ISSN 0930-1045 September 1996 Nr. 56 DM 5,00 Postvertriebsstück C11301F

Die Datenschleuder

#56

Das wissenschaftliche Fachblatt für Datenreisende

Ein Organ des Chaos Computer Club e.V.

ds://finder/editorial.wau

2 Editorial

3 Sorgen und Nöte

5 Was tun bei Zensur?

Mirror-Liste für „radikal“

6 Generation @

8 DeTeHack

9 Sicherheit ist Vertrauenssache

12 Is Not Much Good

14 Hackerjagd im Internet

Impressum

15 Oligopoly

16 Bestellfetzen

Wer mit Menschen, die „informationelle Habenichtse in der 3. Welt“ sind, verkehrt, kennt die Wichtigkeit von Briefpost und elektronischer Post. Eine der übelsten Dinge ist es, einen Menschen von der Kommunikation auszuschließen.

Heinrich von Stephan sorgte als Gründer des Weltpostvereins dafür, daß auch zwischen kriegführenden Staaten geregelter Briefverkehr möglich war. Gegen diese Kulturschöpfung der Kommunikation trotz Krieg verstießen einige deutsche Internet-Provider, indem sie auf ein simples Fax hin sogar den eMail-Verkehr zu XS4ALL sperrten. Die Chaos-Aussage zur Verbindlichkeit von Fax ist kurz: wenn ein Richter glaubt, ein Fax sei rechtsverbindlich, dann faxt man ihm seine Entlassung mit der Absenderkennung seiner vorgesetzten Behörde zu.

Das Problem liegt jedoch tiefer, weil ein meines Erachtens von der „Droge“ Adrenalin abhängiger Staatsanwalt in Karlsruhe der Absender war. Gepusht durch den „Drogendealer“ Rechtsanwalt Michael Schneider von eco/ICTF, lief die Bundesanwaltschaft zu Hochform auf wie einst eine Berliner Staatsanwaltschaft.

Damals wollte die wegen der Zeitschrift RADIKAL zwei Vorstandsmitglieder aus dem zugehörigen Verein in den Knast bringen. Die GRÜNEN nahmen beide daraufhin auf die Europawahlliste. Sie wurden gewählt und das Europaparlament stimmte dagegen, daß die beiden in den Knast kommen für gedruckte Worte. Diese europaweite Blamage der Berliner Staatsanwaltschaft wird aktuell nur durch die globale Blamage der Bundesanwaltschaft bei einem neuerlichen Versuch in ähnlicher Sache übertroffen: statt Sperrung hat die RADIKAL eine Auflagensteigerung zu erwarten, die sie ohne die Bundesfehlwahlschaft nie erreicht hätte.

Absurd, aber wahr: eigentlich ist die Bundesanwaltschaft der gefährlichste Förderer einer „kriminellen Vereinigung“, wenn denn die RADIKAL überhaupt eine solche ist. Zumindest die Sperrung des auf einer getrennten WWW-Seite abrufbaren Textes zum Thema Pressefreiheit ist ein Verstoß gegen die Europäische Menschenrechtskonvention, meint:

Wau Holland
Doyen des CCC

Sorgen und Nöte

Ein Internet-Service-Provider hat's schon schwer. Nicht nur, daß er sich mit diesen nervigen Kunden, auch User genannt, auseinandersetzen muß. Nein, er muß auch immerzu sein System am laufen halten, seine Anbindung auf den preisgünstigsten Leitungen fahren und nun auch noch seinen privaten kleinen Wirtschaftsstandort vor Existenzgefährdung durch böswillige Terroristenjäger schützen.

Die Bundesanwaltschaft, kurz BAW, runzelte nun gegenüber dem neugegründeten ISP-Verein PrivatePornoJäger e.V., auch **Internet Content Task Force** genannt, kräftig die Stirn wegen der Zugänglichkeit von Seiten, die die Texte der in Deutschland inkriminierten Zeitschrift „radikal" enthalten.

Diese Seiten liegen beim holländischen ISP **XS4ALL** der vor einigen Jahren von der ehemaligen Crew der **Hacktik** (holländische Hackerzeitschrift) gegründet wurde. Da XS4ALL die Idee des Freedom of Speech ernst nimmt, haben sie vor einigen Monaten auch nicht das Knie vor der doch recht mächtigen Scientoloy-Sekte gebeugt, die einige Seiten eines XS4ALL-Users beanstandete.

Um Arbeitsplätze, Gewinnmargen und Seelenfrieden zu gewährleisten, empfahl die ICTF, im Netz vertreten durch Herrn Rechtsanwalt Michael Schneider, nun ihren Mitgliedern, XS4ALL für ihre User unzugänglich zu machen. Die Holländer begannen daraufhin, ihre IP-Nummern zu rotieren, was eine Sperre auf IP-Nummer-Basis etwas schwierig macht. Somit war XS4ALL von den allermeisten ISPs aus trotzdem zu erreichen. Da einige ISPs daraufhin begannen, ganze Class-C-Netze zu blocken, wurde die Rotation zwischenzeitlich wieder eingestellt, um nicht völlig unerreichbar zu werden.

Die ICTF argumentiert, daß sie nur die allernötigsten, von der BAW geforderten Schritte unternimmt, um Schaden von ihren Mitgliedern abzuwenden. Den Vorwurf vorauseilenden Gehorsams weist sie scharf zurück, eine Argumentation, die stark an „Aber ich habe doch nur Befehle von Oben ausgeführt" erinnert.

Zugegeben: Es ist schwer für ein Ideal einen mühsam aufgebauten Betrieb zu riskieren. Nur, auf mittlere Sicht wäre es deutlich schlauer gewesen, wenn die ICTF auf gerichtlichem Wege eine Beschlagnahme o.ä. bei ihren Mitgliedern verhindern würde,

indem sie höchstinstanzlich feststellen läßt, daß sie nicht für die Bits verantwortlich gemacht werden können, die auf den Platten dieser Welt liegen. Der jetzige Weg führt geradewegs in die Falle, daß etliche Großbeamte zur Überzeugung gelangen, daß Internet-Zensur zumindest partiell möglich ist, wenn man nur genügend Druck auf die ISPs macht. Das letzte, vor Redaktionsschluß vorliegende Schreiben der BAW an die ICTF spiegelt diese Erkenntnis sehr deutlich wieder:

Briefverteilung im Pariser Hauptpostamt zur Zeit Ludwigs XV.: Hier wird die verdächtige Korrespondenz für das »Cabinet noir« aussortiert

„Mein Telefax-Schreiben vom 30. August 1996 bezog sich ausdrücklich auf die vorgenannte URL und nicht auf eine einzelne IP-Nummer. Daher scheinen mir die Betreiber, welche bislang nur eine IP-Nummer gesperrt haben, ihrer Verpflichtung nicht vollständig Genüge getan zu haben, sofern hierdurch mögliche strafrechtliche Konsequenzen vermieden werden sollen.

Vielmehr erscheint es hierzu notwendig, sämtliche technischen Möglichkeiten auszuschöpfen, um einen Abruf der Druckschrift „radikal Nr. 154“ über die o.a. URL zu unterbinden.“

XS4ALL wird jedenfalls alle technischen und juristischen Möglichkeiten nutzen, um auch den Internet-Usern in Deutschland eine weitere Betrachtung ihrer Seiten zu ermöglichen. Erwogen werden Klagen gegen die ICTF und die BAW wegen Geschäftsschädigung usw. Die von der BAW beanstandeten Seiten sind mittlerweile auf dutzenden Servern auf der ganzen Welt gespiegelt (siehe Mirrorliste), wie das halt bei verfolgten Inhalten im Netz so üblich ist.

Ob auf längere Sicht ein Widerstand gegen ein internationale koordinierte Netzzensur möglich ist, wird sich noch erweisen müssen, aber jetzt schon vor den beamteten Moralhütern in die Knie zu gehen ist ein echter Fehler. Eine langfristige Erhaltung der Freiheit des Wortes im Netz wird nur dann erfolgreich sein, wenn um jeden Fußbreit Boden gekämpft wird. Kompromisse sind hier definitv der erste Schritt in die falsche Richtung.

frank@ccc.de

Was tun bei Zensur?

Was tun, wenn mein Provider einen Server zensiert?

- Beweise sichern (Traceroutes, Logs etc.)
- Höflich auf technische Fehlfunktion aufmerksam machen und Behebung mit Frist anmahnen
- ISP sagt, die Sperre ist absichtlich —> schriftlich anfordern
- Falls daraufhin keine Reaktion, Aufforderung maximal 2 Mal wiederholen
- höflich darauf aufmerksam, machen, daß man gedenkt einen Anwalt zu konsultieren
- Anwalt o. ä. (Verbraucherberatung, Kammer, Verein) einschalten
- Unterlassungerklärung verlangen, sonst einstweilige Verfügung androhen
- Einstweilige Verfügung beantragen
- Auf Schadenersatz klagen

Was tun, wenn ich als Provider zensiert werde?

- Internet-Adressen per Rotation über möglichst viele Class-C-Netze
- Möglichst viele Mirrors von den inkriminierten Inhalten schaffen
- Anonyme Proxies benutzen
- Alternative Routingwege suchen und freischalten
- Modemeinwahlen für Download der inkriminierten Inhalte schaffen

Mirror-Liste für radikal

http://www.jca.or.jp/~taratta/mirror/radikal/
http://www.canucksoup.net/radikal/index.html
http://www.connix.com/~harry/radikal/index.htm
http://burn.ucsd.edu/%7Eats/RADIKAL/
http://www.well.com/~declan/mirrors/
http://www.denhaag.org/~radikal
http://www.knooppunt.be/~daniel/radikal
http://www.dsvenlo.nl/~vvd/radikal/
http://www.why.net/home/static/radi
http://www.xs4all.nl/~jeroenw/radikal/
http://www.dreamy.demon.co.uk/occam/
http://www.ibmpcug.co.uk/~irdial/live_free/
http://zero.tolerance.org/radi/index.htm
http://www.meaning.com/library/radikal/
http://www.xs4all.nl/~irmed/radikal/
http://www.walli.uwasa.fi/~tviemero/radikal http://www.sko.it/~sfede/radi/index.htm
http://bellp.med.yale.edu/index.htm
http://www.euronet.nl/users/funest/radi/index.htm
http://www.charm.net/~gbarren/radikal
http://login.datashopper.dk/~pethern/radikal/
http://emma.unm.edu/radikal
http://www.serve.com/~spg/
http://huizen.dds.nl/~radikal
http://www.ecn.org/radikal
http://home.ipr.nl/~radikal/
http://fine.com/radikal
http://www.lab.net/radikal
http://www.bart.nl/~sz/index.html
http://www.ganesa.com/radikal/
http://www.tacacs.com/radikal/“

Phone: Call and login as „new“
Amsterdam Zoetermeer Maarssen
+31 20 5350535 [V.34], +31 79 3611011 [V.34], +31 346 550455 [V.34], +31 20 4223422 [UUCP], +31 79 3600800 [ISDN PPP], +31 346 553613 [ISDN PPP], +31 20 6265060 [ZyXEL], +31 79 3630569 [ISDN X.75], +31 346 555285 [ISDN X.75], +31 20 4229700 [ISDN PPP], +31 20 4206782 [ISDN X.75]

Generation @

Ein Brief an die Generation X.

Ihr seid unsere Eltern. Ihr steht morgens auf und fahrt zur Arbeit ins Büro oder ins Werk. Ihr geht mittags in die Kantine und abends setzt Ihr Euch vor den Fernseher. Oder Ihr geht in die Kneipe, um Freunde zu treffen. Zu Weihnachten und zu Geburtstagen bekommt Ihr Post von Bekannten und versprengten Mitgliedern der Familie. Und am Wochenende fahrt Ihr raus in Grüne. Oder in den Actionpark da unten im Süden.

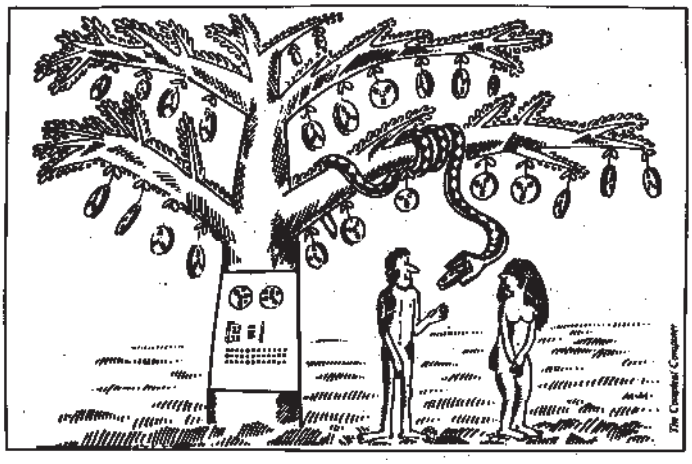
Wir haben unsere Pubertät vor irgendwelchen Fernsehern verbracht, beschäftigt damit, geheimnisvolle Zeichenfolgen in sinnlose Geräusch- und Grafikeffekte umzuwandeln. Wenn es dann geklappt hat, sind wir im Freudentaumel aus dem Keller gestürmt und haben von Euch nur verständnislose Blicke geerntet. Ihr habt uns seit einigen Jahrzehnten jede Weihnachten neues Spielzeug gekauft und wir haben damit lange Nächte dem Knistern und Quäken irgendwelcher Sender in fremden Ländern gelauscht.

Und wenn wir dann früh morgens mit dicken Ringen unter den Augen ins Bett gekrochen sind, haben wir von Euch nur ein unwirsches Murmeln geerntet. Wir haben gespielt. Und ihr habt darüber gelächelt: Fasziniert von blinkenden Lichtern, gefesselt von kleinen schwarzen Käfern. Ihr habt Witze über uns gemacht.

Und wir haben weiter unsere kleinen Kabel verlegt. **Überall.** Und damit haben wir Euch inzwischen die Welt gestohlen.

Ihr steht morgens auf und fahrt zur Arbeit ins Büro. Und da sind sie nun, die Kabel und die Blinklichter. Das Lotus-Notes-Windows95-SAP-Office-Automation-Netz ist da. Oder ins Werk, wo jetzt eine CNC Maschine Teile herstellt, die von einem Roboter unter die automatische Qualitätskontrolle gelegt werden. Mittags in der Kantine steckt Ihr die Chipkarte in die elektronische Kasse, um Euer Essen zu kaufen. Und abends setzt Ihr Euch vor den Fernseher und schaltet die Set-Top-Box ein, um ein Abendprogramm zu kaufen, in dem der Bunderkanzler ersten Musterdrucke der brandneuen Euro-Noten vorstellt. „So ein Unsinn“ hört Ihr uns sagen. „Wir haben eCash – wozu sollten wir das ausdrucken?“

Oder Ihr geht in die Kneipe, um festzustellen, daß an der Stelle jetzt ein Internet-Cafe aufgemacht hat. Zu Weihnachten oder zu Geburtstagen bekommt Ihr Post von versprengten Mitgliedern der Familie. Nur daß jetzt seltsame Absender darauf stehen und Sätze wie „Ich habe mir jetzt eine eMail-Adresse zugelegt." oder „Fax mal wieder." Aber Ihr seid stolz darauf, nichts neueres in die Hand zu nehmen als ein Telefon.



Welches Telefon übrigens? Denn Eure Tochter hat das Telefon abgemeldet und stattdessen ISDN legen lassen. „Ist billiger, Papa. Und bequemer." Und einen Brockhaus hat sie sich besorgt, da auf dieser komischen Silberscheibe. „Ist billiger, Papa. Und bequemer." Ihr kennt das schon.

Als Ihr jung ward, da seid Ihr aufgestanden und habt gegen Eure Eltern kämpfen müssen. Ihr habt ihnen die Welt abgerungen, in einem offenen und fairen Kampf, damals, als wir geboren wurden. Und dann habt Ihr so weitergemacht wie sie. Wir sind anders. Wir haben sie Euch gestohlen, Stück für Stück. Arbeit, Freizeit, Geld, Telefon, Post, Kneipe ... ohne daß Ihr es gemerkt habt. Und wir haben sie umgebaut, klamm und heimlich.

Inzwischen sind einige von Euch aufgewacht und haben gemerkt, daß diese Welt nicht mehr die ist, für die sie die Regeln gemacht haben. Jetzt müssen sie schnell neue Regeln machen, für eine neue Welt, die sie nicht mehr verstehen.

Macht nur. Noch vier Jahre bis ins nächste Jahrtausend. **Wir** sind die Generation @.

Kristian Köhntopp
kris@schulung.netuse.de

Chaos im Äther

Chaosradio ist eine monatliche, dreistündige Radiosendung des CCC Berlin auf dem Berlin-Brandenburger Radiosender Fritz. Sie behandelt klassische Chaosthemen und debattiert aktuelle Trends der Informationstechnik und Ihres Einsatzes.
Informationen zu Chaosradio gibt es unter <http://berlin.ccc.de/Chaosradio/Chaosradio.html>

DeTeHack

Möge der Saft mit ihm sein...

Und es begab sich zum Ende einer Zeit, die im allgemeinen Sprachgebrauch des deutschen Volkes Sommerloch genannt wird, daß ein bekanntes deutsches Wirtschaftswochenmagazin (Wie?Wo?) nichts besseres zu tun hatte, als sich von einem hinlänglich als Gehilfe diverser Dreibuchstabenbehörden bekannten Münchener „Sicherheitsspezialisten“ namens Kim Schmitz alias Kimble einen dicken Bären aufbinden zu lassen. „Betrug im D-Netz“ lautete die vierfarbig-ganzseitige Titelzeile des Heftes, auf den Innenseiten war dann der in seriösem Tuch verkleidete „Computerspezialist“ auf Fotos zu bewundern, die an peinlicher Albernheit etliches in den Schatten stellen.

Kernaussage des Artikels war, dass ein Mitarbeiter einer „Zulieferfirma“ offenbar einiges an Informationen, insbesondere einige (alle?) Ki-Schlüssel von D1-Kunden und eventuell Details zum Aufbau der Algorithmen A3 und A8 weitergeben hat. (Zum genauen Aufbau und Ablauf der GSM-Authentifizierung und den Algorithmen siehe Artikel in dieser Ausgabe) Möglich - und nicht minder wahrscheinlich- ist nach der jetzigen Faktenlage allerdings auch, daß jemand mit einem Stapel D1-Kartenrohlinge und den Informationen und Geräten zur Codierung derselben die geheiligten Werkhallen verlassen hat.

Der Serviceprovider Mobilcom sah sich jedenfalls nach einigen Tagen in der Lage 100.000 Mark als Spende an einen Verein auszuloben, den derjenige bennen könne, der auf Kosten der D1-Nummer 0171-3289966 ein Gespräch führe. Bis zum Redaktionsschluß war von einer erfolgreichen Auslösung dieses doch relativ angemessenen Betrages nichts zu hören.

Kimble weigerte sich nach Aussagen der DeTeMobil bisher auch standhaft, seine angeblich doch so tollen Hackerkünste vorzuführen. Weder die Zusage der Straffreiheit noch ein eher substantielles Angebot von diversen Medien nebst staatsanwaltlicher Bestätigung der Rechtmäßigkeit solchen Tuns konnte ihn bisher dazu bringen. Alle Indizien sprechen dafür, das der weniger für seine Fähigkeiten als Hacker als für seine Breitquatschkünste berüchtigte Kimble Kontakt zu jemand hatte, der auf die eine oder andere Weise Gespräche auf Kosten fremder Rufnummern führen kann/konnte.

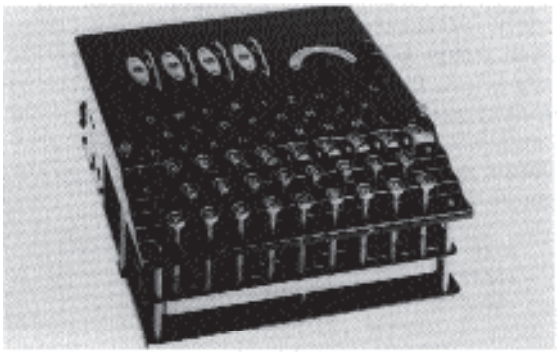
Laut Kimble führt er Gespräche mit der DeTeMobil, die ihm Straffreiheit (und wahrscheinlich einen Batzen Kleingeld) zusi-

chern soll. Ergebnis dieser Verhandlungen wird wohl auch eine Art Stillschweigeabkommen sein, das Kimble verpflichtet, sich nicht mehr zum Thema zu äußern. Hernach dürfte die DeTeDebil eine Pressekonferenz veranstalten auf der verkündet wird, alles sei sicher.

In einem Telefongespräch sprach Kimble von einer „Backdoor“ im Authentication Center (AuC) des HLR, der sich angeblich nur mit Hilfe von Insiderinformationen nutzen lasse. Wir bemühen uns zur Zeit um eine Klärung der technischen Zusammenhänge. Stay tuned.

frank@ccc.de

Sicherheit ist Vertrauenssache



Authorisierung und Verschlüsselung in GSM-Netzen

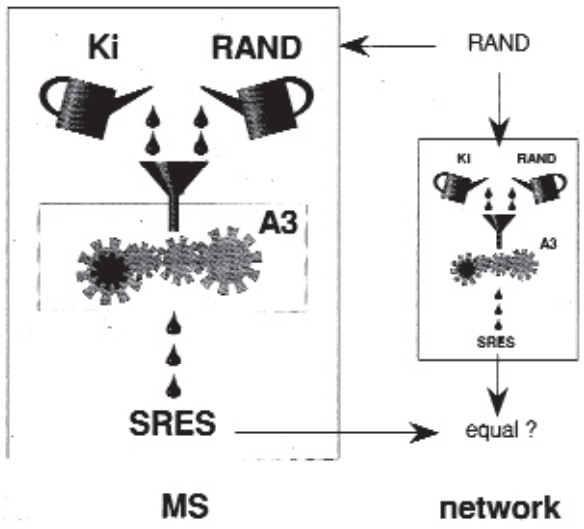
Naja, wirklich konsequent wird die Sicherheit beim Telefonieren auch bei GSM nicht betrieben, eine end-to-end-Verschlüsselung und Authentifizierung gibt es auch bei GSM nicht. Aber zumindest der Hauptangriffspunkt für einen Angriff auf das System, die Funkschnittstelle, wurde ausreichend gesichert.

Die Absicherung der Funkschnittstelle verfolgt zwei prinzipielle Ziele: zum einen die Verschlüsselung der Sprach- und Vermittlungsdaten, um ein Abhören zu verhindern, und zum anderen, um die Identität des Benutzers zu überprüfen. Beide Funktionen sind eng miteinander verwoben.

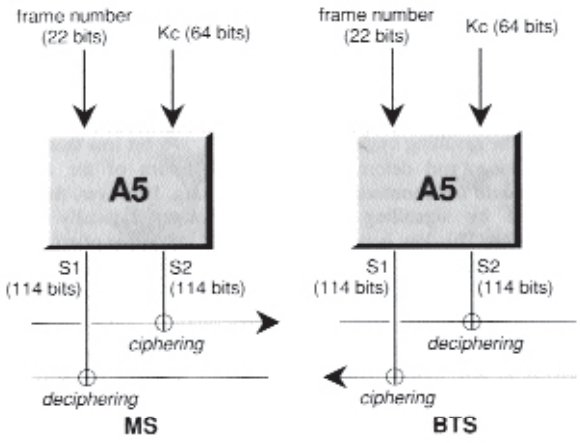
Der wichtigste Sicherheitsparameter des GSM ist der sogenannte Ki. Das ist ein geheimer Schlüssel, der sowohl in der SIM-Karte des Benutzers, als auch im sogenannten Home Location Register (HLR) im Heimatnetz des Benutzers gespeichert ist. Der Parameter Ki wird niemals zu anderen Komponenten des Netzes übertragen.

Die Überprüfung der Identität des Benutzers geschieht unter Benutzung von Ki. Das MSC, die Zentrale, bei der der Benutzer

eingebucht ist, sendet über die Zelle eine Nachricht an das Endgerät mit der Aufforderung, die Authentifizierung durchzuführen. In dieser Nachricht befindet sich ein zufällig gewählter Parameter von 128 Bit Länge, genannt RAND. Das Endgerät schickt diesen Wert an die SIM-Karte weiter.



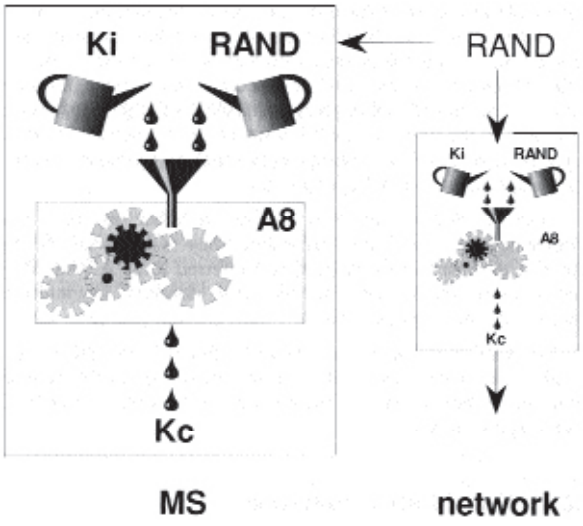
Die SIM-Karte berechnet jetzt aus RAND und Ki mit Hilfe des Algorithmis A3 einen 32 Bit langen Wert: SRES. Dieser wird dann vom Telefon an das MSC gesendet. Zu einem etwas früheren Zeitpunkt hat das MSC mit dem HLR des Benutzers Kontakt aufgenommen und dort ein RAND/SRES-Paar berechnen lassen. Der vom HLR gelieferte SRES wird jetzt mit dem vom Telefon verglichen, sind beide identisch, ist die Authentifizierung erfolgreich.



Gleichzeitig mit der Berechnung von SRES wird mit Hilfe von Ki, RAND und dem Algorithmus A8 ein Parameter Kc von 64 Bit Länge berechnet. Zu einem späteren Zeitpunkt schickt das MSC an das Endgerät die Aufforderung, die Verbindung zu verschlüsseln. Ab diesem Zeitpunkt wird jeder gesendete Burst mit dem Algorithmus A5 verschlüsselt, hierzu werden Kc und eine 22 Bit lange Framenummer als Schlüssel verwendet. Das MSC bekommt seinen Kc wieder vom HLR.

Die Algorithmen A3, A5 und A8 werden von GSM nicht näher spezifiziert. Durch die Einbeziehung des HLR ergibt sich, daß A3 und A8 netzspezifisch sein können, beide werden nur im HLR und in der SIM-Karte benötigt. Im Gegensatz dazu muß jedes MSC dasselbe A5 sprechen, um ein Roaming zwischen Netzen zu erlauben. Das GSM Memorandum of Understanding (MoU), ein Zusammenschluß der Netzbetreiber, hat deshalb einen A5 spezifiziert.

Die A5-Spezifikation ist zwar geheim, allerdings ist schon vor einiger Zeit im Internet ein Sourcecode aufgetaucht, der mit hoher Wahrscheinlichkeit A5 oder eine Vorläuferversion des A5 ist. Die Analyse liest sich recht interessant, besonders, da sich auch aus anderen Quellen ergibt, daß die maximal nutzbare Schlüssellange vom MoU auf einen Wert kleiner 64 bit festgelegt wurde.



Insgesamt ist die Sicherung der Funkstrecke als eher durchschnittlich anzusehen. Da A3 und A8 nicht bekannt sind, läßt sich über deren Sicherheit keine besonders gute Aussage treffen - noch dazu, wo diese netzspezifisch sind und außerdem auf der SIM Platz finden müssen. Wahrscheinlicher ist allerdings ein Angriff auf die Authentifizierung mit gestohlenen Ki.

Anders sieht es bei der Verschlüsselung aus. Da A5 vom MoU standardisiert wurde, ist er entsprechenden Stellen bekannt, diese dürften auch über die notwendige mittelschwere Hardware verfügen, um unten angedeuteten Angriff durchzuführen.

andreas@ccc.de

Is Not Much Good

A closer look at the A5 GSM Encryption Algorithm

>From sci.crypt Fri Jun 17 17:11:49 1994
From: rja14@cl.cam.ac.uk (Ross Anderson)
Date: 17 Jun 1994 13:43:28 GMT
Newsgroups: sci.crypt,alt.security,uk.telecom
Subject: A5 (Was: HACKING DIGITAL PHONES)

The GSM encryption algorithm, A5, is not much good. Its effective key length is at most five bytes; and anyone with the time and energy to look for faster attacks can find source code for it at the bottom of this post.

The politics of all this is bizarre. Readers may recall that there was a fuss last year about whether GSM phones could be exported to the Middle East; the official line then was that A5 was too good for the likes of Saddam Hussein.

However, a couple of weeks ago, they switched from saying that A5 was too strong to disclose, to saying that it was too weak to disclose! The government line now pleads that discussing it might harm export sales.

Maybe all the fuss was just a ploy to get Saddam to buy A5 chips on the black market; but Occam's razor suggests that we are really seeing the results of the usual blundering, infighting and incompetence of bloated government departments.

Indeed, my spies inform me that there was a terrific row between the NATO signals agencies in the mid 1980's over whether GSM encryption should be strong or not. The Germans said it should be, as they shared a long border with the Evil Empire;

but the other countries didn't feel this way, and the algorithm as now fielded is a French design.

A5 is a stream cipher, and the keystream is the xor of three clock controlled registers. The clock control of each register is that register's own middle bit, xor'ed with a threshold function of the middle bits of all three registers (ie if two or more of the middle bits are 1, then invert each of these bits; otherwise just use them as they are). The register lengths are 19, 22 and 23, and all the feedback polynomials are sparse.

Readers will note that there is a trivial 2^40 attack (guess the contents of registers 1 and 2, work out register 3 from the keystream, and then step on to check whether the guess was right). 2^40 trial encryptions could take weeks on a workstation, but the low gate count of the algorithm means that a Xilinx chip can easily be programmed to do keysearch, and an A5 cracker might have a few dozen of these running at maybe 2 keys per microsecond each. Of course, if all you want to do is break the Royal Family's keys for sale to News International, then software would do fine.

It is thus clear that A5 should be free of all export controls, just like CDMF and the 40-bit versions of RC2 and RC4.

Indeed, there seems to be an even faster attack. As the clock control is stop-go rather than 1-2, one would expect some kind of correlation attack to be possible, and on June 3rd, Dr Simon Shepherd of Bradford University was due to present an attack on A5 to an IEE colloquium in London. However, his talk was spiked at the last minute by GCHQ, and all we know about his attack is:

(a) that sparse matrix techniques are used to reconstruct the initial state (this was published as a `trailer' in the April 93 `Mobile Europe');

(b) that he used some of the tricks from my paper `Solving a class of stream ciphers' (Cryptologia XIV no 3 [July 90] pp 285 - 288) and from the follow-up paper `Divide and conquer attacks on certain classes of stream ciphers' by Ed Dawson and Andy Clark (Cryptologia XVIII no 1 [Jan 94] pp 25 - 40) (he mentioned this to me on the phone).

I believe that we have to stand up for academic freedom, and I hope that placing A5 in the public domain will lead to the embargo on Simon's paper being lifted.


COUPÉ-Berufsberatung:

BND-Beamter/in
(mittlerer nichttechnischer Dienst)

Hackerjagd im Internet

Tsutomu Shimomura

„Data Zone – Die Hackerjagd im Internet“

Erscheint im Oktober 96, dtv 15101

„Am 1. Weihnachtsfeiertag des Jahres 1994 fährt der 30jährige Computersicherheitsexperte Tsutomu Shimomura in den wohlverdienten Skiurlaub. Zur selben Zeit hackt sich irgend jemand zu Hause in San Diego in seinen Computer und klaut seine eMails. Tsutomu läßt seine Skier, wo sie sind, schnappt sich seinen 2.4 GB 85Mhz SPARC Laptop samt Funktelefon und nimmt die Verfolgung auf...“

In seinem Buch „Data Zone“ beschreibt Tsutomu Shimomura seine 50 Tage währende Jagd nach Kevin Mitnick. Bis ins Detail rekonstruiert Tsutomu in Zusammenarbeit mit dem Computerjournalisten John Markoff minutiös die Ereignisse und Vorgehensweisen, die zur Verhaftung von Mitnick geführt haben. Sehr anschaulich berichtet er aber auch über seinen eigenen Lebensstil, über die Beziehung die er während der Jagd zu dem Phantom Mitnick aufgebaut hat, über sein Umfeld und alle Ereignisse, die Ihm in diesem Zusammenhang wichtig erschienen.

Ein alles in allem interessanter Einblick in das „ganz normale“ Leben eines Computersicherheitsexperten, der versucht, alles über das „ganz normale“„ Leben eines „echt miesen“ Hackers herauszufinden.

Wer sich mit der Materie überhaupt nicht auskennt, der sei gewarnt. Tsutomus Erläuterungen setzen teilweise ein zumindest rudimentäres Verständnis von Unix voraus. Die ausgewachsenen Hacker seien ebenfalls gewarnt. Die neuesten Tricks und dollsten Hacks werden sie hier nicht finden.

IMPRESSUM
Die Datenschleuder Ausgabe Nr. 56 September 1996
Herausgeber: Chaos Computer Club e.V., ccc@ccc.de, Schwenckestr. 85, D-20255 Hamburg, Tel +49 (40) 4018010, Fax +49 (40) 4917689 **Redaktion:** Redaktion Datenschleuder, ds@ccc.de, Neue Schönhauser Str. 20, D-10178 Berlin, Tel +49 (30) 283 54 87 2, Fax +49 (30) 283 54 87 8 **ViSdP:** Wau Holland (via Redaktion) **Druck:** St. Pauli Druckerei, Hamburg **Mitarbeiter dieser Ausgabe:** Tim Pritlove (tim@ccc.de), Bishop (bishop@ccc.de), FrankRo, fiedel (fiedel@ccc.de), Frank Rieger (frank@ccc.de), Wau Holland (wau@ccc.de) Lars (lars@ibp.de) **Eigentumsvorbehalt:** Diese Zeitschrift ist solange Eigentum des Absenders, bis sie dem Gefangenen persönlich ausgehändigt worden ist. Zur-Habe-Nahme ist keine persönliche Aushändigung im Sinne des Vorbehalts. Wird die Zeitschrift dem Gefangenen nicht ausgehändigt, so ist sie dem Absender mit dem Grund der Nichtaushändigung in Form eines rechtsmittelfähigen Bescheides zurückzusenden. **Mitglieder des CCC e.V.** erhalten die Datenschleuder im Rahmen Ihrer Mitgliedschaft.. Das **Titelbild** zeigt die Zeichnung „Der Spitzel“ von Honoré Daumier. **Diese DS** ist kurz wg. kein Geld.

Oligopoly

E-Plus Service lehnt Sonderkündigungsrecht bei Gebührenerhöhung ab.

Es lächelt das türkise Vögelchen in der Werbung. Wie in der letzten DS berichtet, führt E-Plus zum 1.11.96 eine Gebühr für Kurzmitteilungen (SMS) ein. Da es sich um eine Änderung der Vertragsbedingungen zum Nachteil des Kunden handelt, besteht im allgemeinen ein Sonderkündigungsrecht zum Zeitpunkt der Änderung.

Die E-Plus Service GmbH, hauseigener Provider von E-Plus, sieht das allerdings anders: In den Geschäftsbedingungen, die der Kunde anerkannt hat, räumt sich der Diensteanbieter zwar das Recht ein, die Tarife nach Ankündigung zu erhöhen, nicht jedoch dem Kunden, den Vertrag zu kündigen.

Man stelle sich folgendes Szenario vor: E-Plus erhöht die Grundgebühr auf DM 500 pro Monat, und der Kunde muß laut Vertrag zahlen. Da aber selbst diese Absurdität die Rechtabteilung von E-Plus nicht davon überzeugen kann, daß die Verträge von E-Plus-Service nicht dem Gesetz für Allgemeine Geschäftsbedingungen entsprechen, wird das Thema SMS-Tarifierung mit großer Wahrscheinlichkeit vor Gericht verhandelt werden.

Im Antwortschreiben auf Kündigungen zum 31.10.96 hat der Serviceprovider unmißverständlich zu verstehen gegeben, daß man auf keinen Fall einer außerordentlichen Kündigung stattgeben werde; die Tarife seien schließlich nicht Vertragsbestandteil und können nach 4.3 der Geschäftsbedingungen jederzeit geändert werden.

Der Verbraucherberatung Berlin fehlt der entsprechende Passus in den Vertragsbedingungen, daß bei Preiserhöhungen ein Kündigungsrecht besteht. E-Plus-Kunden, die aus diesem Grund kündigen möchten, rät man dort, dies unverzüglich per Einschreiben-Rückschein zu tun und im Brief darauf hinzuweisen, daß die Tarife sehr wohl Vertragsbestandteil sind.

FrankRo

Bestellfetzen

Ab sofort ist eine Trennung von Bestellungen und Mitgliedsanträgen bzw. Abos notwendig.

Dadurch geht beides schneller. Ggf. Name und Anschrift doppelt eintragen. Danke.

Preise gültig bis zur nächsten Ausgabe (DS57).

Absender, Bezugs- und Bestellanschrift:

Chaos Computer Club e.V.
Schwenckestraße 85
D-20255 Hamburg
Tel +49 (40) 40 18 01-0
Fax +49 (40) 491 76 89

o Ich möchte erstmal mehr wissen; bitte schickt mir die Satzung des CCC e.V. und einen Mitgliedsantrag; 5.- DM lege ich in Briefmarken bei.

o Ich will Mitglied werden, kann aber nur den ermässigten Jahresbeitrag von 60.- DM im Jahr zahlen. Zusammen mit der einmaligen Verwaltungspauschale von 20.- DM zahle ich also erstmal 80.- DM, zahlungsweise siehe unten.

o Ich will Mitglied werden und kann den normalen Jahresbeitrag von 120.- DM zahlen. Inkl. einmaliger Verwaltungspauschale also 140. -DM, zahlweise siehe unten.

o Ich will Mitglied werden und kann einen Förderjahresbeitrag von _____ DM zahlen. Diesen zahle ich hiermit zusammen mit der Verwaltungspauschale von 20.- DM.

o Ich möchte die Datenschleuder abonnieren; zum Normalpreis von 60.- DM für 8 Ausgaben.

o Ich möchte die Datenschleuder abonnieren, kann aber nur den ermässigten Preis von 30.-DM für 8 Ausgaben zahlen.

Die Kohle liegt o in bar o als Verrechnungsscheck o in Briefmarken bei bzw.

o wurde überwiesen am _____ auf das Kto. 59 90 90 - 201 bei der Postbank Hamburg BLZ 200 100 20 des Chaos Computer Club e.V.

Ort/Datum/Unterschrift _____

Literatur

____	05,00 DM	Doku zum Tod von „KGB" Hacker K.Koch
____	29.80 DM	Deutsches PGP-Handbuch + aktuelle Version
____	25.00 DM	Vollständige Dokumentation des CCC'93

Alte Datenschleudern

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

Aufkleber teilweise nur noch Restposten, solange Vorrat reicht.

____	05,00 DM	1 Bogen (68 Aufkleber) „Chaos im Äther"
+	05,00 DM	Portopauschale!

____ Gesamtbetrag o liegt als V-Scheck o in Bar bei bzw.
o wurde am _____ überwiesen auf das Konto 59 90 90 - 201 bei der Postbank Hamburg (BLZ 200 100 20) des CCC e.V.

Name _____

Straße _____

PLZ, Ort _____