die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

Bankenskandale
Bluetooth Security
Der Funker im Forst
Wohlfühllicht im Selbstbau
Standardisierte Umgehungs-techniken

Photo von cefalon. Bild eines fnordlichts in Aktion.

ISSN 0930-1054 • 2005
Diesmal inflationsbereinigte €2,50
Postvertriebsstück C11301F

#88

Erfa-Kreise / Chaostreffs

Bielefeld im AJZ, Heeper Str. 132, mittwochs ab 20 Uhr *http://bielefeld.ccc.de/ :: info@bielefeld.ccc.de*
Berlin, CCCB e.V. (Club Discordia) Marienstr. 11, (Briefe: CCCB, Postfach 64 02 36, D-10048 Berlin),
donnerstags ab 17 Uhr *http://berlin.ccc.de/ :: mail@berlin.ccc.de*
Düsseldorf, CCCD/Chaosdorf e.V. Fürstenwall 232,
dienstags ab 19 Uhr *http://duesseldorf.ccc.de/ :: mail@duesseldorf.ccc.de*
Erlangen/Nürnberg/Fürth, BitsnBugs e.V. "E-Werk", Fuchsenwiese 1, Gruppenraum 5
dienstags ab 19 Uhr *http://erlangen.ccc.de/ :: mail@erlangen.ccc.de*
Hamburg (die Dezentrale) Lokstedter Weg 72
2. bis 5. Dienstag im Monat ab etwa 20 Uhr *http://hamburg.ccc.de/ :: mail@hamburg.ccc.de*
Hannover, Leitstelle511 Kulturcafé, Schaufelder Str. 30, Hannover
2. Mittwoch im Monat ab 20 Uhr *https://hannover.ccc.de/*
Karlsruhe, Entropia e.V. Gewerbehof, Steinstr. 23
sonntags ab 19:30 Uhr *http://www.entropia.de/ :: info@entropia.de*
Kassel Uni Kassel, Wilhelmshöher Allee 71-73 (Ing.-Schule)
1. Mittwoch im Monat ab 18 Uhr *http://kassel.ccc.de/*
Köln, Chaos Computer Club Cologne (C4) e.V. Chaoslabor, Vogelsanger Str. 286
Letzter Donnerstag im Monat ab 19:30 Uhr *http://koeln.ccc.de/ :: mail@koeln.ccc.de*
München, muCCC e.V. Kellerräume in der Blutenburgstr. 17
2. Dienstag im Monat ab 19:30 Uhr *http://www.muc.ccc.de/*
Ulm Café Einstein an der Uni Ulm, montags ab 19:30 Uhr *http://ulm.ccc.de/ :: mail@ulm.ccc.de*
Wien, chaosnahe gruppe wien Kaeuzchen, 1070 Wien, Gardegasse (Ecke Neustiftgasse)
Alle zwei Wochen, Termine auf Webseite *http://www.cngw.org/*

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, Aargau, Bad Waldsee, Basel, Bochum, Brugg, Darmstadt, Dortmund, Dresden, Frankfurt am Main, Freiburg im Breisgau, Gießen/Marburg, Hanau, Heidelberg, Ilmenau, Kiel, Mainz, Mülheim an der Ruhr, Münster/Osnabrück, Offenbach am Main, Paderborn, Regensburg, Stuttgart, Trier, Weimar, Wetzlar, Wuppertal, Würzburg.

Friends & Family

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

Die Datenschleuder Nr. 88

Herausgeber (Abos, Adressen, Verwaltungstechnisches etc.)
Chaos Computer Club e.V., Lokstedter Weg 72,
20251 Hamburg, Fon: *+49.40.401801-0,*
Fax: *+49.40.401801-41, <office@ccc.de>* Fingerprint*:*
1211 3D03 873F 9245 8A71 98B9 FE78 B31D E515 E06F

Redaktion (Artikel, Leserbriefe, Inhaltliches, etc.)
Redaktion Datenschleuder, Pf 64 02 36, 10048 Berlin,
Fon: +49.30.28097470, *<ds@ccc.de>* Fingerprint:
03C9 70E9 AE5C 8BA7 42DD C66F 1B1E 296C CA45 BA04

Druck
Pinguindruck Berlin, *http://pinguindruck.de/*

ViSdP und Produktion
Tom Lazar, *<tom@tomster.org>*

Layout
Dirk Engling, Antenne Springborn

Chefredaktion
Dirk Engling <erdgeist> und Tom Lazar <tomster>

Redaktion dieser Ausgabe
Alexander Neumann, Bastian Ballmann, TabascoEye, Frank Rieger, starbug, Johannes vom Fluss, Julia Lüning, Martin Haase, Nitram, Volker Birk, padeluun

Sehr geehrter Datenschleuderkunde. Bitte begeben Sie sich auf *http://datenschleuder.de.vu/* und geben Sie ihre Mitgliedsnummer, Adresse und DNA-Probe zum Abgleich mit unseren Daten ein.

Zu plump? Zugegeben, die Möglichkeiten des Zugriffs auf unsere Brieftaschen verfeinern sich in letzter Zeit von sehr abstrakten Szenarien hin zu institutsionsunterstützter Einladung zum Nachsehen.

Ging es anfangs noch um das Ergaunern von eBay-Zugangsdaten, mit dem Ziel, über den Umweg der Auktionen Geld umzuleiten, bekamen wir es danach mit Phishing-Mails zu tun. Diese bedurften allerdings der aktiven Kooperation des Geschädigten. In dieser Ausgabe nun widmen wir uns der lange unterschätzten Gefahr elektronischer Lastschriftverfahren (siehe Seite 9) und, weil es ja nach T-OBSOC einfach so kommen **mußte**, endlich einem Direktzugriff auf das Konto durch das beliebte Die-Kundennummer-in-der-Adresszeile-Ersetzen-Spiel (Seite 6).

Daß eine Vereinfachung von Transaktionen nicht immer zu Lasten des Kunden gehen muß, beweist der Erfahrungsbericht eines Microsoft-Homeshoppers (Seite 29). Einmal Kunde läßt einen die sprichwörtliche Kulanz dieser Firma nie wieder ohne Maus zu Haus. Dazu ist ihnen kein Defekt zu unplausibel – und wenn es ein gekrickticktes Bluetooth-Kabel ist.

Letzteres ist – wenn auch im übertragenen Sinne – **wirklich** wahr geworden. Die durchwegs unterdurchschnittlichen Implementationen der drahtlosen Nahfunktechnologie eröffnen dem Sportsfreund ungeahnte Einblicke: Das Ziel ist hierbei nur knapp neben der Brieftasche zu orten und kann, clever ferngesteuert, deutlich mehr Kosten und Ärger verursachen. Ein Abriß der Entwicklungen 2005 und selbstgebastelte Fernerkundungssonden gibt es auf Seite 18.

Selbstgebastelte Nahbeleuchtungssonnen (wie schon auf dem Titel zu bestaunen) in den entspanntesten Farben waren, neben der Nachwuchswerbung, Ziel der Platinenlötkumpel im Erfakreis Köln. Auf der U23 wurde ein schönes buntes Projekt verfeinert; die Protagonisten berichten auf Seite 26.

Derart herausgefordert ließ sich auch der Berliner Club nicht lumpen. Da dort **alles** ein paar Nummern größer ist, errichtete man auf der staatlich geförderten Politik-Erweckungsparty "Berlin 05" eigens einen Tempel zur diskordischen Indoktrination tausender engagierter Jugendlicher. Auf der Seite 33 beschreibt nun eine der Organisatorinnen ihren Blick auf die Veranstaltung.

Man kann diese natürlich auch als Generalprobe für den noch schöneren Chaos Communication Congress ansehen. Im Gegensatz zu den letzten Jahren hat man eine Ausrede mehr, Omi zwischen den Tagen nicht besuchen zu müssen: Der Congress dauert nun vier Tage, geht vom 27. bis zum 30. Dezember und findet traditionell im Herzen Berlins statt: im bcc am Alexanderplatz. Besser informiert unter *https://events.ccc.de/congress/2005*.

Wir sehen uns dort. *<starbug & erdgeist>*

Inhalt

Manche Mails will man einfach nur abdrucken...

Sehr geehrte Damen und Herren, ich lass auf der Seite 292 (CCC: 100100100) meines Kochbuches. Dort war ein Rezept für Apfelkuchen mit Griessguss.

Ich möchte jetzt TIM vom MIT per E-Mail besuchen, ihm einen roten Apfel mit 5 Stübchen zukommen lassen (Seelenbehafteter Menschentest) und ihn mit einem besonderen Gruß grüssen. Können Sie mir bitte sagen, ob ein Tim bei Ihnen per E-Mail erreichbar ist? Vielen Dank.

P.S.: Hören Sie Think?Place, im Gästebuch las ich eine interessante Nachricht von einem User! Ich bin beunruhigt, ich sehe es stark flimmern in der Luft...

Und nein, das ist kein Einzelfall:

Hiermit zeige ich XXX meinen ehemaligen Mittbewohner an. Er hatt angeblich Kinderpornographie und Tierpornographie betrieben. Dieser Verdacht legt sich nahe, da er in der Kneipe AXXX vor anderen und mir eine diesbezuegliche aussage zugegeben hatt das er sich fuer solche dinge interresiere. Seine ehemale anschrift: XXXstr. YY

Seit einiger zeit werde ich im kopf mit kipos staendig bombardiert. dies passierte nachdem ich einen stich im kopf spuerte wo mich jemand umarmt hatt. So vermute ich das mir ein rfid implantiert wurde. ich habe schon mit dem spiegel diesbezueglich gesprochen. und dem ccc eine mail geschrieben. bitte setzen sie sich diesbezueglich mit mir in verbindung. Joerg XXX (AusweisNr XXXXXXXX, Telefon und Aufenthaltsort)

Die Rutschstange hinab ins Hackmobil?

brauche dringend Hilfe hier in FFM dieses WE (Sa-So, 8.-9.10.), bitte zurückmailen oder anrufen, *069-XXXXXXX oder 0172-XXXXX* <XXXconsul>

im Notfall die 110 wählen... <FrankRo>

PenTest

Sehr geehrte Damen und Herren, wir suchen für eine Informations-Veranstaltung am 17. März 2005 in Gelsenkirchen eine Person, die in einer Live-Vorführung deutlich macht, wie wichtig und sinnvoll der Einsatz einer Firewall ist. <*Udo.XXX@XXX-net.de*>

Der Standpunkt des CCC ist eindeutig:
Der Chaos Computer Club führt keine Penetration-Tests und Vorführungen aus. <*julius*>

Nun mag diese Antwort nicht kategorisch genug gewesen sein, denn wenig später:

vielen Dank für Ihre schnelle Antwort. In unserer Informations-Veranstaltung soll kein Penetration-Test durchgeführt werden. Es geht um eine praktische Demo, bei der ein Entscheider verständlich erkennen kann, warum die Benutzung einer (beliebigen guten) Firewall wichtig ist. Es handelt sich nicht um eine Vertriebsveranstaltung.

Wir müssen also weiter ausholen:
Wie stellen Sie sich das vor? Etwa so?:

Ein junger Mann mit Kapuzenpulli, Cap tief im Gesicht, Zigarette im Mund und angeklebtem Bart tritt vor das Auditorium, besetzt mit "Entscheidern", und murmelt unverständliche Sätze. Er präsentiert eine schwarze Kiste, auf der ein Schild mit der Aufschrift "Server" klebt. Auf einem angeschlossenen Monitor erscheinen bunte Symbole. Der Hacker packt seinen Laptop aus und tippt mit hoher Geschwindigkeit wilde Zeichenfolgen in die Tastatur. Dann rauscht es etwas, Kunstnebel steigt auf. Die bunten Symbole auf dem Server verschwinden – statt dessen erscheint ein Totenkopf. Ein Raunen geht durch die Menge. Der Moderator verkündet mit ernster Mine, dass dies mit einer Firewall nicht passiert wäre.

Die Entscheider notieren sich das Wort "Firewall" auf ihrem Einkaufszettel, stopfen sich noch einen Satz Mousepads in ihre Jute-Tasche und verlassen den Raum mit dem Gefühl, heute etwas über IT-Sicherheit erfahren zu haben. <*julius*>

Zum Titelbild der Datenschleuder 086

Was mich beschäftigt: Inwiefern begreift sich der CCC denn als politischer Verein? Bzw. kommt die aktuelle Ausgabe der Datenschleuder mit Absicht autonom daher? Irgendwie hinterlässt das Cover beim Betrachten einen fahlen Beigeschmack wenn man bedenkt, dass der dort kritisch zitierte Generalbundesanwalt Buback von der RAF erschossen wurde.

Ich war generell verwundert, dass der CCC auf der Datenschleuder mit Ausschnitten sozialistischer Zeitungen aufwartet; die Interessen, die er vertritt, sind doch wohl eher von liberaler Natur?! *<Peter>*

Hallo Peter, der Chaos Computer Club ist auf jeden Fall auch ein politischer Verein – jedoch kein parteipolitischer. Die Einführung von biometrischen Pässen (und die damit zwangsweise stattfindende erkennungsdienstliche Behandlung der Bevölkerung) hat eindeutig eine stark politische Komponente – niemand wird diese Maßnahme als einen rein technischen Vorgang einstufen. Das Zitat von Buback ist deswegen hochaktuell, weil genau 30 Jahre später sein Wunschtraum in Erfüllung gegangen ist. Daher fanden wir es das Titelbild wert.

Die Diskussion darüber, wieviel Politik für den Club "gut" ist, führen wir übrigens recht häufig und auch sehr lebhaft. **Die** *Antwort darauf gibt es nicht – aber wir wollen uns ganz deutlich von irgendwelchen Computerbastlern abgrenzen, die sich damit beschäftigen, welches die gerade schnellste Grafikkarte und der billigste Internetzugang sind.*

Ich persönlich finde, daß es viel zu wenig Leute in Deutschland gibt, die fähig sind und sich trauen, technische Entwicklungen mit politischen Tendenzen zu verknüpfen und öffentlich zu äußern. <FrankRo>

Aktualität...

Eure Seiten zum Bereich "/Themen" sind einigermaßen alt. Wie wär's mit einer Aktualisierung, besonders zu den Themenbereichen "Biometrie" oder "Plastikgeld"? *<Jochen R.>*

Gerne! Bis wann schickst Du uns das? <Volker>

Bei der 086 gab es ja Heftungsfehler...

Hi folks, bei mir ist die Datenschleuder **ohne** falschherum eingeheftete Seiten angekommen. Das ist doch nicht normal, oder? Ist das eine Fälschung? Muß ich mir Sorgen ma CARRIER LOST *<Gerd K>*

UM GOTTES WILLEN! Schicken Sie die Schleuder **umgehend** *unter Angabe des Briefträgers zurück. Sie sind hier leider einem plumpen Falsifikats aufgesessen und der Postbeamte hat sich mit dem Fehldruck nach Mauritius abgesetzt.*

Danke für Ihre Wachsamkeit, mit mehr Menschen wie Ihnen könnten wir dem Terror eventuell noch Herr werden. Kameradschaftliche Grüße <erdgeist>

Ein bedauerlicher Fehler unterlief uns:

kleiner, aber etwas peinlicher Tippfehler in der DS 86, Elsterabenteuer im Runner "Hashimemashite, watashi wa neko desu..."

Hashimemashite ▸ Hajimemashite (し ▸ じ)

Dann haut's auch mit「始めまして, 私は猫です」als Bedeutung hin. *<David 'equinox' Lamparter>*

Конечно! Как это могло только происходить с нами? <Эрдгеист>

Data Mining Consultant gesucht...

Gerne würde ich von Ihnen wissen, ob es möglich ist, wenn man die Handy-Nummer und die e-mail-Adresse einer Person kennt, seine Anschrift herauszufinden. Wäre bereit, für diese Information was zu bezahlen. *<ralf.xxx@gmx.de>*

zu a) Ja, wenn die Person einer Eintragung der Mobilfunknummer im Telefonbuch zugestimmt und die Verwertung zur Rückwärtssuche nicht untersagt hat.

zu b) Im allgemeinen ja, wenn man der Person eine Mail an diese Adresse schickt und nach der Anschrift fragt. Wenn man sich nicht traut, eher nicht.

Gern geschehen, ich hätte jetzt gerne 5 EUR und ein Softeis, schickste an <erdgeist@erdgeist.org>

Mami geht nur schnell einklaufen...
So nun weiß ich nicht ob ich genau bei Euch richtig bin ! ich hatte chon mal mit euch kontakt aufgenommen aber durch ein paar umstände war ich eine lange zeit nicht mehr im netz und konnte mich damit beschäftigen . So nun zu meiner Eigendlichen Frage Wo oder wie kann man sich das premiere frei..... lassen ? ! ich würde mich freuen ein paar Antworten oder auchnicht zu bekommen . und wo kann man sich filme .... *<Eine Mutter aus berlin>*

Wir tasten uns, Schlimmes ahnend, vorsichtig an das Problem der Dame heran:
Dieser Satz kein Verb. Bitte schreib doch einfach, was Du wissen möchtest. <Volker>

Und schon gehts los:
... naja ich wuste ja nicht ob man das so frei ausschreiben sollte ! ich wollte gerne filme selber für meine Kinder und mich ziehen aber wo und wie ?

Sorry, der CCC achtet das Urheberrecht. Überrascht? Wir treten für freie Software ein, für den freien Zugang zu öffentlichen Informationen und für den Schutz von privaten Informationen.

Wir treten nicht für beliebiges "Ziehen" ein, da bist Du bei uns an der falschen Adresse.

Und mir wurde gesagt das man die Karte von premiere Kräcken lassen kann oder ist dies nicht mehr möglich nach dem neuen software update von Premiere ?

Wir befassen uns mit Kreativität und Technik. Das "Kräcken lassen" von Premiere find ich ätzend. Warum willst Du unbedingt Premiere bescheissen?

Wenn jemand hier Premiere "knackt", sprich: das Sicherheitssystem re-engineert, dann ist das Neugier und Spass. Es geht doch nicht darum, möglichst rauszuzocken, und für andere das Glotzen kostenlos zu machen, um Premiere zu bescheissen.

Hm. Solltest Du nicht auch ein wenig Vorbild für Deine Kinder sein?

Was hältst Du davon, wenn Du statt Fernsehen und Filme für Deine Kinder lieber einen Ausflug ins Grüne organisierst? Schaust, dass die Kinder an die Luft kommen, Fahrrad fahren, was erleben? Und vielleicht dafür sorgst, daß sie eine Ausbildung machen können, sich mit Kunst, Wissenschaft, Lesen, Leben, Sport und Kultur beschäftigen?

Die Glotze ist doch einfach ätzend. <Volker>

Doch ach! Wir vergaßen die Familienpolitik unter Schröder...
Sorry das ich Der Moral zu nahe gekommen bin . Sicher bin ich mit den Kids drausen sicher machen sie kunst aber auch mal einen Film zu sehen ,gehört dazu zum groß werden !

Nur weil man etwas vom Pc versteht und das besser als andere ist es Traurig zu sehen das man so erhaben tut über andere ! Und die Ausbildung werden Sie schon machen wenn sie Alt genug sind .

Da sie aber noch sehr lange zeit haben, benötigt man auch das nötige kleingeld um so Dinge zu tun wie Kultur ,Sport ,Kunst und Wissenschaft darum bemühe ich mich ,da mir dieses nötige KLEINGELD nicht zuverfügung steht ,ihnen es auf andere Weise dazu legen sprich mal einen Natur Film sehen lassen oder Wisschenschaftliche Sendungen aber wo gibt es diese im Öffendlichen TV ? Am Abend da wo die Kinder Schlafen gehen sollen , vormittags wenn sie in der Schule / Kindergarten sind . Ach ja da gibt es ja noch die Videothek ach ja das kostet ja wieder Geld .

Und nicht zu vergessen Zoo und der Gleichen ja das Kostet alles geld es Gibt Familien die sich dann dank dem Mann dies nicht leisten können, schon mal darüber nachgedacht ? Nicht von ungefähr kommt mein Anliegen muss man erst die halbe Lebensgeschichte offenbaren bis man verstanden wird , weil es viele Leute gibt die kleinkariert und instörnig denken .

... dies hatten wir so bisher noch nie gehört ...
Vergiss die Masche. Sie zieht bei mir nicht. Niemand klaut Kinofilme oder glotzt ohne zu zahlen Premiere wegen der Bildung der Kinder. <Volker>

Zum Thema EC-Karten und Sicherheit

habt Ihr ja schon viele interessante Dinge gebracht, unter anderem ging es auch darum, wie oft welche der Zahlen von 0-9 in PINs auftauchen bzw., wenn ich das richtig verstehe, zweifelt Ihr an, daß diese Verteilung wirklich zufällig ist.

Da ist mir heute was zu aufgefallen: Wenn man eine Reihe schon etwas älterer Geldautomaten vor sich hat, am besten die mit den gebürsteten Metalltasten, sieht man eigentlich sehr gut das sich diese Zahlen **sehr** unterschiedlich abgenutzt sind, obwohl in Material und Oberfläche vollkommen gleich. D.h. eigentlich geben die Automaten auf diese Weise die Häufung gewisser Zahlen sozusagen automatisch zurück!

Sollte man das Tastenbild in verschiedenen Filialen nicht einfach mal per Umfrage auswerten? <*Christoph Freitag*>

Ulkig, genau **darauf** *bin ich auch schon gekommen, allerdings fiel mir dann auf, daß die Null* **sehr** *stark abgenutzt war, was mich wiederum darauf brachte, daß ja auch alle nicht voreingestellten Beträge auf dem Tastenfeld eingetippert werden müssen, die wiederum üblicherweise auf 0 enden.*

Man könnte jetzt theoretisch die am häufigsten abgehobenen Beträge ermitteln und statistisch korrigieren, aber ich fürchte, daß in Berlin-Kreuzberg eher 10EUR und in Radolfzell am See eher so 450EUR abgehoben werden. <*erdgeist*>

Da waren wir erstmal baff...

Hi, was ich bis jetzt so von der "Datenschleuder" gelesen hab fand ich echt gut und muss sagen: WEITER SO!!! Schade, daß es die "DS" nicht als Printmagazin gibt. Es gibt viele Hackermags (2600.com, binrev.com...) mit kleinen Auflagen und grossen Erfolg in der Szene. Also warum ihr auch nicht? So ein kleines DIN A5 Magazin ? ;)

Also, macht weiter so und laßt mich wissen, wenn ihr ein Printmag haben solltet. <*Stefano S.*>

.... und das, wo doch die Webseite noch seltener funktioniert, als die Schleuder erscheint <*erdgeist*>

Obwohl ich mich vor einiger Zeit

schon mal mit Dvorak beschäftigt hatte, hatte ich doch bisher vermieden, meine Tastatur umzustellen. Dein Artikel hat nun dafür gesorgt, daß nun endlich mal diesen Schritt wage.

Allerdings beziehst du dich in dem Artikel nur auf die englische Variante; der Hinweis auf anderssprachliche Layouts fehlt leider. Mit der englischen Variante lassen sich z.B. die Umlaute nicht wirklich nutzen. Deshalb ist das deutsche Layout etwas anders angeordnet; sogar fast alle Tastenbeschriftungen stimmen nach dem Umstecken. Da nicht jeder weiß, daß es auch eine deutsch Variante gibt, wäre es sinnvoll gewesen, darauf hinzuweisen. <*Martin Rost*>

Diese Links sind vielleicht empfehlenswert:

- *http://www.stud.uni-hamburg.de/users/conitzer/dvorak/type-II.html*
- *http://www-lehre.inf.uos.de/~rfreund/dvorak.php*

PS: Bitte lies die Mail lamgsam, ich hab ne halbe Stunde gebraucht, sie zusammenzutippern.

Jukebox

Wer kann mir helfen um an Musik aus dem Internet zu kommen. Mich interessiert die Fabulos 50's,Rat Pack aber auch Volksmusik. Danke <*Hans-Jürgen H.*>

Du könntest z.B. Internet-Radio-Sender hören, das geht völlig kostenlos:
http://www.google.de/search?q=internet+radio

Man kann Musik auch kaufen; jede Menge davon findest Du z.B. auf dem Apple Musicstore, bei T-Online Musicload oder dem Musik-Portal Deines geringsten Misstrauens. <*Volker*>

Data Mining Consultant 2.0

Müßte unbedingt eine Handy Nummer herausbekommen-ich weiß,daß das über die Betreiber fast unmöglich ist. Vielleicht könnt Ihr mit einer Adresse weiterhelfen-soll auch nicht umsonst sein (> Spende) <xxx@web.de>

"Wir sind die Guten. Wir machen so etwas nicht."

Massenhaft Internet-Banking-Löcher durch Netbank-Technik

von Volker Birk

Online-Banking mit der Netbank ist nicht nur für Sehbehinderte barrierefrei – es war lange Zeit auch ohne jede Barriere für alle anderen Nutzer. Wer Kunde ist bei der Netbank oder bei einer der vielen Banken, die mit der Technik der Netbank arbeiten, konnte bis vor kurzem nicht nur die eigenen Kontodaten erreichen, sondern gleich noch die aller anderen Kunden dazu.

Dazu brauchte man nicht einmal ein Paßwort. Der Fehler war wahrscheinlich seit September 2003 in der Banksoftware enthalten und betraf neben der Netbank zudem mindestens alle Sparda-Banken sowie die PSD-Banken. Möglicherweise war das Loch sogar mit dem Demo-Zugang offen. Dies ist die Geschichte eines Hackers, der es gut mit der Bank meinte, und daraufhin 300 EUR überwiesen und wieder weggebucht bekam.

Der Datenschleuder-Redaktion liegen Kontoauszüge von verschiedenen Netbank-Kunden vor, die bisweilen höchst vertrauliche Informationen beinhalten. Ein Netbank-Nutzer ist offensichtlich zum zweiten Mal verheiratet und überweist Unterhalt; zudem hat er hohe Schulden. Ein anderer Netbank-Kunde liebt Bettwäsche des 1. FC Bayern München. Wieder ein anderer überweist monatlich Geld für ein "Gesch.-ltg. Gästehaus".

Ralph Blos *[Name von der Redaktion geändert]*, ein Hacker aus Norddeutschland, zur Redaktion: *"Eigentlich automatisierte ich nur meine eigenen Überweisungen mit Skripten. Ich entdeckte, daß das Feld 'Kontonummer' im Webformular frei belegbar war. Da wurde ich neugierig – ich wollte nur mal probieren, was da passiert."*

Tatsächlich passierte erstaunlich viel. Ohne jede weitere Sicherheitsabfrage lieferte der Netbank-Server alle Daten jedes beliebigen Kontos. Ralph Blos mußte nicht einmal versuchen, irgendwelche Sicherheitseinrichtungen zu überwinden – es gab schlicht gar keine.

Technisches

Wechselt man von der in PHP erstellten Netbank-Homepage zum Internet-Banking, verwendet der Server *www.netbank-money.de* Java Server Pages (.jsp), um die Webformulare für

Kontonummer	Nummer	Blatt	Datum	Kontostand alt EUR
XXXXXX	5	09	28.06.05	[redacted]

Xxxxxxxxxxxx Xxxxxxxx

Bu-Tg	Buchungserläuterung		Wert	Belastungen	Gutschriften
24.06	DIE WORLD-APOTHEKE,	ALTENBEKLV680804Z1 22.06 17.38 MK3	24.06	55,22	
24.06	VISA-ABRECHNUNG	23.06.05 4908[redacted]	24.06	173,30	
24.06	Programmierleistung	IT-Sicherheitsbeauftragter	24.06		300,00
	Netbank AG				
27.06	Berichtigung		24.06	300,00	
28.06	[redacted]	EC 55581511 25.06 17.32 MK3	28.06	46,70	

Kopie des Kontoauszugs, auf dem sehr schön Eingang und "Berichtigung" der Aufwandsentschädigung zu erkennen sind

das Abfragen der Online-Konten zu implementieren. Die Webformulare werden mittels `<form>`-Tags implementiert, deren Inhalt mit POST-Methoden an den Server der Netbank übertragen werden. Die Übertragung funktioniert ausschließlich über HTTPS, wohl an einen Apache-Webserver. Das Session-Management implementiert die Netbank bzw. ihr Systempartner, die Sparda-Datenverarbeitung eG, mit dem Einsatz von `JSESSIONID`-Cookies.

So weit, so sinnvoll. Nur scheint es bis vor kurzem noch überhaupt keinen Test gegeben zu haben, ob ein Benutzer mit einer gültigen Session (und diese kann man schon über den Demo-Zugang bekommen) überhaupt Zugriff auf ein bestimmtes Konto haben sollte.

Das bedeutet, auf der Web-Oberfläche sieht alles in Ordnung aus. Nur die eigenen, also richtigen Konten sind wählbar. In Wirklichkeit vertraute der Netbank-Server aber ausschließlich auf die Daten, die der Webbrowser des Benutzers ihm schickte.

Um die eigenen Kontenbewegungen für seine Zwecke zu automatisieren, nutzte Blos eine HTTP-Bibliothek. Damit war es ihm möglich, den Wert im INPUT-Element mit der Kontonummer auf einen anderen Wert zu ändern. Prompt bekam er statt der eigenen Kontodaten die des anderen Kontos geliefert – mit allen Buchungen, Beschreibungstexten und Nutzerdaten des fremden Kontos.

Ralph Blos wollte das gar nicht erreichen. Aber einmal mit der Nase draufgestoßen, interessierte es ihn schon, wie offen das System der Netbank war. Um es kurz zu machen: Es war völlig offen.

Der Test

Ralph Blos modifizierte eines seiner Skripte, das er eigentlich entworfen hatte, um sich selber einen Zahlungseingang über E-Mail zu signalisieren, und lud einfach mal einen Kontenbereich herunter. Er wollte sehen, wie weit die Lücke ging. Und er stieß dabei auf keine Grenzen.

Ohne weiteres konnte er so listenweise Kontodaten von verschiedenen Netbank-Kunden erhalten. Sein Skript probierte dazu einfach der Reihe nach Kontonummern durch. Nicht alle Kontonummern waren gültig oder belegt, aber in Windeseile hatte Blos megabyteweise Buchungsdaten und Beschreibungen von beliebigen anderen Netbank-Kunden gesammelt.

Und ganz offensichtlich waren diese nicht für seine Augen bestimmt, sie enthielten jede Menge persönliche Informationen. Was sollte Blos jetzt tun? Er hatte ja entdeckt, was möglicherweise schon viel früher andere entdeckt hatten. Wußte die Bank davon gar nichts? Er entschloß sich, zu allererst die Netbank über ihr Problem zu informieren, schon allein damit nicht Schindluder mit den privaten Daten von Dritten getrieben würde. Falls das bereits der Fall war, wollte er sicherstellen, daß die Netbank dem Einhalt gebieten konnte.

Wer ist alles betroffen von diesem Loch?

Einen schlimmen Verdacht hatte Blos – die Netbank gehört ja zur Sparda-Gruppe. Wie sieht es eigentlich bei anderen Banken aus? Und er wurde auch hier sofort fündig.

Schnell ein Konto bei der lokalen Sparda-Bank eröffnet – und Ralph Blos konnte genau so "frei" auf alle Konten dieser Bank zugreifen, wie er es von der Netbank gewohnt war. Das Loch war in allen Online-Banking-Systemen aller Banken enthalten, die zur Sparda-Gruppe gehören oder die Netbank-Technik von der Sparda-Gruppe lizensiert haben. Unter anderem sind das, neben den Sparda-Banken, auch die PSD-Banken.

Alle Kunden- und Kontendaten dieser Banken lagen also jedem völlig offen, der diese jegliche Sicherheit auflösende Lücke kannte.

Netbank – eine ganz spezielle Form von Krisenmanagement

Ralph Blos wandte sich an die betroffenen Banken. Zuerst telefonierte er mit seiner Sparda-

Bank. Dort wurde er von Pontius zu Pilatus weitergereicht. Offensichtlich war man bei der Sparda-Bank auf solche Probleme nicht vorbereitet. Von der Hotline ging´s zum Vorstand. Vom Vorstand weiter zur Technik. Dort wußte man auch nichts mit der Information anzufangen. Blos wurde weiterverbunden zum Rechenzentrum. Endlich erhielt er einen Ansprechpartner.

Blos informierte diesen telefonisch über das Ausmaß des Desasters. Sein Gegenüber bedankte sich und bot ihm daraufhin freundlicherweise eine Bezahlung von 300 EUR für seine Mühen an, welche die Netbank auch prompt auf das Konto von Blos gutschrieb.

Ralph Blos erzählte seinem Vater von der Angelegenheit. Dieser wunderte sich: warum wollten die Leute von der Netbank die technischen Unterlagen, wie beispielsweise die Skripte seines Sohnes, nicht sehen? Warum interessierten sie sich nicht für die Details?

Blos senior rief bei der Netbank an und stellte diese Fragen. Nach einigem Hin und Her erklärte der Netbank-Vertreter, daß sie inzwischen schon gerne Genaueres über den Fall wüßten. Herr Blos würde Besuch von der Netbank bekommen. Und es wäre auch mehr Geld drin, wenn Herr Blos die technischen Details der Lücke offenlege. 3000 EUR bot die Netbank jetzt für die Offenlegung aller Details an, das Zehnfache der bisher zugesprochenen Summe.

Und die Netbank kam ins Haus Blos, vertreten durch zwei Besucher, nach eigenen Angaben ein Prokurist und ein Techniker.

Ralph Blos stellte in aller Ausführlichkeit dar, wie seine Skripte arbeiteten und legte alle Details zu der Lücke offen. Interessiert folgten die Besucher seinen Ausführungen. Als Blos mit seiner Darstellung fertig war, hörte er ein lapidares *"nun ja, das haben wir uns ja auch schon selber so in etwa gedacht"*, und die Besucher verabschiedeten sich.

Wenig später mußte Ralph Blos feststellen, daß es wohl eher auf einen warmen Händedruck rauslaufen würde. Denn statt die versprochenen 3000 EUR nun auszuzahlen, buchte sich die Netbank kurzerhand die bereits gutgeschriebenen 300 EUR wieder zurück. Das ist zwar nicht gerade rechtmäßig, aber eine Bank kann bei ihren Konten scheinbar schalten und walten, wie sie will.

Auch ein Ergebnis

Hatte die Netbank jemals vor, für die Information etwas zu zahlen? Nun, Ralph Blos hatte sich selbst bei der Netbank gemeldet und ihr ihre eigenen Sicherheitsprobleme mitgeteilt. Geld konnte er so wohl hauptsächlich auf freiwilliger Basis, eine Art Finderlohn, erwarten.

Offensichtlich beschränkte man sich bei der Netbank dann auf das Antäuschen von Zahlungen – sogar bei Summen von 300 EUR, wie der Kontoauszug beweist (siehe Abb.). Daraufhin kündigte die Netbank auch gleich das Online-Konto von Blos, und der Rechtsanwalt der Netbank schickte einen Drohbrief (liegt der Redaktion vor).

Conclusio

Eine gute Nachricht gibt´s glücklicherweise für die Leute, die noch ein Konto bei der Netbank oder einer der Sparda- oder PSD-Banken haben: Eine Woche nach dem Besuch der Netbank-Leute bei Blos war die Lücke in deren Software behoben.

Das ist tröstlich zu wissen. Auch wenn es einen technisch versierten Menschen schon sehr wundert, warum man sich überhaupt bei der Netbank auf die Daten aus einem Webformular verließ. Normalerweise sollte es in jeder Online-Banking-Software ein ausgeklügeltes Rechtesystem geben. Eine solche Lücke sollte deshalb völlig unmöglich sein. Denn hätte die Netbank-Software überhaupt ein solches Rechtesystem, so wäre der JSP-Code gar nicht in der Lage gewesen, Daten von fremden Konten in die falsche Session zu liefern, auch dann nicht, wenn ein JSP-Programmierer den besagten Fehler macht.

Internet-Konto-Pirat

eingesandt von Max Mustermann, überarbeitet von padeluun

Duch die momentane Berichterstattung über Handy-Payment bin ich auf die Seite hausaufgaben.de aufmerksam gewurden. Ich war insbesondere interessiert, wie die momentan ihren "Service" abrechnen, nachdem Handy-Payment ja offensichtlich nicht mehr geht. Und was soll ich sagen, es ist tatsächlich noch "bequemer" geworden. Die Abrechnung erfolgt inzwischen über die Firma afendis AG per elektronischem Lastschriftverfahren. Ein Leserbrief in Artikelform...

Der Zugang kostet nur 1 EUR pro Tag. Na gut, das stimmt nicht ganz: Ganz klein darunter steht, daß, falls man nicht innerhalb von 3 Tagen kündigte, man ein Jahresabo für 96 EUR abgeschlossen hätte.

Aber ansonsten braucht man nur ein paar Angaben einzutippen, und schon kann es losgehen:

```
Vorname: Max
Name:    Mustermann
Straße:  Holzweg 1
PLZ:     00815
Ort:     Glücksstadt
Email:   muelleimer@trash-mail.de
```

Das Wichtigste kommt natürlich noch: die Kontodaten. Für einen Versuch waren mir natürlich meine eigenen viel zu schade (immerhin kostet der Spaß ja 96 EUR, wenn man nicht innerhalb von 3 Tagen wieder kündigt bzw. die Kündigung auf rätselhafte Weise verlorengeht).

Die Kontodaten von Max Mustermann hatte ich natürlich auch nicht zur Hand. Naja, Kontodaten gibt es ja im Internet wie Sand am Meer. Warum sollten die immer nur als Einbahnstraße für Zahlungen taugen? Dank *afendis* geht es ja nun endlich auch andersrum. Da Ihr *[der Chaos Computer Club, Anm. d. Red.]* ja für die sinnvolle Nutzung öffentlich verfügbarer Daten steht, habe ich es natürlich prompt mit Euren Daten ausprobiert:

```
Inhaber:     Chaos Computer Club e.V.
BLZ:         20010020
Kontonummer: 599090201
```

Es klappte prima. Sekunden später hatte ich schon die Bestätigungsmail an die Adresse <*muelleimer@trash-mail.de*> erhalten. Damit konnte ich mich sofort anmelden und hatte Zugriff auf die Referate unter *hausaufgaben.de*. Erst jetzt merkte ich, daß mir die Referate eigentlich gar nichts nützen (geh´ nicht mehr zur Schule) und ich auch mit den auf *hausaufgaben.de* angebotenen lustigen Entschuldigungsschreiben für den Fall von Alien-Landungen nichts anfangen kann.

Habe somit sofort wieder gekündigt. Damit sollte sich euer vorübergehender Schaden (ich denke, daß ihr Euch um die Rücküberweisung der Lastschrift bemühen werdet) in Höhe von 1 EUR auch in Grenzen hält. Es ging mir ja schließlich nicht darum, Euch wirklich zu schädigen, sondern ich war mehr daran interessiert, ob das alles ohne zusätzliche Prüfungen einfach so klappt.

Eventuell merken die Mitarbeiter hinter *hausaufgaben.de* auch aufgrund des Kündigungsschreibens (wird vermutlich nicht automatisiert verarbeitet werden), daß etwas nicht stimmt und verzichten ganz auf die Abbuchung des Betrages. Es ist zu hoffen, daß dieses innovative Zahlungssystem Schule macht und ich demnächst auch für mich wirklich sinnvolle Dinge damit "bezahlen" kann, wie z.B. Musikdownloads, Online-Spiele...

Noch was im Ernst: Ich finde das Zahlen per elektronischer Lastschrift überhaupt nicht lustig. Selbst wenn man in aller Regel die Lastschrift zurückholen kann, so muß man

- regelmäßig die Kontoauszüge genau prüfen, damit einem solche Lastschriften überhaupt auffallen,
- sich mit seiner Bank in Verbindung setzten und das Zurückholen der Lastschrift beantragen,
- warten, bis die Lastschrift wieder zurücküberwiesen wurde.

Danach könnte der Spaß erst richtig losgehen, wenn sich nun deren Anwälte meldeten und fragten, warum das Geld wieder weg ist. Das alles kostet Zeit, Nerven und eventuell auch noch Geld (Porto, Fahrtkosten...).

Dazu kommt, daß, falls ein größerer Betrag auf diese Art und Weise abgebucht wurde, man vielleicht andere Dinge nicht fristgerecht zahlen kann. In der Regel wird es nämlich eine ganze Weile dauern, bis das Geld wieder da ist.

Wenn die Lastschrift so hoch war, daß der Dispokredit ausgereizt wurde, dann erhält man vorübergehend auch überhaupt kein Geld von seinem Konto mehr. Das kann also sogar an die Existenz gehen. Da oftmals die eigene Kontonummer mehr oder weniger öffentlich ist (wie z.B. in Eurem Fall), darf es kein Zahlungssystem geben, welches nur aufgrund dieser öffentlichen Informationen Abbuchungen vornehmen kann. Denn es enstehen dem Betroffenen auch bei Rückabwicklung zunächst Nachteile.

Ich hoffe deshalb, daß in der Richtung irgendwas passiert, damit *afendis* und anderen das Handwerk gelegt wird, denn diese Methode der Zahlungsabwicklung ist einfach nur gefährlich.

PS1: Ich habe speziell für diese Mail und die Kündigungsmail an *hausaufgaben.de* einen Mailaccount bei *http://web.de/* angelegt:

Zugangsdaten:

```
Name:      max.mustermann0815@web.de
Passwort:  $afendis
```

PS2: Ihr braucht nicht auf diese Mail zu antworten, ich werde aus Sicherheitsgründen den Account bei *http://web.de/* nie wieder besuchen. Allerdings dürfte dort die Antwortmail der Kündigung von *hausaufgaben.de* ankommen, insoweit solltet ihr vielleicht nochmal überprüfen, ob das auch klargegangen ist (vielleicht lassen die sich sogar eine schöne Antwort einfallen).

PS3: Ich habe die gesamte Sitzung inklusive der Erzeugung des Email-Accounts bei *http://web.de/* über JAP anonymisiert (Kaskade: Regensburg - CCC). Insoweit könnte es sein, daß da noch eine Anfrage hinterher an Euch kommt, weil sie nun nach Rückbuchung der Lastschrift wissen wollen, wer wohl all diese Daten in deren Formular eingetippt hat.

Dies dürfte damit wohl auch ins Leere laufen. Leider wird das auch nicht helfen, *afendis* von ihrer innovativen Zahlungsmethode abzubringen, da sie es als bereits einkalkulierten Einzelfall abtun werden; eure Kontonummer wird auf eine „Blacklist“ gesetzt, ihr werdet das Problem in Zukunft los sein, und es wird wahrscheinlich den Nächsten treffen.

PS4: Falls Ihr das Ganze als langweilig und Zeitverschwendung abtun solltet, nur weil so ein (weiterer) Idiot es lustig fand, Eure Kontodaten irgendwo einzugeben und Ihr was Besseres mit eurer Zeit anzufangen wißt, als (Bagatell-)Lastschriften auf Eurem Konto zu kontrollieren, fände ich es zwar bedauerlich, könnte es aber natürlich nicht ändern.

Schreibt in diesem Fall einfach auf Eure Website, daß ihr wißt, daß Eure Kontodaten mißbraucht werden können, ihr aber darum bittet, das nicht wirklich zu tun. Ich hätte das respektiert, da ja nicht wirklich eine Leistung dahinter steht, diese Daten irgendwo einzutragen.

Kommentar der Redaktion

So ein schöner Artikel für die Datenschleuder. Alle anderen, die bisher unsere Kontodaten bei solchen dubiosen Anbietern eingetragen haben, haben sich die Mühe, einen Artikel darüber zu schreiben und uns zuzusenden, nicht gemacht.

Aber bitte: Nehmt nicht unser Konto, um solche Sachen auszuprobieren; es nervt, immer wieder bei der Bank anzurufen, um sowas zurückbuchen zu lassen (was übrigens ganz einfach geht). Tips für Leute, die ihr Konto im Internet veröffentlichen müssen (weil es zum Beispiel ein Spendenkonto ist): Laßt Euch ein zweites Konto einrichten und gegen das Abbuchen von Lastschriften sperren. Dessen Nummer veröffentlicht Ihr – Euer Hauptkonto bleibt für die Hausaufgabenerschleicher unerkannt.

Internet-Konto-Pirat 2.0

von padeluun

Der Chaos Computer Club empfängt eine Beschwerde via Fax. Auf dem Kontoauszug eines Teilnehmers würde eine Lastschrift von Web.de auftauchen.

Im Buchungstext (so schreibt er) stünde:

```
INFORMATIONEN ZU DIESER
BUCHUNG FINDEN SIE UNTER
HTTPS //KUNDENCENTER.WEB.DE
```

Nun beschwert er sich bei uns, daß sich statt der Webseite von web.de *"Ihre Seite CCC.DE mit keinerlei hilfreichen Informationen"* meldet.

Was ist wohl passiert, denn ich kann mir nicht vorstellen, daß er Alvar Freudes Proxy eingeschaltet hat, der alle Anfragen nach *kundencenter.web.de* auf *ccc.de* umleitet?

Nochmal aufs Fax geguckt: Da fehlt (weil ihn das Datenträgeraustauschformat der Banken nicht kennt) ein Doppelpunkt.

Also nahm ich den "daB" (dümmsten anzunehmenden Browser), den Microsoft Explorer, und tippte in die Adresszeile testweise "https" ein – und was passiert? Genau: Der schaltet sich auf die blöde MSN-Suche um und führt an erster Stelle *www.ccc.de* auf – klick – und schon hält uns OttoNormalKlicker für das Web.de-Kundencenter... Mein Gott, sind WIR böse. Jetzt unterwandern wir schon Microsoft ;-)

Hallo Web.de. Ihr solltet den Text auf dem Kontoauszug ändern in *WWW.KUNDENCENTER.WEB.DE*. Das verstehen auch DAUs und Ihr könnt eine Weiterleitung auf *https://kundencenter.web.de/* einrichten. Nein, nein, schon gut. Der Tip kostet nichts.

Ausbau der "Egelsbach Transmitter Facility"

von den Freunden der Antenne e.V. <ds@ccc.de>

Seit Ende des Zweiten Weltkriegs betreibt das Militär der Vereinigten Staaten südlich von Frankfurt am Main eine Sendestation. Diese steht mitten im Wald und ist schwer zu finden. Hauptsächlich Einheimische dürften den Sender kennen. Einige Kurzwellenhörer kennen ihn auch. Sie sind sich sicher, daß der Sender für den Agentenfunk benutzt wurde.

Unweit der Rhein-Main-Airbase, in der Nähe des Langener Stadtsees, kann man als Spaziergänger auf ein großes, mit bemerkenswerten Antennensystemen ausgestattetes Areal stoßen. Öffentliches Kartenmaterial weist das Gelände als bebaute Fläche aus. Eine Kartendarstellung notiert das Blitz-Symbol für Sender bzw. Antennen. Die Koordinaten sind 50.004101° Nord und 8.611157° Ost. [1]

Eine schwenkbare Kamera filmt den Einfahrtsbereich. Vor dem Tor steht ein halb offener Kasten mit einer Wechselsprechanlage. Daneben ist eine Nummerntastatur mit dem Aufdruck „Cypher(R)". Es gibt keine Torbeschriftung, die den Betreiber benennen könnte. Lediglich ein paar englische Benutzungshinweise an der Gegensprechanlage lassen Vermutungen hinsichtlich der Benutzergruppe zu. Mutmaßlicher Betreiber der Installation ist die Army Security Agency (ASA).

Inventar-Listen des Department of Defense

Der seit 1999 jährlich erscheinende "Base Structure Report" des US-amerikanischen Verteidigungsministeriums listet militärische Einrichtungen auf. Diese Berichte bezeichnen die Einrichtung offiziell als "Egelsbach Transmitter Facility". Sie wird der US Army zugeordnet [2]. Angaben über Anzahl der Beschäftigten läßt das Department of Defense offen. Die folgende Tabelle faßt die Eintragungen der letzten Jahre zusammen.

Stand	Anzahl Gebäude (Besitz)	Fläche Gebäude (Besitz) [Quadratfuß]	Anzahl Gebäude (Miete)	Fläche Gebäude (Miete) [Quadratfuß]	Fläche Gesamt [acre]	PRV [Mio. USD]
30.09.2004	2	1270	3	285	76	1,0
30.09.2003	2	1270	1	6369	76	10,3
30.09.2002	8	10331	keine Angabe	keine Angabe	76	4,3
30.09.2001	8	10331	keine Angabe	keine Angabe	122	4,2
30.09.2000	3	8757	keine Angabe	keine Angabe	122	13,8
30.09.1999	3	8757	keine Angabe	keine Angabe	6	3,8

Merkwürdig erscheinen der Gebäudezuwachs im Jahr 2001 und der Gebäudeschwund zwischen 2002 und 2003. Die gesamte Gebäudefläche beträgt zuletzt nur noch etwa 144 Quadratmeter. Der "Plant Replacement Value" (PRV) gibt die Kosten für einen Neubau an. Warum

diese so stark schwanken, kann man ohne genaue Kenntnis der Zusammensetzung nicht sagen.

Immer wieder Berichte über Bauaktivität

Aus den reinen Zahlenwerten läßt sich zumindest kein Ausbau ableiten. Daß der Sender ausgebaut wird, davon berichten jedoch Spaziergänger: Modernisierungsarbeiten sollen Anfang der 90er Jahre erfolgt sein. Neue Gebäude entstanden in den letzten Jahren. Der Betreiber ließ den äußeren Zaunring ausbessern und das Haupttor ersetzen. Eine mehrere Meter lange Klimaanlage steht in der inneren Umzäunung. Sie sieht neu aus.

In jüngster Zeit wurde ein Radom mit geschätzten 5 Metern Durchmesser errichtet. Darunter versteckt sich wahrscheinlich eine Satellitenschüssel. Zum Ende des Sommers 2005 schraubten Bauarbeiter am Fuß einer neu aufgestellten Satellitenschüssel. Möglicherweise handelte es dabei sich um Vorbereitungen für den Überzug einer Schutzhülle. Der Schüsseldurchmesser beträgt ca. 10 Meter.

Bauarbeiten an der neuen Satellitenschüssel

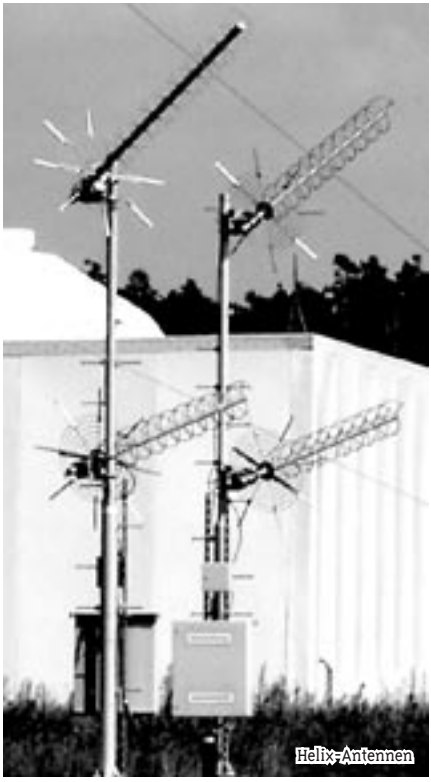
Helix-Antennen (FAH-Serie?)

In den 90er Jahren zog das Militär einen Teil des Personals von der Rhein-Main-Airbase ab. Die Bundesrepublik übernahm im September 2005 das Airbase-Gelände. Zum Ende des Jahres soll die Basis geräumt sein. Beobachter vermuten daher einen Zusammenhang zwischen dem Ausbau der Sendestation und der Schliessung der Rhein-Main-Airbase. Im Rahmen der Airbase-Schliessung wurde Gerüchten zufolge ein SATCOM-Terminal zum Egelsbach-Transmitter verlegt. Die Satellitenschüssel könnte dazugehören. Zahlreiche große Container, die möglicherweise als Umzugskartons dienen, stehen auf dem Gelände.

Nummernstationen

Täglich senden weltweit verteilte Stationen kryptografisch kodierte Nachrichten. Als Morsecode oder maschinell vorgelesene Zahlenkolonnen werden die Nachrichten über Kurzwelle (3–30 MHz) ausgestrahlt. Mit Kurzwelle lassen sich hohe Reichweiten erzielen, denn der Raumwellenanteil reflektiert zwischen Ionosphäre und der Erdoberfläche. Die übertragenen Zahlenreihen können deshalb mit einem Weltempfänger auch in größerer Entfernung gehört werden.

Die synthetischen Stimmen lesen häufig Zahlen vor, weshalb man derartige Sender auch Nummernstationen nennt. Mittlerweile ist man davon überzeugt, daß Nummernstationen der Kommunikation mit Agenten dienen. Ein paar Kurzwellenhörer beschäftigen sich mit Nummernstationen. Sie protokollieren Sendungen, erstellen Sendezeitpläne und klassifizieren Stationen nach ihren Übertragungsverfahren, Nachrichtenformaten und benutzten Frequenzen. Aus deren Beobachtungen ist die "Enigma-Klassifikation" hervorgegangen. Sie sehen in der Sendestation bei Egelsbach eine der europäischen Nummernstationen und ordnen dem Sender die Klasse E05 zu. E05-Stationen senden in englischer Sprache vorgelesene Zahlenkolonnen. Es gibt in allen Erdteilen E05-Stationen. Die verwendete Frauenstimme hat unter Liebhabern den Namen "Cynthia" erhalten. Anfang und Ende ergeben den vermuteten


Helix-Antennen


Drehbare Logperantennen und der Mikrowellenturm

Betreiber. Eine der wenigen Webseiten über den Sender berichtet ferner von "Multi tone PSK"- und 108.86-Baud-FSK-Übertragungen, die von der Station ausgegangen sein sollen.

In der ZDF-Doku "Freund hört mit" erklärt ein Interviewpartner, daß in unmittelbarer Umgebung des Senders die Cynthia-Stimme mit einem Empfänger selbst ohne Antenne hörbar gewesen sei. Deshalb ist man sich ziemlich sicher, daß die Egelsbach Transmitter Facility tatsächlich E05-Sendungen verbreitete. Nach 2003 stellten Zahlensenderbeobachter keine weitere Sendeaktivität fest.

Antennen

Der hohe Mastaufbau für den Mikrowellenrichtfunk gehört seit längerer Zeit zum Inventar. Im Internet verfügbares Fotomaterial der letzten Jahre bildet ihn ab. Zwei Mikrowellenschüsseln hängen an der Mastspitze und peilen grob in Richtung Rhein-Main-Airbase. Vermutlich betreibt man darüber eine Punkt-zu-Punkt-Verbindung. In einem Internetforum behauptet jemand, die Richtfunkschüsseln seien nicht

mehr direkt zur Airbase ausgerichtet. Angeblich sollen sie jetzt mehr in Richtung Zeppelinheim oder Dreieich zeigen. Wie er oder sie das herausgefunden hat, bleibt allerdings offen.

Für den eigentlichen Kurzwellenbetrieb ist das Gelände mit monströsen Antennen ausgestattet. Die großen Drahtantennen und die rotierbaren Antennen bezeichnet man aufgrund ihrer Strahleranordnung als logarithmisch-periodische Antennen (siehe Fotos). Sie können für sehr breite Frequenzbereiche konstruiert werden. Das längste Element der Antenne bestimmt die größte benutzbare Wellenlänge und damit die niedrigste Arbeitsfrequenz. Die maximale Arbeitsfrequenz begrenzt der kleinste Strahler. Je mehr Strahler man auf einer Logper-Antenne anordnet, desto größer ist prinzipiell auch deren Frequenzbereich. Logper-Antennen haben, verglichen mit einem einfachen Dipol, einen Antennengewinn, denn die Sendeenergie wird gezielt in eine Richtung ausgestrahlt.

Die meisten Antennen auf dem Gelände haben horizontal ausgerichtete Strahlerelemente. Damit ist das elektrische Feld der sich ablösenden Wellen horizontal polarisiert. Praktisch bedeutet das für den Empfänger, daß er seine Empfangsantenne ebenfalls horizontal anordnen muß, um möglichst viel elektrisches Feld einkoppeln zu können.

Die großen Drahtantennen sehen Produkten der amerikanischen Firma TCI so ähnlich, daß man TCI auch als Hersteller annehmen kann. Mehrere der installierten Antennen gleichen dem Modell TCI 524. Dessen untere Arbeitsfrequenz liegt ausführungsabhängig bei 4 bis 6 MHz, die maximale Arbeitsfrequenz beträgt 26 bzw. 30 MHz. Der Antennengewinn hängt von der Betriebsfrequenz ab und liegt zwischen 15,5 und 16,5 dBi. TCI verkauft sie als "Super High Gain Log-Periodic Antenna".

TCI bietet eine in zwei Reihen übereinander gestapelte Version des Model 524 als TCI 527 an. Beide Teile der Antenne nehmen die Energie zum Senden über einen gemeinsamen Speisepunkt auf. Sie hat gegenüber dem Modell 524 eine stärkere Richtwirkung und damit einen höheren Antennengewinn (16,5 bis 18,2 dBi). Der nutzbare Frequenzbereich entspricht weitgehend dem der "einfachen" Ausführung. Der Betreiber verfügt über etwa drei Antennen dieses Typs.

Modell 527 und 524 sind auf den Fotos abgebildet. Die Fotos wurden allerdings nachbearbeitet, damit man die Drahtstrukturen überhaupt erkennen kann.

Neben den fest ausgerichteten Drahtantennen stehen für den Funkbetrieb vier drehbare Logper-Antennen bereit. Sie haben jeweils 19 horizontale Elemente. Selbst wenn die Station nicht zum Senden benutzt wird, sind die großen

Eine der kleineren Antennen auf der Nordseite

Eine TCI 524-Antenne. Ausschnitt als Negativbild dargestellt, damit man das Drahtgespann erkennen kann.

drehbaren Antennen geeignete Empfangsantennen für Kurzwelle. Google-Maps zeigt noch den Schatten einer fünften drehbaren Logper-Antenne. Diese muß in den letzten Jahren entfernt worden sein.

In der Nähe des Gebäudekomplexes soll sich eine Drahtantenne des Typs TCI A 613 befinden. Das kann ich nicht bestätigen. Dafür erscheinen in Google-Maps ein paar Schatten von Antennenmasten. Vielleicht spannten die Masten die A 613 auf. Möglicherweise mußten sie abgebaut werden, um Platz für die SATCOM-Installation zu schaffen.

Im nördlichen Teil des Geländes stehen zwei bis drei weitere Drahtantennen (jeweils an einem einzelnen Mast). Deren Drähte sind hauptsächlich vertikal orientiert. Der Bauform nach strahlen die Antennen in alle Himmelsrichtungen.

Ein paar kleinere Masten sind in der Nähe der drehbaren Antennen installiert. Daran kann man ca. ein Dutzend Helix-Antennen sehen. Die Fotos zeigen zwei verschiendene Bauformen. Das eine Modell wird höchstwahrscheinlich von der Firma Astron Wireless Technologies hergestellt (FAH-Serie). Die Helix-Antennen sind im Wesentlichen süd- bis westwärts orientiert und vermutlich auf Satelliten ausgerichtet.

Schlußbemerkung

Um einen Überblick über die Antennenausrichtung zu bekommen, habe ich die Anordnung von Fotos abgelesen und auf das Satellitenbild übertragen. Unklare Stellen sind mit einem Fragezeichen markiert. Bei der nördlichsten 524 bin ich mir nicht so 100%ig sicher. Das Foto von der Stelle war nicht scharf genug. Die doppelt durchkreuzten Punkte stellen Masten dar, die auf neueren Fotos nicht zu sehen sind. Die größeren Kreise sind der oben beschriebene Radom und die Satellitenschüssel. Der Turm mit den Mikrowellenschüsseln und die Helix-Antennen sind nicht eingezeichnet.

Es ist total unklar, warum man die Station nicht demontiert. Die Beobachtungen der letzten Zeit bestätigen immerhin den Verdacht, daß der Sender ausgebaut wird. Es ist natürlich naheliegend, daß die Einrichtung nicht zu Dekora-

tionszwecken umgebaut wird, sondern daß der Betreiber damit konkrete Ziele verfolgt. Über die zukünftige Aufgabe dieses Senders kann man aber nur spekulieren.

Oktober 2005

Quellen

[1] Google-Maps
• *http://maps.google.com/*

[2] DoD, Base Structure Report, Fiscal Year 2005-1999 Baseline
• *http://www.brac.gov/docs/20050527_2005BSR.pdf*
• *http://www.dod.mil/pubs/20040910_2004BaseStructureReport.pdf*
• *http://www.dod.mil/pubs/almanac/almanac/Graphics/BSR_03.pdf*
• *http://www.acq.osd.mil/ie/irm/irm_library/Base%20Structure%20Report%20FY%202002%20Baseline.pdf*
• *http://www.acq.osd.mil/ie/irm/irm_library/Base%20Structure%20Report%20FY%202001%20Baseline.pdf*
• *http://www.defenselink.mil/pubs/basestructure1999.pdf*

[3] US-INTELLIGENCE TX-SITE, Frankfurt / Germany,
• *http://rover.vistecprivat.de/~signals/TABLES/FFM-TX-SITE.HTML*

[4] Egmont R. Koch, "Freund hört mit", ZDF-Doku (über Filesharing beziehbar)

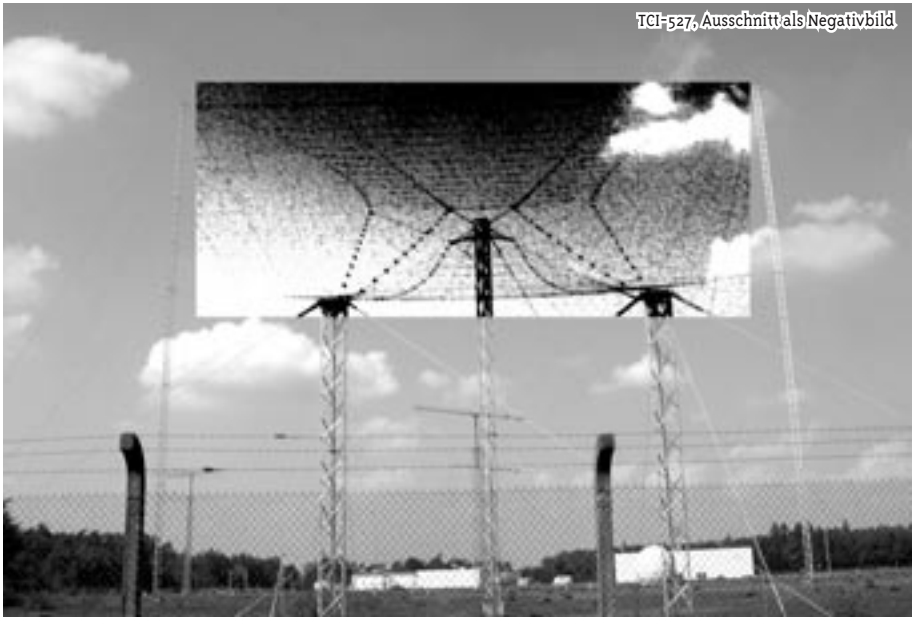
[5] Ausbau TX-Site Langen, Forumsdiskussion vom 17.07. bis 11.09.2005
• *http://www.cold-war.de/showthread.php?t=41*

[6] Ausbau TX-Site Langen? Forumsdiskussion im Oktober 2005,
• *http://www.sis-germany.de/index.php?id=22&view=single_thread&cat_uid=6&conf_uid=7&thread_uid=100*

[7] Webseite der Firma TCI
• *http://www.tcibr.com/*

[8] E5 Counting Station
• *http://www.simonmason.karoo.net/page65.html*

[9] Spy Numbers Station Database
• *http://www.spynumbers.com/numbersDB/*



TCI-527, Ausschnitt als Negativbild

Inside Bluetooth Security

Bastian Ballmann <Crazydj@chaostal.de>

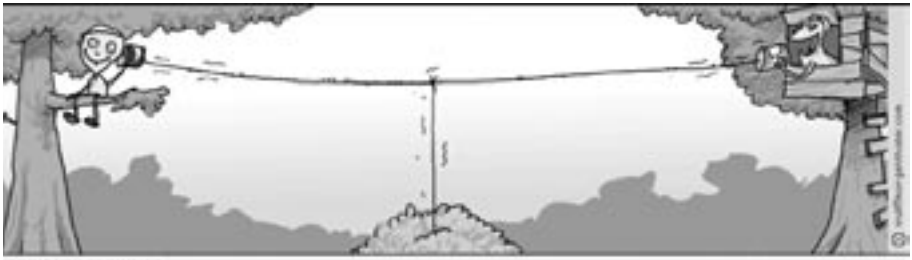
Bluesnarfing, sprich unauthorisiertes Kopieren von Daten, und Bluebugging, die komplette Kontrolle über ein Gerät mit Hilfe von AT Befehlen, sind eigentlich altbekannt [1]. Bluesnarfing wurde erstmals im November 2003 von Marcel Holtmann vorgestellt, Bluebugging im März 2004 von Martin Herfurt. Derartige Techniken wurden auf dem 21C3 [2] präsentiert.

Obwohl die Hersteller informiert wurden und Patches verfügbar sind, ist die Information, daß die Implementationen von Bluetoothtechnologien einiger Hersteller sehr leichtfertig brisante Daten durch die Luft werfen, leider nicht bis zum Konsumenten weitergeleitet worden. So ist es nicht verwunderlich, daß derartige Attacken [3] im Regierungsbezirk in Berlin das *Herrschaftswissen der Republik*, wie es der Spiegel nennt, preisgeben. Nur die Tatsache, daß es nach wie vor keine Scriptkiddie-Tools für derartige Attacken im Netz gibt, verhindert Schlimmeres – oder ist sie vielleicht gar mit schuld an der Misere? Ich weiß es nicht, das ist wohl fast schon eine Glaubensfrage.

Auf jeden Fall stelle ich mir immer noch die Frage, wie solche Sicherheitslücken zustande kommen. Wieso kann man sich bei manchen Handys auf einen Channel, der nicht via SDP gelistet ist, verbinden und dem Telefon munter Befehle senden, die es dann ungefragt ausführt? Man kann diese Lücke sogar dazu verwenden, dem Telefon mitzuteilen, daß es bitte einfach abhebt, wenn man anruft. Dadurch ist eine **Raumüberwachung mit Hilfe einer Yagi-Antenne auf knapp anderthalb Kilometern Entfernung möglich**! Fällt solch eine Eigenschaft aus Versehen und unbemerkt in den Code? Wurde sie zu Testzwekken implementiert und nachher vergessen?

Daß es manche Hersteller irgendwie versäumt haben, bei OBEX FTP eine Authentifizierung einzubauen und man deshalb munter das Telefonbuch sowie den Kalender auslesen kann, kann ich mir ja noch vorstellen. Wie auch immer solche Dinge zustande kommen mögen, die Informationspolitik der entsprechenden Unternehmen ist miserabel.

Dank Blooover [4] braucht man auch noch nicht einmal mehr einen Laptop. Ein Mobiltelefon mit Bluetooth und Java Unterstützung reicht aus, um derartige Attacken fahren zu können. Und wer sich ein wenig mit Bluetooth auskennt,



von wulffmorgenthaler.com

bei eBay z.B. ein Nokia 6310i mit ungepatchter Softwareversion ersteigert, via bash-Script die RFCOMM-Channels des Telefons abklappert und mit der CVS Version von BlueZ vertraut ist, wird diese Lücken ebenfalls schnell finden. Sie sind einfach zu trivial. Eine Einführung in das Thema bietet der Artikel „Bluetooth for fun and profit“. [5]

Bei Nokia kann man sich eine komplette Dokumentation der AT-Befehle [6] herunterladen, und man wird feststellen, daß man mit seiner Bluetooth-Verbindung mindestens genauso viel machen kann, wie der Benutzer an der Handytastatur.

Das Tracken von Personen dank der eindeutigen Bluetooth-Adresse, sowie Blueprinting [7], Erkennen des Herstellers anhand der ersten drei Bytes, brauch ich wohl kaum noch zu erwähnen. Also was gibt's Neues seit dem 21C3?

Bluetooth DoS

Mehrere Angriffsmöglichkeiten, sowohl auf den Bluetooth-Stack, als auch auf Dienste, die über Bluetooth erreichbar sind, können zu einer Denial-of-Service-Attacke führen. Dies wird entweder nur den Bluetooth-Stack oder gleich das ganze Gerät abstürzen lassen.

Ein Beispiel für eine solche Attacke wurde auf dem 21C3 präsentiert, indem einem PDA ein etwas größeres L2CAP Paketchen geschickt wurde und dadurch lustige Nebeneffekte auftraten. Aber anscheinend geht es noch viel einfacher, denn es wurde berichtet, daß der Bluetooth Stack von Nokia 7650, Nokia 6600, Siemens V55, Motorola S55 und Windows 2003 abstürzen soll, wenn sie zu lange mit `l2ping -f` genervt werden. Mehr dazu hier [8].

Dies konnte ich mangels Verfügbarkeit dieser Devices nicht nachprüfen und kann nur sagen, daß mein geliebtes Nokia 6310i nicht weiter interessiert war. Aber ich bin neugierig geworden und habe mich gefragt, ob es bei derart einfachen Angriffen nicht auch die Möglichkeit einer LAND-Attacke, also Senden eines Pakets mit gleicher Absender- wie Empfängeradresse, gibt.

```
#include <stdio.h>
#include <errno.h>
#include <stdlib.h>
#include <sys/socket.h>
#include <bluetooth/bluetooth.h>
#include <bluetooth/hci.h>
#include <bluetooth/hci_lib.h>

#define OCF_ERICSSON_STORE_IN_FLASH     0x0022

typedef struct {
  uint8_t         user_id;
  uint8_t         flash_length;
  uint8_t         flash_data[253];
} __attribute__ ((packed)) ericsson_store_in_flash_cp;

#define ERICSSON_STORE_IN_FLASH_CP_SIZE 255

static void change_bdaddr(int dd, char *btaddr)
{
  struct hci_request rq;
  ericsson_store_in_flash_cp cp;
  bdaddr_t bdaddr;

  memset(&cp, 0, sizeof(cp));
  cp.user_id = 254;
  cp.flash_length = 6;

  str2ba(btaddr, &bdaddr);
  memcpy(&cp.flash_data, &bdaddr, 6);

  memset(&rq, 0, sizeof(rq));
  rq.ogf    = OGF_VENDOR_CMD;
  rq.ocf    = OCF_ERICSSON_STORE_IN_FLASH;
  rq.cparam = &cp;
  rq.clen   = ERICSSON_STORE_IN_FLASH_CP_SIZE;
  rq.rparam = NULL;
  rq.rlen   = 0;

  if (hci_send_req(dd, &rq, 1000) < 0) {
    perror("");
    return;
  }
}

int main(int argc, char *argv[])
{
  int dd;

  if(argc < 3)
  {
    printf("change_btaddr <devnr> <addr>\n");
    exit(0);
  }

  dd = hci_open_dev(atoi(argv[1]));

  if (dd < 0) {
    perror("");
    exit(1);
  }

  change_bdaddr(dd,argv[2]);
  hci_close_dev(dd);
  return 0;
}
```

Manche Bluetooth-Chipsätze erlauben es, mit Hilfe eines HCI-Befehls die Adresse neu zu setzen, doch Vorsicht: Man sollte sich die alte Adresse notieren, sonst isse futsch. Hier ein kurzes Codesnippet für den Ericsson-Chipsatz, das mir freundlicherweise von Marcel Holtmann [9] zur Verfügung gestellt wurde. Die handelsüblich verbauten CSR-Chipsätze bieten solch ein nettes Feature leider nicht an. Eine Liste der Ericsson-HCI-Commands und -Events gibt es hier [10].

Als ich daraufhin die Adresse des Bluetooth-Sticks auf dieselbe wie meines Nokia 6310i gesetzt habe und ein `l2ping` ausführen wollte, bekam ich nur ein *No route to host* um die Ohren gehauen. Ok, aktiv geht es schon mal nicht, also probiert man einen passiven Scan. Auch der zeigte kein Ergebnis. Ich weiß jetzt leider nicht, ob überhaupt ein Paket in die Luft geschleudert wurde oder ob der Stick nur mit sich selber geredet hat, aber ich bin optimistisch, daß es dort draußen einen Bluetooth Stack gibt, der für sowas zu haben ist.

Ok. Weg von L2CAP hin zu OBEX. In der Software eines Sony Ericsson P900 und Nokia 9500 wurden mehrere Möglichkeiten für Deskriptor-Overflow [11] entdeckt. Diese funktionieren mit Hilfe von VCards, deren Dateiname oder Inhalte mehr als 200 Zeichen umfaßten. Laut Aussage des Entdeckers lassen sich diese leider nicht exploiten. Und selbst wenn es eine Möglichkeit gäbe, würde es dem Angreifer nicht viel bringen, weil das Symbian OS diese Dienste mit sehr niedrigen und eingeschränkten Privilegien laufen lässt. Trotz allem kann solch eine Attacke zu einem Denial of Service führen.

Ich habe daraufhin die bluez-utils und die Kernel Bluetooth Implementation gepatched, so daß der Device-Name mehr als die üblichen 248 Zeichen umfaßt, in der Annahme, so etwas könnte vielleicht auch zu einem Overflow führen. Doch Fehlanzeige: Die Firmware des Bluetooth-Sticks liest nur 248 Zeichen und Ende. Eine Möglichkeit des Overflows besteht somit wahrscheinlich nur über die Netzwerkebende, also via Pakete / Payload. Etwas Perl-Code im POC Status zum Thema gibt es hier [12].

Cracking the bluetooth PIN

Zwei israelische Forscher, Avishai Wool und Yaniv Shaked von der Universität in Tel Aviv, haben den Algorithmus des in Bluetooth verwendeten Verschlüsselungsverfahrens *Safer+* geknackt [13]. Nach eigenen Aussagen ist es möglich, eine vierstellige PIN mit einem 3 GHz Rechner in 0.06 Sekunden zu errechnen.

Dazu muß allerdings der gesamte Pairing-Prozess mitgeschnitten werden, dann kann mit der Bruteforce-Methode der Link Key ermittelt werden. Die Tatsache, daß viele Hersteller nur eine vierstellige PIN zulassen, erleichtert solche Angriffe enorm.

Pairing Attacks

Dieselben Forscher haben eine Repairing-Attacke entdeckt, wobei einem Gerät mit gespoofter Bluetooth-Adresse erzählt wird, man hätte aus Versehen den Link Key verbummelt, was einen neuen Pairing-Prozess auslöst und dazu dienen kann, den Pairing-Prozess erneut mitzulesen.

Eventuell ist es nach dem alten Verfahren RST + Spoof möglich, ein Bluetooth Gerät auszuschalten und seine Verbindung zu hijacken?

Bluetooth-Sniffer, die den gesamten Pairing-Prozess, also auch die Layer unterhalb von L2CAP und HCI, mitlesen können, kosten derzeit mehrere tausend Dollar. Da stellt sich mir als Unwissendem in Sachen Firmware-Programmierung die Frage, ob es nicht möglich wäre, eine Open Source Bluetooth Firmware zu entwickeln, die neben dem Spoofen der Bluetooth-Adresse einen Sniffer beinhaltet und direkt das Bruteforce-Konzept mit in den Code gießt.

Directory Traversal via OBEX

Beim Schreiben dieser Zeilen kam über die „full disclosure"-Mailingliste eine Mail [14] in mein Postfach geflattert, die mitteilte, daß es auf einem ungepatchten MacOS X sowie diversen PDAs, wie z.B. dem HP Ipaq 2215, möglich sei, mit einer angepaßten btftp-Version von affix [15] aus dem Root-Verzeichnis eines OBEX FTP-

Servers auszubrechen und somit beliebig im Dateisystem rumzuhüpfen. Alles, was es dazu brauchte, waren die freundlichen Zeichen ../ und die Tatsache, daß es Hersteller gibt, die selbst OBEX FTP ohne Authentifikation erlauben.

Fazit

Die Zukunft wird wohl noch einige nette Spielereien in Sachen Bluetooth parat haben. Die Designer des Protokolls betonen nach wie vor, daß alle Angriffe lediglich Fehler in der Implementation, nicht aber im Design sind. Bei einem angreifbaren, auf einem unbekannten, gebrochenen Cipher basierenden Pairing-Prozess läßt sich über diese Aussage vielleicht langsam, aber sicher streiten. Dennoch steht für mich außer Frage, daß das Design von Bluetooth bei weitem robuster ist, als von manch anderem Protokoll, vor allem durch die Tatsache, daß nur die Firmware an die unteren Layer kommt.

Doch: Schön gedacht ist noch lange nicht schön gemacht!

Bluetooth sollte somit besser nur bei Bedarf angeschaltet werden, und man sollte peinlichst genau darauf achten, welchem Gerät man eine Verbindung gestattet.

Links

[1] *Trifinite.org*
[2] Bluetooth Hacking auf dem 21C3
[3] *http://www.spiegel.de/spiegel/0,1518,360077,00.html*
[4] *http://trifinite.org/Downloads/Blooover.jar*
[5] *http://www.chaostal.de/cgi-bin/parser.cgi?input=article/bluetooth*
[6] *http://ncsp.forum.nokia.com/download/?asset_id=11579;ref=devx*
[7] *http://trifinite.org/trifinite_stuff_blueprinting.html*
[8] *http://www.blog.de/main/index.php/hacking/2005/06/13/d_o_s_to_the_bluetooth_device*
[9] *http://www.holtmann.org/*
[10] *http://www.vs.inf.ethz.ch/res/proj/smart-its/dl/ROK_101_007_revR1C-HCI_ericsson_specific.pdf*
[11] *http://www.securityfocus.com/infocus/1834*
[12] *http://www.datenterrorist.de/devel/bluebuf.tgz*
[13] *http://www.eng.tau.ac.il/%7Eyash/shaked-wool-mobisys05/index.html*
[14] *http://www.datenterrorist.de/index.php?itemid=352*
[15] *http://affix.sourceforge.net/*

PSP Hacking

von TabascoEye <me@tabascoeye.de>

Ein kurzer Abriß über das, was die Playstation Portable, Sonys neue „handgehaltene Konsole“, alles kann – aber eigentlich nicht soll und wie es soweit kam. Hinweis: Der Artikel ist von den schnellen Entwicklungen der PSP Hacking Scene inzwischen teilweise überholt worden (siehe auch Updates am Ende des Artikels).

Hardware

Um den multimedialen Anforderungen an die PSP gerecht zu werden, kommt einiges an interessanter Hardware zum Einsatz. Als CPUs werkeln zwei MIPS R4000 in der schwarzen Hochglanzhülle. Die Kommunikation mit der Außenwelt findet über eine Vielzahl von Schnittstellen statt, WLAN(802.11b), USB, IrDA. Als Speichermedien werden Sonys Memory Stick PRO Duo und das eigens entwickelte Format UMD (Universal Media Disc, von der Größe einer Minidisc mit abgerundetem Caddy) benutzt. Die UMDs fassen bis zu 1,8GB (dual layer) und sind keineswegs so „universal“, wie ihr Name suggeriert, sondern ein proprietäres Format, das Sony speziell mit der PSP und dem Verkauf von UMD-Filmen pushen will. Nachdem mehrere Gruppen es geschafft haben, die UMDs zu dumpen, scheint allerdings sicher zu sein, daß es sich einfach um „kleine” DVDs handelt, ISO9660 formatiert.

Main CPU MIPS R4000 "Allegrex" 1-333Mhz
Media Block MIPS R4000 1-333Mhz
32MB DDR SDRAM (8MB kernel reserved)
32MB NAND Flash Memory
4,3" TFT, 480x272 Pixel (16:9)
USB 2.0 Mini-USB-B-Female
802.11b, IrDA, Memory Stick, UMD
1800mAh 3,6V Li-Ion Akku

Firmware 1.00 und "Hello World"

Bei all den Features wittert der geneigte Chaot bereits viel Platz für seinen Spieltrieb, jedoch hat sich Sony dagegen diverse Schikanen ausgedacht. Die wichtigste dabei ist eine AES 128bit Verschlüsselung der Firmware und der UMDs, wobei beides offensichtlich nicht ordentlich umgesetzt wurde. Denn bald nach dem japanischen Release mit der Firmware-Version 1.00 stellte sich heraus, daß diese quasi nicht abgesichert war. Der Exploit bestand darin, das Update auf Firmware 1.50, die zwischenzeitlich erschienen war, zu entpacken und die Datei `DATA.PSP` durch ein eigenes ELF-Binary zu ersetzen. So gab es im Mai dieses Jahres das erste “Hello World” auf den PSPs der Version 1.00. Damit brach die „Homebrewszene“ los, und schon im Juni gab es das erste inoffizielle PSP-SDK[1], das immer noch weiterentwickelt wird.

USA Release, Firmware 1.50, 1.51, 1.52

Sony versuchte, das Interesse an Homebrew klein zu halten, indem sie weiter für den Patch auf 1.50 warben und die PSP in den USA gleich mit Firmware 1.50 auslieferten. Im Juni veröffentlichte die spanische Gruppe PSP-DEV den sogenannten „Swaploit”, um eigene Software auch auf Firmware 1.50 laufen zu lassen. Der Trick funktionierte mit zwei Memory Sticks, die während des Ladens vertauscht wurden, um so die gewünschte Software zu starten. Am selben Tag brachte Sony ihr Update auf 1.52 heraus, welches sämtliche Löcher der Firmware stopft. Bis jetzt läuft Homebrew ausschließlich auf 1.00 und 1.50.

Der Swaploit war aber aufwendig, und man benötigte zwei Memory Sticks. Dieses Problem löste PSP-DEV mit „KXploit”, indem sie einen Bug im FAT der MemorySticks ausnutzten und so beide benötigten Teile auf einen Memory Stick schreiben konnten.

KXPloit und 1.50 Homebrew

Nach dem Hack erhält man zwei Verzeichnisse, FOLDER und FOLDER%. In FOLDER% befindet sich nun der Teil, der die Firmware täuscht, in FOLDER die eigentliche Software und alle Daten (z.B. ROMs). Durch diesen Trick entstehen allerdings Icons mit dem Schriftzug "Corrupt Data" im PSP Menü. Auch das läßt sich durch einen dirty-filename-Hack lösen, indem man die Verzeichnisse so umbenennt:

```
FOLDER                                  1

FOLDER~1%
```

Das sind 30 Leerzeichen. Der Trick funktioniert aber nicht bei jeder Applikation!

Europa Release und Firmware 2.00

Bis diese Ausgabe in Euren Händen liegt, haben wir das Release am 1. September vermutlich hinter uns. Bisher scheint klar zu sein, daß die PSP hier entweder mit 1.52 plus mitgeliefertem Update auf 2.00 per UMD oder direkt mit 2.00 ausgeliefert werden wird. Einige Gruppen haben angekündigt, bis dahin entweder einen Exploit für 2.00 oder einen Downgrade auf 1.50 zu ermöglichen. Erste Ansätze, Homebrew auf der neuen Firmware 2.00 zum Laufen zu bringen, sehen vielversprechend aus, anscheinend hat Sony sich selbst ein Bein gestellt und die Ausführung von unsigniertem Code im Verzeichnis PSP/UPDATE/ erlaubt...

Die Firmware bringt einige Neuerungen: unter anderem WPA und einen Browser. Allerdings ist das Browsen im Web mit der PSP schon länger und auch ohne 2.00 möglich, dazu weiter unten mehr.

Von Amiga bis Windows95

In der Zwischenzeit zeigte sich die Homebrewszene als äußerst kreativ und hat bis dato über 15 Emulatoren auf die PSP portiert, unter anderem: Amiga 500, Gameboy (Color/Advance), Genesis, MAME, NeoGeo, NES, PC Engine, SNES, Wonderswan und kürzlich sogar den x86 Emulator bochs. Damit läuft auch Linux und Windows95 auf der PSP (Bluescreens für unterwegs!).

Aber Emulatoren sind bei weitem nicht das einzige, was die Community zusammengehackt hat. Es gibt eine Vielzahl selbstentwickelter Spiele und Applikationen. Selbst Sonys Ängste vor Piraterie wurden inzwischen vollständig durch die Software fastloader erfüllt, die es erlaubt, Spiele-ISOs vom Memory Stick zu starten. Neue Software gibt es praktisch täglich, dazu siehe [2] [3] [4].

Websurfen ohne 2.00

Ein netter Hack, um die PSP ins WWW zu bringen, fand sich im Spiel Wipeout Pure. Eine

Spielfunktion macht das Herunterladen von neuen Rennstrecken, neuen Fahrzeugen und anderen Goodies möglich. Das Ganze funktioniert über eine Webseite, die genau wie der Rest des Spielmenüs aussieht. Der einfache Hack bestand nun darin, die Seite, auf die das Spiel zugreift, per DNS auf eine präparierte Seite mit URL-Adreßfeld zu leiten. Brauchbar dafür ist z.B. der DNS 61.171.70.72. Per Softwaretastatur lassen sich URLs eintippen.

```
// Hello World for PSP using PSP-SDK
#include <pspkernel.h>
#include <pspdebug.h>

PSP_MODULE_INFO("Hello World", 0, 1, 1);
#define printf pspDebugScreenPrintf
/* Exit callback */
int exit_callback(int arg1, int arg2, void *common) {
    sceKernelExitGame();
    return 0;
}

/* Callback thread */
int CallbackThread(SceSize args, void *argp) {
    int cbid;
    cbid = sceKernelCreateCallback("Exit Callback",
           exit_callback, NULL);
    sceKernelRegisterExitCallback(cbid);
    sceKernelSleepThreadCB();
    return 0;
}
/* Sets up the callback thread and returns its thread id */
int SetupCallbacks(void) {
    int thid = 0;
    thid =  sceKernelCreateThread("update_thread",
           CallbackThread, 0x11, 0xFA0, 0, 0);
    if(thid >= 0) {
       sceKernelStartThread(thid, 0, 0);
    }
    return thid;
}

int main() {
    pspDebugScreenInit();
    SetupCallbacks();

    printf("Hello World");
    sceKernelSleepThread();
    return 0;
}
```

Hands-On

Die Homebrewszene kämpft leider zur Zeit mit konkurrierenden Gruppen, die sich gegenseitig Code klauen und damit prahlen, als erstes diesen oder jenen Exploit herausgebracht zu haben. An Sourcecode kommt man selten, viele wollen wohl lieber k3wl sein, statt ihren Source zu veröffentlichen, damit jeder was lernen kann. Wer allerdings einsteigen und seine eigene Software schreiben will, findet ausreichend Informationen. Unter anderem bei [1] [5] [6] [7].

Ausblick

Wer weiß, was noch alles entwickelt und gebastelt wird. Und ungeahnte „Spaß am Gerät"- Möglichkeiten werden sich auftun, wenn erstmal die vielen angekündigten Goodies auf den Markt kommen. Wir sprechen hier von Kamera, GPS, Keyboard – alles USB. Bis dahin wird man sich mit dem zufriedengeben, was da ist. Aber auch mit der nackten PSP wurde schon viel gemacht, angefangen beim Serialport-Hack für den Kabelfernbedienungsstecker am Kopfhörerausgang, bis hin zum ins Gehäuse integrierten iTrip, einem UKW-Transmitter [8].

Und Linux nativ? Naja, es existiert ein PSP-Linux Projekt [9], aber es erscheint sehr inaktiv. Um Linux nativ laufen zu lassen, müßte man den verschlüsselten Kernel entladen und herausfinden, wie Details, so zum Beispiel die MMU, umgesetzt sind. Wenn man nicht einfach die Firmware wegflashen möchte, können neuerdings auch Speichermedien, bis hin zu USB-Festplatten, an den Memory-Stick-Slot angeschlossen werden. Dies ist, unbestätigten Gerüchten zufolge, bereits gelungen: ein Hacker soll sich dazu extra ein Interface gebaut haben.

Fazit

Daß die Playstation Portable mehr als eine Spielkonsole ist, sagt Sony selbst. Daß sie komplette Spielesammlungen aus alten Zeiten™ beherbergen wird, selbstprogrammierte Spiele von Entwicklern aus aller Welt, verschiedenste Tools und Applikationen, sogar andere Betriebssysteme – wenn auch nur emuliert – das hätte sich der japanische Mutterkonzern sicher nicht träumen lassen (von den ISOs mal ganz abgesehen). Also – kaufen und Spaß haben. Solange noch kein Exploit für 2.00 existiert, wird man sich wohl oder übel auf eBay umschauen oder selbst eine PSP importieren müssen. Sicher ist: Man benötigt einen möglichst großen Memory Stick.

Update

Die PSP ist in Europa gelandet, Firmware 1.52 und 2.00 auf UMD mitgeliefert. Die Gruppen arbeiten an Downgrades auf 1.50. Vielleicht ist aber auch bald direktes Ausführen von Software auf 2.00 möglich. Abwarten...

Update 2

Das erste "Hello World" für die PSP 2.0 ist aufgetaucht. Es funktioniert über eine PNG-Datei, die das Binary enthält und ausgeführt wird, sobald man sie öffnet. Haltet durch. Von hier aus kann es nicht mehr lange dauern, bis alle Homebrews auf 2.00 laufen.

Update 3

Es gibt einen funktionierenden Downgrader von 2.00 auf 1.50. Wer also auf die tollen Features von 2.00 verzichten möchte und stattdessen Homebrew nutzen will, sollte sich mal auf [2] oder [3] in den Download-Sektionen umschauen.

Update 4

Da die Aktualität dieser Ausgabe der Datenschleuder aufgrund der eingeschobenen Sonderausgabe zum ePass ein wenig hinterherhinkt und sich während des Sommers noch einiges getan hat, hat sich der Autor entschlossen, eine online gewartete Version dieses Artikels zu veröffentlichen [10].

Dort gibt es auch Neuigkeiten zum Thema.

Links

[1] http://ps2dev.org/
[2] http://www.pspupdates.com/
[3] http://www.psp-hacks.com/
[4] http://psp-news.dcemu.co.uk/
[5] http://www.pspupdates.com/lesson[01,02,03].htm
[6] http://www.pspbrew.com/wiki/
[7] http://wiki.ps2dev.org/
[8] http://badacetechshow.com/psp_itrip.htm
[9] http://www.psp-linux.org/
[10] http://www.tabascoeye.de/11/30/das_kleine_schwarze

Fnordlicht

von Alexander Neumann <fd0@koeln.ccc.de>

Auf der Suche nach der ultimativen Beleuchtung mußte ich leider feststellen, daß es so etwas nicht gibt. Deckenfluter und Schwarzlichtröhren sind ja fast schon Standard, also: Selbst ist der Nerd! Erstmal eine Liste machen! Was macht denn die ultimative Beleuchtung überhaupt aus?

Vorüberlegungen

Eine solche Lampe sollte sein:

- vollständig konfigurierbar,
- standalone zu betreiben,
- natürlich auch dynamisch ansteuerbar,
- über einen Standard-Bus in größeren Mengen adressierbar,
- nicht übermäßig teuer,
- ohne größeren Streß und Hardwareaufwand selbst zu löten,
- intelligent, und vor allem:
- tolle Farben erzeugen, je nach Laune.

Leuchtmittel

Als erstes galt zu überlegen, womit man eigentlich "Licht machen" will. LEDs sind toll für sowas: Sehr hell, geringer Stromverbrauch und günstig zu bekommen. Standard-LEDs haben jedoch meistens eine Helligkeit von etwa 20–50 mcd (Milli-Candela), das ist für Beleuchtungszwecke arg dunkel (oder man müßte viele LEDs nehmen, und das wäre dann wieder nicht billig und ziemlich aufwendig zu löten). Mittlerweile gibt es aber auch hellere LEDs mit 5000–7000 mcd, die nicht viel teurer sind. Einziges Manko: Der Abstrahlwinkel beträgt nur 20 Grad. Dies stellt mit einem ordentlichen Diffusor kein größeres Problem dar, aber dazu später mehr.

Farbe

Mit dem RGB-Farbraum und additiver Farbmischung läßt sich ein großer Teil der für den Menschen wahrnehmbaren (und schönen!) Farben erzeugen. Dabei wird einfach mit den drei Grundfarben Rot, Grün und Blau in jeweils verschiedenen Helligkeiten eine möglichst weiße Oberfläche beleuchtet. Die Farbe Weiß ergibt sich bei gleicher Helligkeit aller drei Farben, Schwarz durch die Abwesenheit von Licht. Dies funktioniert natürlich am besten ohne jegliche Beleuchtung von außen, sprich: nachts. Aber das ist ja durchaus gewollt, deckt diese Zeit doch den Hauptlebensrhythmus des gemeinen Nerds zufriedenstellend ab.

LEDs lassen sich nicht wie normale Glühlampen über die angelegte Spannung dimmen, deshalb läßt man die LEDs flimmern und dimmt über das Verhältnis von Einschaltzeit zu Ausschaltzeit (PWM, Pulsweitenmodulation). Damit dieses Geflacker nicht beim Arbeiten stört, benutzt man einen Basistakt von 100Hz, der über der vom Auge wahrnehmbaren Flackerschwelle liegt. Ein Takt dauert also `1/(1*10^6) s=0.1 ms`. Da das Auge ein Problem mit gepulsten LEDs hat (diese werden heller empfunden, als sie der Photonenausbeute nach sind), ist das Verhältnis zwischen gewünschter Helligkeit (H) und Einschaltanteil (E) in einem solchen Takt leider nicht linear, sondern $H \sim E^g$ ($0 \le H \le 1$, $0 \le E \le 1$), wobei g für die Gamma-Korrektur steht. Probieren hat gezeigt, daß g=2 gut funktioniert.

Prozessor

Ich habe mich entschieden, einen Atmel Atmega8 als Prozessor zu benutzen. Dieser Prozessor hat mehrere Features:

- Systemtakt bis 16MHz,
- 8Kb Flashrom,
- 1Kb RAM,
- 512 Byte EEPROM,
- mehrere Timer,

- Interrupts für alle Ereignisse,
- Hardware für Kommunikation via RS232 und I2C,
- geringe Baugröße (28Pin DIL-S Gehäuse),
- günstig (in der Regel um 2,70 EUR bei Reichelt).

Da die in diesem Prozessor eingebaute Hardware-PWM mit 10Bit eine zu geringe Auflösung für 256 „echte" Helligkeitsstufen hat, habe ich mich entschlossen, die PWM in Software selbst zu realisieren.

Bilder von cefalon

Software

Taktet man den Atmega8 mit 16MHz, dauert die Ausführung einer Instruktion (also die minimal mögliche Zeit zwischen einer Ein- und einer Ausschaltphase) `1/(16*10^6)` Sekunden. Einen PWM-Basistakt von 100Hz (also 100 PWM-Takte pro Sekunde) vorausgesetzt, bleiben von diesen `16*10^6` Zyklen pro Sekunde noch `16*10^6/100 = 16*10^4 = 160000` Zyklen für einen PWM-Takt übrig. Nun zeigt sich das nächste Problem: Der Atmega8 ist eine 8Bit CPU und hat nur einen einzigen 16Bit Timer, aber bereits ab einer Helligkeit von `164/256` ist die Anzahl der Takte, in der die LEDs eingeschaltet sein müssen, `(164/255)^2*160000 ≈ 66180`, was nicht mehr mit einem 16Bit breiten Register erfaßbar ist.

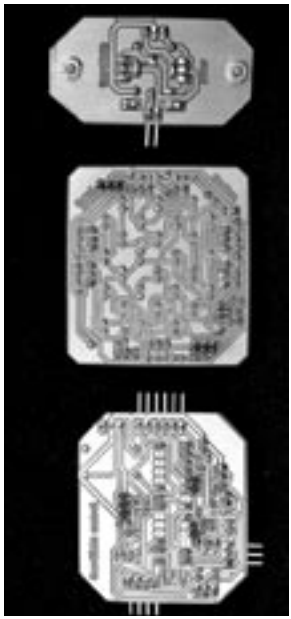
Dieses Problem kann man umgehen, indem nicht die Anzahl der Zyklen vom Einschalten der LEDs bis zum Ausschalten gezählt wird, sondern die Anzahl der Takte zwischen zwei Helligkeitsstufen. Man läßt also den Prozessor mit Interrupts von Zeitschlitz zu Zeitschlitz hüpfen. Wegen der Gamma-Korrektur wird diese Zeit immer länger, ist aber zu jeder Zeit kleiner als 65535 (maximale Anzahl Takte, die der 16Bit Zähler erfassen kann). Die maximale Zeit liegt natürlich zwischen Helligkeit 254 (fast die ganze Zeit eingeschaltet) und Helligkeit 255 (die ganze Zeit eingeschaltet): `160000-(254/255)^2*160000 ≈ 1252`).

Der Atmega8 kann so programmiert werden, daß der 16Bit-Timer ein Register inkrementiert und in einen Interrupt springt, sobald ein voreingestellter Wert erreicht wird. Dies will ich nutzen, um den Status der LEDs zu ändern. Nach dem Sprung in einen solchen Interrupt ist also zu testen, ob eine Statusänderung bei einer der drei Farbkanäle notwendig ist. Wenn ja muß sie ausgeführt werden, anschließend muß der zu erreichende Wert für den nächsten Timerinterrupt geladen werden.

Jetzt haben wir wieder ein Problem: Die Zeit zwischen zwei Zeitschlitzen ist für diese Dinge bis etwa zur Helligkeit 15 zu kurz (der Abstand zwischen dem Zeitschlitz für Helligkeit 0 und 1 beträgt 2 Takte). Dem kann man zum einen durch vorheriges Berechnen der auszugebenden Werte und zusätzlich durch Zusammenfassen der ersten 16 Zeitschlitze zu einem einzigen Interrupt begegnen. Ersteres bewirkt, daß im Interrupt nur noch ein Byte aus dem Speicher in das Ausgaberegister kopiert werden muß. Genug Zeit ist zum Beispiel im letzten Zeitschlitz.

Statische Scripte

Feste Abläufe sind relativ einfach einzubauen: Eine Anweisungskette, bestehend aus einem Byte, welches wiederum aus dem Opcode (höherwertiges Nibble) und Flags (niederwertiges Nibble) zusammengesetzt ist, sowie einem oder drei Bytes Daten, ist schnell implementiert. So kann das Fnordlicht bereits jetzt einfache Scriptabläufe (z.B. „setze Farbkanal R auf Helligkeit X", „fade bis Farbe XYZ und warte darauf, dann springe an den Anfang zurück") aus dem Flash-Rom ausführen.



Ansteuerung

Nach obiger Zielsetzung soll eine Lampe sowohl standalone als auch im Kollektiv zu betreiben sein. Eine einzelne Lampe ist mit dem geringsten Hardwareaufwand seriell anzusteuern, eine Gruppe von Lampen eher per I2C. Der Atmega8 hat da gleich Hardware eingebaut, so daß man sich (von der Lampenseite aus) darauf beschränken kann, die eigene Adresse zu setzen und anschließend auf den entsprechenden Interrupt zu reagieren.

Im Endausbau soll es möglich sein, die Lampe komplett über I2C fernzusteuern, die serielle Schnittstelle wird zur Zeit nur zum Debuggen der Firmware benutzt. Der Fokus wird auf dem Bus zur Ansteuerung liegen, da ja die Beleuchtung von Räumen, also Installationen von mehreren Lampen, im Vordergrund stehen. Die Integration der Kommunikationsschnittstellen in die Scriptsprache („sende Byte X an Lampe Y" oder „warte auf Byte Z"), als auch das Ausführen von Scriptbefehlen aus einem Fifo, das von Extern befüllt wird, sind geplant.

Mailingliste

Da jedes noch so kleine Projekt eine Mailingliste haben muß, hat dieses natürlich auch eine, die Adresse ist *fnordlicht@koeln.ccc.de*.

Mäusejagd

von HomeshopperZ <ds@ccc.de>

Der folgende Artikel wurde der Redaktion anonym zugeleitet. Er wird hier nicht veröffentlicht, um zur Nachahmung anzuregen, sondern um auf ein Problem von Hotline-Services hinzuweisen, das sich insbesondere ergibt, wenn Callcenter-Mitarbeiter nicht genügend geschult sind. Er zeigt, daß Produktidentifikationsnummern wenig Sicherheit bieten. Feedback bitte an die Redaktion <ds@ccc.de>.

Der Fall, daß mal eine Maus, das wohl am häufigsten genutzte Peripheriegerät am Rechner, kaputt geht, ist ja nichts besonderes. Die gute Firma Microsoft bietet für ihre Mäuse vom Typ *Explorer* eine geradezu sagenhafte Garantie von 5 Jahren – bei dieser, gerade in den ersten Versionen von Kabelbrüchen geplagten Maus, auch nicht schlecht. Vor einiger Zeit ging dann auch uns eine uralte *Explorer*-Maus kaputt – also ran an das Telefon und die Microsoft-Hotline beglücken (allgemeine Hotline: 01805-251199, Nachforschungen ergaben, daß ein direkter Anruf bei 01805-672255 viel stressiges Rumgefrage erspart).

Nach ein wenig Geplauder sagte man uns dann: „*Ja, in ein paar Tagen haben Sie dann eine neue. Leider können wir Ihnen aber nur das aktuelle Modell, die Intelli Explorer 4.0 schicken.*“ Neuerdings taucht übrigens ab und zu mal der Satz: „*Die alte Maus schicken Sie uns dann zurück – Modalitäten stehen auf dem Beipackzettel.*“ auf. Merke: Man tauscht also eine knapp 5 Jahre alte Maus gegen ein aktuelles Modell aus.

Schon zwei Tage später war das aktuelle Modell in der Post. Zu unserem Erstaunen stand da absolut nicht von „Schicken Sie die alte zurück“. Also haben wir das auch nicht gemacht. Doch diese Verfahrensweise weckte unseren sportlichen Ehrgeiz.

Schon am nächsten Tag starteten wir den Versuch, mit der Seriennummer der neuen Maus wieder einen Garantiefall vorzutäuschen. Zu unserem Erstaunen hatten wir schon 2 Tage später ebenfalls eine neue Maus – wieder ohne Rücksendeaufforderung. Der nächste Versuch war dann, mit der alten Maus nochmal eine neue zu beschaffen – auch dies lief ohne weitere Probleme. Weder eine Nachfrage seitens der Mitarbeiter, noch auch nur ein Hauch von Rücksendescheinen. Endgültig überzeugt, kam uns die Idee, doch mal zu versuchen, ob das auch bei den kabellosen Bluetooth-Mäusen aus dem Hause Microsoft geht. Wir hatten nämlich gelernt, daß die Worte Kabelbruch und Wackelkontakt offensichtlich essentiell waren, um den Gegenüber von der Echtheit des Falles zu überzeugen. Auch bei der Bluetooth-Maus: Weder eine besondere Nachfrage, noch sonst etwas – „Wir senden Ihnen eine neue zu“.

Offensichtlich kann auch ein Bluetooth-Kabel einen Kabelbruch haben! Gesagt – getan, schon hatten wir neue Bluetooth-Mäuse. Seriennummern (oder sollte man direkt Bestellnummern sagen?) gibt es ja schließlich gut sichtbar auf der Rückseite der Originalverpackung. Einfach zum Mediamarkt oder Saturn – Anruf genügt und die Maus wird frei Haus geliefert – Teleshopping mal anders!

Es ist völlig klar, daß ein Rücksenden der alten Mäuse wohl teurer kommen würde, als einfach eine neue zu verschicken. Die niedrigen Produktionskosten unterschreiten offensichtlich den Aufwand, die zurückgesendeten Teile auszupacken und zu entsorgen, bei weitem. Allerdings geben wir zu bedenken: Rechtens ist unser Verhalten mit Sicherheit nicht – Betrug ist nach wie vor nicht legal. Trotz alledem bedanken wir uns bei Microsoft!

Sicherheitsstandards und die Umgehungstechnik

Johannes vom Fluss

Ein Kunstsportler der Umgehungstechnik ist jemand, der sich mit den Geheimnissen und Rätseln von Sicherheitssystemen auseinandersetzt und versucht, sie zu umgehen. Seine Motivation ist die Freude des Entdeckens und Erforschens, sein Mittel die Auswertung aller ihm zur Verfügung stehenden Informationen. Bei seinen Bemühungen steht ihm ein nicht zu unterschätzendes Hilfsmittel zur Verfügung: der Standard für Sicherheitstechnik.

Der Standard für Sicherheitstechnik orientiert sich an den Empfehlungen der Landeskriminalämter und den Vorgaben des Verbandes der Schadensversicherer. Die Voraussetzung zur Erfüllung dieses Standards durch eine Sicherheitsanlage ist die Sicherung gegen Überwindungs- und Umgehungsmethoden. Überwindungsmethoden zerstören die Sicherheitsanlage, Umgehungsmethoden (wie der Name schon sagt) umgehen sie zerstörungsfrei.

Sicherheitsstandards haben den Vorteil der Kompatibilität der verschiedenen Elemente von unterschiedlichen Herstellern von Sicherheitssystemen. Sie legen die Parameter fest, die zur Massenfertigung notwendig sind. Gleichzeitig bilden sie ein Kommunikationssystem verschiedener Interessengruppen zu einem Thema. Zum Beispiel darüber, welche Verpflichtungen eine Versicherung, ein Versicherter und der Hersteller eines Sicherheitssystems gegenseitig zu erfüllen haben. Sie ermöglichen die differenzierte Zugangs- und Zugriffskontrolle zu gesicherten Räumen oder Informationen. Je komplexer ein Sicherheitssystem ist, desto einfacher sind die Mittel zu seiner Überwindung, desto höher ist sein Sicherheitsstandard? Der Sicherheitsstandard will graduell diejenigen Zerstörungs- und Umgehungstechniken ausschließen, die bis zum Zeitpunkt seiner Normungsfestlegung (Standard) bekannt sind.

Der Standard für Sicherheitssysteme faßt den technischen Wissensstand zu einem bestimmten Zeitpunkt zusammen. Er versucht, die bis zu seiner Festsetzung bekannten Umgehungs- und Überwindungsmethoden auszuschließen. Allerdings entwickeln sich nicht nur die Sicherheitstechnik, sondern auch die Umgehungs- und Überwindungsmethoden ständig weiter: Der Standard für Sicherheitssysteme muß also in regelmäßigen Abständen neu festgelegt werden.

Da jedes Sicherheitssystem seine Grenzen hat, überwindbar oder umgehbar ist, wird durch Standards versucht, auch die Zeitspanne festzulegen, die notwendig ist, um es zu enträtseln. Er deckt aber nicht das gesamte Spektrum der Sicherheit ab. Er kategorisiert sie lediglich je nach Ziel der Sicherung. Je wertvoller das zu sichernde Gut ist, desto wichtiger ist ein hoher Standard des Sicherheitssystems. Je umfassender ein Sicherheitssystem ist, je mehr Funktionen es hat (beispielsweise bei einem Schloß: die Sicherung gegen Aufbohren oder Ziehen des Kerns), desto höher ist sein Sicherheitsstandard. Demnach liegt der Sicherheitsstandard eines Postkastens unter dem eines Tresors, dessen Sicherheitsstandard aber wiederum weit unter dem von Fort Knox.

Dem Umgehungstechniker gibt der Standard Hinweise darauf, wie ein Sicherheitssystem konstruiert sein muß. Durch die Kombinati-

on von Massenfertigung und Massengebrauch entstehen einerseits Fertigungstoleranzen im System, die zur Umgehung genutzt werden können, andererseits läßt die Ähnlichkeit des einzelnen Massenproduktes Rückschlüsse auf andere Sicherheitssysteme gleicher Fertigung zu. Die Kenntnis der Konstruktion eines Sicherheitssystems ermöglicht immer Schlußfolgerungen über dessen Umgehung. Das Wissen über die durch den Standard festgelegte Technik des Systems gibt dem Umgehungstechniker Hinweise auf Beschaffenheit, Toleranzen und Ansprechbarkeit. Dieses Wissen ist ihm eine große Hilfe.

Der Umgehungstechniker hat vielfältige Möglichkeiten, sich über Standards zu informieren. Wenn es in seinem Interesse liegt, ein historisches Schloß zu umgehen, wird er Polizeiberichte über Einbruchstechniken aus der Zeit des Schlosses lesen und Museen besuchen, um Schlösser ähnlicher Bauart zu sehen. Er kann sich auch mit alten Gesetzestexten, beispielsweise Zunftrechten der Schlosserzunft beschäftigen, um festzustellen, welche Techniken (wie die Anfertigung von Ton- oder Wachsabdrücken von Schlössern) verboten waren. Diese Verbote erlauben ihm einen direkten Rückschluß auf erfolgreiche Umgehungstechniken. Ein anderer Weg der Informationsbeschaffung ist das Studium von überall erhältlicher Fachliteratur über Kriminal-, Sicherheits- und Konstruktionstechnik. Nicht zu vergessen sind frei zugängliche Patentschriften.

Das Wissen um die Konstruktion eines Sicherheitssystems kann der Umgehungstechniker auch direkt von dessen Hersteller erhalten: Bei Fachmessen, in Internetforen der Branche, durch Werbung oder Produktbeschreibungen werden ihm die aktuellen Standards detailliert und leicht verständlich nahegebracht. Da aber ein Schloßhersteller in seinen Dokumentationen und Konstruktionszeichungen verständlicherweise wichtige Details verschweigt, interpretiert der Kunstsportler sie mit Vorsicht. In diesem Fall bleibt ihm nur die manuelle Demontage der ihm rätselhaft erscheinenden Schlösser.

Außerdem bleibt dem Umgehungstechniker noch der Erfahrungsaustausch mit Gleichgesinnten, bevorzugt bei geselligen Sportabenden oder Stammtischen der in verschiedenen Städten Deutschlands existierenden Sportgruppen.

Sicherheitssysteme werden wissenschaftlich entwickelt, also kann der Umgehungstechniker wissenschaftliche Methoden nutzen, um sie zu umgehen. Er arbeitet über Rückschlüsse: Wenn er physikalische Parameter und die Technologie eines Sicherheitssystems kennt, kann er dessen Schwachstellen definieren und an ihnen ansetzen, um eine geeignete Strategie der Umgehung zu entwickeln. Mit seinem theoretischen Wissen über Konstruktionstechnik kann er die Informationen, die ihm ein Sicherheitssystem während der Manipulation gibt, einordnen und auswerten. Sobald zu einem in Massenfertigung entstandenen Sicherheitssystem die entsprechende Umgehungstechnik entwickelt wurde, sind alle Systeme der gleichen Bauart umgehbar.

Wenn der Umgehungstechniker beispielsweise an einem Schloß frisches Öl riecht, kann er dadurch auf dessen Schwer- oder Leichtgängigkeit schließen.

Der Standard eines Sicherheitssystems wird als Norm für dessen Konstruktion festgelegt. Er definiert also seine Herstellungs- und Funktionsweise und die Anforderungen, die daran gestellt werden. So kann man von den Anforderungen an ein Sicherheitssystem auf seine Konstruktion schließen: Eine Brandschutztür des Standards T 30 bietet einen Brandwiderstand von 30 Minuten und hält einer Temperaturbelastung von 821 Grad Celsius stand, was auf die Wahrscheinlichkeit der Verwendung bestimmter branchenüblicher Materialien hinweist.

Ein anderes Beispiel für die Umgehung von Sicherheitssystemen durch die Auswertung von Informationen sind Generalschließanlagen. In einem großen Betrieb mit einer Generalschließanlage haben verschiedene Personalgruppen verschiedene Zugangsrechte. Das bedeutet für das Schließsystem, daß es mehrere Zugangsvarianten beinhalten muß, z. B. Schlüssel für nur

eine Tür, für alle Türen einer Abteilung oder sogar für alle Türen im ganzen Betrieb. Wichtige Menschen wie Putzfrauen oder Generaldirektoren müssen zu allen Bereichen Zugang haben, ein einfacher Sachbearbeiter benötigt nur den Schlüssel zu dem Büro, in dem er arbeitet. Es gibt also bei Generalschließanlagen nicht nur eine Möglichkeit des Öffnens, sondern mehrere. Diese verschiedenen Möglichkeiten stehen auch dem Umgehungstechniker zur Verfügung, wenn er das Wesen von Schließanlagen kennt.

Abschließend stellt sich die Frage, was gesichert wird und warum. Gesichert werden sollen Besitz, Eigentum, Privatsphäre und Information. Sicherheit ist der Wunsch nach virtueller Anwesenheit im verschlossenen Raum, gekoppelt mit dem Bedürfnis, daß sich nichts verändert, daß der gesicherte Raum statisch bleibt, daß in diesem Raum keine Zeit vergeht.

Der Ingenieur Friedrich Werner Schlegel schreibt in seiner Kulturgeschichte der Türschlösser:

„Schlösser sind notwendige Zubehörteile zu Raumabschlüssen, zu Türen, die einen umbauten Raum erst zur Behausung werden lassen, in der sich ein Mensch geborgen fühlen kann. Das Schloss ist zugleich eine Defensivwaffe gegen die Unzulänglichkeit der Menschen, die Mein und Dein nicht unterscheiden können. Mit dem Schloss, dem Raumabschluss gewann der Mensch die Freizügigkeit, seine Habe, seinen Besitz und seine Behausung zeitweise verlassen zu können und sie dem Schutz der Schlösser anzuvertrauen. Das Schloss bietet also in erster Linie eine Befriedigung des dem Menschen angeborenen Sicherheitsbedürfnisses."
(Schlegel 1963, Seite 12)

Also liebe Kunstsportler nicht verzagen, denn *„Offen ist gut, aber schneller offen ist besser!"* Zitat nach Arthur Meister, „Sportsfreunde der Sperrtechnik Hamburg".

Smudo, Blinkenkisten und Milchkaffee an der Rakete

von Julia Lüning <julia@devcon.net>

Noch nie war das Hackcenter so schön und noch nie hat mich jemand im Hackcenter gefragt, wo man denn hier bezahlen könne. Nun ja, Camp Discordia [1] war anders. Es war Teil von „Berlin 05 - Festival für junge Politik" [2], das im FEZ Wuhlheide [3] stattfand und an dem über 10.000 politisch interessierte Jugendliche teilnahmen.

Attraktion des Festivals waren die Konzerte von Fanta4, Tocotronic und Stereo Total. Außerdem gab es Workshops, Vorträge, Podiumsdiskussionen im Hauptgebäude und das Camp Discordia in der Clubgaststätte des ehemaligen Pionierparks.

Statt Camping gab es für den CCC Underground-Club-Atmosphäre mit schicker Beleuchtung und Raumgestaltung, erdacht und realisiert durch die Künstler von Pyonen [4] und pentaklon [5], bekannt von den Chaos Communication Camps und der WTH.

"Wir wollen da Spaß haben."

...sagte Markus immer wieder bei den wöchentlichen Orgatreffen. Vor allem, wenn **wieder** ein TelKo-Unternehmen zugegeben hatte, daß es nicht zum FEZ Wuhlheide, dem ehemaligen Pionierpalast im Osten Berlins, liefern kann. Am Ende gab es 6 Mbit/s vom cbxnet [6] per Richtfunk vom Alexanderplatz. Eine überzeugende Technologie!

Nachdem das NOC die Internet-Grundversorgung im Camp Discordia sichergestellt hatte, gab es immer wieder überraschende Anforderungen der Veranstalter. So wurden mehrfach Leute mit „Das Pressezelt hat kein Netz!" aus dem Bett geworfen. Mit viel Flexibilität und noch mehr Netzwerkkabeln konnte das NOC auch diese Probleme im Laufe der Veranstaltung lösen. Da es bei Berlin 05 kaum kreative Techniknutzer gab, funktionierte das Netz durchgehend gut und die Bandbreite reichte für alle aus. So konnten die Spezialisten des NOC die Besatzung der „Fairy Dust"-Rakete noch mit Milchkaffee versorgen.

Das POC [7] war auch wieder dabei und hat das ganze Festival mit DECT-Netz versorgt. Erste Tat der freiwilligen Helfer von Berlin 05 war, ihr Telefon beim POC registrieren zu lassen. Da, wie gewohnt, das Telefon problemfrei funktioniert hat, sorgte die POC-Crew nach dem Aufbau hauptsächlich für den oben erwähnten

Spaß. So lud zum Beispiel das lustige Zugangsberechtigungssystem der Veranstaltung einfach zum Spielen ein. Vier verschiedene Stoffbändchen, sechs verschiedene Badges und zwei verschiedene Papierbändchen verwirrten das Sicherheitspersonal und machten eigene Erweiterungen mittels Farblaserdrucker möglich.

Großen Anteil an der Organisation und Durchführung vom Camp Discordia hatte artevent. Sie haben das Projekt angestoßen, die Clubgaststätte erst bewohn- und bespielbar gemacht und waren das Kommunikationsinterface zu den Visionauten und den Trägern von Berlin 05. Der CCC konnten sich also ganz auf das Programm des Camp Discordia und die Internetversorgung von Berlin 05 konzentrieren.

"Was interessiert eigentlich 16jährige?"

Voraussetzung für die Teilnahme des CCC an Berlin 05 war, daß uns niemand in die inhaltliche Gestaltung vom Camp Discordia hineinredet. Schön und gut – aber was hat der CCC politisch motivierten Jugendlichen eigentlich zu sagen?

Recherchen zur Technikkompetenz bei jüngeren Geschwistern ergaben, daß Durchschnittsjugendliche Email, InstantMessanger und WWW benutzen, fast alle ein Mobiltelefon haben und Filesharing schon lange nichts Besonderes mehr ist. Daran anknüpfend gab

es in den zwei Vortragssälen Alice (300 Plätze) und Bob (200 Plätze) insgesamt 23 Vorträge zu

- Auswirkungen und Rechtssituation von Filesharing
- Anonym Surfen, Email Verschlüsseln, Sicher Chatten
- Überwachung: Internet, Telefon, Mobiltelefon, RFID, Biometrie
- Außerdem: Informationelle Selbstbestimmung, Hacktivismus, Medienkompetenz, Blogs, Open Source, Geschichte und Ziele des CCC

Highlight war eine Podiumsdiskussion mit Smudo (Die Fantastischen Vier, FourMusic [8]), Janko Röttgers (Autor von "Mix, Burn, Rip - Das Ende der Musikindustrie" [9]), Markus Beckedahl [10] und Lutz Diwell über „Filesharing – Segen für Musik oder für ihre Industrie?"

Außer dem CCC waren auch die Wikipedia und die Berliner Lockpicker beim Camp Discordia dabei. Beide füllten je ein Zelt mit eigenen Workshops. In der Nacht von Freitag auf Samstag zeigten wir den Film "23". Freke Over und Tim Pritlove standen anschließend den Zuschauern Rede und Antwort.

"Wo kann man denn hier bezahlen?"

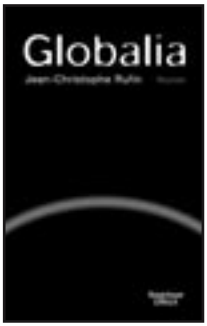
Einige Besucher verwechselten das Hackcenter mit seinen Public Terminals (geliehen von Apple, dem Lehrstuhl für Gesellschaft und Informatik der HU Berlin sowie aus dem cccb) mit einem Internetcafe und waren etwas verstört, als sie sich einfach so an die Computer setzen sollten. Trotzdem wurde das Angebot gut angenommen und die Kombination von Hackcenter, Bar und Sofaecke bot Raum für viele interessante Gespräche. Abends verwandelte sich das Hackcenter vom Camp Discordia dann in die tollste Bar auf dem Gelände. Es gab schickes Licht, elektronische Musik und Club Mate.

„Wir sniffen alles mit!" stand auf dem Beamer im Hackcenter und die Paßwörter und Bilder huschten Tag und Nacht über die Projektionswand. Die vom Congress bekannte Installation von EtherView [11] und dsniff [12] war Aha-Erlebnis und Gesprächsanstoß für viele Besucher. Die Demonstration des Möglichen war eine tolle Ergänzung zur Erklärung der Theorie in den Vorträgen.

[1] Berlin 05
Wiki: *https://berlin05.ccc.de/wiki/Camp_Discordia*
Weblog: *https://berlin05.ccc.de/blog/*
[2] *http://www.projekt-p.de/aktuell/147PGP,0,Berlin05.html*
[3] *http://www.fez-berlin.de/*
[4] *http://www.pyonen.de/*
[5] *http://www.pentaklon.de/*
[6] *http://www.cbxnet.de/*
[7] *http://www.eventphone.de/*
[8] *http://www.fourmusic.com/*
[9] *http://www.lowpass.cc/*
[10] *http://www.netzpolitik.org/*
[11] *http://denisx.dyndns.org/*
[12] *http://naughty.monkey.org/~dugsong/dsniff/*

Drei Buchtips: Global im Netz der inneren Sicherheitsmafia

von padeluun <padeluun@ccc.de>



Mehr Bücher lesen! Denn: „Dummheit allein genügt nicht“, heißt es in George Orwells Roman „1984“. Dieser wird auch herangezogen, wenn es auf dem Klappentext zu dem Buch des „Ärzte-ohne-Grenzen“-Mitbegründer Jean-Christophe Rufins „Globalia“ heißt: „Alles in Globalia ist perfekt. Und alles ist falsch“. Globalia steht für die westliche Welt.

Terroranschläge werden vom Gesellschaftsschutz geplant und durchgeführt – eine Vorstellung, die verschwörungstheoretisch geschulten Hackern bekannt vorkommen mag. Innerhalb Globalias gibt's die perfekte Schilyokratie – pardon – Demokratie; Politiker sind Schauspieler und der Geldadel hat die Fäden der Marionetten und der Macht in der Hand. Die Menschen werden an der Nase herumgeführt. Der moderne Planet ist ein Land ohne Grenzen, ohne Kriege. Das Alter ist abgeschafft, die Vergangenheit ebenfalls. Die Menschen sind rundum versorgt. Alles in Globalia ist erlaubt – bis auf Authentizität. Das Buch ist literarisch sicherlich kein Highlight, aber als ein Geschenk für Anfänger im Bereich „freies, selbstbestimmtes Leben” allemal ein guter Tip.

Ein ganz anderes „Stöffche“ ist da Christiane Schulzki-Haddoutis Buch „Im Netz der inneren Sicherheit“. Akribisch listet sie die Aushebelung der Bürgerrechte auf. Sie beschreibt Techniken, die der täglichen Überwachung dienen und plädiert für eine Besinnung auf eine Zivilgesellschaft, die aus sich heraus ihre Probleme bewältigt, ohne in ein totalitäres System abzugleiten. Ein Buch für Fortgeschrittene, das auf keinem Politikerschreibtisch fehlen sollte.

Der Schwede Pär Ström setzt ein Level tiefer an, beschreibt aber die weiten Kreise einer allumfassenden Überwachungsgesellschaft ebenso deutlich. Private Videoüberwachung in den USA ist genauso Thema wie Echelon und DoubleClick. Und er zeigt kleinere Auswege. Ein Beispiel: Eltern täten gut daran, ihren Kindern gewöhnliche Namen zu geben. Gibt's für den Namen „Ann-Christin Schmidt“ bei Google gerade mal 30 Treffer, so kann eine „Petra Schmidt“ im Schutz von über 30.000 Frauen mit dem gleichen Namen untertauchen. Wer sich einmal rundum ins Thema einlesen möchte, ist mit diesem Buch sicher gut beraten.

Jean-Christophe Rufin: Globalia,
Kiepenheuer & Witsch, Februar 2005,
ISBN: 3462034715, 22,90 EUR

Christiane Schulzki-Haddouti: Im Netz der inneren Sicherheit,
Europäische Verlagsanstalt, September 2004,
ISBN: 3434505822, 14,90 EUR

Pär Ström: Die Überwachungsmafia,
Hanser Wirtschaft, März 2005,
ISBN: 3446229809, 19,90 EUR

Antennenwald bei Frankfurt, siehe Artikel im Heft
(Satellitenbild: Google-Maps)

22nd Chaos Communication Congress
The European Hacker Conference
27. | 28. | 29. | 30. December 2005
http://www.ccc.de/congress/2005

#88