Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club

Blühindi Londschoftin Coldini Zitin

- *Kampf um die Privatsphäre*
- *Hacking Digital TV*
- *Dreiundzwanzig*

ISSN 0930-1045
September 1997, DM 5,00
Postvertriebsstück C11301F

#60

Impressum

Die Datenschleuder Nr. 60
III. Quartal, September 1997

Herausgeber:
(Abos, Adressen etc.)
Chaos Computer Club e.V.,
Schwenckestrasse 85,
D-20255 Hamburg,
Tel. +49 (40) 401801-0,
Fax +49 (40) 4917689,
EMail: office@ccc.de

Redaktion:
(Artikel, Leserbriefe etc.)
Redaktion Datenschleuder,
Postfach 642 860,
D-10048 Berlin,
Tel +49 (30) 28354872,
Fax +49 (30) 28354878,
EMail: ds@ccc.de

Druck: St. Pauli Druckerei Hamburg
ViSdP: Andy Müller-Maguhn

Mitarbeiter dieser Ausgabe:
Andy Müller-Maguhn (andy@ccc.de), Frank Rieger (frank@ccc.de), Tron (tron@ccc.de), Tim Pritlove (tim@ccc.de), Tobias Engel (tobias@ccc.de)

Adressen

Chaos im Internet: http://www.ccc.de & news:de.org.ccc

Erfa-Kreise des CCC

Hamburg: Treff jeden Dienstag, 20 Uhr in den Clubräumen in der Schwenckestr. 85 oder im griechischen Restaurant gegenüber. U-Bahn Osterstrasse / Tel. (040) 401801-0, Fax (040) 4917689, EMail: ccc@hamburg.ccc.de

Berlin: Treff jeden Dienstag ca. 20 Uhr in den Clubräumen, Neue Schönhauser Str. 20, Vorderhaus ganz oben. S-/U-Alexanderplatz, S-Hackescher Markt oder U-Weinmeisterstr. Tel. (030) 28354870, Fax (030) 28354878, EMail: ccc@berlin.ccc.de. Briefpost: CCC Berlin, Postfach 642 860, D-10048 Berlin. Chaosradio auf Fritz i.d.R. am letzten Mittwoch im Monat von 22.00-01.00 Uhr, chaos@orb.de, http://chaosradio.ccc.de.

Sachsen/Leipzig: Treffen jeden Dienstag ab 19 Uhr im Café Ambiente, Petersteinweg, Nähe Neues Rathaus/Hauptpolizeiwache. Veranstaltungen werden p. Mail über den Sachsen-Verteiler (Uni-Leipzig) angekündigt. Infos für Neueinsteiger gibt´s von bubble@sachsen.ccc.de. Briefpost: Virtueller CCC-Sachsen, c/o Frohburger Medienhaus, Leipziger Str. 3, 04654 Frohburg, Tel: (034348) 51153, Fax (034348) 51024, EMail: sachsen@ccc.de, http://www.sachsen.ccc.de

Bielefeld: CCC Bielefeld: Treff jeden Dienstag um 20 Uhr in der Gaststätte Extra, Siekerstraße 23, Bielefeld. Kontakt: M. Gerdes (0521) 121429, EMail: ccc@bielefeld.ccc.de.

Köln: Treff jeden Dienstag um 19:30 bei Abgang! in der Händelstraße 19. Telefonischer Kontakt via 0177-2605262.

Mönchengladbach: Treff: Surfer's Paradise, Bahner 19 in Mönchengladbach vorerst einmal im Monat jeden letzten Freitag, Ab 1. August dann immer Dienstags um 20 Uhr. EMail: gregor@enconet.de

Ulm: Treff jeden Montag um 19 Uhr im Cafe Einstein an der Uni Ulm. Kontakt: frank.kargl@rz.uni-ulm.de.

Frankfurt/Mainz: kriegen sich noch nicht zusammengerauft. Dürfen wir noch hoffen?

Chaos Family

Bielefeld: FoeBud e.V., Treff jeden Dienstag um 19:30 im Cafe Durst in der Heeperstr. 64. Monatliche „Public Domain" Veranstaltung, siehe Mailbox. Briefpost: Foebud e.V., Marktstr. 18, D-33602 Bielefeld, Fax. (0521) 61172, Mailbox (0521) 68000 und Telefon-Hotline (0521) 175254 Mo-Fr 17-19 Uhr. EMail zentrale@bionic.zerberus.de

Stuttgart: Computerrunde Sücrates, EMail norman@delos.stgt.sub.org.

Österreich: Engagierte ComputerexpertInnen, Postfach 168, A-1015 Wien.

USA: 2600, http://www.2600.com

Editorial

Hallo Chaoten,

das letzte Quartal war wieder gefüllt mit Medienereignissen, aus denen wir uns nur leicht verletzt herauswinden konnten.

Zum Beispiel die IFA. Dieses Multimillionen-Multiidioten-OpenAir-Fernseh-Konglomerat, das versuchte, nunmehr schon im dritten Anlauf, den Leuten das digitale Fernsehen schmackhaft zu machen. Wie gering das Interesse der Freaks an diesem Event ist, zeigte dann unser CCC-Treff: nur ein harter Kern konnte sich durchringen, sich in das Gewühl von Plastiktüteninhabern und Stickerjägern zu begeben. Wir haben Verständnis.

Viel Wind gab es im letzten Quartal um EC-Karten, nicht zuletzt aufgrund der Erkenntnisse, die in der letzten Datenschleuder der Öffentlichkeit vorgestellt wurden. Aus gegebenen Anlaß (die Banken wollen nun neue PINs einführen) widmet sich auch diese Ausgabe noch einmal diesem Thema.

Das Projekt Chaosradio läuft nun schon fast zwei Jahre auf Radio Fritz und findet seinen Hörerkreis. Seit August gibt es das Radio aber auch für Leute, die nicht im Raum Berlin/Brandenburg leben: auf dem Internet. Mehr dazu auf unserer Chaosradio Home Page auf http://chaosradio.ccc.de.

Das Ereignis im Sommer war ganz klar die HIP '97 (Hacking In Progress), das Hackerzeltlager in Kotterbos, Holland. Alle waren da und es war schweineheiß. Einen gemäßigten Rückblick dazu findet Ihr in dieser Datenschleuder.

Das Ereignis im Winter soll wie immer der Chaos Communication Congress '97 werden. Er findet wie gewohnt im Eidelstedter Bürgerhaus in Hamburg Eidelstedt vom 27.-29. Dezember statt.

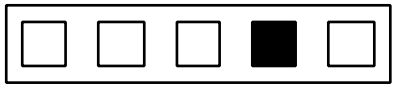
Alle Informationen zum Congress '97 finden sich in der nächsten Datenschleuder und natürlich auf unserer Web Site http://www.ccc.de. Diskussion wie immer in der Newsgroup de.org.ccc.

Achtung Ihr Illuminaten! Die Legion des Dynamischen Diskord ist immer noch wachsam.

Heil Eris!

Index

Die Datenschleuder
Nummer 60, September 1997



Kurzmeldungen

Telefonieren mit der EC-Karte

In ihrem Wahn, EC- bzw. Geld-Karten in Zukunft auch für das tägliche Blumengießen verwenden zu können, kommen die Sparkassen auf immer tollere Ideen. In Zusammenarbeit mit o-tel-o läßt sich die EC-Karte von Kunden der Sparkasse Essen auch als Calling Card einsetzen.

Damit das auch schön „einfach“ geht, hat man eigens ein Gerät entwickelt, in das die EC-Karte eingeschoben wird, und das dann die Calling-Card-Informationen als DTMF-Töne ausspuckt. Das ganze hält man dann emsig an den Telefonhörer, nachdem man eine kostenlose Servicenummer von o-tel-o angerufen hat. Zusatzkosten entstehen - zumindest in diesem Pilotversuch - nicht.

http://www.o-tel-o.de/PRESSE/ARCHIV/SPARKAS.HTM

tim@ccc.de

Mondex broken

We’ve received from anonymous a report on breaking Mondex’s pilot system by TNO along with a confidential 1996 memo describing the break:

TNO’s Ernst Bovenlander gave some details of these attacks (though he didn’t mention Mondex as the target). He showed an electron micrograph of a fuzed link in a smartcard; while intact, this link activated a test mode in which the card contents were simply dumped to the serial port. The TNO attack was to bridge the link with two microprobes. At the last RSA conference, Tom Rowley of National Semiconductor reported a similar attack on an unnamed chip using an ion beam to rewrite the link.

Included is a letter from the Bank of New Zealand to Electronic Frontier Canada attempting to suppress publication of the memo.

http://jya.com/mondex-hack.htm

John Young <jya@pipeline.com>

New bug found in Internet Explorer

Internet Explorer 4.0 bug can open user hard drives to attack. The bug, first discovered by a startup software company, can allow a hostile Web page to overwrite any file on a client’s hard drive. A patch is on its way.

http://cwlive.cw.com:8080/home/online9697.nsf/All/970905internet

The Sept. 8, 1997, edition of Computerworld’s daily.

Mars Rover Fraud

I happened across a web site (http://web.inter.nl.net/hcc/I.Castelijn/) that promised to reveal the _real_ pictures from the Mars Rover, instead of the _fake_ ones released to the public. Since I found the web site regarding the „faking“ of the Apollo moon landings amusing, though totally unbelievable, I decided to view the claimed Mars Rover fakery conspiracy theory, as well.

Imagine my amazement when one of the claimed _real_ pictures contained a view of a wristwatch that I had lost in the Desert outside of Tucson a few years ago. Even the inscription from my mother was still legible!

I’m warning the spooks on this list that if I don’t get my wristwatch back, I’m going to blow the lid off of their whole Mars Rover scam in Smile magazine. I’m serious!

„I AM a number! I am a free man!“

Monty Cantsin, Editor in Chief, Smile Magazine, http://www.neoism.org/squares/smile_index.html

Cyberpath to Psychopaths

CLUE-FINDING COMPUTER BLOODHOUND IS THE POLICEMAN'S NEW BEST FRIEND.

You're the guy next door who commits serial crimes. One day in your mailbox, you find a composite sketch of your face, a psychological profile, a description of your lifestyle and a summary of the gruesome crimes you've committed. Your neighbors receive similar flyers. They are alarmed by the similarities between you and the person described on the flyer, and they call the police.

Direct marketing is now a law enforcement tool, at least in Vancouver. There, a home-grown computerized geographic profiling system enables police to zero in on where a serial criminal is most likely to live by drawing on aerial photographs, land use records, topographical information and other geographical data, which, until now, have been used primarily to develop maps for forestry, mining and resource development.

„We can profile an area where the offender likely lives and do a mail-out asking residents for information," says Det. Insp. Kim Rossmo, head of the Vancouver Police Department's new Geographic Profiling Section, who helped develop the system.

„People are more likely to respond because it is close to home. And how often have you heard that so and so looked like the sketch but the [neighbor or relative] never thought they were capable of committing the crime?

„We've even been successful getting mail-outs into the offender's home, with interesting results," says Rossmo, who declined to elaborate on what those results were.

The police program, called Orion, merges geographic information system (GIS) data with clues from other sources including psychological profiles, aerial photos, postal codes, motor vehicle licensing information, letters criminals have sent to taunt police or victims; census data and land-use records.

When all the information is compiled, the computer calculates various algorithms to produce a so-called „jeopardy surface" - a three-dimensional, multi-colored map that „gives you an optimal searching path for the area," Rossmo says.

The map enables the police to put squad cars in strategic locations, focus searches in targeted areas and avoid expensive, ineffective searches. „Often these cases suffer from information overload. Orion helps police winnow information down to what is relevant. It helps focus an investigation," he adds.

Rossmo began developing an early prototype of what is now Orion as an offshoot of a doctorate he earned at Simon Fraser University. At Simon Fraser, environmental criminologists Paul and Patricia Brantingham had developed a model showing where a criminal lives affects where he is likely to commit a crime.

„So I went at it the other way, to see if you could predict where a criminal lives based on the type of crimes he has committed .... Most offenders commit crimes in their `comfort zone,' which is often not far from where they live."

The RCMP has signed a contract to buy the system from the Vancouver company, Environmental Criminology Research, which markets Orion. A Vancouver-based RCMP officer will begin a year of training with Rossmo in September to learn the system, and the two will continue to work in tandem after that. Ontario Provincial Police are also reported to be „very interested" in the system.

Det. Insp. Kate Lines of the Ontario Provincial Police's behaviorial sciences unit says the OPP is interested in buying the software and has a proposal to do so before management. The goal, she says, is to have a profiler like Rossmo within the unit.

Insp. Ron MacKay, who headed the RCMP's Ottawa-based violent crime analysis branch until his recent retirement at the end of June, says two other officers based in Ottawa and Winnipeg will be trained on the system and work on it part-time in addition to their duties in psychological profiling.

The Orion system is compatible with the RCMP's Violent Crime Linkage Analysis System (ViCLAS), a database of violent crimes and violent criminals that links crimes committed over a period of time or in apparently unrelated locations.

MacKay and Rossmo have already paired the two systems to collaborate on investigations. The combination of the two lead to the arrest of a British Columbia suspect accused in 24 cases of arson. Once ViCLAS linked the fires, MacKay developed a psychological profile that turned out to be „quite accurate" which was fed into the Orion system.

„Kim was able to identify the key area down to 0.02%. The person arrested lived across the street from the area identified," MacKay says.

The RCMP will pay about $225,000 to purchase the software and three Sun UltraSPARC-based workstations. „You can blow that much on one investigation," he says.

Rossmo has been swamped with requests from other forces for Orion's assistance in investigating serial crimes. He is using it to help police in Britain investigate a series of rapes, and recently returned from New York where, for three years, a rapist on Manhattan's east side has been attacking women as they return home from work.

It takes about two weeks to run a case. Rossmo hopes the time will be reduced as the

software is refined. „If I had nothing else to do, I don't think I could handle more than 20 cases a year, but these are all major cases," he says.

Rossmo speculates that the system might have helped police in Ontario link a series of rapes in Scarborough with the sex murders of Leslie Mahaffy and Kristen French in St. Catharines, had it been in place when the police were searching for Paul Bernardo.

„The key is to be able to link the crimes together in the first place," he says, adding that computers can't replace solid police work; they just provide additional investigation tools.

„The whole investigative process is about the intelligent collection and analysis of information. When police are faced with a huge volume of information and limited resources, they have to make the best use of that information.

„This is one more tool," Rossmo says.

Laura Ramsay, Canada, Financial Post

LYING FUCKS!

Behind the ELECTROMAGNETIC CURTAIN

To everyone I know: I've had enough of the bullshit, mind-control fascism surfacing at an increasingly fast pace in an assault on freedom and privacy. I've also had enough of the constant lies of an established political power structure which is now so firmly entrenched in the seat of power that they no longer even bother to tell *_good_* lies. The final straw, for me, was the inevitable announcement that anyone paying the least attention could see coming from a mile away, despite all of the flag-waving, 'land of the free' speeches, and denials by those in power of their true intentions in regard to the future of free speech, liberty and privacy.

5 September 1997, MSNBC: FBI Director Louis Freeh floats a new proposal at a congressional hearing to outlaw non-breakable crypto products.

Accordingly, I am pledging to henceforth exercise my right to free speech, in my own manner, right up to the time when we all face imprisonment for not only free speech, but for freedom of thought, as well. My manner is to call a lying fuck a _lying_fuck_; to call a rat fucker a _rat_fucker_; to call a fucking imbecile a _fucking _imbecile_; to call a Nazi piece of shit a _Nazi_ _piece_of_shit_. In the future, I plan to express myself in a manner which does not give support to the 'quiet lies' that are increasingly being told by the mainstream press and a timid public which are either too tired of fighting the fascists or have too much invested in the current system to risk rocking the boat by calling for an end to bullshit, draconian laws, and increasing oppression and imprisonment of the citizens of what were once free nations. I intend to do

so in my private emails, my public posts, and in the editing of news that I forward to others.

NATION AT RISK?

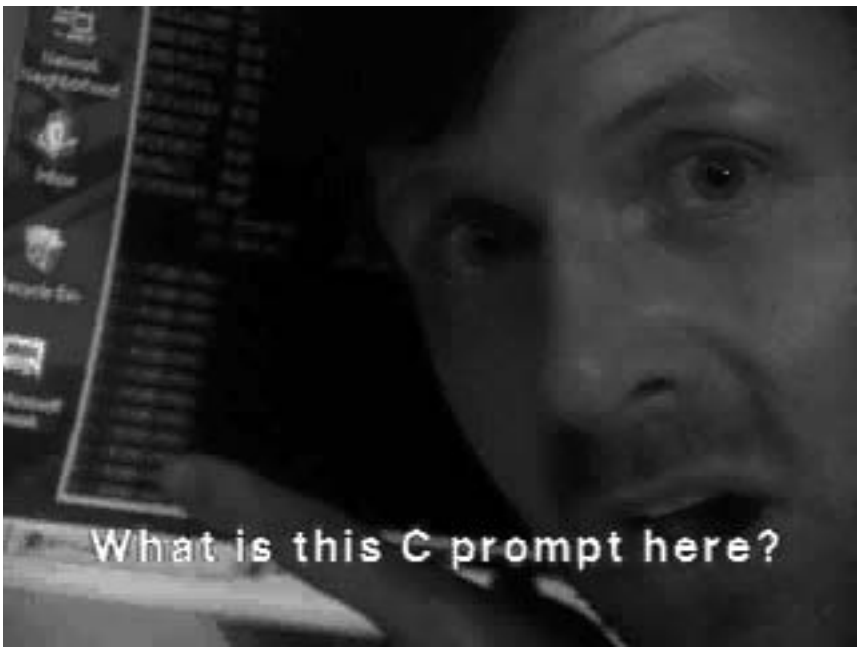
The Fascist White House, Terrorist FBI and co-conspirator intelligence agencies claim that the proliferation of unbreakable encryption products puts the nation at risk. Unnamed Criminals and Mythical terrorists are increasingly using unbreakable encryption products, Lying Fuck Freeh testiLied Wednesday.

I am forwarding this message to everyone in my email address book with the suggestion that they consider doing the same, or to take a similar action which may be more in line with their own character and predelictions. The bottom line: Our elected legislators, politicians, and public servants are *not* going to tell us the truth. The media is *not* going to tell us the truth. If the citizens don't speak truthfully to one another, then there is *no* hope of stemming the escalating assaults on privacy and liberty.

As sole member of the TruthMonger Cult of One: I hereby declare an electronic state of war against the dictatorial, fascist entities who are attempting to build an ElectroMagnetic Curtain around an InterNet that served as a truly democratic forum for Free Netizens until the power structure declared it to be the forefront of a New World, while eschewing any intentions to bring it under the thumb of a New World Order.

I suggest that the Lying Fascist Fucks who are mounting an assault on the freedom and privacy of their citizens lay in some Electronic Body Bags. Perhaps each truthful word I shoot in their direction will be but a negligable 'B-B' in reality, but I refuse to refrain from doing what I can, even if I am wrong about things having reached a stage where enough people will join in resistance to the assault on freedom and privacy to bring down the ElectroMagnetic curtain with a mountain of B-B's.

I can't stop these dictatorial fascists from telling their lies, but I *can* still express my view of their crass assault on the



constitutional rights of myself and others. I *can* call Louis Freeh, Lying Fuck Freeh. I *can* call Bill Clinton, Lying Nazi Schill Clinton. I *can* call Dianne Feinstein, Lying Cunt SwineStein. I not only *can*, but I *will*.

I will fight with bytes, even though I know that, ultimately, these increasingly violent power mongers will respond with bullets if

they perceive a great enough threat to risk exposing their true nature and intentions. I believe that I can fire a lot of B-B's at the ElectroMagnetic Curtain before I 'commit suicide', have a 'tragic accident', or unwittingly fire one of my electronic B-B's in the direction of heavily armed, camoflaged secret troops 'defending' the Electronic Border that the fascists are attempting to build around a formerly Free InterNet.

Am I the only one who has noticed that free speech and private communication on the InterNet posed little 'threat' to society until the government decided to get increasingly involved? Think about it. Who is the enemy? The Public? The Citizens? I think not...

„The Xenix Chainsaw Massacre",
http://bur eau42.base.or g/public/xenix

„WebWorld & the Mythical Circle of Eunuchs",
http://bur eau42.base.or g/public/webworld

„The Final Frontier",
http://www3.sk.sympatico.ca/carljohn

TruthMonger, <tm@dev.null>

Mandatory key escrow bill text, backed by FBI

All encryption products distributed in or imported into the U.S. after January 1, 1999 must have a key escrow backdoor for the government, according to an FBI-backed proposal circulating on Capitol Hill. The measure would impose a similar requirement on „public network service providers" that offer data-scrambling services. FBI Director Louis Freeh talked about this proposal, without disclosing legislation existed, at a Senate subcommittee haring on Wednesday.

Domestic use and sale of encryption has never been regulated.

Attached is an excerpt from the draft „Secure Public Networks Act" dated August 28.

Declan

SEC. 105. PUBLIC ENCRYPTION PRODUCTS AND SERVICES

(a) As of January 1, 1999, public network service providers offering encryption products or encryption services shall ensure that such products or services enable the immediate decryption of communications or electronic information encrypted by such products or services on the public network, upon receipt of a court order, warrant, or certification, pursuant to section 106, without the knowledge or cooperation of the person using such encryption products or services.

(b) As of January 1, 1999, it shall be unlawful for any person to manufacture for sale or distribution within the U.S., distribute within the U.S., sell within the U.S., or import into the U.S., any product that can be used to encrypt communications or electronic information, unless that product:

(1) includes features, such as key recovery, trusted third party compatibility or other means, that

(A) permit immediate decryption upon receipt of decryption information by an authorized party without the knowledge or cooperation of the person using such encryption product; and

(B) is either enabled at the time of manufacture, distribution, sale, or import, or may be enabled by the purchase or end user; or

(2) can be used only on systems or networks that include features, such as key recovery, trusted third party compatibility or other means, that permit immediate decryption by an authorized party without the knowledge or cooperation of the person using such encryption product.

(c) (1) Within 180 days of the enactment of this Act, the Attorney General shall publish in the Federal Register functional criteria for complying with the decryption requirements set forth in this section.

(2) Within 180 days of the enactment of this Act, the Attorney General shall promulgate procedures by which data network service providers sand encryption product manufacturers, sellers, re-sellers, distributors, and importers may obtain advisory opinions as to whether a decryption method will meet the requirements of this section.

(3) Nothing in this Act or any other law shall be construed as requiring the implementation of any particular decryption method in order to satisfy the requirements of paragraphs (a) or (b) of this section.

My report on the September 3 „mandatory key escrow“ Senate hearing: http://jya.com/declan6.htm

Transcript of FBI director Louis Freeh's remarks at Sep 3 hearing, http://jya.com/fbi-gak.txt

Reuters' Aaron Pressman on Commerce Dept backing away from FBI, http://www.pathfinder.com/net/latest/RB/1997Sep05/248.html

Declan McCullagh <declan@well.com>

Geld sparen beim Hotelfernsehen

Oft trifft der gestreßte Reisende abends im Hotel auf einen Fernseher, der die Pay-TV-Kanäle nur gegen ein überhöhtes Entgeld freigeben will. Meist handelt es sich dabei um ein Produkt der Firma Grundig, das die gesperrten Kanäle nach Ablauf der Schnupperzeit hinter einem Overlay aus Videotextklötzchen verbirgt.

Nach Abnehmen des Gehäuses und Herausziehen der Grundplatine auf der Rückseite des Fernsehers zeigt sich links vorne (vorne ist, wo Netzschalter und IR-Auge sind) in der Nähe eines größeren Prozessors ein gesockelter und beschrifteter EPROM.

Nach Entfernung desselben funktioniert der Fernseher wie gehabt, nur ohne die störenden Videotextklötzchen.

frank@ccc.de

A Tribute To The Queen Of Hearts

Paparazzi-Detektor

Die französische Firma CILAS, ein Ableger der Bombenbastler von Aeorspatiale France, hat ein neues Marktsegment für ihren „Sight Laser Detector 400“ entdeckt.

Das Gerät scannt mit einem Laser seine Umgebung mit einer Rechweite von vier Kilometern nach optischen Linsen ab. Wenn der Laserstrahl auf eine solche Linse trifft, entsteht eine spezifische Reflektion, die erkannt und ausgewertet wird. Besonders gut geht das natürlich mit den Teleobjektiven von Paparazzi.

Ursprüngliches Erkennungsziel der Entwicklung waren die Zielfernrohre von Scharfschützen und andere militärische Beobachtungsgeräte. Über Preis, Lieferumfang und Schnittstellen zu automatischen Beschuß-Erwiederungseinheiten des etwa sieben Kilogramm schweren Apparates liegen noch keine Informationen vor.

Eine weitere interessante Anwendungsmöglichkeit dürfte die Aufspürung der diversen Überwachungskameras sein, mit denen die Hüter von Ordnung und Sicherheit ihre Schäfchen bewachen.

frank@ccc.de

Moderne Ermittlungsmethoden in alter Tradition

Die französischen Ermittlungsbehörden haben sich im Mordfall Diana mittlerweile auf die guten alten Traditionen des Focaultschen Überwachungsapparates besonnen.

Die Flics gaben bekannt, daß nunmehr die Funktelefone der am Tatort festgenommenen und gesichteten Reporter überprüft werden. Festgestellt werden soll, ob und wann von den Vertretern der Freien Presse™, Polizei und Krankenwagen angrufen wurden. So soll die etwas dürftige Beweislage der Ermittlungen wegen unterlassener Hilfeleistung erweitert werden.

Ob das Verfahren künftig generell auf alle Funktelefonbesitzer ausgedehnt werden soll, die in Frankreich an einem Unfall vorbeikommen, ist nicht bekannt.

frank@ccc.de

Lady Die!

Ambulantes GSM-Abhören

Die vielgepriesene Abhörsicherheit des GSM-Netzes hat einen neuen Kratzer erhalten. Wie durch die Bundesratsdrucksache 369/97 bekannt wurde, versuchen die Hüter von Ordnung und Sicherheit zur Bekämpfung des Momentan Anvisierten Feindbilds (MAF) Organisierte Kriminalität die Genehmigung für den Einsatz einer bisher wenig bekannten Gerätegruppe namens IMSI-Catcher zu erhalten.

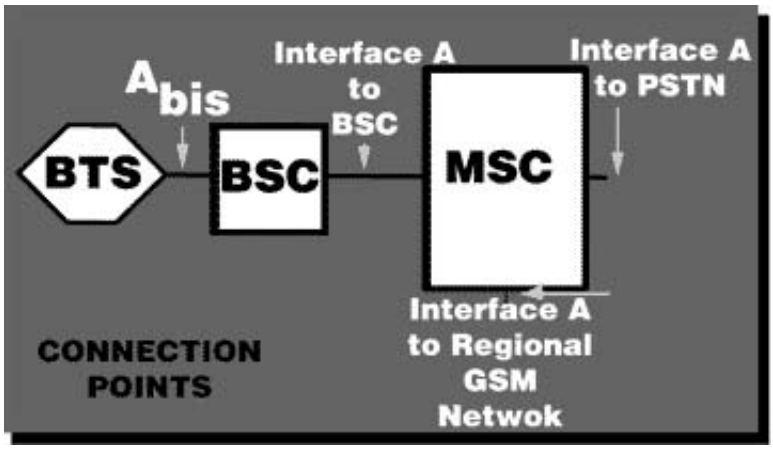
Die International Mobile Subscriber Identification, kurz IMSI, ist die weltweit eindeutige netzinterne Nummer der GSM-SIM-Karte. Die dem Nutzer bekannte Telefonnummer ist immer nur ein Verweis auf die eigentliche Nummer der Karte (IMSI).

Bisher einziger bekannter Typ eines IMSI-Catchers ist das GA 900 von Rhode & Schwarz. Das GA 900 ist eine spezielle Auftragsentwicklung für Polizei und Geheimdienste. Es simuliert gegenüber dem Mobiltelefon alle wesentlichen Eigenschaften einer GSM-Zelle, so daß dieses aufgrund der besseren Empfangsfeldstärke im Nahbereich mit dem GA 900 kommuniziert, statt die echte Zelle zu benutzen.

Dies hat zur Folge, daß alle GSM-Telefone im Empfangsbereich des GA 900 versuchen, sich bei dieser „Zelle“ einzubuchen. Während des Einbuchvorgangs wird die IMSI vom Telefon übermittelt und kann so im GA 900 abgelesen werden. Die Netzbetreiber fürchten, wahrscheinlich berechtigterweise, daß ein solches Vorgehen massive Störungen des normalen Netzbetriebes zur Folge hat.

Offiziell soll das Gerät verwendet werden, um die Rufnummern von Fernsprechteilnehmern zu ermitteln, die versuchen, sich einer Überwachung durch Benutzung von anonymen Karten, geroamten Karten unzugänglicher ausländischer Provider oder Karten, die nicht mit ihrer Person assoziert sind, zu entziehen.

Die IMSI ist aber auch die notwendige Grundlage für Abhöroperationen ohne Mitwirkung des Netzbetreibers. Wenn ein Lauscher auf den Richtfunkstrecken zwischen den Funkzellen und den Mobilfunkvermittlungsstellen (Mobile Switching Center, kurz MSC) gezielt Gespräche von und zu bestimmten Telefonnummern abhören will, benötigt er die IMSI, um die Gespräche zu Identifizieren. Geräte zur Erfassung und Auswertung des Verkehrs zwischen Zellen und MSC sind mittlerweile von verschiedenen Herstellern auf dem Markt.



Eine spezielle Version des GA 900 verfügt zudem angeblich über die Möglichkeit, GSM-Telefonate in der Umgebung gezielt direkt abzuhören.

Um einen entsprechenden Einsatz des Gerätes in der Praxis zu ermöglichen, soll nun auch das TKG geändert werden. In der Änderung soll definiert werden, daß die Beeinträchtigung des Fernmeldegeheimnisses auch unbescholtener Bürger zulässig ist, wenn dies durch die technischen Spezifika

der angewandten Maßnahmen bedingt ist. Im selben Abwasch soll auch der Strafkatalog für Netzbetreiber neugefaßt werden, die ungenügenden Kooperationswillen zeigen. Zur Zeit handelt es sich bei diesem Angriff auf das Fernmeldegeheimnis um eine von der Ländermehrheit getragene Bundesrats-initiative.

Hypothesen

Rein technisch setzt eine taugliche Testumgebung zum Debugging von GSM-Telefonen (und auf dieser Basis setzte die GA 900-Entwicklung höchstwahrscheinlich auf) das Vorhandensein der für die Abwicklung des Telefonats notwendigen Algorithmen A3, A5 und A8 in der Zellensimulation voraus. Wenn also aus der IMSI entweder durch Nachfrage beim Netzbetreiber oder auf anderem Wege der geheime Schlüsselsatz auf der SIM-Karte ermittelt werden kann (Key-Recovery?), steht einem direkten Abhören des Gesprächs bei genügender Nähe zum anvisierten Telefon nichts mehr im Wege.

In der Praxis wird wahrscheinlich eine Kombination von IMSI-Catcher und Abhören der Richtfunk-Verbindung von der Zelle zum MSC eingesetzt.

Wenn das GA 900 wirklich direkt zum Abhören von Telefonaten verwendet werden kann, dürfte die Zellensimulation auf einer transparenten Weiterreichung des Gesprächs an die echte Zelle über ein am GA 900 angeschlossenes modifiziertes Mobiltelefon erfolgen. Dabei könnte dann der Gesprächsaufbau dahingehend manipuliert werden, daß die Verschlüsselung auf der Luftschnittstelle nicht eingeschaltet wird. Diese Funktion ist im GSM-Standard vorgesehen und nach jetzigem Stand der Erkenntnis auch in den Netzen implementiert. Somit wäre die Ermittlung des Ki beim Netzbetreiber überflüssig und die Abhöroperation könnte gänzlich ohne Mitwirkung der Mobilfunkfirma erfolgen.

Über einen bei Rhode&Schwarz unter der Kategorie „Meßgerätezubehör“ geführten bidirektionalen Frequenzumsetzer 900 / 1800 MHz dürfte eine Verwendung des GA 900 für GSM 1800-Geräte (E-Netz) unproblematisch möglich sein.

Gewöhnlich gut unterichtete Kreise ließen durchsickern, daß es zur Zeit ein kleines Problem zwischen Rhode&Schwarz und den Auftraggebern für das GA 900 gibt. Letztere würden das Gerät gerne als Verschlußsache klassifizieren, um eine Verbreitung außerhalb der üblichen Sicherheitsdienste zu verhindern. Dies würde aber den potentiellen Absatzmarkt signifikant verkleinern, was zu einer erheblichen Verteuerung des Gerätes führen würde. Da die Polizeibehörden sowieso chronisch klamm sind, kann man davon ausgehen, daß eine solche Einstufung eher unwahrscheinlich ist.

frank@ccc.de

Chaos Boulevard

Real hackers

CINCINNATI (AP) — A woman accused of letting her three children live in squalor while she spent up to 12 hours a day on the Internet was put on probation Tuesday and ordered to take parenting classes.

Sandra Hacker, who pleaded guilty to misdemeanor child endangering, was arrested June 14 in an apartment that officers said was strewn with broken glass and debris, with children's handprints in feces on the walls. But officers noticed that the area around the computer was clean.

Mrs. Hacker's husband, Alexander Hacker, who is divorcing her, told police that his wife spent up to 12 hours a day browsing the Internet. He complained that their children — ages 2, 3 and 5 — were not receiving proper care.

Mrs. Hacker's lawyer, John Burlew, acknowledged that she spent long hours on the Internet. But he noted that the complaint was made by her husband because of bitterness between the couple.

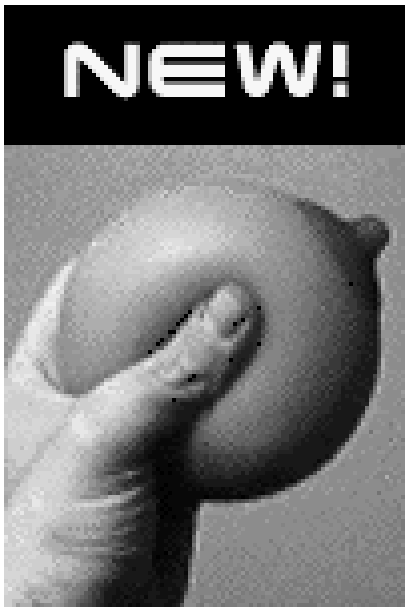
Appearing in Hamilton County Municipal Court, Mrs. Hacker was given a suspended six-month jail sentence, placed on probation for two years and ordered to pay $100 in court costs. She was also ordered to take the parenting classes.

Alexander Hacker could not be reached for comment Tuesday. There was no phone listing for him. He and the children have been living with his parents.

Real Dolls In A Virtual World

Question: Is this for real?!

REALDOLL is a real product, NOT a hoax or prank.



Question: What if I don't fit with RealDoll's sex parts?

REALDOLL's vaginal and anal cavities are made snug to accommodate any insertion. The silicone flesh is soft, slippery, and very elastic. Any petroleum or water-based lubricants can be applied to ease entry. REALDOLL's oral cavity contains soft silicone tongue and teeth. The oral cavity is as snug as the doll's other entries. All of REALDOLL's cavities allow deep insertions.

Question: Tell me more about RealDoll's „suction effect"

When penetrated, a vacuum is formed inside REALDOLL's entries which provides a powerful suction effect. This effect is strongest in REALDOLL's oral entry. Some of REALDOLL's users have reported intense orgasms due to this specific feature.

Question: Tell me more about the doll's Oral Entry option.

With the Oral Entry option, REALDOLL's mouth has a silicone tongue, soft silicone

teeth, and a hinged jaw that opens and closes very realistically.

Question: Does the doll include any electronic features which enhance the pleasure experience such as a vibrating vagina?

REALDOLL does not have electronic features such as vibrators. There's a good reason for that: vibrators are not lifelike. We believe vibrators are used to enliven artificial-feeling vinyl love dolls, but this is not needed with REALDOLL. However, if you enjoy the added stimulation, REALDOLL does work well with such devices. You can use any sex toy imaginable with REALDOLL, and in a very realistic way. Her silicone flesh transfers vibration well.

Question: Can she support herself enough to do it „doggy" style?

REALDOLL can rest on her knees with her upper torso resting on a raised surface, such as a bed or chair.

Question: Tell me more about REALDOLL's breasts.

We use a special formulation of silicone which has a gelatinous consistency. This special silicone gel is used inside REALDOLL's breasts to make them look, feel, and bounce like real breasts.

Question: I want to bathe and shower with my doll. Is there anything I need to be careful about, like water temperature or duration?

Silicone rubber can withstand over 400 degrees of heat. You can soak REALDOLL in a scalding hot bath to give it lifelike body heat. REALDOLL's silicone flesh retains heat very efficiently.

Question: Can water become trapped inside the doll?

No. REALDOLL's head and body are not hollow. REALDOLL is a SOLID love doll.

Question: Do you offer electronic or animatronic versions of REALDOLL?

Not at this time, but we hope to offer such dolls in the future.

Question: What happens when „the honeymoon is over" and I feel that the doll is not for me and wish to return it?

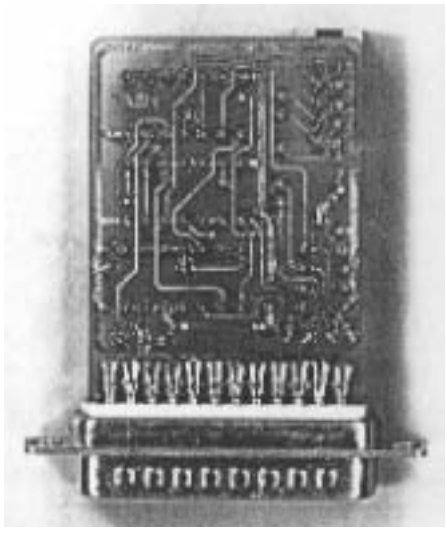
Although we'd like to fully satisfy all our customers, our firm policy is: ALL SALES ARE FINAL.

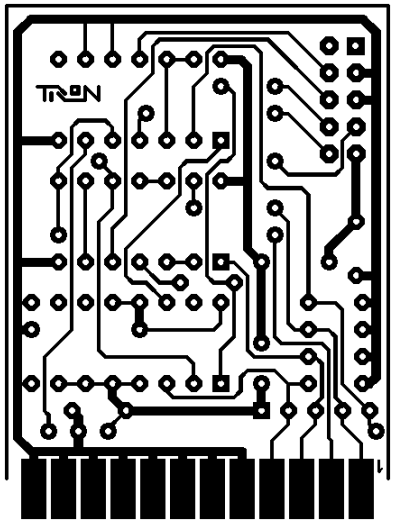
RealDoll Home Page
http://www.realdoll.com/

Hacking Digital TV

Für die Freunde des Digitalen Fernsehens ist es ein häufiges Ärgernis: ferngesteuerte Software-Updates der dBox verhunzen die liebgewonnene Benutzeroberfläche, nützliche Menüpunkte verschwinden über Nacht, bisher einwandfrei funktionierende Funktionen zeigen sich plötzlich bockig. Die Software-Updates werden über den normalen Datenkanal eingespielt, der auch die Fernsehdaten transportiert und sind daher nur schwer zu vermeiden.

Was der ambitionierte d-box-Nutzer sich also wünscht, ist eine Möglichkeit, die Softwareversion seiner immerhin über 1000,- DM teuren Box selbstbestimmt zu wählen. (Backups von legal erworbener Software für den ausschließlich persönlichen Gebrauch sind zumindest bei PC-Software vom Gesetz ausdrücklich gedeckt. Wie es sich bei der internen Software von Geräten verhält, ist etwas unklar.) Vom Eingriff in Mietgeräte sollte aus rechtlichen Gründen Abstand genommen werden. Daß die Garantie auch einer gekauften Box durch Aufschrauben erlischt, sollte selbstverständlich sein.

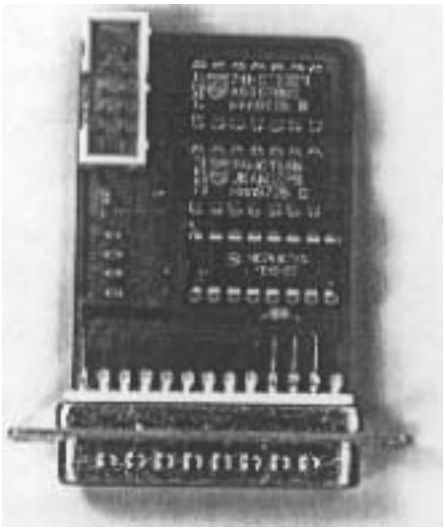




Nachfolgend dokumentieren wir ohne Gewähr eine kleine Bastelanleitung für ein PC-Interface für den Background Debugging Mode, für den es auch einen Port in der d-box gibt.

Beim Prozessor der d-box handelt es sich um einen Motorola 68340, ein Derivat des aus alten Amigazeiten bekannten 68000. Von diesem Prozessor werden alle anderen Subprozessoren der d-box gesteuert (Tuner, Demux, Entschlüsselung etc.) und die Benutzeroberfläche realisiert. Der EEPROM-Speicher für diesen Prozessor besteht entweder aus zwei 29F400 oder einem 29F800, beides ergibt ein Megabyte.

Etwa 80 Kilobyte des Speichers sind durch einen extra Jumper geschützt, in diesem Bereich befinden sich die länderspezifischen Selbsttestroutinen und andere Komponenten, die nicht über den normalen Softwareupdate-Mechanismus verändert werden können. Der Jumper befindet sich in der Nähe des Kabels zur Tunerplatine (XP06) und hat eine grüne Fassung. Er sollte in der Regel **nicht**(!) gesetzt



werden, da ein ahnungsloses Überschreiben des geschützten Bereiches die Box zum akuten Pflegefall machen kann.

Wie die meisten Embedded 68xxx-Systeme verfügt auch die Nokia-d-box über einen Port für den Background Debugging Mode (BDM). Dies ist ein 10-poliger Stecksockel, der sich unter dem Modem-Modul der Box verbirgt. Nach dem vorsichtigen Abheben des Modems ist er deutlich zu sehen.

Nach dem erfolgreichen Aufbau des kleinen BDM-Moduls aus unserem Bastelplan wird nun per Flachbandkabel eine direkte Verbindung zwischen diesem und dem d-box-BDM-Port hergestellt. (Pinbelegung 1:1 identisch) Das BDM-Modul wird dann an den Parallelport des PCs gesteckt. Was noch fehlt ist natürlich die Software. Motorola bietet unter

http://www.mcu.motsps.com/fr_eeweb/pub/mcu332/bd32-122.zip

den BDM32-Debugger zum kostenlosen Download an. Unter

http://www.mcu.motsps.com/fr_eeweb/pub/mcu332/BDM-V090.ZIP

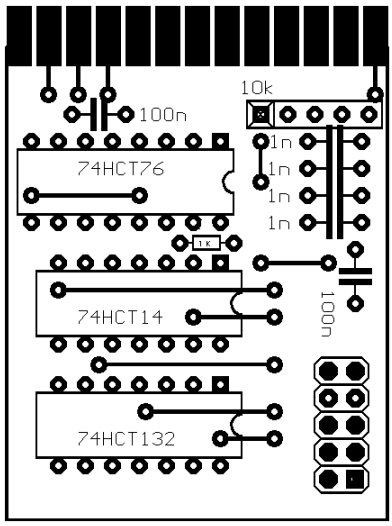
finden sich die C-Sourcen einer älteren Version des BD, die für die Erstellung von Up- und Download-Skripts nützlich sein dürften.

Der BD erlaubt aufgrund der Spezifika der verwendeten EEPROMs nicht das direkte Up- und Download der Speicherinhalte. Diese haben eigene Kommandos für das Schreiben und Lesen von Speicherzellen, die sequentiell ausgeführt werden müssen. Hier ist noch etwas Feinarbeit erforderlich, ein Script für den BD muß erstellt werden, das die Besonderheiten dieser EEPROMs beim Lesen und Schreiben von Speicherzellen berücksichtigt.

Auf dem CCC-Webserver haben wir unter

http://www.ccc.de/Library/HPA/DigitalTV/

neben einem Mirror der Motorola-Freeware auch noch die etwas schwieriger zu



Hacking Digital TV

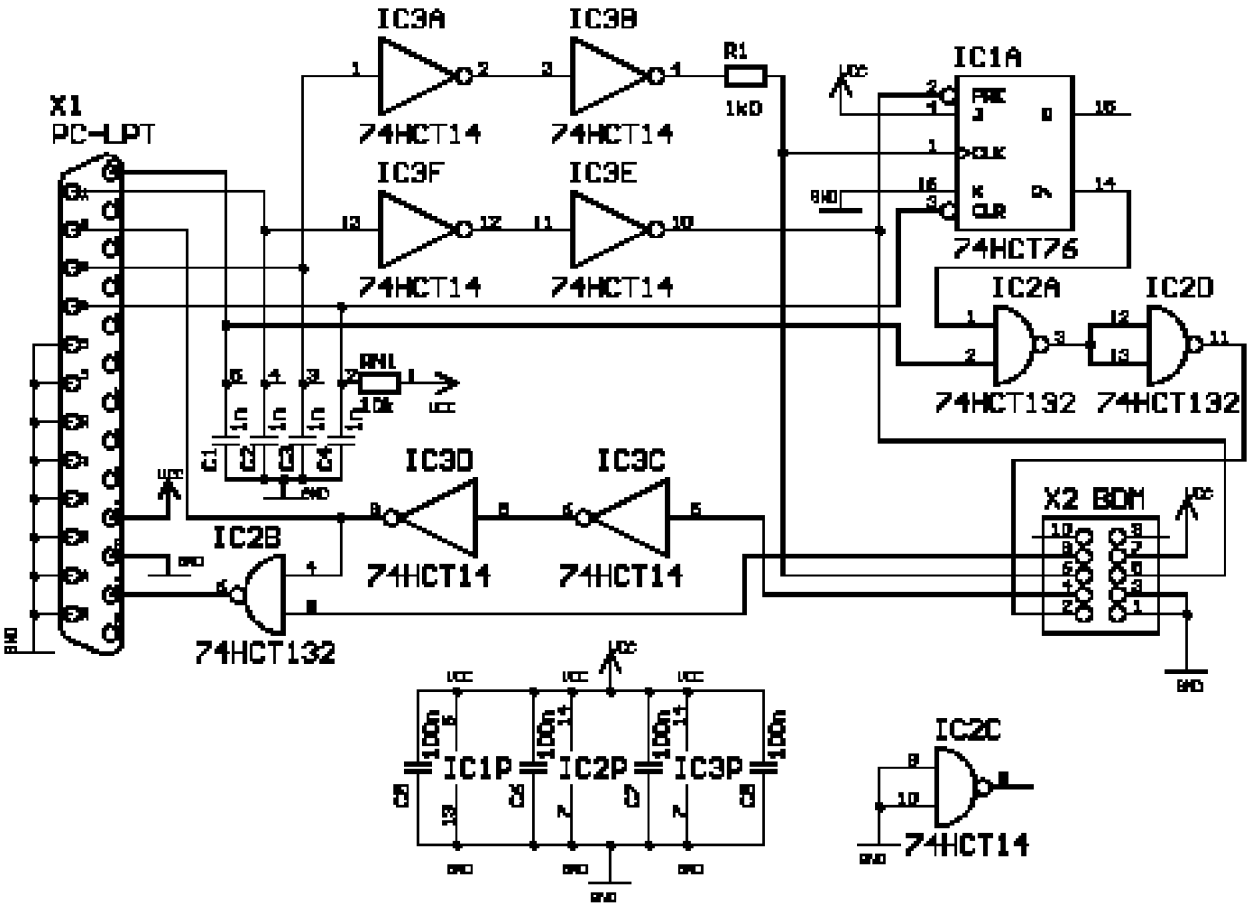
findenden Datenblätter der EEPROMs als PDF abgelegt. Wenn jemand fertige Skripte für Up/Download und ähnliches gebastelt hat, werden diese auch dort zu finden sein.

Nähere Informationen zum BDM und Aufzucht und Pflege der 683xx-Prozessorlinie findet sich auch in der ELRAD 8/1997 S. 66 „Basisarbeit“.

Interessanterweise haben auch die Microtac GSM Telefone (aka PT9x) von Motorola einen 68332-Prozessor nebst dazugehörigem BD-Mode. Hier ist leider kein fertiger Pfostenstecker vorhanden, die BDM-Pins müssen also direkt am Prozessor abgegriffen werden.

Das BD-Modul funktioniert nicht mit dem 68328.

Projekt: tron@ccc.de
Dokumentation: frank@ccc.de



VSt Watch

Rückruf bei besetzt / T-Net-Box

Die T bietet ja nun seit einiger Zeit Rückruf bei besetzt (Completion of Calls to Busy Subscribers) für ISDN-Kunden an (und auch für Analog-Teilnehmer, wenn man hartnäckig ist): Wenn bei einem angerufenen Teilnehmer besetzt ist, kann ein automatischer Rückruf aktiviert werden. So kann man sich das lästige „probieren, ob wieder frei ist“ sparen. Allerdings wird die Aktivierung der Call Completion zurückgewiesen, wenn der angerufene Anschluß eine Rufumleitung - egal welcher Art - aktiviert hat.

Bisher war das ziemlich bedeutungslos, da sich bei den Phantasiepreisen der T sich sowieso kaum jemand den Luxus einer Umleitung leistete. Das hat sich jetzt allerdings geändert: Die T-Net-Box (siehe DS 59), inzwischen offiziell vermarktet, wird durch eine Umleitung aktiviert. Wenn sich die Anrufbeantworter-im-Netz-für-unglaublich-günstige-4-Mark-im-Monat-Sache so durchsetzt, wie von der Telekom geplant, könnte Rückruf bei besetzt zur Unbenutzbarkeit verkommen.

Rückruf bei Nichtmelden / Datenschutz

CCNR (Call Completion on No Reply) ist eines der neuen Leistungsmerkmale, das die T demnächst einführen will. Für den Anrufer ist das sehr praktisch: Wenn sich der Angerufene nicht meldet, kann CCNR aktiviert werden. Die Vermittlungsstelle meldet dem A-Teilnehmer dann einen Rückruf, sobald der B-Teilnehmer den Hörer abgenommen und wieder aufgelegt hat (z.B. zum Zwecke eines Telefongespräches). Dieses Feature ist jedoch datenschutzrechtlich nicht ganz unbedenklich: läßt sich doch so wunderbar eine Überwachung der Nutzung des Zielanschlusses durchführen.

Und trotzdem wird uns immer noch die Einzelverbindungsübersicht ohne XXX anstatt der letzten drei Ziffern mit Hinweis auf den Datenschutz vorenthalten...

Zufälliges Aufschalten bei EWSD

Wie aus gewöhnlich gut unterrichteten Kreisen zu erfahren ist, gibt es in der neuen Siemens-EWSD-Software einen - zwar selten auftretenden, aber vorhandenen - Bug, der dazu führt, daß man nach Abheben des Hörers kein Wählzeichen erhält, sondern auf eine beliebige andere Leitung aufgeschaltet wird.Falls dort zu diesem Zeitpunkt eine Verbindung besteht, kann man diese mit anhören, selbst jedoch nichts sagen.

Weitere neue Leistungsmerkmale

Demnächst werden wohl neue ISDN-Leistungsmerkmale verfügbar sein. Darunter:

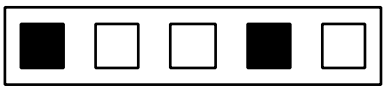
- Keypad-Facilities: Aktivierung von Leistungsmerkmalen über */#-Kombinationen. Gut für ältere Telefone nützlich, die z.B. Rückruf bei besetzt noch nicht von sich aus unterstützen.

- Anrufumleitung während der Rufphase (CD, Call Deflection): Wenn das Endgerät bereits klingelt, kann der Anruf zu einem beliebigen Ziel umgeleitet werden.

- Verbindungskostenübernahme durch den Angerufenen

Wie üblich werden diese Leistungsmerkmale wohl zuerst auf Siemens-EWSD-Anlagen verfügbar sein.

tobias@ccc.de



Chaos Realitäts Schnuller

Contribution to the collaborative future fiction: „The True Story of the InterNet“ by Bubba Rom Dos, et al.

The True Story of the InterNet, Part III, Chapter 8

Nuke ‘em ‘till they glow

Jonathan decadently lounged on the worn sofa swigging Bubbas special reserve straight out of the bottle. He burped and tossed the empty bottle to join the pile of kipple heaped in the corner — an antique pentium-II 400 with it’s case off, a huge heap of hydrocubes, a couple of busted flatscreen monitors, some empty pizza boxes.

Leaning against the wall lay Bubba Rom Dos, snoring quietly, and clutching a half empty bottle of his special reserve.

Jonathan lay back trying to brainstorm a direction to explore to find an exploitable bug in the Hewlett-Packard Fabasoft faba-code verifier. He was fast running out of ideas.

The desire to find an exploit had arisen earlier that day when Bubba Rom Dos had tossed him a hydrocube which contained a particularly interesting deskfab 6 file. The file was named „nuke.fab“. He couldn’t rightly see where Bubba could have come into possession of the file, but Bubba wasn’t too forthcoming on the subject, so Jonathan had contented himself with examining the contents of the ‘cube. He had quickly become engrossed with the contents.

Jonathan had a selection of bootleg PICS fabrication policy files, ranging from `under 18 months’ (for construction of soft cudly toys with no easily swallowable parts) up to `military grade IV’ (good for things like Forestry Commision SWAT team issue rocket launchers, and stealth helicopters etc, if you had a 10m3 volume fabricator and a few GigaWatts on your electricity meter). A good indication that the file was the _real thing_ was that it failed the faba-code verifier with even military grade IV PICS fabrication rating policy file — the verifier refused to ‘fab the file because it rightly diagnosed that it would result in the formation of fissionable material!

(How Jonathan came to be in possession of a military grade IV PICS fabrication policy file is a story for another time).

Now Jonathan also had a hacked fabber — it was hacked to completely by-pass the PICS policy file rating system. This in itself was supposed to be impossible, but Jonathan had found that you could replace the FAPI module signature verifying key embedded in the flipper policy chip by placing a piece of sticky tape over pin 5 of the smart card contact and brute forcing the LEAF field which for some reason seemed to only use a measily 16 bit checksum, which took all of half an hour to brute force. You’d have thought they would have learned and increased the checksum size after Matt Blaze brute forced the clipper chip LEAF in the tessera cards. But in fairness, Jonathan’s attack had one extra wrinkle: the sticky tape. Normally the flipper chip wrote a count of how many smart cards with failed checksums were inserted, and alerted the forces of darkness after 3 false tries, but the sticky tape took care of that. Jonathan supposed the designers had not considered that someone might place sticky tape over pin 5, the pin which was used to signal an insertion of the smart card.

With that hack completed and the flipper policy chip instruction code manual which the cypherpunks had obtained dumpster diving in the Mykotronics dumpster, he was in business. He had then blown a new EPROM with a `customized’ firmware, the policy chip accepted the `Circle of Eunuchs’ FAPI module signature on the hacked EPROM, because there was now nestling comfortably at the heart of the NSA designed `tamper-proof’ fabber flipper chip a DSS key which read:

```
Circle of Eunuchs <coe@dev.null>
```

The original key had read:

```
NSA FAPI signature key <dirnsa@nsa.mil>
```

So much for NSA security, Jonathan chuckled at the rememberance of that exploit.

Anyway, for amusement value, and 1.3 MegaWatts of electricity later (the cowboy had given him a hacked power board account — phree electricity, wheee!), Jonathan’s industrial grade Hewlett-Packard deskfab 9GSII fabber had produced a nice matt black suitcase.

Jonathan watched the instructional 3d-mpeg file included on the hydrocube, and spent a good hour in awe playing with the controls on the suitcase. Satiated with knowledge now that he knew how to operate all of it’s modes, he was lying comatose on the sofa wracking

his brains trying to overcome the next hurdle — how to construct the perfect way to nuke Washington DC. His plan so far was to spam each of the `targets' with a word99 macro virus (thanks Bill Gates) in a document describing his `SFr 10,000,000 campaign contribution' which automatically spooled a mildly modified „nuke.fab" for fabrication, and turned off the fabbers status leds through a Hewlett-Packard firmware bug. Jonathan had all this down pat.

(The modification to „nuke.fab" in case you were wondering was to put the suitcase in detonate with no bypass mode, with an initial count down of 30 seconds).

The problem was — all those congress-critters were bound to be running on a PICS fabrication rating below `national-security-emergency', and so the faba-code verifier would refuse to load the code. Worse still the non-hacked HP deskfab models after mandatory GAF (Goverment Access to Fabbers) was introduced would narc out the owner to the Feds within minutes, thereby alerting the dark forces as to what the plan was.

The wall clock now read 3.30am. Jonathan dozed off to sleep dreaming of glow-in-the-dark congress-critters.

„fifty-eight ... fifty-seven ... „

Jonathan woke grogily to see a group of people huddled over a suitcase. In the middle of the group was Bubba Rom Dos grandiosely counting down, in between swigging from his bottle of special reserve and pressing buttons randomly on the suitcases control panel. Priscilla and Alexis were peering closely at the pretty flatscreen status display, making sage comments as to what the buttons might do, for all the world as if they were playing a video game.

Jonathan came to his senses and screamed at the top of his lungs:

„Nooooo!"

and sprang to his feet. He almost fell over again as the effect of moving that quickly so soon after waking up hit him, his head swimming.

All heads turned to face him.

„Yaieeeeeeee!" yelled Jonathan, as he rudely barged his way to the suitcase control pannel, and began franticallly pushing buttons.

After a short panic attack, he calmed down sufficiently to notice that the display read „no override". Having

absorbed the entire instruction 3d-mpeg, Jonathan knew what that meant. The LCD display read 50 seconds.

Bubba swigged another gulp of his special reserve, and said innocently „What's the problem?"

Jonathan looked fit to explode, his pulse was racing and his head hurt horribly, „It's a nuke!" he screamed hoarsely, „and you've just armed it, and I can't disarm it, and you've got ..." his eyes tore to the display „45 seconds until you're vapourised." Priscilla was already running for the door screaming.

Bubba belched loudly, and looked slightly ill. Alexis gulped and said „What now?".

Bubba tosssed the empty bottle of special reserve on to the growing pile of kipple in the corner, and pulled a fresh bottle from inside his rain mac.

„Lets think rationally here" said Bubba, calmly, pouring himself a shot of special reserve, „can't you um disable it, or um, un-fabricate it or something".

A flash of inspiration hit Jonathan, seeping through his slowly waking brain (he was not a morning person).

He flashed a grin to Bubba and walloped him hard between the shoulder-blades shouting, „You're a genius!" Jonathan then hugged Alexis lifting her off the ground.

Bubba looked puzzled but pleased. Alexis looked a little worried.

Jonathan looked at the display pannel on the suitcase „35 seconds". `No problem' he thought. He slammed the suitcase shut and practically threw it in to the HP deskfab 9GSII fabrication bay, and slammed the door shut.

Then he grabbed the keyboard, and began typing at around 100 wpm.

Chaos Realitäts Schnuller

After a deathly long pause where the terabyte hydro drive light flickered intermittently, the fab drive hummed to life. The lights dimmed with the sudden increase in power consumption. A few seconds later the drive light blinked out, and the deskfab fell silent.

„That," said Jonathan, stabbing the screen

```
-rw-r—r— 1 jon users 7516192768 Oct 4 10:12 tmp00001.fab
```

where the words `tmp00001.fab' were emblazoned in green writing on a black background, „is an armed nuke".

„Now, where was I?" mused Jonathan, and then remembering, rounded on Bubba, „Uh yeah, just where exactly did you find nuke.fab?"

Bubba made an expansive gesture with his hands, and poured himself another shot. Throwing back the shot, Bubba said: „I got it off the web,", and began searching through the pockets to his rain mac, eventually pulling a scrumpled scrap of paper from his pocket, and handing it to Jonathan. „A kindly elderly gentleman with a 9mm uzi gave me this address," he explained. Jonathan looked at the badly scrumpled scrap of paper, and was just able to make out:

```
http://jya.eternity/cryptome/nuke.fab
```

Jonathan looked puzzled, the initials „jya" looked vaguely familiar to him from his reading of old cypherpunks posts. Ah, yes, it was that Architect guy, John Young, who kept getting into trouble over hosting materials that the feds didn't like. So he was using the eternity service now.

Now the panic was over Jonathan resumed his position on the couch, allowing himself to recover from the previous nights hacking session.

„Say Bubba," Jonathan said with his eyes closed, „do you have any ideas of how to by-pass the Fabasoft faba-code verifier on an HP deskfab?"

Bubba finished his mouthful of strong spirits, „Huh? Wassat you say?"

Jonathan explained to Bubba and Alexis the events of the night before and of the plan to nuke Washington DC, and party-way through Priscilla returned, looking a bit sheepish for deserting them at such a crucial time.

„So," said Alexis, „You used the deskfab to copy the armed nuke, hence disabling it?"

„Sure, that's a standard function", said Jonathan, „it's a bit like a 3d photocopier, only you can set it to unfabricate the object being copied at the same time."

„Well," pressed Alexis, miles ahead of Jonathan, and not needing the mini-lecture on deskfab functionality, „couldn't you copy a deskfab?"

Jonathan opened his eyes from his inert position on the couch. „Uh, I dunno, yeah I suppose so...."

Then Jonathan saw the light, a second time that day: „Heh, yeah, okay!" he enthused, „that's a cool idea Alexis."

Alexis and Jonathan excitedly started unplugging the deskfab from the unix box.

„Carry these," said Jonathan and thrust upon Bubba a laptop, the hydrocube containing tmp00001.fab, and a bundle of interface leads. Jonathan and Alexis proceeded to lug the desk fab out back, and down into the basement. Bubba and Priscilla followed puzzled as to what the excitement was.

In the basement was an ancient looking Sun unix box. The screen was one of those huge glass tube affairs. Beside it sat what looked like a refridgerator with clunky looking dials on it.

Jonathan powered up the Sun box. Suprisingly enough it actually booted, and 10 minutes later, after an agoni-

singly slow process where it went through checking (fscking) all it's ancient hard drives, which wirred and clicked noisily, it came up, and the prompt said:

```
Welcome to toad.com
login:
```

Without hesitation, Jonathan logged in as `gnu', and immediately typed in a password. He was in. Bubba and Priscilla exchanged glances. Jonathan explained, „I shoulder surfed the password when John logged in when I was at the physical cypherpunks meet in my grandpas study all those years ago."

„This," he said patting the minifridge sized machine humming noisily in front of them, „is his old machine, `toad.com', old home to the cypherpunks list."

Next Jonathan lugged his deskfab into the refrigerator affair, which apparently was an antique deskfab, sat the lap top on top of it, and hooked the laptop up to the deskfab, and inserted the tmp00001.fab hydrocube into the laptops hyro drive. Then he wandered off in search of a portable power source. He came back lugging an emergency power module `liberated' from the electric company at some point in the past.

He hooked-up the power module to the HP deskfab.

„Now," said Jonathan, „the timing on this is a bit delicate", I think there's only around 20 seconds left on the nuke.

Jonathan set the laptop on time delay to instruct the deskfab to refabricate the primed nuke with 20 seconds left to pop time, but not to start doing that for around 1 minute. Then he slammed the refrigerator sized fabricator door shut, and began typing in earnest on toad.com. The refrigerator started humming, and toad.com's drive started buzzing frantically.

„Gee I hope the transfer rate on these mechanical drives is good enough to copy it before it fabricates the nuke", opined Jonathan.

Jonathan started typing again. „Shit! we're gonna run out of space!" he said. And started typing frantically rm -rf'ing anything that could be rm -rf'ed without stopping the machine. He rm -rf'ed /usr/src, and /usr/spool/ and a bunch of other stuff. He made it with half a gig or so spare, and who knows how few seconds to spare.

The refrigerator-sized deskfab stopped humming, and the hum of the contained HP fabber had stopped too as it had been rudely unfabricated by the antique fabber.

Jonathan was pleased with himself now.

„That," said Jonathan, with a stabbing motion

```
-rw-r—r— 1 gnu users 8589934592 Oct 4
10:42 donation.fab
```

where the words `donation.fab' were emblazoned on the clunky glass screen, „is a freshly fabricated top of the range HP deskfab 9GSII, which is just about to fabricate a suitcase nuke, which will pop a few seconds after being fabricated".

„But will it pass the faba-whatsit verifier?" asked Alexis.

„Er are you sure this is a good idea?" asked Priscilla.

„Of course it is," said Bubba.

„That's a good question Alexis," Jonathan said ignoring the other chatter, „I'm not real sure. I think it should pass because, well, the faba-code verifier isn't _that_ smart, right. I mean to realise that it will build a HP deskfab, which just happens to have freshly downloaded instructions to build fissionable material patterned into it's memory modules, I mean that's like solving the halting problem right?"

Bubba cleared his throat, „If I might make a suggestion here", he said, „now that the high falutin' theoretical stuff is out of the way, the obvious thing to do is try it and see."

„Asplendid suggestion", said Jonathan, begining to type once more, „very good Bubba, the empirical hackers approach."

So Jonathan tried it, and saw. He typed:

```
To: cypherpunks@cyberpass.net
Bcc: president@whitehouse.gov
Bcc: freeh@fbi.gov
Bcc: feinstein@congress.gov
...
Mime-Version: 1.0
Content-Type: multipart/mixed; boundary="—
=_NextPart_000_01BCB88F.57968E50"
Content-Transfer-Encoding: 7bit
```

Chaos Realitäts Schnuller

```
This is a multi-part message in MIME format.
——=_NextPart_000_01BCB88F.57968E50
Content-Type: text/plain; charset=ISO-8859-1
Content-Transfer-Encoding: 7bit

Hello,

Please accept our campaign donation of SFr
10,000,000 in used swiss francs.

Just double click on the enclosed attachment
in your mail reader, and it'll print out
the donation file attached in an HP
compatible fabber. You'll need quite a large
fabber, as SFr 10,000,000 is quite bulky .

Kind regards,
The Circle of Eunuchs

——=_NextPart_000_01BCB88F.57968E50
Content-Type: application/octet-stream;
name="donation.fab"
Content-Transfer-Encoding: base64
Content-Description: donation.fab (DeskFab 6
Document)
Content-Disposition: attachment;
filename="donation.fab"
AasdfAAzxcvAAA1234AA0M8R4KGxGudfghAApoiuAAAS
DFAertyAPgADAP7/CQAGAsdfgAwrtfAA
zxcvAAA1234AA0M8R4KGxGudfghAApoiuAAASDFAerty
APgADAP7/CQAGAsdfgAwrtfAAdfAAzef

[snipped to save space]

4AA0M8R4KGxGudfghAApoiuAAASDFAertyAPgADAP7/C
QAGAsdfgAwrtfAAdfAAzefzxcvAAA123

——=_NextPart_000_01BCB88F.57968E50
```

Bubba, Alexis and Priscilla wandered back up stairs to wait and see, whilst Jonathan sat working on a strategy of how to edit the donation.fab file to get back his laptop, and the top of the range HP deskfab 9GSII without also nuking himself. He reckoned all he'd got to do was edit out the memory module from the desk-fab, by editing donation.fab, and then he'd have it all back with out the nuke.

Jonathan become engrossed in the task at hand.

...

In a splendidly appointed, luxurious penthouse suite, rich in the trappings of wealth and power, in the heart of Washington DC, a bloated congress critter was eating well at the trough. His whores were attentive, dressing him for breakfast, and he had just been bribed $1,000,000 by a telephone company special interest group to throw a few billions in corporate welfare their way.

And that was just before breakfast, before he had even got out of bed!

Now it appeared he had something he should attend to urgently something that had come on his `email address' what-ever one of those was. A minor aide bustled in. The aide seemed quite excited, and explained in fawning tones that a special interest group had mailed him lots of Swiss Francs, SFr 9,000,000 in fact, but that there was something strange... there was no request for favors. He said it was just being printed out now, and perhaps there would be a note with the money.

The congress critter, puffed contentedly on the hookah which one of the whores had lit for him, hmm, yes he could see that this was going to be a good day.

<Fade to blinding white light>

Adam Back <aba@dcs.ex.ac.uk>

EC Foto Love Story

Gabi und Peter wollen einkaufen gehen. Dazu brauchen sie natürlich Geld. Klar, daß Gabi den Peter an den Automaten schickt!

Gut, daß Gabi so schön aufpaßt, damit nichts schief geht mit der PIN. Denn da ist schnell mal ein Finger auf der falschen Taste. Und Gabi will natürlich nicht, daß die anderen lange warten müssen.

Prima Gabi! Du hast ein gutes Herz! Wenn nur alle so mitfühlend wären.

Petra kennt sich mit Computern aus. Hat ja auch nen PC in der Firma. Für den Schwoof heut abend muß aber noch Kohle in den Beutel.

Den Klaus hat sie erst gestern kennengelernt. Ein netter Typ! Hat die Petra auch gleich in seinem schicken roten BMW zur Bank gefahren. Wie lieb von ihm!

Damit Petra nicht überfallen wird, paßt er während der Transaktion gut auf. Was für ein Mann.

Das muß Liebe sein!

Die überwiegende Zahl der EC-Karten-Betrügereien läuft so wie auf unserem Foto: Geheimnummer über die Schulter abgeguckt, dann die Karte geklaut. Auch Fälle, in denen Diebe mit Fernglas oder Minikamera am Geldautomaten an die PIN kamen, sind bekannt. Vorsicht, wenn der Automaten-Nutzer vor ihnen die Tastatur blankzieht! Sie hinterlassen Fingerabdrücke, aus deren Intensität geübte Klauer direkt ihre PIN ablesen können. (Foto: ZKA/nh)

Die ERFA-Kreis-Struktur des CCC e.V.

Irgendwann im Frühjahr 1986 wurde der Chaos Computer Club auch als eingetragener Verein („e.V.“) gegründet. Vor allem das damals eingeführte „zweite Wirtschaftskriminalitätsgesetz“ (WiKg) mit den - bis dato nicht vorhandenen Gesetzen gegen „Ausspähen von Daten“, „Eindringen in Datenverarbeitungsanlagen“ und so weiter ließen es sinnvoll erscheinen, einigermaßen klare Strukturen (Verein), Ziele (Satzung) und Verantwortlichkeiten (Vorstand) zu benennen. Abgesehen davon, erlaubte dies auch, als eigenständige juristische Person ein Konto zu führen, Vereinsräume und Telefonanschlüsse etc.

Die damals in Aussicht stehenden Ermittlungsverfahren (wg. NASA / Span-Hack etc.) sollten klar kanalisiert werden, um eine weitergehende Kriminalisierung der Hackerszene (§129a) zu verhindern und vor allem die Ermittlungsverfahren an (anwaltlich) gerüstete Stellen (Vorstand) zu lenken. Das hat auch soweit ganz gut funktioniert.

Der CCC hat sich damals in der Sicht seiner selbst u.a. als Forum der Hackerszene definiert, der über die Datenschleuder, den Chaos Communication Congress und natürlich die Netzwerke die Gedanken, Forschungsberichte und Aktivitäten der Hackerszene begleitet und – wenn nötig – auch als Vermittler zwischen Hackern, Systembetreibern etc. agiert. Um von vornherein dem ganzen eine möglichst dezentrale Struktur zu geben, kam die Idee auf, regionale und thematische „Erfahrungsaustausch-Kreise“ in die Satzung und Struktur aufzunehmen.

Die regionalen Erfahrungs-Austausch-Kreise (ERFA-Kreise) sollen dabei so eigenständig wie möglich sein und insbesondere ihre Struktur und Organisationsform selbst bestimmen – sei es als eingetragener Verein, lockere Zusammenrottung oder wasauchimmer.

Momentan gibt es in verschiedenen Städten (neben Hamburg in Berlin, Köln, Leipzig, Ulm und Bielefeld, angeblich auch in Mönchengladbach und möglicherweise bald in Frankfurt) feste „Erfa“-Kreise, die sich regelmäßig Dienstag abends treffen.

Prinzipiell müssen nicht alle Mitglieder eines Erfa-Kreises auch Mitglieder des CCC e.V. sein. Lediglich der „Erfa-Repräsentant“, der als Kontaktperson für den CCC e.V. gilt, muß Mitglied des CCC e.V. sein. Es gibt natürlich auch in anderen als den aufgeführten Ballungsräumen Mitglieder und Interessierte an Treffs und Erfahrungs-Austausch im CCC. Für den CCC e.V. selbst ist es allerdings eher

schwierig, einen solchen regionalen Erfa-Kreis ins Leben zu rufen.

Daher empfehlen wir das Prinzip der self fulfilling prophecy: Wer immer in seiner Region einen Erfa-Kreis vermißt, oder einen aufmachen will und Mitglied des CCC e.V. ist, kann sich hierzu per EMail (ccc@ccc.de) erkundigen bzw. selbiges bekundigen. Nach Abschluß aller Sicherheitsüberprüfungen machen wir dann den obligatorischen Dienstag-Treff im Web und in der Datenschleuder bekannt.

Da sich kontinuierliche Arbeit und Koordination schwerlich in einem Cafe oder einer Kneipe realisieren läßt und die Kommunikation unter Computerfreaks meist nicht besonders kompatibel zu „normalen“ sozialen Standards ist (wie z.B. die Eigenschaft, sich gegenseitig in lauteren Tonlagen die Meinung zu sagen oder das Mitführen allzuvieler elektronischer Geräte) ist die Anmietung eigener Räume o.ä. oft irgendwann sinnvoll.

Hierfür stehen allerdings die knappen Mittel des CCC e.V. nicht zur Verfügung. Es gibt lediglich eine Vereinbarung, nach denen die Hälfte der Mitgliedsbeiträge der Erfa-Kreis Mitglieder an den Erfa-Kreis geht. Dies setzt allerdings voraus, daß Mitglieder des CCC e.V. sich diesem gegenüber (z.B. per mail an office@ccc.de) zu einem Erfa-Kreis zugehörig erklären, damit dies entsprechend zur Verarbeitung/Weiterleitung der Beiträge vermerkt werden kann.

Unabhängig davon können natürlich regionale Erfa-Kreise Gelder einsammeln wie sie lustig sind um eigenen Projekte, Räume etc. zu finanzieren und sich dafür eine eigene Struktur schaffen.

Der Erfa-Kreis Berlin beispielsweise agiert als Chaos Computer Club Berlin e.V. und erhebt nicht nur erhöhte Mitgliedsbeiträge um die Räume zu finanzieren, sondern macht einmal im Monat auch eine Radiosendung.

In Zukunft sollte sich die die durch die Erfa-Kreise entstehende dezentrale Struktur auch mehr im Web kenntlich machen. Für anerkannte Erfa-Kreise werden entsprechende Subdomains vergeben (z.B. berlin.ccc.de), die von Erfakreisen verwendet werden können, eigene Ansprechpartner bereitzustellen und einen gezielten regionalen Kontakt zu pflegen. Im wesentlichen sollte dies aus einer Informationsseite im Web, einem Info-EMail-Robot (info@...), einer Mailadresse für Anfragen (ccc@…) und einem internen Mailverteiler (intern@...) bestehen.

Auf dem diesjährigen Congress werden wir versuchen, nicht nur die bestehenden Erfa-Kreise kurz vorzustellen, sondern auch die regionalen Lücken zu schließen.

andy@ccc.de
tim@ccc.de

HIP '97 Rückblick

Schon viel ist geschrieben worden über die HIP: im Spiegel, in der c't und natürlich vor allem im Netz. Und alle warfen sie ein Licht auf den einen oder anderen Aspekt, doch gelang es keinem Artikel, die Athmosphäre, die auf dem holländischen Campingplatz herrschte, treffend zu beschreiben. Auch ich werde dabei scheitern. Warum? Wegen der vielen Multiversen. Doch dazu später.

Zunächst ein paar sogenannte Fakten, basierend auf den Aussagen der Veranstalter. Rund 1500 Leute wurden am professionell organisierten Eingang mit dem obligatorischen Ausweis versehen, der von einigen frisch gehackten Perl-Skripten in Echtzeit produziert wurde. By default wurde man als „Freiwilliger" eingestuft, Sonderstatus gab es für andere Wesen, wie z.B. die Polizei, die einwilligte, sich mit orangen Ausweisen für alle kenntlich zu machen. Die überaus große Beliebtheit dieser Ausweise führte dann aber schnell zu einer unkontrollierbaren Flut von Pseudopolizisten, so daß mal wieder nichts wahr und alles erlaubt war.

Die 1500 Leute brachten auch 1500 Rechner mit - soviele wurden später gleichzeitig auf dem Ethernet gezählt. Diesen Rekord darf die HIP für sich verbuchen: das größte Ad-Hoc-Open-Air-Netzwerk der Welt mit immerhin 720 KByte / sec Internetzugang! Pfiffig wurde das Problem der IP-Nummern-Vergabe gelöst. Für jede Nummer gab es eine passende Wäscheklammer, auf der die Zahlenfolge mit Filzi vermerkt war. Doppelbelegung ausgeschlossen und selbstdokumentierend. Ein Konzept, das sich sicherlich auch auf dem Chaos Congress durchsetzen wird.

Die bereitgestellte Infrastruktur war vom Start weg den gierigen Hackern ausgeliefert. Der portable Telefonzellenblock der PTT (10 Kabinen!) sollte eigentlich den Telefonkartenabsatz fördern. Es dauerte allerdings keine drei Stunden bis die Nachricht über den Platz ging, daß man nach Wahl einer Notrufnummer einen neuen Wählton bekam und danach beliebige Nummern anwählen konnte – kostenlos natürlich. Schnell wurde klar, was dieser Platz an Potential angesammelt hat.

Und so ging es weiter. Das nächste Ziel lautete „Hack-Me", oder genauer: hackme.campsite.hip97.nl. Dieser spartanisch ausgestattete Linux-386-Rechner bot sich der versammelten Hackerschaft als Objekt der Begierde feil und hielt wider Erwarten bis zum letzten Tag durch. Es gelang niemandem, die „Intruder-Alert"-Lampe, die auf dem Rechner montiert war, durch eine Hackattacke zum Leuchten zu bringen.

Viel Schnickschnack wohin es das Auge auch trieb: das HIPcar scannte per Videokamera die Umgebung und eine „Künstlerin" ließ Computerfreaks ihre Vorstellung von Cyberspace in Knete festhalten. Die obligatorischen HIP-T-Shirts fanden

reißenden Absatz – genau wie die in Massen aufgefahrene Coffein-Schock-Cola Jolt.

Im Mittelpunkt des Platzes eine Stätte der Ruhe: Bill Gates' Grab. Diese unerwartete Gewißheit über das Hinscheiden des meistgehaßten Individuums führte zu wahrhaft rührenden Prozessionen zu diesem kleinen Fleck Erde. Linux- und Macintosh-Anhänger fanden dort zu einer kollektiven Gefühlswelt, die man treffend nur mit dem englischen Wort „Relief" beschreiben kann.

Doch welches Gadget man auch betrachtete: den tiefsten Eindruck von allem hinterließen die Teilnehmer selbst. In aberwitzigen Zeltkonstruktionen machten sie aus dem Platz ein wahrhaftiges Rechenzentrum. Stellt Euch das einfach mal vor, Ihr, die Ihr Euren Arsch nicht hochgekriegt habt, um an diesem seltenen Ereignis teilzunehmen: die Gemeinde „Cyberspace", die Virtual Community, saß leibhaftig Chip an Chip und feierte ihre dreitägige Inkarnation bevor sie wieder in das Internet dif-

fundierte. Auch hier beschlich mich wieder ein englisches Wort, das man nur ungenügend ins Deutsche übersetzen kann: strange.

Kommen wir zur Manöverkritik. Eigentlich verstand sich die HIP ja als Kongreß: zahlreiche Workshops und Vorträge standen auf der Tagesordnung. Ein Minuspunkt war die unzureichende akustische Ausleuchtung des übergroßen Zirkuszelts, das sicherlich sehr cool war (aber dafür viel zu heiß!). Das Resultat war, daß man viele Vorträge nur sehr schlecht verstehen konnte (von den eingeschränkten Englisch-Kenntnissen der internationalen Referenten ganz zu schweigen).

Das Workshop-Zelt bot dafür die gewünschte Nähe zum Vortragenden, doch wurde es hier schnell zu eng. Die Weitläufigkeit des Platzes und die Hitze taten ihr übriges, das offizielle Programm an einem vorbeilaufen zu lassen. So konnte die HIP ihr eigentliches Ziel, nämlich eine große Öffentlichkeit für die Themen der Hacker zu finden, nur beschränkt erfüllen. Das Internet, so scheint es, ist dann doch der effektivere Ort, um sich mit Informationen zu betanken.

Der klare Vorteil der HIP '97 ist aber unbestritten: you meet the players!

tim@ccc.de

Dreiundzwanzig

Es war einmal, vor gar nicht all zu langer Zeit, da passierte das, was niemand wollte: Hacker gaben auf ihre heilige Hackerethik einen Scheiß und karrten ihre Protokolle in den Osten für Geld. Der Himmel hing schief im Hackerland und viele Leute schrieben vieles über einen Sachverhalt, den so recht keiner begriff, über den aber jeder was erzählen wollte.

Am Ende der Geschichte stand der mysteriöse Tod des Hackers Karl Koch, der verbrannt in einem Wald bei Hannover aufgefunden wurde. Der SuperGAU war eingetreten und die Presse drehte nun natürlich ganz durch.

Hacker wollten Weltfrieden sichern

Viele mehr oder wenig schlecht recherchierte Bücher sind zu dem Thema erschienen (z.B. „Hacker für Moskau“, „Das Kuckucksei“) doch blieb die Geschichte sicherlich für die meisten immer noch sehr verworren. Was sie auch war.

Fast zehn Jahre später wird die Öffentlichkeit die Geschichte von Karl in einem neuen Aufguß in den deutschen Kinos vorfinden. „23“ heißt dieser Film und trägt im Untertitel den Satz, den wir dieses Jahr nicht ohne Hintergedanken auch als Kongreßmotto ausgewählt haben: Nichts ist wahr, alles ist erlaubt.

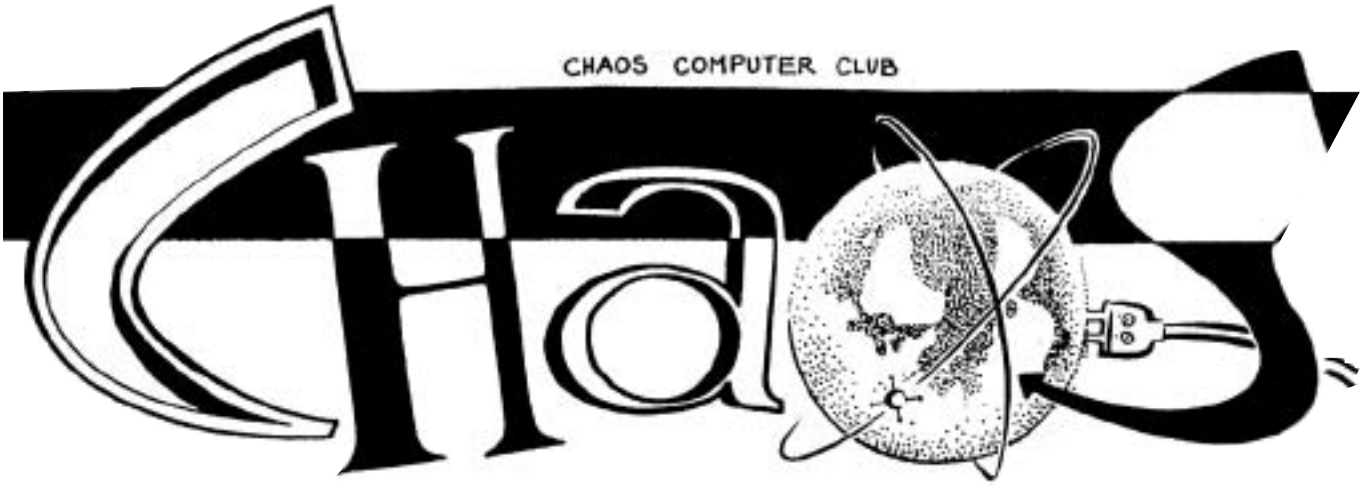
Über den Film, der im Moment gerade gedreht wird, wollen und können wir hier nicht viel sagen. Nur dieses: es ist die Geschichte von Karl und kein detailliertes Protokoll des KGB-Hacks und damit auch nur eine Meinung von vielen. Doch uns ist bewußt, daß dieser Film wieder viele Fragen aufwerfen wird, die nach Klärung und Diskussion verlangen.

Auf dem Chaos Communication Congress in diesem Dezember werden wir daher den Film in einer vorläufigen Rohfassung zeigen und zur Diskussion stellen.

Wer sich mit der Geschichte der damaligen Ereignisse befassen möchte, der sei auf die Dokumentation zum Tod von Karl Koch verwiesen, die beim Chaos Vertrieb erhältlich ist.

WENN DIE NACHT AM TIEFSTEN, IST DER TAG AM NÄCHSTEN.

tim@ccc.de



Communication Congress '97

Nichts ist wahr, alles ist erlaubt!

27.-29. Dezember 1997
Eidelstedter Bürgerhaus
Hamburg Eidelstedt

Geplante Themen

Karl Koch als Kinofilm, Packet-Radio, Kommerzielle Funkdienste, Hacking Chipcards auf die eine oder andere Methode, Carwalking, EC–Karten Unsicherheit, Lockpicking, IP für Anfänger und Fortgeschrittene, 1998 und neue Netzbetreiber, Premium Rate Services, Netzanschluß der Zukunft (ADSL, XDSL etc.), Roboter und Haustiere der Zukunft, Perl as a hacker tool, Krypto Reglementierung und Hintergründe, GSM-Hacking, Satelliten-Lauschen, Pay-TV Hack & Crack, Techno-Terrorismus, Wirtschaftsspionage, Open Souce Information Processing: Geheimdienst selbstgebaut, ISDN-Kryptodevice Vorstellung, Mobilfunk für Fortgeschrittene, Lynchen & Umgang mit Spammern, Kampf dem DNS-Monopol u.a.

Special Event: Deutsche Meisterschaften im Lockpicking

Eintrittspreise

Ideal Standard **DM 42**
Mitglieder d. CCC e.V. **DM 23**
Presse **DM 75**
Gewerbliche Teilnehmer **DM 200**
Schüler, Zuvieldienstleistende, Rentner **DM 30**

Postvertriebsstück C11301F

Der Mitgliedsfetzen

Mitgliedsanträge und Datenschleuderabonnement

o Satzung + Mitgliedsantrag
(DM 5,00 in Briefmarken)

o Datenschleuder-Abo
Normalpreis DM 60,00 für 8 Ausgaben

o Datenschleuder-Abo
Ermäßigter Preis DM 30,00 für 8 Ausgaben

o Datenschleuder-Abo
Gewerblicher Preis DM 100,00 für 8 Ausgaben
(Wir schicken eine Rechnung)

Die Kohle liegt

o in bar
o als Verrechnungsscheck
o in Briefmarken

bei bzw.

o wurde überwiesen am ___.___.____ auf
Chaos Computer Club e.V., Konto 59 90 90-201
Postbank Hamburg, BLZ 200 100 20

Ort/Datum _____

Unterschrift _____

Name _____

Straße _____

PLZ, Ort _____

Tel/Fax _____

E-Mail _____

Der Bestellfetzen

Alle Bestellungen und Mitgliedsanträge an:
CCC e.V., Schwenckestr. 85, D-20255 Hamburg

Literatur

_____	DM 42,00	Mailbox auf den Punkt gebracht
_____	DM 29,80	Deutsches PGP-Handbuch, 3. Auflage + CD-ROM
_____	DM 5,00	Doku zum Tod des „KGB“-Hackers Karl Koch
_____	DM 25,00	Congressdokumentation CCC ‘93
_____	DM 25,00	Congressdokumentation CCC ‘95
_____	DM 50,00	Lockpicking: Über das Öffnen von Schlössern

Alte Datenschleudern

_____	DM 50,00	Alle Datenschleudern der Jahre 1984-1989
_____	DM 15,00	Alle Datenschleudern des Jahres 1990
_____	DM 15,00	Alle Datenschleudern des Jahres 1991
_____	DM 15,00	Alle Datenschleudern des Jahres 1992
_____	DM 15,00	Alle Datenschleudern des Jahres 1993
_____	DM 15,00	Alle Datenschleudern des Jahres 1994
_____	DM 15,00	Alle Datenschleudern des Jahres 1995
_____	DM 15,00	Alle Datenschleudern des Jahres 1996

Sonstiges

_____	DM 50,00	Blaue Töne / POCSAG-Decoder / PC-DES Verschlüsselung
_____	DM 5,00	1 Bogen „Chaos im Äther“
_____	DM 5,00	5 Aufkleber „Kabelsalat ist gesund“

+ DM 05,00 Portopauschale!

_____ Gesamtbetrag

Die Kohle liegt

o in bar
o als Verrechnungsscheck

bei bzw.

o wurde überwiesen am ___.___.____ auf
Chaos Computer Club e.V., Konto 59 90 90-201
Postbank Hamburg, BLZ 200 100 20

Name _____

Straße _____

PLZ, Ort _____