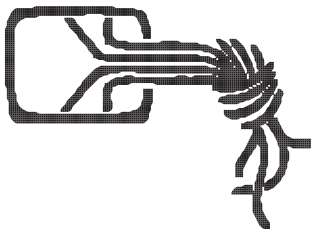
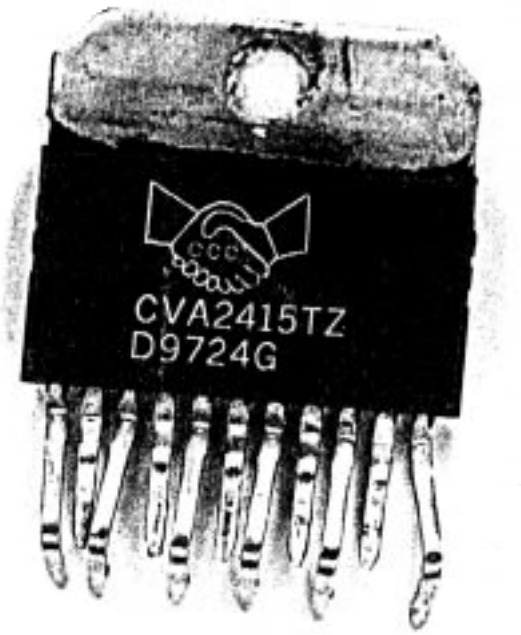
Die Datenschleuder



Das wissenschaftliche Fachblatt für Datenreisende
Ein Organ des Chaos Computer Club



- *Eckpunkte der deutsche*
- *weisses Papier*
- *Chaos Communication Camp*

ISSN 0930-1045
Sommer 1999, DM 5,00
Archivexemplar 1/2015

Impressum

Die Datenschleuder Nr. 67
II. Quartal, Sommer 1999
Herausgeber:
(Abos, Adressen etc.)
Chaos Computer Club e.V.,
Lokstedter Weg 72,
D-20251 Hamburg,
Tel. +49 (40) 401801-0,
Fax +49 (40) 401801-41,
EMail: office@ccc.de
Redaktion:
(Artikel, Leserbriefe etc.)
Redaktion Datenschleuder,
Postfach 640236, D-10048 Berlin,
Tel +49 (30) 280 974 70
Fax +49 (30) 285 986 56
EMail: ds@ccc.de
Druck: St. Pauli Druckerei Hamburg

CvD und ViSdP: dieser Ausgabe:
Andy Müller-Maguhn(andy@ccc.de)

Mitarbeiter dieser Ausgabe:
Djenia, Henriette, Chris, Tim, Zapf Dingbatz

Adressen http://www.ccc.de/ChaosTreffs.html

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

Erfa-Kreise

Hamburg: Lokstedter Weg 72, D-20251 Hamburg, mail@hamburg.ccc.de Web: http://hamburg.ccc.de Phone: +49 (40) 401801-0 Fax: +49 (40)401 801 - 41 Voicemailbox +49 (40) 401801-31. Treffen jeden Dienstag ab ca. 20.00 Uhr in den Clubräumen. Der jeweils erste Dienstag im Monat ist Chaos-Orga-Plenum (intern), an allen anderen Dienstagen ist jede(r) Interessierte herzlich willkommen. Öffentliche Workshops im Chaos-Bildungswerk fast jeden Donnerstag. Termine aktuell unter http://www.hamburg.ccc.de/Workshops/index.html

Berlin: Club Discordia alle zwei Wochen Donnerstags zwischen 17 und 23 Uhr in den Clubräumen in der Marienstr. 11, Hinterhof in Berlin-Mitte. Nähe U-/S-Friedrichstrasse. Tel. (030) 285986-00, Fax. (030) 285986-56. Briefpost CCC Berlin, Postfach 640236, D-10048 Berlin. Aktuelle Termine unter http://www.ccc.de/berlin

Köln: Der Chaos Computer Club Cologne zieht gerade um. Aktuelle Koordinaten bitte unter mail@koeln.ccc.de bzw. http://www.koeln.ccc.de erfragen. Telefonische Erreichbarkeit erst wieder nach vollständigem Bezug neuer Räume.

Ulm: Kontaktperson: Frank Kargl <frank.kargl@ulm.ccc.de> Electronic Mail: contact@ccc.ulm.de Web: http://www.ulm.ccc.de/ Treffen: Jeden Montag ab 19.30h im 'Café Einstein' in der Universität Ulm.

Bielefeld: Kontakt Sven Klose Phone: +49 (521) 1365797 EMail: mail@bielefeld.ccc.de. Treffen Donnerstags, ab 19.30 Uhr in der Gaststätte 'Pinte', Rohrteichstr. 28, beim Landgericht in Bielefeld. Interessierte sind herzlich eingeladen.

Chaos-Treffs: Aus Platzgründen können wir die Details aller Chaos-Treffs hier nicht abdrucken. Es gibt in den folgenden Städten Chaos-Treffs, mit Detailinformationen unter http://www.ccc.de/ChaosTreffs.html:

Bochum/Essen, Bremen, Burghausen/Obb. und Umgebung, Calw, Dithmarschen/Itzehoe, Dresden, Emden / Ostfriesland, Eisenach, Erlangen/Nürnberg/Fürth, Frankfurt a.M., Freiburg, Freudenstadt, Giessen/Marburg, Hanau, Hannover, Ingolstadt, Karlsruhe, Kassel, Lüneburg, Mannheim/Ludwigshafen/Heidelberg, Mönchengladbach, München, Münster/Rheine/Coesfeld/Greeven/Osnabrück, Rosenheim/Bad Endorf, Neunkirchen/Saarland, Würzburg, Schweiz/Dreyeckland: Basel, Österreich: Wien

Worte an die Leser

Glaubten einige von uns bisher, nur mehr oder minder minder gesetzestreue Hacker, die sich mit Verschlüsselungs- und Sicherheitstechnologie beschäftigen sind in der Gefahr, unter unklaren Umständen zu verunglücken, so ist das spätestens seit Anfang Mai vorbei. Der Referatsleiter des Bundeswirtschaftsministeriums, der den in dieser Ausgabe dokumentierten Kabinettsbeschluß zu den Eckpunkten der deutschen Kryptopolitik verfasst hat, fiel aus bislang ungeklärten Gründen noch in der Nacht nach Versand des Dokuments an das Innenministerium aus dem Fenster seiner im dritten Stock gelegenen Wohnung - und überlebte, schwerverletzt. Noch im Dezember hatte er auf dem Chaos Communication Congress über die aktuelle Frontlage des Kryptowars und den Wassenaarverhandlungen berichtet. Natürlich wird es sich alles tragischer aber zufälliger Unfall entpuppen.

Trotzdem verbleibt ein bitterer Nachgeschmack angesichts der offen liegenden Zusammenhänge, in denen man sich beim Einsatz für freie Verschlüsselung nicht nur beliebt macht. Dokumentieren können wir immerhin den zwischenzeitlich verabschiedeten Eckpunktekatalog; ein anderes Projekt des verunglückten ist derweil ins Stocken gekommen. So gibt es bisher nicht verifizierte Hinweise, daß es die oft genannte deutsche Kryptoindustrie gar nicht mehr gibt; die Firmen mit Sitz in Deutschland von Ausländischen Interessenten erworben wurden. Dezentrale Recherchen angenehm. Sinn würde es machen: Die amerikanische Gesetzeslage z.B. gilt ja auch für Firmen in amerikanischem Besitz.

Apropos Amerika: Unsere Werte Justizministerin bekam jüngst Post aus Amerika. Sie hat zwar von dem Thema keine Ahnung, wurde aber trotzdem von einer entsprechenden Stelle gebeten, dafür zu sorgen daß keine harten Kryptoprodukte unter dem Wassenaar-Begriff „public domain“ fallen. Andere nennen es deutsch-amerikanische Freundschaft.

Auf dem Camp (6.-8. August, www.ccc.de/camp) werden wir daher hoffentlich nicht nur viel Spaß am Gerät haben; viele internationale Gruppen wie z.B. die Cypherpunks haben sich angekündigt um mit uns die Lage zu verbessern. Auch im Reengineering-Bereich gibt´s einiges zu untersuchen; bringt mal mit, was es noch zu untersuchen gilt.

Zum Thema Untersuchen haben wir in dieser Ausgabe eine Einführung in die Befreiung von Bits aus Chipkarten; ob das Hacken oder Förderung der Sicherheitsindustrie ist, sollten wir angesichts des derzeitgen Umfelds mal im Detail auf dem Camp diskutieren. Bis dahin viel Spaß beim Sachenpacken... andy@ccc.de

---

Chaos Realitäts Dienst

/Y2K/Banken/Literatur: Ausfallplanung der deutschen Banken

Eines der bislang am detaillierfreudigsten ausgearbeiteten öffentlichen Papier zum Jahr-2000 Problem gibt es vom Bundesverband deutscher Banken. Dort sind vor allem die Dominoeffekte sehr schön geschildert, ohne daß besondere Rücksicht auf die Informationspolitik öffentlicher Stellen genommen wurde. Lesenswert:

http://www.bdb.de/verband/jahr2000/ausfallplanung.htm

/Y2K/Stellungnahmen/Regierung: "Kein Anlaß zur Panik"

Die Bundesregierung hat mittlerweile einen aktualisierten Bericht zum Jahr-2000-Problem vorgelegt. Laut einer Meldung des Heise-Tickers vom 21.04. betone Bundeswirtschaftsminister Werner Müller (parteilos) , daß "zu Panik und großen Befürchtungen" nach allen Experten-Erkenntnissen kein Anlaß bestehe.

http://www.heise.de/newsticker/data/wst-21.04.99-000/

/Internet/GeldohneUmwege Internet-Missbrauch für Kursmanipulationen: Falschmeldung über eine Fusion

Wie die Neue Züricher Zeitung am 8. April berichtete, ist es mehreren bislang nicht identifizierten Betrügern gelungen, durch eine gefälschte Web-Page sowie mit Meldungen am «Messageboard» von Yahoo eine als Bericht der Agentur Bloomberg vorgetäuschte Falschmeldung über einen Kauf der amerikanischen PairGain Technologies Inc. durch die israelische Rivalin ECI Telecom Ltd. für 1,35 Mrd. $ verbreitet. Der Kurs der an der Nasdaq gehandelten Aktien von PairGain legte darauf am Mittwoch vormittag vorübergehend um über 30% zu und schloss gleichentags immer noch um 10% höher, obschon beide Unternehmen schon gegen Mittag eine solche Fusion dementiert hatten und die Agentur Bloomberg selber mitgeteilt hatte, dass die Fusionsmeldung nicht von ihr stamme.

http://www.nzz.ch/online/01_nzz_aktuell/finanz/04_finanz.htm

/Opensource/danndochnoch SGI goes Open Source

Ein Hinderungsgrund gegen den Einsatz von Linux in großen Servern ist immer noch das Fehlen eines Journaling File Systems, das im Falle eines Crashes ohne Filesystemcheck (fsck) auskommt. Bei großen Systemem kann dieser durchaus Stunden dauern, so daß ein Wiederanlauf entsprechend träge wird. Auch die Suchzeiten in Verzeichnissen werden bei sehr großen Dateisystemen (sehr viele Dateien) zu lang. Hilfe kommt aus eher unerwarteter Richtung: Silicon Graphics (SGI) stellt ihr XFS-Dateisystem ab dem Sommer als Open Source zur Verfügung. Man darf auf Performancevergleiche gespannt sein. Mehr Info:

http://www.sgi.com/newsroom/press_releases/1999/may/xfs.html

/Chaos/Hamburg/Bildung Chaos-Bildungswerk Hamburg

Das Chaos-Bildungswerk hat die ersten Veranstaltungen hinter sich gebracht. Mit Elan wurden Vorträge über Programmiersprachen (Scheme, Perl), Netzwerkgrundlagen und ähnliches unters interessierte Volk gebracht. Aktuell stehen PGP, Firewalls, Datenbanken, demnächst Linux und Verhandlungstaktik auf dem Themenplan. Ständig aktuell ist dieser unter http://www.hamburg.ccc.de/Workshops/index.

Kurzmeldungen & Update

html zu finden. Dort gibt es auch Anfahrtbeschreibungen und ähnlich wegweisende Hinweise für den Datenreisenden. Termine sind in der Regel donnerstags um 19 Uhr 30 im CCC, Lokstedter Weg 72. Längere Workshops geraten aber auch schon einmal ins Wochenende. Die Veranstaltungen sind kostenlos, der Erfa-Kreis bittet aber um eine kleine Spende, um Flipchartblöcke, Folien usw. zu finanzieren - wir denken da an etwa 5 Mark, aber das ist absolut freiwillig. Zu einigen Veranstaltungen gibt es Handouts oder Foliensätze auf Papier oder elektronisch gegen Kostenbeteiligung. Irgendwann sollen die Sachen, soweit elektronisch vorhanden (abfotografierte Flipcharts sind nicht wirklich sinnvoll :-) auch ihren Weg ins Netz finden.

pirx@ccc.de

/Dasletzte/Softwaregutachten

Auszug aus einem Artikel in der Neuen Juristischen Wochenzeitschift Computerreport (NJW-CoR) 4/99, Seite 217ff, in dem es eigentlich um die Besonderheiten der Beweisbeschlüsse bei Software und Softwaregutachten geht...:

"Das wäre weiter nicht schlimm, wenn die Systemsoftware nur selten ausfallen würde. Stabile Betriebssysteme wie Unix, OS/2 oder bewährte Großrechner-Systeme laufen heutzutage monatelang ohne Abschaltung oder Ausfall. Das Systemhaus hatte dem Anwender jedoch, aus was für Gründen auch imer, eine notorisch unstabile Betriebssoftware, nennen wir sie W, empfohlen, von der bekannt ist, daß sie schon bei normalen Anwendungen selten mehr als einen Tag lang ohne Fehler läuft."

Autor des Artikels ist Dr Peter Schnupp, öffentlich bestellter und vereidigter Sachverständiger für Systemsoftware und Technik der Softwareentwicklung in Falkenberg-Altgmain.

migri@ccc.de

Best viewed with...

/Durch/DES

Sollte noch *irgendjemand* glauben, DES waere sinnvoll, möge er sich das hier geben: http://search.ietf.org/internet-drafts/draft-simpson-des-as-01.txt

Zitat: "The PPP DES Encryption Protocol" [RFC-2419], "The ESP DES-CBC Cipher Algorithm With Explicit IV" [RFC-2405], and "The ESP DES-CBC Transform" [RFC-1829] have been re-classified to Historic status, and implementation is Not Recommended.

/Datenschutz/Amerika/Ganzvorbei Bank sued over client data sale

Snipped from comp.risks digest 20.44

The state of Minnesota last week sued U.S. Bank for allegedly selling Social Security numbers, account balances and other sensitive customer data to a telemarketing company in exchange for commissions. Apparently several other banks are also hawking customer information, which raises serious privacy concerns. [Source: *ComputerWorld*, article by Kim S. Nash, 14 Jun 1999, http://www.computerworld.com/home/print.nsf/CWFlash/990614AE82 PGN]

Eckpunkte der deutschen Kryptopolitik

Bundesministerium des Innern /
Bundesministerium für Wirtschaft und Technologie

Bonn, den 2. Juni 1999

Eckpunkte der deutschen Kryptopolitik

Einleitung

Programme und Chips zur sicheren Verschlüsselung von Nachrichten waren bis Anfang der Neunziger Jahre ein relativ unbedeutender Nischenbereich der Computerindustrie. Dieser Nischenbereich ist heute jedoch von erheblicher Bedeutung für die wirtschaftliche und gesellschaftliche Entwicklung der Informationsgesellschaft insgesamt. Denn immer mehr entwickelt sich der Produktionsfaktor "Information" zu einem begehrten Rohstoff. Der effektivere Schutz dieses Rohstoffs kann über Erfolg oder Mißerfolg von Unternehmen und damit über Beschäftigungschancen im Informationszeitalter entscheiden und nur durch den Einsatz starker kryptographischer Verfahren läßt sich dieser Schutz heute effektiv gewährleisten. In jedem Fall ist die Leistungsfähigkeit dieser Technologie heute größer als jemals zuvor.

Die Kryptokontroverse in Deutschland

Bei der Kryptokontroverse geht es um die Frage, ob und in welchem Umfang die Nutzung kryptographischer Verfahren gesetzlich beschränkt werden solle. Die Frage ist in vielen demokratischen Industrieländern in den letzten Jahren kontrovers diskutiert worden. Auch in Deutschland fand eine intensive Auseinandersetzung, an der sich die Bundesressorts mit unterschiedlichen Positionen, die Wirtschaft sowie zahlreiche gesellschaftliche Gruppen beteiligten, hierüber statt.

Im Oktober 1997 verabschiedete das Bundeskabinett den "Fortschrittsbericht der Bundesregierung Info 2000: Deutschlands Weg in die Informationsgesellschaft", der eine Passage zur Kryptopolitik enthielt:

"Es wurde innerhalb der Bundesregierung Einvernehmen erzielt, in dieser Legislaturperiode auf eine gesetzliche Regelung des Inverkehrbringens und der Nutzung von Kryptoprodukten und -verfahren zu verzichten, so daß es bei der uneingeschränkten Freiheit der Nutzer bei der Auswahl und dem Einsatz von Verschlüsselungssystemen bleibt. Die Bundesregierung wird die weitere Entwicklung auf dem Gebiet der Kryptographie vor allem im Kontext der europäischen und internationalen Zusammenarbeit aufmerksam verfolgen und ggf. weitere Maßnahmen zur Umsetzung ihrer Ziele einleiten."

Die Bundesregierung hat sich bislang allerdings noch nicht verbindlich und eindeutig positioniert.

Kryptographie und Wirtschaftsinteressen

Vor allem wegen der dynamischen Entwicklung des digitalen Geschäftsverkehrs verzeichnen heute auch die Märkte für Verschlüsselungsprodukte hohe Wachstumsraten. Wichtige Anwendungsbereiche für kryptographische Systeme sind heute (neben dem traditionellen Schutz der Vertraulichkeit) z.B. Urheberschutz, digitale Signatur sowie digitales Geld. Darüber hinausgehend ist Kryptographie eine Querschnittstechnologie, die für die Systemarchitektur und Entwicklung komplexer Electronic Commerce-Anwendungen unverzichtbar ist. Mittelbar geht es hier also um weit größere Märkte, z.B. den der Telekommunikation, des Online-Banking oder der Telemedizin.

Zwar sind heute Sicherheitsstandards, die noch vor wenigen Jahren wegen der hohen Kosten vor allem Großunternehmen und staatlichen Stellen vorbehalten waren, auch für mittelständische Betriebe und private Haushalte erschwinglich. Dennoch werden Verschlüsselungsprodukte in Deutschland derzeit nicht in dem erforderlichen Maße eingesetzt. Hier fehlt es vielfach an dem notwendigen IT-Sicherheitsbewußtsein, obwohl durch die unbefugte Ausspähung, Manipulation oder Zerstörung von Daten erhebliche wirtschaftliche Schäden entstehen können.

Deutsche Kryptohersteller haben gute Aussichten, im internationalen Wettbewerb um neue Märkte mitzuhalten, wenn die notwendigen Rahmenbedingungen hierfür gewährleistet sind. Angesichts der strategischen Bedeutung dieser Branche unternehmen viele wichtige Industriestaaten erhebliche Anstrengungen, um deren wirtschaftliche und technische Leistungsfähigkeit im eigenen Land zu stärken.

Kryptographie und Sicherheitsinteressen

Der Einsatz kryptographischer Verfahren ist von außerordentlicher Bedeutung für eine effiziente technische Kriminalprävention. Dies gilt sowohl für die Gewährleistung der Authentizität und Integrität des Datenverkehrs wie auch für den Schutz der Vertraulichkeit.

Andererseits kann dieser Schutz der Vertraulichkeit auch Straftäter begünstigen: So ist zu erwarten, daß mit zunehmender Benutzerfreundlichkeit der Verschlüsselungsprodukte auch ihre Verbreitung in kriminellen Kreisen zunimmt. Dies kann die Strafverfolgungsbehörden vor Probleme stellen. Rechtmäßig angeordnete richterliche Überwachungsmaßnahmen müssen ihre Wirkung behalten, auch wenn die Zielperson die betreffenden Informationen mit einem kryptographischen Verfahren schützt.

Bislang stellt der Mißbrauch von Verschlüsselung in Deutschland für die Strafverfolgung kein ernsthaftes Problem dar. Eine Prognose für die Zukunft läßt sich hieraus allerdings nicht herleiten. Es ist deshalb erforderlich, in Deutschland aktive Technikfolgenabschätzung im Hinblick auf die Belange der Strafverfolgungs- und Sicherheitsbehörden zu betreiben, um Fehlentwicklungen so frühzeitig zu erkennen, daß ihnen - ggf. unter Zugrundelegung alternativer Strategien - wirksam begegnet werden kann.

Auf der Grundlage der bisherigen nationalen Diskussion sowie der internationalen Entwicklung beschließt die Bundesregierung die folgenden Eckpunkte ihrer Kryptopolitik:

1. Die Bundesregierung beabsichtigt nicht, die freie Verfügbarkeit von Verschlüsselungsprodukten in Deutschland einzuschränken. Sie sieht in der Anwendung sicherer Verschlüsselung eine entscheidende Voraussetzung für den Datenschutz der Bürger, für die Entwicklung des elektronischen Geschäftsverkehrs sowie für den Schutz von Unternehmensgeheimnissen. Die Bundesregierung wird deshalb die Verbreitung sicherer Verschlüsselung in Deutschland aktiv unterstützen. Dazu zählt insbesondere die Förderung des Sicherheitsbewußtseins bei den Bürgern, der Wirtschaft und der Verwaltung.

2. Die Bundesregierung strebt an, das Vertrauen der Nutzer in die Sicherheit der Verschlüsselung zu stärken. Sie wird deshalb Maßnahmen ergreifen, um einen Vertrauensrahmen für sichere Verschlüsselung zu schaffen, insbesondere indem sie die Überprüfbarkeit von Verschlüsselungsprodukten auf ihre Sicherheitsfunktionen verbessert und die Nutzung geprüfter Produkte empfiehlt.

3. Die Bundesregierung hält aus Gründen der Sicherheit von Staat, Wirtschaft und Gesellschaft

Trend: full disclosure

die Fähigkeit deutscher Hersteller zur Entwicklung und Herstellung von sicheren und leistungsfähigen Verschlüsselungsprodukten für unverzichtbar. Sie wird Maßnahmen ergreifen, um die internationale Wettbewerbsfähigkeit dieses Sektors zu stärken.

4. Durch die Verbreitung starker Verschlüsselungsverfahren dürfen die gesetzlichen Befugnisse der Strafverfolgungs- und Sicherheitsbehörden zur Telekommunikationsüberwachung nicht ausgehöhlt werden. Die zuständigen Bundesministerien werden deshalb die Entwicklung weiterhin aufmerksam beobachten und nach Ablauf von zwei Jahren hierzu berichten. Unabhängig hiervon setzt sich die Bundesregierung im Rahmen ihrer Möglichkeiten für die Verbesserung der technischen Kompetenzen der Strafverfolgungs- und Sicherheitsbehörden ein.

5. Die Bundesregierung legt großen Wert auf die internationale Zusammenarbeit im Bereich der Verschlüsselungspolitik. Sie tritt ein für am Markt entwickelte offene Standards und interoperable Systeme und wird sich für die Stärkung der multilateralen und bilateralen Zusammenarbeit einsetzen.

Trend: full disclosure

05.10.1999 There is a new trend in the reporting of security vulnerabilities these days. Many of the problems are being reported by companies that make products to detect these problems. While more people researching the security of products is a good thing, it is certainly having an effect on the free flow of security information. Sometimes this effect is to the detriment of the customers of the product that the flaw exists in.

If a company makes a product that scans for security problems, they are going to want to add their newly discovered vulnerability to their list of things to scan for. They are probably, depending on the seriousness of the problem they have uncovered, going to want to make the advisory of the problem into a full scale press release that will hype their product. Usually the press release won't really tell you how to find the problem or how to solve it. You are going to need to download their product for that.

When security problems exist on production servers accessible from the internet, time is critical. Every day that goes by is another day that the server is exposed. How many people know about the problem? Who is actively exploiting it? It is impossible to tell. Good ethical security practice is to tell the people effected quickly, especially if there are steps they can take to mitigate or eliminate the risk themselves.

The L0pht recently found a problem with Microsoft's IIS 4.0 web server, the showcode problem. It allowed web users to read files anywhere on the web server that the file permissions were set to be world-readable. This turns out to be the case in many web servers that are not locked down properly. The L0pht was surprised at how widespread the problem was. Many high profile e-commerce servers were effected. Many, many corporate web servers were effected.

The research of the problem, which took less than a day, came up with a simple solution. Delete the sample files which made the machine vulnerable. They don't need to be on production servers anyway. We crafted an advisory and gave out the solution.

When we reported this to Microsoft they said that they had known about the problem for "several weeks". They had been notified by WebTrends about the problem, were researching it, and would issue a Security Bulletin. It didn't seem to be that so complicated an issue that would take several weeks to research. And the fix was simple. Just delete the files. No need to download a hotfix or even tweak the registry. What was taking so long?

The L0pht released the showcode advisory to Bugtraq, computer industry reporters, and Microsoft on May 7, 1999, 9:30am EST. Later that day, approximately 1:40 pm EST, WebTrends released a press release about the same problem. It spoke of how WebTrends had discovered the problem. The WebTrends press release didn't tell how to detect the problem and had no solution to the problem. Two things that were present in the L0pht advisory. It seemed that you had to download and run their product if you wanted this information.

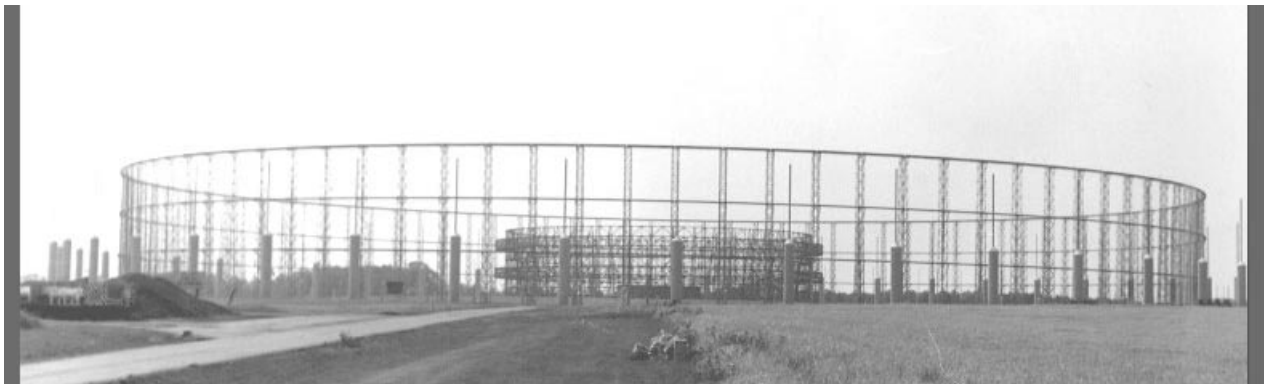
It makes one wonder if the press release was put out at that particular time because the L0pht had informed the public about the problem first. It makes one wonder why Microsoft kept this problem and easy solution to themselves for several weeks.

Many crackers keep security vulnerabilities secret so that they can exploit them without worrying about vendor patches or fixes by system administrators. This is looked down upon highly by the security community as totally unethical. Why keep the vulnerabilities secret unless you are going to exploit them, or perhaps trade them for something?

Now we have software vendors keeping things secret. At least secret for a substantial period of time. Is this the way we want the industry to behave?

This is why full disclosure mailing lists such as Bugtraq and web sites such as Packet Storm Security are so important. They allow customers to get vulnerability reports, and hopefully fixes, in a timely manner. There is no centralized clearinghouse such as the software vendor or some government agency to slow things up for their own ends.

Vulnerability information is extremely valuable both to attackers and customers. Companies and organizations that release this information openly and as soon as possible are doing the security community a service. Those who choose to use the information for their own purposes first put customers at risk.



Design Principles for Tamper-Resistant Smartcard Processors

Oliver Kömmerling
Advanced Digital Security Research
Mühlstraße 7
66484 Riedelberg
Germany
ok@adsr.de

Markus G. Kuhn
University of Cambridge
Computer Laboratory
Pembroke Street
Cambridge CB2 3QG
United Kingdom
mgk25@cl.cam.ac.uk

Abstract

We describe techniques for extracting protected software and data from smartcard processors. This includes manual microprobing, laser cutting, focused ion-beam manipulation, glitch attacks, and power analysis. Many of these methods have already been used to compromise widely-fielded conditional-access systems, and current smartcards offer little protection against them. We give examples of low-cost protection concepts that make such attacks considerably more difficult.

1 Introduction

Smartcard piracy has become a common occurrence. Since around 1994, almost every type of smartcard processor used in European, and later also American and Asian, pay-TV conditional-access systems has been successfully reverse engineered. Compromised secrets have been sold in the form of illicit clone cards that decrypt TV channels without revenue for the broadcaster. The industry has had to update the security processor technology several times already and the race is far from over.

Smartcards promise numerous security benefits. They can participate in cryptographic protocols, and unlike magnetic stripe cards, the stored data can be protected against unauthorized access. However, the strength of this protection seems to be frequently overestimated.

In Section 2, we give a brief overview on the most important hardware techniques for breaking into smartcards. We aim to help software engineers without a background in modern VLSI test techniques in getting a realistic impression of how physical tampering works and what it costs. Based on our observations of what makes these attacks particularly easy, in Section 3 we discuss various ideas for countermeasures. Some of these we believe to be new, while others have already been implemented in products but are either not widely used or have design flaws that have allowed us to circumvent them.

2 Tampering Techniques

We can distinguish four major attack categories:

- **Microprobing** techniques can be used to access the chip surface directly, thus we can observe, manipulate, and interfere with the integrated circuit.
- **Software attacks** use the normal communication interface of the processor and exploit security vulnerabilities found in the protocols, cryptographic algorithms, or their implementation.
- **Eavesdropping** techniques monitor, with high time resolution, the analog characteristics of all supply and interface connections and any other electromagnetic radiation produced by the processor during normal operation.
- **Fault generation** techniques use abnormal environmental conditions to generate malfunctions in the processor that provide additional access.

All microprobing techniques are *invasive attacks*. They require hours or weeks in a specialized laboratory and in the process they destroy the packaging. The other three are *non-invasive attacks*. After we have prepared such an attack for a specific processor type and software version, we can usually reproduce it within seconds on another card of the same type. The attacked card is not physically harmed and the equipment used in the attack can usually be disguised as a normal smartcard reader.

Non-invasive attacks are particularly dangerous in some applications for two reasons. Firstly, the

USENIX Workshop on Smartcard Technology, Chicago, Illinois, USA, May 10-11, 1999.

owner of the compromised card might not notice that the secret keys have been stolen, therefore it is unlikely that the validity of the compromised keys will be revoked before they are abused. Secondly, non-invasive attacks often scale well, as the necessary equipment (e.g., a small DSP board with special software) can usually be reproduced and updated at low cost.

The design of most non-invasive attacks requires detailed knowledge of both the processor and software. On the other hand, invasive microprobing attacks require very little initial knowledge and usually work with a similar set of techniques on a wide range of products. Attacks therefore often start with invasive reverse engineering, the results of which then help to develop cheaper and faster non-invasive attacks. We have seen this pattern numerous times on the conditional-access piracy market.

Non-invasive attacks are of particular concern in applications where the security processor is primarily required to provide *tamper evidence*, while invasive attacks violate the *tamper-resistance* characteristics of a card [1]. Tamper evidence is of primary concern in applications such as banking and digital signatures, where the validity of keys can easily be revoked and where the owner of the card has already all the access that the keys provide anyway. Tamper resistance is of importance in applications such as copyright enforcement, intellectual property protection, and some electronic cash schemes, where the security of an entire system collapses as soon as a few cards are compromised.

To understand better which countermeasures are of practical value, we first of all have to understand the techniques that pirates have used so far to break practically all major smartcard processors on the market. In the next section, we give a short guided tour through a typical laboratory of a smartcard pirate.

2.1 Invasive Attacks

2.1.1 Depackaging of Smartcards

Invasive attacks start with the removal of the chip package. We heat the card plastic until it becomes flexible. This softens the glue and the chip module can then be removed easily by bending the card. We cover the chip module with 20–50 ml of fuming nitric acid heated to around 60 °C and wait for the black epoxy resin that encapsulates the silicon die to completely dissolve (Fig. 1). The procedure should preferably be carried out under very dry conditions, as the presence of water could corrode exposed aluminium interconnects. The chip is then washed with acetone in an ultrasonic bath, followed optionally by a short bath in deionized water and isopropanol. We remove the remaining bonding wires with tweezers, glue the die into a test package, and bond its pads manually to the pins (Fig. 2). Detailed descriptions of these and other preparation techniques are given in [2, 3].

Figure 1: Hot fuming nitric acid (> 98% HNO_3) dissolves the package without affecting the chip.

Figure 2: The depackaged smartcard processor is glued into a test package, whose pins are then connected to the contact pads of the chip with fine aluminium wires in a manual bonding machine.

2.1.2 Layout Reconstruction

The next step in an invasive attack on a new processor is to create a map of it. We use an optical microscope with a CCD camera to produce several meter large mosaics of high-resolution photographs of the chip surface. Basic architectural structures, such as data and address bus lines, can be identified quite quickly by studying connectivity patterns

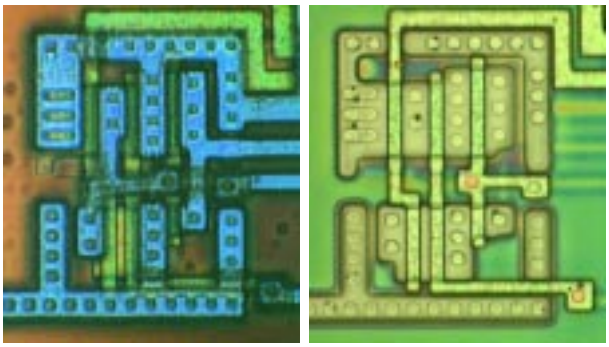


Figure 3: Left: CMOS AND gate imaged by a confocal microscope. Right: same gate after removal of metal layer (HF wet etching). Polysilicon interconnects and diffusion areas are now fully visible.

and by tracing metal lines that cross clearly visible module boundaries (ROM, RAM, EEPROM, ALU, instruction decoder, etc.). All processing modules are usually connected to the main bus via easily recognizable latches and bus drivers. The attacker obviously has to be well familiar with CMOS VLSI design techniques and microcontroller architectures, but the necessary knowledge is easily available from numerous textbooks [4, 5, 6, 7].

Photographs of the chip surface show the top metal layer, which is not transparent and therefore obscures the view on many structures below. Unless the oxide layers have been planarized, lower layers can still be recognized through the height variations that they cause in the covering layers. Deeper layers can only be recognized in a second series of photographs after the metal layers have been stripped off, which we achieve by submerging the chip for a few seconds in hydrofluoric acid (HF) in an ultrasonic bath [2]. HF quickly dissolves the silicon oxide around the metal tracks and detaches them from the chip surface. HF is an extremely dangerous substance and safety precautions have to be followed carefully when handling it.

Figure 3 demonstrates an optical layout reconstruction of a NAND gate followed by an inverter. These images were taken with a confocal microscope (Zeiss Axiotron-2 CSM), which assigns different colors to different focal planes (e.g., metal=blue, polysilicon=green) and thus preserves depth information [8]. Multilayer images like those shown in Fig. 3 can be read with some experience almost as easily as circuit diagrams. These photographs help us in understanding those parts of the circuitry that are relevant for the planned attack.

If the processor has a commonly accessible standard architecture, then we have to reconstruct the

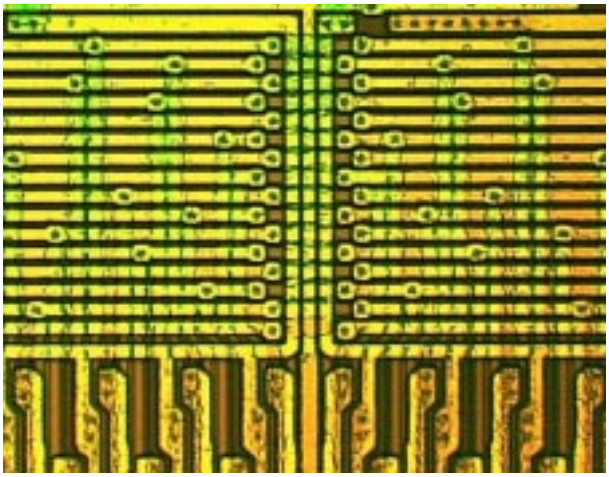


Figure 4: The vias in this structure found in a ST16F48A form a permutation matrix between the memory readout column lines and the 16:1 demultiplexer. The applied mapping remains clearly visible.

layout only until we have identified those bus lines and functional modules that we have to manipulate to access all memory values. More recently, designers of conditional-access smartcards have started to add proprietary cryptographic hardware functions that forced the attackers to reconstruct more complex circuitry involving several thousand transistors before the system was fully compromised. However, the use of standard-cell ASIC designs allows us to easily identify logic gates from their diffusion area layout, which makes the task significantly easier than the reconstruction of a transistor-level netlist.

Some manufacturers use non-standard instruction sets and bus-scrambling techniques in their security processors. In this case, the entire path from the EEPROM memory cells to the instruction decoder and ALU has to be examined carefully before a successful disassembly of extracted machine code becomes possible. However, the attempts of bus scrambling that we encountered so far in smartcard processors were mostly only simple permutations of lines that can be spotted easily (Fig. 4).

Any good microscope can be used in optical VLSI layout reconstruction, but confocal microscopes have a number of properties that make them particularly suited for this task. While normal microscopes produce a blurred image of any plane that is out of focus, in confocal scanning optical microscopes, everything outside the focal plane just becomes dark [8]. Confocal microscopes also provide better resolution and contrast. A chromatic lens in the system can make the location of the focal plane wavelength dependent, such that under white light different layers

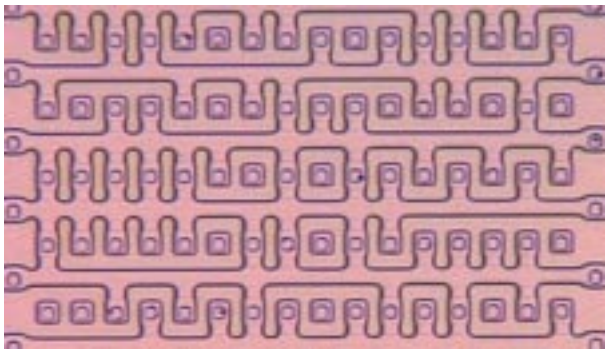


Figure 5: The data of this NOR ROM becomes clearly visible when the covering metal and polysilicon access lines plus the surrounding field oxide have been removed (HF wet etching). The image shows 16×10 bits in an ST16xyz. Every bit is represented by either a present or missing diffusion layer connection.

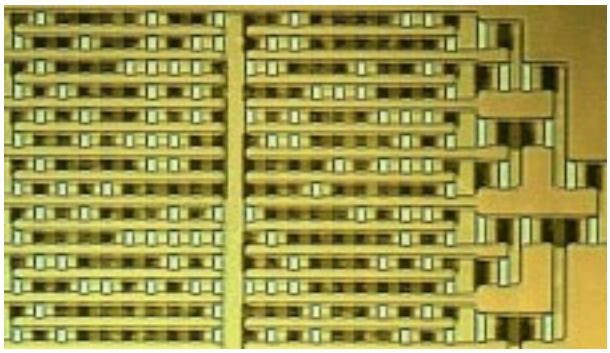


Figure 6: The implant-mask layout of a NAND ROM can be made visible by a dopant-selective crystallographic etch (Dash etchand [2]). This image shows 16×14 bits plus parts of the row selector of a ROM found on an MC68HC05SC2x CPU. The threshold voltage of 0-bit p-channel transistors (stained dark here) was brought below 0 V through ion implantation.

of the chip will appear simultaneously, but in different colors.

Automatic layout reconstruction has been demonstrated with scanning electron microscopy [9]. We consider confocal microscopy to be an attractive alternative, because we do not need a vacuum environment, the depth information is preserved, and the option of oil immersion allows the hiding of unevenly removed oxide layers. With UV microscopy, even chip structures down to 0.1 μm can be resolved.

With semiautomatic image-processing methods, significant portions of a processor can be reverse engineered within a few days. The resulting polygon data can then be used to automatically generate transistor and gate-level netlists for circuit simulations.

Optical reconstruction techniques can also be used to read ROM directly. The ROM bit pattern is stored in the diffusion layer, which leaves hardly any optical indication of the data on the chip surface. We have to remove all covering layers using HF wet etching, after which we can easily recognize the rims of the diffusion regions that reveal the stored bit pattern (Fig. 5).

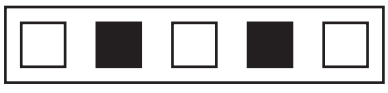
Some ROM technologies store bits not in the shape of the active area but by modifying transistor threshold voltages. In this case, additional dopant-selective staining techniques have to be applied to make the bits visible (Fig. 6). Together with an understanding of the (sometimes slightly scrambled, see Fig. 4) memory-cell addressing, we obtain disassembler listings of the entire ROM content. Again, automated processing techniques can be used to extract the data from photos, but we also know cases where an enthusiastic smartcard hacker has reconstructed several kilobytes of ROM manually.

While the ROM usually does not contain any cryptographic key material, it does often contain enough I/O, access control, and cryptographic routines to be of use in the design of a non-invasive attack.

2.1.3 Manual Microprobing

The most important tool for invasive attacks is a microprobing workstation. Its major component is a special optical microscope (e.g., Mitutoyo FS-60) with a working distance of at least 8 mm between the chip surface and the objective lens. On a stable platform around a socket for the test package, we install several micropositioners (e.g., from Karl Suss, Micromanipulator, or Wentworth Labs), which allow us to move a probe arm with submicrometer precision over a chip surface. On this arm, we install a "cat whisker" probe (e.g., Picoprobe T-4-10). This is a metal shaft that holds a 10 μm diameter and 5 mm long tungsten-hair, which has been sharpened at the end into a < 0.1 μm tip. These elastic probe hairs allow us to establish electrical contact with on-chip bus lines without damaging them. We connect them via an amplifier to a digital signal processor card that records or overrides processor signals and also provides the power, clock, reset, and I/O signals needed to operate the processor via the pins of the test package.

On the depackaged chip, the top-layer aluminium interconnect lines are still covered by a passivation



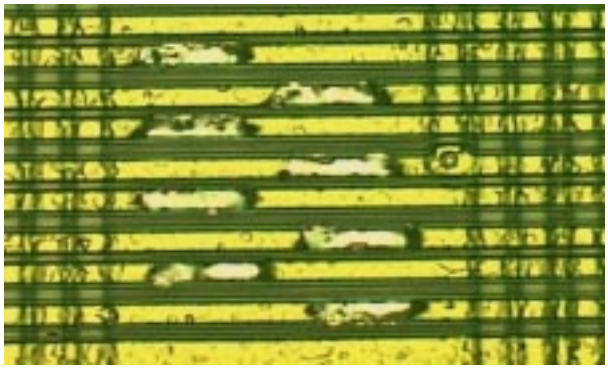


Figure 7: This image shows 9 horizontal bus lines on a depackaged smartcard processor. A UV laser (355 nm, 5 ns) was used to remove small patches of the passivation layer over the eight data-bus lines to provide for microprobing access.

layer (usually silicon oxide or nitride), which protects the chip from the environment and ion migration. On top of this, we might also find a polyimide layer that was not entirely removed by HNO_3 but which can be dissolved with ethylendiamine. We have to remove the passivation layer before the probes can establish contact. The most convenient depassivation technique is the use of a laser cutter (e.g., from New Wave Research).

The UV or green laser is mounted on the camera port of the microscope and fires laser pulses through the microscope onto rectangular areas of the chip with micrometer precision. Carefully dosed laser flashes remove patches of the passivation layer. The resulting hole in the passivation layer can be made so small that only a single bus line is exposed (Fig. 7). This prevents accidental contacts with neighbouring lines and the hole also stabilizes the position of the probe and makes it less sensitive to vibrations and temperature changes.

Complete microprobing workstations cost tens of thousands of dollars, with the more luxurious versions reaching over a hundred thousand US$. The cost of a new laser cutter is roughly in the same region.

Low-budget attackers are likely to get a cheaper solution on the second-hand market for semiconductor test equipment. With patience and skill it should not be too difficult to assemble all the required tools for even under ten thousand US$ by buying a second-hand microscope and using self-designed micropositioners. The laser is not essential for first results, because vibrations in the probing needle can also be used to break holes into the passivation.

2.1.4 Memory Read-out Techniques

It is usually not practical to read the information stored on a security processor directly out of each single memory cell, except for ROM. The stored data has to be accessed via the memory bus where all data is available at a single location. Microprobing is used to observe the entire bus and record the values in memory as they are accessed.

It is difficult to observe all (usually over 20) data and address bus lines at the same time. Various techniques can be used to get around this problem. For instance we can repeat the same transaction many times and use only two to four probes to observe various subsets of the bus lines. As long as the processor performs the same sequence of memory accesses each time, we can combine the recorded bus subset signals into a complete bus trace. Overlapping bus lines in the various recordings help us to synchronize them before they are combined.

In applications such as pay-TV, attackers can easily replay some authentic protocol exchange with the card during a microprobing examination. These applications cannot implement strong replay protections in their protocols, because the transaction counters required to do this would cause an NVRAM write access per transaction. Some conditional-access cards have to perform over a thousand protocol exchanges per hour and EEPROM technology allows only 10^4–10^6 write cycles during the lifetime of a storage cell. An NVRAM transaction counter would damage the memory cells, and a RAM counter can be reset by the attacker easily by removing power. Newer memory technologies such as FERAM allow over 10^9 write cycles, which should solve this problem.

Just replaying transactions might not suffice to make the processor access all critical memory locations. For instance, some banking cards read critical keys from memory only after authenticating that they are indeed talking to an ATM. Pay-TV card designers have started to implement many different encryption keys and variations of encryption algorithms in every card, and they switch between these every few weeks. The memory locations of algorithm and key variations are not accessed by the processor before these variations have been activated by a signed message from the broadcaster, so that passive monitoring of bus lines will not reveal these secrets to an attacker early.

Sometimes, hostile bus observers are lucky and encounter a card where the programmer believed that by calculating and verifying some memory checksum after every reset the tamper-resistance

could somehow be increased. This gives the attacker of course easy immediate access to all memory locations on the bus and simplifies completing the read-out operation considerably. Surprisingly, such memory integrity checks were even suggested in the smartcard security literature [10], in order to defeat a proposed memory rewrite attack technique [11]. This demonstrates the importance of training the designers of security processors and applications in performing a wide range of attacks before they start to design countermeasures. Otherwise, measures against one attack can far too easily backfire and simplify other approaches in unexpected ways.

In order to read out all memory cells without the help of the card software, we have to abuse a CPU component as an address counter to access all memory cells for us. The program counter is already incremented automatically during every instruction cycle and used to read the next address, which makes it perfectly suited to serve us as an address sequence generator [12]. We only have to prevent the processor from executing jump, call, or return instructions, which would disturb the program counter in its normal read sequence. Tiny modifications of the instruction decoder or program counter circuit, which can easily be performed by opening the right metal interconnect with a laser, often have the desired effect.

2.1.5 Particle Beam Techniques

Most currently available smartcard processors have feature sizes of 0.5–1 μm and only two metal layers. These can be reverse-engineered and observed with the manual and optical techniques described in the previous sections. For future card generations with more metal layers and features below the wavelength of visible light, more expensive tools additionally might have to be used.

A focused ion beam (FIB) workstation consists of a vacuum chamber with a particle gun, comparable to a scanning electron microscope (SEM). Gallium ions are accelerated and focused from a liquid metal cathode with 30 kV into a beam of down to 5–10 nm diameter, with beam currents ranging from 1 pA to 10 nA. FIBs can image samples from secondary particles similar to a SEM with down to 5 nm resolution. By increasing the beam current, chip material can be removed with the same resolution at a rate of around 0.25 $\mu m^3\,nA^{-1}\,s^{-1}$ [13]. Better etch rates can be achieved by injecting a gas like iodine via a needle that is brought to within a few hundred micrometers from the beam target. Gas molecules settle down on the chip surface and react with removed material to form a volatile compound that can be pumped away and is not redeposited. Using this gas-assisted etch technique, holes that are up to 12 times deeper than wide can be created at arbitrary angles to get access to deep metal layers without damaging nearby structures. By injecting a platinum-based organometallic gas that is broken down on the chip surface by the ion beam, platinum can be deposited to establish new contacts. With other gas chemistries, even insulators can be deposited to establish surface contacts to deep metal without contacting any covering layers.

Using laser interferometer stages, a FIB operator can navigate blindly on a chip surface with 0.15 μm precision, even if the chip has been planarized and has no recognizable surface structures. Chips can also be polished from the back side down to a thickness of just a few tens of micrometers. Using laser-interferometer navigation or infrared laser imaging, it is then possible to locate individual transistors and contact them through the silicon substrate by FIB editing a suitable hole. This rear-access technique has probably not yet been used by pirates so far, but the technique is about to become much more commonly available and therefore has to be taken into account by designers of new security chips.

FIBs are used by attackers today primarily to simplify manual probing of deep metal and polysilicon lines. A hole is drilled to the signal line of interest, filled with platinum to bring the signal to the surface, where a several micrometer large probing pad or cross is created to allow easy access (Fig. 11). Modern FIB workstations (for example the FIB 200xP from FEI) cost less than half a million US$ and are available in over hundred organizations. Processing time can be rented from numerous companies all over the world for a few hundred dollars per hour.

Another useful particle beam tool are electron-beam testers (EBT) [14]. These are SEMs with a voltage-contrast function. Typical acceleration voltages and beam currents for the primary electrons are 2.5 kV and 5 nA. The number and energy of secondary electrons are an indication of the local electric field on the chip surface and signal lines can be observed with submicrometer resolution. The signal generated during e-beam testing is essentially the low-pass filtered product of the beam current multiplied with a function of the signal voltage, plus noise. EBTs can measure waveforms with a bandwidth of several gigahertz, but only with periodic signals where stroboscopic techniques and periodic averaging can be used. If we use real-time voltage-contrast mode, where the beam is continuously di-

rected to a single spot and the blurred and noisy stream of secondary electrons is recorded, then the signal bandwidth is limited to a few megahertz [14]. While such a bandwidth might just be sufficient for observing a single signal line in a 3.5 MHz smartcard, it is too low to observe an entire bus with a sample frequency of several megahertz for each line.

EBTs are very convenient attack tools if the clock frequency of the observed processor can be reduced below 100 kHz to allow real-time recording of all bus lines or if the processor can be forced to generate periodic signals by continuously repeating the same transaction during the measurement.

2.2 Non-invasive Attacks

A processor is essentially a set of a few hundred flipflops (registers, latches, and SRAM cells) that define its current state, plus combinatorial logic that calculates from the current state the next state during every clock cycle. Many analog effects in such a system can be used in non-invasive attacks. Some examples are:

- Every transistor and interconnection have a capacitance and resistance that, together with factors such as the temperature and supply voltage, determine the signal propagation delays. Due to production process fluctuations, these values can vary significantly within a single chip and between chips of the same type.
- A flipflop samples its input during a short time interval and compares it with a threshold voltage derived from its power supply voltage. The time of this sampling interval is fixed relative to the clock edge, but can vary between individual flipflops.
- The flipflops can accept the correct new state only after the outputs of the combinatorial logic have stabilized on the prior state.
- During every change in a CMOS gate, both the p- and n-transistors are open for a short time, creating a brief short circuit of the power supply lines [15]. Without a change, the supply current remains extremely small.
- Power supply current is also needed to charge or discharge the load capacitances when an output changes.
- A normal flipflop consists of two inverters and two transmission gates (8 transistors). SRAM cells use only two inverters and two transistors to ground one of the outputs during a write operation. This saves some space but causes a significant short-circuit during every change of a bit.

There are numerous other effects. During careful security reviews of processor designs it is often necessary to perform detailed analog simulations and tests and it is not sufficient to just study a digital abstraction.

Smartcard processors are particularly vulnerable to non-invasive attacks, because the attacker has full control over the power and clock supply lines. Larger security modules can be equipped with backup batteries, electromagnetic shielding, low-pass filters, and autonomous clock signal generators to reduce many of the risks to which smartcard processors are particularly exposed.

2.2.1 Glitch Attacks

In a glitch attack, we deliberately generate a malfunction that causes one or more flipflops to adopt the wrong state. The aim is usually to replace a single critical machine instruction with an almost arbitrary other one. Glitches can also aim to corrupt data values as they are transferred between registers and memory. Of the many fault-induction attack techniques on smartcards that have been discussed in the recent literature [11, 12, 16, 17, 18], it has been our experience that glitch attacks are the ones most useful in practical attacks.

We are currently aware of three techniques for creating fairly reliable malfunctions that affect only a very small number of machine cycles in smartcard processors: clock signal transients, power supply transients, and external electrical field transients.

Particularly interesting instructions that an attacker might want to replace with glitches are conditional jumps or the test instructions preceding them. They create a window of vulnerability in the processing stages of many security applications that often allows us to bypass sophisticated cryptographic barriers by simply preventing the execution of the code that detects that an authentication attempt was unsuccessful. Instruction glitches can also be used to extend the runtime of loops, for instance in serial port output routines to see more of the memory after the output buffer [12], or also to reduce the runtime of loops, for instance to transform an iterated cipher function into an easy to break single-round variant [11].

Clock-signal glitches are currently the simplest and most practical ones. They temporarily increase the clock frequency for one or more half cycles, such that some flipflops sample their input before the new

state has reached them. Although many manufacturers claim to implement high-frequency detectors in their clock-signal processing logic, these circuits are often only simple-minded filters that do not detect single too short half-cycles. They can be circumvented by carefully selecting the duty cycles of the clock signal during the glitch.

In some designs, a clock-frequency sensor that is perfectly secure under normal operating voltage ignores clock glitches if they coincide with a carefully designed power fluctuation. We have identified clock and power waveform combinations for some widely used processors that reliably increment the program counter by one without altering any other processor state. An arbitrary subsequence of the instructions found in the card can be executed by the attacker this way, which leaves very little opportunity for the program designer to implement effective countermeasures in software alone.

Power fluctuations can shift the threshold voltages of gate inputs and anti-tampering sensors relative to the unchanged potential of connected capacitances, especially if this occurs close to the sampling time of the flipflops. Smartcard chips do not provide much space for large buffer capacitors, and voltage threshold sensors often do not react to very fast transients.

In a potential alternative glitch technique that we have yet to explore fully, we place two metal needles on the card surface, only a few hundred micrometers away from the processor. We then apply spikes of a few hundred volts for less than a microsecond on these needles to generate electrical fields in the silicon substrate of sufficient strength to temporarily shift the threshold voltages of nearby transistors.

2.2.2 Current Analysis

Using a 10–15 Ω resistor in the power supply, we can measure with an analog/digital converter the fluctuations in the current consumed by the card. Preferably, the recording should be made with at least 12-bit resolution and the sampling frequency should be an integer multiple of the card clock frequency.

Drivers on the address and data bus often consist of up to a dozen parallel inverters per bit, each driving a large capacitive load. They cause a significant power-supply short circuit during any transition. Changing a single bus line from 0 to 1 or vice versa can contribute in the order of 0.5–1 mA to the total current at the right time after the clock edge, such that a 12-bit ADC is sufficient to estimate the number of bus bits that change at a time. SRAM write operations often generate the strongest signals. By averaging the current measurements of many repeated identical transactions, we can even identify smaller signals that are not transmitted over the bus. Signals such as carry bit states are of special interest, because many cryptographic key scheduling algorithms use shift operations that single out individual key bits in the carry flag. Even if the status-bit changes cannot be measured directly, they often cause changes in the instruction sequencer or microcode execution, which then cause a clear change in the power consumption.

The various instructions cause different levels of activity in the instruction decoder and arithmetic units and can often be quite clearly distinguished, such that parts of algorithms can be reconstructed. Various units of the processor have their switching transients at different times relative to the clock edges and can be separated in high-frequency measurements.

3 Countermeasures

3.1 Randomized Clock Signal

Many non-invasive techniques require the attacker to predict the time at which a certain instruction is executed. A strictly deterministic processor that executes the same instruction c clock cycles after each reset—if provided with the same input at every cycle—makes this easy. Predictable processor behaviour also simplifies the use of protocol reaction times as a covert channel.

The obvious countermeasure is to insert random-time delays between any observable reaction and critical operations that might be subject to an attack. If the serial port were the only observable channel, then a few random delay routine calls controlled by a hardware noise source would seem sufficient. However, since attackers can use cross-correlation techniques to determine in real-time from the current fluctuations the currently executed instruction sequence, almost every instruction becomes an observable reaction, and a few localized delays will not suffice.

We therefore strongly recommend introducing timing randomness at the clock-cycle level. A random bit-sequence generator that is operated with the external clock signal should be used to generate an internal clock signal. This will effectively reduce the clock frequency by a factor of four, but most smartcards anyway reduce internally the 3.5 MHz provided for contact cards and the 13 MHz provided for contact-less cards.

Hardware random bit generators (usually the amplified thermal noise of transistors) are not always

good at producing uniform output statistics at high bit rates, therefore their output should be smoothed with an additional simple pseudo-random bit generator.

The probability that n clock cycles have been executed by a card with a randomized clock signal after c clock cycles have been applied can be described as a binomial distribution:

$$\begin{aligned} p(n,c) &= 2^{-c}\left[\begin{pmatrix} c \\ 2n \end{pmatrix}\begin{pmatrix} c \\ 2n+1 \end{pmatrix}\right] \\ &\approx \sqrt{\frac{8}{\pi c}}\cdot e^{-\frac{8}{c}\cdot(n-\frac{c}{4})^2} \quad \text{as} \quad c\to\infty \end{aligned}$$

So for instance after we have sent 1000 clock cycles to the smartcard, we can be fairly sure (probability $> 1-10^{-9}$) that between 200 and 300 of them have been executed. This distribution can be used to verify that safety margins for timing-critical algorithms—such as the timely delivery of a pay-TV control word—are met with sufficiently high probability.

Only the clock signals of circuitry such as the serial port and timer need to be supplied directly with the external clock signal, all other processor parts can be driven from the randomized clock.

A lack of switching transients during the inactive periods of the random clock could allow the attacker to reconstruct the internal clock signal from the consumed current. It is therefore essential that the processor shows a characteristic current activity even during the delay phases of the random clock. This can be accomplished by driving the bus with random values or by causing the microcode to perform a write access to an unused RAM location while the processor is inactive.

3.2 Randomized Multithreading

To introduce even more non-determinism into the execution of algorithms, it is conceivable to design a multithreaded processor architecture [19] that schedules the processor by hardware between two or more threads of execution randomly at a per-instruction level. Such a processor would have multiple copies of all registers (accumulator, program counter, instruction register, etc.), and the combinatorial logic would be used in a randomly alternating way to progress the execution state of the threads represented by these respective register sets.

The simple 8-bit microcontrollers of smartcards do not feature pipelines and caches and the entire state is defined only by a very small number of registers that can relatively easily be duplicated. The only other necessary addition would be new machine instructions to fork off the other thread(s) and to synchronize and terminate them. Multithreaded applications could interleave some of the many independent cryptographic operations needed in security protocols. For the remaining time, the auxiliary threads could just perform random encryptions in order to generate an realistic current pattern during the delay periods of the main application.

3.3 Robust Low-frequency Sensor

Bus-observation by e-beam testing becomes much easier when the processor can be clocked with only a few kilohertz, and therefore a low-frequency alarm is commonly found on smartcard processors. However, simple high-pass or low-pass RC elements are not sufficient, because by carefully varying the duty cycle of the clock signal, we can often prevent the activation of such detectors. A good low-frequency sensor must trigger if no clock edge has been seen for longer than some specified time limit (e.g., 0.5 μs). In this case, the processor must not only be reset immediately, but all bus lines and registers also have to be grounded quickly, as otherwise the values on them would remain visible sufficiently long for a voltage-contrast scan.

Even such carefully designed low-frequency detectors can quite easily be disabled by laser cutting or FIB editing the RC element. To prevent such simple tampering, we suggest that an intrinsic self-test be built into the detector. Any attempt to tamper with the sensor should result in the malfunction of the entire processor. We have designed such a circuit that tests the sensor during a required step in the normal reset sequence. External resets are not directly forwarded to the internal reset lines, but only cause an additional frequency divider to reduce the clock signal. This then activates the low-frequency detector, which then activates the internal reset lines, which finally deactivate the divider. The processor has now passed the sensor test and can start normal operation. The processor is designed such that it will not run after a power up without a proper internal reset. A large number of FIB edits would be necessary to make the processor operational without the frequency sensor being active.

Other sensor defenses against invasive attacks should equally be embedded into the normal operation of the processor, or they will easily be circumvented by merely destroying their signal or power supply connections.

3.4 Destruction of Test Circuitry

Microcontroller production has a yield of typically around 95%, so each chip has to be thoroughly tested

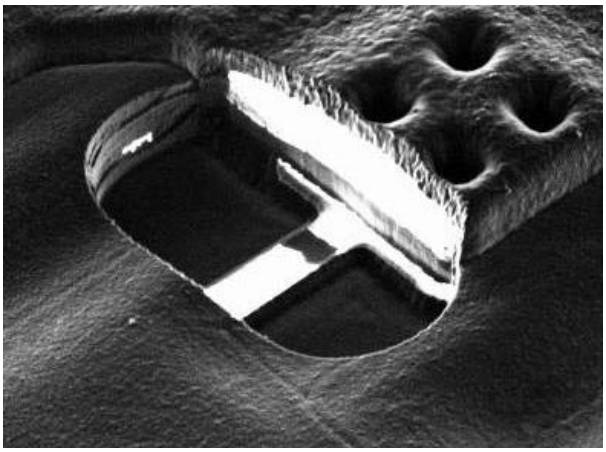


Figure 8: The interrupted white line at the bottom of the cavity in this FIB secondary-electron image is a blown polysilicon fuse next to a test pad (MC68HC05SC2x processor).

after production. Test engineers —like microprobing attackers—have to get full access to a complex circuit with a small number of probing needles. They add special test circuitry to each chip, which is usually a parallel/serial converter for direct access to many bus and control lines. This test logic is accessible via small probing pads or multiplexed via the normal I/O pads. On normal microcontrollers, the test circuitry remains fully intact after the test. In smartcard processors, it is common practice to blow polysilicon fuses that disable access to these test circuits (Fig. 8). However, attackers have been able to reconnect these with microprobes or FIB editing, and then simply used the test logic to dump the entire memory content.

Therefore, it is essential that any test circuitry is not only slightly disabled but structurally destroyed by the manufacturer. One approach is to place the test interface for chip n onto the area of chip $n+1$ on the wafer, such that cutting the wafer into dies severs all its parallel connections. A wafer saw usually removes a 80–200 μm wide area that often only contains a few process control transistors. Locating essential parts of the test logic in these cut areas would eliminate any possibility that even substantial FIB edits could reactivate it.

3.5 Restricted Program Counter

Abusing the program counter as an address pattern generator significantly simplifies reading out the entire memory via microprobing or e-beam testing.

Separate watchdog counters that reset the processor if no jump, call, or return instruction is executed for a number of cycles would either require many transistors or are too easily disabled.

Instead, we recommend simply not providing a program counter that can run over the entire address space. A 16-bit program counter can easily be replaced with the combination of a say 7-bit offset counter O and a 16-bit segment register S, such that the accessed address is $S + O$. Instead of overflowing, the offset counter resets the processor after reaching its maximum value. Every jump, call, or return instruction writes the destination address into S and resets O to zero. The processor will now be completely unable to execute more than 127 bytes of machine code without a jump, and no simple FIB edit will change this. A simple machine-code post-processor must be used by the programmer to insert jumps to the next address wherever unconditional branches are more than 127 bytes apart.

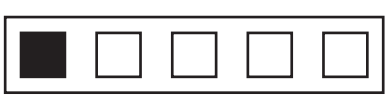
With the program counter now being unavailable, attackers will next try to increase the number of iterations in software loops that read data arrays from memory to get access to all bytes. This can for instance be achieved with a microprobe that performs a glitch attack directly on a bus-line. Programmers who want to use 16-bit counters in loops should keep this in mind.

3.6 Top-layer Sensor Meshes

Additional metallization layers that form a sensor mesh above the actual circuit and that do not carry any critical signals remain one of the more effective annoyances to microprobing attackers. They are found in a few smartcard CPUs such as the ST16SF48A or in some battery-buffered SRAM security processors such as the DS5002FPM and DS1954.

A sensor mesh in which all paths are continuously monitored for interruptions and short-circuits while power is available prevents laser cutter or selective etching access to the bus lines. Mesh alarms should immediately trigger a countermeasure such as zeroizing the non-volatile memory. In addition, such meshes make the preparation of lower layers more difficult, because since the etch progresses unevenly through them, their pattern remains visible in the layers below and therefore they complicate automatic layout reconstruction. Finally, a mesh on top of a polished oxide layer hides lower layers, which makes navigation on the chip surface for probing and FIB editing more tedious.

The implementations of sensor meshes in fielded products however show a number of quite surprising design flaws that significantly reduce the protection (Fig. 9 and 10). The most significant flaw is



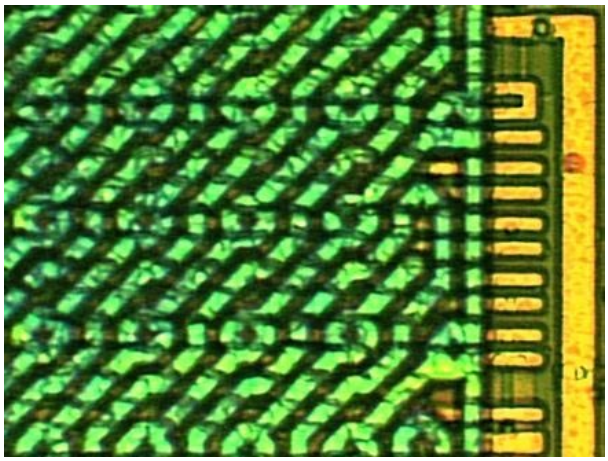


Figure 9: Escape route for imprisoned crypto bits: The ST16SF48A designers generously added this redundant extension of the data bus several micrometers beyond the protected mesh area, providing easy probing access.

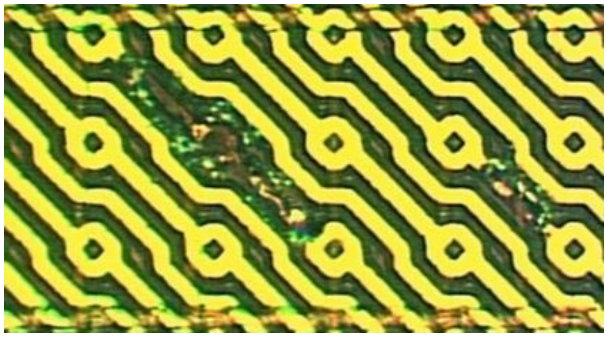


Figure 10: Every second line is connected to VCC or GND at one end and open at the other. Not all are used to supply lower layers and therefore some can safely be opened with a laser for probing access to the bus lines below.

that a mesh breach will only set a flag in a status register and that zeroization of the memory is left completely to the application software. We noted in Section 2.1.4 that a common read-out technique involves severely disabling the instruction decoder, therefore software checks for invasive attacks are of little use.

A well-designed mesh can make attacks by manual microprobing alone rather difficult, and more sophisticated FIB editing procedures will be required to bypass it. Several techniques can be applied here. The resolution of FIB drilling is much smaller than the mesh line spacings, therefore it is no problem to establish contact through three or more metal layers and make deeply buried signals accessible for micro-

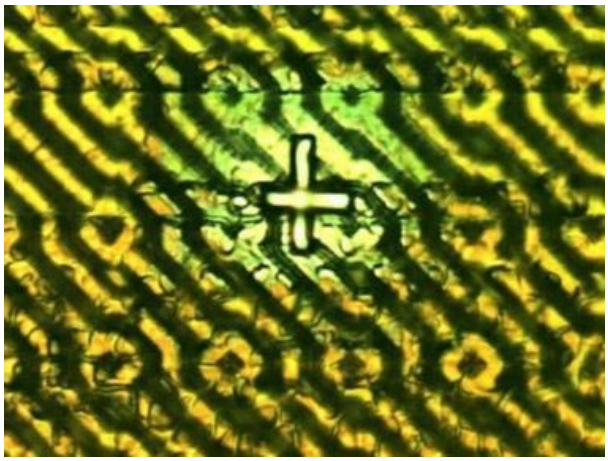


Figure 11: A FIB was used here to drill a fine hole to a bus line through the gap between two sensor mesh lines, refill it with metal, and place a metal cross on top for easy microprobing access.

probing via a platinum or tungsten pad on top of the passivation layer (Fig. 11). Alternatively, it is also possible to etch a larger window into the mesh and then reconnect the loose ends with FIB metal deposits around it.

4 Conclusion

We have presented a basis for understanding the mechanisms that make microcontrollers particularly easy to penetrate. With the restricted program counter, the randomized clock signal, and the tamper-resistant low-frequency sensor, we have shown some selected examples of low-cost countermeasures that we consider to be quite effective against a range of attacks.

There are of course numerous other more obvious countermeasures against some of the commonly used attack techniques which we cannot cover in detail in this overview. Examples are current regulators and noisy loads against current analysis attacks and loosely coupled PLLs and edge barriers against clock glitch attacks. A combination of these together with e-field sensors and randomized clocks or perhaps even multithreading hardware in new processor designs will hopefully make high-speed non-invasive attacks considerably less likely to succeed. Other countermeasures in fielded processors such as light and depassivation sensors have turned out to be of little use as they can be easily bypassed.

We currently see no really effective short-term protection against carefully planned invasive tampering involving focused ion-beam tools. Zeroization mechanisms for erasing secrets when tampering

is detected require a continuous power supply that the credit-card form factor does not allow. The attacker can thus safely disable the zeroization mechanism before powering up the processor. Zeroization remains a highly effective tampering protection for larger security modules that can afford to store secrets in battery-backed SRAM (e.g., DS1954 or IBM 4758), but this is not yet feasible for the smartcard package.

5 Acknowledgements

The authors would like to thank Ross Anderson, Simon Moore, Steven Weingart, Matthias Brunner, Gareth Evans and others for useful and highly interesting discussions.

References

[1] FIPS PUB 140-1: Security Requirements for Cryptographic Modules. National Institute of Standards and Technology, U.S. Department of Commerce, 11 January 1994.

[2] F. Beck: *Integrated Circuit Failure Analysis – A Guide to Preparation Techniques*. John Wiley & Sons, 1998.

[3] T.W. Lee, S.V. Pabbisetty (eds.): *Microelectronic Failure Analysis, Desk Reference*. 3rd edition, ASM International, Ohio, 1993, ISBN 0-87170-479-X.

[4] N.H.E. Weste, K. Eshraghian: *Principles of CMOS VLSI Design*. Addison-Wesley, 1993.

[5] S.-M. Kang, Y. Leblebici: *CMOS Digital Integrated Circuits: Analysis and Design*. McGraw-Hill, 1996.

[6] J. Carter: *Microprocessor Architecture and Microprogramming – A State-Machine Approach*. Prentice-Hall, 1996.

[7] S.M. Sze: *Semiconductor Devices – Physics and Technology*. John Wiley & Sons, 1985.

[8] T.R. Corle, G.S. Kino: *Confocal Scanning Optical Microscopy and Related Imaging Systems*. Academic Press, 1996.

[9] S. Blythe, et al.: Layout Reconstruction of Complex Silicon Chips. *IEEE Journal of Solid-State Circuits*, 28(2):138–145, February 1993.

[10] D.P. Maher: Fault Induction Attacks, Tamper Resistance, and Hostile Reverse Engineering in Perspective. In R. Hirschfeld (ed.): *Financial Cryptography, FC '97*, Proceedings, LNCS 1318, pp. 109–121, Springer-Verlag, 1997.

[11] R.J. Anderson, M.G. Kuhn: Low Cost Attacks on Tamper Resistant Devices. In M. Lomas, et al. (eds.), *Security Protocols, 5th International Workshop*, LNCS 1361, pp. 125–136, Springer-Verlag, 1997

[12] R.J. Anderson, M.G. Kuhn: Tamper Resistance — a Cautionary Note. In *The Second USENIX Workshop on Electronic Commerce Proceedings*, pp. 1–11, Oakland, California, 18–21 November 1996.

[13] J.H. Daniel, D.F. Moore, J.F. Walker: Focused Ion Beams for Microfabrication. *Engineering Science and Education Journal*, pp. 53–56, April 1998.

[14] H. P. Feuerbaum: Electron Beam Testing: Methods and Applications. *Scanning*, 5(1):14–24, 1982.

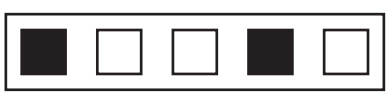
[15] H.J.M. Veendrick: Short-Circuit Dissipation of Static CMOS Circuitry and Its Impact on the Design of Buffer Circuits. *IEEE Journal of Solid-State Circuits*, 19(4):468–473, August 1984.

[16] D. Boneh, R.A. DeMillo, R.J. Lipton: On the Importance of Checking Cryptographic Protocols for Faults. In *Advances in Cryptology – EUROCRYPT '97*, LNCS 1233, pp. 37–51, Springer-Verlag, 1997.

[17] F. Bao, et al.: Breaking Public Key Cryptosystems on Tamper Resistant Devices in the Presence of Transient Faults. In M. Lomas, et al. (eds.), *Security Protocols, 5th International Workshop*, LNCS 1361, pp. 115–124, Springer-Verlag, 1997.

[18] M. Joye, J.-J. Quisquater, F. Bao, R. H. Deng: RSA-type Signatures in the Presence of Transient Faults. In *Cryptography and Coding*, LNCS 1355, pp. 155–160, Springer-Verlag, 1997.

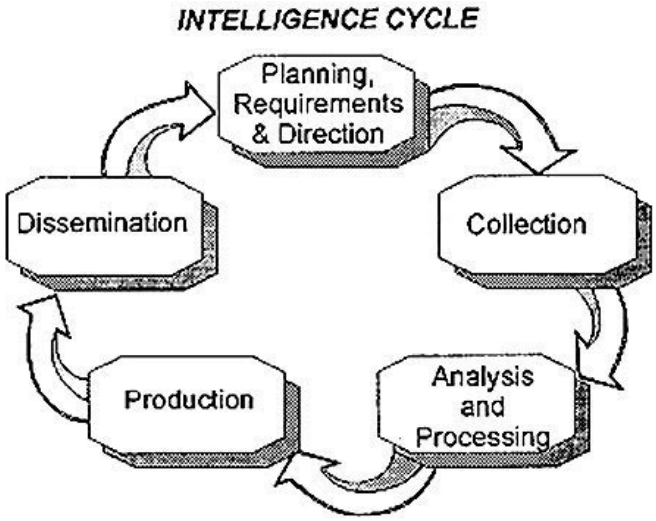
[19] S.W. Moore: *Multithreaded Processor Design*. Kluwer Academic Publishers, 1996.



Zusammenfassung Interception

Dies ist eine redaktionell erstellte Zusammenfassung des aktuellen STOA-Berichts an das Europäische Parlament zu den aktuellen Methoden und Techniken der geheimdienstlichen Telekommunikationsüberwachung. Der vollständige Bericht ist in englischer Sprache im Internet abrufbar, URL am Ende des Artikels.

I. Nachrichtendienstliche Tätigkeiten (*Communications intelligence=Comint*) beinhalten u.a. das verdeckte Abhören der Kommunikation fremder Staaten und werden von nahezu allen Nationen angewandt seit es internationale Nachrichtenverbindungen gibt. Comint wird in großem Maßstab auf industrieller Ebene angewandt und versorgt seine Auftraggeber mit Informationen über diplomatische, ökonomische und wissenschaftliche Fortschritte. Die Möglichkeiten und Aufgaben von *Comint* lassen sich am besten mit Hilfe des *intelligence cycle* darstellen:



1. Planung: Die Auftraggeber - u.a. Ministerien der finanzierenden Regierungen - definieren ihre Anforderungen aus den Bereichen Verteidigung, auswärtige Angelegenheiten, Handel und innere Sicherheit.

2. Datensammlung: Moderne Systeme leiten die gesammelten Daten automatisch über globale Netzwerke an die Analytiker weiter; die Datenauswahl passiert in den meisten Fällen auch automatisch und bedient sich großer Online-Datenbanken, die alle interessanten Ziele beinhalten.

3. Datenaufbereitung: Die entweder automatisch oder von Menschen gesteuerte Umwandlung der gesammelten Daten in ein Standardformat, das sowohl ihren technischen Inhalt, wie weitere Informationen (z. B. Telephonnummern der beteiligten Partner) enthält.

4. Produktion und Verbreitung: Comint beinhaltet die Datenanalyse, -bewertung, -übersetzung und -interpretation der gesammelten Daten in verwertbare Informationen. Diese werden an den Auftraggeber weitergegeben. Die Daten können dabei in unbearbeiteter (aber entschlüsselter und/oder übersetzter) Form, als Kernthesen, Kommentare oder ausführliche Berichte weitergegeben werden. Qualität und Bedeutung dieser Berichte führen zu einer Spezifikation der Abhörmaßnahmen und -themen und schließen damit den Informationskreislauf.

Eine besondere Bedeutung kommt hier der geheimen Sammlung von Handelsdaten zu: denn - so wird argumentiert - wüßten die Betroffenen von Möglichkeiten und Umfang der Abhörmaßnahmen, führte es dazu, daß sie ihre Methoden der Informationsverbreitung ändern und weitere Lauschangriffe so erschweren würden.

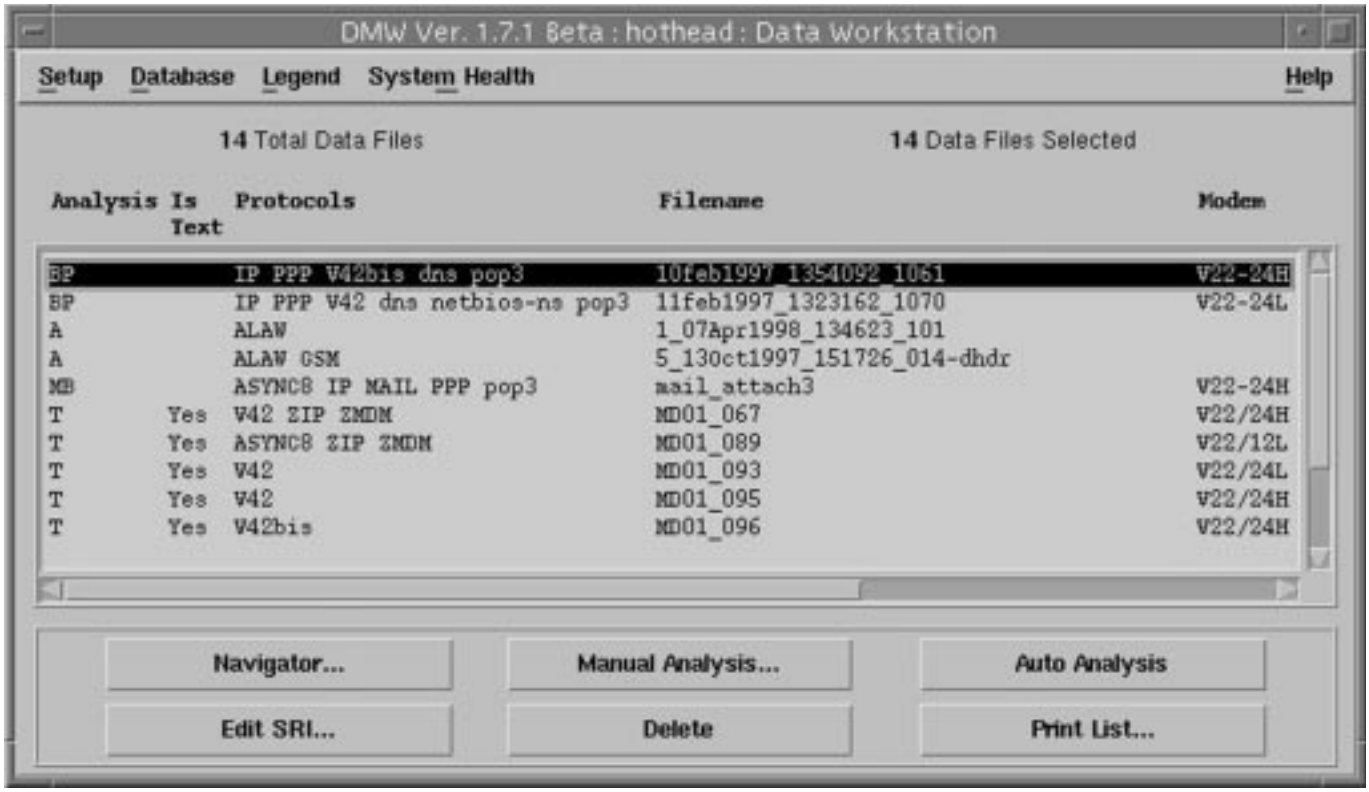
II. Weltweit werden ca. 15-20 Billiarden Euro jährlich für Abhörmaßnahmen ausgegeben. Der größte Teil entfällt dabei auf die englischsprachigen Nationen der UKUSA-Allianz. Abgehört werden Telephonverbindungen, Unterseekabel, das Internet, Richtfunkverkehr und Satellitenverbindungen.

Capabilities 2000

III. Das global vernetzte und weitgehend automatisch arbeitende Abhörsystem ECHELON, von der NSA (*National Security Agency*) entwickelt und betreut, sammelt seit den 1970er Jahren Daten nicht nur militärischer, sondern auch - und das zunehmend - ziviler Natur. Zwar ist kaum etwas über Spionagesatelliten bekannt, die nach 1990 gestartet wurden, doch wurde das System ausgeweitet. Die wichtigsten Bodenstationen befinden sich in Buckley Field, Denver, Colorado; Pine Gap, Australien; Menwith Hill, England und in Bad Aibling, Bayern. Der Unterhalt der Satelliten und der Einrichtungen zur Weiterverarbeitung ihrer Daten beläuft sich auf etwa 1 Milliarde US-Dollar pro Stück. Keine andere Nation der Welt verfügt über eine so weit entwickelte Satellitentechnologie, wie sie von den Satelliten CANYON, RHYOLITE und ihren Nachfolgern repräsentiert wird. Die USA verfügen über mindestens 120 dieser Satelliten. Zur Überwachung des Datenverkehrs wurden sogenannten ‚*Watch-Lists*' angelegt, die Personennamen oder Namen von Organisationen enthalten. Wurden diese bis 1970 von Hand ausgewertet, machte es die Fülle der abgehörten Daten bald notwendig, automatisch gefiltert zu werden. Seit der Mitte der 1980er Jahre setzt man in den Bodenstationen Computer ein, die große Datenmengen aus verschiedenen Bereichen (Namen, Themen von Interesse, Adressen, Telefonummern etc.) automatisch selektieren und weiterleiten. Diese Art der Datensuche und -auswertung kann mit den Suchmaschinen des Internet verglichen werden. Seit der Einführung des ECHELON-Systems aber werden praktisch alle ausgefilterten Informationen direkt an die NSA oder andere Kunden weitergegeben, ohne daß die lokalen Stationen oder Länder wüßten, was abgehört, bzw. an wen es weitergeleitet wurde.

IV. Seit Beginn der 1990er Jahre bemühte sich die Regierung der USA, ein sog. *key escrow*-System einzuführen: Nicht-staatliche Behörden sollten Kopien aller User-Keys bekommen. Eigentliches Ziel dieser Aktionen war es wohl, die NSA mit diesen Schlüsseln zu versorgen und so private und kommerzielle Kommunikation weiterhin erfolgreich abhören zu können. Zwischen 1993 und 1998 versuchten die USA auf diplomatischem Wege die EU-Staaten und die OECD von ihrem *key escrow*-System zu überzeugen; während dieser Bemühungen wurde fortwährend behauptet, das System diene nur der besseren staatlichen Verbrechensbekämpfung, um die Kriminalität und das organisierte Verbrechen unter Kontrolle zu halten. Da die Verhandlungen praktisch ausschließlich von Mitarbeitern der NSA - manchmal unter vollkommenem Ausschluß von Angehörigen der Polizei oder Justiz - geführt wurden, ist es wohl naheliegend anzunehmen, daß das o.g. Argument nur zur Verschleierung der wahren Ziele der Politik der USA diente. Seit 1993 treffen sich Angehörige vieler EU- und der UKUSA-Staaten - außerhalb der Kontrolle des europäischen Parlamentes - jährlich zu Diskussionsforen, um ihre Abhörmaßnahmen zu koordinieren. Sie kommen unter der Schirmherrschaft einer bisher unbekannten Organisation (ILETS=International Law Enforcement Telecommunications Seminar) zusammen; die Gründung von ILETS wurde vom FBI angeregt. Die im Juni 1994 gefaßten Beschlüsse von ILETS orientierten sich im wesentlichen an den Anforderungen eines vorher vom FBI erstellten Dokumentes. Die Kryptographie wurde lediglich im Zusammenhang mit der Netzwerksicherheit erwähnt. Erst 1998 wurde die Kryptographie in größerem Maßstab berücksichtigt. Vermutlich wurden auch in diesem Jahr die Beschlüsse auf das Internet und Satellitenkommunikationssysteme wie Iridium erweitert; sie beinhalten auch zusätzliche Sicherheitsanforderungen für Netzwerkbetreiber und Provider; verlangen persönliche Informationen über Fernsprechteilnehmer und Planungen, die sich mit der Kryptographie beschäftigen.

TK-Überwachung im Jahre 2000



V. *Comint*-Organisationen müssen feststellen, daß die technischen Schwierigkeiten bei der Datensammlung zunehmen und daß es in Zukunft teurer und aufwendiger wird, internationale Kommunikation abzuhören. Für die Zukunft ist es wichtig, diese Probleme auszuwerten und eine politische Basis zu schaffen, die auf Schutzmaßnahmen der Wirtschaft und effektive Kryptographie zielt.

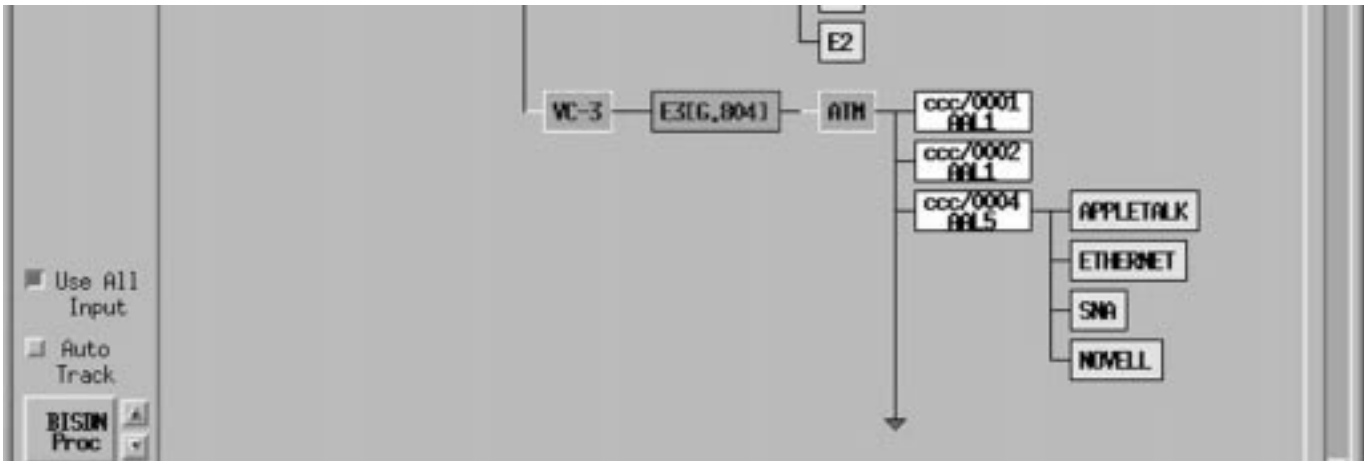
VI. Ausblick - Seit Mitte der 90er Jahre haben Lauscher zunehmend Schwierigkeiten, weltweiten Zugriff auf die Kommunikationsdaten zu erlangen. Diese Probleme werden sich noch vergrößern, da vor allem die leistungsfähigen Glasfasernetzwerke ausschließlich über einen physischen Zugriff abzuhören sind. Verlaufen diese Netzwerke nicht innerhalb eines kollaborierenden Staates oder passieren diesen, ist ein Abhören praktisch nur über die Anbringung eines optischen Repeaters möglich; sehr viele unterirdisch verlegte Glasfasernetze sind also kaum abhörbar. Der nötige Aufwand an technischem Gerät und Energie zur Aufzeichnung und Weiterverarbeitung macht geheime Operationen unpraktisch und gefährlich. Selbst wenn ein Zugang möglich ist, so werden die Abhöraktivitäten doch durch die rapide Ausbreitung neuer Systeme gehemmt, z.T. aus Kostengründen, teilweise auch, weil neue Systeme (z.B. Iridium) über momentan verfügbare Techniken nicht greifbar sind. Der technische Vorsprung in der Computertechnik der *Comint*-Organisatioen hat sich in den vergangenen 15 Jahren aufgebraucht. Sie nutzen Standardsysteme, die denen der führenden Industriebetriebe oder wissenschaftlichen Einrichtungen technisch gleichwertig oder sogar unterlegen sind. Sie sind lediglich TEMPEST-abgeschirmt, strahlen also keine Funksignale aus, die abgehört werden könnten. *Comint*-Organisationen mußten feststellen, daß ihr Krieg gegen zivile und kommerzielle Kryptographie verloren ist. Mehr und mehr wissenschaftliche

und wirtschaftliche Organisationen verstehen sich auf Kryptographie und Kryptologie. Das Internet und der globale Markt haben den freien Fluß von Informationen, Systemen und Software ermöglicht. Der NSA ist es nicht gelungen *key escrow* oder verwandte Systeme mit dem scheinheiligen Argument der Verbrechensbekämpfung durchzusetzen.
In Zukunft wird man wohl in zunehmendem Maße auf menschliche Agenten setzen, um Codes zu sammeln; auch mit verstärkten Bemühungen um fremde Computersysteme ist zu rechnen, z.B. mit Hilfe des Internet (insbesondere um an geschützte Files heranzukommen oder an Informationen, bevor sie verschlüsselt wurden).
Dennoch führten die Versuche, die Kryptographie einzuschränken dazu, daß sich die Verbreitung von effektiver kryptographischer Systeme verzögert hat. Der Preisverfall auf dem Computermarkt hat den *Comint*-Treibenden zudem die Möglichkeit gegeben, schnelle und hochentwickelte Datenverarbeitungs und -sortierungstools zu entwickeln.
Entgegen anders lautender Presseberichte gibt es übrigens - trotz 30 Jahre währender Forschung - noch keine leistungsfähigen *word-spotting*-Systeme, die automatisch Telefongespräche auf nachrichtendienstlich interessante Informationen hin durchsuchen können. Allerdings wurden Sprechererkennungssysteme entwickelt und werden verwendet, die in der Lage sind, die Zielpersonen in Ferngesprächen zu erkennen.

Abschließend soll noch der Ex-CIA Offizier John Millis zu Wort kommen, der die aktuelle Entwicklung aus der Sicht der NSA schildert : „*Sigint* (=*Signals Intelligence*) befindet sich in einer Krise ... Die letzten 50 Jahre hindurch ... in der Vergangenheit, war die Technologie der Freund der NSA, aber in den letzten vier oder fünf Jahren mutierte sie vom Freund zum Feind von *Sigint*. Die Telekommunikationsmedien sind nicht mehr länger *Sigint*-freundlich. Sie waren es. Benutzte man HF-Signale, konnte jeder in Reichweite dieser HF-Signale sie genau so gut empfangen wie der geplante Empfänger. Wir begannen Mikrowellen zu benutzen und man fand einen Weg, auch diese zu verwenden. Gut, wir bewegen uns aber auf Medien zu, an die ziemlich schwer heranzukommen ist. Kryptographie existiert und scheint sich sehr schnell auszubreiten. Das sind wirklich schlechte Nachrichten für *Sigint* ... Es wird eine Menge Geld für neue Technologien nötig sein, um einen Zugang zu bekommen und in der Lage zu sein, die Informationen zu bekommen, die wir unbedingt über *Sigint* bekommen wollen." *henriette*

Der vollständige englische Text ist findbar unter:

http://www.greennet.org.uk/duncan/stoa.htm oder
http://www.iptvreports.mcmail.com/stoa_cover.htm



Minister enttarnte den eigenen Geheimdienst

A good leader is a person who takes a little more than his share of the blame and a little less than his share of the credit.

- John C. Maxwell

Geklaut aus der Frankfurter Rundschau vom 31. Mai 1999 (http://www.fr-aktuell.de/archiv/fr30t/19990531086.htm

Der Minister enttarnte den eigenen Geheimdienst

Bericht an portugiesischen Ausschuss listet Aufgaben und sogar Gehaelter der Spione auf

Von Axel Veiel (Madrid)

Portugal hat keinen Geheimdienst mehr, der diesen Namen verdient. Die 69 Agenten des Landes sind enttarnt. Ihr oberster Dienstherr, Verteidigungsminister Jos Veiga Simo, hatte alles Wissenswerte über sie in einem 120 Seiten starken Bericht zusammenfassen lassen, um eine parlamentarische Untersuchungskommission von der Güte des Dienstes zu überzeugen. Doch der wurde samt Namen und Aufgaben der Spione der Wochenzeitung O Independente zugespielt, die Auszüge veröffentlichte. Minister Veiga Simo trat sofort zurück. Sein Amt übernahm am SonntagVize-Regierungschef und Außenminister Jaime Gama. Einhellig beklagten sozialdemokratische Opposition und regierende Sozialisten am Wochenende den nicht wiedergutzumachenden Schaden. Ministerpräsident Antnio Guterres sprach von einer "schwerwiegenden Beeinträchtigung staatlicher Interessen".

Dabei hatte Veiga Simo es doch "in gutem Glauben gehandelt", wie er versicherte. Schützend war er vor seinen ins Zwielicht geratenen Dienst getreten, dem man nachsagte, er habe undichte Stellen und beschatte hohe Militärs.

Wohl um den Untersuchungsausschuß davon zu überzeugen, dass er nichts zu verbergen habe, liess ihnen Veiga Simo alles zukommen, was von Belang sein konnte. Nicht nur Namen, Herkunft, Ausbildung und Gehälter sämtlicher Spione wurden offengelegt, sondern auch ihre Aufgaben in aller Welt. Sei es die Rolle von Agenten beim Aufstand gegen den Präsidenten von Guinea Bissau oder im Widerstand der Timorenser gegen Indonesien, sei es der Informationsaustausch des Geheimdienstes mit den Kollegen aus Deutschland und anderen befreundeten Staaten: Die Abgeordneten wie auch die Redakteure von O Independente erfuhren einfach alles. Nur den Lesern des Blattes wurde Wichtiges vorenthalten. Die Namen der Agenten wurden geschwärzt.

Die Suche nach Versäumnissen und Verantwortlichen ist mit dem fünf Monate vor den Parlamentswahlen erklärten Rücktritt Veiga Simos freilich keineswegs abgeschlossen. Während die Opposition ihr Augenmerk vor allem auf Nachlässigkeiten im Verteidigungsministerium richtet, konzentriert sich die Regierung auf den Vertrauensbruch in dem von einem Sozialdemokraten geleiteten Untersuchungsausschuss. "Total unverantwortlich" nannte es der Sozialdemokrat Luis Marques Guedes, daß ein so heikler Bericht mit dem Vermerk "vertraulich" ans Abgeordnetenhaus gehen konnte, anstatt mit dem Aufdruck "geheim" hinter Verschluß zu bleiben. Der Minister für parlamentarische Angelegenheiten, Antnio Costa, beklagte derweil, da die Affäre das Vertrauen der Regierung in die Volksvertreter ausgehöhlt habe.

Tröstliche Worte fand am Wochenende nur die Presse. Der Schaden könne zumindest im Ausland so groß nicht sein. Die Geheimdienste der EU- und Nato-Staaten hätten die Zusammenarbeit mit den skandalgebeutelten portugiesischen Kollegen auf das Nötigste beschränkt.

http://jya.com/nsa-patents.htm

National Security Agency-owned patents accessed at the US Patent Office online 28 May 1999. Obtained by search for "National Security Agency," though oddly none of the patents disclose the full name. This does not include all the NSA-sponsored patents, such those not owned/attributable to the agency or those classified and prohibited to public access. Full PTO text of patents mirrored here. See IBM's patent server for text and related images.

http://jya.com/nsa5832478.htm United States Patent 5,832,478 George November 3, 1998
Method of searching an on-line dictionary using syllables and syllable count

Abstract

The present invention is a method of searching an on-line dictionary in any language representation using syllables and syllable count and an on-line dictionary, where the on-line dictionary includes a primary headword field, a segmented primary headword field, additional unsegmented language representation (headword) fields as required, additional segmented representation (headword) fields as required, a syllable count field, additional syllable count fields as required, and a definition field. The user selects a language representation for a query and makes the query in the selected language representation. The present invention then parses the query to determine if segmented syllables were used in the query and how many, if any. If no segmented syllables were used in the query, a character string search for the headword that matches the query is conducted. If the query contains segmented syllables, a syllable search for headwords that contain the same syllables in the same locations is conducted. The present invention returns one or more headwords in the language of the query and their corresponding definitions in the language of the user. Various wildcard symbols may be used for unknown syllables and for characters within a syllable, which may include tones.

http://jya.com/nsa5812609.htm United States Patent 5,812,609 McLochlin September 22, 1998
Communication intercept device using digital drop receivers in multiple tiers

Abstract

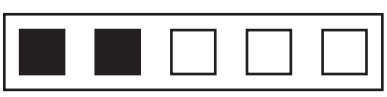
A communications intercept device that includes an analog-to-digital converter for digitizing an analog wideband input signal, a first memory for storing the digitized wideband signal, a first digital drop receiver in a first tier for selecting signals stored in the first memory, a controller for controlling which signals are selected, a second memory for storing the signals selected by the first digital drop receiver, and a second digital drop receiver in a second tier for selecting signals stored in the second memory under control of the controller.

* * *

http://jya.com/nsa5631961.htm United States Patent 5,631,961 Mills , et al. May 20, 1997
Device for and method of cryptography that allows third party access

Abstract

A device for and method of transmitting an encrypted message and an access field from a sender to a receiver, where a third party may intercept and process the transmission. The sender and receiver agree on a session key. The sender raises an element of a Galois Field to the session key; forms a temporary device unique key; encrypts the session key with the temporary device unique key; forms a temporary family key; encrypts an identifier of the sender and the encrypted session key using the temporary family key; encrypts a plaintext message using the session key; forms the access field by concatenating the element of a Galois Field raised to the session key to the encrypted version of the



sender's identifier and the sender's encrypted session key; concatenates the ciphertext to the access field; and transmits the access field and the ciphertext to the receiver. The receiver may recover the plaintext from the sender's transmission. The third party may partially process the transmission to find the identity of the sender. The third party may then request an escrowed key that would allow the third party to recover the plaintext of the sender's message.

* * *

http://jya.com/nsa4897878.htm United States Patent 4,897,878 Boll , et al. January 30, 1990 *Noise compensation in speech recognition apparatus*

Abstract

A method and apparatus for noise suppression for speech recognition systems which employs the principle of a least means square estimation which is implemented with conditional expected values. Essentially, according to this method, one computes a series of optimal estimators which estimators and their variances are then employed to implement a noise immune metric. This noise immune metric enables the system to substitute a noisy distance with an expected value which value is calculated according to combined speech and noise data which occurs in the bandpass filter domain. Thus the system can be used with any set of speech parameters and is relatively independent of a specific speech recognition apparatus structure.

* * *

http://jya.com/nsa4731840.htm United States Patent 4,731,840 Mniszewski , et al. March 15, 1988 *Method for encryption and transmission of digital keying data*

Abstract

A method for the encryption, transmission, and subsequent decryption of digital keying data. The method utilizes the Data Encryption Standard and is implemented by means of a pair of apparatus, each of which is selectable to operate as either a master unit or remote unit. Each unit contains a set of key encryption keys which are indexed by a common indexing system. The master unit operates upon command from the remote unit to generate a data encryption key and encrypt the data encryption key using a preselected key encryption key. The encrypted data encryption key and an index designator are then downloaded to the remote unit, where the data encryption key is decrypted for subsequent use in the encryption and transmission data. Downloading of the encrypted data encryption key enables frequent change of keys without requiring manual entry or storage of keys at the remote unit.

* * *

http://jya.com/nsa4567572.htm United States Patent 4,567,572 Morris , et al. January 28, 1986 *Fast parallel sorting processor*

Abstract

An information processor is described which is especially suitable for efficiently sorting large quantities of binary data. Data in a plurality of storage devices is fed to a plurality of compare-exchange modules and is then selectively passed back to the storage devices by means of multi-input switches. A programmable microprocessor controls passage of data through the various components in an iterative process.

http://jya.com/nsa-patents.htm

http://jya.com/nsa4429180.htm United States Patent 4,429,180 Unkenholz January 31, 1984
Apparatus for simultaneous generation of key at two locations

Abstract

An apparatus for simultaneously generating identical cipher key at two remote terminals in a manner which prohibits interception of the key by unauthorized persons. A circuit comprising three separate wire lines is connected between the two terminals over geographically separated routes. The circuit is randomly completed and broken by a switch at each terminal, the switch position being determined at each terminal by an independent key generator. Cipher key is communicated by comparing the key generator output and the circuit condition.

* * *

http://jya.com/nsa5812609.htm United States Patent 4,161,032 Williams July 10, 1979
Serial arithmetic functions with magnetic bubble logic elements

Abstract

Compact arrangements of two-input magnetic bubble logic gates providing bubble devices for performing serial integer arithmetic on binary integers are disclosed. Using only a small number of different types of logic gates, designs are given for devices for performing serial addition, subtraction, multiplication and division arithmetic operations on binary integers, represented as sequences of magnetic bubbles. All logical interactions use bubble repulsion to prevent bubbles from transferring to adjacent propagation paths via preferred transitions. By using only two-input gates and a pipeline computational structure, hardware design is simplified and advantage is taken of the inherent serial nature of bubble technology. The simple gate interconnection geometry has a minimum of feedback paths and results in devices which are not burdened with excessive numbers of bubble generators, annihilators or crossovers.

* * *

Y2K Problem Papst: Dem Ende der Welt gelassen entgegensehen

Rom Papst Johannes Paul II. hat den Menschen empfohlen, das Ende der Welt mit Gelassenheit und Hoffnung zu erwarten.

„Heutzutage passiert wegen der Fortschritte in Wissenschaft und Technologie und den erweiterten Kommunikationsmöglichkeiten alles mit unglaublicher Schnelligkeit“, sagte das Oberhaupt der katholischen Kirche am Mittwoch vor hunderten Gläubigen in seiner wöchentlichen Audienz auf dem Petersplatz in Rom. „Es ist daher ganz natürlich, über das Schicksal und das Ziel der Menschheit nachzudenken“, erklärte der Papst weiter.

Der 79jährige forderte die Gläubigen auf, dem „finalen Ereignis“ mit „ruhiger Hoffnung“ entgegenzusehen.

Information Operations

Information Operations Violates Protocol I

Escalating trends starting in the Coalition Gulf War and bearing fruit in the NATO Yugoslavia War bring to center stage the combination of infrastructural warfare tactics and modern weapons. When it is viewed in light of recently published US military doctrine on Information Operations (IO), it is clear that the lethal combination of technology and infrastructural targeting is accepted practice for the United States military not only during times of open hostility but, more critically, in times of peace as a political compellence strategy.

Lt. General Michael C. Short, commander of the air war in Kosovo, shed light on the attitude within the US military in the The New York Times, 18 June, 1999:

"Had airmen been in charge it would have been done differently, but that's water under the bridge," he said. "I felt that on the first night, the power should have gone off, and major bridges around Belgrade should have gone into the Danube, and the water should be cut off so that the next morning the leading citizens of Belgrade would have got up and asked, "Why are we doing this?" and asked Milosevic the same question."

NATO stopped short of this direct terror campaign but it did bomb electric systems and other vital civilian infrastructure including a television station which caused the death of journalists which violated Protocol I's protection of journalists. General Short's statement sends a clear signal that, at the highest levels of the United States military command, such behavior is believed to be acceptable and his is not an isolated view.

Earlier in the year, another American General discussed the American strategy for Information Operations (IO) which Joint Publication 3-13 describes as most effective in periods prior to open hostility and as targeting civilian computer, telecommunications, financial, and electric distribution system with high-tech methods such as Electronic Magnetic Pulse (EMP) guns, computer intrusions, viruses, and other IO means.

"The Joint Warfare Analysis Center down at Navy Dahlgren (Va.) is a national resource," explained Major General Bruce A. "Orville" Wright, Deputy Director for Information Operations, Joint Chiefs of Staff, at a Defense Colloquium on Information Operations. "They can tell you not just how a power plant or a rail system is built, but exactly what is involved in keeping that system up and making that system efficient."

"One of the terms I've learned from these guys is SCADA—Supervisory Control and Data Acquisition," he continued warming to the subject. "If you have that acronym in the IO business, you are well ahead of the fight. SCADA basically is the computer control for a power system or railroad or sewer system or water system. We rely more and more on those kinds of systems as potential targets, and sometimes very lucrative targets, as we go after adversaries."

These statements must be viewed within a historical perspective to understand their out-of-step views with international law. Civilian protection during times of hostilities has been a focus of both customary law and international treaty starting in 1863 with the Lieber Rules and then continuing with the 1868 St. Petersburg Declaration, 1922 Hague Rules of Air War, 1938 Resolution of the League of Nations Protection of Civilian Population Against Bombing From the Air in Case of War, the 1956 XIXth International Conference of the Red Cross Draft Rules for the Limitation of the Dangers Incurred by the Civilian Population in Time of War, and the Geneva Conventions of 1949.

Violates Protocol I

At the start of a new millennium, three ideas shine through from 140 years of modern treaty work. First, the means and methods to wage war are not unlimited. Second, technology has increased man's ability to cause massive civilian damage; therefore, treaties protecting the civilian population have become the focus of the Laws of War. Third, jus cogen (rules that may not be negotiated by a state) has been extended to the Laws of War, and jus ad bellum (the right to resort to war) and jus in bello (the method of war) have taken a secondary role to international and customary law.

The next logical step is a comprehensive review of Information Operations weapons and tactics and which places them in a context of Protocol I which is additional to the 4th Geneva Convention of 1949. This task should be shared by the United Nations and the International Committee of the Red Cross.

The United Nations jurisdiction is established by its history of human rights protection and specifically by United Nations Resolution 3384—10 November 1975—which proclaims:

"*All states shall refrain from any acts involving the use of scientific and technological achievement for the purposes of violating the sovereignty and territorial integrity of other states, interfering in their internal affairs, waging aggressive wars, suppressing national liberation…*"

In terms of treaty support to examine the new weapons of Information Operations, Protocol I provides the most direct reference in Article 36—New Weapons:

"*In the study, development, acquisition or adoption of a new weapon, means or method of warfare, a High Contracting Party is under obligation to determine whether its employment would in some or all circumstances be prohibited by this Protocol or by any other rule of international law applicable to the High Contracting Party.*"

The application of Article 36 is extremely important to this discussion because Protocol I does not currently mention IO as a method of attack and second, the definition of attack may need altering. Article 49 (3) reads:

"*The provisions of this Section apply to any land, air or sea warfare which may affect the civilian population, individual civilians or civilian objects on land.*"

Although the IO tactics against physical infrastructure may look similar to land or air warfare, it is not specifically stated so in the treaty. This also ties in with the treaty's definition of attack:

"*Attack means acts of violence against the adversary whether in offense or in defense.*"

The cogent issue boils down to one of semantics. Is a computer intrusion an attack? Is sending a logic bomb to disable a nuclear power plant an attack? The United States has used the popular media to denounce computer system intrusions as *attacks;* therefore, can it be assumed that the attack concept extended to IO is now universal? An examination of Protocol I for IO capabilities can clarify this point.

The key starting point is creating a modern definition of civilian versus military infrastructure. This has become an important issue in a world were much of the military telecommunications traffic passes over civilian networks, and it is difficult to separate electric power production from civilian and military targets. For this reason, it is best to look at this issue as three separate categories.

First, there is infrastructure that is, without dispute, dedicated to military usage. This includes roads, electric production at isolated army bases, and other well defined military objects. These items have never been in question. It is the second area that may be a gray area. This is the area of civilian roads, telecommunications, computer networks, electricity distribution, and water systems that may also feed military installations.

Article 50—Definition of Civilians and Civilian Population offers a method to solve this problem. It states:

(1) In case of doubt whether a person is a civilian that person shall be considered to be a civilian. It continues in (3) The presence within the civilian population of individuals who do not come within the definition of civilians does not deprive the population of its civilian character.

A revision could build on both items (1) and (3). All infrastructure should be considered civilian if it has mixed usage and this is supported by item (3) which, although written to apply to people, may give a hint as to future direction. An appropriate paraphrase may be the following:

The presence of military traffic or usage of civilian infrastructure should not deprive that specific piece of infrastructure from civilian protection and should be assumed to be civilian.

Finally, it is the third area of civilian infrastructure of financial systems, medical systems, food distribution, and media production and distribution systems that should be completely off limits to IO tactics. This prohibition should include physical attacks, system intrusions to include virus and worm production, and psychological warfare.

This third area should include all satellite, paging, and wireless systems as well as radio, television, and internet broadcast systems. In addition, the Protocol should protect all neutral communications nodes such as internet routers on third-party soil, submarine cables, microwave links, and satellite transponders and ground stations. In a mirror of the earlier rule in planning military operations, it should be assumed that targeting all such systems would lead to uncontrollable, systemic failures in the third-party systems; therefore, they should be exempt from targeting.

Article 54—Protection of Objects Indispensable to the Survival of the Civilian Population—may also be applicable to this area. There has been significant discussion in the United States about IO encompassing attacks on financial markets, automatic teller machines, toll road metering systems, mass transit systems to create a panic in the civilian population in the hopes of realizing the dreams of political compellence urged by General Short.

This type of strategic planning should be banned under Article 54 which states:

(2*) It is prohibited to attack, destroy, remove or render useless objects indispensable to the survival of the civilian population, such as foodstuffs, agricultural areas for the production of foodstuffs, crops, livestock, drinking water installations and supplies and irrigation works, for the specific purpose of denying them for the sustenance value to the civilian population or to the adverse party, whatever the motive whether in order to starve out civilians, to cause them to move away, or for any other motive.*

A convention dealing with IO weapons and usage should address the specific issue of indispensable infrastructure to the civilian population in a highly technological dependent society. It should clearly draw a connection between

telecommunications and electric systems to modern healthcare systems and determine and define issues of incidental damage versus targeted damage to the civilian environment.

Continuing with this train of targeting thought, a number of military strategists have described IO attacks on medical record systems that need to be discussed and classified in an updated Protocol I examination. Article 14—Limitations on requisition of civilian medical units may be applicable because it provides guarantees that the needs of the civilian population should be satisfied.

Other strategists have suggested attacks on military medical records by changing blood-types and other vital medical information to cause additional casualties and create confusion. This type of planning is a clear violation of the 4th Geneva Convention and Protocol I. Article 12:

1. Medical units shall be respected and protected at all times and shall not be the object of attack.

Any discussion of IO methods should update the protection afforded to wounded personnel. It should be clearly defined as to the level of protection afforded to medical records or databases containing quantities and types of medical supplies.

The final two areas under review deal with two very important items in relationship to Protocol I and IO:

Targeting of Dangerous Forces

Precautionary Measures

Article 56—Protection of works and installations containing dangerous forces—was a major stumbling block for the United States in ratifying Protocol I. Judge Abraham D. Sofaer, legal advisor, US Department of State explained the position of the United States government on 22 January 1987.

"The study," Sofaer explained referring to a Joint Chiefs of Staff assessment of Protocol I, "concluded that Protocol I is militarily unacceptable for many reasons. Among these are the Protocol unreasonably restricts attacks against certain objects that traditionally have been considered legitimate targets."

The dangerous forces that the United States wanted to preserve the right to attack and destroy included dams, dykes, and nuclear electrical generating stations. Fortunately, 135 other nations disagreed with the US position. Any discussion of IO and Protocol I should include the information systems of these facilities that were so aptly described by General "Orville" Wright.

Attacks on dams could take the form of a system intrusion of the water flow and release system of a dam so that in a rainy season it released water at an improper rate; therefore, the dam would not have released enough water to hold the accumulation of the rainy season and would overflow causing the loss of human life and economic destruction to an adversary.

Other attacks could be as simple as seizing control of the flood gates at a dam which would have the same affect as described above. The discussion of nuclear facilities should seem obvious. There can be any number of scenarios; an IO attack could destroy or damage a nuclear power plant or affect the temperature of water released into a fresh water stream. Once again, any discussion of IO and Protocol I should be expanded to this area.

Finally, meeting the provisions of Article 57 should play a vital role in any IO treaty under the colour of Protocol I. Section 57 (ii) states:

...protocol I violation

Those who plan or decide upon an attack shall: (ii) Take all feasible precautions in the choice of means and methods of attack with a view to avoiding, and in any event to minimizing, incidental loss of civilian life, injury to civilians and damage to civilian objects.

An expectation of limitation and control should be the final barrier to IO weapons because it builds on Article 51 (4):

Indiscriminate attacks are prohibited. Indiscriminate attacks are: (b) Those which employ a method or means of combat which cannot be directed at a specific military objective. (c) Those which employ a method or means of combat the effects of which cannot be limited as required by this Protocol.

IO attack planning should have knowledge of the complete infrastructure not just isolated systems. Without this systemic view, damage could cascade from one system to another and violate the requirement of limited attacks at only specified military systems. This statement holds true because of the interconnected nature of the modern infrastructure and Protocol I discussions should either acknowledge that this provision may not apply to IO weapons or clearly state the level of responsibility for the attack planner in the event of incidental loss of civilian life, injury to civilians and damage to civilian targets.

Article 57 2 (b) may prove the most difficult in a compliance mode.

"An attack shall be canceled or suspended if it becomes apparent that the objective is not a military one or is subject to special protection or that the attack may be expected to cause incidental loss of civilian life, injury to civilians, damage to civilian objects or a combination thereof, which would be excessive in relation to the concrete and direct military advantage anticipated."

It is the requirement to cancel or suspend certain types of IO attacks that will cause problems with Protocol I compliance. For example, internet or network worms or viruses have demonstrated an ability to spiral out of control in related and unrelated systems. In an interconnected world, this may cause damage to vital civilian systems that were not directly targeted. Once it was determined that a vital (non-targeted) civilian system was affected it is very difficult, if not impossible, to withdraw or stop the worm or virus. In essence this creates a form of weapons use treaty that was not intended by this protocol.

Conclusion

It is the opinion of the Centre for Infrastructural Warfare Studies (CIWARS) that the governments of the world have already entered into an IO arms race, and it is only a matter of time before this type of capability will proliferate to guerrilla or terrorist groups. By extending this work to Protocol II as well, which extends the provisions of Protocol I to non-international conflicts and could include guerrilla groups, which have a significant history of infrastructural warfare, the human rights work started in the last millennium will be maintained and advanced.

William Church Centre for Infrastructural Warfare Studies (CIWARS) Email: iwar@iwar.org

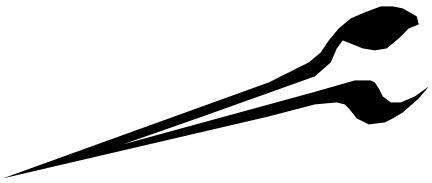
---

?!

Pat. 5224756 : Integrated child seat for vehicle

ASSIGNEES: The United States of America as represented by the Director of the National Security Agency, Fort George G. Meade, MD

Termine



Chaos Communication Camp
6.–8. August 1999

Paulshof, Altlandsberg bei Berlin

http://www.ccc.de/camp/

außerdem

3.-4. Juli 1999 Mitgliederversammlung des Chaos Computer Club e.V.
Wer Mitglied ist, aber noch keine Einladung erhalten hat, möge sich möglichst umgehend an office@ccc.de bzw. die Hamburger Geschäftsstelle (siehe Adressen) wenden.

27.-29. Dezember 1999 Chaos Communication Congress 1999, Berlin

Chaos Bildungswerk Hamburg: Siehe http://www.hamburg.ccc.de/Workshops/index.html

Sa. 10.07.1999 + So 10.07.1999 19.30 h Linux Installation Party - bitte anmelden

Do 15.07.1999 19.30h Linux Grundlagen (kleine Anleitung wichtiger Unix-Tools)

Bestellungen, Mitgliedsanträge und Adreßänderungen bitte senden an:

CCC e.V., Lokstedter Weg 72
D-20251 Hamburg

Adreßänderungen auch per Mail an office@ccc.de

Der Mitgliedsfetzen

Mitgliedsanträge und Datenschleuderabonnement

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

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

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

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

Die Kohle liegt

o als Verrechnungsscheck
o in Briefmarken

bei bzw.

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

Ort/Datum _____

Unterschrift _____

Name _____

Straße _____

PLZ, Ort _____

Tel/Fax _____

E-Mail _____

Der Bestellfetzen

Literatur

_____ DM 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 25,00 Congressdokumentation CCC ‘97
_____ 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
_____ DM 15,00 Alle Datenschleudern des Jahres 1997

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 5,00 Portopauschale!

_____ Gesamtbetrag

Die Kohle liegt
o als Verrechnungsscheck (bevorzugt)
o in Briefnarken

bei bzw.

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

Name _____

Straße _____

PLZ, Ort _____