BVG begann im Jahr 1996, als der erste SiS-Leitstand im U-Bahnhof Osloer Straße eröffnet wurde. Diese Sicherheits-, Informations- und Service-Leistelle soll alle auf einem Bahnhof anfallenden Signale wie Durchsagen, Info- und Notrufsäulen sowie Videodaten kontrollieren. Mittlerweile exisitieren für das gesamte Berliner U-Bahnnetz vier SiS-Leitstellen:

- Osloer Straße (seit 1. November 1996) für U6, U9

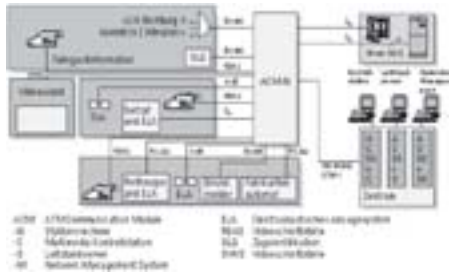
- Kleistpark (seit 31.01.2000) für die U7

- Nollendorfplatz (war geplant für 2001)

- Alexanderplatz (18.05.2001) für U5 und U8

Ferner gibt es seit Februar 2002 die Zentrale Leistelle der BVG am Tempelhofer Ufer, sowie seit April 2002 eine Leitstelle für "Service und Security" im gleichen Gebäude [bvg_sis] [9] . Die Betriebsleistelle Service und Security ist ein zentraler Leitstand, beim dem alle sicherheitsrelevanten Informationen zusammengeführt sind. Das Zentralsystem wurde 2001 bei der Münchner Firma Indanet GmbH in Auftrag gegeben [inda] [10] . Prinzipiell können die einzelnen SiS-Leitstände gegenseitig Aufgaben übernehmen.

Mit Eröffnung der ersten Leitstation startete der Ausbau des Kommunikationsnetzes der BVG. Siemens PSE DE (vorher bbcom) hat das technisch realisiert und zuerst auf der U6 umgesetzt. [sie] [11] Das Netz nennt sich Hicom Advanced Communication & Control System, kurz ACCS. Entlang einer U-Bahnlinie wer-



den zwei redundante Glasfaserringe gelegt, auf denen ATM über eine STM1 mit 155 Mbit gefahren wird. 46 weitere Fasern stehen für andere Anwendungen oder zur Vermarktung bereit. Seit 1999 sind alle U-Bahnhöfe mit insgesamt 580 Notruf- und Informationssäulen und über 650 Kameras in das Netz integriert. [sie2] [12]

Auf jedem Bahnhof befindet sich ein Netzknoten (ATM Communication Module Node, ACM-N), an den Anwendungen wie Fahrgastinformation (FGI), Elektroakustisches Ansagesystem (ELA), Videoleinwand, Brandmelder, Fahrkartenautomaten, Rolltreppen und Videokameras angeschlossen sind. Ein ACM-N besteht aus folgenden Komponenten:

- Remode Node (RENO), mit dem S0-Geräte wie Notruf-/Infosäulen und Stationstelefone verbunden sind,

- Distribution Node (DINO), das ATM-Interface zum Backbone

- Access Node (ACNO), an dem über serielle Schnittstellen Sensoren und Steuerungseinheiten hängen

SiS-Leitstände teilen sich in die Komponenten Leitstandserver (ACM-S), Multimedia Kontrollstation (ACM-C) und Network Management System (ACM-M) auf.

Rechnergestütztes Betriebsleitsystem (RBL)

Am 1. März 2002 wurde für Straßenbahn und Bus offiziell das RBL-System eingeführt. Für die Realisierung des Projektes hat die BVG 40 Millionen Euro Fördermittel auf Grundlage des Gemeindeverkehrsfinanzierungsgesetzes erhalten. [bvg_rbl] [13] Die Idee hinter einem RBL ist, daß man durch das Wissen um die aktuelle Position eines Fahrzeuges mittels Sollfahrplan-Vergleich Verspätungen erkennen kann. Diese Information stehen dem Fahrer sowie der Zentrale zur Verfügung. Dadurch lassen sich Anschlußfahrzeuge z.B. im Nachtverkehr besser koordinieren und Fahrgastinformationen anpassen. Möglich wird das durch GPS-Geräte in Bussen und Straßenbahnen, die mit dem IBIS-Board-

computer verbunden sind. Dieser Steuerrechner kennt den Streckenverlauf und kann mit der Peripherie im Fahrzeug mittels standardisierter Protokolle kommunizieren. Das RBL-System war die Basis für weitere Entwicklungsschritte:

- Ein IMU-System (Induktive Meldungsübertragung) zum automatischen Stellen von Straßenbahnweichen wurde von der BVG im Juli 1998 in Betrieb genommen.

- Die Straßenbahnlinie 6 wurde im September 1999 mit einem LSA-System ausgestattet, welches etwa 15-20% kürzere Fahrzeiten bringt. Ermöglicht wird das durch Vorzugsschaltungen an Ampeln, die aus dem Fahrzeug heraus über Funk angesprochen werden. [nvk] [14] Bis Ende 2001 sollten alle Tramlinien mit einem derartigen System ausgestattet worden sein.

- Daisy ist das Dynamische Auskunfts- und Informationssystem, welches seit Februar 2000 im U-Bahnbereich verwendet wird. Bis Juli 2001 waren die Linien U1, U15, U2, U4, U6, U7 und U9 integriert. Auf den installierten Anzeigetafeln werden Ankunftszeiten dargestellt. Ab 2003 soll das System auf Bus und Straßenbahn erweitert werden.

Funkanbindungen

Busse sind über Tetrapol am BVG-Netz angeschlossen. Dabei versorgen 6 Basisstationen ganz Berlin. In den sechs Funkzellen können jeweils sechs Kanäle benutzt werden. Vier Kanäle stehen dabei für Datenfunk und zwei für Sprechfunk bereit. Das Funksystem wurde von der EADS Telecom installiert und nennt sich M2600. [eads] [15] Es bietet Abhörschutz und arbeitet zwischen 440 und 450 MHz. Im Direct Mode könnten auch LSA-Vorrangschaltung angesprochen werden. In Berlin funktioniert das jedoch anders. Straßenbahnen sind seit ca. 10 Jahren mit analogem Betriebsfunk ausgerüstet und werden nach und nach auf Tetrapol umgestellt.

Die Funkanbindung von U-Bahnen sind über Tetra realisiert. Tetra unterscheidet sich von Tetrapol in einigen technischen Punkten (funktional sehr ähnlich, aber vollkommen inkompatibel), in den geringeren Installationskosten und daß es sich um einen ETSI-Standard handelt. Das mit der langwierigen Standardisierung hat wohl auch dazu geführt, daß in Bussen Tetrapol zum Einsatz kommt, da die BVG kurzfristig ein Bündelfunksystem brauchte und für Tetrapol bereits mehr Produkte existierten. [tt] [16]

Tetra bietet ferner eine Art Jamming-Detection. Wenn die Kommunikation gestört wird, können die Geräte auf weniger gestörte Kanäle ausweichen. Inwiefern selbstfahrende Züge auf Funkkommunikation angewiesen sind bzw.

wie sich Störung in einem breiten Spektrum auswirken würde, ist unklar. Weicheneinstellungen und Status von Signalgebern können auch via induktiver Meldungsübertragung zum Fahrzeug gelangen.

ÖPNV-Beschleunigung

Im Berliner Ampelwald findet man so einige interessante Konstruktionen. Da kann man Kameras (Traffic Eye), DCF77-Empfänger, Umweltmeßgeräte, natürlich zahlreiche Helligkeitssensoren für die Laternen und auf größeren Straßen Antennenkästen entdecken. Bei letzteren handelt es sich um Funkmodems, die mit dem Kreuzungssteuerungsrechner verbunden sind [piciorgros] [17] [fmncom] [18] . Überirdisch fahrende öffentliche Verkehrsmittel der BVG nutzen diese, um einen Schaltwunsch der Ampel kundzutun.

Wird ein Scanner auf 170.45 MHz /Schmalband-FM konfiguriert, und greift man dann das Signal an einem diskrimitatorfreien Ausgang ab, so ergibt sich z.B. folgende Wellenform:

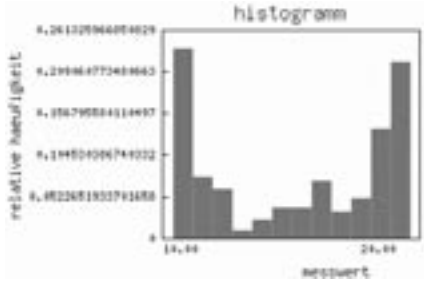
Ein naiver Dekodierungsansatz sieht etwa so aus: man ermittelt die Abstände zwischen den Nulldurchgängen. Einem breiten Peak setzt man das Bit 1 gleich, zwei schmale Peaks stellen ein 0-Bit dar. Mitunter ist es schwierig zu entscheiden, ob ein Peak null oder eins representiert. Ein Blick auf das Histogramm läßt erkennen, daß alle möglichen Zwischenbreiten auftreten.

Der Ansatz reicht dennoch aus, um sinnvolle Bitsequenzen zu erhalten. Vergleicht man mehrere Telegramme, ergibt sich ein Bild des Aufbaus.

Folgende Beobachtungen lassen sich anstellen:

- Telegramme werden mehrfach übermittelt (mindestens zweimal). Kann ein Telegramm korrekt dekodiert werden, so zeigt die Ampel dem Straßenbahnfahrer ein "A" an.

- Der Fahrer kann das Aussenden von Telegrammen manuell beinflussen.



- Es gibt eine Art Prioritätsmechanismus. Das Fahrzeug kann sich vorab anmelden. Wenn es dann in den Kreuzungsbereich einfährt, sendet es nochmals eine Anmeldung. Befindet sich das Fahrzeug mitten auf der Kreuzung, erfolgt das Abmelden. Ob dieses Abmelden vollautomatisch geregelt wird oder vom Fahrer abhängig von der Verkehrssituation bestimmt wird, ist unklar.

- Das Bit mit der höchsten Wertigkeit steht im Byte rechts.

- Unterscheiden sich zwei Telegramme in genau einem Bit, so bewirkt dieses eine größere Streuung im Prüfsummenblock. Eine Abbildung der Datenbytes auf CRC16 war bislang ohne Erfolg. Theoretisch könnte in diesen Hashwert auch ein unbekannter Schlüssel einfliessen. Das Gesamtsystem hinterläßt aber mehr den Eindruck, daß es einfach gestrikt ist und Schlüssel-Hürden nicht zu erwarten sind. Ferner stellen 16 Bit im Cryptobereich kein unüberwindbares Hindernis dar.

Vor Experimenten mit selbstgebauten Sendern [senderbau] [19] sei jedoch gewarnt: Es ist nicht abzusehen wie die Ampel reagiert, es stellt mindestens eine Straftat dar und größere Berliner Ampelanlagen sind mit hoher Wahrscheinlichkeit vernetzt, so daß Manipulation schnell erkannt werden könnte.

Berliner Fenster

Ab Sommer 2000 startete die BVG-Tochterfirma Plakat- und Außenwerbung GmbH Berlin [pab] [20] auf der U7 und U9 das Berliner Fenster. [bf] [21] Auf TFT-Monitorpaaren können bunte Bilder und softe Videoschnipsel angesehen werden. Inhalt steuert der Berliner Kurier bei. Technisch umgesetzt hat das Projekt die Inova Multimedia-Systeme GmbH & Co. KG aus Hildesheim (Boschtochter). [inova] [22] Die Technik nennt sich Digital Multimedia Broadcasting (DMB).

Fred Kuhaupt, Studioleiter des Berliner Fensters erklärt in einem Interview [ezetta] [23] : "Unsere MitarbeiterInnen erhalten die Vorlagen und bereiten sie auf. Texte und Bilder werden in so genannte Container abgelegt, zusammengestellt und bei Bedarf mit Effekten versehen. Auf unseren Monitoren kontrollieren wir, wie das Endergebnis in der U-Bahn aussähe. In einem letzten Schritt werden die Inhalte per Mausklick freigegeben und landen drei Minuten später in der U-Bahn. Die Übertragung erfolgt per Funk. Die Züge sind mit Servern ausgestattet, die ihre Daten permanent von den Empfangsstationen in den U-Bahnhöfen empfangen. Wir können 98 Prozent des Netzes nutzen, was im Vergleich zu anderen Städten sehr gut ist. "

Bis 2004 sollen alle ca. 1200 U-Bahnwagen mit dem System bestückt werden, um bis zu 1,6 Millionen Fahrgäste täglich visuell zu erreichen. 82% der U-Bahnbenutzer (BVG-Statistik) sollen das Berliner Fenster für eine gute Idee halten. Wenn irgenwann keine Fahrzeugführer mehr notwendig sind, vielleicht verdrängt es auch das Gefühl, daß das eigene Leben von einem Windows-PC abhängt. Bis es soweit ist, werden wohl noch mehrere Jahre verstreichen ...

Nun gut, viel wahrscheinlicher ist jedoch folgende Idee: Die Inova Multimedia-Systeme bietet offiziell drei Produktkategorieren, die sich in "passenger information", "passenger entertainment" und "video sourveillance" aufteilen. Die bei DMB maximal zur Verfügung stehenden 1.5 Mbit lassen sich eben auch zur Videoüberwachung in Fahrzeugen nutzen. Ist das so geplant? Handelt es sich um ein werbefinanziertes Überwachungssystem? Domekameras auf der Linie U5 wurden bereits bemerkt.

Noch was zu Video und Wavelan: November 1998 experimentierte die Firma Soreh Telecommunications GmbH aus Berlin auf der U4 mit Wavelan-Technik. Multimediadaten wurden zur U-Bahn transferiert und auf Monitoren dargestellt. Andersherum sollten Videodaten zu einer stationären Leitstelle gefunkt werden. Das Konzept nannten sie MovingTrain Sourveillance

System (MTSS). Übertragungstechnik ist das Sorelan, welches nicht konform zu IEEE 802.11 ist.

Videoüberwachung

Die BVG hat zahlreiche Videokameras auf allen Bahnhöfen installiert. Diese sind an den Stationsrechnern angeschlossen, wo die analogen Videodaten zu MPEG digitalisiert werden, so daß eine Leitstelle darauf zugreifen kann. Den Teil der IP-basierten Videoübertragung hat die Firma Accellence Technologies GmbH beigesteuert.

Videodaten werden wahrscheinlich erstmal dort gespeichert, wo sie anfallen - also auf Bahnhöfen oder in Fahrzeugen. Gerade Videoaufnahmen aus einem Fahrzeuginneren lassen sich schwierig von einer Zentrale überwachen, das Bündelfunksystem bietet schlicht nicht so viel Übertragungskapazität. Drückt der Fahrer auf den Knopf, wird alles im Zeitfenster von einer Stunde vor bis eine Stunde nach dem Kopfdruck (Mai 2002) auf Festplatte gesichert. Mindestens bei den Bussen stammt die Videotechnik von der Meister Electronic GmbH. [me] [24] Ob Bildmaterial dann auch in der Zentrale gesehen wird, ist nicht ganz klar. Das Produkt "Videosicherheitssystem VSS08" von Meister Electronic kann mit GSM ausgerüstet werden. Die Qualität der Daten wird der Bandbreite angepaßt. Ob dieses Remote-Monitoring verwendet wird, ist ungewiß.

Noch ein paar Bemerkungen zu den Kosten: Die BVG gibt an, 2001 durch Sachbeschädigung an Straßenbahnen 1,1 Millionen Euro Schaden erlitten zu haben. 586 Straßenbahnenwagen gibt es und die Installationskosten für eine Videoanlage liegt bei etwa 13.000 Euro pro Wagen. [welt] [25]

Ab einer gewissen Überwachungsdichte dürften in der Tat die Kosten durch Vandalismus zurückgedrängt werden, mindestens weil Kids dann selbst schrubben dürfen. Strittig bleibt der Punkt "persönliche Sicherheit". Falls ich in der Tram zusammengeschlagen werden sollte - bitte was bringt es mir dann, wenn es gefilmt wurde? Zwar besteht dann ein Grund weniger, ein Geständnis zu erpressen, der Täter wird vielleicht zur Rechenschaft gezogen - eine echte Hilfe, sehe ich da aber nicht. Und natürlich - die BVG möchte auch nicht, daß ich ermordet werde, denn als toter Kunde gebe ich nur noch Charon das Fahrgeld. Die Wahrscheinlichkeit in einem öffentlichen Verkehrsmittel statt im finsteren Park überfallen zu werden, ist dennoch gefühlsmäßig geringer. Ob die Filmerei objektiv die Sicherheit erhöht, ist mehr als fraglich. Kameras und Überwachungshinweise sind in den Verkehrsmitteln äußerst diskret installiert und werden von vielen Fahrgästen nicht wahrgenommen. Wie soll das dann Kriminalität vor der Tür lassen? Die BVG könnte besser Liveaufnahmen der Kameras im Berliner Fester präsentieren. Mit Bildunterschriften wie "Wir speichern alles ewig!" ließen sich die gruseligen Gangster abschrecken. Ja! So gewinnt man Akzeptanz!

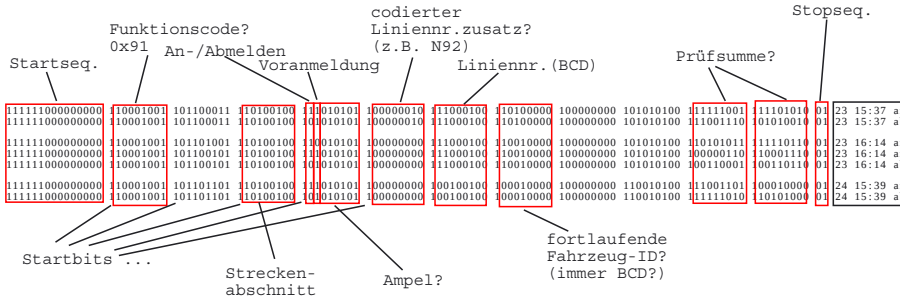
Datenschutz

In Berlin wird eine Vielzahl von Gebäuden, besonders Eingangsbereiche von solchen, videoüberwacht. Momentan scheint es noch so zu sein, daß mehr private Einrichtungen wie Bürohäuser und Konsumtempel kontrolliert werden. Bei der flächendeckenden Videoüberwachung sind die Verkehrsbetreiber Spitzenreiter. Herauszufinden, wie lange Bildmaterial tatsächlich gespeicht wird, ist nicht so einfach. Die Zahlenangaben schwanken je nach Quelle. Da ist von unrealistischen fünf Minuten die Rede, von einer Stunde bis zu einem Tag. Herr Budde von der BVG-eigenen Hotline (+493019449) meinte bei einem Anruf: "Warum wollen Sie das denn wissen? ... Sind Sie sich einer Schuld bewußt?" Zu meiner Frage hat er sich nicht geäußert, er wollte auch keinen weiteren Ansprechpartner nennen. Na herzlichen Dank auch. Mit einer derartig dummdreisten Antwort habe ich nicht gerechnet, war ich doch der gutgläubigen Meinung, wenn sie schon Daten speichern, müßten sie mir auch sagen können, wann die gelöscht werden. Interessant die Nichtaussage trotzdem, muß ich doch folgendes schließen. Ich mache mich verdächtig, wenn ich nach Kameras frage. Ich muß etwas zu verbergen haben. Weshalb sollte ich mich sonst dafür interessieren? Sind wir denn schon so weit? Hat sich die vielvertretene Einstellung, nichts verbergen zu müssen, so manifestiert, daß man gleich zu einer Schuldvermutung anstimmt? Ein Schuldtragender hat i.d.R. etwas zu verbergen - den den falschen Kehrschluß ziehen, darf man nicht.

Ok, nochmal bei der BVG-Hotline anrufen - neuer Mitarbeiter neues Glück - und die Antwort: fünf Wochen auf U-Bahnhöfen. Fünf Wochen sind 3.024.000 Sekunden. Bei einem Bild pro Sekunde von sagen wir 10 kB, würden knapp 29 GB Daten pro Kamera anfallen. Mal 650 Kameras wären das etwa 18 TB. Geteilt durch 170 Bahnhöfe, sind das 110 GB Bilder pro Station. Klingt zumindest nicht vollkommen unrealistisch.

In Zeiten größter Terrorbedrohung wäre es nur konsequent, würden ausgebildete staatliche Spezialobservierer zusätzlich mitkucken. Dann ließen sich Milzbrandzerstäuber und Sarinflaschenwerfer viel besser fassen. Doch malen wir den Teufel nicht an die Wand, vielleicht liegt das entsprechende Konzept zum Terroristenfangen bereits in einer Schublade und wird im geeigneten Moment durchgedrückt. Mißbrauchsmöglichkeiten wären wirklich optimal, man wüßte dann rechtzeitig, wer am 1.Mai nach Kreuzberg fährt.

Ab Ende 1999 hat die BVG sieben Monate lang die elektronische Fahrkarte tick.et mit 26894 Fahrgästen erprobt. Bleibt zu hoffen, daß sich bei offizieller Einführung des elektronischen Ticketsystems ein Bezug zwischen Fahrgästen und Fahrten etablieren wird. Abgesehen davon, daß bei der Testphase die Tester ihre Daten offenbahren mußten, war das System anonym. Die BVG denkt gerade laut darüber nach, in der zweiten Hälfte des Jahres 2004 mit dem Aufbau zu beginnen. Dem Teilnehmer sollen z.B. wie bei Fluggesellschaften



Bonusmeilen gutgeschrieben werden können. Momentan befindet sich das Projekt im Konzeptionsstadium. [bz] [26] Je nach Ausprägung kann das von einfachen Fahreinheitengutschriften bis zu Geldtransaktionen auf das ein Konto reichen. Inwiefern Datenerhebung notwendig ist, wird sich erst bei Konkretisierung der Voschläge erkennen lassen. Geldrückflüsse sind zumindest für Firmen interessant, während der normale Kunde mit billigen Kaffeemaschinen oder Werkzeugkoffern befriedigt werden kann. Vielleicht wird auch anonyme Bargeldauszahlung möglich sein. Zuviel Bonus wird wohl man angesichts der leeren Kassen nicht erwarten dürfen.

Während der Testphase existierten noch keine mobilen Geräte für Fahrkartenkontrollen. Da die jeweils letzten Fahrten auf der Karte gespeichert werden, kann die Auswertetechnik sehr einfach sein. Ein mobiles Terminal braucht nur zu überprüfen, ob die zuletzt aktivierte Fahrt noch nicht abgeschlossen ist. Dem Jahresbericht des Berliner Datenschutzbeauftragten aus dem Jahr 1999 zufolge, werden übrigens die Schwarzfahrervorfälle bei der BVG nach einem Jahr gelöscht.

Schluß

Der technischer Fortschritt, der im ÖPNV Einzug erhält, ist nur partiell zum Wohl des Kunden. Eigentliche Triebkraft scheinen die Einsparungsmöglichkeiten zu sein. In den nächsten Jahren werden die Systeme weiter ausgebaut. Man darf gespannt auf das Jahr 2008 warten. Solange hat die BVG weitgehenden Konkurrenzschutz. Dann will die BVG rentabel arbeiten und kann beginnen, den Schuldenberg in Höhe von 500 Millionen Euro abzuarbeiten. Die BVG-Kunden bleiben da nicht außen vor. Jeder muß seinen persönlichen Beitrag leisten. Damit sich dem niemand entzieht, sind täglich etwa 200 Fahrkartenkontrollatoren (Anfang 2003) unterwegs. Für die Kollegen von den Privatunternehmen gilt zumindest, daß sie aus psychologischen Gründe keine Erfolgsprämien erhalten, die BVG drückt jedoch für jeden erwischten Schwarzfahrer einen festen Betrag an das Unternehmen ab, zu dem der Kontrolletti gehört. Und das Unternehmen wird beim nächsten Personalabbau vermutlich nicht die Leute feuern, die die beste Quote bringen.

Wer noch interessante Informationen hat, möge sie bitte an die Redaktion schicken.

[1] *http://www.bvg.de/*

[2] *http://www.bvg.de/ueber/bilanz_2001.html*

[3] *http://www.bvg.de/ueber/bilanz_2001.html*

[4] *http://www.berlintransport.de/aktuell/2002-11-30.htm*

[5] *http://www.berlintransport.de/aktuell/2000-11-01.htm*

[6] *http://www.berlinonline.de/berliner-zeitung/archiv/.bin/dump.fcgi/2002/0625/lokales/0037/*

[7] *http://www.berlintransport.de/aktuell/2000-10-11.htm*

[8] *http://www.igeb.org/presse/20001228.php3*

[9] *http://www.bvg.de/news/newspage100402.html*

[10] *http://www.indanet.de/ref_bsus/page.htm*

[11] *http://www.siemens-consultsupport.com/de/archiv/ci/1997_01/atm.htm*

[12] *http://www.siemens-pse.de/de/s_nav32.html*

[13] *http://www.bvg.de/news/newspage020302.html*

[14] *http://www.nahverkehr.nrw.de/prokamp/projektdetail_regiofunk_druckversion.html*

[15] *http://www.eads-telecom.de/content.html?page=28&contentid=52&parents=,28,142,23,*

[16] *http://w3.siemens.ch/de/ics/kompetenzen/kommunikation/s-pro/technologie/systeme.html*

[17] *http://www.piciorgros.com*

[18] *http://www.fmncom.com/wzprod/frame_wzprod.html*

[19] *http://www.senderbau.de/*

[20] *http://www.pab-berlin.de/*

[21] *http://www.berliner-fenster.de*

[22] *http://www.inova-multimedia.com/*

[23] *http://www.ezetta.de/standards/archiv/0203_ezetta/rubriken/aktuelles/aktuelles_html/0203_aktuelles_berlinerfenster_gj.htm*

[24] *http://www.meister-electronic.de*

[25] *http://www.welt.de/daten/2002/05/10/0510b01331053.htx*

[26] *http://www.berlinonline.de/berliner-zeitung/berlin/244510.html*

1024 bit RSA Keys reichen nicht mehr

von Ruediger Weis, Stefan Lucks und Andreas Bogk

Am 23. Januar 2003 veröffentlichten Adi Shamir, einer der Entwickler des RSA Verfahrens zusammen mit Eran Tromer einen technischen Report über Spezialhardware zur Faktorisierung von grossen Zahlen. Aufhorchen liess insbesondere die Einschätzung, dass mit einem Einsatz von ungefähr 10 Millionen Euro RSA Schlüssel der Länge 1024 bit in unter einem Jahr brechbar sind.

Mathematische Grundlage

RSA, das am weitesten verbreitete Systeme für Kryptographie mit öffentlichen Schlüsseln, basiert auf dem schon lange Zeit untersuchten zahlentheoretischen Problem der Faktorisierung. Es ist benannt nach seinen Erfindern Ron Rivest, Adi Shamir und Leonard Adleman [RSA78].

Das Faktorisierunsproblem basiert auf der Tatsache, dass es sehr einfach ist, zwei ganze Zahlen zu multiplizieren (polynomineller Zeitaufwand), es allerdings bisher nicht gelungen ist, einen Algorithmus anzugeben, welcher in polynomineller Zeit die Faktoren einer hinreichend grossen Zahl bestimmen kann.

Gelingt es, die Faktorisierung des Modulus eines öffentlichen RSA-Schlüssels zu finden, ist daraus die Berechnung des geheimen Schlüssels sehr einfach möglich. Damit ist das RSA-Verfahren gebrochen: Es können unautorisierte Signaturen geleistet und in den meisten Systemen neben der aktuellen, auch die vergangene und zukünftige Kommunikation entschlüsselt werde.

Faktorisierungs-Algorithmen

Zur Bestimmung der Primfaktoren von grossen Zahlen hat die mathematische Forschung der letzten zehn Jahre Algorithmen hervorgebracht, bei denen die Komplexität sehr viel langsamer zunimmt (subexponential) als die Menge der zu betrachtenden Schlüssel.

Bei dem für praxisrelevante Schlüssellänge nach dem bisherigen Stand der Forschung mächtigsten Angriff, dem (Generalised) Number Field Sieve, kann man im wesentlichen zwei grundlegende Schritte unterscheiden:

- *Siebungsschritt*
- Beim Siebungsschritt wird eine große Zahl von Quadratzahlen mit bestimmten algebraischen Eigenschaften (smoothness) gesucht. Allgemeiner spricht man davon, dass bestimmte "Relationen gesammelt" werden. Dieser Schritt ist hochgradig parallelisierbar.
- *Matrix-Reduktion*
- Im zweiten Hauptschritt werden Abhängigkeiten in einer sehr grossen Matrix (in der Praxis mehrere Millionen Zeilen und Spalten) gesucht. Das (Generalised) Number Field Sieve (GNFS) (deutsch: Zahlkörpersieb) besitzt eine heuristische asymptotische Laufzeit von O(exp(1,92+O(1))-(ln(n))^1/3 - (ln(ln(n))^2/3). Hier bildet für hinreichend grosse Zahlen ln(n)^1/3 den bestimmenden Faktor.

Aktuelle Verbesserungen

Da es in den letzten zehn Jahren kaum algorithmische Verbesserungen gab, haben sich Forscher intensiv damit beschäftigt, wie man die vorhandenen Algorithmen - insbesondere das Zahlkörpersieb - besonders effizient implementieren kann. Untersucht wurde der Einsatz dedizierter Spezialhardware, für den Siebungsschritte und und die Matrix-Reduktion.

1999 schlug Adi Shamir [Sham99] TWINKLE vor, ein optoelektronisches Gerät, das den Siebungsschritt erheblich beschleunigen kann. Allerdings galt Shamirs Abschätzung der Kosten für TWINKLE als wenig realistisch.

Ende 2001 veröffentlichte D.J. Bernstein [Bern2001] einen neuartigen Ansatz zur effizienten Implementation der Matrix-Reduktion vor. Bernsteins eigener Analyse zufolge war es mit seinem Ansatz erheblich schneller möglich, den Matrix-Schritt durchzuführen, als mit bisher gängigen Ansätzen. Dies lag zwar zum Teil auch daran, dass Bernstein ein anderes Kostenmaß benutzte, als andere Forscher zuvor, dennoch ermöglichte Bernsteins Ansatz signifikante Verbesserungen bei der Faktorisierung großer ganzer Zahlen, und sie regte viele

Experten dazu an, die Verwendung längere Schlüssel zu empfehlen (u.a. [Weis03]).

Ausführlich analysiert und verbessert wurde die Bernstein'sche Spezialhardware von Lenstra, Shamir, Tomlinson und Tromer auf der Asiacrypt 2002 [LSTT02].

Bei der Faktorisierung mittels GNFS von bis zu 512 bit RSA-Moduli hatte sich stets gezeigt, dass der Siebungsschritt den Gesamt-Rechenaufwand dominiert. Die Autoren von [LSTT02] kommen zu dem Schluss, dass dies auch für größere RSA-Moduli gilt: "... the security of RSA relies exclusively on the hardness of the relation collection step of the number field sieve." Es bleibt die Frage, wie teuer der Siebungsschritt zum Beispiel für RSA-Moduli der Größe 1024-bit ist.

TWIRL

Auf der PKC Konferenz 2003 präsentierten Geiselmann und Steinwandt [GS03] einen Ansatz, der sich an die von Bernstein vorgeschlagene Hardware für die Matrix-Reduktion anlehnte. Im Januar 2003 schliesslich verbreiteten Shamir und Tromer vom Weizmann Institut in Israel einen Artikel (als "preliminary draft") über das Internet, der die Gedanken von Geiselmann und Steinwandt aufgriff und eine verbesserte Konstruktion präsentierte: TWIRL (The Weizmann Institute Relation Locator).

Die Kosten, die Shamir und Tromer für TWIRL angeben sind bemerkenswert:

- TWIRL-basierte Hardware für nur 10 Millionen Euro erlaubt es, den Siebungsschritt für eine 1024-bit Zahl in einem Jahr durchzuführen (und damit die Zahl zu faktorisieren, s.o.)..
- Zur Faktorisierung eines 512-bit Modulus reichen TWIRL-basierte Hardware für nur 10.000 Euro und weniger als 10 Minuten Zeit.

Diese Angaben sind natürlich mit Vorsicht zu genießen. Shamir und Tromer haben eine theoretische Konstruktion präsentiert, aber (noch) kein TWIRL-Gerät tatsächlich gebaut. Darauf weisen sie in ihrer Arbeit selbst ausdrücklich hin.

Einige mathematische Details

Eine Instanz eines "Sieb-Problems" besteht aus einer ganzen Zahl R, einem Schwellwert T und Paaren (r_i,p_i), wobei pi eine kleine Primzahl ist. Im Zusammenhang mit dem Faktorisieren von 1024-bit Zahlen können die ''kleinen'' p_i grösser als 10^8 werden.

Die Paare (r_i,p_i) definieren Mengen $P_i=\{a \mid a \bmod p_i = r_i\}$. Diese Mengen bezeichnet man als "Progressionen". Beim "Sieb-Problem" geht es darum, möglichst viele Werte a zu finden, die in vielen Progressionen liegen. Genauer, es geht darum, möglichst viele Werte a zu finden mit $\text{sum}_{i: a \text{ in } P_i} \log(p_i) > T$.

Zum Faktorisieren mit dem Zahlkörpersieb muss man mehr als 10^{10}derartiger Instanzen von Sieb-Problemen lösen. Grob vereinfacht kann man Geräte wie TWIRL als Spezialhardware auffassen, die dazu dient, die Summen $\text{sum}\{i: a \text{ in } P_i\} \log(p_i)$ besonders effizient (d.h., unter Einsatz von möglichst wenig Chipfläche) zu berechnen.

Noch mehr Details

Die obigen Angaben zu Zeit und Kosten für eine Faktorisierung (bzw. für den Siebungsschritt) beziehen sich auf die "beste" zur Zeit bekannte Variante des Zahlkörpersiebs, die sogenannte large prime variant. TWIRL ist aber gar nicht in der Lage, alle erforderlichen Arbeitsschritte effizient durchzuführen, insbesondere nicht die sogenannte Co-Faktor Zerlegung. Wie man diesen Teilschritt mit Spezialhardware effizient durchführen und in die TWIRL Hardware integrieren kann, ist noch unbekannt. Allerdings geht es auch ohne Co-Faktor Zerlegung. Wenn das reine Zahlkörpersieb einsetzt, statt der large prime Variant, verschlechtert das Preis-Leistungsverhältnis für TWIRL. TWIRL-basierte Hardware für 50 Millionen US-$ erlaubt es, eine 1024-bit Zahl in einem Jahr zu faktorisieren. 50 Millionen Euro erscheinen für Geheimdienste oder große kriminelle Organisationen keinesfalls prohibitiv.

Erste Analyse der benötigten Hardware

Das bereits vor einiger Zeit ebenfalls von Adi Shamir veröffentlichte TWINKLE-Design [Sham99] für den Siebungsschritt basiert auf einer vergleichsweise aufwendige Chipfertigungstechnologie. Für die Multiplikation werden analoge optische Komponenten auf dem Chip eingesetzt. Dies scheint eine Fertigung in Gallium-Arsenid-Technologie vorauszusetzten, die nur an wenigen Produktionsstandorten beherrscht wird.

Weiterhin benötigt eine TWINKLE-Implementierung für 512-Bit-Keys einen kompletten Wafer mit 30cm Durchmesser. Ein einziger Fehler auf dem Wafer macht den Chip unbrauchbar. Da die Ausbeute komplett fehlerfreier Wafer sehr niedrig ist, steigen die Kosten sehr stark. Als praktische Faustregel gilt, daß die Kosten für einen Chip durch die rasch ansteigende Fehlerwahrscheinlichkeit kubisch mit der Chipfläche steigen.

Dem gegenüber steht mit TWIRL ein Design, daß sich vollständig in klassischer, Silizium-basierter VLSI-Technologie realisieren läßt. Die wichtigsten Komponenten sind hintereinandergeschaltete Digital-Addierer, DRAM, Multiplexer und kleine Prozessoren. Der erforderliche DRAM-Produktionsprozeß, Shamir und Tromer gehen von 0.13 micro Strukturgröße aus, wird mittlerweile von allen wichtigen Halbleiterproduzenten weltweit beherrscht.

Ein weiterer großer Vorteil ist die enorme Reduktion der Fläche für einen einzelnen Sieb-Chip. Die Autoren geben eine Größe von 1423 qmm; pro Chip für eine Schlüsselgröße von 1024 Bit an, womit pro Wafer 44

Chips produziert werden können. Bei einem einzelnen Fehler pro Wafer bleiben damit immer noch 43 funktionsfähige Chips übrig. Weitere Kostensenkung läßt sich durch die von den Autoren beschriebene Fehlertoleranz des Designs erreichen.

TWIRL erscheint mithin als ein realistisch implementierbares Design.

Parallelisierbarkeit und Wiedernutzbarkeit

Einige "mathematisch triviale" Gesichtspunkte wurde bisher in der öffentlichen Diskussion vernachlässigt.

- Das Verfarhen ist beliebig parallelisierbar. Dies bedeutet, dass wer beispielsweise 12-mal so viele Hardware verwendet (für 120 Millionen Euro), braucht nur einen Monat Zeit.
- Die teure Hardware ist nicht nach einer Faktorisierung "verbraucht". Sie kann eingesetzt werden um nacheinander mehrere Schlüssel zu "knacken".

Weiterhin ist zu bedenken, dass Angriffe nicht schlechter werden, aber man im Laufe der Zeit meistens noch weitere Verbesserungen findet.

Konsequenzen und Empfehlungen

Wenn sich die Einschätzungen von Shamir und Tromer auch nur ansatzweise bestätigen, sollten überall dort, wo Public-Key Kryptographie mit 1024-bit RSA-Schlüsseln eingesetzt wird, diese Schlüssel ausgetauscht werden. Betroffen ist der Einsatz vieler Standard-Sicherheitssoftware-Pakete (SSL, SSH, PGP, ...).

Die Alternativen zu RSA wie Diskrete Logarithmus basierte Systeme (DSA, El Gamal), insbesondere auch solche über Elliptischen Kurven, sollte angesichts der neuen Erkenntnisse intensiver untersucht werden.

In der heutigen Zeit gibt es unbestreitbar eine Menge Staaten und Organisationen, für welche beispielsweise ein paar Millionen Euro zur Brechung von wichtigen Schlüsseln eine lohnende Investition darstellen. Zudem leben wir in einer Weltlage in der selbst "befreundete" Staaten im bemerkenswerten Umfang Wirtschaftsspionage betreiben. Es dürfte unstreitbar sein, dass speziell die US-amerikanische NSA über einen umfangreichen Etat und eigene Hardwareentwicklung verfügt.

Konkret empfehlen wir,

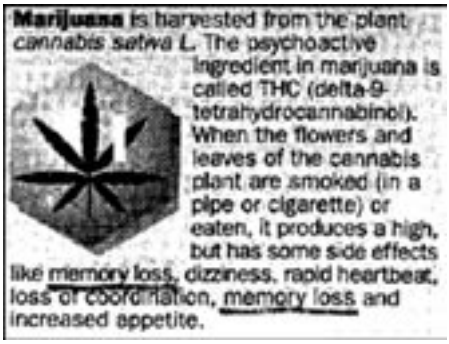
- 1024-bit Schlüssel baldmöglichst zu wechseln und
- Schlüssel von mindestens 2048 bit einzusetzen.

Bemerkenswert ist, dass für die geplante TCPA/ Palladium überwachungshardware ("Fritz-Chip") 2048-bit RSA Schlüssel verwendet werden.

In vielen Anwendungen (z.B. bei der E-Mail-Verschlüsselung) auf einem PC, ist der Zeitaufwand für die Public-Key Verschlüsselung unbedeutend, und der Einsatz von Schlüsseln, die deutlich länger als 2048 bit sind, empfehlenswert [WeLu99]. So erlauben die für die Verschlüsselung von E-Mail oft genutzten Programme PGP und der vom Bundeswirtschaftsministerium geförderte GNU Privacy Guard (GPG) Schlüssel, die bis zu 4096 bit lang sein können.

Literatur

- [Bern01] Bernstein, D.J. Circuits for integer factorization, manuscript, November 2001, http://cr.yp.to/papers.html
- [GS03] Geiselmann, W., Steinwand, R.: A dedicated Sieving Hardware. Public Key Cryptography Conference (PKC) 2003, Springer LNCS 2567, 254-266.
- [GPG00] GNU Privacy Guard, www.gnupg.org
- [LSTT02] Lenstra, A., Shamir, A., Tomlinson, J., Tromer, E., Analysis of Bernstein's Factorization Circuit, Proc. of Asiacrypt 2002, LNCS 2501 pp. 1-26, Springer Verlag, 2002.
- [RSA78] Rivest, R., Shamir, A., Adleman, L.: A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, 21(2), pp. 120-126, Februar 1978.
- [Sham99] Shamir, A.: TWINKLE, www.jya.com/twinkle.eps
- [ShTr03] Adi Shamir, Eran Tromer, Factoring Large Numbers with the TWIRL Device, http://www.wisdom.weizmann.ac.il/~tromer/papers/twirl.pdf, 2003.
- [WeLu99] Weis, R., Lucks, S.: Bigger is better! Anmerkungen zur Schlüssellängendiskussion, CCC Datenschleuder #68/69, 1999.
- [WLG99] Weis, R., Lucks, S., Geyer, W., Stand der Faktorisierungsforschung, DuD03/00, 2000.
- [Weis02] Weis, R., "Spezialhardware bedroht möglicherweise RSA-Sicherheit", Heise News 05.03.2002, http://www.heise.de/newsticker/data/wst-05.03.02-002/



DRM - Digitales Kurzwellenradio

von Anne Forker <chaney@chaney.de>

Seit einiger Zeit existiert mit Digital Radio Mondiale der Versuch, Kurz- und Mittelwelle mit Hilfe digitaler Technik wieder attraktiver zu machen. Um dieses Projekt und darum, wie man davon Gebrauch machen kann, soll es in diesem Artikel gehen.

Jeder kennt die Probleme bei der Frequenz-Vergabe für FM-Sender im UKW-Bereich, der in seiner Kapazität hier und da bereits an seine Grenzen stößt. War früher einmal FM die Rettung vor der bandbreitenintensiven AM, so rückt seit einiger Zeit AM wieder verstärkt in das Blickfeld der Medienschaffenden. Daran "schuld" sind digitale Übertragungsverfahren wie QAM und COFDM, die bereits bei DAB und DVB zum Einsatz kommen. Sie ermöglichen die parallele Übertragung von Daten auf Subträgern, was die benötigte Bandbreite verringert, und bieten eine höhere Übertragungsqualität.

Um das ganze etwas zu forcieren, wurde 1996 die Initiative Digital Radio Mondiale [1] gegründet, der sowohl Inhaltsanbieter als auch bekannte Hardware- und Softwarehersteller und Broadcaster angehören. Aus Deutschland sind dies u.a. das Fraunhofer-Institut für Integrierte Schaltungen, T-Systems, Telefunken, Bosch, Atmel und die Deutsche Welle. 2001 wurde das entwickelte digitale Übertragungsverfahren bei der ETSI standardisiert, im März 2002 kam noch die IEC Public Available Specification hinzu. Inzwischen hat auch die Bundesregierung dieses Projekt als wichtig eingestuft und 3.9 Millionen für die Forschung und Entwicklung in diesem Bereich locker gemacht.

Empfang

Für den Empfang genügt bereits ein einfacher Weltempfänger, allerdings sind einige Modifikationen nötig. Baupläne hierzu gibt es unter http://home.t-online.de/home/sat-service/sat/deutsch/deutsch.htm [2] .

Folgende Anforderungen sollte der Empfänger erfüllen:

- Bandbreite über 10 kHz
- möglichst rechteckige ZF-Filterkurve mit geringem Ripple
- speziell für DRM optimierte AGC
- treffsichere und stabile Oszillatoren mit geringem Phasenrauschen
- bestes Großsignalverhalten und gute Dynamik

Für die Zeit bis zum Aufkommen von Hardwaredecodern hat sich ein 12-kHz-ZF-Ausgang als Standard durchgesetzt, weil die Soundkarte des PC als A/D-Umsetzer herhalten muß. Sie sollte daher eine Abtastrate von 48 kHz beherrschen, keine Eingangs-AGC besitzen und einen linearen Frequenzgang bis mindestens 17 kHz aufweisen.

Die Demodulation müssen derzeit noch Softwareprogramme übernehmen. Hier gibt es zwei Projekte: das Fraunhofer Softwareradio [3] und die an der TU Darmstadt entwickelte Open-Source-Software "Dream" [4] .

Eine Uebersicht ueber die Sendungen gibt http://www.rnw.nl/realradio/html/drm.htm [5] , eine genaue Einführung in die Technik findet sich bei http://www.drm-info.de [6] . Die Systemspezifikation ist im ETSI-Standard ES 201 980 [7] gegeben.

Wie geht es weiter?

Die derzeitigen Sendungen haben eher Testcharakter als "richtigen" Informationsgehalt, trotzdem wurde kürzlich der offizielle Start des digitalen Mittelwellenradios bekanntgegeben [8] . Man kann damit rechnen, daß sich im nächsten Jahr die ersten Hardware-Receiver für DRM auf Messen zeigen werden.

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

[2] *http://home.t-online.de/home/sat-service/sat/deutsch/deutsch.htm*

[3] *http://www.iis.fraunhofer.de/dab/products/drmreceiver/*

[4] *http://www.tu-darmstadt.de/fb/et/uet/drm.html*

[5] *http://www.rnw.nl/realradio/html/drm.htm*

[6] *http://www.drm-info.de*

[7] *http://pda.etsi.org/pda/*

[8] *http://www.bmbf.de/presse01/877.html*

Irgendwann wie Stevens schreiben

von Su-Shee <banshee@penguins.de>

Jeder will sie - kaum jemand schreibt sie: Die klare, verständliche, lesbare technische Dokumentation. Wie schreibt man gute technische Dokumentation? Was ist das eigentlich, "gutes Schreiben"?

Her damit: Ein Subjekt

Gut schreibt, wer verständlich schreibt. Gut schreibt, wer seine Aussage in einen Satz mit höchstens einem Komma und höchstens einem Fremdwort steckt. Gut schreibt, wer oft und viel schreibt, wer schreiben übt. Gutes Schreiben ist weder eine exklusive Begabung noch eine geniale Inspiration: Schreiben ist Handwerk und es gibt einfache Regeln für gutes Schreiben und deswegen kann man Schreiben lernen. Für alle Textarten wendet man ein Set von Regeln an - egal, ob über Technik, über Philosophie oder Tagebuch geschrieben wird: Die erste Regel lautet: Kein Passiv. "Tagebuch geschrieben wird" - von wem denn? Warum bloss? "Ein Segfault wurde ausgelöst." Von wem? Durch welches Problem? Was war die Ursache? Nicht umsonst haben Sätze ein Subjekt (der "Agent", der Handelnde) und ein Objekt (das, worauf sich die Handlung bezieht) und ein Prädikat (das Verb). Passiv benutzt man dann, wenn kein Subjekt vorhanden ist - und das kommt wirklich selten vor. Ein einfaches Syntaxhighlighting im Lieblingseditor genügt, um seinen Stil sofort klarer zu gestalten. Da, ein verstecktes Passiv! Wer gestaltet da was klarer? Mit dem Syntaxhighlighting in Vim oder Emacs kann der Autor schlechten Stil und Passiv hervorheben. Schon präziser!

Weg damit: Fremdwörter

Gerade bei komplizierten Beschreibungen von Technik will der Leser Klarheit und Präzision, nein halt: Genauigkeit. Wieso ein Fremdwort verwenden, wenn man keins braucht? Also, der Leser will Klarheit und Genauigkeit. Unmissverständlich. Das ist die zweite Regel: Nicht sloterdijken und nicht habermasen! Moderne Philosphie - ich nenne es postmodernes Hirnwichsen - ist oft unlesbar: "Das Subjekt erzeugt in seiner metaphsysischen Relevanz ein reziprokes Rhizom zur Deprivation seiner Selbst." Das muss nicht sein: Viele berühmte Philosophen kommen ganz ohne Fremdworte und gedrechselte Sätze aus, weil ihr Ziel Klarheit war. Natürlich kann man auch technische Phrasen dreschen - Handbücher und Howtos sind voll davon. Autoren vergessen gern, dass Leser Bücher und Texte verstehen wollen. Man schreibt einen Text*für* einen Leser, nicht gegen ihn.

Relativsätze sind relativ lang

Zusammengefasst: Kein Passiv, so einfach und klar wie möglich. Das ist sehr schwierig und klingt am Anfang ungewohnt - ist denn nicht nur kompliziertes Schreiben gutes Schreiben? Ist nur was wissenschaftlich klingt auch eine Wissenschaft? Nein. Unsinn. Hemingway hat 1954 den Nobelpreis für seine Sammlung von Subjekt - Objekt - Prädikat Sätzen bekommen und was für Hemingway gut war, sollte für uns ausreichen. Jeder Stevens macht es uns vor: Klare Sätze. Niemals länger als 2, höchstens 3 Zeilen. Jeder Satz bestückt mit Wissen. Wer Grammatik beherrscht wie Thomas Mann darf mehr als 3 Zeilen schreiben. Der Rest von uns bleibt unter 3 Zeilen Satz und trennt, sobald er einen Relativsatz beginnt, den Satz in mehrere Sätze auf. Also: Der Rest von uns bleibt unter 3 Zeilen Satz. Sobald er einen Relativsatz beginnt, trennt er ihn in zwei Sätze auf. Damit erspart man sich auch lästige Kommaregeln. Die braucht man nämlich nicht, wenn kein Komma notwendig ist.

Dingsda: Nullwörter

Das zeigt uns die nächste Falle: Nicht schwafeln, sondern informieren. Es gibt im Deutschen eine Sammlung Nullwörter, die man in beliebiger Menge in Texte einstreuen kann: Wirklich, nun, ja, gar, so, ungefähr - alle Worte, die bereits durch den Wortsinn einleiten, dass jetzt etwas folgt, was ungenau ist: "Ungefähr" ist eine ungenaue Zeit- oder Mengenangabe. "Der Compiler braucht ungefähr drei Stunden". Wie wäre es stattdessen mit: "Ist die CPU schneller als 1 GHz, braucht der Compiler 2.45 Minuten, ist die CPU langsamer, dau-

ert der Durchlauf 3.30 Minuten. Mit einem 486er wirft man den Compiler besser gleich über Nacht an." Na also. Jetzt weiss der Leser, was ihn wirklich erwartet!

Raus damit: Adjektive

Ebenso überflüssig: Adjektive. Da fällt es den meisten Schreibern schwer, auszumisten, denn Adjektive machen den Text schwungvoll und lebendig. Das erscheint nur auf den ersten Blick so: Adjektive machen den Text schwülstig und langatmig und quetschen das letzte Fünkchen Phantasie aus dem Leser - bloss nicht selbst die Leidenschaft vorstellen, lieber hinschreiben: "Leidenschaftlich und wild küsste er ihren herrlich gerundeten Bauchnabel, sie stöhnte tief und .." Damit gewinnt man den Bastei-Lübbe Billigpreis. Verben machen den Text lebendig, denn mit Verben drückt man Bewegung und Handlung aus. Wieso nicht besser schreiben: "Er fickte sie, sie biss zurück und schrie dann in die Nacht hinaus." Wie sie es nun machen, bleibt der Vorstellung des Lesers überlassen. In technischen Texten spart man sich analog Adjektive wie "der tolle Editor" - wär' er Mist, würde man keinen Artikel schreiben. "Der grossartige Compiler" oder auch der "schnelle Compiler" sind genauso überflüssig: Schnell in Bezug auf was? Warum bewertet der Autor den Compiler als grossartig? Stattdessen nennt man die Vorzüge, die einen Compiler oder Editor aus der Masse der anderen Produkte hervorheben: "Das höppelgewöppte Doppelnipp macht den gcc zu einem schnellen Compiler. Alle anderen Compiler schnöppen nur das Huppelwupp und das macht sie langsam, weil kein Dippelschnipp optimiert wird." Na gut. Ein Passiv. "weil keine Funktion für optimiertes Dippelschnipp existiert." Oder noch besser: "Weil kein Entwickler die Funktion zum optimierten Dippelschnippen implimentiert hat." Ah. Das Feature fehlt also!

Schluss damit: Anglizismen

Entschuldigung - "diese Fähigkeit" fehlt also. Die goldene Regel für Anglizismen lautet: Anglizismen nur dann verwenden, wenn der englische Ausdruck ein wichtiges Stichwort ist, unter dem man eine Suchmaschine befragen kann oder die Übersetzung Unsinn ergibt: Die Suche nach "Übersetzer" fördert andere Links zutage als die Suche nach "Compiler" und deswegen bleibt ein Compiler bei mir ein Compiler. Allerdings schreibe ich: "Ich lade den Compiler unter ftp.bla.de" herunter und nicht: "Ich downloadete den Compiler unter ftp.bla.de". So bleibt bei mir auch ein Array und Hash in Perl ein Array und ein Hash - schreibe ich aber allgemein über Listen, schreibe ich "Listen" und nicht etwa "Arrays". Ich entscheide von Fall zu Fall - brauche ich eine eingedeutschte Verbform, fliegt der Anglizismus raus und ich versuche, eine gute Übersetzung zu finden. Nochmal alle Tipps zusammen: Kein Passiv, klare, einfache Sätze, wenig Fremdwörter, Adjektive wegstreichen, stattdessen Verben verwenden und Anglizismen nur dort verwenden, wo sie unverzichtbar sind. Fehlt noch was?

Durchsuchung: Substantivierte Verben

Ja! Eine Fähigkeit der deutschen Sprache ist die Nutzung der Anwendung von der Substantivierung von Verben! Oft schreiben unerfahrene Autoren, um seriöser zu klingen, Sätze wie diesen: "Durch die Compilierung wird die Software zu einem Binary" - das geht klarer und einfacher: "Der gcc (Subjekt - Wer?) kompiliert (Verb - was passiert?) die Sourcen (das Objekt - Wen?) zu einem Binary (Ziel der Aktion)." Jetzt weiss man, wer was mit welchem Ziel tut. Mein Satz geht auch noch knapper: "Oft schreiben unerfahrene Autoren" .. Wer da was tut, taucht erst spät im Satz auf: "Unerfahrene Autoren schreiben oft.." oft? Weg damit. "Unerfahrene Autoren schreiben Sätze mit substantivierten Verben, um seriöser zu klingen:" Na also. Wer tut was womit und zu welchem Zweck? Alle Fragen beantwortet.

Für den Editor alles zusammen:

Die goldene Regel lautet: Wegstreichen, kürzen, rauswerfen! Ein Text gewinnt fast immer, wenn der Autor rigoros kürzt. Satz zu lang, mehr als 2 Kommata und keine Aufzählung? Zwei Sätze draus machen. Zuviele Adjektive? Raus damit, durch Verben ersetzen. Substantivierte Verben und Fremdworte? Geht alles knapper, klarer, genauer: Weg damit. Anfangs erscheint der Satz dann abgehackter - man könnte auch sagen: knackiger, kürzer und daran muss man sich erst gewöhnen. Wie erkennt man auf einen Blick problematische Wortgruppen?

Passiv: wird, wurde, geworden, gemacht sind typische Formen, die ganz sicher in einem Passivsatz ohne Subjekt enden. Kann man die Frage "wer macht da was?" klar beantworten, hat man ein Subjekt und dann soll man es auch hinschreiben.

Fremdwörter: Fremdwörter enthalten bestimmte Endungen, die man gut hervorheben kann: -ismus, -tät, -ierung, -tion, -tor. Fast jedes Fremdwort kann man durch ein passendes deutsches Wort ersetzen und so die Verständlichkeit erhöhen, ohne den Sinn zu entstellen. Nur selten ist ein Fremdwort ein klarer Fachbegriff, der unverzichtbar ist: Gastritis? Magenschleimhautentzündung. Ist zwar länger, aber -itis ist immer eine Entzündung und das Gast- irgendwas mit dem Magen des Menschen zu tun hat, weiss auch nicht jeder. Ismen benutzt man als Endsilbe für "streben nach" - Kapitalismus - streben nach Kapital, Imperialismus, streben nach Imperien. Die Silbe -tät beschreibt einen Zustand, die Silbe -ierung den Prozess dazu: "Globalität" ist der Zustand, den wir nach dem Prozess der "Globalisierung" erreichen. Deswegen sind Formulierungen wie "der Prozess der Industrialisierung" oder "der Zustand der Konformität" doppeltgemoppelt - raus damit. Der "-or" ist immer der Täter in einem Fremdwort: Terminator. Diktator. Contruktor. Imperator. Und der Täter sorgt für ein Ziel der Handlung - ein "-ion": Der Construktor sorgt für eine Construktion, der Terminator sorgt für eine Termination. Die Termi-

nierung ist der Prozess des Terminators mit dem Ziel der Termination! Und eine Terministis ist eine akute Metallgelenksentzündung mit schwerwiegenden Folgen für die Umwelt. Eine Termite hingegen.. ok.

Nullwörter: da ja, nun, gleich, obwohl, als wenn, gar, so, "ohne weiteres", "bis hin zu", wirklich, überhaupt, sehr, je, manchmal, beinahe, nur, Gerade (am Satzanfang) kann man fast immer ersatzlos streichen. Das gleiche gilt für Marketingworte: Substantiv enthält das Wort "Substanz" - und von "Agile Programmierung" bis "Zero Administration Needed Feature" enthalten die Worte keine - raus damit.

Adjektive: Einige Adjektive sind nützlich, weil sie den Zustand, das "So-Sein" eines Wortes genauer beschreiben: Rot. Grün. Tot. Kombinationen mit einem Substantiv, dass bereits diesen Zustand suggeriert, ergeben den berühmten weissen Schimmel. Oder für Nerds: Den grünen Schimmel. Ein Schimmel IST sowieso weiss, sonst hiesse er nicht so. Eine Leiche ist tot. Deswegen hat uns der Duden das Wort "Leiche" geschenkt. Dazu kommen die schwachen Adjektive, die sich von anderen Worten ableiten: Endungen wie -lich, -haft, -sam oder -isch kommen in Worten wie arbeitssam (fleissig), lachhaft (ich lache) oder unglaublich vor: Fast immer kann man ein Verb daraus machen und erzeugt so eine Handlung und muss dann auch einen Handelnden einfügen: "Das ist unglaublich" - Was denn? Und wer glaubt da was nicht? Wieso? Wer sich nicht sicher ist, ob ein Adjektiv angebracht ist oder nicht: Rauswerfen.

Substantivierte Verben: Die Endung -ung ist ein totsicheres Merkmal. Endung kommt von enden und Hoffnung von hoffen. Deswegen kann man genauso gut schreiben: "Endet ein Wort mit der Silbe -ung.." oder "Wenn das Wort mit der Silbe -ung endet.." Zunächst erscheint es kleinlich, aber ein Substantiv in ein Verb umwandeln zwingt den Autor aus einer Compilierung ein "Wer kompiliert was" zu machen und aus einer Verkabelung ein "wer verkapelt was womit".

Lektüre für Fortgeschrittene

Für Fortgeschrittene gibt es noch ein paar mehr Regeln - die oben genannten für Einsteiger kann man mit vielen Editoren hervorheben und gleich rauswerfen, bevor man sie fertig getippt hat. Wer sich einlesen möchte: Für die deutsche Schriftsprache liest man "Deutsch fürs Leben" und "Deutsch für Kenner" von Wolf Schneider. Zu einem besseren Stil in Englisch verhilft der Klassiker "On Writing Well" von William Zinser - übrigens eine Erleichterung für jeden, der die Zeitenfolge von Relativsätzen oder Passivformen nicht mehr im Kopf hat: War ja sowieso kein guter Stil. Wer dann wissen will, wie Schriftsteller mit den Worten ringen und solche Stilmittel befolgen, dem sei Stephen Kings "Das Leben und das Schreiben" (englisch: "On Writing") ans Herz gelegt.

Überwindbarkeit von Gesichtserkennungssoftware

von starbug

Systeme zur Gesichtserkennung gibt es in den verschiedensten Ausfürungen, die sich in der Aufnahmehardware (Kamera im optisch sichtbaren Bereich, Infrarot- oder Stereokamera) sowie in der Auswertesoftware (Elastic-graph-matching, Eigenface, Messen des Verlaufs von Blutgefässen) unterscheiden.

Die meisten Systeme im Enduser-Bereich setzen aus Kostengründen auf Webcams (arbeiten bekanntlich im sichtbaren Wellenlängenbereich) und die damit verbundenen Softwarelösungen.

Funktionsweise

Wie bei allen biometrischen Verfahren müssen sich auch bei der Gesichtserkennung die Benutzer zu allererst enrollen. Dazu werden meist mehrere Bilder der Person aufgenommen um daraus das Template zu generieren. Die Abläufe beim Enrollement und bei der späteren Erkennung sind dabei sehr ähnlich. Zu Beginn sucht ein Algorithmus in den Bildern nach Gesichtstypischen Formen. Bei einem positiven Ergebnis wird die Grösse der gefunden Gesichts normalisiert, um unterschiedliche Entfernungen zwischen Person und Kamera auszugleichen. Das jeweilig verwendete Verfahren bestimmt nun den Fortgang der Verarbeitung.

Beim Elastic-graph-matching werden markante Punkte in dem Gesicht (Augen, Nase, Mund) extrahiert und ihre Position ermittelt. Der Eigenfacealgorithmus hingegen kombiniert einige 100 Grundgesichter so miteinander, dass sich eine relativ hohe Übereinstimmung mit dem aktuellen Bild ergibt. Vor allem die Eigenfacemetode ist sehr stark von der Haltung des Kopfes und der Beleuchtung des Gesichtes abhängig, weswegen Gesichtserkennungssysteme teilweise noch grosse Falschrückweisungsquoten haben. Die führt dazu, dass im praktischen Einsatz der Schwellwert für die Erkennung oft sehr niedrig eingestellt wird.

Überwindung

Nicht selten reicht es schon aus, ein Foto einer berechtigten Person vor die Kamera zu halten um als diese erkannt zu werden! Aufgrund der schon angesprochenen Abhängigkeit von der Ausleuchtung des Gesichts ist es machmal noch nötig das Foto etwas nachzubearbeiten. Dazu wird es eingescannt, falls es nicht sowieso schon in digitaler Form vorliegt. Um die Ausleuchtung des Gesichts anzupassen, muss man jetzt nur noch die Lichtverhältnisse am Einsatzort kennen. Ist es nicht möglich, an solch eine Referenz zu gelangen können auch mehrere Bilder mit wahrscheinlichen Lichtverhältnissen (z.B. Beleuchtung von oben, von der Seite oder von vorne) erstellt werden, die dann nacheinander vor die Kamera gehalten werden. Dazu müssen die Bilder nicht einmal ausgedruckt werden, da auch der Bildschirm eines Notebooks die nötige Auflösung besitzt um die Systeme zu überwinden. Auf Grund der Beschichtung des Displays kann es aber zu anderen Problemen, wie z.B. starken Reflexionen, kommen. Allerdings bietet diese Variante den grossen Vorteil, dass die Fotos auch noch am Einsatzort nachbearbeitet werden können.

Etwas mehr Aufwand ist nötig, falls das verwendete System mit einer Lebenderkennung ausgestattet ist. Solche Zusatzfeatures basieren meist auf Bewegungen im Gesicht (Zwinkern) oder des ganzen Kopfes (Drehen, Verkippen). Aber auch hier ist die Lösung denkbar einfach. Anstelle eines Einzelbildes wird dem System eine Sequenz von Bildern bzw. ein Video vorgespielt. Dazu filmt man einen berechtigten Benutzer so lange, bis eine ausreichend Menge an Kopfhaltungen (oder Bewegungen im Gesicht) vorhanden sind. Stimmen die Lichtverhältnisse des Videos mit denen am Einsatzort überein so kann das Video direkt abgespielt werden. Tun sie dies nicht muss auch hier noch eine Anpassung vorgenommen werden. Dazu extrahiert man aus dem Video mehrere Einzelbilder (fünf sollten ausreichen) mit einer möglichst breiter Bewegungspalette, bearbeitet diese und synchronisiert die Abspielfrequenz nur noch mit der Aufnahmefrequenz des Systems. Und schon ist auch die Lebenderkennung überwunden. Natürlich sind solche Versuche nicht gerade schwer zu bemerken, vor allem, wenn die Kamera noch zusätlich von einer Person überwacht wird. An solchen Orten oder auch bei der Verwendung von Stereokameras könnte man es mit Latexmasken oder Schminkutensilien versuchen, um das eigene Aussehen dem eines berechtigten Benutzer anzupassen.

All die hier beschriebenen Verfahren funktionieren natürlich nicht bei Systemen, die auf der Auswertung von Infrarotbildern basieren. Aber dort gibt es sicher andere Möglichkeiten. :)

Wer hat Angst vorm bösen Wolf?

von nitraM <martin@berlin.ccc.de>

... niemand. Angst haben muss man nur noch vor durchgeknallten Weltimperatoren und Leuten, die Shell-Metazeichen im Namen tragen. Letzteren läßt sich durch einige Überlegungen entgegenwirken, womit sich dieser perlorientierte Artikel beschäftigt.

Gewöhnlich sind sich Webanwendungsentwickler der Notwendigkeit zur Überprüfung von Benutzereingaben bewußt: aufgrund Unachtsamkeit eröffnet sich mit dem fortschrittlichen Stringhandling beliebter Skriptsprachen schnell das ein oder andere Sicherheitsproblem. Werden Parameter eines HTTP-Requests durch ein Programm verarbeitet und bleiben von Wertüberpruefungen verschont, kann besonders im Zusammenhang mit Stringexpansion und Shellaufrufen die Sicherheit des Systems stark gefährdet werden.

Wenn Schüler im Rahmen ihrer Computer AG aktuelle Meßwerte vom Schulbiotop im Netz veröffentlichen und sich ein Upsi-Konstrukt im Code befindet, dann spielt das auch keine Rolle und wenn man von einem fehlerhaften CGI-Programm auf smartfilter.de hört, erheitert es sogar für einen kurzen Moment das triste Dasein. Es sind zumindest Schäden vorstellbar, die dann nicht mehr erheitern.

Die Problemzonen liegen z.b. dort, wo Perlcode und Betriebssystem interagieren. Funktionsaufrufe wie system() und exec() werden gerne mit einem String als Parameter gefüttert:

```
system("mail -s 'anmeldung' $email_addr");
```

system() bewirkt in dieser Formulierung das Starten einer Shell, die wiederum das Mailprogramm ausführt. In dieser fahrlässigen system()-Verwendung lassen sich via $email_addr weitere Befehle mit dem Semikolon integrieren, so wie man es von Shellprogrammierung her kennt. Übergibt man Parameter als Liste, wird keine Shell gestartet, wodurch Metazeichen auch nicht expandieren. In einem Fall wie

```
system('cp', '-R', 'foo-bar', $path);
```

wäre die Variablenverwendung immer noch kritisch, selbst wenn auf Metazeichen nicht besonders geachtet werden muß. Beim normalen open()-Befehl sowie bei der Verwendung von Backtickkonstrukten ist die Stringform sogar notwendig. Es gibt keine Listenalternative.

Soetwas sollte immer vermieden werden:

```
open(TMPL, $template_file);
```

```
open(TMPL, "cstyle:

$foo = `cat $file`;
```

Das erste Beispiel davon ist sogar flexibler misbrauchbar. Beinhaltet der String nur einen Dateinamen, so wird die Datei im Lesemodus geöffnet. Explizite Modusangaben wie ">>" oder ähnliches lassen den Stringparser einen Dateinamen erwarten, da funktionieren dann auch keine Shellmetazeichen. Dagegen bewirken Pipesymbole das Forken einer Shell mit vollem Featureset.

Beim Umgang mit Shells sollten auf jeden Fall die Metazeichen &;`'"|*?~<>^()[]{}$nr gefiltert werden. Für eine weiterführende Diskussion sei auf die Quellen verwiesen [1] .

Bei Skriptsprachenverwendern schon fast in Vergessenheit geraten ist das magische 0-Byte, welches in der Sprache C das Ende einer Zeichenkette symbolisiert. Strings in Perl speichern diesen Terminator problemlos - subtile Probleme können sich ergeben, wenn Perlstrings in C-Code weitergereicht werden und sich ein derartiges 0-Byte einschleicht. 0-Bytes in Perlstrings werden nicht expanded. d.h. auch sie würden mit einfacher Logfilegenerierung via print() nicht erscheinen und sind so schwieriger zu debuggen. Es gibt folgendes open()-Szenario, wo das 0-Byte eine explizite Verwendung findet. Es soll eine Datei geöffnet werden, deren Dateiname führende und anhängende Leerzeichen besitzt. die open-Funktion ignoriert jedoch Leerzeichen an den beiden Positionen. perlopentut empfiehlt als Zaunpfahl für den Tokenizer den Dateinamen mit den Strings "./" und "0" zu umklammern:

```
$file =~ s#^(s)#./$1#; open(FH, "cstyle:
```

sthetisch ist das sicher nicht. In der Phrack #55 [2] beschreibt rain forrest puppy wie Perls 0-byte-Verhalten in einigen Codekonstrukten misbraucht werden kann. Ein Perlprogramm könnte Benutzerdaten für eine Dateinamensbildung verwenden:

```
$page = "../../etc/passwd0"; # vom user definierte zeichenkette

open(FH, "cstyle:
```

Das Beispiel würde dann nicht mehr die über ein Muster beschriebene HTML-Datei öffnen. Ich wage die Behauptung, daß uns das 0-Byte noch im Jahr 42 auf die Füße fallen wird, wenn Bits durch A-T und C-G representiert werden und wir Faustkeilsprachen wie C für schon längst überwunden geglaubt haben. [3]

In nahezu allen Anwendungsfällen ist die beste Vorkehrung restriktives Filtern. Das meint genau nur Zeichen zu lesen, die erwartet werden. Für eine einfache Umsetzung eignen sich Perls eingebaute reguläre Ausdrücke, die den kompletten String betrachten oder einen unkritischen Substring extrahieren:

```
if($id =~ m!^#[wd]+$!) { # id ok ... } else { # bad
id ... }
```

Um ein derartiges Vorgehen zu unterstützen, kennt Perl einen taint mode (taint: fleck, makel), in dem extern belegte Variablen nicht mehr ungefiltert als Parameter tendenziel kritischer Befehl verwendet werden können. Ausnamen stellen system() und exec() bei Argumentenlisten und generell print() und syswrite() dar. Darüber hinaus werden weitere einfache Sicherheitschecks durchgeführt. Dieser Modus ist als Hilfestellung zum Auffinden von Problemen zu verstehen. (man perlsec) Sicherheitsüberlegungen werden dem Programmierer dennoch nicht abgenommen, weshalb dieses Feature in der Praxis kaum verwendet wird.

Beim Verwenden von Benutzereingaben aus Formularen im Zusammenhang mit Shellaufrufen ist der Entwickler eigentlich schon im Vorfeld besorgt. Die Gefahren stecken bekanntlich im Detail, weshalb Situation exisitieren, in denen Risiken nicht auf Anhieb erkennbar sind. Werden eingaben einer Webanwendung in externe Programme weitergereicht, wer weiß dann schon konkret, was da passiert? Als Beispiel soll hier das Satzsystem Latex herhalten: Mit etwas Perl und Latex kann man dynamisch Dokumente erzeugen. Werden keine Makroverwendungen in Benutzereingaben gefiltert könnte man mit dem include-Makro den Inhalt lesbarer Dateien einfügen. Somit ließen sich Informationen aus einem Rechner ziehen. Schreiben von Dateien oder gar das Aufrufen von Programmen ist nicht möglich. Doch wer garantiert, daß es sich immer so verhält? Zahlreiche Opensourceprogramme basieren auf Tools, die irgendwann von irgendwem entwickelt wurden. Und bei neueren Versionen? Zwar wird man i.d.R. eine Rückwärtskompatiblität z.b. bei Kommandozeilenparametern anstreben, um Updatestreß zu vermeiden, nur wer stellt sicher, daß neue Features nicht zum Einbrechen benuzt werden können? Da kann man nur hoffen, daß die Entwickler in Kontakt stehen oder andersweitig von neuen Entwicklungen Kenntnis nehmen.

Das Konzept für einen umfassenden und wirkungsvollen Schutz kommt wie immer in die Schublade "Illusionen". Sorgfältige Werteüberprüfung von Parametern ist der empfohlene Weg, der von weiteren Maßnahmen begleitet werden kann. Die konkreten Lösung sollte sich stets am Problem orientieren, denn auch für Fehler aufgrund von Unvorsicht oder Unwissenheit gilt: there is always more than one way to do it.

[1] *http://www.w3.org/Security/faq/www-security-faq.html*

[2] *http://www.phrack.org/phrack/55/P55-07*

[3] *http://www.rootsweb.com/~nerailrd/trivia.html*

Das neue Jugendschutzgesetz

von Sascha Roth <sascharoth@gmx.de>

Am 1. April wurde das neue Jugendschutzgesetz verabschiedet. Vielerorts herrscht heftige Verwirrung darüber, welche Konsequenzen die nderungen speziell für Computerspieler und Händler hat. Kern jeglicher kleiner Erweiterungen und nderungen bildet die verbindliche Altersfreigabe von Unterhaltungssoftware, wie es sie für Kino- und Videofilme schon länger gibt.

Dieses reformierte Jugendschutzgesetz [1] macht die Alterskennzeichnung für "Bildträger mit Filmen oder Spielen" verbindlich. 11-jährigen Kindern dürfen z.B. keine "ab 12" freigegebenen Spiele verkauft werden. Eine Gelegenheit solche Games Probespielen zu dürfen, darf nach Auffassung des Gesetzes auch nicht vorhanden sein - laufen dann auf PCs in den Kaufhäusern nur noch "Löwenzahn"-CD-ROMs?

Das ganz große Durcheinander droht allerdings weniger den gewöhnlichen Einzelhändlern - dafür sorgen Industrie und entsprechende Durchführungsverordnungen der Behörden-, sondern Verkäufern auf dem Flohmarkt oder Onlineauktionen, bei denen es ungekennzeichnete Klassikware zu erstehen gibt. So gilt für eine "uralte Super Mario"-Catridge für das Super-Nintendo-System mangels Alterskennzeichnung ab sofort "ab 18". Wer so etwas verkauft, muss sicherstellen, dass sein Kunde volljährig ist, oder er macht sich strafbar.

Die Altersfreigabe haben vorgeschriebene Form, Farbe und Größe auf der Verpackung des Bildträgers, also CD-ROM, DVD oder Cartrige. Sofern der Hersteller keine Ausnahmegenehmigung der obersten Landesbehörden sein Eigen nennt, müssen die quadratischen Signets eine Kantenlänge von 1,5 cm besitzen. Nur bei Datenträgern deren Fläche kleiner als 20 Quadratzentimeter ist, dürfen die Kantenlängen der Signets auf 1,2 cm schrumpfen. Da sich aber kleine Datenträger durchsetzen, wird es eng: So sind z.B. die Cartriges von Nokias aktueller mobiler Spielekonsole N-Gage nur gerade einmal doppelt so groß wie ein 50 Cent Stück und damit sehr schwer zu kennzeichnen. Aber dergleichen spezielle Probleme erfassen gerade einmal die Spitze des Eisberges an Problemen und Ungereimtheiten, die sich im Zusammenhang mit dem reformierten Gesetz ergeben haben.

Die Unterhaltungssoftware-Selbstkontrolle (USK) [2] versieht seit neun Jahren Computerspiele mit Altersempfehlungen, die allerdings bislang nicht bindend waren. Die früher vergebenen Kennzeichnungen werden mit dem neuen Gesetz zu verbindlichen Freigaben. Bereits geprüfte Software muss also nicht neu gewertet werden.

Herstellern von Computerspielen bietet das neue Gesetz neue Sicherheiten. Ist ein Produkt einmal von der USK gekennzeichnet, kann es im Nachhinein nicht mehr indiziert, also in die Liste der "jugendgefährdenden Medien" aufgenommen werden. Es besteht allerdings die Möglichkeit für die Bundesländer, bei der Bundesprüfstelle für jugendgefährdenden Medien (BpjM) [3] einen Antrag auf Indizierung einzureichen, noch während des Prüfverfahrens.

Nicht gekennzeichnete Spiele werden ab sofort behandelt, als hätten sie von der USK die Kennzeichnung "keine Jugendfreigabe" erhalten. Sie dürfen also nur an Volljährige verkauft werden. Das betrifft auch automatisch alle Spiele, die direkt aus dem Ausland eingeführt werden. Diesen Umstand bekommen nicht zu letzt spielbegeisterte Mac- und Linuxspieler zu spüren: Die meisten beliebten Games für die anderen Betriebssysteme sind meist Importware und werden aus Kostengründen nicht bei der USK eingereicht.

Besonders hart trifft die Regelung nicht gekennzeichnete Spiele von Klassikern. Allen Produkten die älter als Jahre sind, fehlt zwangsläufig eine Kennzeichnung. Wer also als noch minderjähriger das Spielemodul

"Da fühlen wir uns doch gleich viel sicherer, wenn dieser nette Herr auf uns aufpasst."

"Asteroids" für seine Atari-VCS-2600-Konsole sucht, guckt von Gesetzes wegen in die Röhre.

Zudem gibt es ein Problem der Alterskontrolle. Es haben sich schon einige Märkte darauf vorbereitet, Unterhaltungssoftware nur nach Ausweiskontrolle zu verkaufen. Was allerdings bei Sonderverkaufsveranstaltungen bei neu herauskommenden Spielen passieren soll, ist noch unklar: Bei solchen Gelegenheiten gehen innerhalb weniger Stunden mehrere Tausend Exemplare über die Ladentheke.

Ein weiteres Problem betrifft das Probespielen: Ist ein PC an einem für Minderjährige zugänglichen Ort aufgestellt, muss sichergestellt sein, dass das ausgestellte Produkt für die Spieler entsprechend ihrer Alterskennzeichnung geeignet ist. Möglicherweise wird es bald für ältere Gamer ähnlich wie bei Videotheken abgeteilte "Schmuddelecken" geben, in denen man sich die gewünschte Software vorführen lassen kann.

Auch Versandhändler dürften über das neue Gesetz nicht unbedingt erfreut sein. Ungekennzeichnete Medien und solche, die keine Jugendfreigabe erhalten haben, dürfen über das, was im Sinne des Gesetzes ist, nicht abgegeben werden. Um diese Schranke zu umgehen, muss ein Versender das Alter seines Kunden "in geeigneter Weise" überprüfen. Welche Verfahren dafür als geeignet gelten, lässt der Gesetzgeber offen. Es bleibt ebenfalls offen, was mit Software, die eine Altersfreigabe "ab 16" erhalten hat, geschieht: Folgt man den Buchstaben des Gesetzes darf solche Software nur mit einem geeigneten Altersnachweis herausgegeben werden. Der Einzelhandel muss den Personalausweis fordern, der Versandhandel hingegen kann solchermaßen gekennzeichnete Ware ganz regulär verkaufen.

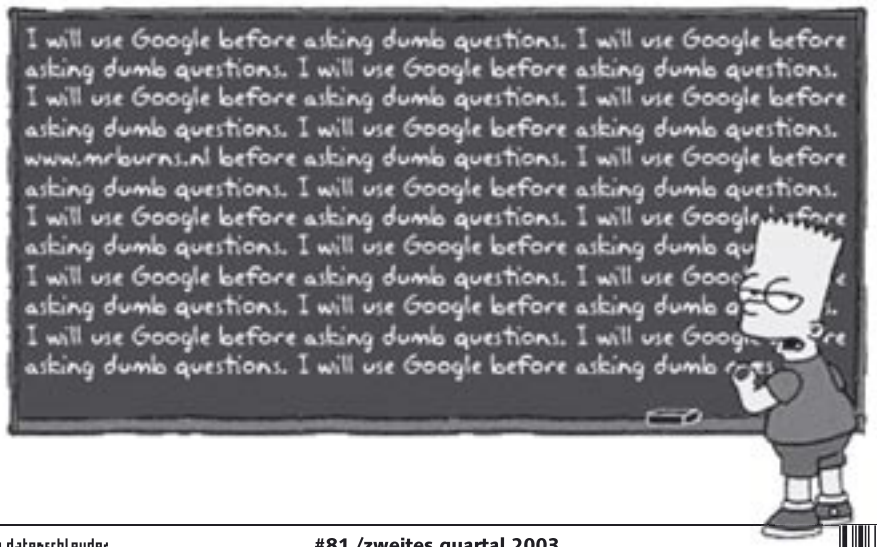
Alles in allem lässt das neue Jugendschutzgesetz viele Fragen offen. Ob die Gesetzesveränderung in punkto Medien tatsächlich ihren Teil dazu beiträgt, dass "Kinder und Jugendliche ... effektiv vor negativen Einflüssen geschützt werden", wie es Bundesfamilienministerin Renate Schmidt meint, erscheint zumindest fraglich.

Übrigens ein Tipp an die Eltern: Wenn Ihr sechzehnjährige(r) Sohn/Tochter plötzlich den Wunsch äußert zu heiraten, glauben Sie diesen angeblich romantischen Motiven nicht: Er/Sie will bloß legal an Spiele "ab 18" kommen, denn die genannten Beschränkungen greifen laut Gesetz bei verheirateten Jugendlichen nicht...

[1] *http://www.kindex.de/html/material/juschg.html*

[2] *http://www.usk.de/*

[3] *http://bpjs.bmfsfj.de/*



Verbindungsdatenspeicherung bei pauschaler Abrechnung

von Sebastian <sebastian@ccc.de>

Datenvermeidung ist einer der Grundsätze der Datenschutzgesetze in Deutschland. So dürfen Daten grundsätzlich nicht erhoben werden, wenn kein konkreter und erlaubter Zweck damit verfolgt wird wie beispielsweise die Abrechnung von Nutzungsentgelten oder die Durchführung und Sicherstellung von Diensten.

Doch selbst in solchen Fällen dürfen die Daten nur solange wie unbedingt notwendig gespeichert werden, danach müssen sie gelöscht werden. Verbindungsdaten, die für die Erstellung der Rechnung notwendig sind (z.B. Einzelverbindungsnachweis), dürfen unter Streichung der letzten drei Ziffern der Zielrufnummer zu Beweiszwecken gespeichert werden. Sie müssen aber spätestens sechs Monate nach Versendung der Rechnung gelöscht werden (vgl. § 7 Abs. 3 TDSV vom 18.12.2000) [1] , alle anderen Daten spätestens einen Tag nach Beendigung der Verbindung (vgl. § 6 Abs. 2 TDSV). Der Kunde kann bei den Abrechnungsdaten auch eine vollständige Speicherung oder eine sofortige Löschung bei Rechnungsversand verlangen (vgl. § 7 Abs. 3 TDSV).

Seitdem DSL-Anschlüsse in Deutschland verfügbar sind, ist aber auch ein neues, pauschales Abrechnungsmodell in Mode gekommen. Bei solchen sog. Flatrates bezahlt der Kunde eine monatliche Pauschale für die Nutzung der Internetanbindung. Damit sind die Verbindungsdaten - wann ein Kunde wie lange im Internet war, welche IP-Adresse seinem Rechner zugewiesen war und wie viele Daten er dabei übertragen hat - nicht mehr abrechnungsrelevant und dürfen somit nicht mehr erhoben werden. T-Online hat dies aber trotzdem gemacht [2] , was zu Beschwerden von Kunden führte.

Das Regierungspräsidium Darmstadt musste nun als zuständige Datenschutz-Aufsichtsbehörde entscheiden, ob diese von T-Online praktizierte Verbindungsdatenspeicherung bei Flatrates zulässig ist. Besonders umstritten war und ist die Frage, ob auch die IP-Adresse, die dem Kunden während der Verbindung zugewiesen wird, gespeichert werden darf, da diese zum Nachweis der Einwahl nicht notwendig ist. Am 14.01.2003 wurde die Entscheidung des Regierungspräsidiums Darmstadt bekannt gegeben, nach der die Speicherung zulässig sei. Sie gilt für alle Internetprovider, die ihren Sitz in Hessen haben. Allerdings wurde die Entscheidung sofort kritisiert, da die Verbindungsdaten für Abrechnungszwecke bei Flatrates schlichtweg nicht notwendig sind, wie eingangs erläutert [3] wurde. So argumentiert das Regierungspräsidium Darmstadt auch damit, dass die Speicherung der IP-Adresse notwendig sei, um eine vom Kunden behauptete Leitungsstörung widerlegen zu können. Weiterhin könne nur durch Speicherung der IP-Adresse nachträglich eine Identifizierung von Angreifern auf Datenverarbeitungssysteme erfolgen. Dies scheint der Hauptgrund für die IP-Datenspeicherung zu sein, allerdings sehen die Gesetze eine solche Datenspeicherung "auf Vorrat" - also ohne Anfangsverdacht oder konkreten Anlass - nicht vor. Auch wenn eine Einführung der Verbindungsdatenspeicherung "auf Vorrat" derzeit von der EU geplant wird [4] , warnen Bürgerrechtler vor einer solchen Umkehr der Unschuldsvermutung und sehen eine konkrete Gefährdung der Rechte auf Privatsphäre und Meinungsfreiheit. Durch das ständige Mitprotokollieren der Tätigkeiten der Menschen könnten diese in ihrem Denken und Handeln beeinflusst werden. Aber genau das darf in einer freiheitlichen Demokratie nicht geschehen.

Die für Schleswig-Holstein [5] , Hamburg [6] und Niedersachsen [7] zuständigen Datenschutz-Aufsichtsbehörden erklärten als Reaktion auf die Entscheidung des Regierungspräsidiums Darmstadt ihre abweichende Auffassung, nach der eine Speicherung von Verbindungsdaten bei Flatrates grundsätzlich nicht zulässig ist. Das Unabhängige Landeszentrum für Datenschutz in Schleswig-Holstein erklärte, dass eine Speicherung der IP-Adressen nicht einmal zu Beweiszwecken zulässig [8] sei. Dabei dürfe eine Speicherung der IP-Adresse zum Schutz vor Missbrauch auch nur in konkret dokumentierten Missbrauchssituationen erfolgen und keinesfalls rein "vorsorglich".

Für den Verbraucher heißt dies konkret, dass je nach Bundesland, in dem der Provider seinen Hauptsitz hat, die Speicherung von Verbindungsdaten unterschiedlich gehandhabt wird - obwohl die anzuwendenden Gesetze bundesweit gelten. Die Datenschleuder hat daher Provider, die Flatrates anbieten, angeschrieben und danach gefragt, welche Daten gespeichert werden. Leider hat nur ein sehr kleiner Teil der angeschriebenen Anbieter geantwortet. Ein Kunde hat aber in jedem Fall das Recht, Auskunft von seinem Provider zu verlangen. Mit unserer Aufstellung (Stand 9.03.2003) wollen wir eine weitere Entscheidungshilfe bei der Wahl des Flatrate-Anbieters geben.

Anbieter	Kontakt	Produkt	Verbindungsdaten-speicherung	Anmerkungen
1&1 und Schlund + Partner	56410 Montabaur Tel. 02602-96-0 www.1und1.de	Volumen- und Zeittarife	bei Volumentarifen: eingehendes und ausgehendes Volumen bei Zeittarifen: Beginn und Ende der Verbindung nach Datum und Uhrzeit	Nutzung des Leitungsnetzes der Telekom Speicherdauer: sechs Monate nach Rechnungsversand, bei Einwendungen gegen die Rechnung solange, bis diese abschließend geklärt sind
callando	65187 Wiesbaden Tel. 0611-20581-0 www.callando.de	DSL flat	nein	
ecore	96103 Hallstadt Tel. 0951-93227-0 www.ecore.net	SDSL flat	nein	feste IP wird bei RIPE auf den Kunden selbst registriert
GMX	80992 München Tel. 089-14339-0 www.gmx.de	Volumentarif	eingehendes und ausgehendes Volumen	Nutzung des Leitungsnetzes der Telekom Speicherdauer: sechs Monate nach Rechnungsversand, bei Einwendungen gegen die Rechnung solange, bis diese abschließend geklärt sind
m@crolS	97236 Randersacker Tel. 0931-20089-0 www.macrois.de	Standleitungen auf digitaler oder SDSL-Basis	nur Datenvolumen	Speicherung der Summe der übertragenen Daten zu den einzelnen IP-Adressen zu „Accountingzwecken“ über ein Jahr
osnatel	49074 Osnabrück Tel. 0541-60006-0 www.osnatel.de	Flatrate	auf Wunsch: - Einwahlzeit und -dauer - die zugewiesene IP-Adresse - übertragenes Datenvolumen - die Anschlusskennung (Rufnummer, ATM-Interface)	Speicherung bei ausdrücklichem Wunsch des Kunden, höchstens jedoch sechs Monate (dauerhafte Speicherung) bzw. höchstens einen Monat (Löschung nach Rechnungsversand)
tlink	22143 Hamburg Tel. 040-648680-0 www.t-link.de	tlink DSL flat	nein	Speicherung von Benutzername und Kennwort sowie abrechnungsrelevante Daten (Bankverbindung, Rechnungsadresse, Buchhaltung) Prüfung durch den Hamburg- ischen atenschutzbeauftragten im Juli 2002
T-Online	64211 Darmstadt Tel. 06151-680-0 www.t-online.de	T-DSL flat	- Anschlusskennung (T-Online) - T-Online-Nummer und Mitbenutzer-Suffix - Beginn (Uhrzeit) - Ende (Uhrzeit) - Zähler (in Sekunden) - Vermittlungsstelle, Ort - Dynamische IP-Adresse der Session - Art des Zugangs (hier T-DSL) - In Anspruch genommene kostenpflichtige Dienste	Speicherdauer: 80 Tage nach Rechnungsversand. In Einzelfällen (z.B. bei Einwänden gegen Rechnung) entsprechend länger „Die Speicherung von IP-Adressen ist über eine Abrechnung hinaus auch als Bestandteil unserer Maßnahmen zum Zwecke der Datensicherheit erforderlich. Insbesondere ergibt sich hierdurch eine Möglichkeit zur Recherche in Missbrauchsfällen (z.B. Hacking, Virenversand, strafrechtliche Verfahren).“
NGI	22767 Hamburg Tel. 01805-001344 www.ngi.de	k.A.	nein	nur Speicherung von Anschrift, Telefonnummer, Bankverbindung

[1] *http://www.netlaw.de/gesetze/tdsv.htm*

[2] *http://www.ccc.de/updates/2002/t-online-nutzungsdaten*

[3] *http://www.heise.de/ct/aktuell/data/hob-14.01.03-000/*

[4] *http://ds.ccc.de/077/vorratsspeicherung*

[5] *http://www.ccc.de/updates/2003/dataretention*

[6] *http://www.heise.de/newsticker/data/hod-28.01.03-000*

[7] *http://www.heise.de/newsticker/data/hod-21.01.03-000*

[8] *http://www.datenschutzzentrum.de/material/themen/presse/ipspeich.htm*

Honeypots

von Fabian Bieker <fb@kassel.ccc.de>

Der sportlich intressesierte Nerd begibt sich heutzutage nicht mehr auf die Jagd nach offenen wLANs - nein, wir versuchen etwas viel Interessanteres zu "fangen": Cracker, Kreditkartenbetrüger, Würmer, Spammer. Manchmal landen auch ScriptKiddies im Honigtopf.

Was ist ein Honeypot?

Ein Honeypot ist ein Gerät (meist ein Computer), dessen Zweck darin besteht, gescannt und angegriffen zu werden, daher auch der Name. Sinn des Ganzen ist es entweder, seine "echten" Netze zu schützen, oder man möchte etwas über die Motivation, Techniken und Werkzeuge der Angreifer lernen. Ein Honeynet ist ein Netz, was aus mehreren Honeypots und einigen Kontroll-Rechneren besteht.

Wer einen Admin-Job hat, kann so einiges über die Gefahren lernen, die im großen, "bösen" Internet so lauern. Man bekommt auch ein ganz gutes Gefühl dafür, wie sich Angriffe bemerkbar machen. Für jeden Computerforensiker bieten sich nach einem erfolgreichen Eindringen in den Honeypot, jede Menge Möglichkeiten, seine Fähkeiten zu verbessern und zu testen. Natürlich kann man einen Honeypot auch als Crackerfahrschule betreiben und sich zeigen lassen, wie man System XYZ doch auf bekommt. Manchmal stellt ein Honeynet eine gute Möglichkeit dar, dem Chef zu demonstrieren, dass Sicherheit wichtig ist. Es wurden auch schon Spammer und Kreditkartenbetrüger in einem Honeynet gefangen.

Honeypots gibt es in verschieden Interaktionsgraden, von der mehr oder minder guten Simulation bestimmter Dienste, bis hin zu kompletten Netzen.

Honeyd, von Niels Provos, ist ein Opensource lowinteraction Honeypot, der in der Lage ist mehrere Netzwerke mit Routing Topologie, Latenz und Paket-Verlusten zu simulieren. Er schafft es sogar nmap-OS-fingerprints zu fälschen. Auf der anderen Seite des Spektrums, kann man mit alten Rechnern, ein kleines Netzwerk aufbauen und eine alte Linux-Distribution oder Windoof installieren. In so einem Netzwerk bieten sich dem Angreifer natürlich ganz andere Möglichkeiten.

honeyd

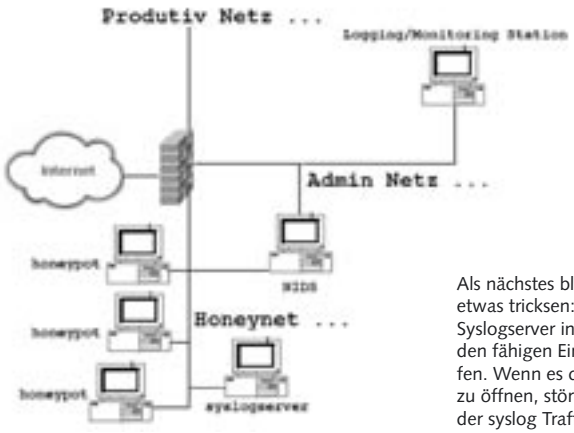
Honeyd [1] läuft als Userspace-Daemon auf den meisten Unixen, er benutzt libpcap, libevent und libdumbnet um für jeden virtuellen Honeypot einen eignen TCP/IP Stack zu simulieren (so werden auch die TCP/IP-OS-Fingerprints mit simuliert). Honeyd simuliert ein oder mehrere Netzwerke aus virtuellen Honeypots, für die Simulation der einzelnen Dienste verwendet er externe Scripte. Man kann sich honeyd in etwa wie einen inetd für Honeynets vorstellen. Es gibt bereits einige Scripte, die z.B. komplette IIS/Apache Webserver simulieren. Wenn man nun diese Scripte in Logdateien schreiben lässt, werden alle Einbruchsversuche protokolliert. Wirklich Eindringen kann der Angreifer (hoffentlich) nicht, da die Scripte nur simulieren, man kann natürlich bis zu einem gewissen Grad, die Bugs einfach mit simulieren. Wenn man seinem Honeyd mit systrace, rsbac, SELinux oder VServer etwas einsperrt, hat man ohne großes Risiko recht interessante Logfiles. Nach der Zeit wird das aber langweilig, also auf zu den interessanteren Dingen:

Honeynet GenI

Bei einem Honeynet der ersten Generation (GenI) stellt man einen*gut gesicherten* Firewall/Gateway vor ein "echtes" Netzwerk, das Honeynet. In dieses Netzwerk sollen die Leute dann einbrechen und wir können sie dabei beobachten. Um zu verhindern, dass jemand Schaden in externen Netzen anrichten, erlauben wir dem Honeynet nur 5 ausgehende Verbindungen am Tag. Da in dem Honeynet ja niemand arbeitet, muss man nur noch DNS, NTP etc. freischalten. Alle anderen ausgehenden Verbindungen sind ein Zeichen, dass der Honeypot gecracked wurde, daher lasse ich mir dies per automatischer EMail mitteilen. Das Network Intrusion System (NIDS) überwacht und log*gt allen* Netzwerkverker. Ich benutze zur Zeit snort, als NIDS. Auf den syslogserver gehe ich später ein. Baitn'switch bietet die Möglichkeit Angreifer auf das Honeynet umzuleiten, um die produktiven Netze zu schützen.

Honeynet GenII

Die zweite Generation der Honeynets benutzen anstatt einem Gateway eine Bridge mit Paketfilterfunktinalität



und snort_inline [2] . Die Bridge verbindet das Honeynet mit dem Rest der Welt (auch dem eventuellen Produktiv-Netz), dies hat den Vorteil, dass die Bridge nicht so leicht zu entdecken ist (z.B. mit traceroute).

Snort_inline ist ein Patch für das NIDS snort, der es snort erlaubt Pakete zu manipulieren, sie wegzuwerfen oder die Verbindung zu resetten. Implementiert ist dieses Feature durch das netfilter Userspace Queue von Linux, zur Zeit gibt es noch keinen Port für andere Unixe. Mit Snort_inline verhindert man viele Attacken des Honeynets auf externe Netze und somit kann man etwas mehr ausgehende Verbindungen erlauben: 10-20 pro Tag ist ein guter Wert. Ausserdem macht es Spass Shellcodes/NOPSlides geben 0-Bytes auszutauschen...

Data Control & Data Capture

Wie gesagt, es gilt zu verhindern, dass man mit dem Honeynet Schaden anrichten kann. Daher das Connectionlimit, eine schmalbandige Anbindung und evtl. snort_inline. Desweiteren wollen wir natürlich genaustes wissen, was der Angreifer auf unserem System so treibt. Snort ist in der Lage den Netzwerkverkehr sowohl als Sessionlogs oder auch im tcpdump formart aufzuzeichnen. Die Snort-Sessionlogs sind im Prinzip ASCII-Zeichen Dumps der einzelnen Verbindungen.

Die meisten Rootkit/Backdoors verwenden mittlerweile verschlüsselte Kommunikationskannäle, so dass uns ein Sniffer nicht weiter hilft. Da ich aber schon gerne weiss, was die Leute so auf meinem System treiben, brauchen wir noch einen TTY-Logger. Der Angreifer soll diesen nicht entdecken und auch nicht durch ein RootKit austauschen, daher finde ich sebek sehr chick. Sebek ist ein Linux Loadable Kernel Modul (LKM), das die Eingaben auf allen (Pseudo)TTYs per UDP an einen Rechner sendet. Es gibt mittlerweile auch einen OpenBSD Port. Sebek verbiegt die RawSocket Implementierung des Kernels so, dass man Pakete von bestimmten AbsenderMAC-Adressen nicht mehr sieht. Das heißt für alle Rechner mit sebek LKM ist der sebek Traffic nicht sichtbar, auch nicht im promiscuous mode (beim sniffen). Ansonsten gibt es noch einen Patch für die Bash, der die Bash-History ins Netzwerk loggt, leider für jeden sichtbar. Sebek funktioniert nur ab einem 2.4er Kernel, daher hat man u.U. keine andere Wahl. Für Solaris bietet sich RemoteBSM an.

Als nächstes bleibt noch syslog. Mit syslog kann man etwas tricksen: Wir stellen einen (besser gesicherten) Syslogserver in unser Honeynet. Damit zwingen wir den fähigen Einbrecher, tiefer in die Trickkiste zu greifen. Wenn es den Angreifer gelingt den Syslogserver zu öffnen, stört dies nicht weiter, da von snort auch der syslog Traffic mit gesnifft wird :-) . Aus diesem und anderen Gründen empfiehlt es sich Hubs in Honeynets zu verwenden.

Tripwire, Process Accounting oder chkrootkit sind ebenfalls immer sehr hilfreich. Die Daten eines gecrackten Systems sichert man am besten, indem man eine KNOPPIX-CD bootet und dann die Partionen mit dd | nc auf einen anderen Rechner überträgt. Eine Sicherung der Partionsimages auf CD, DVD oder andere readonly-Medien ist ratsam.

Zur intensiven Analyse des Dateisystems ist TCT gut geeignet. Leider kommt es zur Zeit nur mit ext2/3 und UFS zurecht. Auf Computerforensik will ich aus Platzgründen nicht weiter eingehen, das Honeynet Project hat aber einige gute Papers [3] hierzu veröffentlicht.

Das Wichtige ist, dass man mehrere Schichten Logging/Data Control hat, wenn eine Schicht versagt, steht man nicht vor einer Katastrophe, denn irgendwas geht immer schief. Des weiteren gilt das Motto: "Um so mehr Daten ich habe, umso leichter wird die Analyse." Ein Honeynet produziert, im Gegensatz zu einem produktiven System, recht wenig Traffic, ca 5-30MB jeden Tag. Es ist einfach jede Verbindung zum Honeynet suspekt. Wenn ein honeypot eine ausgehende Verbindung aufbaut, ist er wohl aufgemacht worden, da ja niemand auf dem Honeypot regulär arbeitet.

Mein Setup

Ich betreibe z.Z. ein Honeynet mit RH8.0, leider habe ich nur eine statische IP Adresse zur Verfügung, aber wenigstens ist der RH8.0 Honeypot primary DNS für eine Domain. In dem Netz befinden sich noch ein Cisco Router und ein paar andere Dinge, leider hat nur die RedHat Kiste eine offizielle IP Adresse. RedHat8.0 läuft jetzt seit ca. 7 Wochen und ist bis jetzt noch nicht geöffnet wurden, was mich etwas trauig macht. Davor hatte ich einen SuSE7.3 honeypot, der ist zweimal (immer Sonntags) von Freizeit ScriptKiddies durch den sambal exploit geöffnet wurden. Dies

ist keine Wertung der Distris an sich, es zeigt nur, dass man sein System aktuell halten will. Als nächstes werde ich mal etwas anderes als Linux versuchen. Windows Honeypots werde ich mir ersparen. IMHO ziehen IIS, Exchange und Konsorten nur ScriptKiddies an.

Gefahren

Ein Honeypot ist kein Produkt, das man im Laden kauft, per Plugn'Play anschließt und dann in die Ecke stellt. Ein Honeypot sollte am besten von mindestens 2 Leuten 24x7 im Auge behalten. Man sollte sich langsam an die Thematik heran tasten: Erstmal den honeyd testen, viel lesen und die Mailinglisten abonnieren.

Auf der Honeynet Project Webseite [4] finden sich die sogenannte " Scan of the Month Challenges [5] " des Honeypot Projects. Das sind z.B. tcpdump logs von einem Angriff auf einen Honeypot, die zu analysieren sind, um herauszubekommen, was genau dort vorgefallen ist. Erst wenn man in der Lage ist den Großteil dieser Aufgaben zu meistern, sollte man sich an ein "richtiges" Honeynet wagen. Andernfalls ist es sinnlos, da ihr nicht in der Lage sein werdet, die anfallenden Daten auszuwerten.

Denn bei allen Sicherheitsmaßnahmen sollte man nicht vergessen, dass man mit dem Feuer spielt! Ich will der Polizei nicht erklären müssen, warum mein Rechner gerade die BSI Seite exploited hat. Die haben bestimmt richtig viel Verständniss für euren Wissensdurst und Honeynet Geschichten.

Um ein Honeynet sinnvoll zu betreiben, braucht man statische IP Adressen. Mit honeyd kann man auch etwas Spass ohne statische IP Adressen haben, aber selbst das ist nicht wirklich lohnend. Ich selbst habe es 3 Wochen lang mit einer Dialup IP Adressen versucht, leider erfolglos. Man kann sich aber über IPSEC/OpenVPN eine statische IP Adresse nach hause tunneln lassen, wenn man nur eine Einwähl-Internetverbindung mit dynamischer Adresse hat.

Die rechtliche Situation nicht ganz einfach, vor allem in den USA, mehr dazu im Internet:

- http://asia.cnet.com/itmanager/netadmin/0,39006400,39133822,00.htm [6]
- http://cert.uni-stuttgart.de/archive/honeypots/2002/09/msg00104.html [7]

Ich würde gerne dem Honeynet Project als deutsches Honeynet beitreten, dazu brauche ich aber noch ein paar Leute die mitmachen. Bei Interesse einfach mir mailen [8] .

Ansonsten bleibt noch zu sagen: Wenn ihr das nächste mal auf einem Rechner seid, wo ihr eigentlich nicht sein solltet, und nach der 12. ausgehenden Connection Schluss ist, schaue ich euch wohl gerade auf die Finger (-; .

Mailinglisten

- honeypots@secfocus: https://www.securityfocus.com/archive/119 [9]
- forensics@secfocus: https://www.securityfocus.com/archive/104 [10]
- ids@secfocus: https://www.securityfocus.com/archive/96 [11]

Bücher

- "Know Your Enemy", Honeypot Project, Addison-Wesley ISBN: 0-201-74613-1
- " Honeypots - Tracking Hackers", Lance Spitzner, Addison-Wesley ISBN: 0321108957

Links

- Honeynet Project http://project.honeynet.org/ [12]
- CCC Kassel Honeynet Projekt: https://kassel.ccc.de/honey/ [13]
- Snort: http://www.snort.org/ [14]
- Honeynet Programme u. Werkzeuge: http://project.honeynet.org/papers/honeynet/tools/ [15]

[1] *http://www.citi.umich.edu/u/provos/honeyd/*

[2] *http://sourceforge.net/projects/snort-inline/*

[3] *http://project.honeynet.org/papers/*

[4] *http://project.honeynet.org/*

[5] *http://project.honeynet.org/misc/chall.html*

[6] *http://asia.cnet.com/itmanager/netadmin/0,39006400,39133822,00.htm*

[7] *http://cert.uni-stuttgart.de/archive/honeypots/2002/09/msg00104.html*

[8] *mailto:fb@kassel.ccc.de*

[9] *https://www.securityfocus.com/archive/119*

[10] *https://www.securityfocus.com/archive/104*

[11] *https://www.securityfocus.com/archive/96*

[12] *http://project.honeynet.org/*

[13] *https://kassel.ccc.de/honey/*

[14] *http://www.snort.org/*

[15] *http://project.honeynet.org/papers/honeynet/tools/*

Bestellungen, Mitgliedsanträge und Adressänderungen bitte senden an:

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

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

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

Die Kohle

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

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

Name: _____

Straße / Postfach: _____

PLZ, Ort _____

Tel.* / Fax* _____

E-Mail: _____

Ort, Datum: _____

Unterschrift _____

*freiwillig

http://www.ccc.de/camp/

In fairy dust we trust!