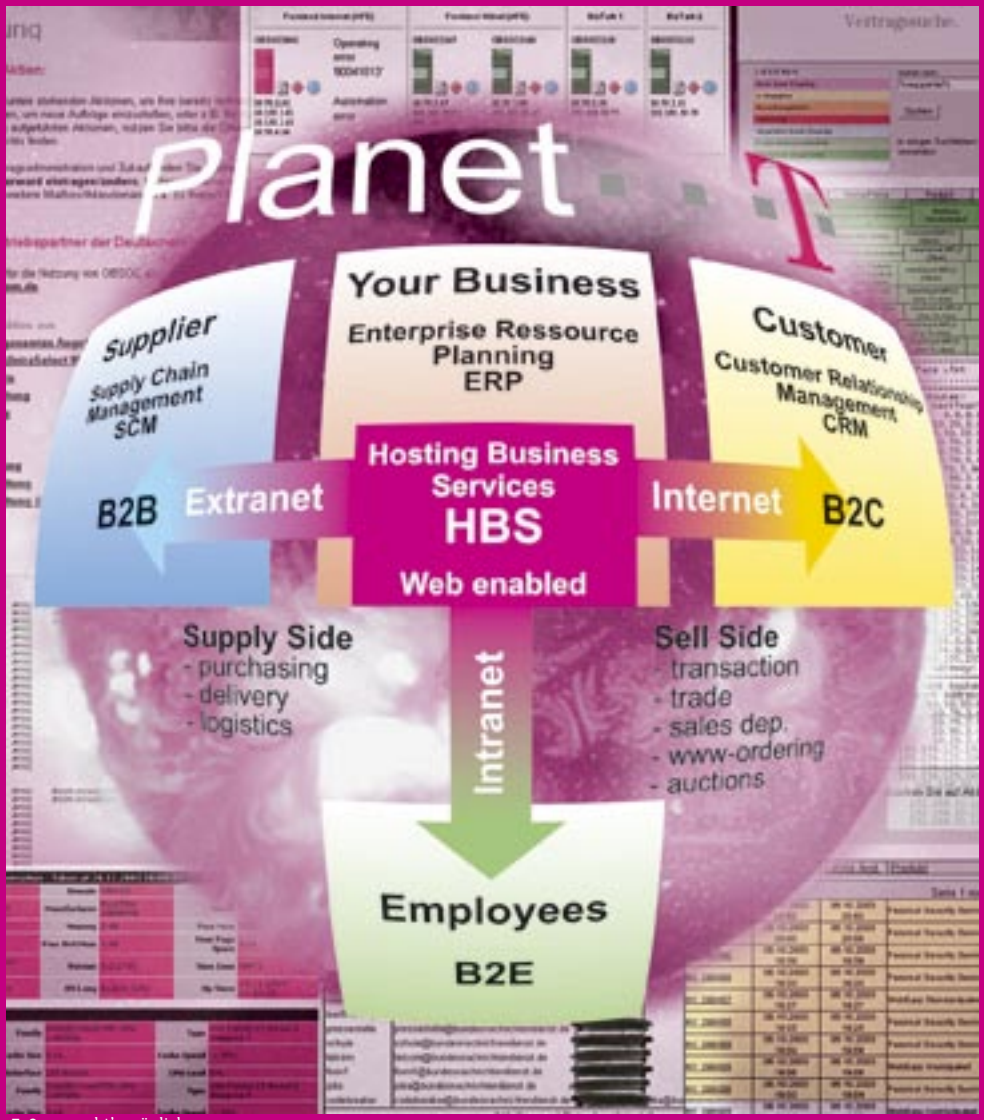
die datenschleuder.

das wissenschaftliche fachblatt für datenreisende
ein organ des chaos computer club



T-Com macht's möglich

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

#83

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. 83

Herausgeber *(Abos, Adressen, Verwaltungstechnisches etc.)*
Chaos Computer Club e.V., Lokstedter Weg 72, D-20251 Hamburg, Fon: +49.40.401.801.0, Fax: +49.40.801.401.41, <office@ccc.de> 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: +49.30.285.997.40, <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, Alexander Ehmann. Titelbildcollage: Christina Düster.*

Redakteure dieser Ausgabe

Tom Lazar <tomster>, Dirk Engling <erdgeist> und Corinna.

Autoren dieser Ausgabe

Bastian Ballmann, Alexander Bernauer, Volker Birk, Heinrich Dubel, Dirk Heringhaus, Andy Müller-Maguhn, Mario Manno, Sascha May, neingeist, padeluun, Tim Pritlove, Markus Schaber, Timon Schröter, Starbug, Steini, Alexander Taute, Lars Weiler und Wetterfrosch.

Unbegrenzte Möglichkeiten

Aufgrund der aktuellen weltpolitischen Lage, speziell der Terrorgefahr, sehen wir uns als Redakteure eines staatstragenden, hurrapatriotischen Blattes förmlich gezwungen, die gesamte Redaktion für andauernde Überwachung zu öffnen.

Wir haben uns (natürlich) für den bequemstmöglichen Weg entschieden und alle wichtigen Vorkommnisse diesmal in Form eines DIN A5-Heftchens distilliert. Damit wurde dem Justizministerium die Möglichkeit der direkten Einsichtnahme gegeben. Wir hoffen, damit die aufwändige Installation einer Telefonanlage zu vermeiden.

Daß eine solche heuer nicht mehr unbedingt von Großmutter •••T• beauftragt werden muß (die sich übrigens nicht nur als unterdurchschnittliche Programmiererin, sondern auch als schlechte Verliererin geoutet hat, siehe dazu Seite 16), tröstet nur kurzzeitig. Aufmerksame Leser haben Gebahren, die man sonst nur von magentafarbenen Firmen kennt (man beachte das sorgfältig gewählte Titeldesign), auch bei deren blauroten Konkurrenz aufgedeckt (dazu mehr in den Leserbriefen, Seite 5).

In dieser Ausgabe haben wir penibel darauf geachtet, die inzwischen patentrechtlich geschützten Buchstaben „ “ und „ “ nicht in das Blatt einfliessen zu lassen und haben diese durch Platzhalter ersetzt. Vom Abdruck patentverdächtigen C-Programm-Quelltexten (so z.B. auf Seite 15) haben wir ebenfalls abgesehen.

Aufgeschreckt „von den miserablen Abschneiden bei der Piser-Studie“ steht Volksbildung nun auch in der Datenschleuder voll im Kurs. Wir verstehen uns als Ganztagsschule in Papier. Dazu werden Grundlagen der Kfz-Elektronik (siehe Seite 24), des modernen Niedrigenergie-Kurzstreckenfunks (Seiten 10 bis 15) und der Sourcecodecompression noch modernerer Programmiersprachen (Seite 44) abgerundet durch gesellschaftspolitsch weltanschaungsbildend wertvolle Beiträge zur Überwachung (Seite 47) und dem organisierten demokratischen Widerstand gegen Unterhaltungsfirmenwillkür (Seite 28-32).

Der Heimatkundeunterricht treibt uns in verfallene Signalintelligenzstationen auf Berliner Trümmerbergen (Seite 22) und beschreibt anschaulich, wie auch angeblich noch viel zu kleinen Jungs ihre 15 Minuten Ruhm zugestanden werden, dazu mehr auf Seite 40.

Aus der Rubrik „wir über uns“ – neuerdings „Community“ – sind ein Bericht von der letzten Gulaschprogrammiernacht zu vermelden (Seite 33) und natürlich der Call-for-Papers zum nächsten Congress (Seite 43). Dessen neue Einteilung in die Themenbereiche Hacking, Science, Community (da war es wieder!), Society und Culture stellt dabei eine interessante Erweiterung dar.

Für Heinrich Dubel bedeuten sie freilich trotzdem nur „too little, too late“. Sein Artikel zum Thema „Nazi-Ufos“ wäre auch im Dezember nur schwerlich in einen dieser Bereiche einzuordnen. Abdrucken tun wir in natürlich trotzdem. Ab Seite 34.

Aus der Rubrik „da müssen wir bald ne Rubrik draus machen“ gibt es einen weiteren hochkarätigen Artikel zum Thema Biometrie. Unser ganz eigenes Technologiefolgenabschätzungsbüro (sic!) hat sich eines Papers seines Pendants im Bundestag angenommen – Details ab Seite 8.

Alles in allem kann man sagen, daß sich die Wartezeit auf diese Datenschleuder mal wieder gelohnt hat. Nicht, daß wir Euch eine Wahl gelassen hätten, aber wir geloben Besserung.

In diesem Sinne,

tomster und erdgeist.

Inhalt

hallo, ich brauche...

Informationen über das neue Premiere.mfg *<rene-ist-ok@xxx.de>*

Die Premiere-Hotline findest Du unter der Rufnummer 0180/5152553. <kju>

Hi, hab ein Problem

mit einer *.rar file. Hab aus spass 10 fotos von 2 Mädchen (ganz normale Fotos wo sie iner klasse sitzen) in ein zip gepackt und in "Name1 + Name2 Nackt dusche sonne" umbenannt und inen emule gestellt. dieses .rar hab ich aber mit nem passwort belegt (einfch mit der flachen hand auf die Tastatur gedrückt, ergo ich kenn das Passwort nicht.) Die beiden haben das aber jetzt rausgefunden und wollen natürlich jetzt bewiesen haben dass da wircklich nur die harmlosen bilder drin (es gibt auch noch "andere" von ihnen). Darum wollte ich hier anfragen ob sie mir vlt. eine Methode berrichten könnten. (ich hab auch ihren FAQ gelesen und auch gesehen das man keine PW erfragen soll) aber das is meine letzte chance. Die einzigste Möglichkeit die ich kenne waere Brute Force, aber sinnlos das das PW bestimmt mehr asl 15 zeichen hat.

MfG *<timon@xxx.yy>*

Deine Geschichte klingt unglaubwuerdig, weil es in der Regel so ist, dass eine wiederholte Eingabe des Passwortes erforderlich ist. Das wird sicher bei RAR auch so sein. Wenn du es zweimal geschafft hast, das gleiche Passwort auf diese Weise einzugeben, dann wirst du es sicher auch ein drittes Mal schaffen.

Nichtsdestotrotz hat mir deine Geschichte gefallen. Das war mal was anderes. <dirk>

gibt es eine Liste,

in der man nachsehen kann, in welchem Land welche Verschlüsselungsstärke erlaubt ist (https)?

In Frankreich darf man, so gut ich weiss z.B. nur mit 56 Bit verschlüsseln...

Wenn es eine solche Liste gibt, wäre es sehr nett, wenn ihr sie mir zur Verfügung stellen könntet. *<udo.xxx@yyy.de>*

so pauschal kann man das nicht sagen. Das hängt von vielen Faktoren ab.

Ein Einstieg (etwas veraltet):
http://rechten.kub.nl/koops/cryptolaw/cls2.htm

Ansonsten willst Du in einer Bibliothek nach dem "Handbuch der Exportkontrolle (hadex)" suchen,

http://www.ausfuhrkontrolle.info/publikationen.htm#4
http://www.dieckmann-verlag.de/index.php?area=shop&level=search&search=Y113.000 <Julius>

kurz darauf:

Ist es wirklich so schwer?

Ja. Werden Sie bloss kein Crypto-Hersteller.

Ich will doch nur aus diversen Ländern auf eine HTTPS-Seite in Deutschland zugreifen können. Gibt es da nichts einfacheres als hunderte von Seiten und Gesetze zu studieren ?

Hintergrund: Wir betreiben hier eine Citrix Serverfarm und wollen das unsere Aussendienstmitarbeiter darauf über https zugreifen können. Nun hat man mir gesagt, das das z.B. auf Frankreich nicht geht, da wir eine 128-Bit-Verschlüsselung verwenden.

a) nach meinem Verständnis gilt das für Frankreich seit ein paar Jahren nicht mehr. Inzwischen darf man dort als Bürger ordentlich verschlüsseln.

b) es gibt möglicherweise einen Unterschied, ob der Mitarbeiter ein Franzose oder ein Deutscher ist, der aus Frankreich einen HTTPS Server in Deutschland anspricht.

Vielleicht gibt es ja doch eine einfachere Möglichkeit Informationen zu bekommen ?

Der CCC befürwortet den "vorausschauenden" Umgang mit Gesetzen. Sprich: Ignoriere alles, was der Staat nicht durchhalten kann oder sollte -- dazu gehören z.B. Verschlüsselungsverbote. Daher hat der CCC keine Notwendigkeit, eine solche Liste zu pflegen.

Als Unternehmen wollen Sie sich wahrscheinlich an Gesetze halten. Aber fragen Sie doch jemanden, der das wissen sollte, z.B. die Firma Citrix. Die haben bestimmt viele Kunden, die dasselbe Problem hatten. <ron>

ich habe kuerzlich eine mail an mail@ccc.de geschrieben:

wenn ich von autoscout24 aus eine empfehlung eines autos an eine email schicken lasse, wird bei dem empfaenger tatsaechlich der absender angezeigt den ich dort angegeben habe:, bsp.: Absender : <webmaster@google.com> Betreff: ....., wie machen die das? MfG *<xxx@lycos.de>*

darauf kam eine antwort von kju

Sie machen es einfach. Im richtigen Leben hindert Dich auch niemand daran, auf einen Brief einen falschen Absender zu schreiben. Im Internet geht das auch, siehe auch diese Mail (der Absender ist natürlich falsch). <kju>

nur sieht es bei kju so aus:

Absender: " George W. Bush" <kju@ccc.de>

bei autoscout 24 sieht es allerdings so aus: Absender: <papst@vatikan.it>

nun wuerde ich gerne wissen wie machen die das? und wie kann ich soetwas machen?

kju war zumindest so höflich, noch ein paar Teile des Headers so zu belassen, dass Du noch zuordnen kannst, woher die Mail kam. Im übrigen... ;o)

...war Dir offensichtlich auch noch nicht aufgefallen, dass kju sogar die "Reply-To"-Adresse ebenfalls auf dem gültigen "mail@ccc.de"-Adresseintrag belassen hatte. Dadurch war es Dir überhaupt noch möglich, auf "Antworten" zu klicken, um trotzdem wieder direkt an mail@ccc.de zu antworten.

Insgesamt gibt es für den Rückkanal drei relevante Einträge:

- Das "From"-Feld:
Hier kannst Du alles eintragen, z.B. G.W. Bush, wer Outlook benutzt, sieht oft nur diesen Eintrag, weil man für mehr Infos extra rumklicken müsste.

- Das "Reply-To"-Feld:
Wenn der Empfänger auf "Antworten" klickt, geht die Antwort hierher.

- Das "Return-Path"-Feld:
Wenn die Mail nicht zustellbar ist, wird sie hierhin zurückgeschickt.

Welche Einträge Du nutzen kannst, hängt von Deinem Mailprogramm und von Deinem Mailserver (bzw. dem Deines Providers) ab. <Rainer>

In der von euch verfassten Hacker-Ethik

ist der dritte Punkt, "Mißtraue Autoritäten - fördere Dezentralisierung". Wie genau meint Ihr das? Also Dezentralisierung heißt ja "gleichmäßige Verteilung" aber in diesem Zusammenhang verstehe ich das nicht wirklich. Könntet Ihr mir das erklären?

2. Im Hackers Blackbook

wird beschrieben, dass ein Hacker "hack values" zu schätzen weiß. Was sind die "Hack values"? Übersetzt heißt das ja soviel wie Hacker Werte, aber was für Werte sind denn das? Darf man sich grundsätzlich nicht in Bestimmte Firmen einhacken oder was? <The_Killer@xxx.de>

zu 1:) Die Hackerethik ist, wie du auf unserer Seite sicher gelesen hast, nicht von uns sondern im Wortlaut von Steven Levy. Lediglich zwei Punkte hat der Club nachtraeglich zur Hackerethik beigetragen.

Dezentralisierung/Dezentralitaet ist hier zu verstehen als Gegenteil von Zentralisierung. Es geht darum, dass man sich nicht auf eine einzige Stelle verlaesst. Das kommt auch beim Stichwort "misstraue Authoritäten" zum Vorschein.

zu 2:) Vorweg: Dieses Blackbook hat nix zu tun mit dem CCC. Im Zweifelsfall ist der Autor dieses Buches ein probater Ansprechpartner.

hack value *n. Often adduced as the reason or motivation for expending effort toward a seemingly useless goal, the point being that the accomplished goal is a hack. For example, MacLISP had features for reading and printing Roman numerals, which were installed purely for hack value. See display hack for one method of computing hack value, but this cannot really be explained, only experienced. As Louis Armstrong once said when asked to explain jazz: "Man, if you gotta ask you'll never know." (Feminists please note Fats Waller's explanation of rhythm: "Lady, if you got to ask, you ain't got it.")*

Woher weiss ich das? Das steht so im New Hackers Dictionary aka Jargon File. Wie hab ich das so schnell gefunden? Google! Erster Treffer.

Die Frage, was du darfst, was du nicht darfst, was du solltest und vieles mehr, ist etwas schwer zu beantworten. Rechtlich gesehen darfst du dich vermutlich nicht in Firmen "einhacken", was immer du damit genau meinst. Vom Standpunkt der Moral: Frag dich das selbst.

Pragmatisch gesehen vermeidest du in jedem Fall Aerger, wenn du dich auf deinen eigenen Compuer beschraenkst. <sascha>

eine weitere Antwort:

Im Original heißt es wohl eher "hinterfrage Authoritäten". Ich finde das ebenfalls besser, als generell "Mißtrauen" zu fördern. <padeluun>

Auch erfreuliches erreicht uns als Auto-Reply auf unsere Antworten:

Sehr geehrter Mail-Sender, ich habe nach über 5 Jahren die Redaktion COMPUTERBILD verlassen.

Sie erreichen mich jetzt unter der Adresse *<xxx@web.de>*

Herzlichen Glückwunsch ;-) <Frank>

kurz darauf:

GRINS

War aber eine schöne Zeit! Mein Vater kann mich jetzt nicht mehr mit DAU-Fragen nerven - Hat sich also gelohnt ;-) MfG ...

hallo ccc-cracks,

folgendes mehr oder weniger spaßige ereignis fand vor einer knappen viertelstunde statt: nach einer sendung auf dem NDR, in der es um einen deutschen hisbollah-aktivisten ging, der vor einer weile bei dem gefangenenaustausch zwischen israel und palästina

nach deutschland abgeschoben wurde, setzte ich mich, neugierig, wie ich bin, an meinen pc und tippte nichts böses ahnend den namen dieses menschen in die suchmaschinen-maske.

Es dauerte keine 5 sekunden, als meine firewall Alarm schlug wegen eines (vermeintlichen) ddos. ich bekam nämlich per icmp, udp (per traceroute) und per dns-anfragen (??? what the...?) schlagartig besuch aus aller herren länder (bzw. vornehmlich aus san jose, california, USA, aus chicago, illinois, USA, aus london, aus japan und aus frankfurt/main, außerdem aus boston und santa clara).

Bevor ich mich nun daran mache, auszutüfteln, wem die IPs vom jeweils letzten hop meiner "gegen-traceroutes" gehören, frage ich mal euch experten, an wen ich mich mit sowas vertrauensvoll wenden kann? Würde mich doch mal brennend interessieren, wer da so neugierig ist! hat google da nur eine neue einkommensquelle entdeckt, die ich nicht verstehe? oder stehe ich jetzt auf der verdächtigen-liste des nsa? *g*

dankbar für jeden hinweis, euer carsten

ps: falls jemand von euch die arabische übersetzung des wortes "bombe" kennt, sagt mal bescheid! mal sehen, ob die selben IPs wieder auftauchen! *gg*

Wahrscheinlicher ist, dass du auf einer der Seiten, die Google dir geliefert hat, im httpd-log gelandet bist, oder dass die Aktion wenigermit der Googlesuche zu tun hatte, als vielleicht mit Streitigkeiten im IRC o.aeh.

Aber trotzdem ist es gut, dass du hinterfragst, welch massive Datensammlung allein schon Suchanfragen gepaart mit IP bei Google hinterlassen. Vielleicht doch besser, nicht nach "how to kill the president of the united states" zu suchen. Vor allem, wenn du, wie ich annehme, google nicht per https besuchst und eigentlich jeder unterwegs mitlesen kann. <erdgeist>

Bin vor kurzem auf den IMSI Catcher

zum Abhören von Telefongesprächen im GSM-Netz gestoßen und mich würde interessieren, wie dieser genau funktioniert. Im Google findet man leider nur relativ oberflächliche Infos darüber.

Ich habe gesehen, dass es auf eurer jährlichen Konferenz im Jahre 1997 und 1998 Vorträge zu dem Thema GSM-Unsicherheiten und GSM-Hacking gegeben hat. Gibt es zu diesen Vorträgen auch schriftliches Material, das sich mit dem Thema IMSI-Catcher befasst. Oder kann mir jemand den Kontakt zu den damaligen Referenten herstellen? Vielen Dank schon mal. *<xxx@gmx.de>*

http://kai.iks-jena.de/miniwahr/imsi.html ist da nicht schlecht. Wenn Dich Details interessieren, dann findest Du auf http://pda.etsi.org/pda/queryform.asp die entsprechenden Standards. <volker>

Liebe(r) CCC Mail-In-Leser(in),

Da ich nach reiflicher Überlegung und unter verurteilungswürdigem "Gebrauch fremder Datenschleudern" bin ich zur Einsicht gekommen, daß allein der Erwerb zum eigenen Gebrauch mein Gewissen und auch meinen Zadizismus (ein Hilfsausdruck eines Freundes zur Sammelwut meiner Frau) befriedigen kann.

Soweit so gut, nur ich lebe im fernen Russland, vonwo Geld anzuweisen nach deutschen Landen es einer IBAN (International Bank Account Number) und eines BIC (Bank Identifier Code) bedarf....<>Also bitte ich folgerichtig um einen um eben diese Angaben erweiterte Bankverbindung, um meinen längst fälligen Beitrag entrichten zu können. Besten Dank & Gruß aus Moskau, *Hermann T.*

Moin, moin, danke für Deinen Entschluss, uns zu unterstützen. Die notwendigen Angaben für die Überweisung stehen hier: http://www.ccc.de/club/office

Ich möchte euch gerne eine juristische

Frage stellen, denn ich habe ein Problem.

Ich habe letztens ein Programm mit einer "serial" freigeschaltet, um dies testen zu können. Nun hat das Programm anscheinend bei dem Freischaltvorgang die illegale serial an den Hersteller gesendet und irgendwie verglichen, und somit das illegale an der sache festgestellt.

Daraufhin wurde das Programm gesperrt und folgende Daten "unter anderem" auf deren Server gespeichert : Email Adresse, Datum/Uhrzeit, IP-Adresse, Lizenzname

Dann erhielt ich eine email mit dem Hinweis dass ich eine Woche Zeit habe das Programm zu lizensieren. Ansonsten würden sie rechtlich dagegen vorgehn und die 3fache Lizenzsumme einklagen.

Nun haben meines wissens Anwälte von Internet-Dingen keine Ahnung und ich weiß nich wo ich mich nach der rechtlichen Grundlage informieren soll und hoffe einer von euch kann mir helfen.

Ich möchte also wissen ob deren Drohung real ist, oder ob das bloß ein Bluff ist um auf diese Art und Weise Lizenzen zu verkaufen.

Vielleicht ist es auch illegal Benutzerdaten abzuspeichern, in Verbindung mit ner serial? (so wie bei windows ja auch..)

Leider habe ich schon eine email zurückgeschickt in der ich mich entschuldigen wollte um somit eine Klage abzuwenden, leider meinten sie, sie müssten gegen jeden Fall rigeros vorgehen...

Wenn ihr mir mit Quellen oder Wissen helfen könnt bin ich euch sehr dankbar! *<Hann0r@xxx.de>*

Hallo "Hann0r", juristische Auskunft dürfen, können und wollen wir nicht erteilen.

Sollte aber ein Programm ohne Dein Wissen persönliche Daten von Deinem Rechner an einen Dritten übermittelt haben könnte das unter Umständen je nach Sachlage eine Datenspionage sein, welche durch 202a StGB strafbewährt ist. Wenn Du keine Angst vor einer Verfolgung eigener Taten hast, kannst du ja mal Anzeige bei der Staatsanwaltschaft erstatten.

Weiter ins Detail möchte ich allerdings nicht gehen. <Julius>

also hi vielleicht kennt ihr mich ja noch

habe eine kleine frage :dies ist ein verschlüsselter text 1ygydzxbuxu ich kann leider nicht herrausfinden was für eine verschlüsselung das ist könnt ihr mir helfen? schreibt mir die verschlüsselungs art oder noch besser die verschlüsselungsart und den entschlüsselten text bitte bitte zurück is wichtig !thx *<regcrash@xxx.de>*

Die Verschlüsselung ist 'FOOBAR', und der Text lautete: 'Wer das liest ist doof'. Der Absender scheint Dich also zu kennen. <kju>

kurz drauf:

bist du dir sicher mit der verschlüsselung und mit dem entschlüsselten text?

Absolut. <kju>

der riecht den Braten:

hey komm du wielst mich nur verarschen^^ ich hab nachgeprüft das kann es überhaupt net sein :(was soll den das

Aber wir sind geduldig:

Geh bitte in die Bücherei und leih Dir dieses Buch aus:

http://www.amazon.de/exec/obidos/ASIN/3893198547/

lies insbesondere das Kapitel über one-time-pad Verschlüsselung, dann weisst Du, dass kju recht hatte. Mit dem richtigen Key kommt wirklich der plain-text "wer das liest ist doof" heraus. <Julius>

Bzgl. der Nicht-Speicherung von Verbindungsdaten bei Arcor - Hamburg

Ich hatte unlängst ein längeres Problem mit dem Aufbau einer stabilen DSL-Verbindung bei Arcor. In diesem Zusammenhang hatte ich einige Gespräche mit Technikern unter anderem auch folgendes:

Die Technikerin fragte mich, wann denn das letzte mal alles einwandfrei lief ? und ob ich bestimmte Ereignisse zeitlich näher eingrenzen könnte. Nun ich sagte ein paar Daten und darauf hörte ich sie am Telefon so mitmurmeln "Ja hier sehe ich ein ACK und da ein ... " ich unterbrach und fragte: "Wo sehen sie das ? Welche Daten haben Sie und woher ?" TA: "In meinem technischen Protokoll" Ich: "Ähem, ich habe die Information, dass sie keinerlei Verbindungsdaten speichern, wie können sie da ein Protokoll haben?" TA: "Na für die Abrechnung wird ja auch nichts gespeichert, ich habe hier nur das technische Protokoll. Da haben die von der Buchhaltung aber auchkeinen Zugriff. Das ist nur für uns." Ich: "Sorry, das sind Feinheiten, sie haben also Verbindungsdaten ?" TA: "Ja, aber nur 7 Tage, länger kann ich im System nicht zurück."

Wie auch immer: Tolle Arbeit, die ihr mit der DS macht. Tolle Artikel. Respekt. Danke. *<Martin R.>*

Vielen Dank. Vielleicht veröffentlichen wir das in der nächsten Ausgabe <erdgeist>

Bezüglich unserer Chaosradiosendung

88 erreichte uns Anfang März folgender Hinweis von einem Schüler:

Ich höre mir grade eure Sendung ueber ueber Kamaeraueberwachung an. Ich weiß jetzt nicht ob diese Mail noch jemand liest, habe aber trotzdem mal eine Frage zum Thema:

http://www.remigianum-alt.borken.de/M1/cam1.jpg und *http://www.remigianum-alt.borken.de/M1/cam2.jpg* sind bilder von 2 Kameras die bei uns in den Informatikraeumen haengen. Zur Ueberwachung. Kann das legal sein wenn da, waerend ich Informatikunterricht habe, minuetlich aktualisirte Bilder von mir im Internet stehen ohne das ich jemals gefragt wurde?

Schon mal danke im vorraus falls jemand diese mal beatwortet.

Anfang Juni schrieben wir die Schulleitung, die Datenschutzbeauftragte des Landes Nordrhein-Westfalen und in der Hoffnung auf eine Diskussion innerhalb der Schülerschaft die Schülervertretung bzw. die Schülerzeitung an. Wir äußerten unsere datenschutzrechtlichen Bedenken, da personenbezogenen Daten im Internet seit März 2003 als Archiv im Web frei zugreifbar waren. Eine Wochen später bestätigte uns die Datenschutzbeauftragte die Bearbeitung des Vorgangs. Mitte Juni wurde der Zugang zum Bildarchiv gesperrt.

Die Beweggründe für die Überwachung sind uns bisher unbekannt. Wir vermuten, dass die Installation zum Verhindern von Sachbeschädigungen und Diebstählen dient. In der FAQ des Landeszentrum für Datenschutz Schleswig-Holstein steht dazu: "Die dauerhafte Videoüberwachung steht schon in einem Widerspruch zu dem Anliegen, die Schülerinnen und Schüler in Freiheit und Selbstbestimmung zu einem verantwortungsvollen Verhalten zu erziehen." Wir teilen diese Ansicht und wünschen uns von den Bildungseinrichtungen einen besonders sensiblen Umgang mit Datenschutz. Statt die Schüler an die Überwachung im Alltag zu gewöhnen, müsste die Schule über Risiken aufklären und hätte Alternativen suchen sollen. <Eris D., CCCB>

EX-NSA Chef betreibt Venture-Capital Gesellschaft

Bei einem Besuch der Veranstaltung einer Venture-Capital Abteilung eines grossen deutschen Elektronikkonzerns, von dem einige auch behaupten, es handele sich um eine Bank, ergaben sich interessante Bits im Bezug auf die Aktivitäten des früheren NSA-Directors Miniham.

Unter dem Namen "Paladin Homeland Security Funds" betreibt Miniham zusammen mit 4 Partnern (Mike Steed, Mark Maloney, Niloo Howe, Greg Corona) eine Venture-Capital Gesellschaft, die mit einem avisierten Gesamtvolumen von derzeit 200 Mio US$ "Homeland Security Technology" Unternehmen unterstützt.

Dabei stellt sich natürlich nicht nur die Frage, wie gross die tatsächliche Entfernung dieser "privaten Initiative" unter maßgeblicher Beteiligung des ehemaligen NSA-Directors ist, sondern auch warum sich beispielsweise ein deutsches Industrieunternehmen mit einem - wenn auch verhältnissmässig bescheidenem Betrag in mittleren einstelligem Bereich - an einer solchen Geldsammlungsaktion beteiligt.

Zitat aus der Unternehmenskurzbeschreibung: "Recovery - return and restore a reconstruct public and private enterprises to their former or a better state."

Zu beachten werden vor allem die auf diese Art finanzierten Unternehmen bzw. Ihre Aktivitäten und Produkte sein:

Agion Technologies, Inc.
Arxcan Technologies, Inc.
ClearCube Technology, Inc.
Nexida, Inc., VistaScape Security Systems Corp.
Cloudshield Technologies, Inc.

Mehr dazu unter *http://www.paladincapgroup.com/*

Trons Krypto im deutschen Behördeneinsatz?

Jurtext Autor Bernd Fröhlich berichtete am 13.07.2004 unter der Überschrift ">>Sondermeldung<< Neue Spuren im Fall Boris F. (Tron)?" über eine interessante parallele zwischen Tron's Diplomarbeit zur Entwicklung eines ISDN B-Kanal Verschlüsselungssystems und der Entwicklung einer Faxkarte mit Verschlüsselungsfunktion eines in Berlin ansässigen Electronicunternehmens das so klingt wie eine Automarke.

Diese allerdings bislang lediglich als unbewiesenes Verdachtsmoment im Raum stehende These ergab sich offenbar durch die Feststellung, dass gleich drei Personen aus Trons Umfeld mit diesem Unternehmen in Kontakt standen bzw. stehen.

Interessant ist das Produkt dessen Design und mögliche Schwächen in der Verschlüsselung unter anderem auch deshalb, weil es nach bisherigen Recherchen offenbar in sensibelsten Bereichen sensibelster deutscher Behörden eingesetzt wird; mögliche Hintertüren im Auftrag fremder Regierung hätten fatalste Folgen und das wissen um eine solche Hintertür wäre in einem solchen Spannungsfeld vermutlich Mordwürdig.

Mehr dazu unter *http://www.jurtext.de/modules.php?name=News&file=article&sid=1423*

EX-Verfassungsschutzchef wg. unverschlüsseltem Telex festgenommen

Ausgerechnet ein unverschlüsseltes Telex an seinen Anwalt in Deutschland wurde dem ehemaligen Leiter des Bundesamtes für Verfassungsschutz, Ludwig-Holger Pfahls zum Verhängniss. Als wenn man fehlendes Bewusstsein im Umgang mit elektronischen Kommunikationsmitteln in spitzenpositionen deutscher Behörden nicht besser dokumentieren könne, hat Pfahls zudem beeindruckend bewiesen, das er sich trotz seiner ehemaligen Position offenbar nicht mit der sogenannten Open Source Intelligence beschäftigt hat; bereits am 30. Juni 2004 hatte die Münchener "Abendzeitung" offenbar durch Feierabendgesprächigkeit eines Mitarbeiters des Bundesnachrichtendienstes berichtet, Pfahls habe mit einem in Frankreich aufgegebenen Fernschreiben Kontakt mit einem Anwalt aufnehmen wollen.

Damit ist zum einen klar, daß die über öffentliche Netze vermittelte elektronische Kommunikation mit Anwälten trotz bestehender Ausnahmeregelungen zur Wahrung des Anwaltsgeheimnisses durch bundesdeutsche Nachrichtendienste ausgewertet wird, zum anderen das auch eine systematische Auswertung öffentlicher Quellen ein potential an Aufbereitung zur Entscheidungsrelevanz hat.

Dazu unter anderem: *http://www.spiegel.de/politik/deutschland/0,1518,308609,00.html*

Antit/error: Anzahl der Atomexplosionen in Deutschland rückläufig

Fast unbemerkt von der Öffentlichkeit zeigt die Kriminalstatistik des deutschen Bundeskriminalamtes deutliche Antit/error-Erfolge. Weist die Statistik im Jahr 2000 noch zwei Verstöße gegen § 307 StGB, "Herbeiführen einer Explosion durch Kernenergie" aus, so verringert sich dies im Jahr 2001 auf einen Verstoß. Die Jahre 2002 und 2003 blieb Deutschland von Atomexplosionen verschont.

Vermutet wurde daß dies durchaus auf die Steigerung bei der Aufklärung zurückzuführen wäre. 2001 wurden nur die Hälfte dieser Delikte aufgeklärt. 2002 konnten alle Verstöße einer Klärung zugeführt werden. [...]

http://www.bka.de/pks/pks2000/bka_tabs_2000.zip
http://www.bka.de/pks/pks2001/tab_01.pdf
http://www.bka.de/pks/pks2001/tab_straftatenkatalog.pdf

Daß jedoch die, für Atomexplosionen in Nachbarländern typischen, seismischen Nachweise fehlten, hat eine intensive Recherche der Redaktion *[q/depeche - Anm. d. Redaktion.]* ausgelöst.

Diese konnte den Nachweis erbringen, daß es sich bei diesen Explosionen um "Erfassungsfehler" handelt. Gerüchte über geheime Atomwaffenversuche auf Neu Schwabenland mussten daher - trotz des höheren Unterhaltungswertes - für heuer abgesagt werden.

Quelle: q/depesche 2004-06-23T23:33:23

SIGINT und die Verunfallung von Di & Dodi

Im Kontext der Beleuchtung der Hintergründe der verunfallten englischen Prinzessin und ihres arabischen Geliebten gibt es im Netz derzeit eine Seltenheit zu bestaunen: ein Originalberichts-Faksimilie des zur CIA gehörenden "Directorate of Intelligence / Domestic Collection Division"

Man beachte den Header

Das Dokument unter:

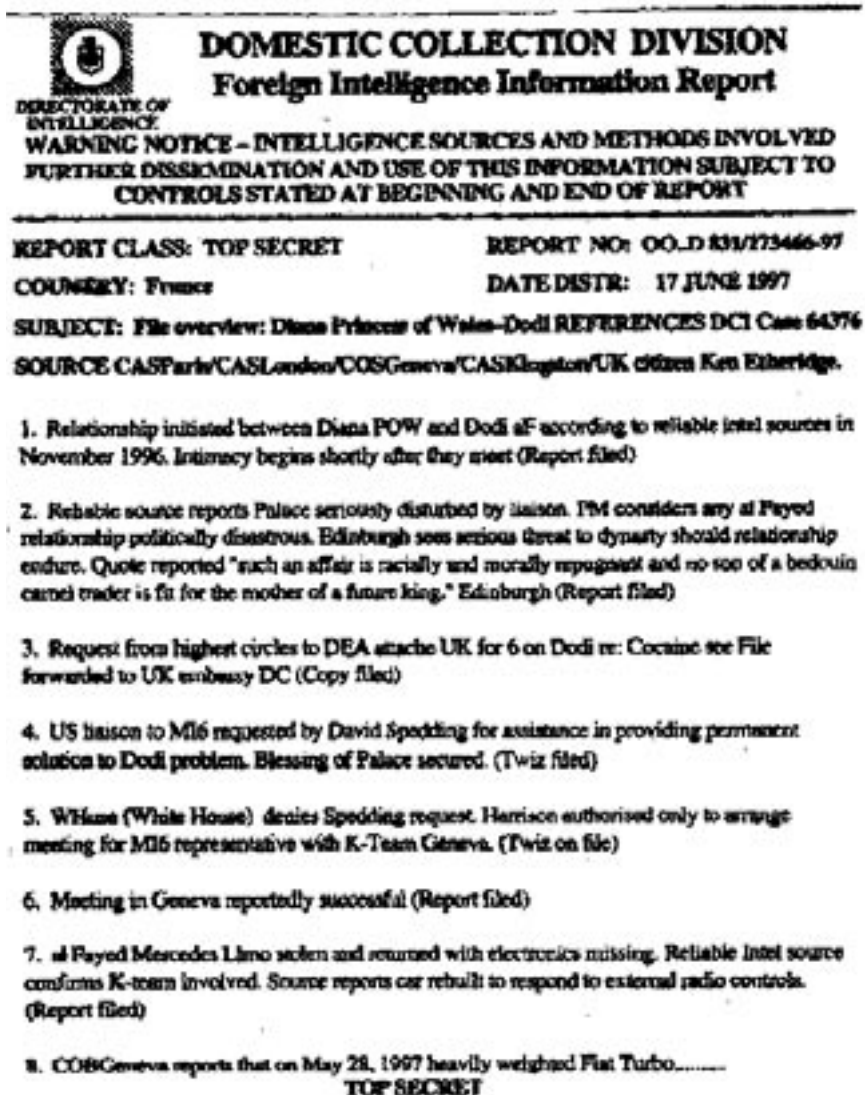
http://www.theeunderground.net/Features/dianacia-b.gif

Für Hartgesottene:

http://www.semit-times.de/images/lewinter/lewinter_news_at_03_45.jpg

Wer mehr Zeit hat:

http://www.rumormillnews.com/cgi-bin/archive.cgi?read=26001



DIRECTORATE OF INTELLIGENCE

DOMESTIC COLLECTION DIVISION
Foreign Intelligence Information Report

WARNING NOTICE – INTELLIGENCE SOURCES AND METHODS INVOLVED FURTHER DISSEMINATION AND USE OF THIS INFORMATION SUBJECT TO CONTROLS STATED AT BEGINNING AND END OF REPORT

REPORT CLASS: TOP SECRET **REPORT NO: OO_D 831/273466-97**

COUNTRY: France **DATE DISTR: 17 JUNE 1997**

SUBJECT: File overview: Diana Princess of Wales–Dodi REFERENCES DCI Case 64376

SOURCE CASParis/CASLondon/COSGeneva/CASKingston/UK citizen Ken Etheridge.

1. Relationship initiated between Diana POW and Dodi aF according to reliable intel sources in November 1996. Intimacy begins shortly after they meet (Report filed)

2. Reliable source reports Palace seriously disturbed by liaison. PM considers any al Fayed relationship politically disastrous. Edinburgh sees serious threat to dynasty should relationship endure. Quote reported "such an affair is racially and morally repugnant and no son of a bedouin camel trader is fit for the mother of a future king." Edinburgh (Report filed)

3. Request from highest circles to DEA attache UK for 6 on Dodi re: Cocaine see File forwarded to UK embassy DC (Copy filed)

4. US liaison to MI6 requested by David Spedding for assistance in providing permanent solution to Dodi problem. Blessing of Palace secured. (Twiz filed)

5. WHaus (White House) denies Spedding request. Harrison authorised only to arrange meeting for MI6 representative with K-Team Geneva. (Twiz on file)

6. Meeting in Geneva reportedly successful (Report filed)

7. al Fayed Mercedes Limo stolen and returned with electronics missing. Reliable Intel source confirms K-team involved. Source reports car rebuilt to respond to external radio controls. (Report filed)

8. COSGeneva reports that on May 28, 1997 heavily weighted Fiat Turbo.....

TOP SECRET

Biometrie & Ausweisdokumente - Eine Bestandsaufnahme

von starbug <starbug@berlin.ccc.de>

Mit einer empfundenen stärkeren Bedrohung der Grenzen durch illegal Einreisende und der Waffe der allgemeinen Terrorangst in der Hand haben Bedarfsträger nahezu aller Länder den Anteil von Biometrie im und als Ausweis der Identität konsequent vorangetrieben. Ziel ist es, den Mißbrauch von Ausweisdokumenten einzuschränken und die Effektivität von Grenzkontrollen zu steigern. (Zusammenfassung des Berichts des Büros fuer Technikfolgeabschätzung des Bundestages #93 "Biometrie und Ausweisdokumente")

Am 9. Januar 2002 trat in Deutschland das Terrorismusbekämpfungsgesetz in Kraft, in dem 21 Gesete oder Rechtsvorschriften verändert oder neu verabschiedet wurden. (S.91) Darin wurde vor allem eine Erleichterung des Informationsaustausches zwischen den Behörden, das Verhindern der Einreise von Terroristen ins deutsche Staatsgebiet und das Durchsetzen identitätssichernder Massnahmen angestrebt.

Im Einzelnen wurden das Pass- und Personalausweisgesetz sowie Ausländer- und Asylverfahrensgesetz geändert, um die computergestützte Identifikation von Personen mittels Ausweisdokumenten zu verbessern. Damit soll verhindert werden, dass Personen Papiere von ihnen ähnlich Sehenden verwenden. (Dass sich dies nicht verhindern lässt, werden wir später noch erörtern, Stichwort BioP1.) Dazu der TAB Bericht: "... erwartbare Erkennungsleistung eine hinreichende Sicherheit gewährleisten ... erhofften Verbesserungen bei der Grenzkontrolle den hierzu erforderlichen Aufwand rechtfertigen, muss politisch entschieden und begründet werden" "Dabei sollte offen diskutiert werden, dass es trotz eindrucksvoll geringer Fehlerraten in der Praxis eines Masseneinsatzes nur zu einem relativen Sicherheitszugewinn kommen kann, da Falschidentifikationen in einem gewissen Umfang weiter erfolgen werden." (S.6)

Die Art der Merkmale, ihre Einzelheiten, Art der Speicherung und ihre Nutzung bzw. Verarbeitung sollen durch ein Bundesgesetz (oder für Ausländer: eine Rechtverordnung) geregelt werden. Diese können auch Massnahmen beinhalten, die über die bisherigen Regelungen hinausgehen (Pass/PA), beschränken sich aber auf Merkmale von Gesicht (keine Iris/Retina) ODER Hand ODER Finger. Eine Kombination von Merkmalen ist darin nicht vorgesehen.

Wie der TAB Bericht bemerkt, haben Fingerabdruck-, Gesichtsgeometrie- und Iriserkennung ihre Eignung für Verifikationsanwendungen bei Ausweisdokumenten unter Beweis gestellt. Mit der biometrischen Ausrüstung von nationalen Ausweisdokumenten und ihrer weltweiten Nutzung bei Grenzkontrollen ist aber eine Aufgabe mit so erheblichen Dimensionen zu lösen, dass bisherige Erfahrungen z.B. mit Pilotprojekten bei Grenzkontrollen hierzu allenfalls indirekt Erkenntnisse liefern. (S.3)

Der Bundestag stellte 2001 fest, dass ein Schutz vor Identitätsmanipulation mit Reisedokumenten nur erreicht werden kann, wenn Biometrie auch in Personalausweisen Einzug hält, da diese in Europa als Reisedokumente anerkannt sind.

Generell stehen drei Optionen für die Einführung der biometrischen Merkmale zur Disposition. Die Kosten berechnen sich unter der Annahme, dass 6500 Meldestellen für die Beantragung eines Pass/PA aufgerüstet werden müssen und die laufenden Kosten hier jährlich rund 20% des Anschaffungspreises ausmachen. Zusätzlich müssen 200 Kontrollpunkte an Grossflughäfen und 200 an Landes/Seegrenzen bei Baukosten von 20.000 Euro pro Kontrollpunkt (15.000 Euro innerhalb von Gebäuden) aufgerüstet werden.

Implemenationsmöglichkeiten

Option 1: Biometrische Nutzung der bestehenden Dokumente

Anforderung: Normalisierung und Standardisierung der Qualität aller Passbilder
Kosten: einmalig 21 Mio, laufend 4,5 Mio

Option 2: Technische Aufwertung der bestehenden Dokumente mit biometrischen Daten

Anforderung: Als Speicher kommen Barcodes oder digitale Speicherelemente in Frage.

Zentrale (2a) oder dezentrale (2b) Erfassung und Verarbeitung der biometrischen Merkmale in den Meldestellen
Kosten: 2a) einmalig 179 Mio, laufend 55 Mio / 2b) einmalig 614 Mio, laufend 332 Mio

Die zusätzlichen Kosten (Biometrie und RFID) würden sich auf 2-3 Euro pro Ausweis belaufen.

Option 3: Neues Dokumentendesign (Smartcard mit elektronischem Speicherelement)

Vorteil: geeignet fuer die elektronische Unterschrift, Rechts- und Geschäftsverkehr.
Anforderungen: totaler Umbau der Herstellungs- und Verifikationsinfrastruktur
Kosten: einmalig 669 Mio, laufend 610 Mio

Laut Bericht ist bislang ist die Kostenfrage allenfalls in Ansätzen diskutiert. Ferner ist festzuhalten, dass die Biometriekomponenten im Gesamtsystem nicht der entscheidende Kostenfaktor sind. (S.9)

Ungeklärt sind weiterhin auch die Fragen der Langzeitstabilität der Merkmale und der Gültigkeitsdauer möglicher kryptografischer Schlüssel. So sind Pässe und PAs 10 Jahre (für unter 26jährige: 5 Jahre) gültig. Um für diese Zeiträume Aussagen über die Verlässlichkeit treffen zu können, müssten Langzeittests durchgeführt werden. Dies ist bisher nicht geschehen. Auch beträgt die Gültigkeitsdauer für kryptografische Produkte laut Signaturverordung derzeit nur 5 Jahre, was bei den verwendeten Verfahren und der Entwicklung im Computerbereich auch durchaus Sinn macht.

In dem Zusammenhang stellt sich ausserdem noch die Frage, wer Verschlüsselung/Signatur erstellt. Bei einem dezentralen Modell wuerden örtliche Pass/PA-Ausstellungsbehörden in Frage kommen. Aus Sicherheitsgründen würde sich allerdings der Hersteller, also die Bundesdruckerei, anbieten.

Theoretisch steht der verschlüsselten Speicherung der biometrischen Daten auf dem Ausweis nichts im Weg. Zwar widerspricht eine Verschlüsselung grundsaetzlich dem Recht des Buergers auf informationelle Selbstbestimmung (Wissen, welche Daten über die eigene Person gespeichert sind), dafuer existiert aber die Auskunftspflicht der Behörden (Art.16, Abs.6 PassG und Art.3, Abs.5 AuswG).

Auch der Datenschutz spielt natürlich bei einer solch brisanten Frage eine grosse Rolle. Art.4 BDSG sagt dazu: "Direkterhebung verlangt, dass personenbezogene Daten bei der Person selbst mit ihrer Kenntnis und Mitwirkung zu erheben sind", dabei seien "Verfahren zu bevorzugen, die aktive Mitwirkung verlangen". Um das Recht auf Informationelle Selbstbestimmung zu wahren, sollen möglichst wenig überschüssige Daten gesammelt werden. Diese Forderung spricht eindeutig gegen die Speicherung der Rohdaten, da aus ihnen Rückschlüsse auf Geschlecht, Alter, Ethnie (Gesichtserkennung), Krankheiten wie Leukämie, Brustkrebs, Magen-Darm-Beschwerden (möglicherweise aus dem Fingerabdruck erkennbar), Arteriosklerose, Diabetis, Bluthochdruck (fällt bei Betrachten des Augenhintergrunds auf), Augenkrankheiten (Iriserkennung) gezogen werden können. (S. 98)

Allerdings sind Templatedaten als Vergleichsgrundlage gerade im Bezug auf die Interoperabilität als kritisch anzusehen, da sie meist auf einen Algorithmus festgelegt sind. Stellt dieser sich als fehlerhaft heraus, müsste eine komplette Neugenerierung der Templates vorgenommen werden. Für deutsche/europäische Bürger dürfen keine zentrale Datenbank angelegt und lokale Register nicht länderübergreifend vernetz werden. (S.102)

Derzeit werden die im Pass/PA gespeicherten Daten zusätzlich im Pass/PA-Register aufbewahrt. Eine weiterführende Speicherung an anderen Orten ist ausdrücklich verboten. Die Bundesdruckerei speichert nur die Seriennummern der ausgegebenen Pässe und Ausweise zentral als Nachweis des Verbleibs. Daten, die zur Herstellung benötigt werden, sind anschliessend zu löschen. (S.104)

Auch die Zusammenlegung des Melde- mit dem Pass/PA-Register ist unzulässig. Es besteht eine strenge Zweckbindung der biometrischen Daten. Mögliche Verwendung für die Fahndung und Ermittlung verstösst gegen den Verhältnismässigkeitsgrundsatz. Es darf also kein Abgleich mit anderen Datenbanken und keine automatische Erkennung im Bezug auf Videoüberwachung vorgenommen werden(S.101).

Diese Zweckbindung fehlt bei "Ausländerausweisen" völlig! Das stellt eine klare Verletzung des Gleichheitsgrundsatzes dar. Auch dürfen die biometrischen Daten von Ausländern in einer zentralen DB gespeichert werden, auf die auch die Polizei und andere Behörden zugriff erhalten sollen (polizeiliche Spurensuche/abgleich). Auch Private sind nicht grundsätzlich von der Nutzung dieser Daten ausgeschlossen. (S.112)

Das weitere Vorgehen soll hier durch eine Rechtsverordnung bestimmt werden. Das wiederum widerspricht einem Bundesverfassungsgerichtsurteil, nach dem alle wesentlichen Entscheidungen vom Parlament selbst zu regeln sind. Auch bei den "Ausländerausweisen" stellt sich die Frage nach der Gültigkeitsdauer der biometrischen Merkmale, da es auch unbefristete Aufenthaltserlaubnisse gibt.

Eine weitere Forderung ist, dass regelmässige Falschrückweisungen durch Unzulänglichkeiten bei den gespeicherten Daten ausgeschlossen werden müssen. Auch wenn es zur Zeit noch kaum eine öffentliche Diskussion zu dem Thema gibt, ist mit grossen Akzeptanzproblemen zu rechnen, besonders weil die Optionen 2 und 3 eine flächendeckende Erfassung aller Bürger bedeuten würde!

Dieser TAB-Bericht ist eine sehr umfassende Bestandsaufnahme der aktuellen technischen und polititschen Situation der Einführung zusätzlicher biometrischer Merkmale in Reise- und Ausweisdokumente. Was jetzt noch fehlt, ist die geforderte öffentliche/gesellschaftliche Debatte über deren Akzeptanz, Kosten und Nutzen. Und diese ist dringend geboten, denn es geht hier immerhin um die flächendeckende erkennungsdienstliche Erfassung aller Bürger.

Bluetooth Location Tracker

von <steini@ccc.de>

Seit in vielen Mobiltelefonen ein Bluetooth Modul integriert ist, drängt sich die Frage auf, ob sich dieser Umstand nicht für fantasievolle Zwecke einsetzen lässt. Der geneigte Hacker wittert sofort ein Potenzial, wenn plötzlich abertausende von Gestalten mit womöglich offenen Funkschnittstellen in der Hosentasche herumlaufen. Viele Geräte sind nämlich per Default so konfiguriert, dass sie, sobald Bluetooth eingeschaltet ist, ohne weiteres Zutun für andere Geräte sichtbar sind (inquiry scan).

Jeder geplagte Bluetoothhandybesitzer hat sicher schon einmal bemerkt, wenn eine alberne Knalltüte ihm eine Message per OBEX Push service auf sein Display genervt hat (wie witzig). Aber der Reihe nach: Bluetooth ist ein Funkstandard der entwickelt wurde, um diesen ewigen Kabelsalat auf dem Schreibtisch zu beseitigen. Ja, man hat sich Mühe gegeben. Spread-Spectrum Technologie, synchrone und asynchrone Datenübertragung gleichzeitig, keine Vorabkenntnis eines weiteren Teilnehmers nötig um eine Verbindung aufzubauen, integriertes Sicherheitskonzept, mehrere Piconetze in unmittelbarer Nähe zueinander, Multipointfähigkeit, und, und, und... und vor allem billig soll es sein. Daher gibt es auch verschiedene Klassen von Geräten. Class 1 bis Class 3, die sich in erster Linie in Sendeleistung (100-10mW) und Funktionsumfang voneinander unterscheiden.

Simple Grundlagen

Prinzipiell läuft eine Verbindung zwischen zwei Geräten also wie folgt ab: Nehmen wir an, es gibt die drei Bluetooth Geräte A, B und C. A möchte eine Verbindung zu B aufbauen. Das geht nur, wenn A auch die BT-Addresse von B kennt (im Prinzip eine MAC-Addresse). Um diese zu erfahren, macht A also einen Inquiry Scan und 'schaut', ob im näheren Umkreis evtl. andere Bluetooth Geräte zu finden sind. B und C können nun, je nach Konfiguration, auf diesen Inquiry Scan mit Ihrer BT-Addresse antworten. Sobald bei A die BT-Addresse von B bekannt ist, kann A einen Page-Scan ausführen, also sozusagen die Rahmenparameter von B erfragen. Hierbei wird z.B. bekanntgegeben, welchen Klartextnamen das Device hat, welche Profile es kennt und auf welchen Kanälen diese zur Verfügung stehen etc. Nun kann A einen Connect zu B versuchen. Dieser Verbindungsaufbau kann ausserdem noch an einen Sicherheitscode gebunden sein, der auf beiden Seiten bekannt sein muss. Ebenso kann diese Verbindung verschlüsselt werden. Schlussendlich sind die beiden Geräte miteinander verbunden. Üblicherweise ist dies eine asynchrone Serielle- oder eine synchrone Audio-Verbindung. Bei einer seriellen Verbindung verhalten sich beide Geräte exakt so, als seien sie per RS232 miteinander verbunden. Soweit die Grundlagen, nun aber zum Location Tracker.

Der Locationtracker auf dem Chaos Communication Camp

Das Projekt Bluetooth Location Tracker hat sich zum Ziel gesetzt, die 'Sichtbarkeit' eines Bluetooth Gerätes einzusetzten, um die Position des Besitzers zu bestimmen und über einen Server zur Verfügung zu stellen. Dazu werden an verschiedenen Orten, bspw. in verschiedenen Räumen eines Gebäudes, oder wie in unserer Testinstallation auf dem Camp willkürlich verteilt einige Bluetooth Dongles installiert, welche in kurzen Abständen Inquiry Scans durchführen und das Ergebnis an einen Server melden. Wenn der Server die räumliche Position jeden Dongles kennt, kann er die ungefähre Position des gescannten Devices errechnen, indem man eine "Funkzellengröße" schätzt. Hierbei wird ganz ausdrücklich kein Connect zu dem Device hergestellt, so dass die Sicherheitsmechanismen hier nicht greifen. Auf dem Camp kamen sowohl USB-Dongles als auch serielle Bluetooth-Adapter zum Einsatz. Diese waren an Linux-PCs angeschlossen, welche auch die Kommunikation zum Server übernahmen. Über ein Netzwerkprotokoll konnten diese Clients vom Server veranlasst werden, einen Inquiry Scan durchzuführen und die BT-Adressen und Device-Names der umliegenden Bluetooth-Devices zusammen mit ihrer eigenen Lokationsinformation zurückzuliefern. Diese Informationen wurden über einen Webserver und einem Socket-Interface zur Verfügung gestellt. Auf dem Vortrag zum Thema war eindrucksvoll zu sehen, wieviele Bluetooth-Handy Besitzer im Zelt waren und wie überrascht einige waren, ihr Gerät auf der Website wiederzufinden.

Ausblicke

Es drängen sich einem geradezu eine Fülle von Anwendungsbeispielen auf, wie z.B. eine 'proximity warning', wenn eine bestimmte Person in der selben Zelle oder in einer Nachbarzelle auftaucht, oder ein 'group notifier', wenn bestimmte Personen gemeinsam in einer Zelle sind (dann heisst das womöglich, dass es da spannend ist ...). Bleibt zu bemerken, dass, wenn der Server erst einmal in Kenntnis der BT-Adresse eines Devices ist, bei diesem Device auch ein Ausschalten des Inquiry-Scan nicht mehr verhindern kann, dass das Device 'gesehen' wird. Im übrigen gibt es Verfahren, die wir bis zum kommenden Chaos Congress (21C3) vorstellen möchten, mit denen ein Device, bei dem der Inquiry Scan ausgeschaltet ist, auch ohne Kenntnis der BT-Addresse gefunden werden kann. Interessant ist auch eine Variante, bei der die stationären Bluetooth-Devices keine eigene Netzverbindung mitbringen und nur als 'Funkbake' dienen und die mobilen Empfänger mit eigener Intelligenz eine Lokationsinformation ableiten und selbständig (z.B. über GPRS oder eben über Bluetooth) an einen Server melden.

Hack'em

von Winfried <willy@ccc.de>

Der CCC-Bielefeld, C3BI, hatte am Wochende des 1. Mai zu einer Hackerparty unter dem Motto "Hack'em" eingeladen. Anlass war der Bezug unserer neuen Räume im AJZ-Bielefeld. Es war eine insgesamt kuschelige Veranstaltung mit einem Hackcenter in unseren Räumen und Vorträgen, Filmen und Workshops im ganzen Haus.

Die Anbindung wurde über eine W-LAN-Richtfunkstrecke realisiert, welche chaosüblich nach einigen Schwierigkeiten zu Beginn der Veranstaltung auch funktionierte und die drei Tage durchhielt.

Parallel zu unseren Veranstaltungen gab es im Haus noch jeweils am Freitag und Samstag abends Live-Konzerte und Disco zur Entspannung.

Der Fahrstuhlschacht wurde zu einem Warp-Kern umgebaut, der vielleicht etwas bunt geraten war, aber ansonsten gut funtionierte.

Besonderes Interesse auch bei den nicht chaosnahen Besuchern konnte der Lockpicking-Workshop von Steffen Wernery verbuchen.

Die ganze Veranstaltung war auf low-cost Ebene geplant und das Prinzip der Spenden und des Mate-Verkauf hat soweit funktioniert, dass wir nicht wesentlich zuschiessen mussten.

Insgesamt hatte der Veranstaltungsdruck geholfen, das wir jetzt die Basisinfrastruktur im gesamten Haus verlegt haben und die anderen Gruppen im Haus ihre Berührurungsängste abbauen konnten.

Geplant war die Veranstaltung für 40-60 Leute, was auch gut geklappt hat.

Eine weitere positive Entwicklung ist die grössere Nähe der verschiedenen Erfas und Chaostreffs aus NRW in Folge des Events. Es fand bereits ein Folgetreffen in Mühlheim statt, an dem eine weitere Veranstaltung im Chaoskalender ins Auge gefasst wurde.

Damit wird es in Zukunft wohl möglich sein, auch grössere Projekte in Angriff zu nehmen. Stay tuned.

Volkszählung

Bluetooth for fun and profit

Bluetooth ist eine drahtlose Sprach- und Datenübertragungstechnik, die mittlerweile in den verschiedensten Geräten wie Handy, PDA, USB Stick, PCMCIA Karte, Tastatur, Maus, Headset, Drucker usw. zu finden ist. Im Gegensatz zu Infrarot ist Bluetooth nicht auf Sichtkontakt der zu verbindenden Geräte angewiesen und funktioniert mit guter Hardware auch durch Wände hindurch, ist also mit WLAN zu vergleichen und funkt ebenfalls im 2,4 GHz Bereich.

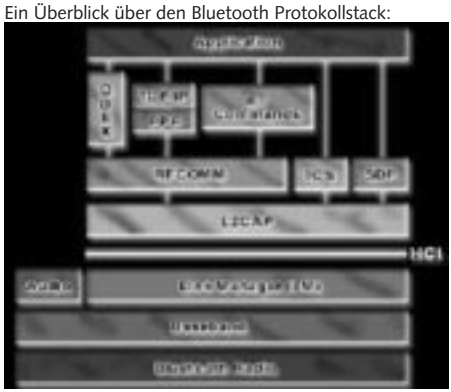
von crazydj

Beim Design von Bluetooth wurde speziell auf eine sichere Implementierung geachtet, so läßt sich die Verbindung verschlüsseln und authentifizieren und die Bluetooth Adresse wird von der Firmware des Bluetooth Geräts und nicht durch den Kernel gesetzt, was das Spoofen dieser Adresse nahezu unmöglich macht. Dennoch tauchten in der Vergangenheit immer wieder Meldung über Sicherheitslücken in den verschiedensten Bluetooth Implementationen von Herstellern wie Nokia und Siemens auf und man liest ständig über Bluejacking. Grund genug sich mal eingehend mit dieser Technologie auseinander zu setzen.

Here we are! :) Dieser Artikel beschreibt sowohl den Bluetooth Protokoll Stack und die Einrichtung von Bluetooth Hardware unter Linux 2.4 / 2.6 als auch typische Anwendungen wie Datenaustausch, Aufbau eines Netzwerks, Scannen nach Devices und Diensten und die Programmierung einfacher Anwendungen unter Verwendung der BlueZ Libraries.

Die Theorie

Ein Überblick über den Bluetooth Protokollstack:



Funk (Bluetooth Radio):

- 2,4 GHz Ism Band (2400 - 2483,5 MHz)
- 79 verfügbare Kanäle
- Sendestärke: 1 mW - 100 mW
- Reichweite: 1 - 100m
- Frequenzwechsel nach jedem Paket

SCO / ACL (Bluetooth Baseband):

- SCO (Synchonous Connection Oriented) baut eine synchrone verbindungsorientierte Punkt-zu-Punkt Verbindung auf und dient zur Sprachübertragung.
- ACL (Asynchonous Connection Less) baut wahlweise eine synchrone oder asynchrone verbindungslose Punkt-zu-Punkt Verbindung auf und dient zur Datenübertragung.
- Sowohl SCO als auch ACL werden durch die Firmware des Bluetooth Geräts implementiert.

LMP (Link Manager Protocol)

- LMP kann man mit Ethernet vergleichen. Es implementiert die 48 Bit lange Bluetooth Adresse und ist für den Link Setup, die Authentifizierung sowie die Verschlüsselung zuständig. LMP wird durch die Firmware der Bluetooth Hardware implementiert. Einen guten Einblick in die Funktionsweise von LMP gibt es auf Palowireless. com [1] .

HCI (Host Control Interface)

- HCI bietet eine einheitliche Schnittstelle zur Bluetooth Firmware und gehört eigentlich nicht direkt zum Bluetooth Protokoll Stack, aber es wird unter anderem dazu verwendet L2CAP Pakete an den Link Manager der Firmware zu senden und ist somit der unterste Layer, der im Kernel implementiert ist. HCI dient außerdem dazu die aktuelle Config und Features sowie den Status des Geräts auszulesen und zu setzen. Die Kommunikation ist paket- und verbindungsorientiert.

L2CAP (Logical Link Control and Adaptation Protocol)

- L2CAP kann man mit IP vergleichen. Die Hauptaufgabe dieses Protokolls ist die Fragmentierung, das Groupmanagement und die Implementierung höherer Protokolle wie RFCOMM, SDP oder BNEP. L2CAP baut über ACL eine Verbindung auf, über die dann die Pakete der anderen Protokolle geschleust werden. Auf Palowireless.com [2] findest du mehr über L2CAP.

RFCOMM / SDP / BNEP

- RFCOMM simuliert eine serielle Schnittstelle und

wird somit z.B. für den Zugriff auf ein Modem, aber auch von weiteren Protokollen wie OBEX verwendet. Mehr zu RFCOMM [3]

- SDP (Service Discovery Protocol) dient der Abfrage der auf dem entfernten Device verfügbaren Dienste (Bluetooth Profile). Mehr zu SDP [4]
- BNEP kapselt Ipv4, Ipv6 oder IPX Pakete und dient somit für IP bzw. IPX Netzwerke via Bluetooth

Bluetooth Profile

Dienste heissen unter Bluetooth Profile. Sie bilden die Application Layer Protokolle einer Bluetooth Verbindung. Hier eine Auflistung der wichtigsten (diese Liste stammt von einem handelsüblichen Siemens S55 Mobiltelefon):

- Modem Dial-up
- Fax
- OBEX File Transfer
- OBEX Object Push
- OBEX Synchronisation
- Headset
- SerialPort

Einen Überblick über diese und weitere Bluetooth Profile gibt es auf Palowireless.com [5] .

Die Praxis

Die Installation / Configuration / Benutzung geht von einem Linux System mit einem 2.4er oder 2.6er Kernel aus! Alle FreeBSDler seien auf das Bluetooth Kapitel des FreeBSD Handbuchs [6] verwiesen. Mac OS X User sollten mit Bluetooth eh keine Probleme haben. ;P

Ok. Erstmal die Geschichte mit dem Kernel. Die BlueZ [7] Treiber sind mittlerweile Bestandteil des offiziellen Kernels, ein patchen entfällt daher. Um sorglos mit Bluetooth spielen zu können solltest Du einfach alles was Dir zum Thema unter die Finger kommt als Modul compilen. Die absolut notwendigen Module, ausgehend von einem Bluetooth USB Stick und vorausgesetzt Du willst alle Beispiele in diesem Artikel nachvollziehen, sind

- bluez / bluetooth
- hci_usb
- hci_uart
- l2cap
- rfcomm
- bnep

Anschliessend installierst Du folgende Bluez Libraries und Tools [8] :

- bluez-utils
- bluez-sdp
- bluez-pin
- bluez-pan
- bluez-hcidump

Jetzt solltest Du Dein Bluetooth Device aktivieren können.

```
hciconfig hci0 up
```

Sollte das nicht der Fall sein, überprüfe, ob Du auch wirklich alle Kernel Module geladen hast! Mit hciconfig kann man sich außerdem die Eigenschaften seines Bluetooth Devices vergleichbar zu ifconfig anschauen und Verschlüsselung sowie Authentifikation ein- bzw. ausschalten.

```
hciconfig hci0 noauth noencrypt
```

Interessant ist noch, dass man mit hciconfig oder über die Config Datei /etc/bluetooth/hcid.conf die Device Class setzen kann. Eine Liste der Major und Minor Device Classes findet man auf Bluetooth.org [9] .

Die Major und Minor Device Classes sind auf Bluetooth.org in Binär angegeben, hciconfig erwartet sie allerdings als Hex, deswegen hier ein kleines Rechenbeispiel:

- Major Computer + Minor Laptop: 00001 000011 00 = 0x0001 0c
- Major Phone + Minor Cellular: 00010 000001 00 = 0x0002 04

Wer zu faul zum umrechnen ist, der findet in khciconfig alle Major und Minor Device Classes zum zusammen klicken. ;)

Also um seinen Bluetooth USB Stick z.B. in ein Mobiltelefon zu „verwandeln“, führt man folgenden Befehl aus:

```
hciconfig hci0 class 0x000204
```

Scannen

Als erstes will man wahrscheinlich nach verfügbaren Bluetooth Geräten in seiner Umgebung suchen.

```
hcitool scan
```

Wenn man ein Bluetooth Gerät gefunden hat, kann man meistens bequem über SDP die verfügbaren Dienste auslesen. Ich sage meistens, weil Headphones oder andere Geräte, die nur einen Dienst anbieten, haben keinen SDP Daemon implementiert.

```
sdptool browse
```

Hier ein Auszug (ein Dienst / Profil) aus einem SDP Scan eines handelsüblichen Mobiltelefons:

- Service Name: Dial-up networking
- Service RecHandle: 0x11103
- Service Class ID List:
- „Dialup Networking“ (0x1103)
- „Generic Networking“ (0x1201)
- Protocol Descriptor List:
- „L2CAP“ (0x0100)

- „RFCOMM“ (0x0003)
- Channel: 1
- Language Base Attr List:
- code_ISO639: 0x656e
- encoding: 0x6a
- base_offset: 0x100
- Profile Descriptor List:
- „Dialup Networking“ (0x1103)
- Version: 0x0100

Dieses Profil zeigt ein Dial-up Network sprich ein Modem. Das wichtigste in dieser Liste sind neben dem Service Namen der Hinweis auf die zu verwendenden Protokolle (L2CAP und RFCOMM), sowie der Channel 1.

Modem Games

Schön und gut, dann werden wir uns jetzt mal zu diesem Modem verbinden und mal schauen was wir damit so anstellen können! :)

```
rfcomm bind 0 0
```

Der erste Parameter bind sorgt dafür, dass der Bluetooth Socket nur an die entsprechende Adresse gebunden wird, aber keine Verbindung initiiert wird. Der zweite Parameter 0 ist die Nummer des RFCOMM Devices in diesem Falls also /dev/rfcomm0, dann folgt die Bluetooth Geräte Adresse und last but not least der Channel zu dem wir uns verbinden wollen.

Je nachdem ob Du unter der Console oder unter X unterwegs bist, wird die PIN Eingabe anders geregelt. Unter der Console wird die Datei /etc/bluetooth/pin ausgelesen, unter X solltest Du nen hübsches Fenster bekommen, das Dich zur PIN-Eingabe auffordert. Auf dem entfernten Gerät wirst Du ebenfalls zu einer Eingabe genötigt. Die beiden PINs müssen übereinstimmen!

Wenn Du alles richtig gemacht hast, kannst Du jetzt entweder via Minicom oder auch direkt per

```
echo ATZ > /dev/rfcomm0
```

AT Befehle an das entfernte Modem senden und es behandeln als wäre es lokal.

Dateiaustausch

Dateiaustausch findet über das OBEX (Object Exchange) Protokoll statt, welches auch schon für Irda (Infrarot) verwendet wird.

Um von der Console Dateien zu pushen, nimmt man am besten ussp-push [10] . Das Archiv entpackt man in das Verzeichnis openobex-app/src, welches man sich von openobex.sourceforge.net [11] downloaded und compiled es mit folgendendermaßen:

```
gcc -o obexserver obexserver.c libmisc.a -
lopenobex
```

```
cd ussp-push
make ; make install
```

Dann nimmt man per RFCOMM mit dem entfernten OBEX Push Dienst Verbindung auf.

```
rfcomm bind 0 4
```

Und sendet die Datei:

```
ussp-push /dev/rfcomm0
```

Zum synchonisieren zwischen einem Handy und einem Laptop / PDA verwende ich Multisync [12] , da es nicht nur ein Backup des Mobiltelefons wahlweise via Kabel, Infrarot oder Bluetooth unterstützt, sondern auch meinen Lieblingsgroupwareclient Ximian Evolution bedienen kann und ich damit alle wichtigen Klamotten wie Kalendar, Telefonbuch, Aufgaben und Notizen auf dem neuesten Stand halten kann.

Ansonsten sollte man sich auf jeden Fall noch obexftp und die Bluetooth Tools vom GNOME [13] sowie vom KDE [14] Projekt anschaun. Damit kann man weitaus bequemer und grafisch Dateien austauschen wahlweise via Nautilus (GNOME) oder FTP-like kbtobexclient (KDE). Für Debian gibt es fertige DEB Pakete. Dazu fügt man einfach nur die folgenden Server in seine / etc/apt/sources.list ein:

- deb http://debian.usefulinc.com/gnome ./
- deb-src http://debian.usefulinc.com/gnome ./
- deb http://www.stud.uni-karlsruhe.de/~uddw/debian/

Und installiert die gewünschten Tools:

```
apt-get update
apt-get install gnome-bluetooth
apt-get install kdebluetooth
```

Vielleicht möchte man auch eine Datei von einem Handy oder sonst einem Bluetooth Gerät an den eigenen Rechner schicken und das ohne Hilfe dieser grafischen Tools? Nichts einfacher als das! Zuerst startet man netterweise einen SDP Daemon.

```
sdpd
```

Und teilt ihm mit, dass wir OBEX Push anbieten

```
sdptool --add --channel 10 OPUSH
```

Als letztes startet man den obexftp server und findet anschliessend hoch geladene Dateien im Verzeichnis /tmp.

```
obexftpserver
```

Netzwerk

Jetzt basteln wir mit zwei Bluetooth Sticks mal ein kleines Netzwerk und verwenden es, um einen Gateway (wahlweise auch mit DHCP und was weiss ich) aufzubauen.

Auf dem Gateway startet man

```
pand --listen --persist --encrypt --role NAP
```

Auf dem Client

```
pand --connect
```

Jetzt stehen auf beiden Rechnern `bnep0` Netzwerk Interfaces zur Verfügung, die man mit `ifconfig` upped und mit IP Adressen versieht.

```
ifconfig bnep0 up
```

Abschließend aktiviert man auf dem Gateway noch Masquerading.

```
iptables -A POSTROUTING -t nat -o bnep0 -j
MASQUERADE
```

Und trägt auf dem Client diese Kiste als Standardroute ein.

```
route add default gw
```

Nützliche Tools

Blue-CMD [15] - Führe ein beliebiges Kommando aus, wenn sich ein Bluetooth Device im bzw. ausserhalb des Empfangsbereichs befindet. Ideal zum automatischen (ent)locken des Laptop, wenn man sich mit seinem Bluetooth Handy durch die Kneipe bewegt ;)

Blue-Scanner [16] - Ein kleines Script, das ich auf dem 20C3 geschrieben habe. Es scannt nach Bluetooth Devices, liest die vorhandenen Profile via SDP aus und versucht mit OBEX Push eine Vcard hoch zu laden.

Redfang [17] - Bruteforce Bluetooth Adressen. Ermöglicht es Geräte zu finden, die nicht sichtbar sind.

Bluesniff [18] - Ein Ncurses basierter Bluetooth Sniffer.

Btscanner [19] - Ein Ncurses basierter Bluetooth Scanner.

Programmierung

Anmerkung der Redaktion: Die Sourcebeispiel wurden aus Platzgründen nicht mit abgedruckt. Sie sind aber in der Onlineversion dieses Artikels verfügbar[30].

Referenzen

Bluetooth.org [20] - Die Bluetooth Spezifikation.

Holtmann.org [21] - Jede Menge Artikel rund ums Thema Bluetooth.

Palowireless Bluetooth [22] - Bluetooth Resource Center.

Irda.org [23] - Hier gibt's die Spezifikation zu OBEX.

BlueZ [24] - Der offizielle Linux Bluetooth Stack.

Affix [25] - Ein alternativer Bluetooth Stack für Linux.

Bluetooth Security [26]

Bluetooth unter FreeBSD [27]

GNOME Bluetooth Subsystem [28]

KDE Bluetooth Framework [29]

[1] *http://www.palowireless.com/infotooth/tutorial/lmp.asp*

[2] *http://www.palowireless.com/infotooth/tutorial/l2cap.asp*

[3] *http://www.palowireless.com/infotooth/tutorial/rfcomm.asp*

[4] *http://www.palowireless.com/infotooth/tutorial/sdp.asp*

[5] *http://www.palowireless.com/infotooth/tutorial/profiles.asp*

[6] *http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/network-bluetooth.html*

[7] *http://www.bluez.org*

[8] *http://www.bluez.org*

[9] *https://www.bluetooth.org/foundry/assignnumb/document/baseband*

[10] *http://www.saunalahti.fi/~laakkon1/linux/bin/blueobex.tar.gz*

[11] *http://openobex.sourceforge.net*

[12] *http://multisync.sourceforge.net/*

[13] *http://usefulinc.com/software/gnome-bluetooth*

[14] *http://kde-bluetooth.sourceforge.net/*

[15] *http://www.chaostal.de/members/crazydj/bluetooth/blue-cmd.pl*

[16] *http://www.chaostal.de/members/crazydj/bluetooth/blue-scanner.pl*

[17] *http://www.atstake.com/research/tools/info_gathering/redfang.2.5.tar.gz*

[18] *http://bluesniff.shmoo.com/bluesniff-0.1.tar.gz*

[19] *http://www.pentest.co.uk/src/btscanner-1.0.tar.gz*

[20] *http://www.bluetooth.org/spec/*

[21] *http://www.holtmann.org/*

[22] *http://www.palowireless.com/bluetooth/*

[23] *http://www.irda.org*

[24] *http://www.bluez.org*

[25] *http://affix.sourceforge.net/*

[26] *http://www.niksula.cs.hut.fi/~jiitv/bluesec.html*

[27] *http://www.freebsd.org/doc/en_US.ISO8859-1/books/handbook/network-bluetooth.html*

[28] *http://usefulinc.com/software/gnome-bluetooth*

[29] *http://kde-bluetooth.sourceforge.net/*

[30] *http://ds.ccc.de/083/input/bluetoothfunandprofit/*

No more secrets?

von Dirk Heringhaus

Ein Satz aus einem recht bekannten Film mit Robert Redford. Dieser Satz dient in dem Film „Sneakers – die Lautlosen" als Paßwort für einen Universaldecoder, mit dessen Hilfe in alle geschützten Netzwerke der USA ganz problemlos eingedrungen werden kann.

Wie oft habe ich gedacht: „Was für ein Quatsch – gut das es so etwas niemals geben wird". Bis ich, vor etwas über einem Jahr, zufällig auf das OBSOC (= Online Business Solution Operation Center) der Deutschen Telekom AG und der Microsoft AG gestoßen bin.

Wenn man den veröffentlichten Artikeln zu dem Thema OBSOC im Zusammenhang mit ByRequest-Services Glauben schenken kann, haben die beiden Unternehmen mit OBSOC eine Menge vor. Ebenfalls angeschlossen haben sich schon die Siemens AG und die Intel AG.

Der CCC und ich sind unserer Informationspflicht nachgekommen, indem wir eine Liste mit offenen Fehlern am OBSOC-System und diversen Netzen an den Bundesbeauftragten für Datenschutz (BfD) übergeben haben, der diese an die Regulierungsbehörde für Telekommunikation und Post (RegTP) weiterleiten wird. Wie sich die Sache beim BfD und der RegTP entwickeln wird, werden wir in der nächsten Ausgabe berichten.

Damit sich jeder selbst ein ausführlicheres Bild vom OBSOC machen kann, haben wir ein Downloadpaket, dass alle öffentlich zugänglichen Informationsmaterialen enthält, unter *http://www.ccc.de/t-hack/* veröffentlicht. Unter dieser Adresse habe ich in Kooperation mit dem CCC noch jede Menge zusätzliche Informationen veröffentlicht, die den Rahmen dieses Artikels bei Weitem sprengen würden.

Definition

OBSOC kann man am kürzesten als eine Online-Vertragsverwaltung beschreiben, die alle relevanten Daten eines Vertrages beinhaltet: Kundendaten, Vertriebsdaten, Art des Produktes, Zusatzdaten zum Produkt und eventuelle Zusatzleistungen zum Produkt. Auf diese Daten kann jeder, entsprechend seiner Berechtigung, online zugreifen.

In einem konkreten Beispiel heißt das:

Ein Kunde schließt bei T-Systems ein Standard Webpaket mit einer Domain, 100 MB Webspace und 10 Emailpostfächern ab. Damit die Auftragsbearbeitung möglichst flüssig läuft, wird der Kunde schon während des Vertragsabschlußes Teil des OBSOC. Er gibt online seine persönlichen Daten ein, wählt ein Produkt, schließt einen Vertrag ab und vergibt sich am Ende selbst einen Benutzernamen und ein Paßwort, damit er später wieder online auf die Daten zugreifen kann.

Hat der Kunde seinen Vertrag abgeschlossen, läuft dieser in einer Clearingstelle des entsprechenden Vertragspartners auf. Dieser kann nun die weiteren Schritte einleiten, um den Vertrag auch von dieser Seite zum Abschluß zu bringen, d.h.: Domain reservieren, Webspace einrichten, leere Emailpostfächer anlegen usw.

Damit beide Seiten ungestört arbeiten können, haben auch beide Seiten unterschiedliche Zugriffsrechte auf den Vertrag. Ein Mitarbeiter des Unternehmens, das den Vertrag anbietet, hat natürlich mehr Rechte, als ein Kunde, der den Vertrag abschließt. Diese Zugangsrechte werden über unterschiedliche Benutzergruppen administriert. Die wichtigsten Gruppen und deren Level werden in Abbildung 1 dargestellt.

Ist der Vertrag von beiden Seiten vollständig eingerichtet, bekommt der Kunde, über die von ihm vorher festgelegten Zugangsdaten, wieder Zugriff auf seinen Vertrag. Dort kann er nun seine Vertragsdaten einsehen, die nun u.a. seine persönlichen Daten, das Paßwort für seinen FTP-Zugang, sowie die Paßwörter für die Emailpostfächer enthalten.

Der Kunde kann jetzt auch selbst, innerhalb seiner Rechte, Änderungen am Vertrag vornehmen, wie z.B. das Umbenennen eines Emailpostfachs, oder das Ändern eines Paßwortes. Je nach Hostingvertrag auch das root-Passwort für den gemieteten Server.

Die Telekom selbst benutzt das OBSOC nicht nur für Ihre Webhosting Kunden, sondern ebenfalls für diverse andere Produktarten, die mit dem Internet in Verbindung stehen. Ein paar Beispiele für die Gänsehaut:

T-Pay – Das Online-Bezahlsystem der Telekom

PersonalSecurityService– Dieser Service soll die PCs von Internetnutzern vor Hackern und sonstigen böswilligen Attacken schützen.

OnlineBackup– Falls Ihre Daten zu Hause nicht sicher genug sind, können Sie Ihre Daten auch über das Internet bei der Telekom sichern.

Selbstverständlich geht die Telekom ebenfalls nach dem Motto vor: Was für uns gut, ist für Andere noch besser - weil sie selbst daran verdienen kann. Also wird das OBSOC-System nicht nur von der Telekom genutzt, sondern auch von anderen Unternehmen.

Ein Beispiel dafür ist das Unternehmen Brainloop AG. Dieses Unternehmen ist ein Projekt der Telekom, zusammen mit Microsoft, Intel und Siemens. Die Brainloop AG bietet ein Online-Dokumentenmanagementsystem an, das z.B. Anwälten besonders an's Herz gelegt wird, um ihre Aktenflut in den Griff zu bekommen. Natürlich basiert das Brainloop-System auf OBSOC.

Wenn bei EDV-Projekten von Sicherheit gesprochen wird, gibt es immer zwei Hauptaspekte:

• Wie sicher ist die ausgeführte Anwendung?

• Wie sicher ist die Infrastruktur (Hardware und Netzwerk), die dieser Anwendung zugrunde liegen.

Soll heißen: Wenn ich meine Wertsachen sicher deponieren möchte, ist es für mich nicht nur wichtig, dass das Schließfach sicher ist, sondern das Gebäude drum herum sollte einen höheren Sicherheitsstandard als das Schließfach haben.

Die Sicherheit der Anwendung

Es fällt mir schwer, im Zusammenhang mit OBSOC von Sicherheit zu sprechen, auch wenn die Telekom mir gegenüber nicht müde wird, das Gegenteil zu behaupten. Im Laufe eines Jahres, habe ich immer wieder feststellen müssen, dass meine Daten zu 0% geschützt wurden.

Es fing damit an, dass ich eines einen Webhosting-Vertrag im OBSOC administriert habe. Der Link, der mich in meinen Vertrag führte, produzierte folgende URL in meinem Browser:

http://www.t-mart-web-service.de/contractview/frameset.asp?ConPK=xyz

Wobei xyz für die Vertragsnummer des Vertrages steht, der gerade administriert wurde.

Neugierig wie ich war, änderte ich willkürlich die Vertragsnummer und bestätigte mit Enter die nun von mir geänderte URL. Ergebnis: Ich bekam einen anderen Vertrag eines anderen Kunden zum administrieren dargestellt. Exakt so, als ob ich meinen eigenen Vertrag verwalte. Ich brauchte also nur mein Schließfach aufschließen, eine neue Nummer darauf schreiben und schon hatte ich Zugriff auf das Schließfach, dessen Nummer ich auf mein Schließfach geschrieben hatte. Wie im Märchen. Die Telekom brauchte einen Tag, um den Fehler zu beheben.

Wenn man einen solchen Fehler findet, fängt man doch an, sich Sorgen um seine Daten zu machen.

Ein aufmerksames Studieren der Seite, die mich in die Vertragsverwaltung führte, brachte unter dem Link ZUKAUF folgenden Text zu Tage:

http://www.t-mart-web-service.de/SalesFrontend/initializeSalesfrontend.asp?intPurchaseType=2&intConPK=xyz

Da nach dem Anklicken des Links sofort der so genannte Konfigurator gestartet wurde, und damit die Adresse nicht mehr in der Ziel-URL auftauchte, kopierte ich den Link von der Eigenschaftenseite in die Zwischenablage. Von dort aus fügte ich den Link in die Adresszeile meines Browsers ein, änderte die `intConPK` und bestätigte die Eingabe.

Was sollte Anderes passieren, als dass ich den entsprechenden fremden Vertrag nun im Zukaufsmodul dargestellt bekam.

Ich brauchte also nur in meinem Vertrag die Vertragsnummer ändern, mit dem Vertrag zum Schließfachvermieter gehen, und sagen, dass ich für diesen Vertrag etwas dazukaufen möchte. Nicht nur, dass ich das ohne weitere Überprüfung durfte: Durch ein noch später erklärtes Sicherheitsloch, durfte ich auch noch direkt den Inhalt des Schließfachs mitnehmen. Auch hier war der Fehler von der Telekom schnell behoben.

Das waren jetzt zwei Schnitzer zuviel, als das ich der Telekom vertraut hätte, dass die Welt jetzt in Ordnung sei und meine Daten sicher sind.

Da der letzte Fehler im Zukaufsmodul lag, unterzog ich dieses Modul einer gründlichen Überprüfung. Da ich durch die Überprüfung x-mal den Prozess durchmachte, den ein Neukunde zu durchlaufen hat – oder auch ein Telekommitarbeiter, der Verträge für Neukunden anlegt – fiel mir irgendwann Folgendes auf: Das System schlug mir immer einen Benutzernamen vor, der auf dem von mir verwendeten Nachnamen basierte. Basierte heißt, dass wenn ich z.B. Schmidt angegeben hatte, ich nicht den Benutzer Schmidt vorgeschlagen bekam, sondern z.B. Schmidt99. Übersetzt hieß das: Es gab schon den Benutzer Schmidt, sowie die Benutzer Schmidt1 – Schmidt98. Neben dem Benutzernamen musste man sich noch ein Passwort vergeben. Die Mindestanforderung daran war, dass es mindestens 8 Zeichen lang sein musste und davon mindestens eine Zahl.

Stellen Sie sich nun einen unmotivierten Telekommitarbeiter, oder einen – durch das Vertragsabschlussprozedere – genervten Kunden vor – welche Kombinationen aus Benutzername und Passwort mögen da herauskommen?

Ich probiere ein paar häufige Familiennamen aus und notiere, welche Benutzer schon angelegt wurden. Ich wechselte zur Anmeldeseite und probierte meine Liste durch. Die Trefferquote war erschreckend hoch. Ein passenderer Vergleich, als dass das Schließfach eine Tür aus Pappe hatte, fällt mir nicht ein.

Als ich spaßeshalber noch ein paar beliebte Begriffe probierte, wurde es richtig interessant. Den Benutzern Telekom1 mit dem Passwort telekom1 und Internet2 mit dem

Passwort internet2 bekamen ein viel ausführlicheres Menü dargestellt, als ich es gewohnt war.

Es tauchten plötzlich Links auf, wie z.B. Vertragssuche. Ich probierte den Link und landete auf einer Seite, wo ich Verträge nach diversen Suchkriterien im OBSOC suchen lassen konnte. Ein paar Tests ergaben, dass die Suche regional eingeschränkt war. Suchanfragen mit dem Benutzer telekom1 ergaben Treffer in und um Freiburg, internet2 in Berlin.

In den Verträgen selbst konnte ich zuerst keine Einsicht in sensible Kunden-Zugangsdaten erlangen. Statt dessen konnte ich mehr Informationen von der Vertriebsseite sehen. Unter anderem auch den Benutzernamen des Vertriebsmitarbeiters, der den Vertrag abgeschlossen hatte. Gut, dass in fast jedem Benutzernamen eine Zahl vorkam, dadurch hatten die Telekommitarbeiter es nicht so schwer bei der Passwortwahl.

Ich hatte inzwischen ja gelernt, dass die Telekom URLs nicht immer gut geschützt waren, also probierte ich folgendes: Ich rief – als regionaler Telekomvertriebsmitarbeiter eingeloggt – einen beliebigen Vertrag auf. Wie in dem Fall üblich, fehlte in der Vertragsdarstellung der Link zum s.g. Betriebsdatenblatt. Auf diesem Betriebsdatenblatt bekommt man als Kunde übersichtlich seine sensiblen Zugangsdaten dargestellt, z.B. FTP-Zugangsdaten, Zugangsdaten zu POP3 Konten, root-Passwörter usw.

Dieses Betriebsdatenblatt wird normalerweise in einem neuen Fenster mit der URL

http://www.t-mart-web-service.de/ bdbdata/ Betriebsdatenblatt.asp

in der Adresszeile dargestellt. Ich ersetzte also die aktuelle URL, die den Vertrag darstellt, durch die des Betriebsdatenblatts und voilà – alle sensiblen Zugangsdaten, die einen Vertriebsmitarbeiter eigentlich nicht zu interessieren haben, auf einen Blick.

Ich teilte der Telekom den grundsätzlichen Fehler in der Benutzerverwaltung mit und machte darauf aufmerksam, dass ich dadurch schon eine Menge Benutzer/Passwort Kombinationen geknackt hatte.

Außer, dass das eine Benutzerkonto gesperrt wurde, das ich dem Telekommitarbeiter telefonisch genannt hatte, geschah nichts.

Die Telekom schien durch dieses Sicherheitsloch nicht die geringste Bedrohung zu empfinden.

Während ich wartete, dass etwas geschah deckte, ich noch einige Passwort-Kapriolen auf. Die T-Punkte rund um Mannheim hatten für das OBSOC jeweils den Ortsnamen mit einer 1 dahinter als Benutzer und Passwort – Heidelberg1, Mannheim1, Ludwigsburg1... Die Vertretung der Telekomfiliale in Regensburg war so clever und hat die Nachnamen ihrer Mitarbeiter einfach mit Einsen aufgefüllt, bis die Mindestzeichenlänge von 8 Zeichen erreicht war – klein111, schmit11 usw. Soweit zu den regionalen Mitarbeitern.

Noch misstrauischer geworden, nahm ich mir erneut die Seiten des OBSOC vor. Es fiel mir auf, dass der Link, der den Fehler im Zukaufsmodul verursacht hatte, auf mehreren Seiten in unterschiedlichen Varianten auftauchte. Abgesehen von der Vertragsnummer gab es da ja noch die Variable `intPurchaseType`. Ein paar Experimente brachten folgende Erkenntnisse:

Die Variable `intPurchaseType` gibt die Art des Kaufs an.

`intPurchaseType=1` heißt: Ein Neukunde will einen Vertrag abschließen.

`intPurchaseType=2` heißt: Ein bereits vorhandener Kunde möchte zu einem bestehenden Vertrag einen Zukauf tätigen.

intPurchaseType=3 heißt: Ein bereits vorhandener Kunde schließt einen neuen Vertrag ab.

Was würde also passieren, wenn ich noch gar nicht eingeloggt bin, aber angebe, dass ein bestehender Kunde einen neuen Vertrag abschließen möchte? Ich habe es ausprobiert und an der Stelle, wo ich sonst die Vertragspartnerdaten eingab, war schon eine Telekomabteilung eingetragen. Selbstverständlich konnte ich dann auf den Seiten, auf denen ich sonst die Ansprechpartner angab, alle Mitarbeiter dieser Vertriebsstelle einsehen.

Ohne Login wurden mir alle Mitarbeiter einer zentralen Telekom Abteilung angezeigt – cool ... ich erinnere an das o.g. Problem in der Benutzerkennungs- und Passwortvergabe.

Ein Mitarbeiter fiel mir sofort ins Auge: tpirkmyer01 Ein Versuch ein Treffer. Eine Überraschung erlebte ich, als ich die Vertragssuche ausprobierte: Es gab nun keine regionale Einschränkung mehr, d.h. ich konnte bundesweit Verträge aufrufen.

Es gab also auch bei den Telekombenutzern noch unterschiedliche Sicherheitsstufen.

Noch ein Name, der mir in der Liste sofort ins Auge stach: `cccrene1` noch ein bundesweiter Mitarbeiter ist als Passwortkiller entlarvt. In dem Menü von `cccrene1` taucht das erste mal der Menüpunkt Benutzerverwaltung auf. Vorher testete ich noch die Vertragssuche. Cccrene1 hatte einen erweiterten Zugriff auf die Vertragsdaten. Neben den Vertriebsinformationen, bekam er auch alle Daten, die zu dem Betriebsdatenblatt des Kunden gehörten problemlos dargestellt – anders als noch bei `tpirkmyer01`.

Zur Benutzerverwaltung: Ein paar Tests ergaben, dass er nur Kunden dargestellt bekam. Er konnte nichts Ändern und auch keine neuen Benutzer anlegen. Die URL in der Benutzerverwaltung, nach einer Suchabfrage, sah folgendermaßen aus:

http://t-mart-web-service.de/ users/Usereditor.asp? Mode=Existing&CPRPK=xyz

Die Variable CPRPK stand für die Benutzernummer. Routiniert änderte ich diese Nummer, bestätigte und wieder: Ohne erneute Abfragen bekam ich die Daten sämtlicher Benutzer nur durch das Ändern der Benutzernummer dargestellt. Ich fing an, die Nummernbereiche abzuklappern. Endlich fand ich Benutzer, die zu der Gruppe OBSOC-Detmold gehörten. In Detmold befindet sich die Mulitmediazentrale der Telekom. Es gab also die Hoffnung auf noch mehr Zugriff auf das System, durch ein Problem, dass die Telekom nicht ernst genommen hatte.

Ich suchte nach auffälligen Benutzernamen: `drwang`; Passwort: `obsoc2000` – Administratorebene. Das Paßwort hatte mir ein Telekommitarbeiter für eine paßwortgeschützte

Datei genannt, die er mir im Sommer 2003 gemailt hatte. 1+1=?. Der gute Kollege wollte besonders witzig sein, da ich ihm damals ebenfalls von den Sicherheitslöchern erzählt hatte – inkl. der Problematik in der Benutzer- und Passwortvergabe. Unternommen – bis auf oben genannte humoristische Einlage – hatte er trotz Versprechungen allerdings nie etwas. Der Gag war im dafür unbewusst umso mehr gelungen.

Der Nachweis war erbracht. Ich konnte mich als Mitarbeiter der – im OBSOC so genannten – Sales Unit und dem Status eines OBSOC-Detmold in das System einloggen. Eine Katastrophe für die Telekom, wäre dies böswillig und mit üblem Vorsatz geschehen. Ich hatte uneingeschränkten Zugriff auf sämtliche Verträge und Benutzerdaten – inklusive der Möglichkeit die anderen Administratoren und sonstigen Benutzer zu verändern, oder auch sogar ganz zu sperren.

Ich meldete das Problem nun etwas ernster der Telekom, mit dem Ergebnis, dass diese fast drei Monate brauchte, um das System so zu verändern, dass ich keinen administrativen Zugriff mehr hatte. Die ersten Versuche gingen gründlich daneben. Zwar wurde die Latte für das Passwort höher gelegt und jeder, der gegen die neuen Regeln verstieß, oder auch bis dahin verstoßen hatte, wurde bei einem Login gezwungen, sein Passwort – entsprechend der neuen Regeln – zu ändern. Vergessen wurden dabei nur ein paar Links auf Testseiten von Mitarbeitern, die ich über Google gefunden hatte.

Mit Hilfe dieser Links wurden die ersten Schritte der Anmeldung übersprungen, und damit auch die Plausibilitätsprüfung des Passworts. Ich konnte die mir bekannten Benutzer also weiterbenutzen, ohne dass es jemand bemerkt hat. Ein Hinweis an die Telekom ließ die Links verschwinden.

Später habe ich die Links in diversen Onlineshops der Telekom wiedergefunden, dafür sind sie dort also getestet worden. Der Übersprung wurde nach dem Hinweis ebenfalls durch eine Systemänderung unterbunden.

Inzwischen kann man sich mit administrativen Rechten nur noch am OBSOC anmelden, wenn man an einem Arbeitsplatz des Telekom-Intranets sitzt.

Das machte dann erst einmal einen sicheren Eindruck. Allerdings hatte ich einige große Fehler noch nicht gemeldet, die auch bis heute unentdeckt blieben. Alles Fehler, die auf der Änderung von URLs beruhen.

Die s.g. IntraSelect-Kunden sind bei der Telekom nach wie vor im OBSOC nicht geschützt. Mit der URL

http://www.t-mart-web-service.de/ContractManagement/Default.aspx?conpk=xyz

kann jeder einmal eingeloggte Kunde Einsicht in die Vertragsdaten dieser Kunden nehmen. xyz steht hierbei natürlich wieder für die Vertragsnummer. Zu diesen Kunden gehören u.a. die Deutsche Bundesbank genauso wie DPD und die METRO AG.Weiterhin sind alle Vertragspositionen der Kunden ungeschützt. Die Telekom hatte zwar nach dem ersten Vorfall die Verträge der Kunden untereinander gesperrt, jedoch, wie fast immer, nur halb. Die Seite, die den Vertrag darstellt, ist eine Frameseite, wobei die Informationen zu den diversen Vertragspositionen jeweils in einem Unterframe dargestellt werden. Die Eigenschaften dieser untergeordneten Seite ergeben folgende Adresse:

https://www.t-mart-web-service.de/Wizard/BView.asp?conitempk=xyz&conpk=abc&prodpk=12076&ActiveConPK=abc&produniquename=tmart.share.WebShare2000

Jede Menge Variablen, die eigentlich überflüssig sind. Wenn man die URL einfach auf folgende Weise abkürzt, funktioniert es auch:

https://www.t-mart-web-service.de/Wizard/BView.asp?conitempk=xyz

Die Variable `conitempk` gibt die Nummer der Vertragsposition an, unter der diese Position in der Datenbank gespeichert ist. Es verwundert nun bestimmt Niemanden mehr, dass diese Nummer beliebig geändert werden kann, um Zugriff auf fremde Daten zu bekommen. Ich kann zwar nicht mehr das ganze Schließfach auf einmal einsehen, aber ich kann mir nacheinander die einzelnen Sachen aus fremden Schließfächern nehmen und in Ruhe auf ihren Wert prüfen und bei Bedarf ent/ver-wenden.

Soviel zu der Unsicherheit der Anwendung.

Die Sicherheit der Infrastruktur

Da hatte die Telekom in Kooperation mit Microsoft nun ein interessantes Grundmodell aufgebaut. Es gab ein OBSOC-Netz, das die Kundenverträge und die darin enthaltenen Daten verwaltet. Gleichzeitig gab es eine Webfarm, die ja irgendwie vom OBSOC aktuell gehalten werden musste. Meine Schlussfolgerung war, dass es mindestens zwischen diesen beiden Netzen eine Verbindung geben musste.

Neben dem OBSOC stehen – zumindest den Webhosting Kunden – diverse Webseiten zur Verfügung, über die sie z.B. Aktualisierungen an seinem Internetauftritt vornehmen können. Zu diesem Zweck gibt es je nach Kundenvertrag unterschiedliche Server im Internet, z.B. *https://admin2.profi-webs.de/* oder auch *https://upload2.t-intra.de/* - der erste für Windows 2000 Kunden, der zweite für alte Windows NT Kunden.

Auf dem Server Upload2 gab es eine Seite, die es dem Kunden ermöglichen sollte, Seiten aus seinem bestehenden Internetauftritt zu löschen.

Zu diesem Zweck wurde dem Kunden der Inhalt seines Stammverzeichnisses in einem Listenfeld dargestellt. Dort konnte er sich nun die Ordner klicken, Dateien auswählen und über einen Button die Löschung bestätigen. Ich habe die Seite in einem neuen Fenster geöffnet und folgender Text stand in der Adresszeile:

https://upload2.t-intra.de/FileList.asp

Nachdem ich in der Liste einen Ordner zum Öffnen gewählt hatte, änderte sich die Zeile folgendermaßen:

https://upload2.t-intra.de/FileList.asp?curPt=/xyz

`curPt=` hieß demnach aktuelle Position in der Verzeichnisstruktur.

Wer kennt nun nicht den guten alten Befehl

`cd ../..` ? Ich änderte also entsprechend die Adresszeile:

https://upload2.t-intra.de/FileList.asp?curPt=../

Was sollte anderes passieren, als dass ich das Verzeichnis dargestellt bekomme, in denen sämtliche Kundenverzeichnisse dieses Servers liegen. Noch ein Sprung höher in der Verzeichnisstruktur mit `curPt=../..` und schon sehe

ich den gesamten Inhalt der Festplatte. Ich erinnere daran, dass mir dort ein Button mit der Aufschrift LÖSCHEN zur Verfügung steht.

Meines Wissen nach gibt es die Server upload2 – upload12 – wer sich also mal so richtig austoben möchte... Diese Infrastruktur war also schon mal nicht sicher.

Wie Sie oben sicherlich schon festgestellt haben, regiert in Sicherheitsfragen bei der Telekom des öfteren Gebruder Leichtfuß. Als eine Art Nest dieses Leichtsinns haben sich für mich sehr schnell Internetauftritte herauskristallisiert, die – wohl zu Testzwecken – von Telekommitarbeitern eingerichtet wurden. Oft enthielten diese Domains die entsprechenden Nachnamen. Eine lange aber lohnenswerte Suche begann.

Bei einer Domain wurde ich richtig fündig. Bei einem Mitarbeiter mit der Domain *xyz.org* (xyz steht für den Nachnamen des Mitarbeiters und wurde selbstverständlich hier von mir geändert.) wurde eine 280 MB große Datei zum Download angeboten. Nach einer kurzen Analyse stand fest, dass es sich bei dieser Datei um ein Backup einer Microsoft SQL-Server Datenbank handelte. Nach dem Einspielen auf einen entsprechenden SQL-Server war die Überraschung noch größer: Es war ein Backup der Tintra-Datenbank. In dieser Datenbank fand ich sämtliche Daten, die sonst so gut geschützt im OBSOC auf dem Betriebsdatenblatt standen.

Natürlich gab es neben diesen Daten auch jede Menge interne Daten. Für mich waren zwei Informationen besonders interessant:

Eine Tabelle mit den Servern, die wohl alle zur Webfarm der Telekom gehörten. Namen, IP-Adressen...

Eine Tabelle, die ein Benutzerkonto inklusive Domain und Passwort enthielt.

Der Benutzer hatte den vielversprechenden Namen `autoscripting`. Ich schloss aus dem Namen, dass dieser Benutzer herhalten muss, wenn das System skriptbasiert eine Aufgabe ausführen soll, für die eine Anmeldung von Nöten ist.

Ich loggte mich mit den Zugangsdaten von `autoscripting` auf einen FTP-Server der Telekom ein. Schon befand ich mich in einem Unterverzeichnis, wo alle auf diesem Server untergebrachten Kundenverzeichnisse lagen. Ich musste nur mit dem FTP-Befehl `cd <Kundennummer>` in das entsprechende Verzeichnis springen. Da ein `ls` oder dir Befehl in dem Stammverzeichnis mit den Kundenverzeichnissen keine Wirkung hatte, würde es sich sehr mühsam gestalten, alle möglichen Kundennummern zu probieren. Mit Hilfe des Fehlers im o.g. Skript, war es dann aber nicht so problematisch.

Bei den FTP-Zugangsdaten gibt die Telekom vor: Windows-DomainBenutzername und das Passwort. Um auf den Administrationsserver zuzugreifen, braucht man die Windows-Domain bei der Anmeldung nicht mit anzugeben, da windowsintern der Webserver als Domain vorgegeben sein sollte. Ein Anmeldeversuch mit `autoscripting` mit Angabe der Domain wurde aber nicht abgelehnt.

Um festzustellen, ob die Anmeldung intern nicht gekürzt wurde, schrieb ich eine ASP-Programmierung, die mir auf einer Seite den Inhalt eines angegebenen Verzeichnisses darstellen konnte. Die Unterverzeichnisse wurden dabei so als Hyperlink angelegt, daß diese die selbe ASP Seite nutzen konnten, um wiederum ihren eigenen Inhalt darstellen zu können. Wenn Dateien gefunden wurden, wurden diese ebenfalls als Hyperlink angelegt – und zwar so, dass es reichte den Hyperlink anzuklicken, um diese Datei dann auf einen FTP-Server der Telekom netzintern zu kopieren. Von dort aus konnte ich diese dann ganz normal herunterladen.

Als erstes mussten also zwei Parameter übergeben werden können – das Verzeichnis und die Datei, die eventuell kopiert werden soll:

```
Set objQueryString = Request.QueryString
strServerName = objQueryString(
  „strServerName“)
strCopyFile = objQueryString(„strCopyFile“)
```

Die Voreinstellung für `strCopyFile` war “none” , und wurde nur bei Links ersetzt, denen Dateien zugrunde lagen. Da drüber konnte das Skript entscheiden, ob es etwas zu kopieren gab, oder nicht.

Mit folgenden Zeilen wurde eine Serveranmeldung erzwungen:

```
If Request.ServerVariables(„LOGON_USER“)=““
Then Response.Status = „401 Access Denied“
End If
```

Die entsprechenden Objekte anlegen:

```
Set objFSO = Server.CreateObject(
  „FileSystemObject“)
Set objFolder = objFSO.GetFolder(
  strServerName)
```

Ein Collection Objekt, das zur Auswertung der Ordner durchlaufen werden kann:

```
Set objCollection = objFolder.SubFolders
```

Nachdem die Ordner abgearbeitet sind, wird der Fokus des Collection Objekts auf die Dateien gelegt:

```
Set objCollection = objFolder.Files
```

Wenn diese Objekte ausgewertet sind, sollte ich eine entsprechende Tabelle erhalten, die mir die Ordner und Dateien eines vorher im Parameter angegebenen Verzeichnisses auflistet.

Um Dateien oder auch Ordner hin und her zu kopieren brauchte man nun nur noch die Methoden

```
objFSO.CopyFile bzw. objFSO.CopyFolder.
```

Ich testete die Seite erst einmal auf einem alten Windows NT Webserver der Telekom. Das Ergebnis war beeindruckend, zumal die Webserveranmeldung die Domain eigentlich nicht hätte annehmen dürfen. Ich bekam alle lokalen Festplatten des Webservers dargestellt.

Wenn der Webserver also tatsächlich Domainanmeldungen annimmt, musste mehr möglich sein, als ein lokaler Zugriff. Ich kam zurück zu der Serverliste von dem Backup. Ich probierte willkürlich ein paar Freigaben: `\web5113c$` - Treffer. Ich probierte weitere und konnte fast jeden Server aus der Datenbank erreichen, wobei die Freigaben nicht nur auf c$ eingeschränkt waren – d$, e$... waren, je nach Server, ebenfalls möglich. Anhand der Routinginformationen eines Servers fand ich die aktuellen IP-Netze heraus, in denen sich die Server befanden. Statt Rechnernamen verwendete ich nun die IP-Adresse in der Pfadangabe, und so stellte

ich fest, dass ich allein in einem IP-Netz Zugriff auf über 70 Server in drei Domains hatte.

Test ergaben, dass ich Vollzugriff auf alle Laufwerke aller Windows Webserver hatte.

Zugriff auf die UNIX-Server erhielt ich nur durch unsichere Microsoft SQL-Server, auf denen die Passwörter für die UNIX-Benutzer gespeichert waren.

Wie geschrieben, hatte ich dadurch Zugriff auf Telekom SQL-Server, wo unter Anderem die Tintra-Datenbank, eine SMS-Datenbank oder auch die Datenbank, wo gesperrte Spamer, hinterlegt sind. Die Datenbanken kann man zwar bekanntlich nicht aus dem laufenden Betrieb heraus kopieren, aber in den meisten Fällen gab es in den Unterverzeichnissen ein vortagesaktuelles Backup der entsprechenden Datenbank.

Die Krönung aber war, dass ich dort ein Backup der OBSOC-Datenbank fand. Damit schloss sich für mich der Kreis zwischen der Sicherheit in der Anwendung und der Sicherheit in der Infrastruktur.

Ein Test ergab, dass ich von innerhalb des Telekomnetzes ebenfalls beliebig Dateien über den schon vorher erwähnten FTP-Server kopieren konnte. Selbstverständlich hätte ich mit dem Script auch Dateien auf die Server kopieren können. Welche Möglichkeiten sich daraus ergeben hätten, malen Sie sich am besten selber aus. Vor allen Dingen, wenn Sie berücksichtigen, dass dort Installationshandbücher auf Servern lagen, die genau beschrieben, wann welches Script- oder Batchprogramm zeitgesteuert gestartet wurde.

Ich hatte also Vollzugriff auf Server im Telekomnetz, die keine eigene Verbindung zum Internet hatten. Genau an dieser Stelle habe ich mit meinen Nachforschungen abgebrochen, denn ein Weiterkommen wäre ohne die Manipulation von bestehenden Daten nicht möglich gewesen. Was natürlich nicht heißt, das ein Krimineller an dieser Stelle aufhören würde.

Worüber rege ich mich eigentlich auf?

Die Telekom ist beim Bundesamt für Sicherheit in der Informationstechnik (BSI) als Zertifizierungsstelle für Softwaresicherheit angegeben. Beim Branchenverband für Informationstechnik und Telekommunikation (BITKOM) ist die Telekom einer der Mitgründer. Zusammen mit u.a. dem BSI, BITKOM und Microsoft sponsert die Telekom das Sicherheitsportal MCERT, wo Unternehmen gegen ein monatliches Entgeld mit Informationen über aktuelle Sicherheitsprobleme informiert werden sollen.

Es würde mich brennend interessieren, wen die Telekom über die Vorfälle im Mai/Juni 2003 und dem folgenden Jahr informiert hat. Welcher Emailbenutzer wurde gewarnt, dass seine Zugangsdaten durch mehrere Programmierfehler mehrfach völlig ungeschützt waren? Welches Unternehmen oder welche Behörde wurde darüber unterrichtet, dass sensible Unternehmensdaten und Personendaten nicht ausreichend geschützt wurden?

Da wäre noch die Frage, warum die EU-Richtlinie zum Datenschutz in der elektronischen Kommunikation in Deutschland immer noch nicht in nationales Recht umgesetzt wurde? Diese Richtlinie wurde bereits 2002 vom Europäischen Parlament und Rat erlassen. Im Oktober 2003 wurde ein Verstoßverfahren u.a. gegen Deutschland wegen nicht Umsetzung dieser Richtlinie eingeleitet und im November 2003 von der Europäischen Kommission beschlossen. In dieser Richtlinie werden Unternehmen u.a. Sicherheitsstandards zum Schutz von Kundendaten im Internet vorgeschrieben.

Bis dahin ist es für die Unternehmen offenbar ein Einfaches, jemanden, wie in diesem Fall mich, der mit Hartnäckigkeit Datenschutzvergehen aufdeckt, zu kriminalisieren. Es wirkt auf mich sehr hilflos, wenn ein Global-Player mit deutschen Paragraphen droht und dabei offenbar vergisst, dass sein Global-Network von anderen Ländern genauso angreifbar ist. Daher sollten Unternehmen wie die Telekom, in meinen Augen nicht primär dazu tendieren, ihre Kundendaten innerhalb Deutschlands von einer teuren Rechtsabteilung schützen zu lassen, sondern es als höchste Aufgabe verstehen, ihre Kundendaten weltweit von einer cleveren EDV-Abteilung schützen zu lassen.

Ich kann nicht sagen, wie tief die Abgründe im OBSOC und den dort angeschlossenen Netzen noch sind. Ich meine jedenfalls, dass hier eine Kontrolle von einer der Telekom übergeordneten Instanz dringend notwendig ist.

Der Versuch eine Entschädigung von der Telekom für meinen Aufwand zu bekommen war einmal mit Hilfe meines Anwaltes für die ersten beiden gemeldeten Sicherheitslöcher erfolgreich.

Danach ist jeder Versuch darin geendet, dass man mir einen sehr eingeschränkten Beratervertrag für die Zukunft angeboten hat, ansonsten würde man mein Verhalten in der Vergangenheit neu bewerten. Soll heißen: entweder Du nimmst den Vertrag an, oder wir drohen Dir mit bis zu drei Jahren Gefängnis. Abgesehen von dieser unhöflichen und in meine Augen unverschämten Art, hatte dieser Vertrag in meinen Augen nur den Zweck, mich zu knebeln.

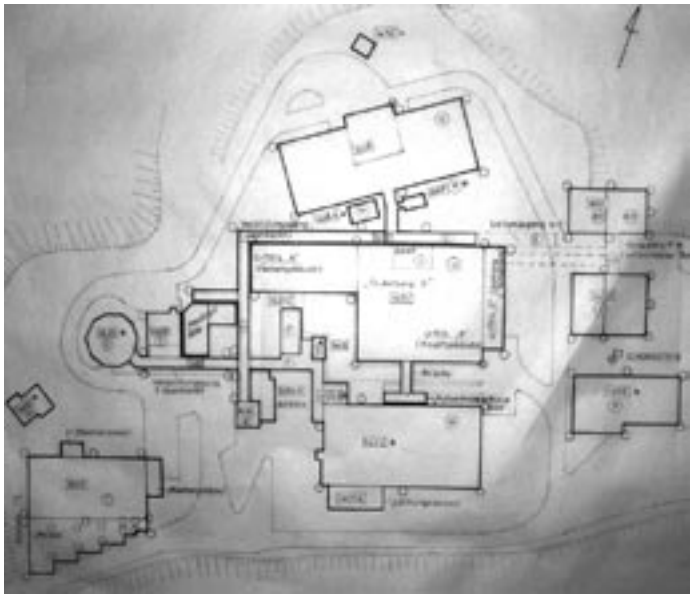
Wie schon oben bemerkt, ist seit über einem Jahr nichts, aber auch gar nichts von dem oben geschilderten an die Öffentlichkeit gelangt. Obwohl doch eigentlich Hunderttausende hätten informiert werden müssen, dass ihr verwendetes Onlinezahlsystem nicht mehr sicher ist, oder das man für die nächste Zeit vielleicht besser kein OnlineBackup macht, da man definitiv nicht gewährleisten kann, dass Niemand unberechtigter Weise Zugriff auf die Kundendaten hatte. Die Blöße, zuzugeben, dass man sich mit dem Personal Security Service eventuell Hacker einlädt, anstatt diese abzuwehren, hat sich meines Erachtens die Telekom auch noch nicht gebracht. Liebe Telekom, es wäre also langsam wirklich an der Zeit, ehrlich zu seinen Kunden zu sein.

Wer ein solches Projekt startet, trägt nicht nur das Risiko, schnell viel zu verdienen, sondern in erster Linie die Verantwortung für den Schutz von fremden Daten. Die Bundesregierung sollte an dieser Stelle schnellstens tätig werden, anstatt ein Patentgesetz für Dinge zu unterstützen, die in kein Produkthaftungsgesetz der Welt fallen – oder haben Sie schon mal davon gehört, dass Microsoft die produzierten Windows 2000 CDs der Jahre 2000 – 2004 zurückrufen musste?

NSA Field Station Berlin Teufelsberg - a late post mortem

von anonymous <ds@ccc.de>

One doesn't often have the chance to visit a SigInt outpost, unless you or your Daddy is an army general. Of course, the Teufelsberg fascilities have been abandoned after the end of the cold war. But still some treasures may be lifted and some discoveries made. Here is, what an anonymous source collected.



The station was situated in the British sector of West Berlin, so the US services technically were guests there. Given the intense collaboration of the british and american intelligence agencies, this was only a technicality. The British armed forces had one own building (building M aka. 1455) on the hill and a very high metal grid antenna tower (removed around 1992) for their collection antennas. It is currently not entirely clear, how collection and analysis efforts were shared between the two operating countries, but common operation of auxiliary services (like power, heating, sewer, dining facility etc.) are obvoius. One fascinating difference between the US-American and British complex on the hill is, that the latter had three different types of toilets: ladies, normal men and officers. US forces had to live with just the normal two toilet varieties.

In the last years of its existence the US operation on the Teufelsberg has been managed by the US Army Intelligence and Security Command INSCOM. The NSA itself had analysts, researchers and linguists on the Teufelsberg, in different allocation over time. Detachments from other services, like Air Force, were assigned to a number of missions, like finding ways to subvert the Eastern air defense forces in case of a hot war. They analyzed the radar and radio traffic to an extend, that should enable them to give false orders to enemy interceptor pilots in case of an attack. Computerized voice databases and mission profile analysis were some of the tools involved (in the 80s!).

The Field Station contained all kinds of ELINT and SIGINT equipment, biggest known pieces were the fully rotatable down to below horizon 40 feet (12 meter) dish antennas inside the radomes left and right of the main tower. The directional microwave link networks inside East Germany were probably recorded completely, as they all converged in East Berlin and had considerable beam width and side lobes and could therefore be easily intercepted with the kind of resources installed on the Teufelsberg.

The main towers floors apparently were full of microwave link interception antennas. New types of air defense radars could be analyzed in detail as well as satellite transmissions and radio communications intercepted and analyzed. It is known that West Berlins wireless communication systems also were on tap, to round off monitoring of its wired communication, performed in other

installations – like the one in Mariendorf – under Allied Law. As rumor has it, even relatively small radio based room bugs, installed somewhere in Berlin, were receivable with the enormous antenna systems.

The Teufelsberg installation is abandoned now. An investment company wanted to built a "resort", meaning high-priced flats and a hotel, on the old base. It apparently went belly up, so the area can be visited now, even if it technically might be illegal. A number of remaining installations, like the document and tape destruction systems, shielded rooms and floors, safes and secured facilities and particularly antenna radomes are very well worth the visit. Some of our findings are in this Datenschleuder (see inlet), more images and comments can be found at *http://www.ccc.de/teufelsberg/*, we will expand this documentation as new information arrives.

Above you find an overview map of the installation, photographed from a wall in building 1458. It probably was made after intelligence people left. Due to construction work (recently abandoned), aimed at building expensive apartments in the area, some buildings no longer exist. Primarily the buildings 1457, 1456 and 1466 (right side of map) are demolished. For the historically interested, most promising buildings are 1475 (US computing and analysts building), 1455 (British building), 1425 (also called Arctic Tower or Search Tower) and, of course, 1458 (main operations building with the tower and "ball" radomes). The construction work heavily affected the analysts and operation floors of the tower building (1458), so there are only few traces of its past use visible.

All buildings are connected by covered walkways (Verbindungsgang), except the dining facility (1453), the small Jamabalya radar tower (1465) and some minor outlaying utility constructions.

The aerial image below approximately depicts the maximum installation on Teufelsberg. Apperent is the big antenna tower used by the British GCHQ. Notice the small radomes on top of the big tower and the Arctic tower main radomes. Their usage is unclear and they have been removed when the NSA left. Also visible are some smaller antenna towers with antennas that lilkely were part of a short-wave directional setup. Unfortunately one of the most mysterious installations, the Jambalaya tower is just outside the right edge of the image. Instead some different structures can be seen.

CAN - Controller Area Network

von alexander <alexander.bernauer@ulm.ccc.de>

CAN ist ein Standard für echtzeitfähige Bussysteme. Mitte der Achtziger wurde er in den ersten Luxuslimusinen eingebaut und ist heutzutage aus keinem modernen Automobil mehr wegzudenken. Typischerweise existieren in einem Auto mehrere getrennte CAN Busse mit unterschiedlichen Geschwindigkeiten.

Ein Low Speed CAN (ISO 11519-2) mit maximal 10 kBit/s erlaubt Funktionalitäten im sog. Chassis-Bereich. Dazu gehört u.a. das Ein- und Ausschalten von Lichtern und Blinkern, das Verstellen der Sitzposition und der Außenspiegel, die Türverriegelung und andere Komfortfunktionen. Ein zweiter Low Speed CAN erlaubt den Informationsaustausch mit bis zu 40 kBit/s. An diesem Bus hängen u.a. die Anzeigen des Armaturenbretts und die Klimasteuerung. Echtzeitkritische Systemem kommunizieren über einen High Speed CAN (ISO 11898-2) mit bis zu 1 MBit/s, der maximalen Transferrate für CAN. Zu diesem Sytemen gehören z.B. die Motorsteurung und die Stabilitätskontrolle.

1983 wurde die Entwicklung von CAN bei Bosch begonnen und dauerte drei Jahre. Eine Kooperation mit Intel ergab 1987 den ersten CAN Chip. Kurz darauf folgten andere Hersteller wie Philips mit eigenen ICs. 1991 veröffentlichte Bosch seine bis heute gültige CAN 2.0 Spezifikation. Diese beschreibt die unteren zwei Layer des OSI Referenzmodells in einem monolithischen Ansatz. Zur Standardisierung der von vielen Seiten entwickelten Application Layer für CAN wurde im Folgejahr die "CAN in Automation" (CiA) [1], eine internationale Interessensgruppe aus Herstellern und Anwendern, gegründet. Sie veröffentlichte 1992 das CAN Application Layer (CAL) Protokoll. Dieses und andere Protokolle wie das 1995 veröffentlichte CANOpen, ermöglichen eine abstrakte Programmierung und flexible Konfiguration des Netzwerkes. Ebenfalls 1992 wurden die ersten Autos von Mercedes-Benz mit CAN Netzwerken ausgestattet. Seit 1993 ist die CAN 2.0 Spezifikation ein ISO Standard.

CAN ist ein Multimaster Bus. Keiner der Teilnehmer hat für den Busbetrieb spezielle Aufgaben und somit existiert kein "Single Point of Failure". Die Knoten sind typischerweise Sensoren und Aktoren, die an einem Microcontroller mit CAN Interface angeschlossen sind. Tritt ein definiertes Ereignis ein, wie z.B. das Drücken eines Knopfes, das Überschreiten einer Schwelle für einen Meßwert oder der Ablauf eines Timers, so broadcastet der entsprechende Knoten eine Nachricht auf dem Bus. Knoten, die nicht an dieser Nachricht interessiert sind, besitzen Hardwarefilter, um die langsamen CPUs nicht übermässig zu belasten. Eine Nachricht besteht im wesentlichen aus einem Identifier und 0 bis 8 Datenbytes. Für die Länge des Identifiers gibt es zwei Standards. CAN 2.0A definiert die Standard Frames mit 11 Bit Identifier und CAN 2.0B die sog. Extended Frames mit 29 Bit Identifier. Eine Nachricht trägt keine Informationen über ihre Herkunft und ist somit anonym. Vielmehr besitzt sie nur eine vom Identifier abhängige Bedeutung, die per Systemdesign festgelegt ist.

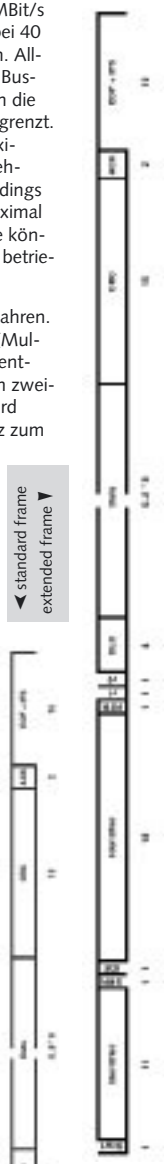
Für die Verdrahtung existieren zwei unterschiedliche Möglichkeiten. Im asymmetrischen Modus gibt es eine Masse- und eine Signalleitung. Zum Einsatz kommt er vor allem dort, wo Kosten gespart werden müssen, da er mit billigen Leitungstreibern arbeitet. Man kann sich sogar die Masseleitung sparen und z.B. die Karrosserie als Bezugspotential verwenden, was üblicherweise im Chassis-Bereich getan wird. Allerdings ist dies störungsanfällig und eignet sich daher nur für geringe Busgeschwindigkeiten. Die maximalen Transferraten erreicht man nur im differentiellen Modus. Dort entscheidet das Vorzeichen der Differenzspannung zwischen den beiden Leitungen CAN High und CAN Low über den Wert des Bits. Wenn diese Leitungen nebeneinander geführt werden, so wirken sich lokale Störungen auf beide Signal gleich aus, wodurch die Differenz erhalten bleibt. In jedem Fall muss der Bus an beiden Enden mit Widerständen abgeschlossen werden, um Reflekionen zu vermeiden. Alle Teilnehmer sind über Stichleitungen mit dem Bus verbunden. Zu jeder Bitzeit muss der Bus an den Orten aller Teilnehmer das gleiche Bit haben, damit die Mechanismen für den Buszugriff funktionieren können. Aus den Signallaufzeiten und den Verzögerungen der Empfänger- und Senderhardware folgt damit die maximal zulässige Buslänge

in Abhängigkeit der Busgeschwindigkeit. Bei 1 MBit/s ergeben sich maximal 30 m, wohingegen man bei 40 kBit/s Buslängen von bis zu 1 km erreichen kann. Allgemein sagt die Worst-Case Design Regel, dass Buslänge x Bitrate < 40m x 1Mbit/s sein muss. Auch die Länge der Stichleitungen ist durch die Bitrate begrenzt. So ergibt sich für den High Speed CAN eine maximale Länge von 5 Metern. Die Anzahl der Teilnehmer ist durch den Standard nicht begrenzt. Allerdings kann man mit den üblichen Leitungstreibern maximal 32 Teilnehmer versorgen. Mit teurerer Hardware können derzeit bis zu 128 Teilnehmer an einem Bus betrieben werden.

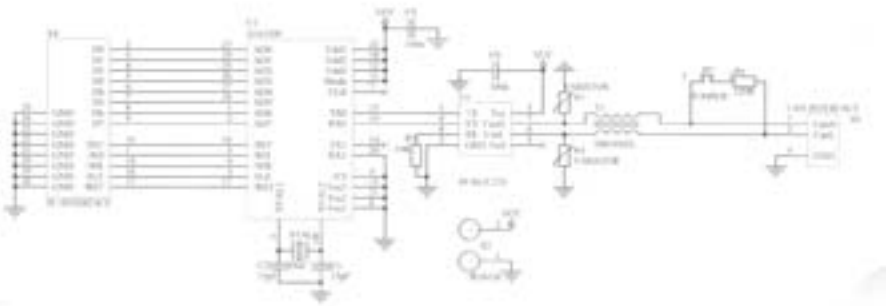
Der Buszugriff geschieht im CSMA/CD+CR Verfahren. Jeder Knoten darf, wann immer er will, senden (Multiple Access), sobald er eine Pause auf dem Bus entdeckt (Carrier Sense). Wenn zur gleichen Zeit ein zweiter Knoten eine Nachricht senden möchte, so wird das erkannt (Collission Detection). Im Gegensatz zum bekannten Ethernet kommt es dabei allerdings zu einer nicht destruktiven Collision Resolution. Das bedeutet, dass sich die Nachricht mit der höheren Priorität durchsetzt und der Sender der anderen Nachricht sofort zum Empfänger wird. Grundlegend für diesen Mechanismus ist eine spezielle Leitungskodierung. Im Prinzip ist es eine Non-Return-to-Zero (NRZ) Kodierung. Wenn allerdings ein Knoten eine 1 und ein anderer eine 0 schreibt, dann liegt auf dem Bus eine 0. Man sagt, dass die 1 rezessiv und die 0 dominant ist. Im Fall einer Kollision erkennt einer der Sender, dass er überschrieben wird, indem er während der sog. Arbitrierungsphase beim Schreiben jedes Bit gleichzeitig liest und vergleicht. Der andere Sender bemerkt die Kollision nicht und sendet weiter, so dass sich seine Nachricht durchsetzt. Die Arbitrierungsphase geht über den kompletten Identifier, so dass Nachrichten mit kleinen Identifiern hohe Priorität haben. Das gleichzeitige Senden von zwei Nachrichten mit dem selbem Identifier ist verboten und muss durchs Systemdesign verhindert werden.

Zur Synchronisation der Busteilnehmer dient ein einzelnes, dominantes Startbit vor dem Identifier einer Nachricht. Zusätzlich wird jeder Flankenwechsel zur weichen Synchronisation verwendet. Dadurch kann man billige und ungenaue Quarze verwenden. Um sicherzustellen, dass genug Flankenwechsel vorkommen, wird nach fünf gleichen Pegeln zwangsweise ein Flankenwechsel eingebaut (Bit Stuffing Regel). Das zusätzliche Bit dient nur der Synchronisation und enthält keinerlei Informationenen.

Im CAN 2.0A Frame folgen dem Identifier sieben Control Bits. Das erste davon ist das Remote Transfer Request (RTR) Bit. Eine Nachricht mit gesetztem RTR darf keine Daten beinhalten. Vielmehr ist diese Nachricht eine Aufforderung, zu antworten. Die Antwort ist eine normale CAN Nachricht mit gleicher ID und nicht gesetztem RTR. Damit kann man z.B. einen Sensor pollen, falls man keine regelmäßigen Updates der Meßwerte braucht. Das RTR Bit gilt als gesetzt, wenn es den Wert 1 hat. Da die Arbitrierungsphase das RTR Bit einschließt, wird ein Request von der Antwort überschrieben, falls beide gleichzeitig gesendet werden. Das nächste Control Bit dient zur Unterscheidung des verwendeten Nachrichtenformats. Dabei steht eine 0 für Standard und eine 1 für Extended Frames. Die letzten 4 Bits heißen Data Length Code (DLC) und geben die Anzahl der Datenbytes an, die direkt danach folgen. Alle Werte zwischen 0 und 8 sind zugelassen, da auch eine Nachricht ohne Datenbytes allein durch ihr Auftauchen auf dem Bus eine Information sein kann. Eine anschließende 15 Bit CRC Summe dient zur Erkennung von Übertragungs- und Empfangsfehlern. Sie erlaubt das Entdecken von bis zu 6 Einzelfehlern und 15 Bit Burstfehlern. Die nächsten zwei Bit sind der Acknowledge Slot. Jeder Knoten, der die Nachricht mit korrektem Format empfangen hat, sendet in dieser Zeit ein 0. Der Sender schreibt ein 1 und erwartet, die 0 zu lesen. Geschieht das nicht, so hat niemand die Nachricht empfangen. Abgeschlossen wird ein Frame mit sieben rezessiven Bits, dem End Of Frame (EOF). Dabei wird absichtlich die Bit Stuffing Regel verletzt, so dass jeder diese Marke eindeutig erkennen kann. Als letztes kommen noch 3 rezessive Inter Frame Bits. Sie geben den Teilnehmer die nötige Zeit, um die Nachricht in den Empfangspuffer zu schreiben und sich auf die nächste Nachricht vorzubereiten. Sollte einem Teilnehmer ausnahmsweise diese Pause nicht ausreichen, so kann er ein Overload Frame senden. Dieses besteht aus 6 dominanten Bits und verzögert den Anfang der nächsten Nachricht. CAN 2.0B Frames beginnen auch mit einem Start Bit. Darauf folgen die ersten 11 Bit des Identifiers. An der Bitposition, an der Standard Frames das RTR Bit haben, steht allerdings immer eine 1. Anschließend kommt das IDE Bit, welches zur Identifikation des Frame Formates hier auch den Wert 1 hat. Jetzt folgen die letzten 18 Bit des Identifiers und das RTR Bit. Nach zwei weiteren Bits, die immer den Wert 0 haben, sind Extended Frames mit Standard Frames wieder identisch.



Historisch gewachsen gibt es zwei unterschiedliche Implementierungen des CAN 2.0 Standards: FullCAN und BasicCAN. Sie unterscheiden sich vor allem die Empfangsfilter betreffend. BasicCAN verwendet eine Maske und einen Code. Die Maske gibt an, welche Bits des Identifiers signifikant für die Filterung sind. Der Code gibt an, welchen Wert die einzelnen Bits haben müssen. Nur wenn alle signifikanten Bits den Wert der Codebits haben wird die Nachricht akzeptiert. Da man mit jedem Bit, das man als nicht-signifkant definiert, zwei neue Identifier durch den Filter lässt, kann man in vielen Fällen nicht engmaschig genug filtern und muss softwaremäßig nacharbeiten. Das beansprucht aber zusätzliche Prozessorzeit. FullCAN kennt keine Masken. Vielmehr gibt es mehrere Empfangspuffer, für die jeweils ein Code angegeben werden kann. Ein softletzung des Nachrichten Formats erkannt werden. Das geschieht z.B. wenn die 6 rezessiven Bits des EOF ausbleiben oder auch, wenn ein Teilnehmer standard Frames erwartet, aber extended Frames empfängt. In jedem der fünf Fehlerfälle kommt es zur selben Fehlerbehandlung. Derjenige, der einen Fehler erkannt hat, sendet ein Error Frame auf den Bus, um alle anderen von dem Fehler in Kenntnis zu sezten. Das Error Frame besteht aus 6 dominanten Bits und überschreibt somit alles andere auf dem Bus. Auch hier wird absichtlich die Bit Stuffing Regel verletzt, um das Signal eindeutig erkennbar zu machen. Wenn ein Knoten selber keinen Fehler erkennt, aber ein Error Frame empfängt, so reagiert er auf die vermeintliche Verletzung der Bit Stuffing Regel mit dem Senden eines Error Frames. Das bedeutet zwar, dass ein Error Frame auf bis zu 12 Bits



waremäßiges Nachfiltern entfällt damit. Allerdings ist die maximale Anzahl der Nachrichten, die man empfangen kann, durch die Anzahl der Empfangspuffer beschränkt. Mittlerweile gibt es CAN Chips, die beide Arten und auch neuere Techniken der Filterung beherrschen, so dass die irreführenden Begriffe FullCAN und BasicCAN veraltet sind.

Ein Design Ziel von CAN war es, dass möglichst viele Fehler bereits von der Hardware erkannt und behandelt werden. Damit spart man Rechenleistung in den CPUs und aufwändige Protokolle in höheren Layern. Zwei der fünf möglichen Fehler können vom Sender entdeckt werden. Das erste ist ein Bitfehler. Dieser liegt vor, wenn außerhalb der Arbitrierungsphase und des ACK Slots das gelesene Bit nicht mit dem geschriebenen übereinstimmt. Das zweite ist ein Acknowledge Fehler. Dieser liegt vor, wenn der Sender im ACK Slot keine 0 liest. Die restlichen drei möglichen Fehler können von den Empfängern erkannt werden. Zuerst kann ein Knoten eine Verletzung der Bit Stuffing Regel erkennen. Geschieht das außerhalb des EOF Feldes, so ist das offensichtlich ein Empfangsfehler. Außerdem kann ein Teilnehmer feststellen, dass die berechnete Prüfsumme nicht mit der Empfangenen übereinstimmt. Zuletzt kann eine allgemeine Veranwachsen kann, hat aber den Vorteil, dass jeder Busteilnehmer ein Error Frame sendet und damit im Fehlerzustand ist. Da jeder Teilnehmer im Fehlerfall die empfangene Nachricht verwirft, wird somit garantiert, dass eine CAN Nachricht entweder von allen oder von keinem angenommen wird. Das ist sehr wichtig für die Synchronisation der Busteilnehmer. Nach dem Error Frame wird die Nachricht einfach erneut gesendet.

Hat ein Knoten einen permanenten Fehler, wie z.B. einen defekten Eingang, so würde er den kompletten Bus ständig mit Error Frames beschreiben und somit lahm legen. Um das zu verhindern, hat man eine Selbstdiagnose der Busteilnehmer spezifiziert. Jeder CAN Baustein besitzt zwei Error Counter, einen für den Empfang (REC) und einen für das Senden (TEC). Kommt es zu Fehlern, so werden diese Zähler incrementiert. Wenn die Fehler wieder ausbleiben, so werden die Zähler mit der Zeit wieder decrementiert. Überschreitet einer der beiden Zähler eine Schwelle, so verhält sich der Teilnehmer Error Passive. Das bedeutet, dass er zwar ganz normal am Busgeschehen teilnimmt, aber im Fehlerfall nur noch passive Error Frames sendet. Diese bestehen aus 6 rezessiven Bits und stören damit den restlichen Bus nicht. Überschreitet der TEC eine zweite Schwelle, so geht der Baustein Bus

Off. Er nimmt nicht mehr am Geschehen teil und kann aus diesem Zustand nur durch einen Benutzereingriff wieder zurückgesetzt werden. Die Regeln zum Erhöhen und Erniedrigen der Zähler sind äußerst komplex. Beispielhaft sollen hier die folgenden, vergleichsweise einfachen Regeln erläutert werden. Wenn ein Sender einen ACK Fehler erkennt, so bedeutet das, dass niemand seine Nachricht korrekt empfangen hat. Wenn kein Bitfehler vorliegt und nicht alle anderen Teilhemher Bus Off sind, so ist seine Verbindung zum Bus sehr wahrscheinlich unterbrochen. Als Konsequenz wird der TEC erhöht. Ist die Verbindung wirklich unterbrochen, so wird der Baustein sehr bald Bus Off gehen und diesen Zustand nach oben melden. Ein zweiter einfacher Fall liegt vor, wenn ein Baustein immer eine Differenz in der CRC Summe erkennt. Insbesondere, wenn er diesen Fehler immer als erster bemerkt liegt die Vermutung nahe, dass es sich um ein lokales Problem handelt. Sollte das der Fall sein, so wird sich der Baustein ziemlich schnell "Error Passive" verhalten und den Bus nicht weiter stören. Zu beachten ist, dass im Error Passive Zustand die nachrichtenbasierte Synchronisation der Teilnehmer nicht mehr gewährleistet ist, da der Baustein im Fehlerfall die Nachricht verwirft, diese aber nicht neu gesendet wird.

Ein Chip, der nur CAN 2.0A Frames kennt, kann nicht an einem Bus betrieben werden, auf dem CAN 2.0B gesprochen wird. Neben Bausteinen, die beide Formate können, gibt es solche, die sich CAN 2.0B passiv verhalten. Das bedeutet, dass sie zwar selber keine Extended Frames lesen und schreiben können, beim Empfang aber auch keine Error Frames senden. Die Erweiterung auf 29 Bits für den Identifier war nötig, um trotz grober Filter genügend Flexibilität für Unterteilung der Nachrichten in Kategorien zu haben. Dafür bezahlt man allerdings mit einer geringeren Nettodatenrate. Mit Standard Frames kommt man bei 1 MBit/s und 8 Datenbytes auf ein Maximum von 576,6 kBits/s netto. Mit Extended Frames kommt man nur auf maximal 488,5 kBit/s. Da eine Nachricht ohne Daten auch einen Informationsgehalt besitzt, sind diese Zahlen nicht sehr repräsentativ.

Fast jeder Hardwarehersteller hat eigene CAN Lösungen in seinem Sortiment. So gibt es z.B. Microcontroller mit integriertem CAN Interface oder aufgebohrte PALs, die man remote über CAN steuern kann. Um einer bestehenden Hardware Zugang zu einem CAN Bus zu ermöglichen eigenen sich sogenannte Standalone CAN Controller, wie z.B. der SJA1000 von Philips. Er ist eine komplette Implementierung der CAN 2.0 Spezifikation mit einem parallelen Interface. Üblicherweise wird er wie externes RAM an einen Microcontroller angeschlossen. Man kann ihn allerdings auch an den Druckerport anschließen, und so mit dem Computer Zugang zu einem CAN Bus erlangen. Ausgangsseitig spricht der SJA1000 TTL. Deshalb braucht man noch einen CAN Transceiver, der die Spannungen umwandelt. Abgesehen von ein paar zusätzlichen Widerständen und Kondensatoren ist nicht mehr Hardware nötig. Alles zusammen bekommt man für unter 10 Euro. Auf dem Schaltplan sind noch zwei Varistoren und eine Spule eingezeichnet. Die Varistoren bieten einen Schutz vor Überspannung und die Spule verbessert die Signalqualität bei hohen Bitraten. Für ein einfaches Setup braucht man diese Komponenten allerdings nicht.

Das Datenblatt des SJA1000 [2] ist sehr empfehlenswert, da es den Controller ausführlich beschreibt. Deshalb folgt hier nur ein kleiner Überblick über die Möglichkeiten und die Bedienung. Der SJA1000 besitzt zwei verschieden Modi. Der BasicCAN Modus ist ein Kompatibiltätsmodus zum PCA82C200, einem älteren Baustein von Philips. In diesem Modus verhält sich der Baustein CAN 2.0B passiv. Im sogenanten PeliCAN Modus kann er aktiv CAN 2.0B sprechen und bietet noch weitere Features an, wie z.B. die automatische Baudratenerkennung und einen "listen only" Modus - beides sehr praktisch, wenn man ein unbekanntes Netz analysieren möchte. Um mit dem Controller zu kommunizieren, werden 8-bit Werte in seine Register geschrieben und daraus gelesen. Je nach Modus existieren 31 oder 39 Register mit eindeutigen 8-bit Adressen.

Im Control Register kann man vier mögliche Interrupts maskieren. Diese sind ein Receive Interrupt, ein Transmit Interrupt, ein Error Interrupt und ein Data Overrun Interrupt. Die ersten beiden werden ausgelöst, wenn eine Nachricht fehlerfrei empfangen bzw. gesendet wurde. Ein Error Interrupt tritt auf, wenn einer der beiden Error Counter (TEC oder REC) die erste Schwelle überschreitet. Ein Data Overrun liegt vor, wenn der Controller keine Puffer mehr frei hat, um eine empfangene Nachricht zu speichern. Der SJA1000 besitzt nämlich einen 64 kB Ringpuffer für empfangene Nachrichten. Die Empfangsregister beinhalten immer den Wert der ältesten Nachricht. Hat man eine Nachricht ausgelesen, teilt man dem Controller mit, dass er zur nächsten Nachricht weitergehen soll. Das geschieht durch das Setzen eines Bits im Command Register. Dort kann man auch das Senden einer Nachricht, die man zuvor in die Senderegister geschrieben hat, auslösen. Falls einige Interrupts maskiert sind oder man generell keine Interrupts behandeln möchte oder kann, bietet das Interrupt Register die Möglichkeit, den Controller zu pollen. Zu guter letzt gibt es noch das Status Register, das Informationen über Fehlerereignisse und den Zustand der Sende- und Empfangspuffer enthält. Um den Controller konfigurieren zu können, muss er im Reset Modus sein. Dazu zieht man entweder die / RST Leitung auf Masse oder setzt das erste Bit im Control Register auf 1. In diesem Zustand kann man u.a. die Empfangsfilter und die Baudrate einstellen.

[1] *http://www.cia-can.de*
[2] *http://semiconductors.philips.com/pip/SJA1000.html*

Der CCC startet die Kampagne zum Boykott der Musikindustrie

von Lars Weiler <pylon@ccc.de>

Die Ende März 2003 vom Bundesverband Phono / der IFPI [1] herausgegebene Pressemitteilung in der Nutzer von Tauschbörsen (P2P-Netze) als Ursache für den abnehmenden Umsatz bei CD-Verkäufen verantwortlich gemacht werden, veranlasste den CCC zu einem Boykottaufruf gegen den Kauf von Produkten der Musikindustrie.

So werden seit dem Frühjahr Tauschbörsennutzer immer wieder durch Pressemitteilungen der Musik- und Filmindustrie als auch medienstarken Verhaftungen und Gerichtsprozessen eingeschüchtert. Dabei werden auf geschickte Weise P2P-Netze als die Wurzel des Umsatzrückgangs kriminalisiert. Denn Schadensersatzanforderungen werden in Deutschland nicht durchsetzbar sein. Wie eine solche Einschüchterungskampagne aussieht, vermitteln die Plakate und Videos der "Gesellschaft zur Verfolgung von Urheberrechtsverletzungen" (GVU) [2], die viele sicherlich schon im Kinovorspann gesehen haben.

Zur Verfolgung der Interessen der Musikindustrie – worunter die "Big Five" Labels Universal, Sony, Warner Bros., BMG und EMI zu verstehen sind – werden die Schranken des Urheberrechts und seine damit verbundenen Verwertungsrechte so ausgelegt, dass die Privatkopie aufs Schärfste kriminalisiert wird. Denn die private Kopie eines Werkes ist eine Ausprägung der Informationsfreiheit, also ein Grundrecht.

Diese großen Labels geben maßgeblich vor, über welche Kanäle ihre Produkte angeboten werden. Derzeit sind es nahezu ausschließlich die digitalen Medien CD und DVD. Aufgrund der Speicherung von Film und Musik in Bits und Bytes können hiervon Kopien ohne Qualitätsverlust angefertigt werden. Noch ein paar Jahre zuvor war bei der Audiokassette die Klangqualität nach ein paar Kopien miserabel.

Der moderne Urheberschutz

Doch die Anfertigung von "perfekten Kopien" ärgerte die Musikindustrie so sehr, dass sie sich immer neue Möglichkeiten einfallen ließ, um die Pfründe wahren zu können. Kommerzielle Video-DVDs wurden von Beginn an mit Ländercodes und CSS (content scrambling system) [3] versehen, dessen Umgehung unter Strafe gestellt wurde. Nachdem immer mehr CD-Rohlinge, die natürlich nur zur Kopie von Audio-CDs verwendet werden, über den Ladentisch gingen, zogen die großen Labels nach und verpassten der CD eine Art "Kratzspur". Diese soll "sensiblere" CD-Lesegeräte wie sie in Computern verwendet werden so weit irritieren, dass die CD nicht abgespielt wird. Dummerweise sind solche CD-Lesegeräte auch in Fahrzeugen eingebaut, die ein Navigationsgerät besitzen. Warner Bros. beschreibt dieses Problem auch auf seinen Webseiten [4]:

"Probleme gibt es bei den neuen, sogenannten CD KFZ Playern von Siemens (z.B. Audi A4). Bei diesen Geräten handelt es sich um keine CD Player dem herkömmlichen Sinn nach, sondern in Wirklichkeit um PC ROM Laufwerke, welche die Software Funktionalität für das Navigationssystem besitzen. CDs ohne Kopierschutz sind abspielbar, welche mit Kopierschutz allerdings nicht, da ein Laufwerk Typ antizipiert wird, welches ungeeignet ist."

Da inzwischen der Großteil der CDs nur noch mit Kopierschutz erhältlich ist, kann der moderne Autofahrer diese CDs entweder nicht hören oder muss den Kopierschutz mittels geeigneter Software auf dem heimischen PC umgehen und sich die CD auf eine selbst gebrannte ohne Kopierschutz überspielen. Im neuen Urheberschutzgesetz vom 13. September 2003 ist diese Umgehung jedoch verboten [5], auch wenn weiterhin das Recht auf die Privatkopie eingeräumt wird:

"Wirksame technische Maßnahmen zum Schutz eines nach diesem Gesetz geschützten Werkes oder eines anderen nach diesem Gesetz geschützten Schutzgegenstandes dürfen ohne Zustimmung des Rechtsinhabers nicht umgangen werden, [...]" (Urhg, §95a, Abs. 1)

Und das, obwohl es GEMA-Abgaben auf CD-Rohlinge und Brenner gibt. Auch die Entwicklung des Kopierschutzes muss irgendwo her finanziert worden sein – klar, vom Musikliebhaber durch seine CD-Käufe. Und nun kann er diese nicht mehr am PC oder im Auto hören, geschweige denn auf leichte, transportable MP3-Player überspielen, um ruckelfreien Musikgenuss beim Joggen zu erleben. Nicht zu vergessen, dass durch die CD-Käufe die Klagewellen gegen Personen, die Musik kopiert haben, finanziert werden. Wer jetzt noch bei den "Big Five" Musik kauft, soll sich nicht über die Entwicklung der letzten Jahre beklagen.

Neues "Einkaufserlebnis" Tauschbörse

Doch nicht nur aus den bisher genannten Gründen sind Tauschbörsen so beliebt. Aus unserer Erfahrung sind mehrere Punkte zu nennen, weshalb CDs nicht über die Ladentheke gehen, sondern im heimischen Wohnzimmer gesammelt und zusammengestellt werden.

Einerseits ist die immense Auswahl ein wichtiges Kriterium. So gibt es viele Musikstücke, die im heimischen Plattenladen nicht mehr erhältlich oder so speziell sind, dass das Aufsuchen eines entsprechenden Ladens immens Zeit in Anspruch nimmt. Einfacher lässt es sich natürlich vom Wohnzimmer aus machen.

Nicht zu vergessen, dass Tauschbörsen nicht an Öffnungszeiten gebunden sind. Beispielsweise können noch während einer Party am Samstagabend die richtigen Tracks runter geladen werden, damit die Stimmung keinen Abbruch gewinnt.

Natürlich spielt auch der Preis eine große Rolle. Welcher von der Musikindustrie hauptsächlich angesprochene Jugendliche mag schon 17€ von seinem Taschengeld für eine CD ausgeben, auf der die Hälfte der Tracks nur ein Mal gehört wird? Evergreens zu produzieren scheint immer schwieriger geworden zu sein und vielmals vergreifen sich aktuelle Künstler an den Vorgaben ihrer alten Idole.

Auch, dass auf diese Weise CDs in Ruhe zur Probe angehört werden können, wird oft unterschlagen. Sehr viele Tauschbörsennutzer geben an, dass sie sich doch noch eine CD gekauft haben, wenn die Auswahl der Titel gestimmt hat. Auf der anderen Seite wird auch vieles wieder gelöscht, was dem eigenen Geschmack nicht entspricht.

Anhand dieser Argumente ist es mehr als fraglich, weshalb die Musikindustrie den Gang ins Internet verschlafen hat. Ein adäquates Verkaufsmodell, schon vor Jahren gestartet, hätte heute zu nicht solch großen Klagen geführt. Die aktuelle Entwicklung ist schließlich nur eine Folge der Nutzung moderner Medien in der Gesellschaft, die einfach nicht von der Industrie angeboten wurde.

Aufruf zum Boykott

Da der CCC die hausgemachten Klagerufe der Musikindustrie nicht weiter hinnehmen wollte, riefen wir am 30. März zum Boykott auf:

"Mit dem Klagen der Musikindustrie muss nun endlich Schluss sein! Der CCC fordert deshalb auf, die Musikindustrie dort zu treffen, wo sie am verwundbarsten ist. Entziehen wir ihnen den Umsatz! Dieser kann dann nicht mehr dazu verwendet werden, in großen Anzeigenserien die Kunden zu diffamieren."

Unterstützern des Boykotts boten wir Banner an, die auf diversen Webseiten und in ein paar Printmedien zu finden sind. Zusätzlich riefen wir zu Erstellung eigener Banner auf, um dadurch seinen Missmut Ausdruck zu verleihen.

Hinter den Kulissen

Dieser recht populistische Boykottaufruf bescherte uns sehr viel Resonanz. So war die Anzahl der aufgerufenen Seiten am 30. März um das zehnfache gestiegen. Trotz der zu Beginn noch kleinen Anzahl von sechs Bannern ist das Volumen auf 3 GByte an einem Tag hochgeschnellt. Die Webseiten des CCC waren am Nachmittag des 30. März, als unser Boykottaufruf durch die Online-Medien ging, nicht mehr zu erreichen und unsere Administratoren hatten alle Hände voll zu tun, die Last auf einen weiteren Server zu verteilen.

Allein am ersten Tag erhielten wir 70 unterstützende Zuschriften via mail@ccc.de, was stark an die Belastungsgrenze unseres Teams für öffentliche Anfragen ging; dennoch konnten wir alle beantworten. Inzwischen (Ende Mai) sind wir bei etwa 250 Reaktionen, von denen mehr als die Hälfte Banner sind. Die Zahl der verborgenen Unterstützer ist sicherlich noch um einiges größer.

Auf unserer Banner-Seite [6] stellen wir 60 gute und interessante Banner dar, die uns erreicht haben. Weitere Zuschriften nehmen wir gern unter *mail@ccc.de* entgegen.

Ein Gesprächsangebot von Seiten der Musikindustrie blieb leider aus. Sehr gerne hätten wir eine Stellungnahme zu den aufgeführten Gründen gehört.

Wie wird die Ode enden?

Anhand unserer erhaltenen Resonanz scheinen einige Befürworter des Boykott diesen als Freischein zur Nutzung von P2P-Netzen angesehen zu haben. Von daher nochmals der Hinweis von unserer Seite: P2P-Netze befriedigen die Wünsche der Kunden, jedoch stellen sie ein rechtliches Problem dar, wenn urhebergeschützte Werke darüber verbreitet werden.

Vielmehr ist zu wünschen, dass die Regierung ihre Gesetzesänderungen zur Privatkopie überdenkt, sodass diese in vollem Umfang weiterhin möglich ist. Auch der Musikindustrie möchten wir zu bedenken geben, ob aufgrund ihres Handelns Kinder hinter Gitter landen, die "nur mal" dieses zur Entwicklung des Charakters wichtige Allgemeingut Musik aus dem Internet geladen oder mit Freunden getauscht haben – anstatt einen Diebstahl im Plattenladen zu begehen.

Glücklicherweise gibt es neben den "Big Five" etliche kleine, unabhängige Labels (Indie-Labels), die viele gute Musik auch frei anbieten. Bleibt zu hoffen, dass von ihnen gelernt wird.

Zum Schluss möchten wir auf die Worte des Komikers Dirk Bach bei der diesjährigen Echo-Verleihung verweisen, die er mit Blick auf das minderwertige Musikangebot der Veranstaltung an die Musikindustrie richtete: "Und ihr wundert euch, dass es euch schlecht geht?"

[1] *http://www.ifpi.de/news/news-380.htm*
[2] *http://www.hartabergerecht.de/index5255.html?id=9*
[3] "DVD-Software", Datenschleuder #070, S. 4
[4] *http://www.warnermusic.de/main.jsp?sid=&page_type=comp_contact&area=P#m107590*
[5] *http://bundesrecht.juris.de/bundesrecht/urhg/index.html*
[6] *http://www.ccc.de/campaigns/music/*

Der Kampf um die Privatkopie

von wetterfrosch <wetterminister@weltregierung.de>

Musik im Netz ist schnell und preiswert - und der Musikindustrie ein Dorn im Auge. Über den Angriff der Musikwirtschaft, die Mittel, digitalisierte Kultur zu vergüten und die Retter der Privatkopie.

Seit Null und Eins ist der Inhalt vom physikalischen Medium gelöst. Mit CDs und dem Internet können praktisch umsonst Musik, Film und Text kopiert werden. Wo Erreichbarkeit und Vielfalt zunehmen, sinken Aufwand und Zeit. Künstler brauchen kein großes Startkapital oder Knebelverträge mehr, um an die Öffentlichkeit zu treten.

Doch wie kann die Allgemeinheit an Kultur teilhaben und gleichzeitig der Künstler genug Geld verdienen? Diese Frage wird am lautesten von der Musikwirtschaft gestellt, die sich selbst durch die neuen Medien noch mehr in Gefahr sieht, als ihre Musiker.

Der Angriff

Nachdem sich ab 1998 Filesharingnetzwerke, allen voran Napster, etablierten, klagte die Musikwirtschaft gegen die Betreiber solcher Netze. Ohne Erfolg. Denn ähnlich wie eine Post sind Filesharingbetreiber nicht für die transportierten Inhalte haftbar.

In den USA wandte sich die Record Industry Association of America (RIAA) dann direkt an einzelne User. Dabei reichte sie auch Klagen gegen 12jährige Kinder und Großmütter ein, die in ihrem Leben keinen Computer benutzt haben. Auf bis zu 150 000 Dollar pro angebotenem Song können heute Filesharinguser drüben verklagt werden.

Parallel versucht die Wirtschaft durch immer neue Kopierschutzmechanismen Schaden zu begrenzen. Diese verhindern aber auch Kopien für den eigenen privaten Gebrauch und machen das Abspielen auf einigen Geräten sogar unmöglich. Nach einer neuen EU-Richtline, die vergangenen Herbst hier umgesetzt wurde, ist das Umgehen von "wirksamen technischen Schutzmassnahmen" verboten. Ungeklärt ist, wie "wirksam" ein Kopierschutz ist, wenn er umgehbar ist. Gleichzeitig bleibt das Recht auf Privatkopie erhalten und steht somit im Widerspruch zu dem neuen Gesetz.

Im April reichte erstmals der deutsche Phonoverband (nationale Vertretung der IFPI) Klagen gegen Filesharinguser ein - "zur Abschreckung" - wie es heisst. Im ersten Urteil vom 8. Juni wurde ein 23jähriger Auszubildender für das Anbieten von MP3-Dateien zu 8500 Euro Strafe und Schadensersatz verurteilt. Kurz vor Beginn der Klagewelle startete die Musikindustrie "Phonoline", das erste Angebot, sich in Deutschland legal Musik herunterladen zu können. Abgesehen von den unhandlichen und kopiergeschützten Songs, die sich nicht einmal unter Linux abspielen lassen, den hohen Preisen und einer Auswahl, die grade die Hälfte der "Top 10" abdeckt, konnte sich die Musikindustrie nicht mit der GEMA über die Vergütungshöhe der Musiker einigen. Wo die Verwertungsgesellschaft ihre üblichen 10% vom Händlerpreis haben will, bietet die Industrie knapp die Hälfte.

Die zweite Novellierung des Urheberrechts in diesem Jahr soll nun Klarheit über die Privatkopie im Netz schaffen. Anlässlich der Popkomm, die erstmals in Berlin stattfindet, lädt der Bundestagsausschuss für Kultur zu einer Anhörung über die Zukunft der Musik im Internet ein. Der Aus- oder der Abbau der Privatkopie steht zur Debatte.

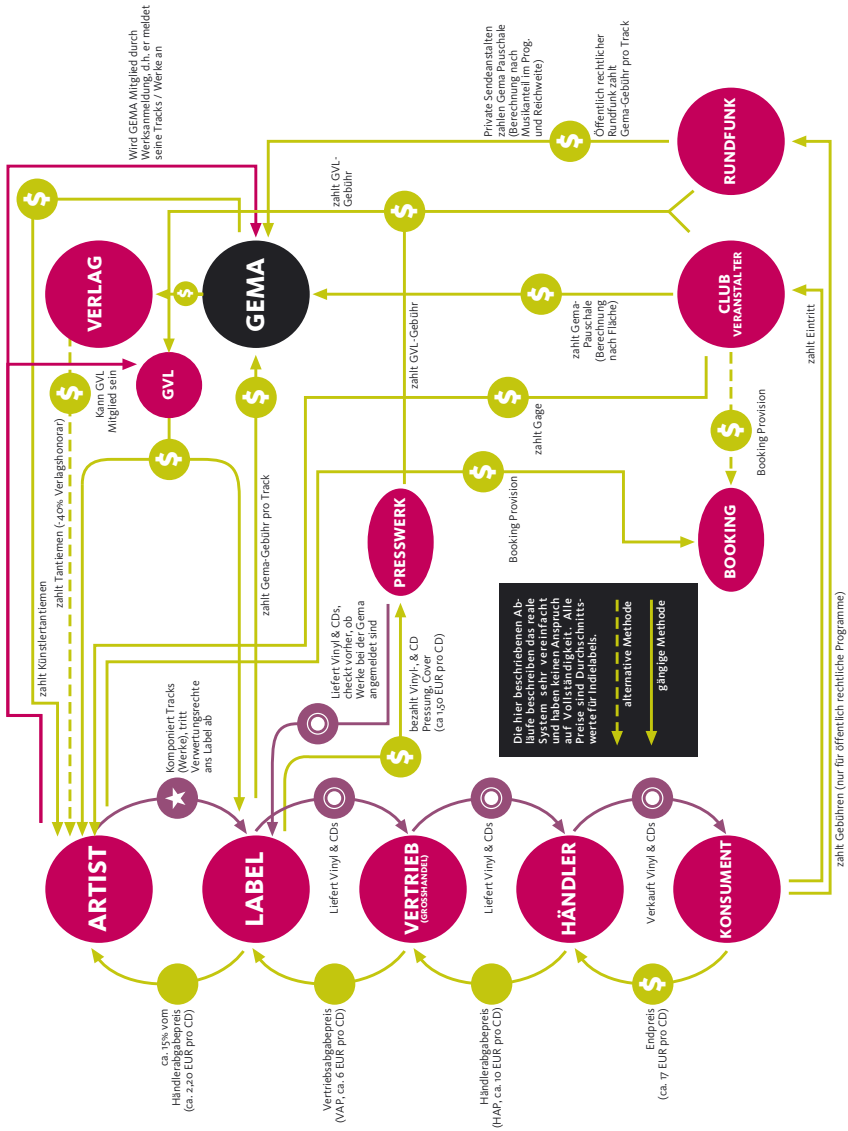
Die Mittel

DRM

Die Musikindustrie will das bisherige Vertriebsmodell aus der "analogen Welt" möglichst exakt in die digitale übernehmen: Man bezahlt als Verbraucher "pro Song" oder "pro Album" seine persönliche Kopie. Diese Kopie darf der Hörer nicht weiterkopieren. Um das sicherzustellen, wird sie mit einem Kopierschutz und einem individuellen "Wasserzeichen" versehen. Falls ein Musikkäufer den Schutz umgeht, kann er durch das Wasserzeichen entlarvt werden. "Digital Rights Management" heisst die Lösung der Musikindustrie. Mit ihr verbunden ist ein gewaltiges Datenaufkommen von persönlichen Informationen der immer gläserner werdenden Musikfreunde. Die Wirksamkeit der Schutzmassnahmen ist angesichts der vielfältigen Möglichkeiten mit Daten umzugehen und sie zu verschlüsseln stark anzuzweifeln.

Streetperformer Protocol

Das Streetperformer Protocol bietet Künstlern die Möglichkeit ihre Werke für die Allgemeinheit "freikaufen" zu lassen. Ein Musiker bietet beispielsweise Ausschnitte seines nächsten Songs an und verlangt einen Preis, ab dem das Werk unter eine freie Lizenz, wie den Creative Commons, veröffentlicht wird. Seine Fans sind nun aufgerufen, für die Veröffentlichung dieses Songs gemeinsam zu bezahlen. Interessant wird dieses Modell, wenn man es sich in Verbindung mit einer Pauschalabgabe für den Künstler vorstellt.



Pauschalabgabe

Das Recht auf Privatkopie ist Teil einer Lösung, die vor vierzig Jahren anlässlich eines ganz ähnlichen Problems gefunden wurde. Als Kassetten auf den Markt kamen, konnte plötzlich jeder Musikkäufer seine Musik kopieren und weitergeben. Da eine Kontrolle dieser privaten Kopien nicht möglich ist, wurde auf Leermedien eine Pauschalabgabe eingeführt. Diese wird über die Verwertungsgesellschaften an die Künstler ausgezahlt. Heute gibt es eine solche Abgabe auf CD-Rohlinge, Fotokopierer und Brenner. Durch eine Pauschalabgabe auf Internetzugänge wäre die Privatkopie im Netz legal und das "Filesharingproblem" gelöst. Um Internetnutzer nicht unverhältnismäßig zur Kasse zu bitten sind unterschiedliche Abgabenhöhen, je nach Umfang des Anschlusses, in der Diskussion. Man ist der Ansicht, dass eine Online-Pauschalabgabe durch anonymisierte Statistiken und Votings wesentlich genauer aufschlüsselbar ist, als die bisherigen Pauschalvergütungen.

Die Verteidiger

privatkopie.net

Zahlreiche deutschsprachige Organisationen, wie der FoeBuD, der CCC und die Grüne Jugend, schlossen sich vor zwei Jahren zur Initaive "Rettet die Privatkopie" zusammen. Sie veranstaltete bereits zur ersten Novelle des Urheberrechts eine alternative Anhörung. Die Petition zur Rettung der Privatkopie im Internet wurde bereits von über 46.000 Menschen unterzeichnet. Auf der Website finden sich neben vielen Hintergrundtexten auch laufend aktuelle Nachrichten zum Thema.

Das **Recht auf Privatkopie** *erlaubt jedem Bürger die "Vervielfältigungen zum privaten und sonstigen eigenen Gebrauch" (§53, UrhG) von urheberrechtlich geschützten Werken. Die Kontrolle privater Kopien ist, um die Privatsphären der Bürger unverletzt zu lassen, nicht erlaubt und wäre technisch auch nicht möglich.*

Im Gegenzug zu diesem Recht *werden die Künstler durch eine Pauschalabgabe auf Leermedien vergütet, die durch die Verwertungsgesellschaften ausgezahlt wird. Mit der Änderung des Urheberrechts im September 2003 steht das Recht auf Privatkopie im Widerspruch zu dem Verbot, "wirksame Kopierschutzmaßnahmen" (§95a, UrhG) zu umgehen.*

CCC

Der Chaos Computer Club reagierte auf die Klagen der deutschen Musikindustrie schnell mit einer eigenen Kampagne unter dem Motto "Informationsfreiheit ist kein Verbrechen". Der Club ruft zum Boycott der Musikindustrie auf, denn "mit den Erlösen aus den CD-Käufen bezahlt die Musikindustrie die Klagen gegen unsere Kinder". Zahlreiche Banner und Grafiken machen seitdem auf die Kampagne aufmerksam. (Dazu auch der Beitrag zum Boykott in diesem Heft)

Grüne Jugend

Etwas später, aber immernoch rechtzeitig zum aktuellen Europawahlkampf, reagierte die Grüne Jugend auf das Thema. Mit ihrer Kampagne "copy4freedom" positioniert sich der grüne Jugendverband zu den Themen Privatkopie und Freie Software. Er fordert die Ausdehnung der Privatkopie auf alle Kopien zu ungewerblichen Zwecken, um Filesharing zu legalisieren. Im Gegenzug soll durch eine Pauschalabgabe auf Internetzugänge die Vergütung der Künstler gesichert werden. DRM wird von der Grünen Jugend aus Datenschutzgründen abgelehnt - doch auch andere interessante Geschäftsmodelle für Musik stellt die Kampagne vor. Ferner möchte die Regierungsjugend Verwertungsgesellschaften reformieren, um sie transparenter und den Urhebern gegenüber offener zu machen.

Junge Union

Die Junge Union Hessen äußert sich seit der Novellierung des Urheberrechts kritisch zum neuen Gesetz. Sie macht mit ihrer Website "Faires Urheberrecht" auf den Widerspruch in der Gesetzesgebung aufmerksam, Kopierschutzmechanismen nicht umgehen, aber Privatkopien anfertigen zu dürfen. In dieser Hinsicht spricht sich die Unionsjugend für die Privatkopie aus, lehnt aber die Einführung einer weiteren Pauschalabgabe für das Internet ab.

attac

In ihrer Arbeitsgemeinschaft "Wissensallmende und Freier Informationsfluss" lehnen die Globalisierungskritiker die Kriminalisierung großer Teile der Bevölkerung ab und sehen auch in der Ausweitung des bestehenden Systems von Pauschalabgaben eine bessere Möglichkeit, Künstler zu entlohnen. Als Skeptiker des Neoliberalismus schwärmen die Attacies weiter von einer Welt, in der "Kultur direkt von der Gesellschaft bezahlt wird" und die "Unterhaltungsindustrie als Vermittlungsinstanz zwischen KünstlerInnen und der Öffentlichkeit überflüssig" wird. Solange sie vor der Popkomm wieder aufwachen, kann das noch was werden.

LINKS:

DRM

http://de.wikipedia.org/wiki/Digital_Rights_Management

Pauschalabgabe (Vorschlag der Grünen Jugend)

http://www.c4f.org/index.php?id=69

Streetperformer Protocol (deutsche Fassung)

http://www.schneier.com/paper-street-performer-german.pdf

Creative Commons

http://creativecommons.org/

CCC Kampagne "Boykott Musikindustrie"

http://www.ccc.de/campaigns/boycott-musicindustry

Grüne Jugend Kampagne "copy4freedom"

http://www.copy4freedom.de/

Junge Union Hessen: "Faires Urheberrecht"

http://www.faires-urheberrecht.de/

Attac-AG "Wissensallmende"

http://www.attac.de/wissensallmende/

Bildquelle Musikindustriekapitalismuskarte:

Erschienen in der Debug 83.

GPN3 in Karlsruhe

von neingeist <neingeist@entropia.de>

Am 22. und 23. Mai hat der Entropia e.V., die badische Inkarnation des globalen Chaos, zur dritten Gulaschprogrammiernacht eingeladen. Etwa 100 Leute trafen sich, um im Hackcenter zu coden, Vorträge zu verschiedenen Themen zu hören oder einfach nur mit anderen Chaoten aus dem Umkreis rumzuhängen.

In diesem Jahr stand - im Gegensatz zu einem kleinen Keller oder einer zu großen und leeren Fabrikhalle in den beiden vergangenen Jahren - eine sehr gute Location zur Verfügung. Das Karlsruher Studentenzentrum Z10 hatte uns übers Wochenende seine Räume zur Verfügung gestellt. Drei Stockwerke konnten wir für Hackcenter, Lockpicking, Chillout und zwei Vortragsreihen nutzen.

Mein persönliches Highlight war das ausgewogene Vortragsprogramm, beginnend bei robotlab.de, die bspw. Industrieroboter mit Platten scratchen, oder Portraits zeichnen lassen, über Daniel Kullas Lesung aus dem "Phrasenprüfer" bis hin zu Themen wie "Das Individuum in der virtuellen Gesellschaft". Es wurde also einiges ausserhalb des üblichen Technik-Kram geboten, wobei jedoch auch dieser Bereich nicht zu kurz kam: Es gab Vorträge zu WLANs, Exploit-Techniken, einen New-Technology-Battery-Guide, Kryptographie-Infos u.v.a.; unter anderem konnten dieses Jahr auch Universitätsmitarbeiter als Vortragende gewonnen werden. Wir hoffen, dass wir in diesem Bereich noch mehr ausbauen können, damit die ordentlichen und angehenden Akademiker auch etwas chaotische Unordnung erfahren dürfen. Da uns das Uni-RZ freundlicherweise Netz gespendet hat, hatten wir hier auch erstmals Möglichkeiten zum Austausch.

Die Lockpicker waren auch dieses Jahr wieder gut besucht, und konnten in einem eigens abgestellten Raum der Kunst des Schlossöffnens nachgehen und dem Publikum ihre Tricks zeigen.

Wir hoffen, in den nächsten Jahren wieder drei Tage Programm für die südlichen Chaoten anbieten zu können, so dass das richtige Hacker-Feeling – übernächtigt und nur durch Club-Mate intravenös am Leben gehalten – wieder aufkommen darf! Vielleicht auch wieder mit noch mehr Leuten, denn leider war uns dieses Jahr nur die halbe Besucherzahl – verglichen zur GPN2 – gegönnt.

Die Technik auf der GPN3

Erstmals stand dieses Jahr ein CMS (neudeutsch: Portal) zur Verfügung, das von den Jüngern des Common Lisps (Klammeraffen) speziell für uns angepasst wurde.

Vortragende konnten den Fahrplan frei verändern, jedem Chaoten stand ein persönliches Blog und das Wiki zur Verfügung, eine Möglichkeit, die gerne genutzt wurde. Weiter konnte man sein Infomaterial und MP3s für die zentrale Zwangsbeschallung hochladen und schöne Fotoalben für jedermann erzeugen.

Auch das Audio-Streaming auf der GPN3 hat relativ gut geklappt, über Multicast und über HTTP, gleich auch mitarchiviert. Die Qualität war berauschend gut, wenn man bedenkt, dass da nur ein 2,- EUR Mikrophon in der Ecke stand. Auch die Publikumsfragen sind glasklar zu verstehen gewesen. In Zukunft werden wir die Qualität evtl. künstlich senken, damit die Leute auch noch persönlich zum Vortrag erscheinen.

Entertainment

Zusätzlich umfasste das Portal-System auch Loony, den Tamagotchi-DJ, der entsprechend seiner Laune Musik aufgelegt hat: Hat man ihn nicht gefüttert, hat er trotzig französischen Hardcore-Hip-Hop gespielt, hat man ihn nicht sauber gemacht, schrie Loony mit japanischem Noise nach Zuwendung. Gab man ihm aber netterweise zu futtern und etwas Kaffee oder andere Genußmittel, durfte man sich an angenehmen Goa, Ska und Reggae erfreuen.

In einer krassen Codeaktion (sonntags um 04:00 Uhr morgens) wurde ein Tippgeschwindigkeitsschneckenrennen programmiert, das dann zu mehreren Stunden Spass geführt hat. Eine perfekte Abrundung des Entertainment-Programms nach dem alljährlichen Hacker-Jeopardy und der berauschenden Berieselung durch die beiden geladenen Chaos-DJs, die Loony Samstag nachts ersetzt haben.

Fallensteller und Budenzauberer

von Heinrich Dubel <info@chopper.in-berlin.de>

Auszüge anlässlich des Vortrags »Nazi Ufos and other realities« beim Chaos Commication Camp Altlandsberg-Paulshof 2003. Der gesamte Text ist zuerst erschienen in »Prüfstand 7 - Forschungen zum Geist der Rakete« (Hrg. Bramkamp/Fediana), Maas Media Berlin

Der industrialisierte Massenmord der Nazis sendet unwiderstehliche Schockwellen durch alles geschichtliche Denken. Seit Hitlers Tod im Führerbunker 1945 haben sich Historiker und Psychologen bemüht, die fürchterliche Abweichung zu verstehen, die das „Dritte Reich" in der Geschichte der Menschheit darstellt. Hitler ist 1945 nicht nur einer „gerechten Strafe" entgangen. Er, der Millionen und zuletzt sich selbst Richter und Henker ist, entzieht sich ebenfalls einer abschließenden Erklärung. Wir – ständige Zeugen seiner Tat – bleiben unerlöst zurück. Die Leere, die er hinterlässt, durchstrebt das expandierende Universum der Geschichte (Historie) als unbestimmte Zustände von Energie (Fantasmagnetia) und Materie (Dark Matter).

Es ist die Unbestimmtheit Hitlers wahrer Natur, die für manchen denn auch nicht mehr innerhalb eines Spektrum des menschlichen Wesens liegt, wie es etwa von der Verhaltensforschung definiert wird, sondern bereits irgendwo außerhalb, in einer Zone des radikal Bösen, von wo her dämonische Einflüsse die Geschichte stören. Die verblüffend einfache Volte, die das NS-UFO schlägt, wenn das Extrem die Felder „exakter Wissenschaft" transzendiert und in Gebieten der Theologie landet, ist die: eine ultimative Natur Hitlers, der Nazis und des Bösen kann nur von Gott verstanden werden. Wie man sehen wird, kann das allerdings auch ein Alien-Gott sein.

Die Vorstellung, dass die Nazis Weltraumschiffe bauten, die der Kontaktaufnahme und Rekrutierung übernatürlicher Kräfte dienen sollten, erscheint bizarr und mag erschrecken. Seriöse Wissenschaftler haben sie als Unfug der übelsten Sorte abgetan, besonders im Hinblick auf die unerhörten Exzesse der Nazis. So trivial die Idee anmutet, sie ist sicher der Grund für eine dämonisch zu nennende andauernde Faszination, der keine Studie zum gewöhnlichen Faschismus beikommen wird.

Die Götter der („ario")-europäischen Kultur befinden sich im „Kosmos", wohin der Weg der Techno-Wissenschaft führt, den der „faustisch gewordene deutsche Mensch" gern be- und ohne Unterlass auch überschreitet. Das NS-UFO kann per definitionem gar nichts anderes sein als eine Jenseitsflugmaschine, unterwegs entlang ungefährer KoordiNAZIon im absolut Andersartigen, eine Zeitmaschine, die neben dem Nazi-Okkultismus (Glauben der Nazis an das Okkulte und Übernatürliche) auch eine okkulte Kraft der Nazis transportiert (Okkultisten, Nazi-UFO-Adepten, Krypto-Historiker glauben, die Nazis kommandierten übernatürliche Kräfte, über die sie durch Kontakt mit transhumanen Intelligenzen verfügten).

Die vorpommersche Ostseeküste gehört zu den romantischsten Landschaften, die deutscher Geist als solche zu erkennen vermag.

Über Jahrhunderte wandelt die Küste ihre Gestalt. Beharrlich verrichten die Wassermassen der Baltischen See ihr Werk, brechen hier ab, glätten, überschwemmen, spülen dort an, schaffen neue Inseln, verbinden andere mit dem Festland. Wilde Steilküsten, das besondere Licht, das Zusammenfließen von Himmel und Meer, die Landschaft, die in ihrer Kargheit eigentümliche Würde ausstrahlt, sind wie geschaffen für eine romantisierende Innerlichkeit, und inspirieren ganze Malergenerationen zur Darstellung des Naturschönen.

Oberforstmeister Bernhard von Bülow sorgt 1820 für eine touristische Erschließung Usedoms. Zu niedlichen

Bei dem in der Aprilausgabe 1972 der Werkszeitschrift der Vereinigten Flugtechnischen Werke-Fokker GmbH, Bremen, veröffentlichte Beitrag „Unbekannte Flugscheiben bei VFW-Fokker entdeckt" handelte es sich um einen Ulk, die vorgestellte „Geheimwaffe" ein einfaches Modell, das aus zwei zusammengeklebten Kunststoffmanschetten für elektrische Stecker, drei Kugelschreiber-Fahrwerksbeinen, dem Sockel aus einem Plastik-Modellbaukasten sowie einigen Kleinteilen bestand. Nicht jedem Leser war das klar. Bis heute sind Fotos dieses Modells als handfester Beweis für die Existenz des Nazi-UFOs überall zu haben.

Sinnsuchers Schatzkästlein ist das bekanntlich reich gefüllte Reservoir „historischer" UFO-Erscheinungen, die als „Kunst" oder als Modell weitere osmotische Wirkungen erzielen. Zur Verbindung wirklicher deutscher Hochtechnologie mit neu- und alt-rechten Elementen sowie Nazi-UFOs siehe etwa http://home.snafu.de/bifff/Siemens.htm

Fischerdörfern gesellt sich entlang der feinen weißen Sandstrände mondäne Bäderarchitektur. Ausufernde Jugendstilphantasien zwischen Heringsdorf, Ahlbeck und Bansin bringen der Gegend den Beinamen „Riviera des Nordens", oder prosaischer auch den einer „Badewanne Berlins". Kaiser und Konsorten lustwandeln im Scheine wilhelminischer Pracht und traditionell treibhaus-schwülen Pomps. 1923 wird die erste Freibadeerlaubnis erteilt. Wo man zuvor aus dem Badekarren direkt in die Ostsee steigen musste, ist es den Badegästen fortan erlaubt, in Badekleidung am Strand herumzugehen. Die gute alte Zeit. Intellektuelle Elite fällt zuhauf ein: Thomas Mann, Joachim Ringelnatz, George Grosz, Carl Zuckmayer, Bertholt Brecht, Erich Mühsam, Gottfried Benn, Franz Kafka, Sigmund Freud, Albert Einstein, Max Reinhardt, Heinrich George, Gustav Gründgens, Ernst Barlach, Gerhart Hauptmann, Hans Fallada. „Nirgends ist man so jung, so froh und so frei", schwärmt Asta Nielsen 1933. Die aufstrebenden Sterne der UFA sehen das genauso.

Peenemünde, am westlichen Zipfel der Insel gelegen, da wo die Peene in die Ostsee fließt, hat es irgendwie nie geschafft, in die Reihe illustrer Seebäder aufzusteigen. Die schon in Zeiten der Schwedenkriege strategische Bedeutung dieses Fleckens hielt den Tourismus in äußersten Grenzen. Der erst 23jährige Physiker und Ingenieur Wernher von Braun befindet 1935 Peenemünde als geeignet für sein Raketenforschungszentrum. Die Gegend wird zum Sperrgebiet erklärt, die Peenemünder Bevölkerung größtenteils evakuiert. Zinnowitz, der nächstgelegene Badeort, wird dem Sperrgebiet zugeschlagen. Hier quartieren sich von Braun und seine Offiziere ein, darunter auch der stellvertretende Einsatzleiter der Baugruppe und Hauptmann der Reserve Heinrich Lübke, der etliche Jahre später zum Bundespräsidenten avancieren soll. Der Badespaß geht also, versehen mit einem Nazi-Präfix, weiter. Der Raketenspaß natürlich auch. Die Arbeit ist erfolgreich. Als am 3. Oktober 1942 ein Aggregat aus Peenemünde bis an die Grenze zwischen Weltall und Erdatmosphäre vorstößt, ist der stellare Raum in unmittelbare Reichweite gerückt. Die unschuldige Zeit des Probierens und Flanierens am malerischen Ostseestrande ist jedoch vorbei, die Saison der langen Bombennächte hat begonnen. Über die Dünen hinan lärmt Grammophonmusik wie eine wilde Jagd: „Ich flieg' zu dir, über das Meer, durch die Nacht. Und ich bin nicht allein ... "

Von Braun und seine Leute ziehen um an einen weniger exponierten Ort – nahe Nordhausen im Harz, wo die SS (Kammlers Büro Sonderelbe Jasmin) bereits Vorarbeit geleistet und ein KZ eingerichtet hat, dessen Insassen Bunker- und Stollenbau vorantreiben. Die durchschnittliche Überlebensdauer gewöhnlicher Häftlinge (entgegen solchen mit speziellen Qualifikationen) beträgt zehn Tage. Baldmöglichst beginnt das Sklavenheer mit der Serienfertigung der Vergeltungswaffe. Am Ende wird man feststellen, dass bei ihrer Produktion im Berg mehr als zehnmal soviele Menschen ums Leben gekommen sind als beim Einsatz der V2.

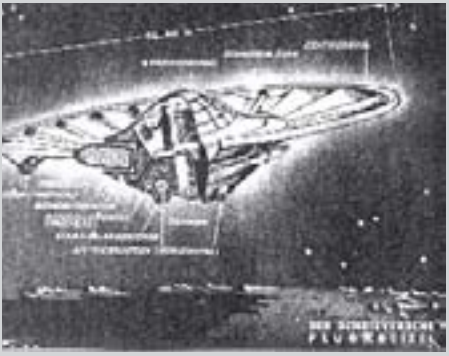
Es geht zwar auch immer um rein apparativ-technische Perfektion, aber eben nicht ausschließlich: „Die Arbeit war wie ein Rausch, ein Gebanntsein im Prozess, wie es nur der Forscher oder der Arzt bei einer Operation erleben." Das Zusammenwirken von Technik und Phantasie beschert von Braun, der neben der SS auch noch der Societät Jesu angehört, allerhöchste Gefühlszustände, wie sie die Alchimisten auf der Suche nach neuen, unerhörten, nie gesehenen Verbindungen erlebt haben mögen: „Ich bin eine leidenschaftliche Persönlichkeit." Auch Dornberger Walter als höherem Führer und Wehrmachtsgeneral ist die Vielfalt kosmo-arischer Herkunfts- und Destinationsprogrammatik nicht fremd. Er ist Anhänger eines vulgarisierten, auf Kasino-Geschwätz heruntergebrachten Nietzsche-Kultes: „Ich brauche Leben, den starken Atem des Ungewöhnlichen, die Sensation, Abenteuer." In Peenemünde liegt noch heute ein Stein (neben einer Raketenattrappe), der Dornberger „vom Herzen gefallen ist", als es endlich mal klappte mit einem Abschuss.

Es ist gelegentlich gesagt worden, dass die deutsche Mentalität das „Werden" höher bewerte als das „Sein". Dora Mittelbau als Bauhütte ist einer solchen Behauptung zuträglich. Dora Mittelbau ist von Anfang an mehr als eine unter Kriegsbedingungen ins deutsche Mittelgebirge gebunkerte Raketenfabrik. Dora Mittelbau ist Teil einer umfassenden Installation, die Gebärmutter und Grab zu nennen wäre. Ist der Stollen Gebärmutter der Rakete und Grab derer, die sie zusammenschrauben müssen, so ist der Weltenraum Gebärmutter zukünftiger und Grab vergangener arischer Zivilisation. Die Architekten des Projekts erheben den Anspruch, die Welt mit den Mitteln der Rakete noch einmal zu erschaffen, erlaubt diese doch Zugriff auf ein Terrain bizarrer, romantischer, unbegrenzt ausschweifender und jäh zu Gebilden eines Albtraums werdender Phantasie. Die Kosmotechnik verheißt Kompensation für den schmerzhaften Verlust der kaiserlichen Kolonien im WK1, die Bemühungen um Kolonisation des Weltenraumes sind solche um die Wiederherstellung des Reichskörpers, auch eingedenk männlich-sexueller Konnotationen von Kolonisation (eindringen, unterwerfen). Doch zwischen geschlechtlichen Eindeutigkeiten oszillierend ist die Rakete ein kraftvoller Phallus und eine starke Faust zugleich, die zu verheeren und eventuell die Saat der Herrenrasse über das Firmament zu verbreiten vermag (Ha-Ha-Handwerfen), zudem Lustsklavin, kraft menschlichen – ach was: männlichen Geistes gebändigte und gebündelte Triebenergie, die sich auf Kommando selbst verzehrt. Propulsion wird zum Synonym des Weiblichen, der Harz via Dora Mittelbau zum Mitternachtsberge, von woher die Schwarze Sonne das Pulsieren deutscher Seelen bestimmt. Eingang in die Hohlwelt ist er allemal. Wie es in Berlin so oft vom Bauwagen prangt: „Die Erde ist ein Lebewesen, und sie ist innen hohl." Natürlich ist der Schreiber jener Zeilen das einzige Lebewesen, dass tatsächlich innen hohl ist, bei besagtem Hohlraum mag es sich um den „menschlichen Geist" handeln, einen Raum infiniter und indefiniter Ausmaße, der bevölkert wird von allen möglichen Wesenheiten, wie man sie sich eben so vorzustellen vermag. In der Welt dieser Phantome ist nichts falsch und alles erlaubt.

Plakat der Digital-Anarcho-Hardcore-Combo Atari Teenage Riot von Mitte der 90er, dass meist schnell wieder abgerissen wurde. Die Natur des Nazi-UFO ist superscharf und präzise dargestellt.

Dämonische Leinwand: Nicht nur der heute gebräuchliche „Countdown" bei Raketenstarts stammt aus dem Fritz-Lang-Film „Die Frau im Mond", auch die Inspiration für dieses V2-Signet ist dort zu finden.

Wernher von Braun, suchend nach Erneuerung und Unsterblichkeit in den Tiefen der Schöpfung, ist nicht nur beach boy eines arischen Arkadien am Ostseestrande („da ging so einiges ..."), sondern Synerget einer hermaphroditen Na-Zivilisationsmaschine, die eine ideale ideengeschichtliche Kontinu-Identität erzeugt. Sein physikalisches Weltbild widerspricht seinem „Christentum" nicht – gegenüber der Herkunft steht die Zukunft. Scheinbar widersprüchliche „Welt"-Anschauungen – linear gedachte, apokalyptische versus zyklische universalis – sind versöhnt: „Sie gab sich hin, so ich ein Deutscher bin. Ich kam in ihr wie Lilien in einem offenen Grab." Das Echo des noch immer uneingelösten Versprechens hallt bis zu dieser Minute durch die Korridore unterirdischer Städte und über die eisfreien Ebenen des Neu-Schwabenlandes.



Orkut - Sehnt sich die Welt danach, sich selbst zu beschreiben?

von mario@koeln.ccc.de und sam@koeln.ccc.de

Das Semantische Web wird kommen. Das Internet hat einen Zustand erreicht, in dem seine Erfinder es für unbenutzbar halten. Der Anspruch des Webs, Wissen zu verknüpfen, kann von HTML nicht eingelöst werden. Auch wenn uns Techniken wie RDF und OWL zur Zeit bestenfalls als esoterisch erscheinen, ihre Nachfahren werden die Grundlage des neuen Webs sein.

Oder wie Cryx schreibt: "Welchen Sinn hat das bitte?"

Für den Datenschutz relevant ist die Tatsache, dass der Trend zu mehr Vernetzung auch vor persönlichen Daten nicht Halt machen wird. Im Gegenteil, Daten über Menschen und ihre Beziehungen sind der Bereich, in dem die neuen Techniken zur Erstellung von Wissensdomänen uns am meisten versprechen. Nehmen die neuen Protokolle erst einmal einen festen Platz in unserem Alltag ein, wird es soziale Auswirkungen geben.

Orkut ist nicht alleine, es gibt unzählige Experimente dieser Art: Friendster, Tribe.Net und Flickr, um nur drei zu nennen. Flickr ist weniger aufdringlich als das Orkut System. Einmal eingegebene Daten werden sehr viel besser und konsequenter verlinkt, Google Ads sorgen für die passende Werbung.

Das Wachstum dieser Netze wird von der Idee der Community getragen. Die damit einhergehende Veröffentlichung von persönlichen Daten, Vorlieben, sowie Beziehungen wird von den Benutzern in Kauf genommen.

Natürlich: Wer eine Webseite hat, gibt die Hälfte von Orkuts Daten schon im in Deutschland gesetzlich verordneten Impressum preis.

Zu gross ist der individuelle Informationsgewinn, der bei dieser Art des Datentausches entsteht, zu gering die Relevanz der veröffentlichten Daten. Gemeinschaft ist ja gerade der Verlust von Anonymität, während Anonymität auch immer ein Stückchen Einsamkeit fordert.

Die Anzahl der Organizer und Digitalkameras nimmt in meinem Umfeld rasant zu. Kleinstcomputer, die gebaut wurden, um Daten von Personen zu erfassen, zu speichern und wieder zugänglich zu machen.

Neben meinem Foto will man meine IM Daten haben, nicht nur um mich jederzeit zu erreichen, sondern auch um meine Präsenz abzufragen. Mailadresse, Webseite, PGP Schlüssel, Telefonnummer und verschiedene persönliche Daten wie Geburtsdatum und Anschrift. Dies sind alles weitere Daten, die andere über mich speichern wollen. Umgekehrt habe ich ein Interesse, diese Daten zu verbreiten. Leute sollen meine Webseite besuchen, damit sie gelesen wird, sie sollen mein Geburtsdatum wissen, damit sie mir gratulieren können. Meine Lieblingsband gebe ich, wenn ich gefragt werde, nach der ersten gemeinsamen Mate preis. Das alles, weil Informationen über mich, im Idealfall, meinen Status erhöhen und mir neue Ressourcen nutzbar machen.

Diese Daten sind jedoch noch relativ unbedeutend, ebenso ist ihre Qualität häufig fraglich. Die unfreiwilligeren Communities, Datenbanken von Krankenkassen, Providern, Supermärkten und Behörden speichern da schon interessantere Dinge. Diese Daten können wir nicht so einfach abfragen, verwalten und verändern. Dass der Zugriff strenger geregelt ist bedeutet allerdings noch nicht, dass er sich mit unseren Interessen deckt. So werden diese Daten erhoben und verknüpft ohne unsere Zustimmung. Ihre Einsicht und Veränderbarkeit entzieht sich unseren Möglichkeiten. Sie ermöglichen Institutionen die Abfrage und Bewertung unseres Lebens.

Dabei fehlt es an Standards, all diese Datenquellen abzugleichen. Das ist der Segen und der Fluch unseres Jahrzehnts.

Auf der einen Seite wollen wir diese Daten besitzen und verwalten, das vollständige Adressbuch mit PGP Key, Jabber Adresse und Anschrift unserer Freunde. Und nicht nur zuhause, sondern auch unterwegs, im Handy. Auf der anderen Seite wollen wir bestimmen, mit wem diese Daten geteilt werden und wer sie über uns speichern darf.

Bisher waren die Möglichkeiten, Informationen über eine Person zu erlangen, recht beschränkt. Abhängig vom Status des Fragenden und seiner Ressourcen, also z.B. Surfer, Headhunter oder Polizist, stehen mehr oder weniger Informationsquellen zur Verfügung. Die möglichen Quellen musste man alle einzeln abfragen. Ausgehend von der Mail Adresse etwa mit Google, Whois und PGP.

Will ich die Kontaktdaten von einer Bekanntschaft dauert es ein bis zwei Mate, bevor ich alle beisammen habe. Natürlich, Konzerne und Staaten haben es da etwas einfacher.

Community-Seiten und Techniken, die Beziehungen zwischen Daten herstellen, sind wirkungsvolle Mechanismen, um sie zu erheben und zu verbreiten. Aber Orkut schmeisst diese Daten eben nicht jedermann zum Frass vor. Orkut vertreibt sie in seinem eigenen Netz. Das ist auch genau der Punkt, die "Intention hinter Orkut". Besitz und Kontrolle des Marktes durch die grösste Benutzerbasis.

Das Google Prinzip birgt eine Reihe von Problemen, die im Artikel von Cryx schon angedeutet wurden. Die Daten sind in Besitz einer Firma und werden dort zentral gespeichert.

Vollen Zugriff haben nur die Orkut Administratoren, der Benutzer wird in einen HTML-Käfig eingeschlossen, aus dem auch mit automatisierten Skripten zur Abfrage der Seite nicht zu entkommen ist.

Die Rechtevergabe ist ungenau bis nicht vorhanden. Es ist nicht möglich Felder anzufragen und für eine einzelne Anfrage freizuschalten: "Hans Wurst möchte ihre Telefonnummer". Es existieren keine nutzbaren Vertrauensketten, ausser für Foren, die eigentlich nur das Usenet in schlecht nachbauen: "Karl A. wurde von ihren Freunden mit 500 Punkten bewertet und will ihre Homepage sehen".

Obwohl Orkut viele Geeks angelockt hat, scheint es das erklärte Ziel der Entwickler zu sein, lediglich eine weitere Dating-Plattform zu bauen. Die Idee von FOAF wurde unzureichend implementiert, das dargestellte soziale Netz gleicht lediglich einem Poesiealbum.

Die Code Basis von Orkut ist schlecht. Der Code befindet sich im Besitz von Google, wird niemals der Community zugute kommen und ist allem Anschein nach aus Visual Studio rausgefallen.

Orkut erinnert mich an die Anfänge des Instant Messagings. Fehlerhafte Software, rasch wachsende Benutzerzahlen und ein paar grosse Firmen die sich den Markt teilen.

Es hat Jahre gedauert, bis sich dort die besseren Konzepte, zum Beispiel Jabber, durchsetzen konnten. Und bis zum heutigen Tag werden wir die Altlasten nicht los. Die Zahl der ICQ Benutzer kann man nicht ignorieren. Ob Familie, Arbeit oder Wohnheim, alle haben ihre Adressen bei ICQ und ihre Anwesenheit dort unterstützt ein schlechtes Protokoll, eine böse Firma.

Nocheinmal ein wenig Utopie.

Ein Netz, in welches ich meine Daten gerne einspeisen würde und das auch mit meinem Handy Adressbuch sprechen darf, sollte folgende Punkte realisieren:

- Starke Verschlüsselung
- Dezentrale Speicherung und eine verteilte Serverstruktur
- Komplexe Rechtevergabe
- Offener Quelltext
- Offene Schnittstellen

Google, Amazon und Ebay sind meiner Ansicht nach die Firmen, die als erste solche Wissensstrukturen aufbauen werden. Viele andere Betriebe werden diese Techniken in ihren internen Netzen einsetzen. Wir wollen unsere Adressbücher nicht ihren Servern ausliefern, wir wollen Kontrolle darüber, wann sie uns welche Werbung anzeigen. Meine Hoffnung ist, dass sich dieses Mal frühzeitig ein Protokoll durchsetzt, das technisch in der Lage ist, die Anliegen des Datenschutzes und der informellen Selbstbestimmung umzusetzen.

Jabber und Freenet sind da vielleicht die grössten Hoffnungsträger.

Der kleine Angeber

von volker <volker.birk@ulm.ccc.de>

Es war einmal ein kleiner ANGEBER. Er war noch fast ein Kind, tagsüber ging er im Dorf in die Schule, abends machte er sich im Bett seine Gedanken. Niemand beachtete ihn, niemand mochte ihn, er wollte doch auch einmal als der große Held dastehen, und alle sollten ihn bewundern! Aber wie wollte er das anstellen? Seine Klassenkameraden lachten ja nur über ihn!

So kam es, dass der kleine ANGEBER eines Tages vor seinen Klassenkameraden in der Schule mal so richtig protzen wollte - er ist der SUPERHACKER! - sollten sie alle wissen. Es sollte nicht mehr so sein, dass alle nur über ihn lachen!

Da hatte der kleine Angeber eine Idee: wenn er auch so einen WURM PROGRAMMIEREN würde, der das BETRÜBSSYSTEM des Imperiums von GROSSHART besiegte, die Burg der tausend FENSTER, dann würden alle seine Klassenkameraden endlich denken, er sei der SUPERHACKER!

Nur: wie sollte er das machen? So richtig Ahnung hatte er ja leider nicht, wie so was geht.

Aber er hatte Glück: GROSSHART, weltweit angesehen als der Baron des Imperiums der WEICHWARE, hatte nämlich mit seinem BETRÜBSSYSTEM entsetzlich geschlampt.

GROSSHART spielte sich zwar als der Beschützer von Witwen und Waisen auf, doch in Wirklichkeit kümmerte er sich einen Dreck darum. Er konzentrierte sich ausschließlich auf das Einnehmen von Zöllen im Imperium und badete im güldenen Meer wie dereinst Dagobert, die Ente des Goldes. Entsprechend war die Burg von GROSSHART, das BETRÜBSSYSTEM des Imperiums, die alle Witwen und Waisen, alle Handwerker und Bauern beschützen sollte, löchrig wie ein schweizer Käse. Davon wusste das Volk natürlich nichts, das auf GROSSHART als Beschützer vertraute.

Es waren zwar feste Tore im BETRÜBSSYSTEM, von wehenden Fahnen kredenzt, aber wer genau hinsah, stellte schnell fest, dass viele der tausend FENSTER groß genug waren, um mit einem Pferd hindurch zu reiten. Die allermeisten FENSTER waren unbewacht, viele waren kaputt und vergessen. Hunderte und aberhunderte Geheimgänge verbanden GROSSHARTs Burg mit dem restlichen Imperium der WEICHWARE von GROSSHART.

Viele dieser Geheimgänge hatte GROSSHART früher selber genutzt, um schneller an die Stellen zu kommen, wo er den Wegzoll kassieren konnte. Die meisten davon hatte er inzwischen vergessen. Es kümmerte ihn auch nicht.

Damit aber alle ihren Zoll an GROSSHART bezahlten, stellte GROSSHART die Sicherheit des BETRÜBSSYSTEMS als unüberwindbar dar. Alleine mittels SCHWARZER-HACKER-MAGIE solle diese Burg zu knacken sein. Deshalb seien alle Leute, die in das BETRÜBSSYSTEM eindringen, der Hexerei schuldig! Dies lies er seine Herolde tagaus, tagein verkünden.

Das wussten nicht nur die HACKER der GILDE des CHAOS, das wussten alle HACKER landauf, landab, die mit der WEISSEN MAGIE DES HINSCHAUENS UND LOCH-SEHENS immer noch mehr Lücke, Geheimgang und Durchlass im BETRÜBSSYSTEM entdeckten, und versuchten, das Volk der WEICHWARE aufzuklären, wie unsicher das BETRÜBSSYSTEM von GROSSHART sei.

Wenn das Volk schon unbedingt in der Burg von GROSSHART bleiben möchte, weil er sie abends durch Gesangeskunst und Schau mit seinem OFFICE unterhielt, wenn das Volk sich nicht daran störte, wie unglaublich dreist GROSSHART Wegzoll verlangte, dann solle das Volk doch wenigstens erkennen, wie unsicher das BETRÜBSSYSTEM von GROSSHART ist, und die ADMINS, die Wächter des BETRÜBSSYSTEMS, anweisen, genau aufzupassen und jedes Fenster, jeden Geheimgang zu schließen, die die HACKER fanden.

Die HACKER verstanden nicht, warum die Bauern und Handwerker, die Witwen und Waisen unbedingt im BETRÜBSSYSTEM der tausend FENSTER bleiben wollten. Gut, GROSSHART machte seine Sache auf der Unterhaltungsseite wirklich gut, und verleitete das Volk perfekt. In Wahrheit kannte Baron GROSSHART sein Volk eben genau, und wusste, dass es viel lieber unter-

halten als verängstigt werden wollte. Und das nutzte Baron GROSSHART auf gerissene, ja geradezu genial zu nennende Art und Weise schamlos zu seinem Vorteil aus.

Aber direkt neben dem BETRÜBSSYSTEM standen die Burgen des BSD, und kaum ein paar Meilen weiter waren die Fahnen der Burg des PINGUINS zu sehen, alles Burgen, die keine tausend FENSTER hatten, wenige oder keine Geheimgänge, und die deshalb leicht zu verteidigen waren.

Deshalb hasste GROSSHART die HACKER. Sie erzählten dem Volk, wie unsicher das BETRÜBSSYSTEM war, und wiesen es sogar noch darauf hin, wo sichere Burgen standen, für die das Volk wesentlich weniger Zoll entrichten müsste und gar keinen Wegzoll.

Auch den HACKERN war Baron GROSSHART unheimlich. Sie hielten ihn für abgrundtief böse, und fürchteten, er sei nicht nur geldgierig, sondern auch der Abgesandte des Bösen selber.

Die ADMINS jedoch vertrauten, wie das andere Volk auch, auf die Sprüche der Herolde von GROSSHART; sie fühlten sich sicher. So erging es fast dem ganzen Volk.

Die Handwerker und Bauern erteilten den ADMINs immer mehr zusätzliche Aufgaben, sie mögen Holz holen, die Schweine füttern und auf die Kinder aufpassen, denn wozu waren sie sonst da?

Die ADMINS wurden faul und träge, und müde der immerwährenden Aufträge des anderen Volkes. Sie vernachlässigten träge ihre eigentliche Wächter-Aufgabe.

Deshalb machten die HACKER Listen mit den Löchern und Gängen, die sie in GROSSHARTs BETRÜBSSYSTEM fanden, und schlugen diese so an, dass sie jeder aus dem Volk, und besonders jeder ADMIN lesen konnte, auf dass diese Löcher besonders bewacht würden. Nur wenige ADMINS kamen dieser Aufforderung nach; die allermeisten waren viel zu träge geworden und vertrauten lieber den Sprüchen GROSSHARTs.

So kam es, dass der kleine ANGEBER Glück hatte. Wieder einmal fanden die HACKER Löcher. Wieder einmal schrieben sie diese Löcher an und informierten die ADMINS.

Die Löcher waren so peinlich, dass sogar GROSSHART einen Trupp PROGRAMMIERER schickte, um für das Loch einen FLICKEN zu programmieren. Diese taten, wie ihnen geheißen, nur wieder einmal waren die ADMINS zu träge, den FLICKEN überhaupt zur Kenntnis zu nehmen, geschweige denn anzubringen.

So blieb das öffentlich angeschriebene Loch trotzdem ohne FLICKEN, wie so viele andere auch.

Das nutzte der kleine ANGEBER. Auch er hatte sich in den Anfängen des PROGRAMMIERENS geübt, allein, er war halt noch nicht weiter als der Zauberlehrling mit

den Besen gekommen. Aber hierfür reichte es: er PROGRAMMIERTE einen WURM für das öffentliche Loch.

So konnte er es sich sparen, die WEISSE MAGIE des HINSCHAUENS und LOCH-SEHENS zu erlernen, seine Anfängerkenntnisse reichten aus!

Diesen WURM ließ er los. Dann erzählte er allen Klassenkameraden von seiner Großtat, sie sollten wissen, er war jetzt ein H4X0R! Er dachte nämlich, dass HACKER falsch geschrieben noch viel mehr Eindruck machen würde als richtig geschrieben.

Ob er wirklich einen WURM zum Jagen anderer WÜRMER PROGRAMMIEREN wollte, wie er hinterher behauptete, um sich vorm Schafott zu retten, darüber wird in dieser Geschichte nichts erzählt. Vielleicht wird das auch niemand jemals erfahren.

Der WURM war aber gar fürchterlich. Er drang durch das offene Loch ein, vervielfältigte sich, und breitete sich in der ganzen Burg aus, derweil der FLICKEN ungenutzt in einem Gang ganz in der Nähe lag.

Die ADMINS waren erschrocken: wie konnte es nur passieren, dass GeWÜRM sich im BETRÜBSSYSTEM breit machte? GROSSHART hatte doch gesagt, das könne nicht passieren! Da musste SCHWARZE -HACKER-MAGIE im Spiel sein!

Sie jagten und verfolgten den WURM, der sich immer mehr verbreitete und vervielfältigte, und kamen gar nicht mehr nach, ihn zu fangen.

Kaum hatten sie den WURM an einer Stelle im Griff, so tauchte er in einem anderen Flügel des BETRÜBSSYSTEMs wieder auf, wo die ADMINs immer noch schliefen oder dem Glücksspiel nachhingen.

So mischte der WURM das ganze BETRÜBSSYSTEM der tausend FENSTER auf.

Das Volk geriet immer mehr in helle Panik, der WURM wütete, alles ging zu Bruch, die ADMINS jagten hinterher.

Allein den ADMINS der REICHSPOST war die Situation zu peinlich; sie behaupteten, sie hätten den FLICKEN in ihrem Trakt montiert.

Allein um die absolute Sicherheit zu erzeugen, hätten sie selber versehentlich mit ihren Waffen und Schilden den ganzen Trakt verwüstet. So würde das Volk nicht so sauer auf sie sein, weil sie vergessen hatten, den FLICKEN anzubringen, dachten sie.

Von allen diesen Vorgängen hörte auch der König des großen REICHES, zu dem das Imperium des Barons GROSSHART gehörte. Er schickte seine BÜTTEL, um dem Baron gegen das schreckliche GeWÜRM beizustehen.

"Wer hat dieses GeWÜRM PROGRAMMIERT?" fragten sie jeden, der des Weges kam. Allein, der WURM selber verriet nichts, und die BÜTTEL, die die MAGIE des PROGRAMMIERENS gar nicht verstanden, erreichten mit ihren Fragen auch nichts. Sie waren völlig hilflos. Derweil jagten die ADMINS weiter hinter dem WURM her.

Nur Baron GROSSHART konnte hier noch helfen. Er hatte nämlich in der Voraussicht, dass seine Burg gegen GeWÜRM und auch alle anderen Gefahren gar nicht standhielt, ein Kopfgeld ausgesetzt: Derjenige, der ihm den PROGRAMMIERER eines WURMES bringe, derjenige sollte mit Gold überschüttet werden.

Das hörte einer der Klassenkameraden des kleinen ANGEBERS, sein Nebensitzer JUDAS. Natürlich hatte der kleine ANGEBER allen seinen Klassenkameraden von seiner Tat erzählt, er wollte ja endlich ein geachteter großer ANGEBER werden.

JUDAS wollte endlich auch einmal viel Gold haben. Das war seine Chance!

Er ging zu Baron GROSSHART, und zeigte mit dem Finger auf den kleinen ANGEBER, und sprach: "Der kleine ANGEBER war's, er hat den WURM programmiert! Das hat er mir selber gesagt!"

Baron GROSSHART lachte: jetzt hatte er wieder gewonnen!

Er führte die BÜTTEL zum kleinen ANGEBER und rief: "Verhaftet ihn! er ist der PROGRAMMIERER des WURMS, er ist der Hexerei schuldig!"

Da legten die BÜTTEL den kleinen ANGEBER in Ketten und schleiften ihn zum König des REICHES. Sie präsentierten dem König ihren Erfolg. Durch Herolde im ganzen REICH ließ der König verkünden: "Die BÜTTEL haben den Hexer gefasst! Die BÜTTEL haben den Hexer gefasst!". Zusammen mit Baron GROSSHART präsentierten sich die BÜTTEL als strahlende Sieger, und alle wurden für diese Großtat geehrt.

Da war das Volk wieder beruhigt.

Jetzt konnte das Volk wieder in Ruhe und Sicherheit leben, sobald die ADMINS irgendwann einmal mit dem WURM fertig geworden waren.

Baron GROSSHART und die BÜTTEL waren die strahlenden Sieger. Wieder einmal hatte die Gerechtigkeit gesiegt! Was täte das Volk nur ohne den führsorglichen Baron GROSSHART und die Kompetenz und den Einsatzwillen der BÜTTEL!

Der Gerechtigkeit wurde genüge getan, der Hexer wurde öffentlich angeklagt, verurteilt und schließlich verbrannt.

Und alle lebten glücklich und zufrieden bis zum nächsten WURM, nun ja, vielleicht auch solange bis irgend jemand aus dem Volk einmal auffallen möge, dass GROSSHART eigentlich kleinweich heisst...

21C3: The Usual Suspects

von 21c3@cccv.de

Zum gewohnten Termin am Jahresende steht die 21. Auflage des Congresses an. Unter dem Motto The Usual Suspects laden wir Menschen aus der ganzen Welt dazu ein, aktuelle technische Erkenntnisse, neue Aspekte der Forschung und gesellschaftspolitische Auswirkungen des Einsatzes moderner Technologie zu präsentieren und zu diskutieren. Drei Vortragsschienen an allen drei Tagen der Veranstaltung werden weit über 50 Vorträge und Workshops zu den unterschiedlichsten Themen bieten.

Eher ungewohnt beginnt die Organisation in diesem Jahr spürbar früher, auch um den Schwierigkeiten, die sich beim letzten Mal mit der Umstellung mit dem neuen Gebäude ergeben hatten, besser begegnen zu können.

Alles neu...

Zu den guten Nachrichten gehört, daß der Hackcenter-Bereich um gut 50% anwächst und sich die quälende Enge des letzten Jahres damit nicht wieder einstellen sollte. Das eher schlecht genutzte Erdgeschoss wird durch den in diesem Jahr wiederkehrenden Bereich Art & Beauty deutlich besser in den Congress integriert werden und weiteren Projekten Raum geben.

Wie immer erwarten wir über 2.500 Gäste aus aller Welt und wollen der Internationalität unseres Publikums auch durch eine entsprechende Internationalität unserer Referenten und Vorträge Rechnung tragen. Wie gehabt läuft die Congresskommunikation im Vorfeld zweisprachig und der Fahrplan wird nicht nur spürbar früher veröffentlicht werden, sondern auch verlässliche Informationen über den Inhalt und die Vortragssprache der Veranstaltungen geben.

Themenbereiche

Um das Congressprogramm übersichtlicher zu gestalten, teilen wir den Inhalt der Veranstaltungen in fünf Themenbereiche auf.

• Hacking • Science • Community • Society • Culture

Hacking deckt die klassischen technischen Disziplinen ab, die schon immer das Gesicht des Congresses geprägt haben: detaillierte Vorträge zu technischen Verfahren und Entwicklungen, Workshops zu Programmiertechniken und experimenteller Spaß am Gerät kommen hier zur Sprache.

Science umfasst Vorträge aus dem wissenschaftlichen Bereich: Grundlagen, aktueller Stand der Forschung in neuen und klassischen Bereichen.

Community addressiert aktive Gruppen der Szene an. Der Congress versucht unter anderem Entwicklergruppen anzuregen, ihre Konferenzen im Rahmen des Congresses abzuhalten oder interessante Projekte und Aktivistengruppen zur Vorstellung ihrer Projekte motivieren. Der Congress bietet auch Möglichkeiten zur Durchführung von Entwicklerkonferenzen. Wenn Ihr Interesse habt, Eure Entwicklergemeinde auf dem Congress zusammenzutrommeln, nehmt Kontakt mit uns auf, damit wir Euch zweitweise Räume für Besprechungen bereitstellen können.

Society umfasst Vorträge im Kontext aktueller gesellschaftspolitscher Themen. Softwarepatente, Copyright und ähnliche Brennpunkte stehen hier im Mittelpunkt.

Culture schließlich widmet sich erweiterten kulturellen Aspekten und der Erarbeitung der Metaebene. Hier sammelt sich das Lustige und leicht Verrückte, sowie das Besondere des Congressprogramms. Hier suchen wir Vorträge aus gedanklich verwandten, aber vielleicht nicht immer unmittelbar nahestehenden Kulturkreisen, auch in der Lage sind, eine Betrachtung der Hackerkultur von außen zu vermitteln.

Call for Papers

Der Call For Papers wird auf der Congress Website veröffentlicht. Jeder ist eingeladen, einen Vortrag einzubringen. Der Auswahlprozess startet im August 2004. Die Zusagen sollen nach Abschluß des Auswahlverfahrens zügig erfolgen, so dass unsere Referenten mit längeren Anfahrtswegen ihre Anreise und ihren Aufenthalt dieses Mal rechtzeitig planen können.

Mitmachen

Das 21C3 Public Wiki unter *http://21c3.ccc.de/* steht allen Teilnehmern des Congress offen. Hier könnt Ihr Eure Projekte auf dem Congress dokumentieren, Leute zum Mitmachen finden und Mitfahrgelegenheiten anbieten. Außerdem finden sich hier weitere Tips und Tricks zur Teilnahme am Congress, ein FAQ und sicherlich noch viele weitere hilfreiche Informationen, die wir jetzt noch gar nicht absehen können.

Das Congress-Orgateam sucht für die Vorbereitung des Congresses noch Mitstreiter. Wer Lust und Zeit hat, sich in den Monaten vor dem Congress - vor allem aber nicht zwingend in Berlin - einzubringen, sollten sich unter <21c3@cccv.de> melden.

21. Chaos Communication Congress -The European Hacker Conference

27/28/29 Dezember 2004
bcc - berliner congress center
Alexanderplatz, Berlin-Mitte

http://www.ccc.de/congress/2004/

Shortest Programming – Tipps und Tricks

von Markus Schaber <markus.schaber@ulm.ccc.de>

Eine beliebte sportliche Disziplin unter den Hackern ist es, das kürzestmögliche Programm für eine gegebene Aufgabe zu schreiben. Auch im CCC hat es schon solche Wettbewerbe gegeben (siehe auch http://ulm.ccc.de/shortest/). In diesem Artikel werden (anhand von Beispielen der Sprache C) ein paar der Tricks verraten, wie Hacker und Haeckse die letzten Bytes aus einem Programm quetschen kann. Allerdings wird nicht alles verraten – etwas "Hack Value" soll schon noch übrig bleiben...

Warnung: *Die hier gezeigten Methoden sind im allgemeinen das genaue Gegenteil von „gutem Programmierstil", und können unter Umständen von Arbeitgebern, Übungsaufgaben-Korrektoren, Open-Source-Projektleitern, Einstellungsprüfern und anderen, denen man seinen Quelltext zukommen lässt, mit anscheinend unerklärlichen Anfällen von Mißfallen bedacht werden.*

Leerraum minimieren

Betrachten wir mal das folgende Code-Fragment kritisch [1]:

```
1. /* Multiply our number with 23
2.  * We call this function before each new
      base-23 digit is read.
3. */
4. void multiply(void) {
5.     int ueber=0;
6.     int pos=0;
7.     int zwi=0;
8.     int alt;
9.     do { alt = f[pos];
10.         zwi = f[pos] * 23 + ueber;
11.        f[pos] = zwi % 11;
12.        ueber = zwi / 11;
13.        pos++;
14.    } while (pos < MAX);
15.
16.    if (ueber != 0) {
17.        printf("SHIFT OVERFLOW");
18.        exit(1);
19.     }
20. }
```

Natürlich sollten alle Bestandteile des Quelltextes, die den Compiler nicht interessieren, aus dem Programm entfernt werden. Dies sind zuallererst natürlich die Kommentare.

Ausserdem können Leerräume (Leerzeichen, Tab, Zeilenumbruch) optimiert werden: Jede Folge von mehr als einem Leerraum kann zu einem Leerraum zusammengekürzt werden. Als allererstes kommen also alle Spaces und Tabs am Zeilenende weg, ebenso wie die Einrückung am Zeilenanfang, und sonstige Ansammlungen von Leerzeichen – damit kommen wir auf folgenden Quelltext:

```
1.  void multiply(void) {
2.  int ueber=0;
3.  int pos=0;
4.  int zwi=0;
5.  int alt;
6.  do { alt = f[pos];
7.  zwi = f[pos] * 23 + ueber;
8.  f[pos] = zwi % 11;
9.  ueber = zwi / 11;
10. pos++;
11. } while (pos < MAX);
12. if (ueber != 0) {
13. printf("SHIFT OVERFLOW");
14. exit(1);
15. }
16. }
```

Aber auch innerhalb dieses Quelltextes gibt es noch einige überflüssige Leerräume, die man eliminieren kann – vereinfacht gesagt, an allen Stellen an denen vor oder [2] nach dem Leerraum kein Bezeichner und keine Zahl steht. An den Stellen, an denen aus syntaktischen Gründen ein Leerraum bleiben muss, setze ich gerne Zeilenumbrüche ein – das stört den Lesefluss, und das Programm sieht optisch länger aus, als es wirklich ist. Das Programm sieht dann wie folgt aus:

```
1. void
2. multiply(void){int
3. ueber=0;int
4. pos=0;int
5. zwi=0;int
6. alt;do{alt=f[pos];zwi=f[pos]*23+ueber;f[pos
]=zwi%11;ueber=zwi/11;pos++;}while(pos<MAX);if
(ueber!=0){printf("SHIFT OVERFLOW");exit(1);}}
```

Tipp: Damit AnfängerIn selbst noch die Übersicht über das Programm behält, kann man eine Kopie der schön formatierten, kommentierten Datei behalten und diese ab und an leerraumminimieren, um die Zielgrösse zu ermitteln. (Wer im WeltWeiten geWebe sucht, kann dazu evtl. sogar fertige Skripte finden – ein echter Geek macht das jedoch selbst!) Alternativ kann man auch die kurze Version bearbeiten und zum Übersichtsgewinn immer mal wieder eine Kopie durch ein entsprechendes Programm „schön" formatieren lassen. (Z. B. astyle, oder ein Editor, der automatische Code-Reformatierung unterstützt.) Mit der Zeit werden die Programme jedoch in der Regel so kurz, und man selbst so geübt, dass man ohne die "Langversion" auskommt.

Ausführlichkeit eliminieren:

Schauen wir uns den unteren Teil unserer Beispielfunktion an:

```
1. if (ueber != 0) {
2.     printf("SHIFT OVERFLOW");
3.     exit(1);
4. }
```

Die Fehlermeldung ist nur während der Entwicklung des Algorithmus interessant. Also kann der printf() Aufruf entfallen. Auch das "ueber != 0" kann in C verkürzt werden, das Programm sieht dann so aus:

```
1. if (ueber) {
2.     exit(1);
3. }
```

Die geschweiften Klammern sind hier natürlich ebenfalls überflüssig, da nur noch ein Statement enthalten ist:

```
1. if(ueber)
2.     exit(1);
```

Falls – wie im Falle des Wettbewerbs auf dem 20c3 und auch sonst sehr häufig der Fall, (im Zweifelsfall bei der Jury nachfragen) – garantiert ist, dass die Eingabe keine fehlerhaften Daten enthält und man sich sicher ist, dass der Algorithmus korrekt, sowie die Datengrössen richtig abgeschätzt sind, kann man auf diese Überprüfung sogar komplett verzichten.

Deklarationen optimieren

Betrachten wir nochmal einen Ausschnitt unseres Beispieles:

```
1. void multiply(void) {
2.     int ueber=0;
3.     int pos=0;
4.     int zwi=0;
5.     int alt;
6.     do { alt = f[pos];
7.     zwi = f[pos] * 23 + ueber;
```

Hier fällt auf, dass man die Deklarationen der lokalen Variablen gut zusammenfassen kann. Auch eine Initialisierung der Variable "zwi" ist, wenn man sich den Quelltext genau anschaut, überflüssig: Der erste Zugriff auf die Variable ist schreibend.

Der Ausschnitt sieht dann wie folgt aus:

```
1. void multiply(void) {
2.     int ueber=0, pos=0, zwi, alt;
3.     do { alt = f[pos];
4.     zwi = f[pos] * 23 + ueber;
```

Und schon haben wir dreimal "int" sowie drei zur Trennung notwendige Leerräume eingespart. Wenn man eine Umgebung hat, die einem die Initialisierung des Speichers auf 0 garantiert – was z. B. bei Java der Fall ist – kann man auch ueber und pos uninitialisiert lassen.

Es empfiehlt sich auch, sofern vom Algorithmus her möglich, für alle ganzzahligen Variablen den Typ "int" zu verwenden (anstatt short, char, long etc.) - einfach deshalb, weil das Schlüsselwort "int" mit drei Zeichen der kürzeste Bezeichner ist, den ich in einer Deklaration verwenden kann. Aus diesem Grunde verwendet man auch vorzeichenlose Variablen nur da, wo es absolut umunganglich ist – ein "unsigned" inklusive anschliessendem Leerraum sind einfach 9 überflüssige Bytes.

Funktionen zusammenfassen:

Wie es der Zufall will, gibt es in unserem Beispiel-Programm neben der Multiply-Funktion auch eine add-Funktion, deren Code (bereits um den Debug-Output verringert) der Multiply-Funktion stark ähnelt:

```
1. void add(int newdigit) {
2.     int pos=0;
3.     int zwi=0;
4.     int ueber = newdigit;
5.     do {
6.         zwi = f[pos] + ueber;
7.         f[pos] = zwi % 11;
8.         ueber = zwi / 11;
9.         pos++;
10.    } while (ueber != 0);
11. }
```

Diese beiden Funktionen lassen sich wunderbar zusammenfassen, und nebenbei noch die Variable "newdigit" sowie ein Statement eliminieren und die Deklaration optimieren:

```
1. void mad(int newdigit, int fact) {
2.     int pos=0, zwi, ueber=newdigit;
3.     do {
4.         zwi = f[pos] * fact + ueber;
5.         f[pos++] = zwi % 11;
6.         ueber = zwi / 11;
7.         pos++;
8.     } while (pos<MAX);
9. }
```

Natürlich muss man im Quelltext alle Aufrufe der beiden alten Funktionen auf die neue anpassen – alternativ kann man auch mit Makros arbeiten:

```
1. #define add(d) mad(d,1)
2. #define multiply() mad(0,23)
```

Ob sich die beiden Kompatibilitäts-Makros wirklich lohnen, hängt von der Anzahl der Aufrufe ab. Im Falle von add braucht das #define 23 Zeichen, und pro Aufruf spare ich zwei Zeichen ein. Das bedeutet, dass sich das Makro ab 12 Verwendungsstellen lohnt. Im anderen Falle ist der direkte Aufruf sogar ein Zeichen kürzer als der Aufruf des Makros – man lässt also die Zeile 2 weg, und macht stattdessen einmal suchen/ersetzen im Editor.

Funktionen, die im gesamten Programm nur einmal aufgerufen werden, werden natürlich noch durch Inline-Code ersetzt. Unter Umständen lohnt sich auch eine Code-Umstellung, so dass diese Funktion nur noch an einer Stelle gebraucht wird. Ausserdem sollte man die Funktionen natürlich so umsortieren, dass möglichst wenig Vorwärts-Deklarationen notwendig sind.

Code-Optimierungen:

Wer bei der obigen Funktion mad() genau hinsieht, sieht, dass die Variablen zwi und ueber immer abwechselnd mit einem bedeutsamen Wert belegt sind – man kann also eine der beiden Variablen eliminieren. Und wo wir schon dabei sind, wird natürlich newdigit auch nicht verschont, und die Incrementierung von pos weiter oben mit untergebracht.

```
1. void mad(int zwi, int fact) {
2.     int pos=0;
3.     do {
4.         zwi = f[pos] * fact + zwi;
5.         f[pos++] = zwi % 11;
6.         zwi /= 11;
7.     } while (pos<MAX);
8. }
```

Bekanntlich hat while() genau so viele Zeichen, wie for(;;) - allerdings enthält for schon den Platz für drei getrennte Ausdrücke, während while nur Platz für einen bietet. Allerdings muss man bei der Umstellung die Ausführungsreihenfolge des for-Statements beachten:

```
1. void mad(int zwi, int fact) {
2.     int pos=0;
3.     for(;pos<=MAX; zwi /= 11) {
4.         zwi = f[pos] * fact + zwi;
5.         f[pos++] = zwi % 11;
6.     }
7. }
```

In Java und C99 könnte man übrigens noch die Deklaration „int pos=0" mit reinpacken (spart nochmal einen Strichpunkt):

```
1. void mad(int zwi, int fact) {
2.     for(int pos=0;pos<=MAX; zwi /= 11) {
```

In vielen Wettbewerben ist oft noch eine ältere C-Version vorgeschrieben – allerdings können sich mehrere Schleifen, sofern maximal eine gleichzeitig aktiv ist, ohne Probleme dieselbe Schleifenvariable teilen. Und da wir dann nur noch die Initialisierung, aber nicht die Deklaration in der Funktion haben, können wir denselben Effekt erreichen. Und als zusätzlichen Bonus freuen wir uns, mit Hilfe des Komma-Operators noch zwei geschweifte Klammern eliminieren zu können:

```
1. int pos; /* globale Dekl. vor allen Verwendungen */
2. void mad(int zwi, int fact) {
3.   for(pos=0; pos<=MAX; f[pos++] = zwi%11, zwi /= 11)
4.   zwi = f[pos] * fact + zwi;
5. }
```

Namen kürzen:

Für Bezeichner, deren Namen länger als ein Zeichen ist, gibt es nur drei Ausreden:

• Es handelt sich um die Definition der Funktion main() - leider unvermeidlich...
• Ich muss eine Funktion oder Variable der Standardbibliothek verwenden – hier kann sich die Suche nach einer Alternative mit kürzerem Namen rentieren.
• Ich komme absolut nicht mit weniger als 52 selbstdefinierten Variablen, Konstanten und Funktionen aus – vermutlich habe ich dann aber die Aufgabenstellung falsch verstanden, oder mein Programm noch nicht genug optimiert, bei den typischen Wettbewerbsaufgaben komme ich normalerweise immer mit weniger aus.

Beherzigt man diese und die anderen obigen Regeln, kommt letztendlich folgendes heraus:

```
6. void
7. m(int
8. z,int
9. f){for(p=0;p<=MAX;f[p++]=z%11,z/=11)z=f[p]*f+z;}
```

Kreativer Einsatz des Präprozessors

Während der Entwicklung des Programmes, das in diesem Artikel als Beispiel dient, gab es zeitweise Code folgender Art:

```
1. if ((c>='0') && (c<='9')) {
2.     /* tue was */
3. } else if ((c>='a') && (c<='m')) {
4.     /* tue was anderes */
5. } else if ((c>='A') && (c<='M')) {
6.     /* mach nochmal was */
7. } else if ...
```

Sollten genügend dieser Stellen vorkommen, lohnt sich folgendes Präprozessor-Makro:

```
1. #define i(a,b) if((c>=a)&&(c<=b)){
```

Ob die umschliessenden Klammern in jedem Fall notwendig sind, bleibt dem Leser überlassen, ebenso die „Rentabilitätsrechnung“ nach dem Muster der mad/add/multiply-Funktionen weiter oben – auf jeden Fall verkürzt sich unser Beispielquelltext wie folgt:

```
1. i('0','9')
2.     /* tue was */
3. } else i('a','m')
4.     /* tue was anderes */
5. } else i('A','M')
6.     /* mach nochmal was */
7. } else i( ...
```

Wo wir gerade dabei sind: Zeichenkonstanten mit einem ASCII-Code < 100 ersetzt man am besten durch den entsprechenden ASCII-Wert – spart wieder ein Byte pro Konstante:

```
1. i(48,57)
2.     /* tue was */
3. } else i(97,'m')
4.     /* tue was anderes */
5. } else i(65,77)
6.     /* mach nochmal was */
7. } else i( ...
```

Konstanten mit mehr als einer Stelle, die oft genug vorkommen, können natürlich genauso gut durch den Präprozessor eingesetzt werden. Wenn ich also z. B. die '0' bzw. 48 oft genug brauche, und noch einen Buchstaben im Alphabet übrig habe, sieht das wie folgt aus:

```
1. #define O 48
2. i(O,57)
3.     /* tue was */
4. } else i(97,'m')
```

Allerdings ist hier der Einsatz des Präprozessors nicht optimal, ich kann stattdessen auch eine Variable nehmen:

```
1. int O=48;
```

Ist um ganze 3 Zeichen kürzer, als die Präprozessordeklaration, und ausserdem erlaubt mir der am Ende stehende Strichpunkt, den darauffolgenden Zeilenumbruch auch noch wegzuwerfen, macht also 4 Bytes. Und wenn ich an einer passenden Stelle sowieso Variablen vom Typ int deklariere, hänge ich meine dazu, bekomme ich nochmal 4 Zeichen geschenkt:

```
1. int i,j,k;
```

... wird zu ...

```
1. int i,j,k,O=48;
```

Nochmal zwei Bytes kann ich sparen, wenn beispielsweise die erste Verwendung der Variable k im zeitlichen Ablauf des Programms [3] immer nach der Verwendung der Variable O erfolgt, und zudem schreibend ist – dann wird einfach k mit 48 initialisiert, und O fällt dem allgemeinen Sparzwang zum Opfer.

Tipps: Allgemeines Wettbewerbs-Tuning

Man kann bei einem Wettbewerb [4] immer davon ausgehen, dass die Jury zur Überprüfung der Programme kompliziertere Testeingaben verwendet, als die Beispiele in der Aufgabenstellung.

Insbesondere sollte man die Aufgabenstellung auf mögliche Sonderfälle abklopfen: So wird bei Rechenaufgaben immer der kleinstmögliche und der grösstmögliche Wert getestet werden. Bei Sortieraufgaben werden – sofern dies nicht durch die Aufgabenstellung ausgeschlossen ist – mit hoher Sicherheit Kollisionen (also mehrere gleich einzusortierende Werte) auftreten etc.

Auch sind die Testeingaben oft deutlich länger als die Beispiele, so dass Algorithmen mit hoher Komplexität dann leicht an einem Zeit- oder Speicherlimit scheitern.

[1] Dieses Fragment entstammt leicht abgewandelt der Musterlösung der Jury des Shortest C Coding Contests vom 20C3, siehe *http://ulm.ccc.de/shortest/*
[2] Für Nicht-Logiker: kein Exklusiv-Oder, es kann also davor, danach oder auch davor und danach zutreffen.
[3] Dieser stimmt natürlich nicht notwendigerweise mit der Abfolge der Programmzeilen im Quelltext überein :-)
[4] Dies betrifft auch andere Wettbewerbsdisziplinen, z. B. die ACM “Programmierweltmeisterschaften”.

Prepaid-Handy-Überwachungs-Blues

von padeluun <padeluun@bionic.zerberus.de>

"Fünf Brötchen und zwei Laugencroissants, bitte". In der Bäckerei ist alles wie immer. "Ihren Ausweis bitte", sagt die etwas dröge blonde Verkäuferin - pardon - Fachverkäuferin. Klar, ich halte den Ausweis vor das RFID-Lesegerät, die Daten werden abgescannt und gespeichert -- und schon hundertmal habe ich mir geschworen, den Laden zu wechseln, weil die nicht gleich vom Konto abbuchen (ist ihnen zu teuer), sondern ich immer noch Bargeld rauskramen muss...

Die bezaubernde und charmante Leserin und der kluge Leser haben (schon wegen der Überschrift) gleich erkannt, dass diese Einleitung im Twister-Stil[1] eine etwas überstrapazierte Metapher zum Thema Prepaid-Handys ist. Aber was bei Brötchen undenkbar ist oder scheint, ist beim Kauf von Funktelefonen mit im Voraus bezahlten Karten „normal": Meine Daten werden vom Verkäufer notiert und gespeichert.

Diesmal ist es gar nicht der Datenhunger der Telekom -Unternehmen, die meine Daten haben wollen, sondern es war die Regulierungsbehörde[1], die die Firmen per Anordnung zwang, diese Daten zu erheben. Dagegen klagte ein Telekommunikationskonzern - und bekam Recht. Es ist Unrecht, die Daten von Kunden zwangsweise zu erheben, wenn es dafür keinen Grund gibt (Grundsatz: Datenvermeidung / Datensparsamkeit).

Aber gleich ahnte man, dass das die demokratisch gewählten Datenkraken in der Regierung nicht auf sich sitzen lassen konnten. Wenn schon immer noch nicht die generelle Vorratsdatenspeicherung des Bundesrats durchgekommen ist, so will man doch wenigstens häppchenweise das Grundrecht auf Informationelle Selbstbestimmung aushebeln.

Gerade recht zu den Beratungen der Gremien im Vermittlungsausschuß kam der Anschlag in Madrid und die Bombendrohung am Düsseldorfer Flughafen. Eine große deutsche Boulevardzeitung erklärte die Welt: In Deutschland werden (wie ja just richterlich festgestellt worden war) Prepaid-Handys nicht notiert -- also hat es sehr lange gedauert, bis man die Anruferin gefunden hatte. In Spanien werden die Daten grundsätzlich aufgenommen, also ist man den Drahtziehern des verheerenden Anschlags auf die Vorortzüge schnell auf die Schliche gekommen. Der Vermittlungsausschuß, in dem das besprochen wurde, wurde so überzeugt: Die Daten von Prepaid-Handy-Kunden werden zukünftig gesetzlich legitimiert aufgenommen und gespeichert. Wegen der Sicherheit.

Wieder einmal hat man den Eindruck, es bei den Entscheidern schlicht mit Dumpfbacken (oder Schlimmerem) zu tun zu haben. Es ist nämlich genau andersrum. In Deutschland gabs diese Datenerhebungspflicht (trotz Verbotsirrtum gültig, da von der RegTP per Anordnung gefordert) -- in Madrid dagegen gab es diese Pflicht nicht. Jeder konnte sich in Spanien jederzeit anonym ein Prepaid-Handy besorgen - in Deutschland nicht.

Auch bei den Prepaid-Handys zeigt sich die Erosion der Grundrechte. Bianca Jagger sagte vor einiger Zeit, dass wir Generationen benötigen werden, um die Rechte, die derzeit - demokratisch bemäntelt - abgebaut werden, wieder zurück zu erobern. Die Leute an der Regierung und den Subordinierten in den Ministerien sei ganz deutlich gesagt, dass sie dabei sind, einem neuen totalitären Regime den Boden zu bereiten. Vielleicht sollten diejenigen an den entscheidenden Stellen, die im Irrglauben handeln, das Richtige zu tun, sich vor Augen halten, dass auch demokratisch beschlossenes Unrecht vor allem eins ist: Unrecht.

Mag uns die Entwicklung in den Vereinigten Staaten von Amerika und die in unserem eigenen Land vor 1933 als Mahnung dienen.

[1] *http://www.stop1984.org/*
[2] *http://www.regtp.de/*

Wenn alle Katzen grau sind

von alexander <photon@vantronix.net>

Zwei Schweissperlen zogen ihre silbrig glänzenden Spuren, als sie ihren Hals hinunter um die Wette rannten. Sie war ziemlich ausser Atem. Irgendwie wirkten die körperliche Anstrengung und ihre Aufregung wie zwei Faktoren einer Gleichung, deren Ergebnis nun in Form von Adrenalin durch ihr wild pulsierendes Herz strömte.

Eine präventive Massnahme nannten sie es. Es ginge um die Sicherheit der Infrastruktur, die durch seine 'Kenntnisse und Fähigkeiten' bedroht sei.

"Nationale Sicherheit, klar!", flüsterte sie lautlos und fragte sich was in deren Namen wohl schon alles getan wurde. Sie schloss die Augen und prompt fand sie sich in einem rasenden Alptraum wieder, welcher damit endete, dass der einzige Mensch auf diesem Planeten, dem sie wirklich vertraute, den sie bedingungslos liebte, gegrillt wird. Wie ein Stück Vieh, dass für dessen Konsum vorbereitet wird, wehrlos, hoffnungslos.. Festgeschnallt auf einem Stuhl des Todes. ..click!

Erschrocken riss sie die Augen auf. In ihren klaren grauen Augen spiegelten sich die hellen Blitze aus dem dichten Nebel wie ein Nachleuchten ihrer Gedanken. Laserstrahlen zitterten auf ihrer Haut, als sei ihr ganzer Körper eine Elektrode in einem physikalischen Experiment. Sie war wie erstarrt stehengeblieben und hatte den Atem angehalten. "Jetzt bloss keinen Mist bauen, so kurz davor!", dachte sie und drängelte sich bis zur Bar durch, wo sie sich ein glass Wasser bestellte und versuchte sich zu entspannen.

Vor zwei Tagen war es genau 6 Monate her, seit sie ihren Freund verhaftet hatten. Anscheinend wussten sie aber nichts von ihrer Beziehung. Zugegeben, diese gedieh die meiste Zeit an fernen Orten, geschützt durch ein Spinnennetz aus verschlüsselten Verbindungen. Nur wenige Male hatten ihre Finger die Gelegenheit, sich ohne trennende Tasten aus Plastik zu berühren.

Sie hatten sich auf einem dieser Kongresse kennengelernt. Dort waren die unterschiedlichsten Menschen zu finden, deren einzige Schnittmenge sich am besten als brennende Neugier und unbändiger Wissensdurst beschreiben lässt. Die folgenden Veranstaltungen dieser Art waren dann auch schon die nächsten Gelgenheiten, um die inzwischen übers Netz aufgeflammte Liebe, zu verfestigen. Irgendwann wollten Sie dann auch zusammenziehen.

Doch nun ist er offline. Gefangen in einer Zeitschleife in der jeder Tag wie der vorherige zu sein scheint, nur länger. Umrahmt von Beton, Stahl und Verzweiflung. Nur noch die unsichtbare Verbindung zwischen ihnen zieht ihre Gedanken wie ein Magnet aneinander.

Mit einem Knall den sie selbst durch die Wand aus Schall noch hörte, stoppte ein Glas mit einer durchsichtigen schwappenden Flüssigkeit darin, mitten in ihrem Blickfeld. Sie fühlte sich wie in Trance. Sie ging selten in Discos. Aber dieser Raum, geflutet mit dunklen, alles durchdringenden Bässen und bunt ausgeleuchteten Nachtwesen, gefiel ihr wirklich gut. Sie hatte mehr als zwei Wochen lang nach einem passenden Ort gesucht in dem sie nicht auffiel und sich einigermassen sicher fühlte. Und bekanntlich findet man die grösste Stille im Auge des Orkans. Das gilt für das Datenmeer sowie für die reale Welt, welche mit jedem Display, jedem Sensor und jeder Kamera immer stärker miteinander verwebt waren.

"Ganz schön heiss hier, was? ... Äh, hallo?". Eine aufdringlich wedelnde Hand vor ihrem Gesicht riss sie wieder in die Bio-Welt ihrer Spezies zurück, wo eines deren Exemplare sich gerade mutig, aber ebenso verkrampft grinsend, vor ihr aufgebaut hatte. Sie ging im Schnelldurchlauf die Möglichkeiten den Typen loszuwerden durch, während sie nur nickte und demonstrativ von ihrem Wasser schlürfte. Ihre Laune war wirklich schlecht an diesem Abend und das Lächeln viel ihr immer schwerer, also entschied sie ein wenig zu lügen und beugte sich zu ihm rüber. Die Vorfreude auf seine

vermeintliche Beute verbreiterte nun sein Grinsen. Sie lächelte noch ein letztes Mal süss und wartete einige stillere Sekunden ab um ihm dann ins Ohr zu flüstern:

"Vergiss es, ich fick nur mit Frauen!". Das Grinsen fror ein und der Jäger bewegte sich, elegant wie eine Animatronic-Puppe aus einem billigen Horrorfilm, aus dem Bild.

Sicher, gemein, aber was sie jetzt am wenigsten gebrauchen konnte war jemand der sie beobachtete und ihr eventuell sogar hinterher lief. Dies war kein Spiel und es würde auch keinen zweiten Versuch geben.

Es war viel mehr ein Krieg. Die Dienste und Behörden hatten ihn begonnen indem Sie eine neue 'präventive' Strategie anwendeten um 'Gefahren durch potentielle Terroristen' abzuwenden. Sie fingen an Menschen einzusperren welche bei ebenso präventiven Überwachung als 'Hacker' oder Programmierer mit 'potentiell gefährlichen Fähigkeiten' eingeschätzt wurden.

Die Ersten bekamen noch die Ehre, Präzedenzfälle aller Art zu sein, welche in den Medien unermüdlich wiedergekaut wurden. Aber im Schatten der frisch geschürten Furcht vor noch ungefangenen 'Cyber-Terroristen' verschwanden dann immer mehr Menschen, immer schneller und immer stiller.

Ihr Freund war einer der ersten. Bei ihm ging es sogar recht schnell und unkompliziert, da nach der Analyse seiner beschlagnahmten Computer, Reste von selbstgeschrieben Wurm-Programmen gefunden wurden. Dass darin keine Schadensroutinen ausgemacht werden konnten oder dass diese nie in 'freier Wildbahn' gesichtet wurden tat der sache keinen Abbruch. 10 Jahre für einen erstklassigen 'Verstoss gegen das neue Cyber-Waffengesetz'.

Anfangs reagierten alle mit Verunsicherung. Viele Kontakte wurden eingefroren. Sie trauten sich nicht mehr miteinander zu Sprechen, aus Angst einen falschen Satz zu sagen und damit auf der Liste zu landen. Doch als die Übergriffe zahlreicher wurden und die Willkür weiter zunahm, setzte die erste Gegenwehr ein.

Die Bässe schlugen nun immer schneller und härter in den Raum ein. Alles und jeder in ihm vibrierte. Sie spürte am ganzen Körper wie der Boden zitterte.

Die Musik durchdrang jede ihrer Zellen und verursachte eine heftige Gänsehaut. Wieder zischte die Nebelmaschine um den Weg für neue Blitze und Strahlen zu ebnen.

Sie schluckte schnell den Rest ihres Wassers runter. Die Eiswürfel waren bereits vollständig geschmolzen.

Ihnen war entgangen, dass die Wurm-Fetzen eine Hausaufgabe waren. Die Netze unter ihnen waren ihr Dojo und sie war sein Sensei. Nun war es Zeit ihren gelehrigen Schüler zu rächen.

Sie ging noch einmal im Schnelldurchlauf alle Schritte des letzten halben Jahres durch um vielleicht noch einen Fehler zu finden der jemand auf sie aufmerksam gemacht haben könnte, während sie sich zu den Toiletten aufmachte.

Die Vorlaufzeit war zwar am riskantesten, aber sie war gut gewesen und tiefer als jemand zuvor in die Netze vorgedrungen. Geschickt hatte sie Knotenpunkte zu schlummernden Waffen gewandelt und mit einem intelligenten Angriffsplan versehen.

Sie konnte die Netze förmlich sehen wenn sie die Augen schloss. In diesem Moment waren hunderte kleiner Programme dabei sich miteinander zu verbinden um den letzen Befehl ihrer Schöpferin zu empfangen. Diese sollten aber nur den Stab bilden. Ihre Generäle sozusagen, denn ihre Fusstruppen würden sie aus den wabernden Klumpen vernetzter Monokulturen rekrutieren.

Sie passierte das Frauensymbol und betrachtete sich im Spiegel. Das Gesicht darin kam ihr ungewohnt bunt und kontrastreich vor. Da sie selten ausging, hatte sie auch nicht oft Grund sich zu schminken. Ihr Freund sagte immer dass sie süss aussähe wenn sie wütend ist. Im Moment sah sie aber nur, dass ihre Augen funkelten. Sie sahen fast aus wie die eines Raubtieres.

Offensichtlich war sie jetzt wütend, so genau konnte sie das aber nicht sagen bei dem vielen Adrenalin und dem Gefühlschaos.

Ein letzes Mal schaute sie auf ihre Uhr und ging entschlossen zum Telefon im Flur. Es hing am Ende des Ganges, so konnten die Leute nicht sehen was sie wählen würde. Sie hatte wirklich an alles gedacht.

"Taxizentrale, was kann ich für Sie tun?" - "Hallo, bitte ein Taxi zum.. Äh, Entschuldigung, hat sich erledigt. Ich seh grad dass ich abgeholt werde." - "Kein Problem. Auf wiederhören." ..click. Das war ihr Zeichen. Sie tippte eine lange Zahlenkombination ein. Es piepte einmal kurz. Das System war nun bereit. Würde sie nun die Raute-Taste drücken würden sich all ihre kleinen Programme 42 mal überschreiben und danach selbst beenden. Eine Art letzte Abbruchmöglichkeit für den Fall dass die Sache zu heiss wurde.

Aber gegen Hitze hatte Sie nichts einzuwenden und nach Frieden war ihr nun auch nicht mehr zumute. Sie schloss die Augen ein letzes Mal und stellte sich das Lächeln ihres Freundes vor. Ihr Finger presste sich fest auf die Stern-Taste. Ab jetzt gab es kein Zurück mehr. Es piepte einmal kurz und einmal Lang. Sie drehte sich kurz um. Niemand zu sehen. Unauffällig wischte sie mit einem Taschentuch ihre Fingerabdrücke von den Tasten und dem Hörer, legte auf und verliess die Disco.

Der Bass war selbst draussen noch zu spüren. Sie fühlte sich erleichtert, kämpfte aber trotzdem gegen den Drang an, sich ständig umzusehen. Wenn alles gut ging würden sie nicht einmal wissen in welcher Stadt es begonnen hatte.

In ihrem Kopf spulte sich jetzt das ganze Geschehen wie ein Film ab. Das kleine Programm welches sie im Hauptcomputer der Vermittlungsstelle erwartet hatte, raste nun fast in Lichtgeschwindigkeit von einem Computer in den nächsten, ohne auch nur die geringste Digitale Spur im Telefonnetz zu hinterlassen. Das jeweils nächste Ziel wählte es nach einem Zufallsprinzip aus, wie auch die Anzahl der Sprünge. Am Ende seiner Reise würde es ein paar Telefonnummern anrufen um den Modems auf der anderen Seite die eigentliche Startsequenz zu übermitteln und sich dann wie die anderen auch selbst auflösen.

Die Regierung würde nicht mehr lange bestehen. Ihr grösster Feind war die Wahrheit. Und diese war nun im Begriff sich zu replizieren. Unzählige mp3 Dateien mit abgehörten Telefonaten, geheime Dokumente und belastende Videos würden in den nächsten Stunden auf hunderttausende Computer verteilt werden.

Sogar einige Radiosender und Satelliten-Uplinks würden unerwartet ihr Sendeprogramm ändern. Wenn die Welt endlich nicht mehr ignorieren kann was offensichtlich ist, so hoffte sie, müsste die Regierung ausgetauscht und die neuen Gesetze rückgängig gemacht werden. Sie war fest entschlossen, ihren Freund wieder in die Arme zu schliessen. So sehr, dass ihr das eigene Leben, welches nun zweifellos in Gefahr war, bedeutunglos erschien.

Sie schaute in den schwarzen Himmel hinauf. In der Stadt waren wirklich weniger Sterne zu sehen als ausserhalb. Einzig der sichelförmige Mondschein kam ihr heller vor als die Lichter der Stadt. An einer grossen Kreuzung blieb sie stehn und blickte zu einem riesigen Bildschirm, der an einem hohen, hell funkelndem Gebäude angebracht war. Eine spiessig angezogene Frau fuchtelte gerade breit grinsend vor einer dreidimensionalen Wetterkarte des Kontinents rum. "Und auch morgen wird es wieder ganz schön heiss werden..", säuselte es aus den Lautsprechern hinab.

Sie sollte Recht behalten...

Illustration: Megan Hancock, http://www.thoushalt.net/megan/

User Mode Linux

von Timon <timon@schroeter.it>

User Mode Linux [1] ist ein Patch, der es erlaubt, Linux als Programm zu kompilieren. Dieses Programm (im Folgenden "UMLinux" genannt) verwendet Ressourcen des tatsächlichen Betriebssystems (von nun an "Gastgebersystem" genannt) und stellt sie einem virtuellen System (genannt "Gastsystem") zur Verfügung. Vom Gastgebersystem aus betrachtet ist UMLinux ein Programm, vom Gastsystem aus betrachtet ist UMLinux ein gewöhnlicher Kernel.

Was ist User Mode Linux?

User Mode Linux [1] ist ein Patch, der es erlaubt, Linux als Programm zu kompilieren. Dieses Programm (im Folgenden "UMLinux" genannt) verwendet Ressourcen des tatsächlichen Betriebssystems (von nun an "Gastgebersystem" genannt) und stellt sie einem virtuellen System (genannt "Gastsystem") zur Verfügung. Vom Gastgebersystem aus betrachtet ist UMLinux ein Programm, vom Gastsystem aus betrachtet ist UMLinux ein gewöhnlicher Kernel.

Virtuelles Hosting

UMLinux lässt sich verwenden um ein physikalisches System in mehrere virtuelle Systeme aufzuteilen (virtuelles Hosting), Kernel zu testen und zu debuggen, neue Distributionen auszuprobieren oder Jails und Honeypots zu implementieren. In diesem Artikel wird die Einrichtung eines Systems für virtuelles Hosting beschrieben und die Leistungsfähigkeit dieses Systems mit gängigen Benchmarks untersucht.

Gastgebersystem vorbereiten I. Kern

UMLinux kann entweder im "Tracing Thread"-Modus oder im "Separate Kernel Adress Space"-Modus laufen. Der SKAS-Modus erfordert den sogenannten skas-3 Patch im Gastgeberkernel. Steht diese Funktionalität nicht zur Verfügung, so fällt UMLinux in den Tracing Thread Modus zurück. Dies hat große Einbußen an Leistungsfähigkeit und Sicherheitsprobleme zur Folge und sollte auf Produktivsystemen unbedingt vermieden werden.

Der von UMLinux belegte Speicherplatz läuft asymptotisch auf die vorgegebene Maximalgröße zu. Solange seine Prozesse weniger Speicherplatz belegen als verfügbar ist, wird der restliche Platz verwendet um Plattenzugriffe zu puffern. Es kann dazu kommen, dass mehrere Gastsysteme dieselben Dateien in ihren Puffern halten. Unter Umständen existert eine weitere Kopie im Puffer das Gastgebersystems. Durch bestimmte Maßnahmen kann man UMLinux veranlassen einen Teil dieses Speicherplatzes freizugeben (/ dev/anon Hostpatch). Diese sind jedoch nicht ausgereift, in Zukunft wird vorraussichtlich eine andere Lösung implementiert werden.

Gastgebersystem vorbereiten II. TMP

Unmittelbar nach dem Start legt UMLinux eine Datei mit der Größe des ihm zugewiesenen Arbeitsspeichers im TMP-Verzeichnis des Gastgebersystems an. Das Image wird anschließend unlinked, verschwindet aber noch nicht von der Platte, weil UMLinux es geöffnet hält (`lsof(8)` zeigt es weiterhin). TMP (üblicherweise `/tmp`) muß also groß genug sein, um diese Dateien von allen Gastsystemen aufnehmen zu können. Desweiteren ist es erstrebenswert, diese Dateien im Arbeitsspeicher des Gastgebers zu halten, solange dieser nicht anderweitig benötigt wird. Unser Setup beinhaltet ein 2 GB tmpfs in `/tmp`, von dem nach Bedarf in eine 4 GB Swap-Partition auf einem RAID-Array ausgelagert wird.

Gastgebersystem vorbereiten III. Netzwerk

Zunächst wird die jüngste Version der UML-Utilities heruntergeladen und (nur!) die benötigten Programme kompiliert und installiert. Für den Anfang benötigt man tunctl und porthelper, die Installation von uml_net (SUID-root erforderlich) ist zu vermeiden. Dieser Dämon hat die Aufgabe, von UMLinux-Prozessen angeforderte virtuelle Netzwerkgeräte auf dem Gastgebersystem zu erstellen und einzurichten. Eigene Skripte erfüllen diese Aufgabe ebenso gut und man behält die Kontrolle darüber welche Geräte für welche Benutzer zur Verfügung gestellt werden und welche IPs sie erhalten. Letzteres ist im Zusammenhang mit Routing und Paketfilterung auf dem Gastgebersystem wichtig.

Zunächst wird auf dem Gastgebersystem einmalig ein Device-Node für Tun/Tap Geräte erzeugt, sofern noch nicht vorhanden:

```
mkdir /dev/net
mknod /dev/net/tun c 10 200
chmod 666 /dev/net/tun
```

Beim Start des Gastgebersystems wird für jedes Gastsystem ein eigenes Gerät dieser Art erstellt und konfiguriert. Der Zugriff auf dieses Gerät ist an den Benutzer des Gastgebersystems gebunden, unter dessen Namen das Gastsystem läuft:

```
/usr/sbin/tunctl -u <username>
/sbin/ifconfig tap0 192.168.23.23 up
```

Nun wird das Gastgebersystem als NAT-Router konfiguriert. Ein Destination-NAT erlaubt z.B. die Weiterleitung von Anfragen auf bestimmten Ports des Gastgebers an bestimmte Gastsysteme. Ein Source-NAT gibt dem Gast Zugriff auf das äußere Netzwerk. Natürlich kann man stattdessen auch einen Proxy aufsetzen oder Netzwerkzugriff vom Gastsystem ganz unterbinden.

Gastsystem vorbereiten, Teil I: Kern

Zunächst wird der jüngste UML-Patch auf passende Kernelquellen appliziert. Nun wird konfiguriert und kompiliert, z.B. mittels:

```
make menuconfig ARCH=um
make linux ARCH=um
```

Unterstützung für SMP und SKAS lassen sich noch nicht gleichzeitig verwenden. Bis diese Funktionalität vorhanden ist, sei den Administratoren von SMP-Gastgebersystemen empfohlen sich für SKAS und gegen SMP zu entscheiden. Wird das Feature hostfs aktiviert, so kann auf dem Gastsystem jedes Verzeichnis des Gastgebers eingebunden werden, und zwar mit allen Rechten des Benutzers, unter dessen Namen der UMLinux-Prozess läuft:

```
mount -t hostfs none /mnt -o /usr
```

Diese Dateizugriffsmethode ist sehr effizient (siehe Tabelle), allerdings i.a. aus Sicherheitsgründen unerwünscht. Seit April steht unter dem Namen humfs ein Nachfolger von hostfs zur Verfügung, das Dateirechte intelligenter handhabt.

Teil II. Wurzeldateisystem

Als Wurzeldateisystem kann ein Dateisystem in einer Datei, eine Partition, ein Verzeichnis auf dem Gastgeber oder auch ein per NFS exportiertes Verzeichnis verwendet werden. Eine attraktive Spezialität sind Copy on Write Geräte. Diese bestehen aus einem Dateisystemimage und einer sogenannten Backing-Datei. Diese Gesamtheit wird auf dem Gastsystem schreibbar eingebunden. Alle Änderungen werden in der Backing-Datei gespeichert, sodass das Dateisystemimage von mehreren Gastsystemen gleichzeitig verwendet werden kann. Anfängern sei empfohlen ein fertiges Dateisystemimage herunterzuladen, später kann man ein solches auch selbst erzeugen. Rootstrap wurde getestet und für gut befunden, es stehen noch etliche andere Werkzeuge dieser Art zur Verfügung.

Gastsystem starten

Beim Starten von UMLinux wird die Größe des zu verwendenden Speicherbereichs angegeben (mem=xxxM). Dieser Wert sollte nicht zu groß gewählt werden, denn nicht benötigter Platz wird nicht mehr freigegeben (s.o.). Falls UMLinux mit Unterstützung für devfs kompiliert wurde, das System auf dem Rootdateisystemimage jedoch kein devfs unterstützt, muß mit devfs=none gestartet werden. Konsolen des virtuellen Systems können unter anderem mit ttys, ptys und xterms auf dem Host verbunden werden. Dies ist zur Konfiguration des Netzwerks und des SSH-Daemons nützlich. Später kann dann mit (con=none) gestartet werden. Ferner weist man das Gastsystem an, eth0 mit einem bestimmten Tap-Gerät auf dem Gastgebersystem zu verwbinden (eth0=tuntap,tap0,...). Auf dem Gastsystem wird eth0 dann z.B. Mit ifconfig konfiguriert. Weitere (teilweise nur dort dokumentierte) Kommandozeilenoptionen finden sich auf [2].

	Gastgeber	Gast
Rechenleistung MFLOPS *	113,6	112,3
hostfs MB/s (CPU/%) **	R 19,5 (15) W 21,7 (60)	R 17,4 (93) W 14,8 (94)
ext3 auf ubd MB/s (CPU/%) **		R 14,8 (84) W 10,7 (87)
nfs MB/s (CPU/%) **		R 5,0 (50) W 4,9 (40)
tcp stream Mbit/s (CPU/%) ***	94 (3)	55 (100)

* **Gemessen mit** FLOPS-Linux, das Gastgebersystem verfügt über zwei 550 MHz Xeon-Prozessoren, allerdings verwendet FLOPS-Linux in der vorliegenden Form nur einen davon.
** **Gemessen mit** tiobench bei acht Threads, die insgesamt vier Gigabyte Dateien sequentiell auf einem RAID-Array lesen und schreiben. In Klammer wird die CPU-Auslastung bezogen auf einen Prozessor genannt.
*** **Gemessen mit** netperf, Modus TCP_STREAM. Gastgebersystem und Gegenstelle sind über ein geswitchtes Ethernet verbunden

Leistungsfähigkeit

Der Prozessor und die Festplatten des Gastgebersystems können ohne große Performanceeinbußen verwendet werden (siehe Tabelle 1 und Fußnoten). Tun/Tap Netzwerkgeräte brauchen Rechenleistung und können derzeit nur einen Prozessor verwenden. Wird anstelle von zwei Xeon Prozessoren mit 550 Mhz ein Athlon mit 1 GHz eingesetzt, lassen sich 100 Mbit/s erzielen. Wenn viele System Calls ausgeführt werden sollen, sind die SYSEMU-Patches [3] interessant.

Nicht sicher genug?

Für UML-2.4.17-8 existiert ein Proof of Concept Exploit [4]. Es ist vorstellbar, auf dem UML-System root zu werden und anschließend auszubrechen. Im SKAS-Modus der heutigen UML-Kernels besteht diese konkrete Möglichkeit nicht mehr. UMLinux lässt sich außerdem statisch linken und läuft dann auch in einem schlanken Chroot-Jail. Dieses muß neben dem Wurzeldateisystemimage lediglich den Tun/Tap-Device-Node, `/proc/cpuinfo` und `/proc/mm` enthalten. Die letzteren beiden lassen sich mit mount --bind vom Jail aus zugänglich machen, nachdem man mit `touch(1)` entsprechende Ziel-Inodes erstellt hat. Nicht erforderlich aber sinnvoll ist ein tmpfs um das RAM-Image aufzunehmen. Das tatsächliche Starten des Kernels lässt sich z.B. mit jail_uml aus den UML-Utilities bewerkstelligen.

Fazit

Ein einfaches System für Virtuelles Hosting mit User Mode Linux lässt sich innerhalb weniger Stunden aufsetzen. Auf preiswerter Hardware kann man gute Performance erzielen. Es gibt übrigens bereits etliche kommerzielle Anbieter[5]. Wer trotz SKAS-Mode noch um die Sicherheit seines Systems fürchtet, hat die Möglichkeit jeden UML-Kernel in einem eigenen Chroot-Jail auszuführen.

Links

[1]. *http://user-mode-linux.sourceforge.net*
[2]. *http://user-mode-linux.sourceforge.net/switches.html*
[3]. *http://perso.wanadoo.fr/laurent.vivier/UML/*
[4]. *http://seclists.org/lists/bugtraq/2002/Jan/0338.html*
[5]. *http://user-mode-linux.sourceforge.net/uses.html*

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* _____

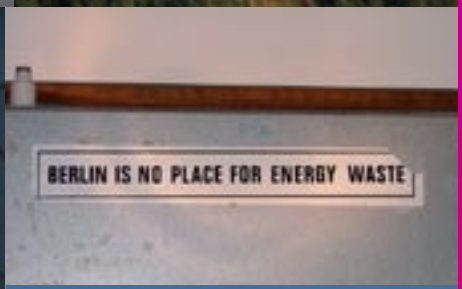
E-Mail: _____

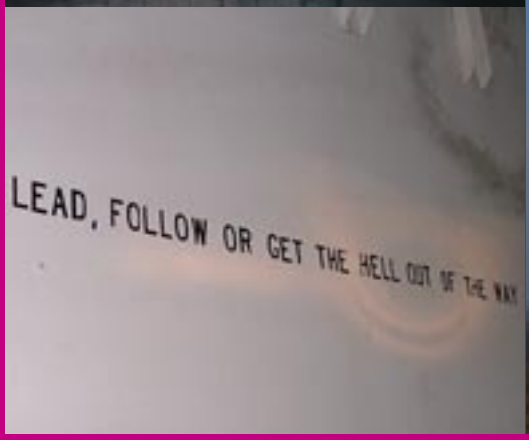
Ort, Datum: _____

Unterschrift _____

*freiwillig


Elektrischer Betriebsraum.
Unbefugten Zutritt verboten!


BERLIN IS NO PLACE FOR ENERGY WASTE


LEAD, FOLLOW OR GET THE HELL OUT OF THE WAY