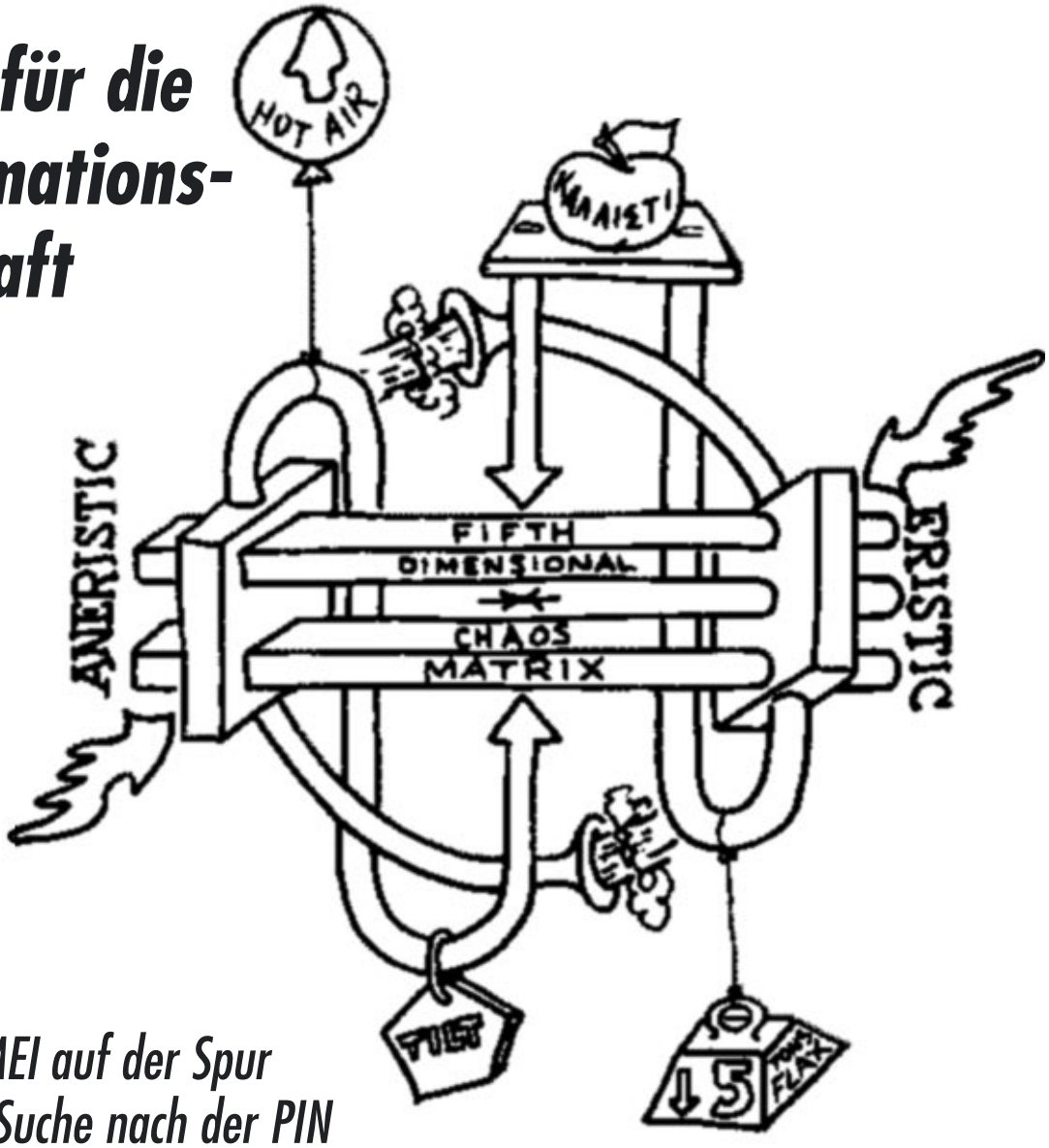
Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club

Nahrung für die Desinformations-gesellschaft



- *GSM: Der IMEI auf der Spur*
- *EC: Auf der Suche nach der PIN*
- *Bastelecke: UniProg Universalprogrammer*

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

#61

Impressum

Die Datenschleuder Nr. 61
IV. Quartal, Dezember 1997

Herausgeber:
(Abos, Adressen etc.)
Chaos Computer Club e.V.,
Schwenckestr. 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:
Andreas Bogk (andreas@ccc.de), Andy Müller-Maguhn (andy@ccc.de), Frank Rieger (frank@ccc.de), Tron (tron@ccc.de), Tim Pritlove (tim@ccc.de), Tobias (tobias@ccc.de), Wau Holland (wau@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, Aufzeichnungen der Sendungen im Internet abrufbar, Feedback an 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 Suecrates, EMail norman@delos.stgt.sub.org.

Österreich: Public Netbase, http://www.t0.or.at/

Engagierte ComputerexpertInnen, Postfach 168, A-1015 Wien.

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

Editorial

Hallo Chaoten,

diese Welt ernst zu nehmen wird einem manchmal gar nicht leicht gemacht (siehe Meldung rechts).
Und trotzdem immer wieder: nein, bitte kein Kryptoverbot, nein, bitte keine Security by Obscurity, nein, bitte keine Online-Zensur, und so weiter und so fort.

Ein Dauerbrenner dieses Jahres ist die EC-Karte. Langsam schwant auch dem letzten, daß das wohl alles nicht so klug war, was sich die Herren da vor einigen Jahren ausgedacht haben. Nun knistert's in der Büchse der Pandora und wir können nur darauf hinweisen, daß wir es ja gleich gesagt haben. Aber auf uns hört ja keiner.

Keiner? Gemessen an der Last, die unser Web Server in den letzten Monaten zu vertragen hatte und an der Zahl von Anfragen, die uns täglich per EMail erreichen zeichnet sich ein anderes Bild am Horizont ab. Durch die Ausweitung des Internet und der wachsenen Aufmerksamkeit der Gesellschaft für Medien- und Sicherheitsproblematiken, hat der CCC als Vermittler alle Hände voll zu tun. Doch das dezentrale System des Clubs erweist sich gerade hier als relativ robust. Viele Fragen können beantwortet werden, wenn auch nicht alle.

Und noch was: Voranmeldungen zum Congress können durch eine Überweisung des Eintrittspreises auf das Konto 599090-201, BLZ 200 100 20, Postbank Hamburg unter Angabe des Namens (wichtig) getätigt werden. Natürlich könnt Ihr auch an der Abendkasse zahlen. Die offizielle Ankündigung findet Ihr hinten im Heft.

Aktuelle Informationen zum Congress finden sich bald auf http://www.ccc.de.

Keep The Faith!
Fnord?

Index

Hodge-Podge Transformer	❐❐❐❐❐		
Impressum	❐❐❐❐■	Bastelecke: UniProg	❐■■■❐
Adressen	❐❐❐❐■	EC: Auf der Suche nach der PIN	■❐❐❐■
Editorial	❐❐❐■❐	offset.c	■■❐❐❐
CRD Kurzmeldungen	❐❐❐■■	Liebe Telekom	■■❐❐■
Microsoft Press Release	❐❐■■❐	Leserbriefe	■■❐■❐
eMailPress Kurzmeldungen	❐❐■■■	VSt Watch	■■❐■■
Corporate Message Recovery	❐■❐❐❐	Literaturhinweise	■■■❐■
Deutsche Kryptopolitik	❐■❐❐■	CCC '97 Ankündigung	■■■■❐
Der IMEI auf der Spur	❐■❐■■	Mitgliedsfetzen	■■■■■
Wissenswertes zu Mobiltelefonen	❐■■❐■	Bestellfetzen	■■■■■

Chaos Realitäts Dienst: Kurzmeldungen

Hackers break into NYC subway electronic message signs

NEW YORK (October 24, 1997 00:16 a.m. EDT) -- Electronic signs telling subway riders to "Watch your step" and "Have a great day" were flashing confusing messages Thursday because of computer hackers.

The signs at a Manhattan subway station briefly displayed the message, "Volume Fourteen, Number Three," and "The Hacker Quarterly."

"The Hacker Quarterly" is a Long Island-based magazine that chronicles the activities of computer hackers. It was not clear what the message was meant to convey.

Editor Emmanuel Goldstein said he knew nothing of the incident.

"I hope nobody was confused and thought it came from us," said Goldstein, whose magazine offers tips on hacking into computer systems but does not condone destructive behavior.

The electronic signs have been invaded before, said Julio Lussardi, a Transit superintendent.

"It's more of a nuisance than anything else," Lussardi said.

Panne bei neuer EC-Karten Software

Anfang November (Montag 4.11.) gab es in der Genossenschaftlichen Rechenzentrale (GRZ) in Ahlen (Nähe Hannover) bei der Einspielung neuer Software für die Geldautomaten (GAA) ein kleines Softwareproblem. Rund 13.000 Kunden wurde bei einer Verfügung einfach der hundertfache Betrag vom Konto abgezogen.

Betroffen waren, wie aus gewöhnlich gut unterrichteten Kreisen zu erfahren war, nicht nur Kunden von Volks- und Raiffeisenbanken aus Niedersachsen, Hamburg, Schleswig-Holstein, Bremen, Mecklenburg-Vorpommern, Sachsen-Anhalt und Brandenburg, die am Montag ihre Scheckkarte benutzt haben, sondern auch ein Mitarbeiter des Rechenzentrums selbst. Als der Kauf eines Fahrrads über 380.- DM zum Anruf seiner kontoführenden Bank aufgrund überschreitens der Dispogrenze mit der 38.000 DM Lastschrift führte, glaubte man offenbar auch dort an eine Unregelmäßigkeit.

Die Falschbuchungen seien aber bereits storniert und niemand müsse einen Schaden befürchten, gab der Leiter des Rechenzentrums bekannt. Die fehlerhafte Software hatte insgesamt statt 2,7 Millionen Mark 270 Millionen abgezogen und Geschäften sowie Tankstellen gutgeschrieben.

(Wenn die Zahlen aus den Agenturmeldungen stimmen – 13000 Kunden an einem Tag mit Gesamtumsatz 2.7 Mio DM – sind das im Schnitt knapp über 200.- DM pro Kunde)

BXA RFC on Export Controls

"The Bureau of Export Administration (BXA) is reviewing the foreign policy-based export controls in the Export Administration Regulations to determine whether they should be modified, rescinded or extended. To help make these determinations, BXA is seeking comments on how existing foreign policy-based export controls have affected exporters and the general public."

`http://jya.com/bxa100897.txt`

John Young <jya@pipeline.com>
October 10, 1997

Abhör- & Überwachungssysteme

Nicht nur das amerikanische Echelon-System zeigt, in welche Richtung sich das Abhören von Telekommunikationsverbindungen entwickelt; es werden nicht mehr gezielt Anschlüsse überwacht, sondern der *gesamte* Verkehr wird nach entsprechenden Stichworten durchsucht, bzw. nach entsprechenden Verbindungsdatensätzen strukturiert betrachtet.

Die technischen Fortschritte auf dem Gebiet der maschinellen Spracherkennung und der Einsatz sog. "Wortbanken" (BND-Sprachgebrauch, im Englischen heißt es "word spotting") sind enorm. Auch vollautomatische Zusammenfassungen/Einordnungen ganzer Gespräche sind durch "Natural Language Processing" mittlerweile möglich.

Ein Papier von David A. James von der Universität Cambridge ist jetzt im Netz verfügbar:

`ftp://svr-ftp.eng.cam.ac.uk/pub/reports/james_thesis.ps.Z`

Neues Einsatzgebiet für den Militärischen Abschirmdienst

Der militärische Abschirmdienst (MAD) hat offenbar ein neues Einsatzgebiet: die Aufdeckung rechtsextremistischen Verhaltens bei der Bundeswehr.

Die Unterscheidungskriterien zum dort "normalen" Verhalten sind uns zwar nicht bekanntgeworden, dafür aber eine kleine Beobachtung am Rande: beobachtet und überwacht werden offenbar auch die, die das schon vorher beobachtet haben: nämlich entsprechende Journalisten.

Wer hier wen mit welcher Motivation ausspäht, kann schlußendlich wohl nur spekuliert werden.

Singapore TOILET ALERT

SINGAPORE (Reuters) - A drive to keep public toilets clean and dry is meeting with overwhelming success, the Ministry of Environment said in a "toilet alert" Tuesday.

Chaos Realitäts Dienst: Kurzmeldungen

The statement said that in the first week "5,000 Singaporans have called the Clean Public Toilets hotline to identify Singapore's model toilets and to vote for their top five favorite toilets." The ministry launched a poster competition earlier in the month featuring three model toilets and inviting the public to identify their locations, as well as to nominate their favorite public toilets in five categories of locations. Various prizes are involved, including a return trip to Hong Kong to be won in a draw. Singapore is known for public campaigns promoting causes ranging from discouraging littering to encouraging people to have more children.

22 Oct 1997, declan@well.com, http://netlynews.com/

US Terrorist Targets

US State Department today published the latest list of terrorist organizations (and multiple aliases) which are now targets of sanctions:

`http://jya.com/dos100897.txt`

And related foreign assets control announcement:

`http://jya.com/fac100897.txt`

08 Oct 1997, John Young <jya@pipeline.com>

Abhörsicherheit – ein Zusatzprodukt der Telekom

Für "Kunden, die einen erhöhten Sicherheitsanspruch oder einen konkreten Abhörverdacht haben" bietet die Telekom jetzt auch die Suche nach illegalen Abhöreinrichtungen als Dienstleistung an. Auf ausdrückliche Nachfrage eines Datenschleuder-Redakteurs auf der SITEC´97 (Sicherheitsmesse) in Berlin werden allerdings tatsächlich nur Maßnahmen gegen illegales Abhören angeboten. Insofern ein eher unattraktives Produkt, allerdings mit einer recht anschaulichen Broschüre, der wir hier ein paar Bilder entnommen haben.

Für den unwarscheinlichen Fall, daß es doch jemanden interessiert:

`http://www.telesec.de`

crd@ccc.de

Quellen im Netz

Polizei Baden-Württemberg. Ohne Worte.

`http://www.polizei-bw.de/virtuell.htm`

Amtsblätter des BMPT – im wirklichen Leben deutlich schwieriger zu bekommen:

`ftp://ftp.cs.tu-berlin.de/pub/doc/telekom/amtsblatt/`

Europol-Protokoll & Vertrag

`http://www.datenschutz-berlin.de/jahresbe/96/texte/egc316.htm`

Text des deutschen Europol-Gesetzes

`http://www.datenschutz-berlin.de/jahresbe/96/texte/europol.htm`

Das (in Deutschland noch nicht beschlossene) Zusatzprotokoll über die Immunität von Europol (der Hammer):

`http://www.infolinks.de/cilip/ausgabe/57/protokol.htm`

Microsoft Press Release

REDMOND, Wash.--Oct. 21, 1997-- In direct response to accusations made by the Department of Justice, the Microsoft Corp. announced today that it will be acquiring the federal government of the United States of America for an undisclosed sum.

"It's actually a logical extension of our planned growth," said Microsoft chairman Bill Gates. "It really is going to be a positive arrangement for everyone."

Microsoft representatives held a briefing in the oval office of the White House with U.S. President Bill Clinton, and assured members of the press that changes will be "minimal." The United States will be managed as a wholly owned division of Microsoft. An initial public offering is planned for July of next year, and the federal government is expected to be profitable by "Q4 1999 at latest," according to Microsoft president Steve Ballmer.

In a related announcement, Bill Clinton stated that he had "willingly and enthusiastically" accepted a position as a vice president with Microsoft, and will continue to manage the United States government, reporting directly to Bill Gates. When asked how it felt to give up the mantle of executive authority to Gates, Clinton smiled and referred to it as "a relief." He went on to say that Gates has a "proven track record," and that U.S. citizens should offer Gates their "full support and confidence." Clinton will reportedly be earning several times the $200,000 annually he has earned as U.S. president, in his new role at Microsoft.

Gates dismissed a suggestion that the U.S. Capitol be moved to Redmond as "silly," though did say that he would make executive decisions for the U.S. government from his existing office at Microsoft headquarters. Gates went on to say that the House and Senate would "of course" be abolished. "Microsoft isn't a democracy," he observed, "and look how well we're doing.

When asked if the rumored attendant acquisition of Canada was proceeding, Gates said, "We don't deny that discussions are taking place.

Microsoft representatives closed the conference by stating that United States citizens will be able to expect lower taxes, increases in government services and discounts on all Microsoft products.

About Microsoft: Founded in 1975, Microsoft (NASDAQ "MSFT") is the worldwide leader in software for personal computers, and democratic government. The company offers a wide range of products and services for public, business and personal use, each designed with the mission of making it easier and more enjoyable for people to take advantage of the full power of personal computing and free society every day.

About the United States: Founded in 1789, the United States of America is the most successful nation in the history of the world, and has been a beacon of democracy and opportunity for over 200 years. Headquartered in Washington, D.C., the United States is a wholly owned subsidiary of Microsoft Corporation.

eMailPress: Kurzmeldungen

/emp 29.09.97 – Die CCC-Mehrfrontendiplomatie bezüglich der dBox ist schwierig. Grob vereinfacht hier eine Rechtsauffassung des CCC: für jeden technisch versierten Besitzer einer dBox ist es nach dem letzterwähnten Update dringend notwendig, die Software auszulesen, zu zerlegen und verbessert wieder ins Gerät zu schicken (Bauplan Datenschleuder 60). Denn man hat als Besitzer das Recht, u.a. die bezahlte und später durch Update entfernte Funktionalität der dBox "Video-CD abspielen" selbst wiederherzustellen. Die Auffassung einiger Mitarbeiter von Premiere, Telekom, DF1 und Beta-Research, das könnte "Softwarediebstahl" sein, ist insofern nicht haltbar. Richtig ist jedoch, daß der CCC an korrektem diplomatischem Umgang mit diesen Mediengiganten auch dann interessiert ist, wenn man unterschiedliche Meinungen hat.

/emp 30.09.97 - Der CCC ist bei Fragen der Kryptosicherheit nicht nur mit den Banken solidarisch, sondern auch mit den Pay-TV-Betreibern. "Schwache Verschlüsselung" kann ihnen nicht zugemutet werden. Pay-TV-Betreiber haben wie jeder Bürger das Recht auf "starke" Verschlüsselung mit mehr als nur 40 oder 56 Bit. Denn nur diejenigen Pay-TV-Systeme taugen etwas, die gegen Angriffe von Piraten "gehärtet" sind. Es hat doch keinen Zweck, Pay-TV mit Verfahren zu verschlüsseln, die heute jeder bessere Geheimdienst binnen Minuten knackt und morgen kann das jeder. Im Zeitalter der frei programmierbaren Computer mit ständig steigender Rechenleistung sind die von der EU geplanten "Verbotsschilder" für Entschlüsselungsversuche schlicht und ergreifend Unfug und behindern den technischen Fortschritt bei der Kryptoforschung. Zuwenig bedacht wird dagegen ein Pferdefuß: Denn je perfekter die Verschlüsselung, desto gründlicher ist die Überwachung. Pay-TV macht Einzeladressierung und -abschaltung noch perfekter als beim Militär mit AFN-TV. Was beim Militär die "Verstanden"-Meldekette war, wird das Modem an der dBox. Der Anschluß des Fernsehers ans Telefon ohne Kontrolle, welche indirekten Informationen darüber zurückfließen, ist in seinen Konsequenzen noch nicht durchdacht. Welchen Zugriff staatliche Stellen auf so gesammelte Bits und Zeitverläufe haben dürfen, ist ebenfalls ungeklärt. Um es überspitzt zu formulieren: bei Ausstrahlung von Pornos, die nachträglich klassifiziert werden als "dem Besitzverbot unterliegend", könnten anhand der Dekoderdaten Kundenadressen ermittelt und Hausdurchsuchungen angeordnet werden. Denn die Möglichkeit der Aufzeichnung hat ja bestanden.

/emp 01.12.1997 - Seit den ersten oberirdischen Atombombentests sind die zerstörenden Auswirkungen des "elekromagnetischen Pulses" (EMP) auf elektrische Geräte bekannt. Inzwischen ist es in Thüringen gelungen, diesen Effekt ohne die atomaren Nebenwirkungen zu erzeugen. Ein in einen Rucksack passendes, etwa 20 kg schweres steckdosentaugliches Gerät zerstört zuverlässig alle elektronischen Geräte im Nahfeld. Damit ist die Einrichtung eines abhörsicheren Raumes möglich, der garantiert wanzen- und handyfrei ist. Auf dem Chaos Communication Congress vom 27.-29.12. in Hamburg soll ein Raum dafür reserviert werden. Das Betreten dieses Raumes – insbesondere mit elektronischer Ausrüstung – erfolgt auf eigene Gefahr. Immerhin gab es schon eine Brandblase, als der Siliziumchip einer Uhr versuchte, durch das Plastikgehäuse auf den Arm zu tropfen.

Wau Holland
wau@ccc.de

Corporate Message Recovery

Nach jahrelanger Entwicklungsarbeit war es endlich soweit: die neue Version von PGP, mit der Nummer 5.0 für nichtkommerziellen und 5.5 für kommerziellen Einsatz, erschien. Jetzt ist eine Diskussion um ein neues Feature dieser Version aufgekommen, im Zusammenhang mit der in Anbetracht der bisherigen US-Politik merkwürdigen Export-Freigabe von PGP.

Das neue Feature heißt Corporate Message Recovery (CMR). Es sorgt dafür, daß man public keys so konfigurieren kann, daß Mails, die an den Besitzer dieses Schlüssels geschickt werden, auch mit dem public key eines weiteren Benutzers verschlüsselt werden. Gedacht ist das ganze für Firmen, die gerne PGP einsetzen wollen, aber auch dann noch die Nachrichten eines Mitarbeiters lesen können müssen, wenn dieser vom Bus überfahren wird.

Der Vorwurf wurde laut, PGP hätte jetzt eine Software, die GAK-fähig (Government Access to Keys) sei, und nur deshalb hätte PGP eine Exportgenehmigung bekommen. Mithin seien PGP jetzt die Bösen.

Allerdings bestehen zwischen GAK und CMR gewisse Unterschiede. Der wichtigste Unterschied ist der, daß CMR es zwar dem Besitzer des CMR-Schlüssels erlaubt, die Dokumente zu entschlüsseln, die mit aktiviertem CMR erstellt wurden, nicht jedoch Nachrichten des Original-Schlüsselbesitzers zu fälschen oder gar jede an den Original-Schlüsselinhaber gerichtete Mail zu entschlüsseln.

GAK hingegen erlaubt das, und generell alles, was auch der Original-Schlüsselbesitzer kann. Außerdem bietet CMR die Möglichkeit, ein flexibles, vernetztes System zum Wiederherstellen von Nachrichten zu bilden, es muß mitnichten immer der Firmenchef sein, der alle Nachrichten lesen kann, es kann auch nur der jeweils Vorgesetzte oder ein Kollege sein.

Die Lösung für Skeptiker von CMR ist einfach: der Source von PGP ist verfügbar, und ein Entfernen von 10 leicht zu findenden Zeilen schaltet CMR ab, schließlich findet CMR ja beim Sender statt. Insofern kann man PGP nur dazu gratulieren, eine Lösung für ein Problem geschaffen zu haben, von dem die US-Regierung behauptet, nur GAK könne es lösen. Und diese Lösung kommt ohne die Nachteile von GAK aus.

Und besser als das bisherige Vorgehen der Firmen, einfach eine Sicherheitskopie des private key des Mitarbeiters in den Tresor zu legen, ist CMR allemal.

andreas@ccc.de

Deutsche Kryptopolitik

In der DDR wurde in der Schule gelehrt, daß die Regierung in der BRD im wesentlichen von den Interessen der Wirtschaft bestimmt wird. Nach 1989 stellte sich heraus, daß da noch eine gehörige Anzahl von anderen Lobbygruppen eine Rolle spielt, daß die Regierung aber tatsächlich nichts ernstes gegen die Interessen von Banken, Industrie und ADAC unternehmen kann. Diese Umstände wurden bisher von der Realität nicht widerlegt.

In den letzten Wochen kamen Zweifel auf. Das deutsche Innenministerium verfolgt unbeirrbar das völlig realitätsferne Ziel einer Kryptoregulierung in der einen oder anderen Form. Alle in den USA gescheiterten Vorstöße werden nochmal in Deutschland ausprobiert. Ob Schlüssellängenbegrenzung, Key Escrow, Key Recovery oder staatlicher Verschlüsselungschip mit Hintertür – in den USA längst am Widerstand von Industrie und Aktivisten gescheitert, in Deutschland neu aufgelegt.

Trotz massiver und klarer Stellungnahmen von Banken und Industrie gegen jedwede Form der Beschränking von Kryptographie gibt es offenbar ein starkes eigenständiges Interesse bestimmter Teilbereiche der Regierung daran, das Mitlesen aller Nachrichten bis in alle Zukunft zu ermöglichen. Nur: für wen? Die deutschen Geheimdienste haben schon immer die Möglichkeit gehabt, Informationen an der Quelle abzuschöpfen. Wenn man in eine Telefonverbindung nicht eindringen kann, verwanzt man halt das Telefon, auch wenn das teurer kommt. Das sich die wirklichen Kriminellen nicht von Verboten beeindrucken lassen, sondern die Werkzeuge verwenden, die optimale Ergebnisse bringen, ist bekannt. Die Mafia läßt sich durch das Kriegswaffenkontrollgesetz schließlich auch nicht daran hindern, Leute mit Maschinenpistolen zu erschießen.

All dies wissen die Verantwortlichen im Innenministerium natürlich auch. Wo liegt also der tiefere Grund für ein derart massives Beharren auf einer offensichtlich sinnlosen und nicht durchsetzbaren Regelung?

"Höhere Politk" lautet die gängige Floskel. Das ist sowas ähnliches wie "Nationale Sicherheit". Diese Begriffe werden benutzt, wenn es keine rationalen Gründe für Handlungen mehr gibt, sondern es um reine, absolute Macht geht. Wenn es an die elementaren, nicht-öffentlichen Grundfesten eines Staates geht.

Im Falle des Kryptoverbotes könnte es sich durchaus um geheime Verträge zwischen der Bundesrepublik und den USA handeln, die die Zusammenarbeit in Sicherheits-, Verteidigungs- und Geheimdienstfragen regeln. Daß es solche Verträge geben muß, ergibt sich zwingend aus der Art des Umgehens mit den Abhörstationen der NSA auf deutschem Boden (z.B. in Bad Aibling).

Wie weitreichend die Verträge sind, ist unklar. Nicht unwahrscheinlich ist, daß die deutsche Regierung sich schon zu Zeiten der Gründung der Republik und erneut bei der Neufassung der Verträge 1989 dazu verpfli-

chtet hat, den Amerikanern Mithörmöglichkeiten bis in alle Zukunft zu gewährleisten.

Ohne eine Reglementierung der Verschlüsselung wäre eine solche Verpflichtung nichts mehr wert. Davon, daß die US-Regierung schon in der Frühzeit der Bundesrepublik dafür sorgte, daß die Bundeswehr Verschlüsselungssysteme auf Basis einer modifizierten Wehrmachts-Enigma verwendete, kann man heute ausgehen. Die Erkenntnis, daß die Enigma überhaupt geknackt wurde, war zu diesem Zeitpunkt noch nicht öffentlich.

Die USA haben über die Jahre dreistellige Milliardenbeträge in ihre weltweite Überwachungsinfrastruktur investiert. Die diesem Netz zugrunde liegenden Methoden und Verfahren sind teilweise dem zivilen Stand der Technik Jahre voraus.

Daß dieses Geld nun nicht einfach so als Verlust verbucht werden kann, dürfte klar sein. Die Daumenschrauben, die bei der Gründung der BRD eingebaut wurden, werden offenbar nun angezogen. Die "Bündnisstreue" wird eingefordert.

frank@ccc.de

GSM: Der IMEI auf der Spur

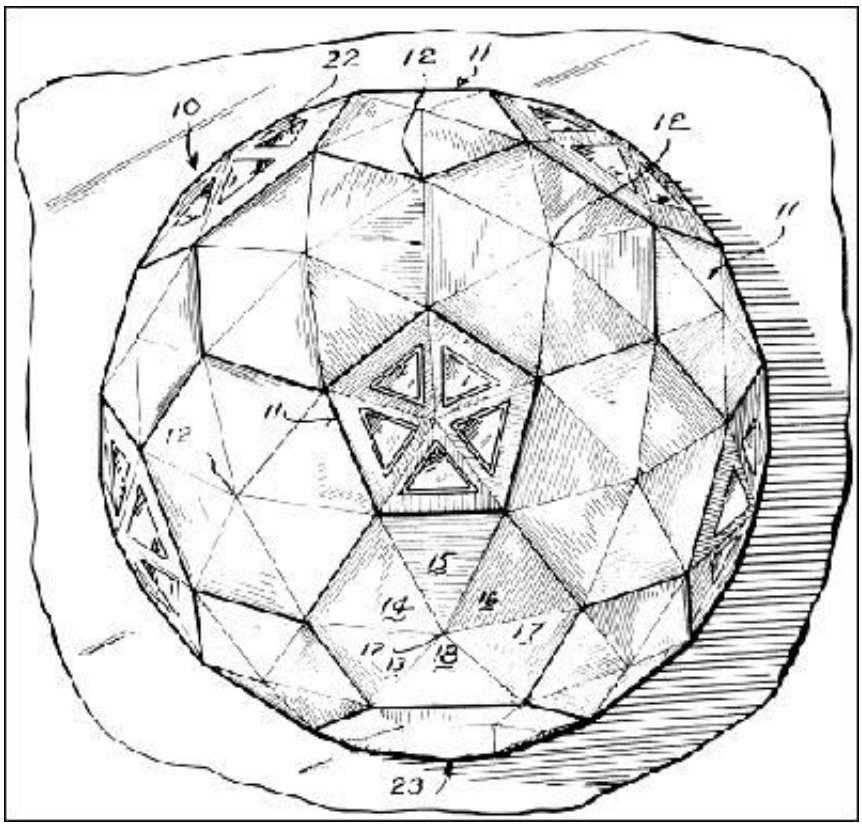
Die Suche nach entwendeten GSM-Telefonen erfolgt zumindest beim D2-Netz auf Wunsch des Kunden im Netz; das entwendete Gerät wird mit seiner Identifikationsnummer (IMEI-– International Mobil Equipment Identity) im Netz geblacklistet.

Wenn der ursprüngliche Inhaber die "Wiederbeschaffung" des Gerätes wünscht und Anzeige wg. Diebstahls gestellt hat, ermittelt D2 den Einbuchversuch des Gerätes mit den dabei anfallenden Daten: Kartennummer et cetera. Jeder Einbuchversuch mißlingt, weil das Gerät vom Netz abgewiesen wird und eine Einbuchung mit der geblacklisteten IMEI nicht möglich ist.

Diese Daten werden dann den Ermittlungsbehörden übermittelt. Offenbar reichen einigen Staatsanwaltschaften – insbesonders in den neuen Bundesländern – diese Daten dann um

Hausdurchsuchungsbeschlüsse bei den Karteninhabern auszustellen.

Damit werden de fakto digitale Daten als beweiserheblich anerkannt, was nur als fragwürdig bezeichnet werden kann. Digitale Daten gelten "normalerweise" als "Dokumente des Augenscheins" mit freier Beweiswürdigung durch den Richter. Das heißt, der Richter muß aufgrund der Umstände eines Falles entscheiden, ob er die digitalen Daten als Beweis anerkennt.



Das Bundesministerium für Forschung und Technologie etwa, hat ja genau deswegen die Signaturverordnung als Gesetz eingebracht, damit digitale Daten bzw. digital unterschriebene Daten einen rechtsverbindlichen Charakter zur Abwicklung von Geschäften über das Netz in Zukunft haben. Insofern ist fraglich, ob die Praxis bei GSM-Telefonen langfristig Bestand hat; schließlich sind IMEIs auch nur digitale Daten, die in irgendwelchen schlecht gesicherten (E)EPROMs der Telefone zu finden und zu verändern sind.

.

Die Datenschleuder
Nummer 61, Dezember 1997

Wissenswertes zu Mobiltelefonen

Die hierzulande verwendete GSM-Technologie samt dazugehörigen Handys bietet dem engagierten Techniker ein breites Einsatzfeld. Im folgenden ein paar Ergebnisse der Feldforschung in diesem Bereich.

Bei fast allen handelsüblichen Telefonen ist die Konfiguration des Gerätes in einem EEPROM im Geräteinneren gespeichert. Bei einem älteren Motorola-Telefon der 5000er Serie sieht daß dann z.B. so aus:

```
EEPROM 8Kbyte

000E-001D  Power Level Table
0052-0059  IMEI
005A-00D3  Flex Data (Konfiguration
           der Leistungsmerkmale)
013B-01BA  Hardware-Info
033F-0357  Begrüssungstext beim
           Einschalten des Gerätes
036F-0371  Security Code (byteweise gedreht)
0372-0373  Unlock Code (byteweise gedreht)
0FBC-1EC7 Phonebook
```

Auf diesem Weg bekommt man bei Motorola-Telefonen die IMEI heraus, die sich nicht, wie eigentlich bei allen GSM-Telefonen vorgesehen, durch Drücken der Tastenkombination *#06# ermitteln läßt.

Interessant ist auch der Bereich "Flex Data". Wenn Motorola beispielsweise für den ja nicht gerade geringen Preis von knapp DM-1000 ein Handy des Types "Traveller" unter die Leute bringt, so hat es trotzdem nicht die Funktion einer Uhr verdient, erst das noch einige Blaue teurere "StarTac 85" hat eine solche.

Nun ist das Nichtvorhandensein der Uhr aber nicht etwa ein Hardwareproblem, nein, die Uhr ist schon eingebaut, sie muß nur noch im Bereich „Flex Data“ aktiviert werden, was ganz einfach durch das Setzen eines Bytes geschieht.

Ähnliche versteckte Features hält auch Ericsson bereit. Durch das Setzen eines einzelnen Bytes bekommt das altbewährte GH337, oh Wunder, einen Taschenrechner spendiert.

In einen Testmodus kommt man beim gleichen Gerät (und möglicherweise auch noch bei anderen Modellen von Ericsson) durch Drücken der Tasten >*<<*<*, es werden zum Beispiel Softwareversionen angezeigt. Einfach mal mit rumspielen, man kann das Telefon in diesem Modus nicht zerstören.

Zum Schluß noch ein Feature zu AEG-Telefonen der neueren Baureihe (9050 und baugleiche D&E-Netz-Geräte). Trägt man in die sich im Telefon befindliche Karte bei Speicherplatz 99 den Namen "FELDTEST" sowie eine beliebige Rufnummer ein, und ruft diesen Eintrag dann auf, hat man von diesem Zeitpunkt an einen Menüpunkt mehr: den DIAGNOSE-Mode.

Viel Spaß beim Spielen

Quark Telefonmann

UniProg – Der Universalprogrammer

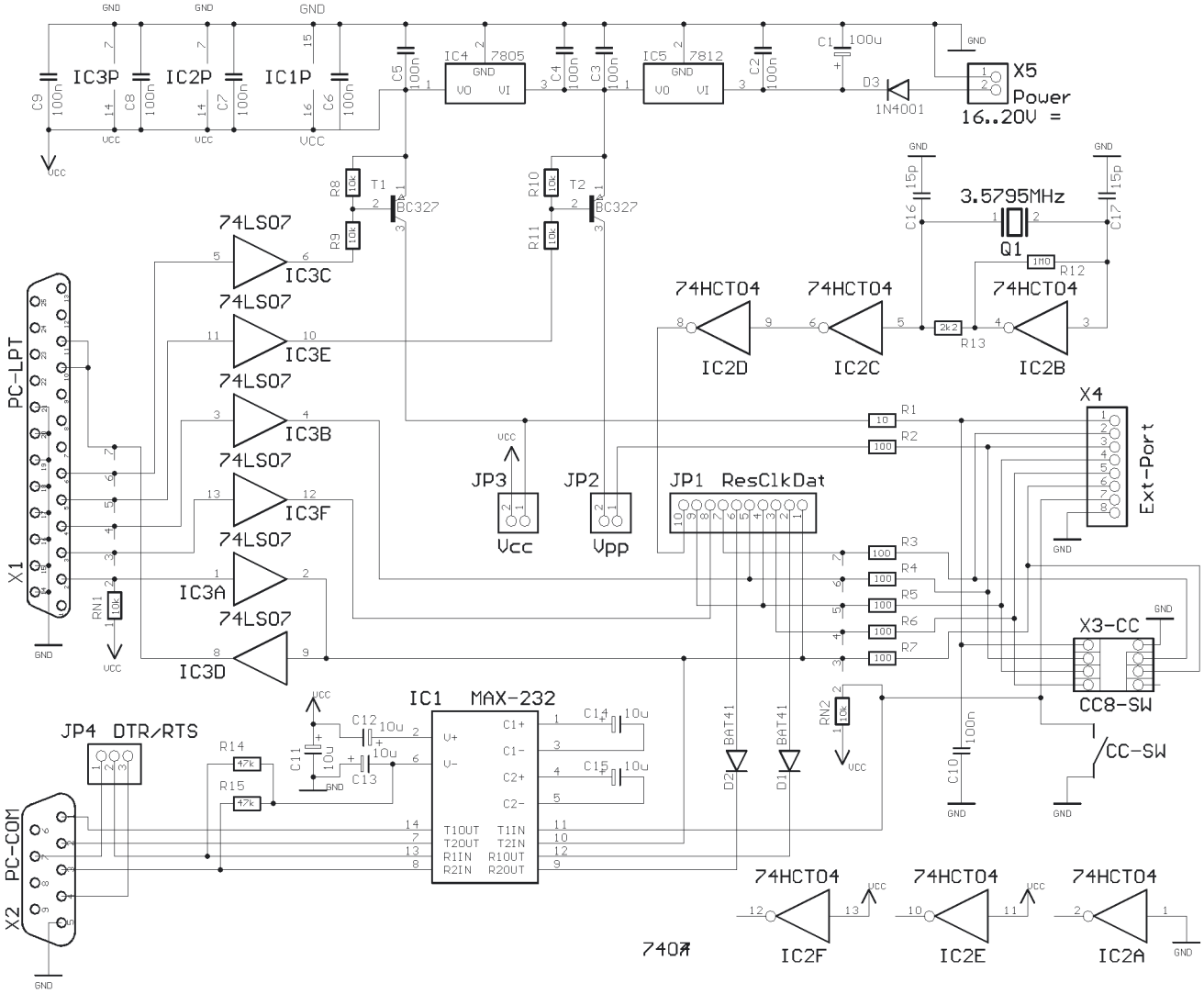
Als Teil 2 unserer Datenschleuder-Bastelserie haben wir diesmal ein kleines Nachbauprojekt für einen universelles Programmiergerät für Chipkarten (Speicher-, Prozessor- und Batteriekarten), EEPROMs (parallel und seriell) und diverse Microcontroller.

Auch die für einige Anwendungsfälle besonders interessanten PIC-Chipkarten lassen sich mit dem UNIPROG problemlos bearbeiten. Wie üblich finden sich auf den nachfolgenden Seiten Layout, Bestückungsplan und Schaltplan. Die Doku und Software für die unterschiedlichen Anwendungsfälle findet sich auf dem CCC-Webserver unter

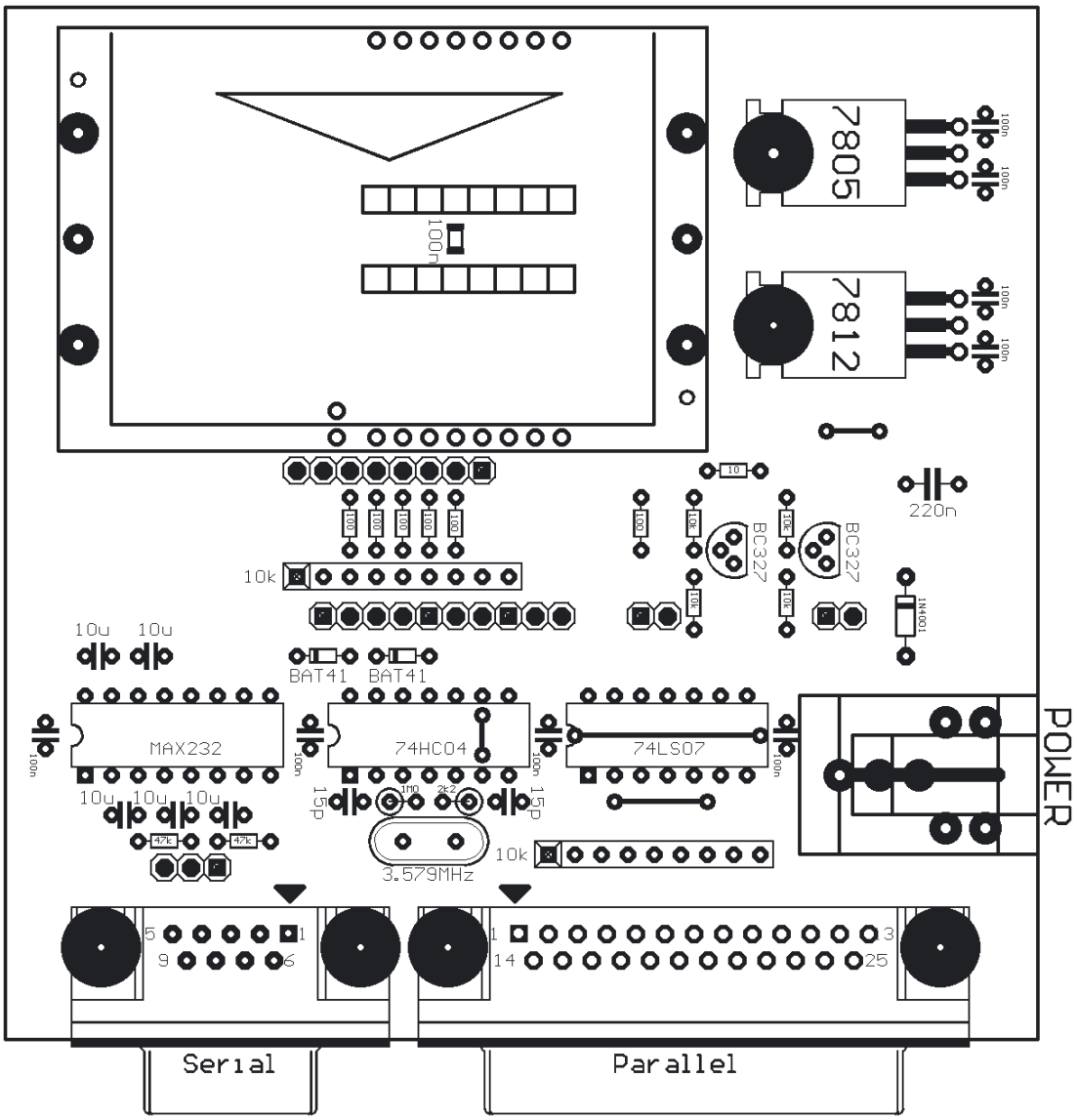
`http://www.ccc.de/Library/HPA/ChipCards/UniProg.html`.

Dort findet sich auch eine Bauteilliste. Beim Aufbau sollte der Bestückungsplan als Richtlinie benutzt werden, da der Schaltplan erst nachträglich zur besseren Orientierung erstellt wurde.

Platinen und möglicherweise auch fertig aufgebaute Geräte wird es dieses Jahr auf dem Chaos Congress in Hamburg (27.12.-29.12.1997) geben.



Chaos Bastelecke



Stückliste (mit Conrad-Bestellnummer)

1x	16 70 96 -44	MAX232	4.95	2x	40 04 40 -44	R= 39k	0.20
1x	16 88 74 -44	74LS07	1.85	1x	40 06 10 -44	R= 1MO	0.20
1X	16 41 94 -44	74HC04	0.95	2x	41 43 10 -44	RN= 8*10k	0.55
2x	18 96 18 -44	14pol. P-Sockel	0.75	2x	45 71 40 -44	C= 15p	0.20
1x	18 96 26 -44	16pol. P-Sockel	0.85	1x	45 24 40 -44	C= 100n SMD	0.35
1x	18 20 44 -44	Q = 3.579545MHz	1.95	8x	45 30 99 -44	C= 100n	0.45
1x	17 92 05 -44	7805	1.75	5x	48 17 26 -44	C= 10uF/16V	1.20
1x	17 92 30 -44	7812	1.75	1x	47 31 11 -44	C= 100uF/25V	0.40
2x	15 58 10 -44	T= BC327	0.30	1x	73 79 92 -44	Printbuchse	1.90
1x	16 22 13 -44	D= 1N4001	0.15	1x	74 11 83 -44	D-Sub Stiftleiste	1.80
2x	15 30 36 -44	D= BAT41	0.65	1x	74 13 45 -44	D-Sub Buchseleiste	1.50
1x	40 00 17 -44	R= 10	0.20	1x	73 24 78 -44	Stiftleiste	1.25
6x	40 01 30 -44	R= 100	0.20	1x	73 05 13 -44	ChipKartenKontakte	12.95
1x	40 02 97 -44	R= 2k2	0.20	1x	74 29 02 -44	Jumper	1.65
4x	40 03 78 -44	R= 10k	0.20	4x		Drahtbrücken	

.

Jumper Settings

```
Vcc   Vpp   ResClkDat   Port      Type
##    ..    ##..##..##  Ser     : Proz. Card
..    ##    .##.......  Par     : Pic Prog
..    ..    .##.......  Par     : Mem. Card
##    ..    ...##..##.  Ser     : Batt. Card
```

Die etwas ungewöhnliche Konstruktion mit parallelem und seriellem Interface ist auf die speziellen Anforderungen bei der PIC-Programmierung zurückzuführen. Da der Bauteilaufwand minimal sein sollte, blieb nur der Weg über die parallele Schnittstelle.

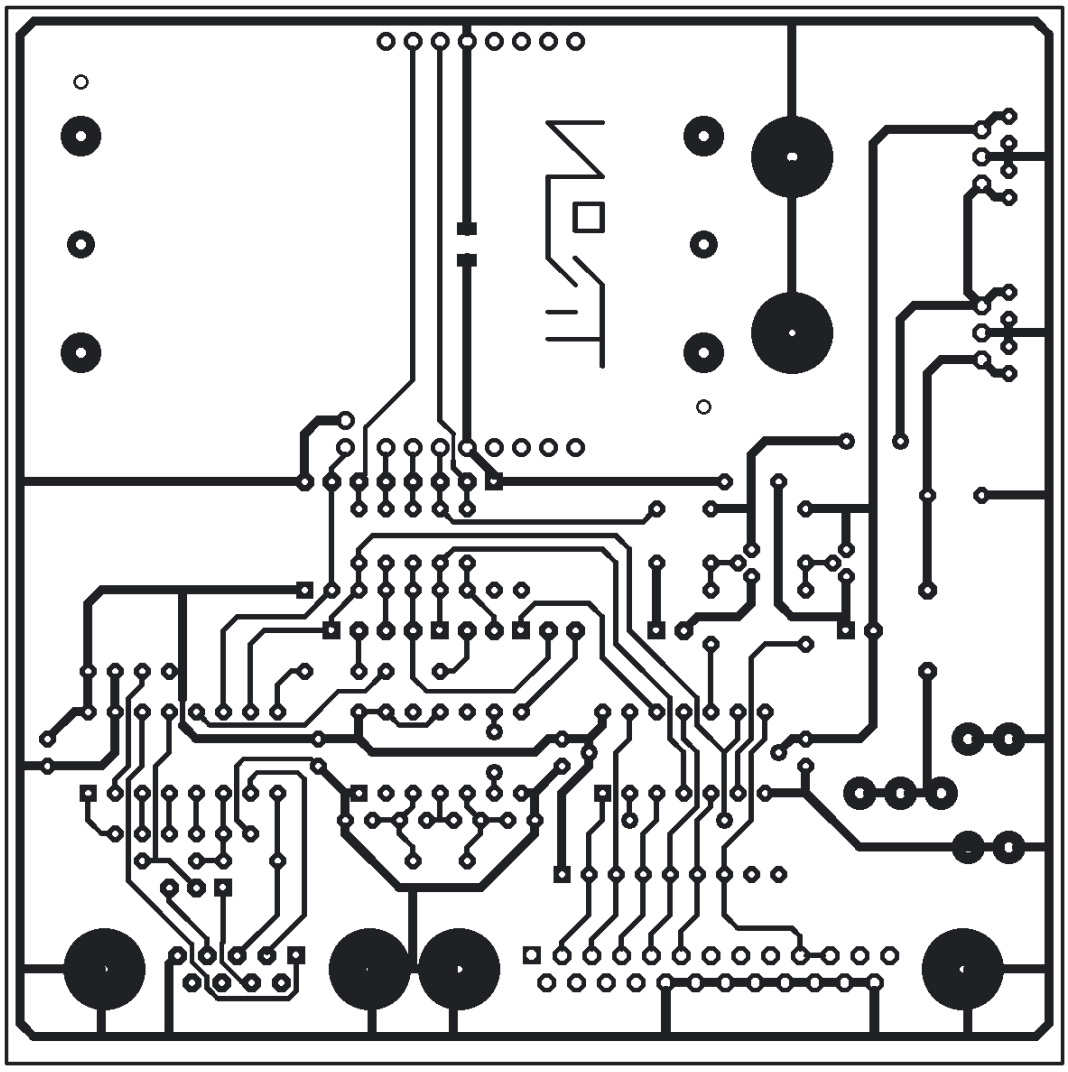
Projekt: tron@ccc.de
Doku: frank@ccc.de

Nachtrag zur D-Box Bastelanleitung aus DS60

Da der Schaltplan erst nach dem vollständigen Aufbau des Gerätes erstellt wurde, hat sich ein kleiner Fehler eingeschlichen.

Der Stecker für den BDM-Port wurde im Schaltplan verkehrt herum eingezeichnet. Ausschlaggebend für den Aufbau ist der Bestückungsplan, der war vor dem Schaltplan da.

frank@ccc.de



EC: Auf der Suche nach der PIN

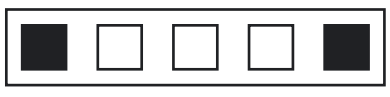
Gar nicht so richtig vorgesehen war der Wirbel, den eine kleine Demonstration einer der vielen EC-Karten Spielereien vor einem Fernsehsender verursachte.

Andreas war bei der "Netznacht" eines großen deutschen Fernsehsenders, und damit es in der langen Nacht nicht so langweilig wird, hatte er auch ein bißchen was zum Spielen mitgebracht (siehe Source Code). Es ging dabei um die praktische Vorführung der schon länger gerichtsverbindlich bekannten Feststellung (siehe DS 59), daß sich die PIN einer "alten" EC-Karte mit der Wahrscheinlichkeit 1:150 erraten läßt, wenn nur die Offsets bekannt sind.

Der eigentliche Grund für die Schlagzeilen in den Zeitungen und die Aufregung in den anderen Medien war allerdings gar nicht diese Nachtsendung, sondern ein anschließend gedrehter Beitrag eines unseriösen Wirtschaftsmagazins des selben Fernsehsenders, der in seiner Pressevoraberklärung behauptete, "die PIN-Nummern seien ohne Aufwand und ohne spezifische Kenntnisse zu entschlüsseln [...] Das habe am Wochenende ein Mitglied des Hamburger Chaos Computer Club [...] demonstriert.

Von einer Entschlüsselung im Sinne einer Ausrechnung des PIN-Codes kann allerdings nicht die Rede sein, es geht nur darum, die Anzahl der Rateversuche auf eine sinnvolle Anzahl zu reduzieren.

Die zugrunde liegende Mathematik lieferte Markus Kuhn schon vor einiger Zeit (siehe nebenstehendes Dokument). Dabei sind 2 Faktoren für die Eingrenzung der (theoretisch 9999) Möglichkeiten verantwortlich. Zum einen die bereits hinreichend (in der Datenschleuder 59) besprochene Umwandlung der internen hexadezimalen Zahlen in Dezimalziffern nach Modulo 10. Zum anderen die 3 Offsets, die für die ursprünglich vorgesehenen 3 Pool-Schlüssel jeder EC-Karte beigefügt waren; sie wurden dem Rechenergebnis der



Probability Theory for Pickpockets— ec-PIN Guessing

Markus G. Kuhn – mkuhn@acm.org – 1997-07-30
COAST Laboratory, Purdue University, West Lafayette, Indiana 47907-1398, USA

This abstract briefly describes an algorithm for determining the most likely 4-digit PINs associated with a debit card used at EuroCheque (ec) ATMs. We determine the probability of every PIN based on knowledge of the PIN-generation method and the data on the magnetic stripe. A card thief could use this strategy to optimally select the three PINs that he can try on a stolen card before it will be invalidated. The analysis shows a significant security problem of the PIN-generation algorithm, which allows the presented PIN-guess strategy to achieve a considerably higher success rate than a random guess would. The reader is assumed to be familiar with basic probability theory. The analyzed PIN-generation algorithm has been used by German banks from 1981 until 1997 according to documents available to the author.

Users of ec-cards cannot select their own PIN. The bank calculates the PIN for each customer as illustrated in the diagram. A 16-digit decimal number is formed by concatenating five digits of the bank routing number, the ten digit account number, and a single digit card sequence number. This number is transformed into a 64-bit pattern by encoding each digit with its 4-bit binary value (BCD). The result is encrypted using the DES algorithm with a secret 56-bit institute key K_I. The resulting 64-bit ciphertext can be written as a 16-digit hexadecimal number. We take the digits 3–6 and replace all occurrences of the letters A–F by digits 0–5 respectively. If the first of those four digits is a 0, we replace it by a 1. ATM networks owned by the card-issuing bank know K_I. They reconstruct the PIN the same way and compare it with what the customer has entered. ATM networks of other banks use a pool key K_{P1} instead, which results in a different PIN of course. The magnetic stripe of each card contains a 4-digit correction offset O_1 that an ATM using K_{P1} has to add without carry-over to the digits 3–6 of the decimalized DES result, to get the PIN known by the customer. In the decimalized DES result obtained with a pool key, a leading zero is not replaced. Since K_{P1} is known by all banks in Europe, it could be compromised more easily. Therefore, there exist two backup pool keys K_{P2} and K_{P3} and the card stripe stores two corresponding offsets O_2 and O_3. The emergency plan should K_{P1} be compromised one day is to switch to K_{P2} and overwrite O_1 on all cards at the next ATM visit. The problem that the designer of this PIN-handling system had not understood is that these pool key offsets provide valuable hints for someone who tries to guess a PIN.

From track 3 of the magnetic stripe of a card, we know the 12 offset digits

$$\begin{aligned}\text{Offset 1:}\quad & O_1 = (O_{1,1}, O_{1,2}, O_{1,3}, O_{1,4})\\ \text{Offset 2:}\quad & O_2 = (O_{2,1}, O_{2,2}, O_{2,3}, O_{2,4})\\ \text{Offset 3:}\quad & O_3 = (O_{3,1}, O_{3,2}, O_{3,3}, O_{3,4})\end{aligned}$$

Our goal is to determine four PIN digits

$$\hat{P} = (\hat{P}_1, \hat{P}_2, \hat{P}_3, \hat{P}_4)$$

that are most likely the actual PIN for this card.

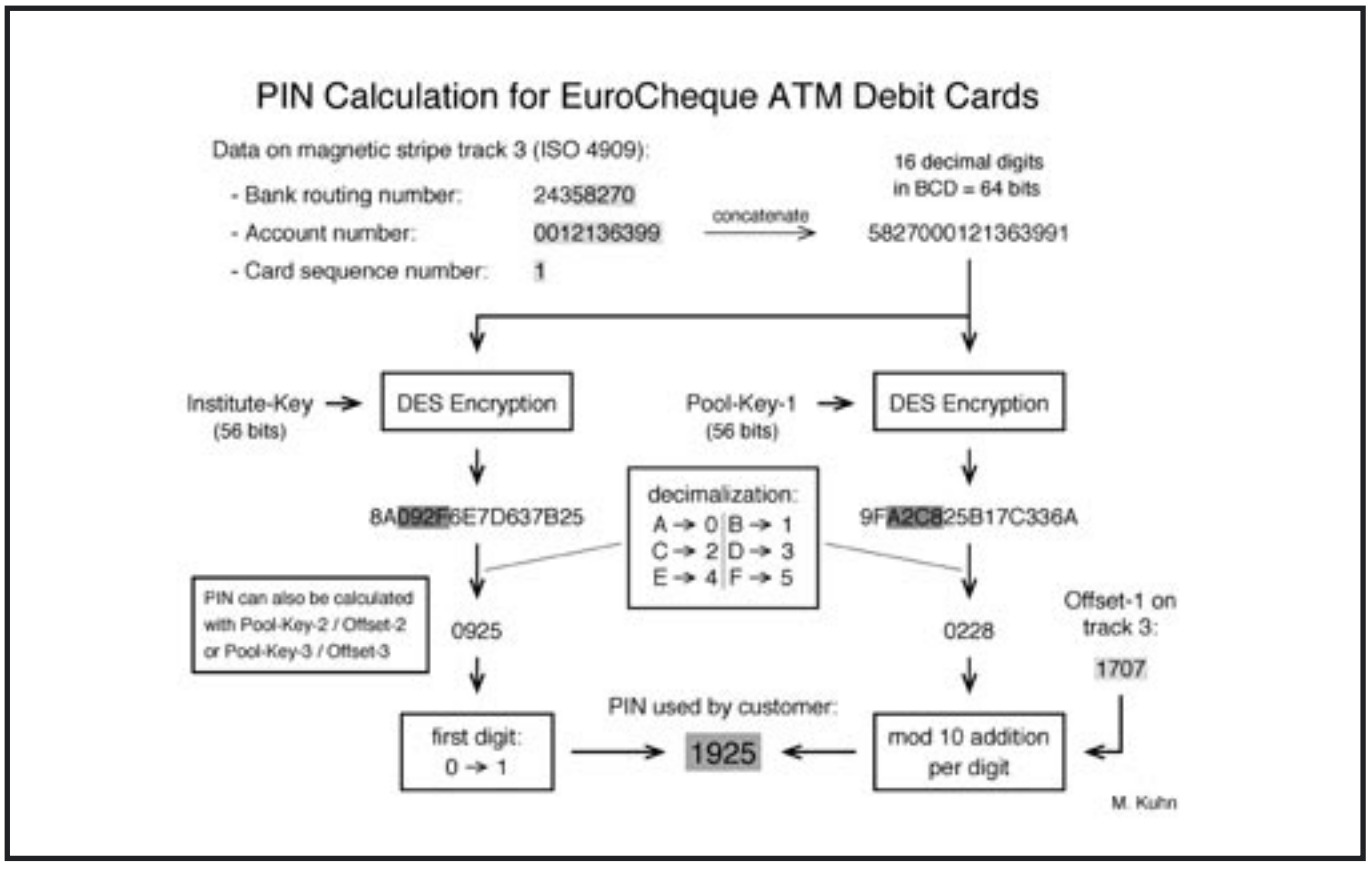
EC: Auf der Suche nach der PIN

DES-Verschlüsselung von Kontonummer, BLZ und Kartenfolgenummer jeweils für den Pool-Schlüssel hinzugefügt, damit letztlich die selbe PIN wie mit der Verschlüsselung mit dem Institutsschlüssel rauskommt.

Inwieweit diese mathematische Spielerei bei den gegenwärtigen PINs noch gilt ist unstrittig, bei den zukünftigen PINs ist es bei derzeitiger Informationslage noch etwas unklar. Noch haben nicht alle Geldinstitute auf neue PIN-Codes umgeschaltet und somit behält auch der Offset 1 noch seine theoretische Möglichkeit. Der Behauptung des Zentralen Kreditausschusses, auch heute seien schon "alle" Automaten "nur" noch im Online-Betrieb kommt dabei nur eingeschränkte Bedeutung zu. Denn ob der Pool-Schlüssel noch benutzt wird oder nicht, ist für einen "Errater" mit allen drei Offsets zunächst mal piepschnurzegal. Er will ja "nur" die PIN.

Auch gibt es widersprüchliche Aussagen zur Verbindlichkeit der Aussagen des Zentralen Kreditausschusses. Die Behauptung "alle Automaten sind nur noch online" ist vermutlich eine etwas verkürzte Version von "wir haben beschlossen, daß alle Automaten der bei unserem Verband angehörigen Geldinstitute nach unseren Richtlinien online seien müssen. Wenn sie sich nicht an unsere Richtlinie halten, tragen sie selbst die Haftung für etwaige Auszahlungen, die sie trotzdem gemacht haben“.

Anders formuliert: der ZKA kann offenbar nur Empfehlungen ausprechen. So wird auf einer ganz anderen Baustelle ja auch gerade versucht, den zunächst einmal totgeborenen deutschen Homebanking-Standard HBCI den



Let $\tilde{P}_j$ denote the random variable representing the j-th digit of the actual PIN of a card, and let $\tilde{O}_{i,j}$ denote the random variable representing the j-th digit in offset number i (for all $1 \leq i \leq 3, 1 \leq j \leq 4$). We assume that all hexadecimal digits of the four DES results are mutually independent and that the 16 digits are uniformly distributed, a required characteristic of any good block-cipher algorithm such as DES. Then, the distributions of these random variables are due to the applied decimalization method (see diagram) as follows:

$$p(\tilde{P}_j = k) = \begin{cases} 0/16, & \text{if } j = 1 \text{ and } k = 0 \\ 4/16, & \text{if } j = 1 \text{ and } k = 1 \\ 2/16, & \text{if } j > 1 \text{ and } k \in \{0, 1\} \\ 2/16, & \text{if } k \in \{2, \ldots, 5\} \\ 1/16, & \text{if } k \in \{6, \ldots, 9\} \end{cases} \tag{1a}$$

$$p(\tilde{O}_{i,j} = k | \tilde{P}_j = l) = \begin{cases} 2/16, & \text{if } (l - k) \bmod 10 \in \{0, \ldots, 5\} \\ 1/16, & \text{if } (l - k) \bmod 10 \in \{6, \ldots, 9\} \end{cases} \tag{1b}$$

A most likely PIN $\hat{P}$ is a P for which the conditional probability $p(\tilde{P} = P |$ for all $i : \tilde{O}_i = O_i)$ is maximal. Since all digits of the PIN are determined independently of each other, we can determine a most likely j-th PIN digit $\hat{P}_j$ as a P_j that maximizes $p(\tilde{P}_j = P_j | \forall i : \tilde{O}_{i,j} = O_{i,j})$ and get a most likely PIN simply as the combination of the most likely digits for each position.

We can turn around this conditional probability as follows (BAYES' theorem)

$$\begin{aligned} p(\tilde{P}_j = P_j | \forall i : \tilde{O}_{i,j} = O_{i,j}) &= \frac{p(\tilde{P}_j = P_j \wedge \forall i : \tilde{O}_{i,j} = O_{i,j})}{p(\forall i : \tilde{O}_{i,j} = O_{i,j})} \\ &= \frac{p(\forall i : \tilde{O}_{i,j} = O_{i,j} | \tilde{P}_j = P_j) \cdot p(\tilde{P}_j = P_j)}{p(\forall i : \tilde{O}_{i,j} = O_{i,j})} \\ &= \frac{p(\forall i : \tilde{O}_{i,j} = O_{i,j} | \tilde{P}_j = P_j) \cdot p(\tilde{P}_j = P_j)}{\sum_{k=0}^{9} p(\forall i : \tilde{O}_{i,j} = O_{i,j} | \tilde{P}_j = k) \cdot p(\tilde{P}_j = k)} \end{aligned}$$

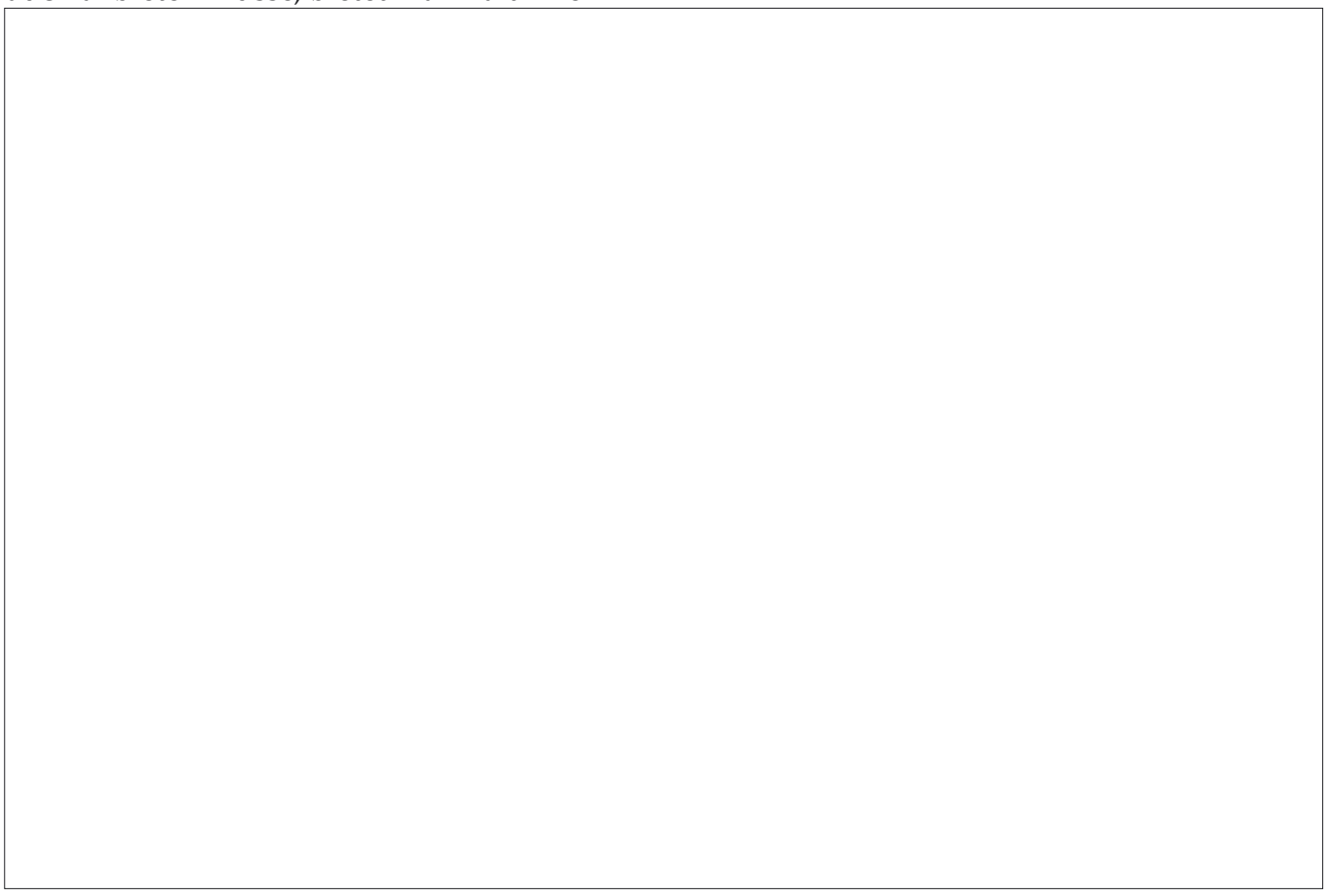
and since we assumed the DES results with the three pool keys to be mutually independent, we can replace the conditional probabilities for the combination of digits from all three offsets by the product of the probabilities for the individual offset digits, and thus we get

$$p(\tilde{P}_j = P_j | \forall i : \tilde{O}_{i,j} = O_{i,j}) = \frac{\prod_{i=1}^{3} p(\tilde{O}_{i,j} = O_{i,j} | \tilde{P}_j = P_j) \cdot p(\tilde{P}_j = P_j)}{\sum_{k=0}^{9} \prod_{i=1}^{3} p(\tilde{O}_{i,j} = O_{i,j} | \tilde{P}_j = k) \cdot p(\tilde{P}_j = k)}. \tag{2}$$

This formula uses only the known distributions given in (1). Based on it, we can easily write a small program to calculate $p(\tilde{P}_j = P_j | \forall i : \tilde{O}_{i,j} = O_{i,j})$ for all $P_j \in \{0, \ldots, 9\}$ given $O_{1,j}$, $O_{2,j}$, and $O_{3,j}$, and determine a $\hat{P}_j$ for which this probability is maximal. We do this for all four digit positions j and get this way a most likely PIN candidate $\hat{P}$. The probability that

EC: Auf der Suche nach der PIN

Instituten von ZKA-Seite aufzuzwängen; und die spielen da auch nur bedingt mit – weil es Geld kostet und nix bringt. Ein leitender Angestellter einer Bank kommentierte das neulich in einem Hintergrundgespräch so, daß man sich zunächst einmal zurücklehne und gucke, ob sich den HBCI am Markt – vor allem am Softwaremarkt – überhaupt durchsetze. Wenn man tatsächlich HBCI u.a. auch anbieten müsse, bietet man halt zwei



Basisfunktionalitäten, die nicht zu teuer sind.

Wir müssen also in unserem Bild von der Situation womöglich zwischen den Geldinsituten auf der einen Seite und dem ZKA auf der anderen Seite unterscheiden. Die Institute vermeiden tunlichst, sich zur Unsicherheit der EC-Karte zu äußern, sondern überlassen dies dem ZKA.

Ist aus der Sicht der Banken auch verständlich: selbst wenn denen die Geldautomaten nur so um die Ohren fliegen und einer nach dem anderen leergemacht wird, halten sie die Schnauze. Für eine Bank ist der *Glaube* des Kunden an die Sicherheit der Bank existenziell - *nicht* die Sicherheit selbst.

Auf diese Annahme gestützt, geben ihr ja die Kunden das Geld. Das ist also zunächst mal ganz neutral formuliert das Geschäftsprinzip einer Bank. Die Reaktionen der Kunden auf ein Eingeständnis etwaiger Unsicherheit können nur als katastrophal für die Banken erahnt werden; vor allem, nachdem man sich mehr als 10 Jahre in der Behauptung versteift hat, daß das System sicher sei.

Der ZKA ist also als Verband (und somit letztlich Dienstleister) der Banken für die

this PIN is correct is the product of the probabilities that the individual digits $\hat{P}_j$ are each correct, as calculated above. It can get as high as $0.948\% \approx 1/105$.

We have so far described how to find a most likely PIN for a specific card for which we know the offsets, and we can calculate its success probability. We now calculate, what success probability we expect if we do not have the offsets of a specific card given, but if we pick a random card. This can be estimated per digit position j with another small program as follows. We try all 16^4 possible combinations for the four hexadecimal digits (W, X, Y, Z) in each of the four DES results that determine one digit in the PIN and one in each offset. We determine from this quadruple—like a bank does when a new card is issued—the j-th digit of the PIN and the three offsets as follows:

$$\begin{aligned} P_j &:= \begin{cases} W \bmod 10, & \text{if } W \bmod 10 > 0 \text{ or } j > 1 \\ 1, & \text{if } W \bmod 10 = 0 \text{ and } j = 1 \end{cases} \\ O_{1,j} &:= (P_j - X) \bmod 10 \\ O_{2,j} &:= (P_j - Y) \bmod 10 \\ O_{3,j} &:= (P_j - Z) \bmod 10 \end{aligned}$$

This way, we have generated a set of 16^4 simulated cards that has the same PIN and offset digit distribution that we expect from the set of all cards in circulation. Now, we determine a most likely PIN digit $\hat{P}_j$ as described above for each of those 16^4 cards. Since we know for each of these simulated cards the correct PIN digit P_j, we can count which fraction of the 16^4 calculated most likely PIN digits $\hat{P}_j$ is correct and equals the corresponding P_j.

The results of this program run are the following probabilities for a correct guess for each of the four PIN digit positions j:

digit 1: $0.27856 \approx 28\% \approx 1/3.6$
digit 2: $0.20312 \approx 20\% \approx 1/4.9$
digit 3: $0.20312 \approx 20\% \approx 1/4.9$
digit 4: $0.20312 \approx 20\% \approx 1/4.9$

Note that if the banks had used a good PIN generation algorithm, we would have expected a random guess success rate of 11% for the first digit (no leading zero) and 10% for the remaining three digits. By multiplying the actual four per-digit success probabilities above, we get a success probability of $0.0023346 \approx 0.233\% \approx 1/428$ for the most likely PIN. Since a thief has at least three attempts, and since most second or third best PINs have a similar success chance, the probability to get access to the account is roughly three times the success probability of the most likely PIN, this means in the order of $0.7\% \approx 1/150$. Had the banks used a good PIN-generation algorithm, we would have expected only a $1/3000 \approx 0.033\%$ success rate in three attempts, because there are 9000 possible PINs (1000–9999). In other words, the security of the ec-PIN system is worse than that of a good system with only three digit PINs, where we would expect a $1/300 \approx 0.33\%$ success rate in three attempts.

This text did not discuss techniques that allow more than three attempts to enter a PIN. It also did not discuss the cost of determining the DES keys using a brute-force search with special hardware. Both are in the author's opinion valid additional serious concerns regarding the security of the EC card system.

The author wishes to thank Bodo and Ulf Möller from the University of Hamburg for their help and for their suggestions in this analysis.

EC: Auf der Suche nach der PIN

Öffentlichkeitsarbeit in dieser Sache und die technischen Vereinbarungen und Betriebszustände zuständig. Nach außen hin wird professionellstmöglich behauptet, alles sei in Ordnung. Nach innen hin gibt es zwei Problemstellungen: die technische Unsicherheit einzugrenzen und dafür zu sorgen, daß keine Bank in dieser Situtation durchdreht.

Der konkrete Fall ist ein gutes Beispiel für die desolate Lage der Banken und des ZKA. Da gibt es zum Beispiel ja den Beschluß das alle Inlandsautomaten online zu sein haben - auch und gerade mit dem "alten" Poolkey-Verfahren und daher die Offsets im Prinzip - und für den inländischen Betrieb - gar nicht mehr auf der Karte sein müssen. Damit wurde auch beschlossen, daß die Offsets bei Benutzung der Karte im Automaten gelöscht werden, damit sie nicht als Angriffspunkt für einen Angreifer dienen können. Na dann ist ja alles gut, oder?

Blöderweise geht da so ein CCC-Blag in eine Fernsehsendung und auf der EC-Karte des Redakteurs finden sich - oh' Wunder - alle Offsets. Und was tut der ZKA? Der ZKA kotzt. Aber nur nach innen. Denn nach außen wird er ja dafür bezahlt, gute Miene zu machen. Nach innen hin allerdings muß natürlich dem "verantwortlichen" Institut eins auffe Mütze gegeben werden, dafür, daß es offenbar die "Empfehlung" (Anweisung) ignoriert hat, die Offsets auf der Karte zu löschen. Irgendjemand hat behauptet, genau das wäre passiert. Alles Quatsch?

Was die Verwendung der Offset-Felder beim "neuen" PIN-Verfahren "ohne" Poolkey betrifft, ist noch etwas unklar. Zumindest bis zum Congress. Und an der Haftungsfrage wurde natürlich auch nix geändert.

Soweit ein bißchen ein Metablick mit eingrenzbaren subjektiven Faktoren.

andy@ccc.de

offset.c

Das nebenstehende Programm zeigt eine einfache Implementierung der statistischen Analyse der Offsets der EC-Karte.

Der Aufruf ist

```
offset 0 1234 5678 9012
```

für alte EC-Karten (die vierstelligen Zahlen sind die drei Offsets) und

```
offset 5 1234 5678 9012
```

für die neuen EC-Karten.

Viel Spaß am Gerät

andreas@ccc.de

offset.c

```
/*
 * offset.c
 */
#include <stdio.h>

int p[15][10] = {
     { 0, 4, 2, 2, 2, 2, 1, 1, 1, 1 },    { 2, 2, 2, 2, 2, 2, 1, 1, 1, 1 },
     { 2, 2, 2, 2, 2, 2, 1, 1, 1, 1 },    { 2, 2, 2, 2, 2, 2, 1, 1, 1, 1 },
     { 2, 2, 2, 2, 2, 2, 1, 1, 1, 1 },    { 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 },
     { 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 },    { 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 },
     { 1, 1, 1, 1, 1, 1, 1, 1, 1, 1 },    { 2, 2, 2, 2, 2, 2, 1, 1, 1, 1 }
};
int po(int pin, int offset) {
     return p[4 + n][(pin + 10 - offset)%10];
}

int main(int argc, char* argv[]) {
     int stelle, stelle2, offset, i;
     int probdivisor, probdivsum, probsum[4], prob[4][10];
     int stellen[4];
     double pinprob;

     n = atoi(argv[1]);
     for(stelle = 0; stelle < 4; stelle++) {
          probdivsum = 0;
          for(i=0; i<10; i++) {
               probdivisor = p[stelle + n][i];
               for(offset = 0; offset<argc - 2; offset++) {
                    probdivisor *= po(i, argv[offset + 2][stelle] - '0');
               }
               prob[stelle][i] = probdivisor;
               probdivsum += probdivisor;
          }
          probsum[stelle] = probdivsum;
     }
     for(stelle = 0; stelle<4; stelle++) {
          for(i=0; i<10; i++) {
               printf("%f ", (float)(prob[stelle][i]) / (float)(probsum[stelle]));
          }
          printf("\n");
     }
     for(stellen[0] = 0; stellen[0] < 10; stellen[0]++) {
          for(stellen[1] = 0; stellen[1] < 10; stellen[1]++) {
               for(stellen[2] = 0; stellen[2] < 10; stellen[2]++) {
                    for(stellen[3] = 0; stellen[3] < 10; stellen[3]++) {
                    pinprob = 1.0;
                    for(stelle = 0; stelle< 4; stelle++) {
                         printf("%i", stellen[stelle]);
                         pinprob *= ((float)(prob[stelle][stellen[stelle]]) /
                              (float)(probsum[stelle]));
                    }
                    printf(" %lf\n", pinprob);
                    }
               }
          }
     }
}
```

Liebe Telekom,

die betriebsbedingte Unsicherheit in Zusammenhang mit dem Konzept der Security By Obscurity bei der Einführung der Telefonguthabenkarten scheint für Dich allmählich zu einem echten Problem zu werden.

Erst knapp ein Jahr ist es her, daß Dir die Einführung neuer Telefonkarten in Anbetracht der geringen Mißbrauchszahlen betriebswirtschaftlich zu kostspielig erschien. Mittlerweile besteht das Problem, gewisse Unternehmensentscheidungsbereiche vom Sinn einer solchen Maßnahme zu überzeugen, wohl nicht mehr. Dafür ist Dein eigentliches Problem – die "Schäden" durch Telefonkartenbetrug – ein bißchen erwachsener geworden.

Fast täglich erreichen uns Meldungen zu diesem Thema. Wie die aus Hanau, wo nach Polizeiangaben in der jüngsten Vergangenheit allein in dieser Region ein Schaden von rund 100.000 Mark durch derart gefälschte Telefonkarten entstand. Auch wurde aus düsteren Quellen von einer Fabrik in Ungarn berichtet, die offenbar professionell aussehende nichtleerwerdende Wundertelefonkarten inklusive Aufdruck Deines Logos herstellte.

In einer Pressemeldung heißt es, "die Anrufe zum Nulltarif führen zu erheblichen Umsatzeinbußen bei der Telekom, die zusätzlich von ausländischen Telefongesellschaften für die benötigten Leitungen zur Kasse gebeten wird. Diese Kosten sind in der Schätzung noch nicht enthalten und werden von der Telekom unter der Decke gehalten."

Das ist schade, denn genau diese Kosten sind ja die "realen". Deine Schätzungen der Umsatzeinbußen gehen – ähnlich wie bei "Raubkopien" – von der irrigen Annahme aus, die Leute hätten sonst für die Gespräche bezahlt bzw. sich all die Software gekauft, die sie sich illegal kopiert haben.

Nun versuchst Du die Wunderkarten durch entsprechende Software im Netz anhand ihres Timings zu erkennen und ihre Verwender dann mit entsprechenden mobilen Einsatzgruppen abzugreifen. Das klingt aber lästig für alle Beteiligten und ist wohl als minder elegante Lösung zu bezeichnen.

Die Meldungen der Berliner Polizei betreffen daher in letzter Zeit auch primär Einsätze am Sonntag, wo offenbar genug Beamte für so einen Unsinn zur Verfügung stehen. In Berlin wird von einem Schaden von 150.000 DM pro Monat geredet, als Täter werden vorwiegend Asylbewerber angegeben, was angesichts ihrer eingeschränkten Kommunikationsmöglichkeiten mit der Heimat wohl eher wenig verwunderlich ist. Vom Menschenrecht auf doch zumindest weltweite, ungehinderte Kommunikation ist diese Welt an einigen Stellen doch noch weit entfernt.

Man sollte meinen, daß Du für Deine Eskapaden in den letzten Dekaden genug bezahlt hast, um es endlich besser zu wissen.

Doch solange Du nicht begreifst, daß nur eine offene Dokumentation aller Systeme und die endgültige Verabschiedung von der Geheimniskrämerei Dir in das nächste Jahrtausend helfen, solange mußt Du auch weiterhin unseren Hohn und Spott ertragen, wenn es dann wieder alles nicht nach Plan verläuft.

Mit eristischem Gruß
Deine Freunde vom CCC

andy@ccc.de
tim@ccc.de

Hi Chaosleutz!

Im meinen letzten Tschechien-Aufenthalt hab ich eine kleine Entdeckung mit meinem D1-Handy gemacht: Man kann das lokale Telefonnetz abhören:

1. In das Netz roamen...

2. +4925619139999999 wählen

IF Besetzt goto 2

IF nix kommt ins Mic blasen, auf Echo warten

IF kein echo goto 2

IF echo auf gespräch warten

und schon kann man abhören.

Mein Siemens S6-Handy trennt die Verbindung leider automatisch nach 2 Min. weil keine echte Verbindung zustande kommt. "Tln. hebt nicht ab" und das geht nur wenn grade ein lokaler Telefonanschluß Hörer abgenommen hat und noch nicht gewählt sonst -> Besetzt

Das funzt übrigens im Netz der RadioMobil [CZ Pægas] besser als im EuroTel [CZ EuroTel]

das wars...
CU
SQUelcher
[IRCler im #heidelberg]

P.S: Wann lernen die dt. Netzbetreiber mal die Groß/Kleinschreibung für ihren Netznamen, wer wird schon gern von D1-TELEKOM oder D2 PRIVAT angeschrien ? ;)

KM

Bad Times

Wenn Sie eine E-Mail mit dem Titel "Bad Times" erhalten, löschen Sie sie sofort, ohne sie zu lesen. Es handelt sich hierbei um den bislang gefährlichsten E-Mail-Virus. Er wird Ihre Festplatte formatieren. Und nicht nur die, sondern auch alle Disketten, die auch nur in der Nähe Ihres PCs liegen. Er wird das Thermostat Ihres Kühlschranks so einstellen, daß Ihre Eisvorräte schmelzen und die Milch sauer wird. Er wird die Magnetstreifen auf Ihren Kreditkarten entmagnetisieren, die Geheimnummer Ihrer EC-Karte umprogrammieren, die Spurlage Ihres Videorekorders verstellen und Subraumschwingungen dazu verwenden, jede CD, die Sie sich anhören, zu zerkratzen. Er wird Ihrem Ex-Freund/der Ex-Freundin Ihre neue Telefonnummer mitteilen. Er wird Frostschutzmittel in Ihr Aquarium schütten. Er wird all Ihr Bier austrinken und Ihre schmutzigen Socken auf dem Wohnzimmertisch plazieren, wenn Sie Besuch bekommen. Er wird Ihre Autoschlüssel verstecken, wenn Sie verschlafen haben und Ihr Autoradio stören, damit Sie im Stau nur statisches Rauschen hören. Er wird Ihr Shampoo mit Zahnpasta und Ihre Zahnpasta mit Schuhcreme vertauschen, während er sich mit Ihrem Freund/Ihrer Freundin hinter Ihrem Rücken trifft und die gemeinsame Nacht im Hotel auf Ihre Kreditkarte bucht.

"Bad Times" verursacht juckende Hautrötungen. Er wird den Toilettendeckel oben lassen und den Fön gefährlich nah an eine gefüllte Badewanne plazieren. Er ist hinterhältig und subtil. Er ist gefährlich und schrecklich. Er ist außerdem leicht violett. Dies sind nur einige der Auswirkungen. Seien Sie vorsichtig. Seien Sie sehr, sehr vorsichtig.


FLATULENZ

poing@star.trek.org,
http://star.trek.org/~poing/

VSt Watch

010: Wahl des Long-Distance-Carriers

Wenn Anfang 98 der freie Wettbewerb auf dem deutschen Telekommunikationsmarkt über uns hereinbricht, wird sich das anfangs hauptsächlich dadurch bemerkbar machen, daß man sich aussuchen kann, über wessen Leitungen man nun seine Ferngespräche führt.

Auswählen kann man (ähnlich wie in den USA), in dem man vor die gewünschte Nummer 010XX wählt. 'XX' steht dabei für die Verbindungsnetzbetreiberkennzahl – mit 33 telefoniert man zum Beispiel über Ma ·T···el, 11 steht für o.tel.o usw. (s. Tabelle). Wer jetzt schon mal Wettbewerb spielen will, kann das (sofern die VSt schon dafür konfiguriert wurde) ausprobieren: 01033<telefonnummer> funktioniert oft schon. Je nach VSt (EWSD/S12) gibts da noch kleine Besonderheiten – viel Spaß beim Ausprobieren.

CLIP fürs Volk: *31#

Ebenfalls ab Anfang 98 gibt es endlich auch Rufnummernübermittlung *an* analoge Anschlüsse. Übertragen wird die Rufnummer mit 1200 Baud zwischen dem ersten und zweiten Klingelton (standardisiert nach ETS 300 659-1).

Damit sich diesen Dienst auch jemand freischalten läßt (die T will sich mit DM 3 pro Monat daran bereichern), wird die Voreinstellung für die Rufnummernübermittlung aller Analoganschlüsse von CLIR (Calling Line Identification Restriction, die Rufnummer wird nicht zum B-Teilnehmer übermittelt) auf CLIP (Calling Line Identification Presentation, die Nummer wird übermittelt) geändert: Rufnummernübermittlung für alle. Wer damit nicht so unbedingt einverstanden ist, kann Gegenmaßnahmen ergreifen:

- Wenn man *31# vor der eigentlichen Nummer wählt, wird die eigene Rufnummer für diesen Anruf unterdrückt.
- Durch einen Anruf beim T-Service kann man es dann auch wieder ganz abschalten lassen.

Rechnung online ··· EVÜ unzensiert

Die folgenden Punkte haben nicht unbedingt etwas mit dieser Rubrik zu tun, passen aber gut zu "was ändert sich 98 bei der T":

- Demnächst gibt es die T-Rechnung online im Web: Dort wird man dann nach Eingabe von Benutzernamen/Passwort Kosten für Gespräche direkt nach deren Beendigung abrufen können. "Nach Beendigung" wahrscheinlich nur, damit man nicht auch noch die Kosten für die laufende Internet-Verbindung sieht…
- Außerdem gibt es ab Januar die Einzelv erbindungsübersicht endlich ohne 'XXX': allerdings muß man das jeweils bei der ·T··· beauftragen.

Rufumleitung erweitert

Bisher galt ja bekanntlich: ein umgeleiteter Anruf kann nicht nochmal umgeleitet werden. Wenn die Signalisierung mitspielte (was zwischen Mobilfunk- und Festnetzen nicht immer gegeben ist), war das auch so. Jetzt hat man bei der T wohl gemerkt, daß das oft nicht mehr ausreicht. Das könnte durch die erste Massenrufumleitungsnutzung, die T-Net-Box, ausgelöst worden sein.

Folgendes Szenario soll die Problematik verdeutlichen: Angenommen, man hat zwei

Verbindungsnetzbetreiberkennzahlen

```
10 Teleglobe GmbH, Frankfurt
11 o.tel.o communications GmbH, Düsseldorf
12 Tele Danmark Internetz GmbH, Hamburg
13 Tele Europe s. A., Luxembourg
14 EWE TEL GmbH, Oldenburg
15 RSL COM Deutschland GmbH, Frankfurt/Main
18 debitel Kommunikationstechnik GmbH & Co KG
19 CityLine Telefondienste GmbH
20 ISIS Multimedia Net GmbH, Düsseldorf
22 NetCologne GmbH, Köln
23 Communikationsnetze Süd-West GmbH & Co. KG, Stuttgart
24 Telepassport GmbH
25 CityKom Münster
28 Colt Telecom GmbH, Frankfurt
30 TelDaFax Telefon-, Daten- und Fax-Transfer GmbH & Co. KG, Wetter (Hessen)
33 Deutsche Telekom AG, Bonn
34 NEFkom Telekommunikation GmbH & Co. KG, Nürnberg
40 PLUSNET Gesellschaft für Netzwerk Services mbH, Düsseldorf
41 HanseNet Telekommunikation GmbH
42 CityCom Wuppertal Multimedia GmbH
43 KielNet GmbH Gesellschaft für Kommunikation, Kiel
44 VEW TELNET Gesellschaft für Telekommunikation und Netzdienste mbH
46 KomTel Gesellschaft für Kommunikation und Informationsdienste GmbH, Flensburg
49 ACC Telekommunikation GmbH, Düsseldorf
50 TALKLINE PS PhoneServices GmbH, Elmshorn
55 ESPRIT Telecom Deutschland GmbH, Düsseldorf
60 Telecom-InfoService GmbH, Wien (A)
66 Interoute Telecom Deutschland GmbH, Frankfurt
69 Primus Telecommunications Ltd., Düsseldorf
70 Mannesmann Arcor AG & Co., Eschborn
71 DeTeMobil Deutsche Telekom MobilNet GmbH, Bonn
72 Mannesmann Mobilfunk GmbH, Düsseldorf
77 E-Plus Mobilfunk GmbH, Düsseldorf
78 3U Telekommunikation GmbH i.G., Löbau
79 VIAPHONE GmbH, Frankfurt
80 Telegate Aktiengesellschaft für telefonische Informationsdienste, Herrsching
85 WESTCom GmbH, Heidelberg
88 WorldCom Telecommunication Services GmbH, Frankfurt
89 Münet Telekommunikations GmbH, München
90 VIAG INTERKOM GmbH & Co. KG, München
97 AT & T-Unisource Communication Services (Deutschland) GmbH, Frankfurt
98 STAR Telecommunications Deutschland GmbH, Frankfurt
```

Quelle: BAPT

Anschlüsse A und B. Für B ist eine T-Net-Box eingerichtet und die Umleitung dahin aktiviert. Wenn man jetzt eine Rufumleitung von A nach B einschaltet, hat ein Anrufer, der A anruft, bis vor kurzem ein "Dieser Anschluß ist vorübergehend nicht erreichbar" gehört, da die Umleitung auf die T-Net-Box bereits die zweite gewesen wäre. Inzwischen kann man wohl an allen VSts mindestens zweifach umleiten, es gibt jedoch auch Berichte von drei und mehr hintereinanderschaltbaren Umleitungen.

tobias@ccc.de

Literaturhinweise

»The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance«

by Bruce Schneier and David Banisar
John Wiley & Sons, 1997
ISBN: 0-471-12297-1
747 pages
Retail: $60 hardcover

Trying to keep up with the advancements in cryptography and digital telephony, the government has advocated controversial new tools that will allow them to monitor electronic communications. On the other side of the spectrum, privacy advocates are vehemently opposed to any government monitoring whatsoever.

The Electronic Privacy Papers is a collection of previously unreleased documents dealing with privacy in the Information Age. Combining public government pronouncement, public reactions, and previously classified documents released under FOIA, this book paints a clear picture of government policies towards encryption and privacy and how they will impact individuals and companies involved with the Internet.

Issues covered include:

~ The economic and political rationale for demanding digital wiretapping and surveillance.

~ The legal foundations, and limitations to, government surveillance.

~ Government strategies for soliciting cooperation from telephone companies and equipment manufacturers.

~ Which policies industries and individuals can expect the government to pursue in the future.

»Rechtsextremisten auf dem Datenhighway«

von Thomas Pfeiffer
ISBN 3-928970-06-2

Funktion und Bedeutung computergestützter Kommunikation für die Netzwerke am rechten Rand.

Eher politisch als technisch. Bestellanschrift: Antifa Dortmund-Nord c/o Taranta Babu Humboldtstr. 44, D-44137 Dortmund, Antifa-Do.Nord@anarch.free.de

»Lauschziel Wirtschaft«

von Manfred Fink
Boorberg Verlag
ISBN 3-415-02194-7

Abhörgefahr und -techniken, Vorbeugung und Abwehr. Eher Überblick als Detail, eher Abwehr als Angriffsperspektive.

»Underground«

Suelette Dreyfus
ISBN 1-86330-595-5
http://www.underground.org/book

Tales of hacking, madness and obsession on the electronic frontier. Wer hatte das nochmal empfohlen?

14. CHAOS COMMUNICATION CONGRESS

Chaos

Nichts ist wahr.
Alles ist erlaubt.

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.) ··· CyberPets ··· Perl As A Hacker Tool ··· Krypto-Reglementierung und Hintergründe ··· GSM-Hacking ··· Techno-Terrorismus ··· Adbusting ··· Satelliten-Lauschen ··· Pay-TV Hack & Crack ··· Wirtschaftsspionage ··· Open Source Information Processing: Geheimdienst selbstgebaut ··· ISDN-Kryptodevice Vorstellung ··· Mobilfunk für Fortgeschrittene ··· Lynchen & Umgang mit Spammern ··· Kampf dem DNS-Monopol ···

Special Event: Deutsche Meisterschaften im Lockpicking

Aktuelle Informationen unter http://www.ccc.de

Wo? Wann?

27.–29. Dezember 1997
Eidelstedter Bürgerhaus
Alte Elbgaustraße 12
Hamburg Eidelstedt

Eintrittspreise

Ideal Standard	DM 42
Schüler, Zivis, Rentner	DM 30
Mitglieder des CCC e.V.	DM 23
Presse	DM 75
Gewerbliche Teilnehmer	DM 200

Tageskarten DM 20 ermäßigt DM 15

Bestellungen, Mitgliedsanträge und Adreßänderungen bitte senden an:

CCC e.V., Schwenckestr. 85, D-20255 Hamburg

Adreßänderungen auch per Mail an office@ccc.de

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 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

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 als Verrechnungsscheck (bevorzugt)
o in Briefnarken

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 _____