die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club

Biometrie zum Anfassen.

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

#84

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 640236, D-10048 Berlin) >> donnerstags ab 17 Uhr http://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, Bad Waldsee, Basel, Bochum, Darmstadt, Dortmund, Dresden, Frankfurt am Main, Freiburg im Breisgau, Gießen/Marburg, Hanau, Heidelberg, Ilmenau, Mainz, Mülheim an der Ruhr, Münster/Osnabrück, Offenbach am Main, Paderborn, Regensburg, Stuttgart, Trier, Weimar, Wuppertal.

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. 84

Herausgeber *(Abos, Adressen, Verwaltungstechnisches etc.)*
Chaos Computer Club e.V., Lokstedter Weg 72, D-20251 Hamburg, Fon: +49.40.401801-0, Fax: +49.40.801401-41, <office@ccc.de> Key fingerprint: 0891 587D 8936 CB96 0EFE F4B0 B156 0654 617C AB8E

Redaktion *(Artikel, Leserbriefe, Inhaltliches, etc.)*
Redaktion Datenschleuder, Postfach 640236, D-10048 Berlin, Fon: +49.30.28097470, <ds@ccc.de> Key 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 *Tom Lazar, Dirk Engling*

Redakteure dieser Ausgabe
Tom Lazar <tomster> und Dirk Engling <erdgeist>

Autoren dieser Ausgabe
Volker Birk, Andy, Sascha May, Mario Manno, padeluun, Wetterfrosch, Alexander Bernauer, Alexander Taute, Starbug, Timon Schröter, Markus Schaber, Pylon, neingeist, Steini, Tim

Wer regelmässig ins Kino geht, dem wird aufgefallen sein, dass die Geschichte von immer ausgeklügelteren Zugangskontrollen eigentlich immer die Geschichte deren Überwinding ist. Eine lückenlose Dokumentation ihrer Niederlagen.

Seit James Bond werden Iridien verpflanzt. Seit Tom Cruise's Aufritt in Mission Impossible weiss man, wie man durch ganzköpfige Masken (menschliche oder elektronische) Gesichtserkennungen überlistet. Redford trickst in Sneakers Spracherkennungssoftware aus und in MacGyver hat kein Fingerabdruckssensor eine Chance gegen R. D. Andersons phantasievollen Methoden. In Gattacca wird ein Mensch sogar bis auf die Ebene des genetischen Fingerabdrucks nachgeahmt und der Protagonist überwindet spielend Blut-, Urin- und Haaranalysen. Da werden Finger abgeschnitten, Gewebeproben beschafft, heimliche Fotos gemacht, oder gar die hinter dem Sensor stehenden Systeme "gehackt", stets scheitern elektronische Barrieren am Erfindungsreichtum des menschlichen Geists.

Immer lässt sich das zu vermessende Objekt Mensch emulieren, in seine zu erfassenden Einzelmerkmale zerstückeln und fast beliebig in ein für die Erkennung stimmig genug erscheinendes Gesamtbild rekonstruieren.

Nichtsdestotrotz vergeht kaum eine Woche, in der nicht grossspurig behauptet wird, mit der Vermessung des Menschen würde eine drastische Verbesserung der Sicherheit für alle erdenklichen Anwendungen einhergehen.

Die Schlagzeilen: Biometrie in Ausweisen, Einkaufen mit dem Fingerabdruck, Massenspeicheltest, automatische Abgleiche mit der Verbrecherkartei mit Aufnahmen bei Grossveranstaltungen, Irisscans am Flughafen, sogar die Überführung von Einbrechern anhand unvorsichtig stehengelassener Flatulenzen.

Man kann seinen Computer bis auf Freigabe durch die Fingerabdruckmaus sperren, sein Zuhause mit Irisscannern vor unbefugtem Zutritt sichern, mit Unterschrifts- und Spracherkennung spielen und durch eine Locke vom Sohnemann Mami in arge Erklärungsnot bringen.

Doch während die Überwindbarkeit der Systeme den Experten in Rage oder Verzückung versetzt (von anderen, immer wieder gern beschrieben, Schwächen einmal abgesehen), kann sie für Otto Normalbürger zu ernstlichen Schwierigkeiten führen. Während die einen erst gar keine oder nicht ausreichende Merkmale mitbringen, geben andere diese zu bereitwillig weg. Und dabei sei nicht nur an zufällig am Glas oder Klinke hinterlassene Spuren gedacht. Es ist mittlerweile Usus, an der Schmuddelvideothek ums Eck genau die Merkmale in hochauflösend scannen zu lassen[1], mit denen man dank Schily demnächst bei der Ausreise erkannt werden möchte.

Während man bei seiner EC-Karte noch darauf achtet, sie nicht in jeden vorbeikommenden Schlitz zu schieben, wird es wohl noch eine Weile dauern, bis es in das öffentliche Bewusstsein dringt, wie wichtig es ist, das Recht an seinem Merkmal nicht allzu leichtfertig aufzugeben.

Auch die Bevorratung der Daten hat ihre Tücken. Selbst unter der Annahme, dass „Der Staat die Guten" und „die Firma mit der Datenbank™ die Integren" sind, hat uns auch das Kino gelehrt, dass das System niemals fehlerlos ist und schon ein manipulierter Eintrag gerade für den Helden zum Verhängnis werden kann.

Denn das grundsätzliche Problem ist und bleibt, wie bei jeder modernen Technologie, das übersteigerte Vertrauen in die komplexe Technik. Biometrie kann ein Hilfmittel sein. Sie sollte aber nicht den gesunden Menschenverstand ersetzen.

Solange man mit einem Flachbildschirm vor dem Gesicht am Grenzbeamten scheitert, kann sie sogar vor Terroristen schützen. *<erdgeist>*

[1] *http://www.welt.de/data/2004/09/08/329601.html*

Inhalt

Pornografie

mir ist es gerade wieder passiert, dass ich bei einer Suche zu einem völlig seriösen Thema auf ein pornografisches Foto unter der Rubrik Pictures in der Suchmaschine alltheweb.com gestoßen. Darf man euch so etwas schicken...

Aber klar. Keine Porno-Sammlung ist komplett.

und ihr sperrt das dann?

Sperren? Damit andere es nicht finden, und dann kann man es tauschen? Das ist doch unfair!

Es surfen auch Jugendliche und Kinder und ich finde so etwas erschreckend und krank. *<claudia>*

Oh, ach so. Du hast versehentlich an die falsche Adresse gemailt. Bitte versuch es stattdessen auf cdf@cfaith.va. <Volker>

zu: T-Hack in DS #83

Hallo, Klasse Arbeit!

Der Artikel beweist leider wieder mal die Herangehensweise der großen T-Com. (Wie es sich für einen Weltkonzern gehört, ist das mit Sicherheit auch auf andere übertragbar.)

Hervorragend ist die Dokumenation des Schriftverkehrs!

Dies zeigt einem detailiert den 'Stimmungs- und Richtungswechsel' vom großen 'T' am Ende. (Wenn ignorieren nicht hilft einfach drohen...)

Der letzte Brief an die Telekom hätte auch von mir seien können,daraus spricht die Enttäuschung für die Mühen der letzten 12 (!) Monate. Das beweist die Arroganz und Ingoranz dieser Firma gegenüber ihren Kunden; die nun wirklich nicht mehr zu übertreffen ist.

Über eine weitere Berichterstattung würde ich mich (und auch andere) sehr freuen. *<tschesch>*

ebenfalls zu: T-Hack in DS #83;

`es antwortet fdik`

Was ich dann aber nicht verstehe sind die Forderungen die Sie dann ihrerseits für den angeblichen Aufwand an die Firmen stellen.

Der CCC hat keinerlei Forderungen gestellt - er bietet auch keinerlei Dienstleistungen an.

Das ist Dirks Privatsache. Und Dirk hat das auch nicht im Namen des CCC, sondern als Aufwandsentschädigung für seine eigenen persönlichen Leistungen gestellt.

Wenn wir als CCC die Vorgänge veröffentlichen und dokumentieren, so dokumentieren und veröffentlichen wir selbstverständlich alles - das findet wohl auch Dirk OK, obwohl er sich von einiger Seite jetzt Kritik anhören muss für seine Forderung, seine Leistungen wenigstens zu honorieren, auch finanziell.

Natürlich sind desolate Zustände in einem Kundendatenbanksystem (das ich persönlich als schützenswertes Gut ansehe) dann doch ziemlich beunruhigend v.a. wenn es - zumindest aus meiner Sicht als Laie - so einfach erscheint diese einsehen zu können.

Es geht nicht nur um's Einsehen.

Die Systeme standen über ein Jahr lang sperrangelweit offen. Unter anderem wurde auch das System T-Pay darüber verwaltet. Man darf alle Transaktionen, die auf derart unsicheren Rechnern ausgeführt werden, als kompromittiert betrachten.

So sperrangelweit offen wie das System der T-Systems für die T-Com war, war dort mit an Sicherheit grenzender Wahrscheinlichkeit nicht nur Dirk unterwegs - der hat nur die T-Iekom angesprochen und versucht, das ganze zu regeln. Nachdem ihm das trotz langwieriger Verhandlung mit der T-Com nicht gelungen ist, haben wir uns entschlossen, das ganze zu veröffentlichen, damit was passieren muss.

Denn immerhin geht's nicht nur um Webseiten, sondern um die persönlichen Daten und das Geld (T-Pay!) von 250.000 T-Com-Kunden. Ein Jahr lang hat das anscheinend niemand "gejuckt".

Das ist der eigentliche Skandal.

Trotzdem ist eine Entschädigungsforderung für die freiwillig geleistete Arbeit in meinen Augen schon eher als peinlich bis beschämend anzusehen.

Das müssen Sie dann Dirk erklären - allerdings muss ich sagen, dass ich das nicht so sehe.

Haben Sie T-Iekom-Aktien? Sind Sie deutscher Steuerzahler? Dann überlegen Sie sich doch bitte: wo wäre Ihr Geld besser angelegt gewesen, bei den "Experten" von der T-Systems, die solch ein System gestalten, oder bei Dirk, dem schlecht wird, wie das System aussieht, und der deshalb der T-Com anbietet (selbstverständlich gegen Bezahlung!) das System in Ordnung zu bringen, oder wenigstens dabei mitzuhelfen.

Oder hat Dirk irgendeine Pflicht, überhaupt irgendwas zu tun? Er hätte sich genausogut aus der Affäre drücken können, indem er gelacht hätte und alles weitere abgehakt.

Oder ist Dirk verpflichtet, der T-Systems kostenlos Schulungen zu geben und die T-Com kostenlos mit Dienstleistungen zu versorgen? Ist da ein Honorar nicht eher angebracht?

Ich verstehe ehrlich gesagt immer noch nicht, warum die T-Com Dirk nicht sofort engagiert hat, und zusammen mit ihm die katastrophale Situation umgehend bereinigt. Das wäre meiner Ansicht nach das einzig sinnvolle und korrekte Vorgehen der T-Com gewesen.

Insofern ist der Begriff der scheinbaren Ethik wohl eher deplaziert.

Nein. Der CCC steht voll und ganz hinter der Hackerethik, und dies ist kein Lippenbekenntnis.

Und einen Hacker oder Computerexperten nach seinem Aussehen zu beurteilen (bzw. allg. Menschen) tun wahrscheinlich - leider - die meisten Menschen.

Viele tun das, ja. Viele vertrauen auch auf scheinbar seriöse Großunternehmen, weil die alles viel besser können. Und viele Menschen müssen hart lernen, wie die Realität leider aussieht:

T-Com Internet, das Mautsystem unter den Internetlösungen.

Warum arbeiten also dermassen fähige Leute wie Sie nicht in entsprechenden Unternehmen und entwickeln, testen etc. statt einem offenbar scheinheiligen "Ehrenkodex" so viel Zeit zu opfern.

Die allermeisten von uns tun das. Der CCC ist ein Verein. - Sind Sie in einem Sportverein, Musikverein, sonstigen Verein? Und trotzdem arbeiten Sie noch? ;-)

`Die Diskussion wurde fortgesetzt. Es war auch nicht die einzige Anfrage in diese Richtung, doch soll sie stellvertretend für andere hier abgedruckt stehen.`

Ebenfalls auf DS #83 Bezug nehmend:

Auf Seite 6 gibt es eine Meldung über Atomexplosionen. Die Bezeichnung ist schlicht weg schlecht. Es handelt sich wohl um Kritikalitätsstörfälle. *<xxx@gmx.de>*

Die Bezeichnung ist nicht von uns sondern steht so in der Kriminalstatistik des BKA bzw im Gesetz. Lies einfach Paragraph 307 StGB nach:
http://dejure.org/gesetze/StGB/307.html <Jürgen>

Wie wärs mit solchem Toilettenpapier beim Congress im BCC? *http://www.jinx.com/scripts/details.asp?affid=-1&productID=285*

Oder vielleicht mit "TCG" Bedruck, oder einem anderen solchen Wort, bei dem man sofort anfängt zu hyperventillieren und Magenschmerzen bekommt (natürlich begleitet von heftigen Schweißausbrüchen)? *<Denis>*

Sehr lustig, aber leider auch sehr teuer. Das müssten wir auf den Eintrittspreis aufschlagen, und das geht nicht. <Tim, Congressorga>

To: "XXX-Hotelverzeichnis"

Sehr geehrte Damen und Herren, gerne möchte ich Ihnen folgende URL für Ihre Seite 'Links' vorschlagen:

http://www.xx-hotelverzeichnis.de - redaktionell gepflegtes Hotelverzeichnis

XX-Hotelverzeichnis ist ein redaktionell gepflegtes Unterkunftsverzeichnis. Wir präsentieren den XX Besucher ausgewählte XX Hotels und Pensionen sowie weitere Informationen zur Stadt XX.

Danke recht herzlich, Redaktion XX-hotelverzeichnis.de

Sehr geehrter Herr Malinkskiy, gerne möchte ich Ihnen folgende URL für Ihre unverlangte Werbung vorschlagen:

http://www.dejure.org/gesetze/StGB - redaktionell gepflegtes Gesetzbuch

Das Strafgesetzbuch ist ein redaktionell gepflegtes Verzeichnis von Untaten. Es präsentiert dem Besucher ausgewählte und auch weniger ausgewählte Straftaten sowie weitere Informationen zu den Folgen bei Begehen gleicher.

Bitte belästigen Sie uns nicht erneut. Danke recht Herzlich. <kju - Redaktion mail@ccc.de>

Lehrreiche Konversation mit yy@gmx.de:

Wir, 20 Prüflinge suche dringen Prüfungsfragen für die Prüfung zum Industriefachwirt der IHK. im September 2004.

Wenn du mir eure Anschriften gibst, kann ich sie euch zuschicken (oder die Liste an die IHK geben, möge das Los entscheiden).

Wir konnten Sie bis uns bis heute nicht organisieren.

Ihr bekommt das Wissen in der Berufsschule und dem Betrieb "organisiert".

Überlegen wir doch mal was die Prüfung soll: Ihr sollt "beweisen", dass ihr einen gewissen Bildungsstand habt, der euch qualifiziert eine bestimmte Berufsbezeichnung zu haben. Wenn ihr Leute davon überzeugen könnt euch auf illegalem Wege Prüfungsunterlagen zu besorgen, ohne dass diese Leute einen Nutzen von haben, dann solltet ihr Gebrauchtwagenhändler werden, denn dann schafft ihr es auch Leuten kaputte Autos anzudrehen.

Könntet Ihr uns da weiterhelfen, oder kennt Ihr jemanden der das könnte.

Ja, sag "Hallo" zu deiner Hand. Sie wird das Buch halten welches die Informationen beinhaltet die du benötigst.

Helfen kann ich euch mit einem Ratschlag: Trinkt Club Mate. Das hält wach und man kann mehr lernen. Mit besten Grüßen nach Berlin, <Enno>

rm -rf

könntet Ihr helfen? Auf einem PC wurden diverse Dateien auf der Festplatte gelöscht, die nun wieder hergestellt werden sollen. Erwarte gern Eure Antwort. *<xxx@aol.com>*

Vielleicht stellt euch ja der Hersteller der Daten die Daten wieder her?

Oder der, ders geloescht hat? Mama hat immer gesagt, wers kaputt gemacht hat, muss es wieder heile machen.

Vielleicht kannst du das sogar aus dem Papierkorb holen?

Will sagen: deine Frage ist ein wenig unspezifisch, um sie hier so weitraeumig zu beantworten. Vielleicht geizt du einfach in einer weiteren Mail weniger mit Details. <erdgeist>

```
...eine weiter Mail kam - wie soll es anders
sein? - nicht.
```

Netz-Lotsen

Guten tag habe eine frage,wenn ich von einem die ip adresse habe,wie bekomme ich den passenden port dazu herraus??? *<yyy@aol.com>*

Was genau meinst Du mit "Port"? Den Einwahlport seines Providers, auch als "Host" bekannt? Oder den Softwareport seines Rechners, auf dem die Verbindung, deren IP Du siehst, läuft?

Ersteren findest Du mit "ping -a ipadresse" heraus. Letzteren kennt (hoffentlich) Deine Firewall. <Rainer>

Catch them while they're young

`Anfrage von <aaa@gmx.de>, einem Nachwuchshacker:`

Hallo lieber Computer Chaos Club ich stehe grade erst am Anfang meiner Karriere als Hacker (lerne gerade C++) und forsche momentan wie ihr...

Sei dir der Risiken bewusst: keine Freundin mehr, lange Haare, und nie mehr duschen ;)

...eigentlich im Zusammenhang mit der Warez Szene steht!

Hrmm..an sich: garnicht.

Also so wie ich diesen Begriff kenne ist die Warez Szene am (nicht immer legalen) Verbreiten und/oder Tauschen von kommerzieller Software beteiligt.

Solche Dinge werden vom Club nicht unterstützt. Viele der "Hacker"-Programme stehen eh unter der GPL, sind also frei. Somit besteht die Notwendigkeit auch nicht wirklich.

Ich konnte leider keine Informationen zwischen Euch und dieser Szene bisher finden doch ihr seit genauso Hacker wie sie und verfolgt die gleiche Ethik!

hrmm..die Ethik ist nicht ganz eindeutig definiert. Aber Hacker und Warez Menschen sind an sich zwei Gruppen, so wie der ADAC und Autoschieber in etwa. Bei denen ist die Gemeinsamkeit das Auto, bei uns das Netz/Computer/etc. - aber ohne, dass es wirklich miteinander zu tun hat.

Die Ursprünge der Hacker/Warez/Demoszene liegen wohl beieinander, aber das war vor meiner Zeit, da können andere sicher mehr zu sagen.

So würde mich nun interessieren welche Verbindungen ihr pflegt und vor allen Dingen wie Ihr zu ihnen steht und welche Einstellung Ihr habt.

"Wir" pflegen seitens des Clubs eigentlich keine Verbindung dahin. Wenn, dann wären es einzelne Mitglieder. Aber was die privat machen hat mit dem Club nichts direkt zu tun.

Pisastar des Monats

sers wollt fargen wohl mann das sicher ned fragt aber ich will das hacken lernen sicher schwirig aber könnt ihr mir vl tips geben oder links *<flash@xxx.at>*

Du hast vermutlich eine falsche Vorstellung von der Bedeutung des Begriffes Hacken. Lies:

http://koeln.ccc.de/c4/faq/index.html#NA0
http://koeln.ccc.de/prozesse/writing/artikel/hacker-werden.html
http://koeln.ccc.de/prozesse/writing/artikel/hacker-howto-esr.html <kju>

ttt@gmx.de quengelte:

ihr seid aber nicht sehr reaktionsfreudig oder? Wo muss ich denn das hinsenden damit da eine Reaktion kommt?

**reaktion* Wollte nur vermelden: email ist da und wird wahr genommen. Ich werde sie nachher nochmal lesen und verstehen und antworten :)*

An dieser Stelle verweist die Redaktion Datenschleuder auf https://www.ccc.de/faq/communication#questions

Amt für Lizenzfragen

[...] Deshalb meine Frage an euch als Betreiber des ccc.de - Servers: Besitzt ihr irgendeine Lizenz für diesen Server oder wisst ihr von der Existens einer solchen? Ich hoffe mein Vater wird euch als Experten akzeptieren. *<bbb@gmx.de>*

Für den Betrieb eines Webservers ist keine Betriebserlaubnis notwendig. Auch wenn dies prinzipiell auch gut und vernünftig so ist, mag man sich anbetrachts der Mengen an geknackter und mißbrauchter Server manchmal auch darüber ärgern.

Du brauchst auf jeden Fall also keinerlei "Lizenz", außer gegebenenfalls für das verwendete Betriebssystem und/oder die Serveranwendung. Höchstens ein SSL-"Zertifikat" könnte unter Umständen Sinn machen, damit kannst Du sicher (verschlüsselt) Webseiten anbieten. <kju>

Die Nacht der denkenden Drucker

hallo, hab vor längerer zeit ein faszinierend erschreckendes erlebnis gehabt, und ich glaube ihr seid die richtige adresse, an die ichz mich wenden kann. ich (eigentlich wir) kauften damals einen neuen hpdeskjet 3816 und um die druckqualität zu prüfen scannte ich in guter sehr qualität (hohe auflösung) einen funfzig eurscheinchen und als ich beim ausdrucken zusah brach der drucker plötzlich ab mit seinem eigentlichem auftrag und schrieb eine internetadresse unter das halbfertige bild, die mich zu einer internationelen homepage führte die mir sagte was man machen darf und was nicht!!!! das muss man sich mal verallgegenwärtigen, wenn alles geprüft wird was geruckt wird, was das für praxen und kanzeleinen bedeuten kann!! ich hoffe ich konnte euch auf ein "interssantes" phänomen hinweisen *<jjj@lycos.de>*

Klar, das ist auf jeden Fall ein sehr interessantes Infostueckchen. Konntest du das reproduzieren mit anderen gescannten Noten? Wenn's dich interessiert, dann schau dir mal http://www.cl.cam.ac.uk/~mgk25/eurion.pdf an. Da ist in wenigen Worten zusammengefasst, wie Fotokopierer Banknoten erkennen und den Ausdruck verfaelschen. <Sascha>

Wieder Prüfungsfragen

Hallo Leute, habe Eure Adresse von einem Freund, der mir sagte, Ihr könnt uns weiterhelfen. Es geht um Prüfungsfragen für den Industriemeister im fachübergreifenden Teil Herbstprüfung 2004. Also die kommende Prüfung, zu hacken bei der www.XXX.de oder vielleicht noch einfacher da wo die Fragen gedruckt werden beim Bertelsmann Verlag GmbH Co KG Bielefeld Auf dem Esch 4 (Offsetverfahren, muss ja irgendwo im System hinterlegt sein). Den Weg wisst Ihr sicher besser als wir. Wir das sind angehende Meister die diesen kostenbewussten, rechts- und zusammenarbeitsbewussten Scheiß einfach nicht in die Birne kriegen fachlich aber zu gebrauchen sind. Fakt ist, wir betteln hier um Prüfungsfragen und sind gleichzeitig bereit Euch zu bezahlen.

Die Summe ist verhandelbar, kleinlich sind wir da nicht. Sollte Euch die Sache reizen, es eilt da die Prüfungen am XX.XX.2004 stattfinden. *<xxx@freenet.de>*

Der Freund hat Dir bullshit erzählt. Das Ausspähen von Daten ist eine Straftat nach Strafgesetzbuch:

StGB § 202a - Ausspähen von Daten

(1) Wer unbefugt Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, sich oder einem anderen verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Willst Du bzw. wollt Ihr die Karriere als Meister wirklich mit einer Straftat beginnen? Wenn Du nicht in der Lage bist, eine Meisterprüfung - mit den dazu notwendigen sozialen und kostenrechnungsmässigen Kompetenzen - zu absolvieren, solltest Du vielleicht besser Geselle bleiben, oder?

Und: Wieso kommt Ihr auf die abstruse Idee, wir sollten in Eurem Auftrag Straftaten verüben? <cefalon>

tut mir leid, dass ich Euch belästigt habe anscheinend seit Ihr die falschen Leute oder einfach zu blöd. Wer sich nicht vorstellen kann das es Leute gibt die diesen Job auch ohne diesen ganzen theoretischen Kram gut machen können, dann tut es mir leid. Eine Adresse habe ich noch, vielleicht sind diese Leute nicht so realitätsfremd wir Ihr. Frag doch einfach einmal nach, wer seine Meisterprüfung ohne Hilfe gemacht hat. Wir müssen nebenbei alle arbeiten und können nicht, munter auf den Tasten hacken. Träumt weiter, sorry für die Störung und spielt weiter den arroganten Weltverbesserer .

Treffer, versenkt.

Raubkopierer

Sorry Leute, "Musik ist nicht illegal, Niemals" ist einfach nur dumm. Hier geht's nicht um die Privatkopie. Hier geht's um Diebstahl. Tut nicht so scheinheilig. Es stimmt, dass die Musikindustrie viel Mist gebaut hat und auch immer noch viel Mist baut. Ich als Musiker allerdings habe ein existenzielles Problem, wenn Leute für meine Musik nicht bezahlen wollen. *<Peter Oertel>*

Nein, es geht schon um die Schranken bzw. die Reichweite des Urheberrechtes.

Wir stellen nicht das Urheberrecht als solches in Frage sondern betonen nur dessen Sozialbindung. Unsere Kampagne ist - zugegebenermassen - relativ populistisch. Es ging aber darum einen Gegenpol zu der ebenfalls populistischen Kampagne der Industrie ("Raubkopierer sind Verbrecher") zu schaffen, welches ebenfalls juristischer Blödsinn ist.

Es ist halt schwierig in einer Kampagne das diffizile Gefüge zwischen Urheberrecht -> Verwertungsrecht -> Schranken -> Schrankenschranken plakativ zu erklären.

Uns ist natürlich klar, dass es Urheber heutzutage schwerer haben, Ihre Werke vergütet zu bekommen, aus diesem Grund unterstützt der CCC auch Initiativen wie der Kulturflatrate.

Es gibt viele Fragen die in diesem Bereich bis jetzt ungelöst sind. Eine schlichte Kriminalisierung aller Tauschbörsennutzer und eine flächendeckende Einführung von DRM-Systemen sind unserer Ansicht nach ein Schritt in die falsche Richtung. <Julius>

Ermittlungsverfahren gegen George W. Bush und andere

In deutlichen Worten skizziert der renommierte amerikanische Rechtsanwalt Stanley Hilton seine Sammelklage von Opfern des 11.09. gegen George W. Bush und andere. Hier ist nicht von "Schlamperei" oder "Pflichtverletzungen" die Rede, sondern von aktiver Planung und Durchführung der Angriffe im Auftrag von amtierendem Präsident und Innenminister. Es geht auch nicht im Stile von Mutmassungen und Theorien zur Sache, sondern Zeugenaussagen und Beweismitteln stehen zur Verfügung. Eine wirklich andere Darstellung des Sachverhalts, nachzulesen unter
http://prisonplanet.com/articles/september2004/130904hiltontranscript.htm

Was flog eigentlich ins Pentagon?

Mit der Frage der tatsächlichen Ereignisse am 11.09. beschäftigt sich auch ein rund fünfminütiges (2,9 Mb) Shockwave, was den Namen ausnahmsweise verdient. Die mit vielen Links zu den Originalzeugenaussagen und Dokumenten untermauerte Darstellung passt eher zu den Aussagen von Herrn Hilton s.o. als zur offiziellen Realität:
http://www.contramotion.com/movies/pentagon1.swf

Verhaftung Gravenreuth W..äh Syndikus

Als wenn die Nachrichtenlage derzeit nicht absurd genug wäre, mußte sich auch noch der zusammen mit Günther von Gravenreuth niedergelassene Anwalt Bernhard Syndikus wg. Verdachts der gewerbsmässigen unerlaubten Verwertung urheberrechtlich geschützter Werke gemäß §§106,108,108a UrhG sowie weiterer Delikte (von Geldwäsche war die Rede) verhaften lassen. Ausgangsbasis war ein Ermittlungsverfahren bei der Staatsanwaltschaft Mühlhausen, die Hausdurchsuchungen wurden vom LKA Thüringen koordiniert. Insgesamt wurden nach Medienberichten 3 Tatverdächtige verhaftet und haben teilweise bereits Geständnisse abgelegt. Der Tatverdächtige Syndikus steht offenbar unter dem Verdacht, die illegal erwirtschafteten Einnahmen von ftpworld.de als Kontenverwalter in einer komplexen Konstruktion verwaltet zu haben.

Die "zufällige" Anwesenheits eines öffentlich-rechtlichen Fernsehteams, das vielorts Empfindungen der Genugtuung durch die in der abendlichen Tageschau ausgestrahlten Bilder eines in Handschellen verhafteten Syndikus transportiert, ist allerdings auch noch Grundlage einer anderweitigen Betrachtung. Aus dem Umfeld der Kanzlei Gravenreuth gibt es den Verdacht, dass es sich um ein nachrichtendienstliches Manöver gegen Gravenreuth selbst aus dem Umfeld von Peter Gauweiler handelt. Hintergrund soll die äußerste Nervösität einiger Herrschaften in Bayern aufgrund von weiteren Aussagen im Kontext der Verhaftung von Ludwig Holger Pfahls sein. Gravenreuth soll persönliche gute Kontakte zum verautounfallten Staatsanwalt Jörg Hillinger gehabt haben, der u.a. die Ermittlungen gegen Max Strauss führte.

Die Schadensfreude über den Imageschaden von Gravenreuth und Syndikus im Rahmen des Ermittlungsverfahrens FTPWORLD.DE wird sich trotzdem keiner nehmen lassen wollen. Gravenreuth selbst stand schließlich verschiedentlich im Verdacht im Kontext von Geheimdienstkontakten u.a. Schützenhilfe für Kim Schmitz (dessen Kooperation mit "ex"-BfV Hartmut Pohl hinreichend bekannt sein sollte) geleistet zu haben.

EBay Hack?

Als umstritten kann derzeit die Methode gelten, mit der ein noch unbekannter Hacker versucht, einen Beratervertrag bei Ebay Deutschland zu ersteigern. Mit Verweis auf ein gravierendes Sicherheitsloch, das es ermöglicht, Accountinformationen inkl. Zugangsdaten auszuspähen, wird versucht, dem EBay Vorstand nahezulegen, ein Beratervertrag käme billiger als ein Rufschaden sowie die Optionen der kriminellen Schädigung von Ebay Kunden. Vermutlich ist das richtig, ob es die richtige Herangehensweise ist, ist wohl eine andere Frage.

Gewöhnlich gut unterrichtete Kreise berichten, der Trick basiere wohl darauf, ein eigenes - möglichst attraktives - Angebot für einen Artikel bei Ebay zu plazieren und dabei die zur Verfügung stehenden Freiheiten bei der Gestaltung der Produkt-Website vollständig auszunutzen.

Für das Geschäftsmodell Schadensbewahrung eines Doofen, im juristendeutsch "Geschäftsführung ohne Auftrag", gibt es wohl noch kein ordentliches Vorgehen. Vielleicht findet sich ja mal ein Jurist, der das ordentlich ausarbeitet?

Absurder geht's bald nimmer:

EC-Kartenrechtssprechung des BGH

Am 05.10. hat der für das Bankrecht zuständige XI. Zivilsenat des Bundesgerichtshofs unter dem Aktenzeichen XI ZR 210/03 eine Entscheidung in Sachen gestohlene ec-Karte zuungunsten des Bankkunden entschieden. Die Urteilsbegründung lag zum Redaktionsschluss der Datenschleuder noch nicht vor, vermutlich wird sie auch diesmal kein Hinweis auf mögliche Befangenheit des Gerichts durch die Inanspruchnahme von Krediten seitens der Richter enthalten.

In der Presseerklärung des BGH wird dem Kunden, dem die EC-Karte entwendet wurde, wie so oft eine grobe Verletzung der Sorgfaltspflicht vorgeworfen, wie schon oftmals in der Vergangenheit bezieht sich der Anscheinsbeweis, der Kunde habe den PIN-Code zusammen mit der Karte aufbewahrt auf die mittlerweile 128-Bit Breite Schlüsselbreite des Institutsschlüssels - die für einen kriminellen Täter viel warscheinlichere Möglichkeiten der Ausspähung bzw. sonstige Verschaffung des PIN-Codes gelten als "nicht hinreichend dargetan". Was auch immer das heißt.

Zitat: *„Das Berufungsgericht hat sachverständig beraten festgestellt, es sei mathematisch ausgeschlossen, die PIN einzelner Karten aus den auf ihnen vorhandenen Daten ohne vorherige Erlangung des zur Verschlüsselung verwendeten Institutsschlüssels zu errechnen. Daß die Eingabe der zutreffenden PIN durch den Dieb der ec-Karte hier dadurch ermöglicht wurde, daß dieser zuvor die persönliche Geheimzahl des Karteninhabers bei Abhebungen an Geldausgabeautomaten ausgespäht hat, war nicht hinreichend dargetan."*

Immerhin erhält die Presseerklärung des Bundesgerichtshof einen Hinweis darauf, daß es mit der Behauptung der Banken, das von Ihr verwendete Verfahren zur Berechnung des PIN-Codes sei total sicher und Details seien geheim, in Zukunft nicht getan ist:

"Zugleich hat der Bundesgerichtshof aber deutlich gemacht, daß kartenausgebende Kreditinstitute verpflichtet sein können, in Zivilprozessen der vorliegenden Art (im Rahmen berechtigter Geheimhaltungsinteressen) nähere Angaben über die von ihnen getroffenen Sicherheitsvorkehrungen zu machen, um gegebenenfalls auch deren Überprüfung durch Sachverständige zu ermöglichen."

Der Chaos Realitäts Dienst stellt dem Bundesgerichtshof oder anderen interessierten Parteien im Rahmen von zivilrechtlichen Auseinandersetzungen mit den Banken gerne auch die Informationen zur Verfügung, die die Banken vermutlich auch in Zukunft nicht freiwillig bei Prozessen zur Verfügung stellen. Mail *input@crd.ccc.de*.

Aus der Abteilung gute Manieren und höfliche Korrespondenz

http://static.thepiratebay.org/dreamworks_response.txt

```
Date: Sat, 21 Aug 2004 18:21:43 -0100 (GMT)
From: anakata
To: KMWLAW@flash.net
Subject: Re: Unauthorized Use of DreamWorks SKG Pro-
perties
On Mon, 23 Aug 2004 KMWLAW@flash.net wrote:
> Dennis L. Wilson, Esq.
> KEATS McFARLAND & WILSON, LLP
> 9720 Wilshire Blvd., Penthouse Suite
> Beverly Hills, CA 90212
> Tel: (310) 248-3830
> Fax: (310) 860-0363
>
> August 23, 2004
>
> VIA ELECTRONIC MAIL
> AND U.S. MAIL
>
> ThePirateBay.org
> Box 1206
> Stockholm 11479
> SWEDEN
>
> tracker-40-aa-5f-03-412675c8@prq.to
>
> Re: Unauthorized Use of DreamWorks SKG Properties
>         http://www.thepiratebay.org
>
> To Whom It May Concern:
>
> This letter is being written to you on behalf of our
> client, DreamWorks SKG (hereinafter „DreamWorks").
> DreamWorks is the exclusive owner of all copyright,
> trademark and other intellectual property rights in
> and to the ^ÖShrek 2^Ö motion picture.  No one is
> authorized to copy, reproduce, distribute, or
> otherwise use the ^ÖShrek 2^Ö motion picture without
> the express written permission of DreamWorks.
[...]
> As you may be aware, Internet Service Providers can
> be held liable if they do not respond to claims of
> infringement pursuant to the requirements of the
> Digital Millennium Copyright Act (DMCA). In
> accordance with the DMCA, we request your assistance
> in the removal of infringements of the „Shrek 2"
> motion picture from this web site and any other sites
> for which you act as an Internet Service Provider.
> We further declare under penalty of perjury that we
> are authorized to act on behalf of DreamWorks and
> that the information in this letter is accurate.
> Please contact me immediately to discuss this matter
> further.

As you may or may not be aware, Sweden is not a state
in the United States of America. Sweden is a country in
northern Europe.

Unless you figured it out by now, US law does not app-
ly here.

For your information, no Swedish law is being violated.

Please be assured that any further contact with us,
regardless of medium, will result in

a) a suit being filed for harassment
b) a formal complaint lodged with the bar of your legal
counsel, for sending frivolous legal threats.

It is the opinion of us and our lawyers that you are
fucking morons, and that you should please go sodomize
yourself with retractable batons.

Please also note that your e-mail and letter will be
published in full on http://www.thepiratebay.org.
Go fuck yourself.

Polite as usual, anakata
```

Stahl schmilzt nicht bei 250 Grad

ist auch das Ergebniss einer Studie, die die tatsächliche Einsturzursache des WTC's am 11.09. untersucht. Mehr unter *http://www.911truth.org/article.php?story=20041112144051451*

Wissenschaftler stützen These vom elektronischen Wahlbetrug in den USA

Heise berichtet am 19.11. über den Zusammenhang des Einsatzes elektronischer Wahlmaschinen und Stimmanteilen für George W. Bush.

http://www.heise.de/newsticker/meldung/53464

T-Hack Nachbeben

Auch beim in der letzten Schleuder berichteten T-Hack ging es ja mehr oder weniger um "Geschäftsführung ohne Auftrag". Etwas unglücklich ist dabei wohl die Differenzierung zwischen dem Interesse des Sicherheitslochfinders und dem CCC gelaufen; berechtigterweise wurden wir kritisiert, weil wir dem Finder quasi CCC-Webspace zur Erlangung eines Beratervertrages zur Verfügung stellten.

Trotzdem war es aus Sicht des CCC grob korrekt, die Sache durch Veröffentlichung zu unterstützen, da verschiedene Kommunikationsversuche ja nicht funktionierten. An der Interessens-Differenzierung arbeiten wir noch.

Finanzkrise in Bonn: beide Schlüssel zur Entleerung der Parkautomaten abgebrochen

Eine unglaubliche Provinzposse zu genießen unter *http://www.general-anzeiger-bonn.de/index_frameset.html?/news/artikel.php?id=80624*

Admin Passwort der Diebold Voting Maschinen: "1111"

Mehr schmerzhafte Wahrheit darüber unter *http://washingtontimes.com/upi-breaking/20041112-112037-7263r.htm*

Linux Distributionstool verursacht bereits 1/3 des Netztraffics..

Das äh.. Linux-Distributionstool Bittorrent verursacht nach Angaben einer Studie der britischen Web-Marktforschungsfirma CacheLogic bereits ein Drittel des weltweiten Internet-Traffics. Mehr unter *http://futurezone.orf.at/futurezone.orf?read=detail&id=256367&tmp=41652*

BKA-Präsident glaubt, daß OBL Bush zur Wiederwahl verhelfen wollte

Angesichts der kurz vor der US-Wahl aufgetauchten Videobotschaft von Osama Bin Laden mutmast BKA-Präsident Jörg Ziercke "Ich kann nur vermuten, dass er wollte, dass Bush wieder gewählt wird." Mehr dazu unter *http://www.r-archiv.de/modules.php?name=News&file=article&sid=1609*

Schily will, daß BKA das Fernmeldegeheimniss ignorieren kann

Natürlich nur als "präventive Maßnahme zur Gefahrenabweht" möchte Innenmnister Schily dem BKA erlauben, Telefongespräche präventiv zu überwachen. Wenn Schily so weiter macht, fühlt sich die Redaktion Datenschleudern legitimiert, im Rahmen des §20 GG Art (4) Herrn Schily zwecks Abwehr von Gefahren für die Verfassung und den Rechtsstaat abzuhören.

http://www.reuters.de/newsPackageArticle.jhtml?type=politicsNews&storyID=613911&section=news

Besungene Technologieentwicklung

Ein Beitrag zum Thema Technologie-Entwicklung wegen der Pornos? *http://forporn.ytmnd.com/*

Datenschützer CCC **bitten um Mithilfe.**

Belohnung

Im Zusammenhang mit geltendem Landes-, Bundes- und Menschenrecht weisen Datenschützer auf folgende Personen hin:

Ulla Schmidt
Bundesgesundheitsministerin
Die Gesundheitskarte kommt 2006, das ist beschlossen. Nicht klar ist, welche Funktionen sie hat, welche persönlichen Daten auf ihr und in Datenbanken abgespeichert werden und wer Zugriff auf sie hat. Hier droht nicht nur ein weiteres Instrument eines Überwachungsstaates, sondern auch ein zweites Toll Collect.

Dieter Schwarz
Gründer von Lidl
Mitarbeitern, die sich privat treffen, droht die Kündigung. Kassen werden heimlich videoüberwacht. In Tschechien waren Toilettengänge zur Arbeitszeit verboten. Frauen duften dort nur dann außerhalb der Pausen aufs Klo, wenn sie mittels eines Stirnbandes weithin verkündeten, dass sie ihre Tage haben.

Otto Schily
Bundesinnenminister
Schily treibt die Erfassung biometrische Merkmale in Ausweisen international voran: In den Reisepässen der EU-Bürger werden künftig Gesichtsbilder und Fingerabdrücke elektronisch integriert. Was im Zuge der Sicherheitshysterie verschwiegen wird ist, dass diese Merkmale nicht fälschungssicher sind.

Fujio Mitarai
Präsident von Canon
Was bei Farbkopierern von Canon wie ein leichter, unkorrigierbarer, Gelbstich aussieht, ist brisant: In ihm ist die Seriennummer des Kopierers kodiert, auf welchem die Kopie angefertigt wurde. Jede Kopie ist rückverfolgbar. Handbücher und Servicehefte zum Gerät verschweigen das.

Zygmunt Mierdorf
Vorstandsmitglied der Metro AG
Mit weltweit eindeutigen Funketiketten möchte Metro den Weg ihrer Waren nachvollziehen. Dass sich die unbemerkt auslesbaren RFID-Chips auch auf Payback-Kundenkarten befanden, wurde verheimlicht. Nachdem dieser Skandal publik wurde, nahm Metro die Karten unter öffentlichem Protest zurück.

Janelly und Jean-Rene Fourtou
EU-Abgeordnete und Universal-Chef
Die französische Parlamentarierin bewirkte federführend die EU-Richtlinie zur massiven Verfolgung privater Internetnutzer, denen Urheberrechtsdelikte vorgeworfen werden. Dies kommt dem Chef des Musikgiganten Universal, ihrem Mann, sehr gelegen. Niveauvolle Lobbyarbeit.

Erwin Huber
Bundesinnenminister Bayerns
Huber brachte in das neue Telekommunikationsgesetz erfolgreich die Forderung ein, dass mit dem Verkauf einer Prepaid-Karte auch die persönlichen Daten des Käufers erfasst werden müssen. So gibt es keine Möglichkeit mehr, anonym ein Mobiltelefon zu besitzen und mit ihm zu telefonieren.

Dirk Teubner
Geschäftsführer von Armex
Kinder werden nun an eine elektronische Kette gelegt. Teubner will an der panischen Haltung von Eltern, stets das vermeintlich Beste für ihre Kinder tun zu müssen, Geld verdienen: Per SMS können Eltern das Mobiltelefon ihres Kindes orten. So werden Kinder zu unmündigen, aber willigen Untertanen erzogen.

Wer diese Personen an ihrem Handeln hindert, wird belohnt mit

mehr informationeller Selbstbestimmung und mehr Schutz der Privatsphäre.

„Das Grundrecht gewährleistet ... die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf ‚informationelle Selbstbestimmung' sind nur im überwiegenden Allgemeininteresse zulässig." *Bundesverfassungsgericht, 1983*

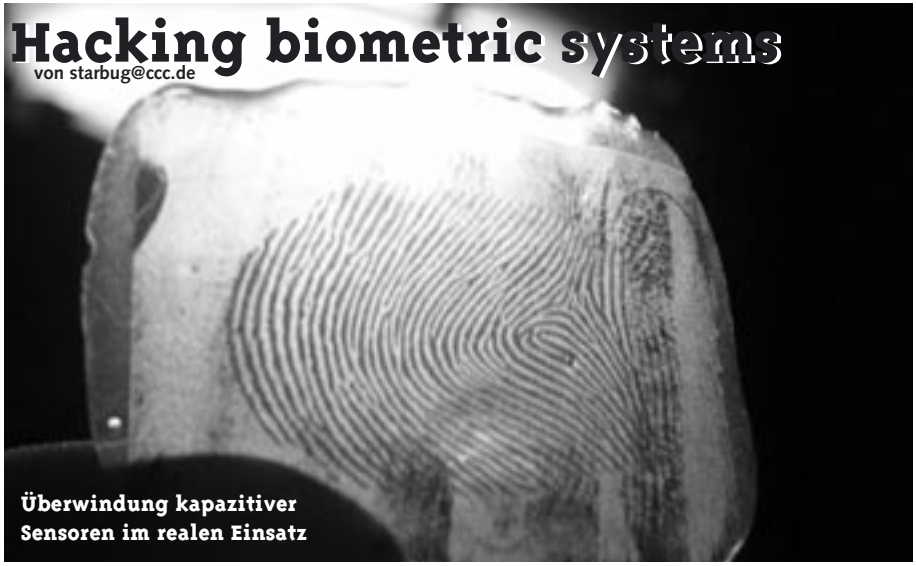
"Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, seine Wohnung und seinen Schriftverkehr oder Beeinträchtigungen seiner Ehre und seines Rufes ausgesetzt werden. Jeder hat Anspruch auf rechtlichen Schutz gegen solche Eingriffe oder Beeinträchtigungen." *Menschenrecht, Artikel 12*

Hinweise finden sich an jeder Stelle.

Um Mithilfe bittet der Chaos Computer Club und der FoeBuD I https://berlin.ccc.de/Fahndungsplakat I v0.4 Oktober 2004 I V.i.S.d.P.: M. Schmidt, Oderbergerstraße 23, 10435 Berlin

Hacking biometric systems

von starbug@ccc.de



Überwindung kapazitiver Sensoren im realen Einsatz

Nach dem c't Bericht zur Überwindbarkeit von verschiedenen biometrischen Systemen Mitte 2002 (http://www.heise.de/ct/02/11/114/) kam von einigen Seiten, der Vorwurf, dass es sich bei den Tests nur um Laborversuche gehandelt hätte. Vor allem die Firmen der getesteten Systeme meinten, dass solche Überwindungen in der Realität nicht durchführbar wären.

Da diese Feststellungen ja durchaus nicht von der Hand zu weisen waren lag der Fokus der weiteren Arbeiten darauf, die "Angriffe" auch in der Öffentlichkeit unbemerkt durchführen zu können. Die Erfolge sollen hier, am Beispiel eines erfolgreichen "Angriffs" auf das Bezahlsystem des Offiscom-Shops in Offenburg dargestellt werden.

Bezahler per Fingerabdruck im Officecom-Shop

Gestartet wurde der Einsatz des Fingerabdrucksystems "digiPROOF" Anfang 2003. Die Firma "it-werke" rüstete dazu den Officecom-Shop (http://www.officecom-shop.de/index1.php) mit einem kapazitiven Sensor aus. Mitmachen kann jeder, der ein eigenes Konto und ausreichend ausgeprägte Fingerabdruckmerkmale besitzt. Dazu füllt man lediglich ein Formular mit der eigenen Bankverbindung aus, beweist die eigene Identität anhand des Ausweises und lässt einen Finger in das System einlernen.

Will man einen Artikel kaufen, gibt man lediglich seinen Namen an und legt den Finger auf den Sensor. Der Betrag wird dann automatisch vom Konto abgebucht.

Szenarien des "Identitätsdiebstahls"

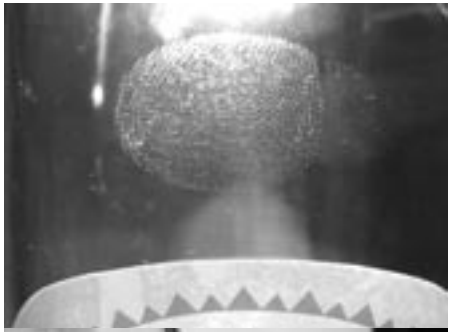
Beim Einsatz von biometrischen Systemen zur Authentifikation eines Bezahlvorgangs sind zwei Szenarien des "Identitätsdiebstahls" denkbar. Im ersten Fall stiehlt eine unberechtigte Person die Daten eines regulären Benutzers um so auf seine Kosten einzukaufen. Bei der anderen Möglichkeit arbeitet der berechtigte Benutzer mit und gibt freiwillig seine Daten der anderen Person weiter.

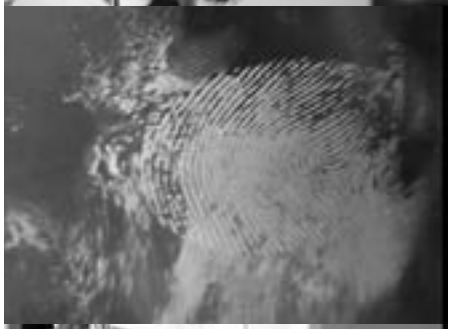
Szenario 1: Zur Durchführung benötigt man sowohl den Namen eines regulären Benutzers als auch einen Fingerabdruck des zur Verifikation verwendeten Fingerabdruckes. Den Namen und den verwendeten Finger erhält man am einfachsten bei der Überwachung eines Bezahlvorganges. Abdrücke von Fingern mit ausreichend guter Qualität hinterlässt man täglich bis zu 25 mal (http://www.ep.liu.se/exjobb/isy/2004/3557/exjobb.pdf). Guckt euch nur mal eure Türklinke an oder den Hochglanzumschlag einer Zeitschrift, welche ihr freundlicherweise kurzzeitig gehalten habt, während ich mir die Schuhe zubinden musste...

Szenario 2: Dieses hat den Vorteil, dass man sich die Suche nach einem Benutzer und die Suche nach Fingerabdrucken erspart. Allerdings steht man hier dann dem Problem gegenüber, dem Ladenbesitzer und eventuell der Polizei erklären zu müssen, dass man an diesem Tag mit Sicherheit nicht einkaufen war. Ein gut gewähltes Alibi sollte aber Beweis genug sein.

Überwindung

Geht man vom ersten Szenario aus, ist es nötig, die hinterlassenen Fingerabdrücke sichtbar zu machen um sie weiterverarbeiten zu können. Muss die Abnahme vor Ort (z.B. an einer Türklinke) geschehen, sollte man ein Verfahren wählen, das möglichst schnell den Abdruck





sichtbar macht. Hierfür eignet sich das, aus der Polizeiarbeit bekannte, Bestäuben des Abdrucks mit Grafitstaub, Ruß oder anderen Farbpigmenten. Dabei bringt man neben dem Abdruck eine ausreichend große Menge Pigmente auf und streicht diese mit einem sehr feinen buschigen Pinsel vorsichtig über die Fettrückstände. Sind alle Teile gleichmäßig bedeckt nimmt man den Abdruck mit einem Stück durchsichtigem Klebeband ab. Gerüchteweise gibt es auch gewisse Inhaltsstoffe von Spülmitteln (Fit) die mit dem Fett eine Verbindung eingehen und durch UV-Bestrahlung sichtbar werden. Wenn jemand da mehr weiß, wäre ich für einen Hinweis dankbar.

Hat man ausreichend Zeit den Abdruck sichtbar zu machen, bietet sich der Einsatz von Cyanoacrylat, einem Hauptbestandteil von Sekundenkleber, an. Von diesem bringt man eine kleine Menge in einen Flaschenverschluss oder eine Überraschungseihälfte und stülpt das Ganze über den Abdruck. Das ausgasende Cyanoacrylat reagiert mit den Fettrückständen des Fingerabdrucks zu einer festen weißen Substanz. Durch Erwärmen kann man das Ausgasen beschleunigen, so dass auch hier nach ca. 10 min ein deutliches Fingerbild zu sehen ist. Die so oder mittels aufgepinselter Pigmente sichtbar gemachten Abdrücke werden mit einer Kamera oder einem Scanner digitalisiert und grafisch nachbearbeitet. Neben einigen automatischen Bearbeitungsschritten (Anpassen von Kontrast und Threshold) müssen manche Fingerlinien von Hand nachgezeichnet werden. Es ist daher ratsam, mehrere Abdrücke zu haben, um schlecht abgebildete Teile ersetzen zu können. Eine Software, wie sie benutzt wird, um Panoramafotos zusammenzustellen könnte hierbei hilfreich sein.

Die aufbereiteten Fingerbilder werden dann in eine 3D-Form überführt. Sie dient als Grundlage für die Herstellung der Attrappen. In den wenigen existierenden Publikationen zu dem Thema wird Gelatine als Attrappenmaterial und fotostrukturierbare Leiterplatten als Form verwendet. Da deren Bearbeitung, insbesondere der Ätzschritt, aber sehr aufwendig sind wurde nach Alternativen gesucht. Dabei stellte sich heraus, dass der Toner eines Fotokopierers auf einer Folie eine ausreichende Dicke besitzt, um für die Abformung genutzt zu werden. Auch die Gelatine besitzt einige negative Eigenschaften. In dünnen Schichten ist sie nicht besonders widerstandsfähig und trocknet sehr schnell aus. Außerdem muss sie zum Abformen unter Temperatureinfluss verflüssigt werden. Hier hat sich nach längeren Experimenten eine gut zu verarbeitende, stabile und billige Alternative ergeben: “Ponal” Holzleim.

Er trocknet nicht aus und ist auch sonst deutlich widerstandsfähiger. So kann man den Finger mit der angeklebten Attrappe weiterhin normal benutzen ohne den Abdruck zu beschädigen. Zur besseren Verarbeitbarkeit und Erhöhung des Feuchtigkeitsgehalts kann man dem Holzleim eine kleine Menge Glycerin zusetzen. Gut durchmischt wird die Masse in einer dünnen Schicht auf die Form gerakelt, so dass nach dem Aushärten des Klebers (ca. zwei Stunden) eine Fingerabdruckattrappe von nur ca. 0,2 mm Dicke bleibt. Zum Ankleben dieser eignet sich wasserunlöslicher Maskenkleber von “Mastix” recht gut. Da die Sorte für medizinische Anwednungen

extrem teuer ist, kann die alkoholbasierte verwendet werden. Allerdings beginnt der Alkohol den Holzleim nach ca. zwei Stunden zu zersetzen. Das sollte aber für die normale Anwendung nicht relevant sein.

Konsequenzen für den Einsatz von Fingerabdrucksystemen

Wie dem Artikel zu entnehmen ist, ist es möglich Attrappen von Fingerabdrücken mit sehr geringem Aufwand und einfachsten technischen und finanziellen Mitteln herzustellen und sie unbemerkt einzusetzen. Auch überwachte Szenarien bieten so gut wie keinen Schutz, da die Attrappen weitgehend unsichtbar sind. Anders als beim Zutritt zum Zoo von Hannover oder beim Bezahlen im Heilbronner Biergarten kann im Officecom Shop großer finanzieller Schaden angerichtet werden. Der Kunde oder Ladenbesitzer kann sehr schnell mehrere 1000 Euro verlieren.

Aber auch die Aufnahme von Fingerabdrücken in internationale Reisedokumente ist mit Blick auf diesen Artikel als überaus fragwürdig einzuschätzen. Die versprochene zusätzliche Sicherheit bei der Identitätsüberprüfung von Einreisenden existiert kaum. Auch weiterhin können Personen mit gestohlenen oder geliehenen Dokumenten einreisen, selbst wenn ihre Abdrücke in irgendwelchen Täterdatenbanken vorliegen. Da die Aufnahme zusätzlicher biometrischer Daten in Reisedokumente augenscheinlich so gut wie keinen Nutzen hat, im Gegenzug aber datenschutzrechtlich überaus bedenklich ist und außerdem mit sehr hohen Kosten zu rechnen ist sollte das Projekt nochmals kritisch begutachtet werden!

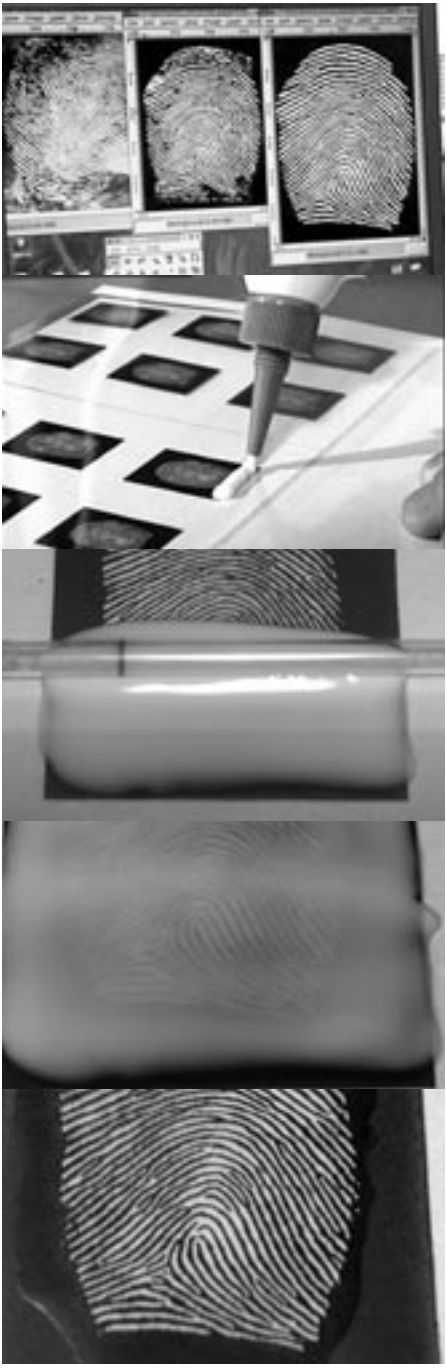
Einkaufen im Officecom-Shop (eine Tatsachenschilderung)

Um die Funktionsfähigkeit auch ausserhalb des Labors zu überprüfen ging es auf nach Offenburg. Schon lange vorher hatte ich mich angemeldet und testweise auch schon etwas gekauft. Sowohl das Enrollment als auch die spätere Verifikation funktionierte vollkommen problemlos.

Jetzt musste also auch noch der kopierte Fingerabdruck unbemerkt verwendet und korrekt erkannt werden. Vor dem Laden wurde dazu die vorbereitete Attrappe auf einen anderen als den eingelernten Abdruck geklebt. So könnte bei einer Nichterkennung der Kopie immernoch der richtige Finger, mit der Ausrede der Verwechslung, verwendet werden.

So ging ich dann also etwas nervös in den Laden und suchte nach einem billigen und halbwegs sinnvollen Artikel. Ein Spezialmouspad war das Produkt der Wahl. Noch viel nervöser ging ich zur Kasse und gab meinen Namen an, der nach längerer Suche dann auch gefunden wurde. Mit zitternden Händen legte ich den Finger mit der Attrappe auf den Sensor. Würde die Kopie akzeptiert werden und würde die Attrappe unerkannt bleiben?

Ja. Alles lief glatt. Unbehelligt verliess ich den Shop und wenige Tage später wurde der Betrag von meinem Konto abgebucht.



Schlüssel verlieren

von Stefan Grundmann

Es begann damit, dass sich auf einem Juke-Box-System (nennen wir es mal FBAVP) im Laufe der Zeit einige Daten angesammelt hatten, die sensibel genug sind, um sie vor Kompromittierung durch RECHNER WEGTRAGEN zu schützen. Die offensichtliche Lösung (ein Crypto-Filesystem benutzen) war nicht ganz zufriedenstellend, denn die FBAVP sollte weiterhin unbeaufsichtigt, oder zumindest ohne Anwesenheit eines Menschen mit root-Rechten, bootbar sein.

Einleitung

Im Folgenden wird ein System vorgestellt, bei dem die zur Nutzung des Crypto-Filesystems benötigten Schlüssel auf einem anderen Rechner abgelegt sind und bei Bedarf abgeholt und benutzt werden. Es werden Stärken und Schwächen dieses Systems kurz diskutiert, eine Proof-Of-Concept Implementierung wird vorgestellt.

Konzepte

Verschlüsselung auf Filesystem-Ebene soll "kalte" Daten schützen, also deaktivierte Filesysteme (mehr dazu z.B. in [0]). Die zur (De-)Aktivierung von Crypto-Filesystemen normalerweise notwendige Interaktion eines Administrators wird von einem Programm übernommen, das periodisch versucht die Schlüssel von einem Server abzuholen.

Wenn der Server erreichbar ist und den richtigen Schlüssel zurückgibt, wird das Crypto-Filesystem aktiviert, ansonsten wird es deaktiviert. Dieser Ansatz hat gegenüber einem herkömmlichen Crypto-Filesystem zusätzliche Probleme: es muss verhindert werden, dass beim Starten des weggetragenen Rechners das Crypto-FS automatisch aktiviert wird, des weiteren muß die Sicherheit der Schlüssel auf dem Server und während der Übertragung zum Client bedacht werden.

Andererseits kann die automatische (De-)Aktivierung von Crypto-Filesystemen die Administration von Rechnern vereinfachen und Hacker vor unangenehmen Behördenterminen bewahren (weil sie eines Morgens um 5:30 doch etwas zu verpeilt waren).

Proof-Of-Concept Implementierung

Der Server wurde in Python[1] implementiert und verwendet SSL mit Client-Zertifikaten. Clients verbinden sich und senden einen Request-String. Der Server sucht den zu dem Request-String passenden Eintrag in seiner Konfiguration und sendet dem Client den dort gespeicherten Schlüssel. Optional kann vom Server überprüft werden, ob die IP-Addresse, von der aus der Client versucht seinen Schlüssel zu erlangen, die selbe ist, die der DNS-Server zurückgibt, wenn er nach einem ebenfalls in der Konfiguration gespeicherten FQDN gefragt wird. Sollte diese Überprüfung fehlschlagen kann der Server entweder diesen Client blockieren (es wird nicht mehr auf Anfragen mit diesem Request-String geantwortet) oder den Eintrag (und damit den Schlüssel) löschen.

Der Client benutzt GBDE[0] verschlüsselte UFS Filesysteme (auch in File-Backed Memory Disks) was die unterstützten Betriebssystem auf FreeBSD-5 und FreeBSD-6 [3] einschränkt. Es wird die Verwendung mehrerer Volumes zugelassen, die individuell konfiguriert werden können (Timeouts, Zertifikate, verwendete Schlüssel-Server usw.).

Die High-Level Funktionalität der Clients wurde ebenfalls in Python, die Low-Level Funktionalität (mdconfig, gbde*, mount) in Pyrex[2] und C implementiert.

Nach dem Start des Clients werden für jedes Volume die folgenden Aktionen ausgeführt:

Aufkleber in Kleinstwagen

```
      Filesystem deaktivieren
      Solange nicht gestoppt:
        Schlüssel vom Server abholen
        nicht erfolgreich:
          Filesystem deaktivieren, STOP
        erfolgreich:
          Filesystem ist aktiviert:
            MD5-Hash der Server Antwort !=
gespeichertes Hash:
              Filesystem deaktivieren, STOP
          Filesystem ist deaktiviert:
            Filesystem aktivieren
            MD5-Hash des Schlüssels speichern
```

Das Fehlschlagen einer Aktion führt zur Deaktivierung des Filesystems, ob (nach einer Wartezeit) ein neuer Versuch unternommen wird das Filesystem zu aktivieren, oder ob das betroffene Volume bis zum Eingriff eines Administrators deaktiviert bleibt, kann konfiguriert werden.

Szenarien

i) Der oben erwähnte Juke-Box-Rechner wird weggetragen: entweder die Löschung der relevanten Schlüssel auf dem Server wurde zeitnah durch einen Anruf veranlaßt oder die FBAVP versucht von ihrem neuen Platz (auf dem Labortisch eines für die Rechnerwegträger arbeitenden IT-Spezialisten) aus, die Schlüssel vom Server zu bekommen, was ebenfalls zur Löschung selbiger führt.

ii) Es klingelt an deiner Tür und dieses mal haben sie 'ne USV dabei! Jetzt hilft eigentlich nur der Griff zum Sicherungskasten... locker entfernst du den Akku aus deinem PDA (auf dem der Schlüssel-Server für alle deine Crypto-Filesysteme läuft) und die von den Eindringlingen zu lösende Aufgabe hat sich vom Rooten deiner Server (bequem auf dem Labortisch des IT-Spezialisten, mit vollem Zugriff auf die Konsole und das lokale Netz) in Finden von Spuren der Schlüssel im RAM der Server gewandelt.

Abschließende Betrachtungen

Beim Einsatz des vorgestellten Systems muß der Sicherheit der auf dem Server gespeicherten Schlüssel besondere Aufmerksamkeit gewidmet werden. Die Konfiguration des Servers (und damit die Schlüssel) in einer mit zufälligem Schlüssel verschlüsselten Memory-Disk zu halten ist eine gute Idee; Intrusion Detection Sensoren im Server und ein Hostingcenter im Ausland ebenso.

Die Methoden mit denen der Server den Standort des Clients überprüft sind zwar ausbaubar (An welchem DSLAM hängt der Router vor dem Rechner? Ist Dienst X auf Rechner Y, der sich im selben Subnetz wie der Client befindet, erreichbar? ...), aber im schlimmsten Fall (die Rechner werden nicht abgebaut, sondern vor Ort analysiert) unwirksam, da hilft nur ein Telefonat.

Der Client Teil der Proof-Of-Concept Implementierung des Systems ist nicht ausreichend auf mögliche Rückstände von Schlüsselmaterial im Speicher überprüft worden, der Server-Teil sollte neu geschrieben werden. Eine Verwendung des Clients auf anderen Betriebssystemen sollte nach Austausch der Low-Level Funktionalität möglich sein.

Ach ja, Sourcecode gibt's auch: [4].

Links

[0] GBDE - GEOM Based Disk Encryption

[1] Python

[2] Pyrex - a Language for Writing Python Extension Modules

[3] FreeBSD

[4] Exile

Hacker-Stories

Kurzgeschichten von, für und gegen Hacker

Syngress Autorenteam: Ryan Russel, Tom Mullen (Thor), FX, Joe Grand, Ken Pfeil, Dan "Effugas" Kaminsky, Ido Dubrawsky, Mark Burnett, Paul Craig Vorwort von Jeff Moss, CEO von Black Hat Inc.

Eine süffisante Gute-Nacht-Lektüre für jeden Hacker. In zehn Kurzgeschichten des hauptsächlich US-amerikanischen Autorenteams werden unterschiedliche Arten des Hackens gezeigt. Sowohl Servereinbrüche als auch die Anwendung von Social Engineering oder das Virenschreiben werden in den fiktiven Geschichten vorgestellt. Größtenteils klingen sie sogar realistisch und könnten durchaus in dieser Form stattgefunden haben.

Der Leser sollte eine gehörige Portion an Wissen über Netzwerke oder diverse Tools (wie beispielsweise nmap) mitbringen, denn nicht immer wird alles erklärt. Da die Geschichten in den Jahren 2002 und 2003 spielen, sind sie sogar sehr aktuell. An vielen Einbruchsvarianten hat sich bis dato nichts geändert.

Das Buch wird durch einen Anhang zu "Sicherheitsregeln" abgerundet, welcher Anwendern und Administratoren Hinweise zur Planung und Absicherung von Rechnern in Netzwerken an die Hand gibt.

Folgend ein Ausschnitt aus "Hackse und die Netzwerge" von FX, einem Stammgast beim Chaos Communication Congress:

Bei einer Hacker-Konferenz in Las Vegas hat h3X einmal einen jungen Kerl beobachtet, der war kaum achtzehn, wie der einen Rechner gekapert hat. Der Typ hat von h3X gedacht, sie wäre so eine Hackerhure mit praktisch Null Hacking-Skills. Wie gewöhnlich dachte der Typ, er könnte ihr mit seiner Geschwindigkeit imponieren. Also hat er, nachdem er auf einem Rechner root-Rechte bekam, auf ein anderes xterm gewechselt und ein Rootkit per FTP übertragen. Sekunden, nachdem das Paket auf dem Zielrechner eingetrudelt war, hat er sein vorbereitetes Skript namens 31337kit.sh angeworfen und war völlig davon überzeugt, dass er seine überragenden Hacking-Skills eindrucksvoll demonstriet hat. h3X hat sich die ganze Geschichte angeschaut, den Typ angelächelt, der prompt von seinem Stuhl hochsprang und sich wohl schon Hoffnungen über die kommende Nacht, den nächsten Tag und ein gemeinsames Leben gemacht hat. Aber trotz seiner extrem hoffnungsvollen Wünsche war ihr Lächeln keine Einladung, die Welt mit zukünftigen Hackergenerationen zu bevölkern.

Immer noch lächelnd fragte h3X: "Darf ich mal?" Der Typ wirkte verwirrt, hatte aber nichts dagegen und rutschte rüber, damit sie an die Tastatur kam. Als sie sich nach vorne beugte, streifte ihr Haar seine Wange, und er konnte sich kaum auf das root-System konzentrieren. Aber statt weiter diese Kiste zu hacken, gab h3X nur zwei Buchstaben ein, drückte langsam auf die Eingabetaste und ging einen Schritt zurück, um sicherzugehen, dass der Typ sich auf den Monitor konzentrierte und nich auf ihre Kurven. Als der Happy Hacker auf den Monitor schaute, begriff er nicht, was er dort sah:

```
Linux:~# ls
ld.so can not find libc5.so .....
Linux:~#
```

"Hör mal, Alter", sagte h3X, "hast Du 'ne Ahnung was ein dynamischer Linker ist?" Der Kerl schaute sprachlos auf den Monitor, und ihm dämmerte, dass hier irgendwas nicht ganz stimmte. h3X dachte kurz daran, seine vitalen Funktionen zu checken, um zu sehen, ob er noch am Leben war, aber der Typ war einfach nur geschockt. Also fuhr sie fort: "Dein Rootkit hat die Binaries ersetzt, die mit den Bibliotheken auf diesem System dynamisch gelinkt waren. Leider waren die Binaries von diesem Rootkit nicht auf die Libs verlinkt, die auf diesem System sind, sondern auf eine ältere Version. Du hast die Binaries zerschossen. Du hast deine Anwesenheit nicht versteckt. Im Gegenteil, du hast sie so laut wie möglich rausposaunt, weil sogar die grundlegenden Funktionen von Systemadministration und -operationen jetzt versagen werden. Das kannst du nicht wieder reparieren, und das System wird in ... sagen wir 24 Stunden einer forensischen Analyse unterzogen."

Unser Junior-Hacker konnte kaum unglücklicher dreinschauen. Aber dann änderte sich sein Gesichtsausdruck, und Ärger stieg in ihm hoch. Er klappte den Laptop mit Schmackes zu, klemmte ihn sich wie ein Schulbuch unter den Arm und ging aus dem Raum, um das zu tun, was die meisten Kerle seines Alters machten: nach Hackerhuren mit weniger Hirn suchen (aber in den nächsten vier Jahren war er erfolglos).

Hacker Stories

mitp-Verlag/Bonn, Übersetzung aus dem Amerikanischen von Jürgen Dubau, ISBN 3-8266-1450-X, 19,95

HackerPort - I/O-Pins via USB

Fast jeder Hardware-Hacker, der diese Überschrift liest, wird wahrscheinlich denken: HackerPort und USB? Was hat das denn miteinander zu tun? Denn eigentlich wird der Begriff "hacker port" in Kreisen der Hardware-Hacker als Deckname für den Parallelport des PCs benutzt.

Der alte "hacker port"

Die meiste selbstgebaute Hardware, die an den PC angeschlossen werden soll, wird an den Parallelport des PCs angeschlossen. Der Grund ist klar: Nur der Parallelport des PCs bietet die Möglichkeit, jeden einzelnen Pin der 12 Ausgänge und 5 Eingänge mit einem eigenen Bit in den Parallelport-Registern unabhängig von den anderen Pins und Bits zu schreiben bzw. lesen. Das macht es möglich, viele Hardware-Interfaces und -Protokolle mit einem Parallelport zu emulieren. Und wenn einmal die Anzahl der I/O-Pins nicht reicht, so benutzt man einfach mehrere Parallelports.

Das Problem

Das hört sich ja alles sehr gut an, aber leider ziehen dunkle Wolken am Hardware-Hacker-Himmel auf: Einige große Konzerne, die maßgeblich an der Entwicklung des PCs arbeiten, haben sich entschlossen, den alten Parallelport (und auch die seriellen Ports) durch etwas neueres zu ersetzen.

Das ist im Prinzip auch verständlich, denn die Hardware des Parallelports benutzt noch immer den 8-Bit ISA-Bus. Dies ist sogar auf PCs der Fall, die keinen einzigen ISA-Slot mehr besitzen. Dort befindet sich intern in einem Chip ein ISA-Bus mit der Parallelport-Hardware. Das ist auch der Grund dafür, dass selbst auf modernen PCs mit Taktfrequenzen von einigen GHz, ein Zugriff auf den Parallelport etwa eine MikroSekunde dauert. Das ist natürlich sehr viel, wenn man es einmal mit der Ausführungszeit eines MOV-Befehls von unter einer NanoSekunde auf solchen PCs vergleicht.

Um diesen veralteten ISA-Bus komplett loszuwerden, muss man auch den Parallelport entfernen. Also wird gemäß der Vorgabe der großen Konzerne der Parallelport durch den Universal Serial Bus (USB) ersetzt.

Der erste Schritt dazu ist bereits vollzogen, jeder PC hat mittlerweile mindestens einen USB-Port. Der zweite Schritt ist das Wegfallen des Parallelports. Das kann man bei neueren Notebooks schon sehr deutlich erkennen. Heute haben sie oft schon keine seriellen Ports mehr und einige werden sogar bereits ohne Parallelport gebaut. Auch auf den Desktop-Rechnern hat dies schon begonnen, die Anzahl der seriellen Schnittstellen sinkt langsam von zwei auf null, je nach Hersteller des Motherboards. Es kann daher erwartet werden, dass in ein paar Jahren der Parallelport in den meisten PCs nicht mehr vorhanden sein wird.

Leider ist der als Parallelport-Ersatz gedachte USB für einen Hardware-Hacker kein guter Ersatz, denn USB erlaubt es nicht, einzelne Bits einfach zu steuern. Es wird ein ziemlich komplexes serielles Protokoll benutzt, um über die zwei Datenleitungen die Geschwindigkeit von 12MBit (USB 1.1) oder sogar 480 MBit (USB 2.0) zu erreichen. Und wie schließt man nun seine selbstgebaute Hardware an den PC an?

Eine mögliche Lösung

Natürlich ist es möglich, Hardware an den USB anzuschließen. Allerdings müsste man dazu in jede selbstgebaute Hardware ein USB-Interface einbauen und jedes Mal einen Treiber schreiben. Das wäre aber viel zu viel Aufwand, wenn man z.B. nur mal ein paar Relais zum Schalten der Zimmerbeleuchtung an den PC hängen will. Außerdem wäre damit die Schwelle für Anfänger im Bereich des Hardware-Hackens sehr hoch.

So kam mir die Idee, eine kleine, günstige, relativ universelle Schaltung zu entwickeln, die man an den USB anschließen kann und die dann ein Interface zur Verfügung stellt, welches dem Parallelport ähnelt. Natürlich soll diese Schaltung nicht dazu dienen, Drucker an den PC anzuschließen, denn dazu gibt es ja USB-Parallelport-Konverter [1] für ein paar Euro in jedem PC-Laden. Es soll vielmehr ein Interface sein, welches auf die Bedürfnisse der Hardware-Hacker zugeschnitten ist.

Wenn die Software, der Schaltplan und eventuell sogar ein Layout kostenlos aus dem Internet heruntergeladen werden kann, kann jeder mit ein klein wenig Erfahrung im Bereich Hardware eine solche Schaltung bauen und das neue Interface dann für die Dinge nutzen, für die man sonst den Parallelport genutzt hätte.

Wegen der zusätzlichen Interface-Logik, die für den USB-Teil dieser Schaltung benötigt wird, sind leider nicht alle Eigenschaften des Parallelports realisierbar. Z.B. ist die IRQ-Leitung, die mit dem ACK-Bit des Parallelports verbunden ist, nicht per USB simulierbar, weil USB ein Polling-basiertes Protokoll ist. Das heißt,

der USB-Host-Controller im PC fragt jedes Gerät periodisch, ob es etwas senden möchte. Das macht es unmöglich, so etwas wie einen richtigen Interrupt zu realisieren und führt dazu, dass jede Aktion über USB ungefähr eine MilliSekunde Reaktionszeit hat.

Aber es ist besser, ein paar individuell kontrollierbare I/O-Pins mit einer relativ hohen Verzögerungszeit zu haben als gar keine...

Einige Standard-Aufgaben, die eine schnellere Reaktion benötigen, können vom ohnehin notwendigen Mikrocontroller in der neuen Schaltung übernommen werden.

Der neue HackerPort

Derzeit ist der Prototyp des HackerPorts in Arbeit. Die Hardware ist bereits fertig und besteht hauptsächlich aus einem USB 1.1 Interface-Chip und einem Mikrocontroller. Aus zwei Gründen fiel die Wahl auf USB 1.1: Erstens kenne ich kein USB 2.0 Chip, der noch für jeden von Hand lötbar wäre. (Die haben alle furchtbar kleine Pins.) Zweitens gibt es immer noch Hardware-Hacker, deren PC oder Notebook noch kein USB 2.0 hat.

Alles, was ich für den HackerPort entwickle, wird unter der GNU Public License veröffentlicht. Das ermöglicht es anderen mitzumachen und sichert gleichzeitig, dass der HackerPort für jeden benutzbar ist. Außerdem darf so keine Firma Geld mit meiner Entwicklung machen, ohne mir einen Cent abzugeben.

Die Hardware besteht aus dem Mikrocontroller PIC18F442, dem USB-Interface USBN9604, 5 Latches 74HC573 und ein wenig Kleinkram. Den Schaltplan, die Firmware für den Mikrocontroller und einen Treiber für Linux findet man unter:

http[s]://1stein.schuermans.info/hackerport/

Eigenschaften des HackerPort

Verbindung zum PC via USB 1.1

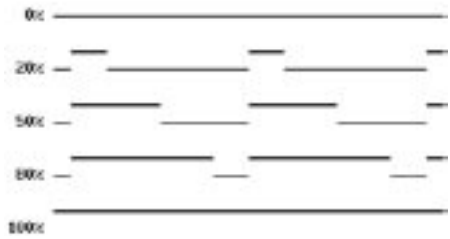
Angeschlossen wird der HackerPort an einen USB-Port. Dabei kann ein USB 1.1 oder ein USB 2.0 Port verwendet werden. Allerdings läuft der HackerPort immer nur mit 12MBit. Die Stromversorgung erfolgt über USB vom Rechner.

16 digitale Ausgänge & 16 digitale Eingänge

I/O-Pins waren der Hauptgrund, dieses Gerät zu entwickeln. Also gibt es auch 16 Ausgänge und 16 Eingänge, mit denen man alles Mögliche ansteuern kann. Allerdings ist es wegen der USB-Latenz nicht möglich, öfter als jede Millisekunde auf die Ausgänge zu schreiben oder von den Eingängen zu lesen. Eine Abfolge von schnellen Schreib- bzw. Lesezugriffen ist aber durch den Mikrocontroller realisiert.

2 Ausgänge mit Pulsweitenmodulation (PWM)

Eventuell wäre eine Art analoger Ausgang wünschenswert gewesen. Aber analoge Ausgänge sind schwer mit Digitalelektronik zu realisieren. Also wird ein Signal benutzt, welches zwischen 0V und 5V wechselt. Dieses Signal hat immer die gleiche Frequenz, aber der Prozentsatz der Ein-Periode kann zwischen 0 und 100 eingestellt werden. Die feste Frequenz ist in 3 Stufen einstellbar.



5 Analogeingänge

Analogeingänge sind nützlich, wenn man veränderliche Widerstände (z.B. Temperatursensoren) einlesen will. Da der Prozessor fünf Analogeingänge hat, kann man die ja auch alle benutzen.

I2C-Master

Serielle EEPROMs, IO-Expander, einige Sensoren und vieles mehr wird an den so genannten I2C-Bus angeschlossen. Meist sind diese Geräte I2C-Slaves, also wird der HackerPort I2C-Master. Der I2C-Bus ist zur Zeit noch nicht in der Software implementiert.

UART

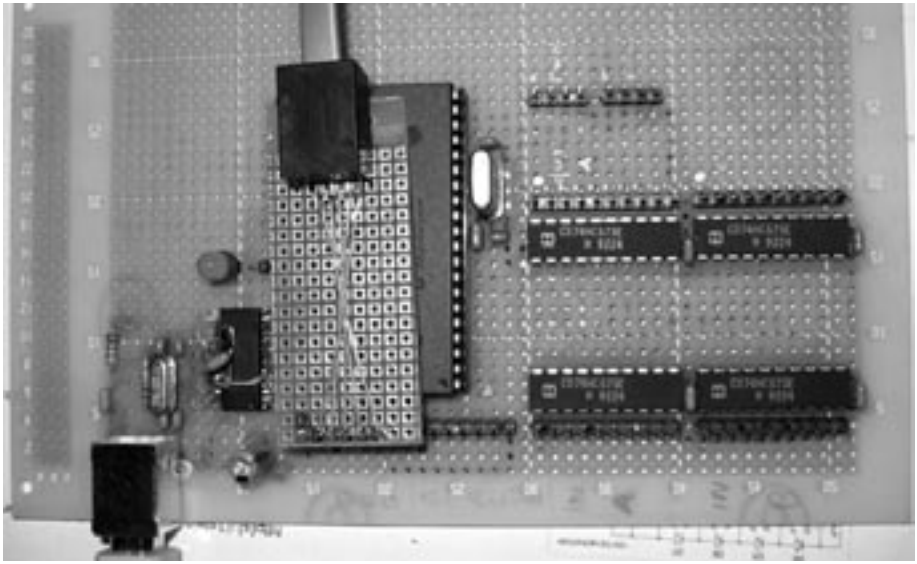
Der UART im HackerPort ist fast wie ein serieller Port des PC. Allerdings gibt es hier nur die Pins RX und TX. Die Steuersignale wie RTS, CTS usw. gibt es nicht. Also wird Hardware-Handshaking nicht funktionieren.

JTAG-Master

Der HackerPort soll einmal einen JTAG-Master-Port enthalten. Damit könnte man dann einige Mikrocontroller (z.B. AVR) und FPGAs programmieren. Dafür fehlt aber zur Zeit noch die Software.

PIC-Programmer

Da im HackerPort ein PIC-Mikrocontroller verbaut ist, muss es auch eine Möglichkeit geben, andere PIC-Mikrocontroller mit dem HackerPort zu programmieren. Es ist dann möglich für einen Freund den PIC18F442 mit der HackerPort-Firmware zu programmieren, so dass er seinen eigenen HackerPort bauen



kann. (Ein HackerPort kann sich nicht selbst programmieren, indem man einfach den PIC-Programmer-Anschluss nochmal mit dem Prozessor verbindet.) Leider ist auch hier die Software noch nicht geschrieben.

Aufbau und erste Schritte

Zunächst lädt man sich die Liste der benötigten Teile "parts.txt" herunter. Wenn man alle Teile besorgt hat, lötet man gemäß "schematic.ps" einen HackerPort daraus zusammen. Dabei sollte man den Microcontroller in einen Sockel setzen. Das Komplizierteste ist das Einlöten des USB-Interface-Chips, da man dieses nur in SMD-Technik bekommt. Ich habe den Chip einfach von oben auf eine normale Lochrasterplatine geklebt und dann mit feinen Drähten die Pins durch die Löcher der Platine nach unten verlängert.

Nun muss die Firmware "HackerPort.hex" bzw. "HackerPort.bin" aus "HackerPortFirmware-X.X.X_XXXX-XX-XX.zip" in den Prozessor geflasht werden. Dazu benötigt man ein Programmiergerät für den PIC18F442 - entweder ein offizielles oder ein selbstgebautes. Je nach Programmiergerät muss man dazu den Mikrocontroller wieder aus seinem Sockel herausnehmen. Wenn man kein Programmiergerät aber etwas Glück hat, kennt man jemanden, der einem den PIC18F442 programmieren kann. Falls man damit auch noch kein Glück hat, kann man sich den Prozessor von mir flashen lassen. Eine gute Gelegenheit ist da z.B. der Chaostreff Aachen oder der jährliche Chaos Communication Congress in Berlin. Später wird das Programmieren mit einem zweiten (schon fertigen) HackerPort möglich sein.

Nachdem der HackerPort fertig aufgebaut und programmiert ist, sollte man ihn mal testweise mit 5V aus einem Netzteil versorgen. Wenn man keinen übermäßig hohen Strombedarf (d.h. über 100mA) feststellt, kann man das Netzteil wieder abklemmen und den HackerPort über USB an den PC anschließen. Wenn man USB-Debug-Support in den Kernel einkompiliert hat, sollte man im Kernel-Log feststellen können, dass der PC den HackerPort gefunden hat. Auf jeden Fall sollte man ein neues unbekanntes Gerät im USB-Device-Filesystem finden können.

Nun lädt man sich den neusten Treiber "hkp_drv-X.X.X_XXXX-XX-XX" herunter

```
$ wget http://1stein.schuermans.info/
hackerport/hkp_drv-X.X.X_XXXX-XX-XX.tar.bz2
```

und entpackt diesen.

```
$ tar jxvf hkp_drv-X.X.X_XXXX-XX-XX.tar.bz2
hkp_drv-X.X.X_XXXX-XX-XX/
hkp_drv-X.X.X_XXXX-XX-XX/Makefile
hkp_drv-X.X.X_XXXX-XX-XX/hkp_drv.h
hkp_drv-X.X.X_XXXX-XX-XX/hkp_drv.c
hkp_drv-X.X.X_XXXX-XX-XX/hkp_drv_test.c
$ cd hkp_drv-X.X.X_XXXX-XX-XX
```

Nach dem Anpassen des Verzeichnisses mit den Kernel-Quellen im Makefile kann man den Treiber kompilieren

```
$ cd kernel-2.4
$ vi Makefile
$ make
gcc -Wall -O2  -I/usr/src/linux/include -
DMODULE -D__KERNEL__ -c -o hkp_drv.o hkp_drv.c
```

oder alternativ

```
$ cd kernel-2.6
```

```
$ vi build26
$ su -c ./build26
```

Nun muss man noch als "root" das Kernelmodul laden und die Device-Nodes erstellen.

```
su
insmod hkp_drv.o (bzw. hkp_drv.ko für Linux
2.6)
for((i=0;i<16;i++)); do mknod /dev/hkp$i c 180
$[176+i]; chmod 666 /dev/hkp$i; done
exit
```

Dann kann man das Testprogramm kompilieren und starten

```
$ cd ../test
$ ./hkp_drv_test /dev/hkp0
HackerPort driver for Linux - test application
version X.X.X date XXXX-XX-XX
part of the hacker port project - http[s]://
1stein.schuermans.info/hackerport/
Copyright (C) 2003-2004 1stein
<1stein@schuermans.info>
Copyleft: GNU public license - http://www.gnu.
org/copyleft/gpl.html
```

Jetzt kann man mal probieren, mit dem HackerPort zu kommunizieren:

```
hacker port> hw_ver
 hardware variant code: 00
 hardware version: X.X.X
 hardware date: XXXX-XX-XX
```

Als nächstes allokieren wir alle Anschlüsse des Hacker-Ports

```
hacker_port> own +out_ab +in_ab +pwm_ab
+analog_abcde +ser
 owned output ports: out_A out_B
 owned input ports: in_A in_B
 owned PWM outputs: pwm_A pwm_B
 owned analog inputs: analog_A analog_B
analog_C analog_D analog_E
 serial port owned
```

und geben ein paar Werte an die Output-Pins aus:

```
hacker port> acts 2
hacker port - action 0> out_a 0x55
hacker port - action 1> out_b 0xAA
 action 0: output port A: 85 = 0x55
 action 1: output port B: 170 = 0xAA
```

Wenn jetzt LEDs an den Output-Pins angeschlossen wären, würde jede zweite LED leuchten - eben die LEDs mit gesetzem Bit.

Zum Test lesen wir mal die offenen Analogeingänge ein:

```
hacker port> act
hacker port - action> analog_all
 action: analog input A: 19 =   92mV
 action: analog input B: 39 =  190mV
 action: analog input C: 53 =  259mV
 action: analog input D: 67 =  327mV
 action: analog input E: 80 =  391mV
```

und erhalten ein paar Werte aus den Störungen in der Luft.

Man erkennt hier schon das Prinzip, dass man mehrere Aktionen zusammengefasst an den HackerPort übergibt. Dadurch muss man nicht auf das Ende der ersten Aktion waren und spart somit die USB-Latenz ein.

Wie die restlichen Kommandos heißen und funktionieren, lässt sich leicht selbst herausfinden:

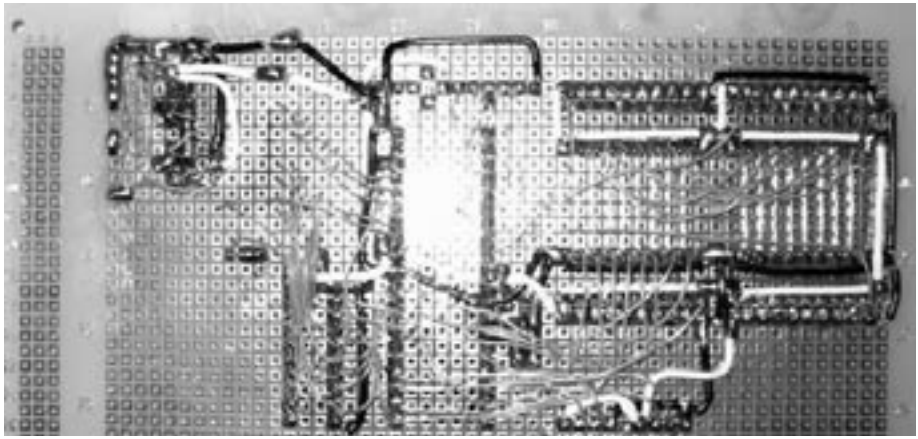
```
hacker port> help
```

Nur ein Kommando sei hier noch verraten:

```
hacker port> exit
```

beendet das Testprogramm.

[1] USB-Paralleport-Konverter sind nicht als Parallelport-Ersatz für Hardware-Hacker zu gebrauchen, weil man mit ihnen keine einzelnen Bits setzen kann. Diese Konverter bekommen vom PC die Daten und senden sie streng nach Drucker-Protkoll an den Drucker.



Nerds'n'family

von erdgeist

Ne Bäckerlehre. Irgendwas profanes. Da hat man sich dann schon einmal durchgerungen, am Kaffeetisch im Familien- und Freundeskreis der Eltern teilzunehmen, fährt extra raus in die Pampa und dann das.

Computerexperte. VERDAMMT!

"Mein Sohn ist Computerexperte!" Und das mit einem Lächeln, dass dieses Wort nach "Bundeskanzler" klingen lässt, oder "Bankdirektor". Nun weiß man, dass man verloren hat.

Alles kommt wieder hoch. All diese "Mutti, du kennst dich doch mit diesem Betriebssystem viel besser aus, als ich". Nein tut sie nicht und dann beweist sie, während man schwitzend durch irgendwelche Systemsteuerungshilfen klickt, dass sie es doch besser weiß. Klar sie würden es alleine schaffen, jedes Mal, aber sie brauchen einen ja, damit man die Fehler macht, die sie vermeiden wollen, nur um dann ganz generös darüber hinwegschauen zu können und einem ganz unauffällig zu zeigen, wieviel Erfahrung sie schon gesammelt haben. Als ob das nun nicht schon alles genug wäre, und Telefon- und Benzinkosten beliebiger Höhe verursacht hätte, sitzt man an dieser bekloppten Kaffeetafel und schluckt und versucht, alle Ähnlichkeit mit Bill Gates zu vermeiden, stopft sich mehr Kuchen in den Mund und schluckt und versucht, nicht wie ein völliger Trottel auch noch rot zu werden, als ob man stolz drauf sei. Aber eigentlich weiß man, dass es keinen Zweck hat. Man hat verloren.

Das sieht man daran, dass einen alle mit so ganz anderen Augen angucken. Man ist plötzlich ein Nützling. Ein Trottel zwar, aber nützlich. Und man sieht an seinem inneren Auge schon die Situationen vorbeihuschen:

Der Cousin, der sich "irgendwo im Interweb einen Trojaner-Virusprogramm" eingefangen hat und man darf da antanzen, klickt ein wenig herum, bekommt in der Browseradresshistory Ferkelwörter zu sehen, die einem einen ungefähren Eindruck verschaffen, mit welcher

Hartnäckigkeit da gesucht wurde und von denen ein Großteil da nicht im Traum einfallen würde, obwohl man ja selber auch nicht völlig... aber egal! Man nickt ein paar mal bedeutend und schüttelt hier und dort den Kopf und wenn der Cousin dann irgendwas von "Iloveyou" und "Melissa" brabbelt, fällt einem nix weiter ein als "Ja, hab ich auf Heise gelesen, aber weiß ich jetzt auch nicht" und dann sieht man dieses schnippische "Pah". Dieses "und du willst was von Computern verstehen". Und zu NetBSD und dem Apache, den man vorhin installiert hat und dem CryptoFS, an dem man grade codet, gibts nur ein "hab ich längst durchgespielt" und man weiß, dass man Federn verloren hat, aber da nie wieder hin muss.

Und da sitzt man nun, kaut auf Gabel und Kuchen und alle warten auf den Startschuss zur Hatz. Da gibt es immer einen widerlichen neuen Liebhaber irgendeiner Tante, der einem ganz scheinheilig zwei völlig aus der Luft gegriffene Monitortypen an den Kopf wirft und man soll nun entscheiden, welchen er kaufen soll nur um mit dieser Meinung gleich auseinander genommen zu werden. Man rettet sich mit Phantastereien über Lochmasken vom LCD Schirm und ist erlöst.

Vorerst nur, dank derselben blöde Tante, die den Typen angeschleppt hat, die macht nämlich einen Witz über Bankräuber mit ihren Lochmasken. Die Meute hat nun mit der gestrigen Bildzeitung und dem schlimmen Banküberfall genug zu tun, um vom heroischen Fluchtversuch abzulenken, den man dann notdürftig als Toilettenbesuch getarnt, unternimmt. Säße man noch da, wenn sie sich einem wieder widmeten, liefe man leicht Gefahr, jegliche Selbstachtung zu verlieren.

Stattdessen steht der sehr verständnisvolle Opa im Flur, der unbedingt wissen will, was man denn da so gerade arbeitet und irgendwie tut es einem ernsthaft Leid, dass das enttäuschte Nichtverstehen in seinen Augen schon nach dem zweiten Buzzword durchfackelt.

Und wieder übermannt einen ein Bild drohenden Übels. Situation: gemütlicher Abend, Programmieren an der Weltverbesserung. Grundnahrungsmittel und Brot, eine gute Playlist, nächsten Morgen nicht früh aufstehen... und dann natürlich plötzlich Telefon. Und dann vier Stunden irgendeinem Verwandten oder Bekannten eines Verwandten nur unter Zurhilfename eines XP auf dem Scancomputer in der Firma als Referenz beschreiben wie man unter Win95 versteckte Dateien einblendet und DLLs ins Pluginverzeichnis des CD-Rippers kopiert, dass natürlich nicht über den Startknopf im zweiten Menü sondern im Explorer, der aber dummerweise Arbeitsplatz heißt...

Dabei kann man gerade noch verhindern, auf dem Rückweg vom Klo in das Nachbarskind zu rennen, dass inzwischen schon groß und ansehnlich geworden ist, und steht paralysiert da, wie man es aus schlechten Filmen kennt, wo auch der ekligste, pickelige Computerhacker doch noch das Cheerleadermädchen abbekommt, und bestätigt alle Stereotype und huscht durch das Wohnzimmer zurück in das ehemalige Zimmer, das längst zum Büro umfunktioniert wurde und tastet sein Gesicht nach Pickeln ab.

Noch während man den Obstkuchenfleck auf seinem Alt-F4-Shirt breit reibt, hört man vor der Tür die Nachbarskinder tuscheln und "wenn du mich ärgerst, hol ich meinen großen Bruder und der haut dich" scheint obsolet zu sein, jetzt bedrohen sie sich mit "dann hackt der dein Konto" und das geht spätestens dann schief, wenn sie übermütig den Dorffaschos mit "und der macht dir Punkte in Flensburg" drohen.

Und langsam reift die Erkenntnis, dass man seinen Eltern erzählen will, man würde jetzt Bäcker oder Kfz-Mechaniker oder Bankdirektor.

Oder Bundeskanzler!

Dvorak für die Massen

von Corinna, <corinna@geekin.de>

Hast du dich auch schonmal beim Anblick einer handelsüblichen QWERTZ-Tastatur gefragt, wie die Anordnung der Tasten zustande kam? Auf den ersten Blick ist kein Muster erkennbar. Auf den zweiten auch nicht...

Bei näherer Betrachtung ist die QWERTZ-Tastaturbelegung (benannt nach der Buchstabenfolge oben links) ziemlich abstrus. Um ihr "Muster" zu finden muß man ihre Enstehungsgeschichte kennen.

Anfang des 19. Jahrhunderts baute der Italiener Pellegrino Turri die erste Schreibmaschine. Mit ihrer Hilfe konnte eine blinde Frau schreiben. In den folgenden Jahrzehnten gab es viele verschiedene Patente und Prototypen, aber keiner war nennenswert erfolgreich.

Auftritt: Christopher Sholes

Der Erfinder Christopher Sholes begann 1867, Versuche zum Schreibmaschinenbau durchzuführen. Das größte Problem war damals das Verheddern der fliegenden Typen: Wenn man zu schnell tippte, passierte es leicht, dass die Type des nächsten Buchstabens die des vorherigen im Fall stoppte, so dass dieser erneut gedruckt wurde. Erschwerend hinzu kam, dass das Papier von der Rückseite her beschriftet wurde. So tippte man unter Umständen lange den gleichen Buchstaben, bis man das Malheur bemerkte.

Sholes ordnete die Buchstaben häufiger Kombinationen (im Englischen) weit entfernt voneinander an, um den Tippvorgang gezielt zu verlangsamen. (Das war zu dieser Zeit völlig legitim, da Geschwindigkeit eine untergeordnete Rolle spielte. Getippt wurde per Adler-Suchsystem: Mit einem Finger kreisen, zielen und zustossen.)

Der Prototyp dieser Maschine wurde ab 1874 vom amerikanischen Waffenhersteller Remington produziert. Die dortigen Ingenieure nahmen allerdings noch eine winzige Änderung vor: Das "R" wanderte an seinen jetzigen Platz in der obersten Reihe. Dadurch konnten die Verkäufer bei Vorführungen das Wort "typewriter" relativ schnell auf einer einzigen Reihe schreiben.

Das Problem der sich verheddernden Typen wurde kurz danach behoben und Geschwindigkeit rückte in den Fokus: der Legende nach gewann Frank McGurrin, der erste Zehn-Finger-Tipper, 1888 auf der Remington einen bedeutenden Schnellschreibwettbewerb, woraufhin Remingtons, und damit QWERTYs, Siegeszug begann.

Wahrscheinlicher ist, dass sich die Remington dank Sholes' diverser technischer Verbesserungen am Markt durchsetzte. Endgültig Quasi-Standard wurde QWERTY, als auch Remingtons größte Konkurrenz Underwood das Layout übernahm. Bald gab es QWERTY-Tippkurse und in den Büros QWERTY-geschultes Personal.

Auftritt: August Dvorak

Der Psychologe und Pädagogikprofessor August Dvorak entwickelte zusammen mit seinem Schwager William Dealey in den 30er Jahren das nach ihm benannte Tastaturlayout. Die beiden sind Mitautoren des Buches "Typewriting Behaviour" von 1936. Den im Buch geschilderten Erkenntnissen über die Physiologie des Tippens wird im Dvorak-Tastaturlayout Rechnung getragen:

- je häufiger der Buchstabe, desto besser erreichbar (alle Vokale liegen auf der Grundreihe)
- starke Finger werden öfter benutzt als schwache
- häufige Handwechsel

Als Nebeneffekt der besseren Erreichbarkeit häufiger Buchstaben ist Dvorak sehr angenehm erlernbar: im Allgemeinen lernt man ja zuerst die Grundreihe. In Dvorak sind da schon eine Menge "real life"-Wörter dabei (Du, Nase, Stadt, Herde, Studentin). Bei QWERTZ tippt man, in Ermangelung sinnvoller Kombinationen, nur stur die Buchstaben.

Nun stellt sich die Frage: Warum hat sich dieses überlegene Tastaturlayout nicht gegen QWERTY durchsetzen können?

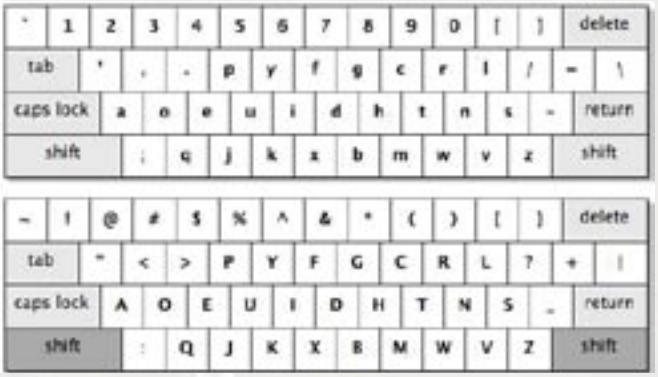


Abb.23: Dvorak Layout

Die Kontroverse

Die Dvorak-Tastaturbelegung ist eines der Paradebeispiele der Marktwissenschaftler dafür, dass im freien Wettbewerb nicht zwangsläufig das beste Produkt gewinnt, sondern auch Faktoren wie Standards und bisherige Marktverteilung eine große Rolle spielen. Liebowitz und Margolis, zwei Ökonomen die offenbar anderer Meinung sind, haben 1990 einen Artikel veröffentlicht, der Dvoraks Scheitern auf eine tatsächliche Unterlegenheit des Layouts gegenüber QWERTY zurückzuführen versucht. Über diese Attacke ist sehr viel geschrieben und diskutiert worden. Die ganze Debatte leidet darunter, daß sich die Beteiligten gegenseitig massive Befangenheit vorwerfen. Wenn die QWERTY-Befürworter die Zeit, die sie in den FlameWar gesteckt haben, in "Dvorak lernen" investiert hätten, hätte sich die ganze Kontroverse erübrigt. Was für QWERTY "typewriter" war, ist für Dvorak "Das ist ein Test". Die Finger bleiben für den ganzen Satz auf der Grundreihe. (Dem aufmerksamen Leser entgeht an dieser Stelle nicht, daß zumindest die Autorin ziemlich befangen ist ;))

Fazit

Dass es bei massivem Gerät wie Schreibmaschinen schwierig war, die Tastaturbelegung zu ändern leuchtet ein. Aber im Zeitalter des Computers, in dem man das Tastaturlayout mit einem einzigen Kommando (oder diversen Klicks) ändern kann, gibt es wahrlich keinen Grund, immer noch in einer Anordnung zu tippen, die vor über 100 Jahren aus mechanischen Gründen, mit dem expliziten Ziel uns zu bremsen, entwickelt wurde.


Dvorak † 1975

Für wen lohnt der Umstieg?

- Vieltipper (keine schmerzenden Sehnen mehr)
- Regelmäßige Tipper, die das vermutlich die nächsten 2-3 Jahre bleiben
- Adler-Suchsystem-Tipper

Du solltest besser nicht umsteigen, wenn...

- Du deine Rechner (mit QWERTZ-Usern) teilen mußt
- Du schon sehr gut Zehn-Finger-QWERTZ beherrschst (und keine Schmerzen hast)
- Du keine Möglichkeit hast, die Umstellung einige Zeit durchzuziehen

Wie lange dauert der Umstieg?

Das hängt ganz davon wie viel man tippt und wie konsequent man umstellt. Faustregeln:

- Nach ca. einer Woche denkt man nicht mehr über jeden einzelnen Buchstaben nach.
- Nach gut zwei Monaten schreibt man flüssig und kennt auch langsam die Sonderzeichen.
- Nach ca. 6 Monaten hat man seine alte QWETRTY-Geschwindigkeit eingeholt.
- Für den Rest des Lebens tippst Du schneller, effizienter und entspannter.

Links:

Allgemeine Infos:
http://www.mwbrooks.com/dvorak

Geschichtlicher Hintergrund:
http://home.t-online.de/home/ulf.bro/dvorak/Querty-fluch.html

Zur Kontroverse:
http://www.mwbrooks.com/dvorak/dissent.html
http://wwwpub.utdallas.edu/~liebowit/keys1.html

Dvorak7Min:
http://www.linalco.com/ragnar/dvorak7min-1.6.1.tar.gz

Wired WLAN

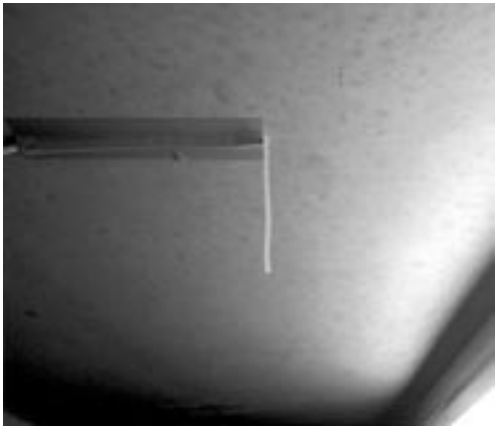
von Michael Holzt <kju@ccc.de>

Exklusiv für die Datenschleuder möchte ich von meiner etwas anderen Methode zwei Räume zu vernetzen berichten. Dank meiner netten Vermieterin konnte ich mir nämlich vor kurzem einen grossen Wunsch erfüllen: Endlich ein eigener Bastelraum für die diverse, in verschiedenen Verfallsstadien befindliche Hardware, wo auch ruhig kreative Unordnung herrschen darf. Frei nach dem Motto: Chaos in den Keller! Eine echte Empfehlung für den, der kreativ mit Technologie umgehen möchte.

Doch was benötigt ein anständiger Hack-Keller außer vier Wänden, Tischen und Regalen? Richtig: Elektrizität... und Netzwerk. Die Tatsache, dass keine Steckdose vorhanden war, konnte zum Glück in einer etwas abenteuerlichen Schrauberei unter Spannung mit dicken Gummihandschuhen und auf einem Müllsack stehend (zwecks Isolierung) gelöst werden. Blieb noch das Problem der Vernetzung. Wenn zwischen der Wohnung und dem Keller fünf Stockwerke und dicke Wände liegen, ist jede Hoffnung auf Wireless LAN vergebens. Powerline-Modems (welche auf Grund der Funkstörungen sowieso nicht zu empfehlen sind) waren auch keine Alternative, da es sich um verschiedene Stromkreise handelte.

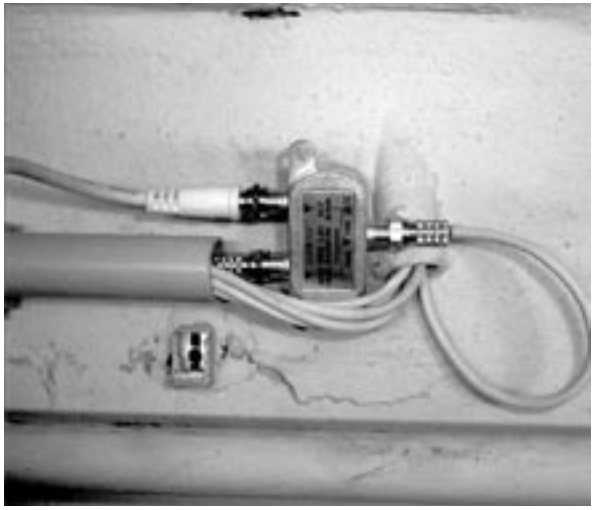
Doch in der Not kam ein Umstand zu Hilfe: Das Haus ist komplett für Kabelfernsehen ausgerüstet, und jede Wohnung wird durch ein eigenes Kabel versorgt, welches im Keller in einer Hausunterverteilung endet. Und besser noch: Die Kabel nehmen von dieser Verteilung einen Weg direkt durch meinen neuen Bastelkeller, in dessen Wänden sie dann im Steigrohr verschwinden. Diesen Umstand auszunutzen drängte sich geradezu auf. Doch wie bekommt man ein Signal über dieses Kabel, ohne für Störungen des Fernsehempfangs zu sorgen?

Als Funkamateur dachte ich natürlich sofort an eine Lösung mit Hochfrequenzsignalen, und die für die Vernetzung vorgesehene Funktechnik findet sich praktisch in jedem Hacker-Haushalt: Wireless LAN. Erste Versuche, das Signal über die Schirmung des Koaxkabels zu führen, schlugen leider fehl, also blieb nur noch die Möglichkeit das Wireless LAN Signal mitsamt dem Kabelfernsehsignal über den Leiter zu führen. Doch um dies ohne Störungen durchführen zu können, muß auf beiden Seiten Kabel-TV und WLAN zusammengeführt, respektive wieder getrennt werden. Es werden also Weichen und Filter benötigt.



Ein Selbstbau solchen Equipments wäre sicherlich auch nicht allzu aufwendig geworden, aber wie sich schnell herausstellte, hat der Kommerz bereits fertige Lösungen dafür entwickelt, wenngleich unter dem Namen "Sat-Einspeisung" und nicht "WLAN-Einspeisung". Werfen wir einmal einen Blick auf den technischen Hintergrund: Kabelfernsehen verteilt sich recht breitbandig über den Frequenzbereich 5 bis 862 MHz, wohingegen das von einem Sat-LNB abgegebene Signal zwischen 950 und 2400 MHz liegt. Da sich diese Signale also nicht in die Quere kommen, kam irgendwann jemand auf die Idee, diese einfach zusammenzuführen, um so sowohl Sat-TV als auch kabelgebundenes oder terrestrisch empfangenes Fernsehen über vorhandene Kabel führen zu können (z.B. um via Kabel-Fernsehen das Lokalprogramm zu bekommen und über Satellit die Sender, die nicht im Kabel verfügbar sind).

Dank dieser genialen Idee, die ihre Umsetzung in preiswert verfügbaren Weichen und Fernsehdosen fand, hatte ich nun eine Lösung für mein Problem. Zwar liegt das WLAN-Signal zwischen 2400 und 2500 MHz, und damit über der Spezifikation der Sat-Weichen, aber es war technisch nicht zu erwarten, daß dort gefiltert wird. Zumindest rief der günstige Preis von 4 Euro für eine Sat-Einspeiseweiche und 6 Euro für eine satfähige TV-Dose den Wunsch hervor, dies einfach mal auszuprobieren.



Bevor ich zu einer Erklärung meines Aufbaus komme, möchte ich die Auflösung vorwegnehmen: Der Testaufbau funktionierte nicht nur auf Anhieb, sondern sogar noch viel besser als ich es je vermutet hätte. Was ich also tat war folgendes: Die alte TV-Dose in der Wohnung wurde durch die neue Dose ersetzt. Dies war aus zweierlei Gründen notwendig: Zum einen hat die neue Dose eine F-Buchse für den Anschluß des Sat-Receivers. Dort wurde nun mein Accesspoint über ein selbstgebautes Adapterkabel RP-SMA auf F angeschlossen. Zum anderen war die alte Dose sowieso nur auf TV ausgelegt, und filterte das WLAN-Signal einfach weg.

Auf der anderen Seite, in meinem Keller also, wurde die Sat-Einspeiseweiche verbaut, wie auch auf dem Foto zu sehen ist. Auf der linken Seite befindet sich unten der Anschluss der Hausverteilung des Kabelfernsehens. Links oben ist der Anschluss für die Sat-Einspeisung, oder in diesem Fall für mein WLAN-Signal. Und auf der rechten Seite wird das zusammengeführte Signal abgegeben und verschwindet im Steigrohr, um in meiner Wohnung zu enden. Um etwas Luft in der Kabellänge zu gewinnen, musste ich übrigens, unter Angst von einem meiner Nachbarn dabei überrascht zu werden, ein neues Kabel von der Unterverteilung bis in meinen Keller ziehen. Zum Glück ließ sich das Schloß der Verteilung merkwürdigerweise zerstörungsfrei mit einem Schraubendreher öffnen...

An den Sat-Anschluss sollte nun eigentlich ein zum Client modifizierter Accesspoint oder eine Wireless LAN Karte angeschlossen werden. Dank der Spezifikationen von Wireless LAN, die vorsehen, daß eine Karte auch durch ein vollständig reflektiertes Signal nicht zerstört werden darf, ist es gefahrlos möglich, zwei WLAN-Sender direkt miteinander zu verbinden. Doch es kam ganz anders: Für einen ersten Test schloß ich einfach ein kurzes Stück Sat-Kabel an, an dessen Ende ich etwa 10cm der Schirmung entfernt hatte. Als mir mein Notebook, welches im Raum auf dem Tisch lag, anschließend eine Verbindung mit 48 MBit/s anzeigte, bin ich vor Überraschung dann auch fast aus den Latschen gekippt... Die Idee mit dem AP als Client war damit gestorben, und das abisolierte Kabel wurde einfach als Antenne an die Decke geklebt (siehe linkes Foto).

Etwas Feintuning an der Antennenposition hat noch etwas gebracht, ich freue mich über Werte wie folgende (an einer Prism54-Karte):

Bit Rate: 54Mb/s
Link Quality = 159/0
Signal level = -61 dBm
Noise level = -225 dBm

Das Experiment war also auf ganzer Linie erfolgreich und kann womöglich auch anderswo für ähnliche Probleme zum Einsatz kommen. Wenn die Signalqualität zu schwach ist, kann durch den Anschluss einer Karte auf der zweiten Seite mit Sicherheit eine saubere Verbindung mit voller Geschwindigkeit erreicht werden. Ein paar warnende Worte müssen allerdings dennoch sein: Die Lösung ist technisch nicht wirklich ganz sauber: Funk-Signale (wie auch WLAN) werden normalerweise über Kabel mit 50 Ohm Wellenwiderstand geführt, wohingegen Koaxkabel für Fernsehempfang 75 Ohm Wellenwiderstand haben. Die Verwendung des Kabelfernsehkabels führt hier also zu einer fehlerhaften Anpassung, was wiederum zu Reflektionen führt. Auf Grund der geringen Sendeleistung von WLAN-Karten sind hier aber weder Probleme noch Störungen zu erwarten. Und nicht vergessen die nach FTEG vorgeschriebenen Messungen durchzuführen und die Lösung CE zu zertifizieren, denn sonst macht Ihr Euch unter Umständen einer Ordnungswidrigkeit schuldig *zwinker*...

PS: Als nächster Schritt soll auch noch DECT über das Kabel geführt werden, damit ich auch endlich im Keller telefonieren kann. Dazu ist dann aber doch der Selbstbau einer Weiche notwendig.

Gläserner Patient 2004

von Manuela Münchow

Die Gesundheitsreform brachte nicht nur die Praxisgebühr, sondern auch den Gläsernen Patienten. Möglich wird dies durch der Kombination eines vorgeschriebenen Diagnoseschlüssels und der Übermittlung personenbezogener Daten für Abrechnungszwecke an die gesetzlichen Krankenkassen.

Ein grundlegender Schritt zur heutigen Situation wurde mit einer früheren Gesundheitsreform gelegt. Seit dem 1.1.2000 müssen Abrechnungsdaten in maschinenlesbarer Form übermittelt werden; zusätzlich ist die Verwendung des WHO-Diagnoseschlüssels "ICD10" (International Classification of Diseases and Related Health Problems, 10th edition) für einheitliche Diagnosekriterien generell eingeführt worden.

Dabei gab es verschiedene Editionen für den ambulanten und den stationären Bereich. (Zuvor wurde nur in der stationären Behandlung die Vorgängerversion ICD9 eingesetzt.) Schon damals wurde die Verwendung eines Diagnoseschlüssels zur Standardisierung der ärztlichen Bewertungen von Ärzten heftig kritisiert. [1, *2]

Während im stationären Bereich direkt mit den Krankenkassen abgerechnet wird, läuft die Abrechnung im ambulanten Bereich über die Kassenärztlichen Vereinigungen als Zwischenstelle. Damals war die Abrechnung im ambulanten Bereich, bis auf wenige Ausnahmen, fallbezogen und damit anonym, während die gesetzlichen Krankenkassen alle Abrechnungsdaten aus dem stationären Sektor versichertenbezogen erhielten. Am 1.1.2004 trat das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung - GKV-Modernisierungsgesetz (GMG) [3] in Kraft. Dabei gab es grundlegende Eingriffe in den Abrechnungsmodus - die Vergütung wurde von Kopfpauschalen auf morbiditätsorientierte Regelleistungsvolumina umgestellt.

Die gesetzlichen Krankenkassen erhalten jetzt alle Daten mit der zugehörigen Krankenversichertennummer (SGB V § 106a, 284, 295, 301 [4]). In einer Veröffentlichung des Datenschutz Hessen heißt es hierzu:

"Infolge dieser neuen versichertenbezogenen Übermittlung der ärztlichen Abrechnungsdaten in der ambulanten Versorgung erhalten die Krankenkassen erheblich mehr personenbezogene medizinische Daten der Versicherten als bisher. Dass dies durch das neue Vergütungssystem zwingend geboten ist, wurde den Datenschutzbeauftragten bisher nicht ausreichend dargelegt. Die Datenschutzbeauftragten sind zu diesen im Schnellverfahren realisierten Änderungen des ursprünglichen Gesetzentwurfs nicht rechtzeitig und nicht ausreichend beteiligt worden. Dadurch war u. a. eine Diskussion über Möglichkeiten der Pseudonymisierung der Versichertendaten nicht möglich. Bei der künftigen Umsetzung der neuen Regelungen muss sichergestellt werden, dass keine umfassenden Versichertenprofile bei den Krankenkassen entstehen und die Daten ausschließlich zweckgebunden verwendet werden" [5]

Darüber hinaus sollen die Leistungs- und Abrechnungsdaten aller Versicherten pseudonymisiert in einem zentralen Datenpool zusammengeführt werden (SGB V §303a ff. [4]), was im Detail weitere Fragen des Datenschutzes aufwirft. Gleichzeitig wurden die verschiedenen Editionen der ICD-10 für den ambulanten und den stationären Bereich zusammengeführt zur ICD-10-GM (German Modification) [6], die vom Deutschen Institut für Medizinische Dokumentation und Information (DIMDI) im Geschäftsbereich des Bundesministeriums für Gesundheit und Soziale Sicherung (BMGS) betreut wird. Dieser Diagnoseschlüssel beinhaltet medizinische und psychologische Schlüssel, darunter auch Informationen über die Persönlichkeit und die Lebensumstände der Patienten wie "Psychische und Verhaltensstörungen" (Kategorie F), oder "Faktoren, die den Gesundheitszustand beeinflussen und zur Inanspruchnahme des Gesundheitswesens führen" (Kategorie Z).

Darüber hinaus enthält er einige obskure Zustandsbilder und teilweise diskriminierungsträchtige Informationen, die das Privatleben der Patienten gefährlich bloßlegen können. Ob solche Daten für die Krankenkassenabrechnung wirklich nötig sind, ist zweifelhaft. Z.B. "Beratung in Bezug auf Sexualorientierung, -einstellung oder -verhalten" (Z70; schließt auch Beratung für Dritte mit ein!), "Probleme mit Bezug auf die Lebensführung" (Z72), "pathologisches Spielen" (F63.0), "gesteigertes sexuelles Verlangen" (F52.7), spezielle sexuelle Vorlieben ("Störungen der Sexualpräferenz" (F65) mit "Fetischismus" (F65.0), "Fetischistischer Transvestitismus" (F65.1), "Sadomasochismus" (F65.5), ...).

Zumindest bei einem Teil der Patienten, denen diese Zusammenhänge bekannt sind, erzeugt die versichertenbezogene Datenübermittlung Misstrauen und kann

das Arzt-Patienten-Verhältnis belasten. Vor allem für den psychotherapeutischen Bereich kann ein massiver Vertrauensverlust befürchtet werden, was sich negativ auf die Behandlung auswirken kann [7].

Nicht umsonst fand das Arzt-Patienten-Verhältnis schon im "Hippokratischen Eid" besondere Beachtung durch den Satz " Über alles, was ich während oder außerhalb der Behandlung im Leben der Menschen sehe oder höre und das man nicht nach draußen tragen darf, werde ich schweigen und es geheimhalten." [8] Diese Entwicklung kann also weder im Interesse der Ärzte noch in dem der Patienten sein. Das grundlegende Problem ist, dass ein Instrument, das für statistische Erhebungen und Auswertungen konzipiert wurde, auch für Abrechnungszwecke eingesetzt wird. Während für ersteren Verwendungszweck möglichst detaillierte Datensätze sinnvoll sind, aber anonyme Daten völlig ausreichen, sind für die neue Anwendungsmöglichkeit personenbezogene Daten erwünscht.

Das Bundesministerium für Gesundheit und Soziale Sicherung erhofft sich durch "Datentransparenz" Möglichkeiten zur Kosteneinsparung [9], während der Vorteil für die Krankenkassen durch Missbrauchsvorbeugung und Effizienzsteigerung offensichtlich ist. Hier haben aber die Patienten ein berechtigtes Interesse am Schutz und einer Beschränkung der Verbreitung sensibler Daten. Aus Sicht des Datenschutzes ist es also höchst zweifelhaft, ob das wirtschaftliche Interesse der Krankenkassen und des Ministeriums eine personenbezogene Datenerhebung in dieser Detailliertheit rechtfertigen. Darüber hinaus wurde hier die Grundlage für eine bedenkliche mögliche zukünftige Entwicklung geschaffen. Krankenkassen können ein Interesse daran haben, Patientendaten über Generationen hinweg zu speichern und zu nutzen für statistische Auswertungen und zur Erstellung von Familienkrankheitsgeschichten. Mit zukünftigen Gesetzesänderungen könnten die maximalen Aufbewahrungszeiten für diese Daten ausgedehnt oder ganz aufgehoben werden, darüber hinaus könnten weitere Stellen eine Zugriffsberechtigung auf diese Daten erhalten.

Welche Konsequenzen bzw. praktischen Maßnahmen kann man als Patient ergreifen, um seine persönlichen Daten zu schützen? Es gibt für den Patienten keine sichere Möglichkeit der Einflussnahme bzw. Kontrolle, welche Informationen bei der Krankenkassenabrechnung die Praxis verlassen. Welche Daten abrechnungsrelevant sind und welche nicht, liegt im Ermessen des behandelnden Arztes. Als Patient kann man nur seinen Arzt auf die Datenschutzproblematik aufmerksam machen und bei sensiblen Kontaktanlässen auf seine Diskretion und sein Taktgefühl bei der Diagnoseverschlüsselung vertrauen. Wem das nicht genug Sicherheit gibt oder wer gänzlich Datenspuren vermeiden will (z.B. bei einer psychotherapeutischen Behandlung), der kann nur noch darauf verzichten, die Leistungen seiner Krankenkasse in Anspruch zu nehmen.

Man muss sich einen Arzt suchen, der bereit ist, seine Dienste direkt in Rechnung zu stellen. Zur Vermeidung von Pannen sollte man dabei darauf achten, seine Krankenkassenkarte auf gar keinen Fall auszuhändigen. Dabei muss man berücksichtigen, dass in einer Arztpraxis die Krankenkassenkarte nur einmal pro Quartal in den Kartenleser eingelesen werden muss. Wer sehr vorsichtig sein will, kann dazu noch getrennte Ärzte für Kassenabrechnungen und "Privatangelegenheiten" nutzen und sensible Informationen entsprechend trennen. (Wenn man schon bei Datenschutz im Gesundheitswesen ist: es ist auch interessant zu wissen, dass Schweigepflicht-Entbindungserklärungen beim Abschluss einer privaten (Zusatz-)Krankenversicherung nur in begrenztem Umfang zulässig sind [10].)

Es gibt auch eine aktuelle und umfangreiche Materialsammlung zu diesem Thema im Internet [11]

Quellen:

[1] *http://www.haeverlag.de/archiv/n1198_2.htm* Niedersächsisches Ärzteblatt ICD10-Pro und contra

[2] *http://www.bundesverfassungsgericht.de/entscheidungen/frames/2000/4/10* Bundesverfassungsgericht: "Verschlüsselungspflicht von Krankheitsdiagnosen in der vertragsärztlichen Versorgung nach dem Diagnoseschlüssel ICD 10-SGB V"(BverfG, 1 BvR 422/00)

[3] *http://www.bmgs.bund.de/downloads/GKV_Modernisierungsgesetz.pdf* GMG (BGBl. I 2003, 2190)

[4] *http://www.bmgs.bund.de/download/gesetze_web/sgb05/sgb05xinhalt.htm* SGB V

[5] *http://www.datenschutz.hessen.de/Tb32/K14P01.htm* Datenschutz Hessen: "Datenschutzrechtliche Aspekte der Reform der gesetzlichen Krankenkassen"

[6] *http://www.dimdi.de/de/klassi/diagnosen/icd10/ls-icdhtml.htm* ICD-10-GM online beim DIMDI

[7] *http://www.bvvp.de/qualitaet/datensicher.html* Bundesverband der Vertragspsychotherapeuten e.V.: "zur Datensicherheit in der Psychotherapie" (Anm.: veraltet in Bezug auf Situation im Datenschutz)

[8] *http://www.ruhr-uni-bochum.de/zme/bauerhip.htm* Hippokratischer Eid

[9] http://www.die-gesundheitsreform.de/glossar/datentransparenz.html Glossar des BMGS zur Gesundheitsreform: "Datentransparenz"

[10] *http://www.datenschutzzentrum.de/material/themen/gesund/versentb.htm* Unabhängiges Landeszentrum für Datenschutz zu Schweigepflicht-Entbindungserklärungen

[11] *http://www.bvsm.de/icd10/* Aktuelles und umfangreiche Materialsammlung bei der Bundesvereinigung Sadomasochismus e.V.

Buchbesprechung "Trusted Computing"

"Trusted Computing", herausgegeben von Prof. Dr. Christian Koenig, ist im Verlag "Recht und Wissenschaft" erschienen. Der Verlag ist bekannt für seine "Reihe Kommunikation und Recht", in welcher technische Sachverhalte aus juristischer Perspektive beleuchtet werden. Das Buch gliedert sich in drei Teile: Technik, Recht und Gesellschaftliche Implikationen.

Der erste Teil erklärt leicht verständlich die technischen Grundlagen von TCPA und DRM Systemen. Allerdings liegt hier die veraltete TCPA Spezifikation v1.0 zu Grunde. Jedoch werden gegen Ende des Buches Ausblicke auf TCPA v1.2 nachgeliefert. Im zweiten Kapitel wird die zentrale technologische Kritik an TCPA/Palladium knapp zusammengefasst. Unter anderem stellen die hier angeführten Zitate großer Unternehmen die behauptete Neutralität der DRM Technologie schwer in Frage.

Im zweiten großen Abschnitt wird ausführlich auf die rechtlichen Konsequenzen des "trusted computing" im Hinblick auf Wettbewerbsrecht, Patentrecht sowie Datenschutz und Urheberrecht eingegangen. Die überraschend zahlreichen und vielfältigen Probleme, die sich hier auftun, bieten dem interessierten Techniker einen durchaus lehrreichen Einblick in die Welt der Paragraphen.

Aus dem dritten Teil des Buches ist besonders der Artikel von Volker Grassmuck zu empfehlen. Er schafft es, die aus der neuen Technologie resultierenden, gesellschaftlichen Implikationen fundiert und überzeugend als Bedrohung unserer Rechte darzustellen

Das durchweg gelungene Bemühen, das komplexe und anspruchsvolle Thema TCPA so verständlich und facettenreich wie möglich darzustellen, machen dieses Buch zu einer lohnenswerten und informativen Lektüre.

Neben dem sehr aufschlussreichen Kapitel von Koenig/Neumann zur rechtlichen Lage gehören die Artikel von Volker Grassmuck und Rüdiger Weis zur Pflichtlektüre eines jeden, der sich mit TCPA auseinandersetzen möchte. Beide haben die Bemühungen des CCC um eine fachliche Diskussion in der Vergangenheit entscheidend begleitet und vorangetrieben.

Wer sich das Buch nicht gleich kaufen will, kann die Thesen von Rüdiger Weis in der Datenschleuder 82, Seite 12 finden. Einen Ausblick auf mögliche Konsequenzen von TCPA bietet ein Artikel in der Datenschleuder 80 auf Seite 8.

Abschließend sei allen, deren Interesse an diesen oder verwandten Themen geweckt wurde, hier nochmal das Buch "Free Software" von Volker Grassmuck empfohlen.

ISBN: 3-8005-1341-2

Autor: Koenig, Prof. Dr. Christian/Neumann, Andreas/ Katzschmann, Tobias (Hrsg.)

Bestellungen, Mitgliedsanträge und Adressänderungen bitte senden an:

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

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

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

Die Kohle

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

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

Name: _____

Straße / Postfach: _____

PLZ, Ort _____

Tel.* / Fax* _____

E-Mail: _____

Ort, Datum: _____

Unterschrift _____

*freiwillig

21C3

the usual suspects