

# **TCPA - resistance is futile?**

Ruediger Weis

cryptolabs Amsterdam

# Outline

- Einführung
- TCPA Trust
- Kryptographische Probleme
- Netzwerk Probleme
- TCPA und GPL
- Konsequenzen

# Literatur

- Ross Anderson,  
TCPA / Palladium FAQ  
<http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html>
- Lucky Green,  
Trusted Computing Platform Alliance:  
The Mother(board) of all Big Brothers,  
<http://www.cypherpunks.to>
- Felix von Leithner, Frank Rieger, Max von Malotki,  
Chaosradio 78
- Heise Ticker, ct

# Um was es geht

"Treacherous computing is  
a major threat to our freedom".

Richard Stallman

# Bill speaks

"We came at this thinking about music, but then we realized that e-mail and documents were far more interesting domains."

Bill Gates, Microsoft

# Wissensvernichtung

"You could create Word documents that could be read only in the next week."

Steven Levy, MSNBC/Newsweek

# Es hat bereits begonnen.

"Microsoft may provide security related updates to the OS Components that will be automatically downloaded onto your computer. These security related updates may disable your ability to copy and/or play Secure Content and use other software on your computer."

Microsoft, Windows Media Player EULA

# Microsoft Lizenzen

- Viele Endnutzer-Lizenzen vom Microsoft sind innerhalb der EU juristisch nicht haltbar.
- Beispielsweise postulierte Microsoft ein Verbot mit Frontpage Microsoft-kritische WWW Seiten zu erstellen.
- TCPA könnte verwendet werden, *rechtswidrige*, verbraucherunfreundliche Lizenzen technisch zu erzwingen.



# TCPA und Betriebssysteme

- Microsoft beherrscht einen überwältigenden Anteil des Betriebssystem-Marktes.
- TCPA und Palladium können daher schwerlich isoliert betrachtet werden.
- TCPA bringt auch Probleme für Linux.

# Der TCPA Trust

”AMD had no choice.”

# Trusted Computing Platform Alliance

Gegründet 1999 von:

- Intel
- Microsoft
- HP
- Compaq
- IBM

Die Liste der Mitglieder befindet sich *nicht* im öffentlichen Bereich des WWW Servers ([www.trustedcomputing.org](http://www.trustedcomputing.org)).

# IT Firmen

360 Degree Web

3Com Corporation

Access360

Acer

ActivCard Inc.

Adhaero Technologies

Adobe Systems Inc.

Advanced Micro Devices

aeSec Corporation

Aladdin Knowledge Systems

Algorithmic Research Ltd.

# IT Firmen

American Express Company  
American Megatrends Inc.  
Argus Security Corporation  
Atmel Corporation  
ATMEL Rousset  
Authentium, Inc.  
Autotrol Uruguay S.A.  
Baltimore Technologies Ltd  
BERGDATA AG  
BindView Development  
Blueice Research

# IT Firmen

Broadcom Corporation

Carraig Ltd

Caveo Technology LLC

Cavium Networks

CE-Infosys Pte Ltd

Cerberus Information Security Limited

Certicom Corp.

Check Point Software Technologies Ltd

CHECKFLOW

Chrysalis-ITS

Cimarron Systems Incorporated

# IT Firmen

CipherKey Exchange Corporation

Cloakware Corporation

Communication Intelligence Corporation

Compagnie Européenne de Développement SA

Compal Electronics, Inc.

Compaq Computer Corporation

Computer Elektronik Infosys GmbH

Crypto AG.

Cygate ESM Oy

CYLINK Corporation

Dell Computer Corporation

# IT Firmen

DICA Technologies Inc.  
DigiGAN, Inc  
Digital Innotech Co.  
Digital Persona Inc.  
Discretix Technologies Ltd.  
e-PCguard.com, Inc.  
eCryp, Inc.  
Eltan Comm B.V.  
Enova Technology Corporation  
Ensure Technologies  
Entrust Technologies Ltd.



# IT Firmen

ERACOM Pty Ltd

Ethentica

Excalibur Solutions, Inc

FARGOS Development, LLC

FINGLOQ AB

First Access, Inc.

Fortress Technologies Inc

Fujitsu Limited

Fujitsu-Siemens-Computers

Gateway, Inc.

Gemplus Corporation

# IT Firmen

GLOBEtrotter Software

Hewlett-Packard Company

Hitachi, Ltd. PC Div.

HyperSecur Corporation

I/O Software, Inc.

ICSA.net

ID Tech

IdentAlink Limited

Infineer Inc.

Infineon Technologies Corporation

Infineon Techno. Asia Pacific Pte Ltd

# IT Firmen

InfoCore, Inc.

Insyde Software Corp.

Integrity Sciences, Inc.

Intel Corporation

Interlok Technologies L.L.C.

International Business Machines

International Service Consultants Ltd.

Internet Dynamics, Inc.

Internet Security Systems

InterTrust Technologies

Iomega Corporation

# IT Firmen

Kasten Chase Applied Research

Keycorp Ltd.

Keyware Technologies, Inc.

Lanworks Technologies Co.

Legend (SHENZHEN) R&D Center, L. Group Ltd.

Lexign

Liquid Audio, Inc.

Litronic Inc.

LOGISIL Consulting

M-Systems Flash Disk Pioneers

M3S Enterprises

# IT Firmen

Macrovision Corporation  
Massive Media Group  
Media DNA Incorporated  
Medialogic Co., Ltd  
Miaxis Biometrics Co.  
Micron Electronics, Inc  
Microsoft Corporation  
Mitac International Corporation  
Mobile-Mind, Inc.  
Motorola  
National Semiconductor  
nCipher Inc.

# IT Firmen

NDS Limited

NEC Corporation

Net Nanny Software International

NetActive Inc.

NetAtmosphere Inc.

NetOctave, Inc.

NetSecure Software Canada

Network Associates, Inc.

New Trend Technology Inc.

Novell, Inc.

nVidia

O2Micro

# IT Firmen

Open Source Asia PC Guardian  
Philips Semiconductors  
Phoenix Technologies, Ltd.  
Pijnenburg Custom Chips B.V.  
Precision Digital Hardware  
Pricewaterhouse Coopers  
Prism Resources, Inc.  
Pro-Team Computer Corp.  
Protect Data Security Inc.  
Rainbow Technologies, Inc.  
Raytheon Company  
Raz-Net Inc.

# IT Firmen

Redstrike B.V.

RSA Security, Inc.

SafeNet, Incorporated

SAFLINK Corporation

SAGEM MORPHO, Inc.

SAGRELTO Enterprises, Inc.

SAMSUNG ELECTRONICS CO.

SAS Institute

Schlumberger, Smart Cards

Science Applications International Co.

Scienton Technologies Inc.

SCM Microsystems



# IT Firmen

Sectra Communications AB

Securant Technologies

Secure Computing Corporation

Secure Systems Solutions

Siemens AG

Softex, Inc.

SPYRUS, Inc.

SSH Communications Security, Inc.

Standard Microsystems Corporation

STMicroelectronics

Symantec Corporation

Symbol Technologies, Inc

# IT Firmen

Texar Software Corp.

Thales e-Security, Inc.

TimeCertain, LLC

Titan Systems Corporation

Toshiba Corporation

Trend Micro, Inc.

Tripwire, Inc.

Trispen Technologies

TrueTime Inc.

TruSec Solutions

Trustpoint Corporation

TVN Entertainment Corporation

# IT Firmen

Ubizen

Utimaco Safeware AG

ValiCert Inc. VeraSafe, Inc.

Veridicom, Inc.

Verisign, Inc.

Viewpoint Engineering

Voltaire Advanced Data Security Ltd

Wave Systems Corp.

Wincor Nixdorf

WinMagic, Inc.

WinVista Corporation

# TCPA Übersicht

Ermöglicht Fremdkontrolle  
über den persönlichen Computer

# Vorgänger

- Bill Arbaugh, Dave Farber, Jonathan Smith, “A Secure and Reliable Bootstrap Architecture”, IEEE Symposium on Security and Privacy (1997).
- US patent: “Secure and Reliable Bootstrap Architecture”, U.S. Patent No. 6,185,678, February 6th, 2001.
- James Anderson, “Computer Security Technology Planning Study”, USAF, 1972.

# Administrator Rechte

TCPA erzwingt 3 Levels von Zugriffsrechten.

Privileged access	TCPA members only
Underprivileged access	platform owner
Unprivileged access	non-TCPA applications

# Keymanagement

- **Endorsement Key:**  
Eindeutiger RSA Schlüssel erzeugt vom **Hersteller**.  
Dieser ist unterschrieben mit Hersteller Schlüssel,  
welcher wiederum unterschrieben ist mit dem **TCPA  
master key**.
- **User Keys:**  
Ein oder mehrere User RSA Keys unterschrieben von  
einer "Privacy CA" .

# Crypto

In RSA/SHA-1 we trust.



# Cryptographic operations

Tamper-resistant hash and key store.

- Hashing (SHA-1, HMAC).
- Random number generation (RNG).
- Asymmetric key generation (2048-bit RSA).
- Asymmetric key enc/dec (2048-bit RSA).

# SHA und SHA-1

- SHA basiert auf MD4.
- Erste SHA Version bot nicht die erwartete Sicherheit.
- Änderung ohne genaue Begründung.
- Wir ahnen inzwischen warum.

# Gebt das Hash frei!

NIST, October 12, 2000: SHA-256, SHA-384, and SHA-512.

”The current approved hash algorithm, SHA-1, produces a message digest of 160 bits, providing no more than 80 bits of security against collision attacks.”

- SHA-1 produziert nur 160 bit Output.
- SHA-256, SHA-512 noch praktisch ungetestet...

# Microsoft Key-Management

- Mitte 2001 vergass MS sein Server-Zertifikat zu verlängern. Niemand konnte sich bei MSN und Passport anmelden.
- Ebenfalls 2001 warnte Microsoft vor einem von einem Unbekannten erschlichenen "Microsoft" Zertifikat von Verisign.
- `nsa_key`

# Black Box Crypto

Verdeckte Kanäle leicht zu implementieren.

# Trusted Plattform Module (TPM)

- Fritz Chip
- Momentan festverlötete Smartcard
- Später Integration in Prozessoren (LaGrande)

# Sicherheit und Vertrauen

Michael Plura, ct 26/2002, S.56

Interview mit Thomas Rosteck, Leiter des Product Marketing für Sicherheits-ICs bei Infineon und seinem Chef.

- **ct:** Ist es schwierig diese [TPM] Funktionen zu validieren?
- **Rosteck:** Nein, es gibt eine Test-Suite, die überprüft, ob alle Funktionen vorhanden sind und funktionieren.

# Busverschlüsselung

- **ct:** Wie werden die Daten auf dem Bus verschlüsselt, also die Kommunikation mit dem Prozessor?
- **Rosteck:** Die Daten werden auf dem Bus nicht verschlüsselt, aber die meisten Befehle sind digital signiert.



# Keine Busverschlüsselung!

- X-Box: Bus einfach abhörbar. (MIT)
- Timing: Signaturerzeugung zu langsam.

# Hintertüren

- ct: Gibt es eine Hintertür ?
- Rosteck: Nein.
- ct: Wirklich nicht?

# All Your Keybit are belong to us

Weis, Ruediger, Lucks, Stefan,  
"All Your Keybit are belong to us -  
The Truth about Blackbox Cryptograpy",  
SANE 2002, Maastricht 2002.

# Hauptergebnisse

- Es ist möglich geheime Informationen aus einem "beweisbar sicherem" Blackbox-System "beweisbar sicher" herauszuschmuggeln.
- Selbst eine Hardwareanalyse kann nicht aufdecken, welche Informationen durchgesickert wurden.

# Sophisticated Bit Smuggling

**Beispiel: Nutze den IV von Block Cipher Modis.**

Seien  $E_{\text{pub}}$  der Public Key der Designerin Dora und  $K'$  ein zusätzlicher Secret Key festverdrahtet im Device.

Wir generieren den IV folgendermassen:

- Sei

$$Y = E_{\text{pub}}(K)$$

- wähle  $(n - 1)$  random bits

$$(r_1, \dots, r_{n-1}) \in \{0, 1\}^{n-1}$$

# Sophisticated Bit Smuggling II

- abhängig von  $(r_1, \dots, r_{n-1})$  und  $K'$ , erzeuge pseudozufällig  $(z_1, \dots, z_m) \in \{0, 1\}^m$   
(z.B. Streamcipher( $(r_1, \dots, r_{n-1}, 0) \oplus K'$ ))

- berechne

$$p = \bigoplus_{1 \leq i \leq m} z_i y_i$$

- und nutzte

$$(r_1, \dots, r_{n-1}, p) \in \{0, 1\}^n \text{ als IV.}$$

# Nutzung des verdeckten Kanals

- Mit der Kenntnis von  $K'$  kann Dora  $(z_1, \dots, z_m)$  aus  $(r_1, \dots, r_{n-1})$  berechnen.
- Sie sammelt  $m$  linear unabhängige Vektoren, diese erlauben dann

$$(y_1, \dots, y_m) = Y = E_{\text{pub}}(K)$$

durch die Lösung eines Linearen Gleichungssystems zu berechnen.

- Mit  $Y$  kann sie  $K$  bestimmen.

# Angenehmes Abhören

Bemerkenswert ist, dass nur

- eine kleine Anzahl
- von zeitlich nicht notwendigerweise zusammenhängenden Ciphertexten
- passiv abgehört

werden muss.



# Hardware Analyse

- Durch Hardwareanalyse kann man  $K$  und  $E_{\text{pub}}$  finden.
- Doch dann müsste man das zu Grunde liegende Public Key Verfahren brechen.

# All Your Key are belong to us



- Dieses "verräterische" Logo gehört sicher jemandem und wird hier nur zur wissenschaftlichen Dokumentation verwendet!-)

# Weitere Manipulationsmöglichkeiten

- Zufallszahlenquelle
- Schlüsselerzeugung
- ...

# Hintertüren und Zertifizierung

- **Rosteck:** Nein. Wir haben vorhin über die Tests gesprochen - es gibt natürlich auch eine Sicherheits-Zertifizierung der Bausteine, wobei dem Zertifizierer die Entwicklungsdokumentation für diesen Baustein offengelegt wird.

# Wer zertifiziert?

- NSA?
- BSI?
- ...

# Lawful Interception?

Ein Beispiel aus den Niederlanden.

- Paul Wouters, Patrick Smits,  
Dutch tapping room not kosher
- <http://www.fnl.nl/ct-nl/archief2003/ct2003-01-02/aftappen.htm>

## Zusatzfrage:

- Wie funktioniert Lawful interception,  
wenn TCPA sicher wäre?

# Computernetzwerke

”DNS Rootserver hoch zehn.”

# Zentralisierte Netzdienste?

- Approved Hardware List (HCL)
- Serial Number Revocation List (SRL)
- Document Revocation List (DRL)
- Timeserver



# Ein Single Point of Failure

... ist sicher keine gute Idee.

Aber Dezentralisierung ist wegen des Schlüsselmanagements nicht trivial.

- Ist ein "trusted" Rechner ohne Netz praktisch nicht mehr nutzbar?

# GPL und TCPA

Cooperation oder Hijacking?

# GNU/Linux und TCPA

- Mindestens zwei Firmen arbeiten einer "TCPA-enhanced" version von GNU/Linux.
- Nach einer kostspieligen Evaluation wird *eine* Version unterzeichnet.
- Diese Entwicklung muss unter GPL bleiben, jede Änderung macht die Signatur ungültig.
- Dies ist in jedem Fall ein Verstoß gegen die Grundphilosophie von Freier Software.

# Software Evaluation

”The evaluation is at level E3 - expensive enough to keep out the free software community, yet lax enough for most commercial software vendors to have a chance to get their lousy code through.”

Ross Anderson

# Hijacking GPL

”People believed that the GPL made it impossible for a company to come along and steal code that was the result of community effort. This helped make people willing to give up their spare time to write free software for the communal benefit. But TCPA changes that. . . . The point is this: once people realise that even GPL’ed software can be hijacked for commercial purposes, idealistic young programmers will be much less motivated to write free software.”

Ross Anderson

# Interoperabilität

- XML Office
- MS blockiert beim Winword-Dateiformat.
- TCPA Container behindern Datenaustausch.

# Conclusion

Es drohen zwei Welten zu entstehen,  
eine TCPA Welt und die Freie (Software) Welt.

# Philosophie

- Offene Netzze haben eine Wissensexplosion ausgelöst.
- TCPA bedroht die Wissensgesellschaft.
- Es drohen zwei Welten zu entstehen, welche Schwierigkeiten haben werden Informationen auszutauschen.



# The OS War is over

- Windows bedeutet Sklaverei.
- US Gesetze gelten auch für Apple.  
Die Zeit läuft ab.
- GNU/Linux ist momentan die Alternative.
- Natürlich wird es auch zukünftig BSD, Minix (GPL) und weitere Exoten geben.  
Und das ist auch gut so.

# Lucky's Patent

**Subject:**

Re: Wired: Can a Hacker Outfox Microsoft?

Thanks. Hope it works.

# US Law

”One political sentence: Even if Microsoft would be the nicest US company of the world it would still be a company under US law and I do not want to give a foreign government control over my computer systems not even for fighting terrorists.”

Ruediger Weis, Programmkomitee-Mailingliste USENIX/CARDIS2002

# Most wonderful

”I think the US is the most wonderful and benevolent country in the world, and I still would not want the US Government putting a black box in my computer. (Just because the country is great does not mean that some of the officials are not corrupt.) Much less give control to a company like Microsoft, which clearly operates on a different ethical basis than I do.”

US-Bürger auf Programmkomitee-Mailingliste USENIX/CARDIS2002

# Nachtrag

- **18.1.2003:**

Richard Purcell, der oberste Datenschutzbeauftragte von Microsoft, tritt zurück.

- **21.1.2003:**

Palladium heisst jetzt:

Next-Generation secure Computing Base  
for Windows

# Kontakt

Dr. rer. nat. Ruediger Weis, Dipl.-Math.  
cryptolabs Amsterdam

• `ruedi@cryptolabs.org`

• `www.cryptolabs.org`

© Ruediger Weis 2002 and 2003

unter der GNU Free Documentation License

<http://www.gnu.org/copyleft/fdl.html>

Produced with GPL software. Typesetting:  $\text{\LaTeX}$ .

PGP fingerprint = C8 B5 52 AC 05 EA C7 2A EB 31 E3 FB 65 DD 7A 76