



# DRM und "Trusted Computing"

Ruediger Weis

cryptolabs Amsterdam

CRYPTOLABS

# Overview

---

- TCG and Microsoft
- Digital Restrictions Management
- Enforcement
- New Idea: Owner Override

# Bill Gates zu Palladium

---

Obgleich es wiederholt bestritten wurde, war der Ausgangspunkt für die Entwicklung von TCPA und Palladium Überlegungen zum Digital Restrictions Management (DRM).

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

Bill Gates, Microsoft

# Gates Interview 03/03

---

- "Palladium überprüft die Integrität von Software und kann dadurch helfen, die Urheberrechte zu schützen.
- "das gute Recht jedes Urhebers, seine Inhalte zu verteilen, wie es ihm gefällt.
- "Es wird immer einen Weg geben, Schutzmechanismen zu umgehen."

Focus

# CCC Fahndungsplakat 0.2



# 'Ein Chip sie zu knechten '

---

- Richard Stallman:

- ▶ *"Treacherous computing is a major threat to our freedom".*

- CHIP:

CeBIT-Highlights 2003: Die besten Produkte

- ▶ **"Bremse des Jahres": IT-Allianz TCPA**

# Planned Hardware Changes

---

- Memory curtaining
- Secure input and output
- Sealed storage
- Remote attestation

# 'The right way to look at this'

---

"The right way to look at this is you are putting a virtual set-top box inside your PC. You are essentially renting out part of your PC to people you may not trust."

**Ron Rivest**, ACM Turing Award Winner 2002.  
( $\approx$  Nobel Price for Computer Science)



# Whitfield Diffie

---

RSA Conference, San Francisco, April 2003.

**Whitfield Diffie**, Inventor Public-Key Cryptography.

- "(The Microsoft approach) lends itself to market domination, lock out, and not really owning your own computer. That's going to create a fight that dwarfs the debates of the 1990's."
- **"To risk sloganeering,  
I say you need to hold the keys  
to your own computer"**

# Ron Rivest

---

**Prof. Ron Rivest (MIT)**, Developer of the RSA Algorithm and the MD4-hash function family.

- "We should be watching this to make sure there are the proper levels of support we really do want".
- "We need to understand the full implications of this architecture. This stuff may slip quietly on to people's desktops, but I suspect it will be more a case of a lot of debate."

# TCG and Microsoft

---

- Microsoft will use TCG1.2 for Longhorn.
- **Microsoft controls ca. 90%** of the Operation Systems market.
- TCG and Palladium **SHOULD NOT** be discussed separately.
- TCG brings also **problems** to Open Source Software like GNU/Linux.

# Windows Media Player EULA

---

"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."

# Enforcement

---

- "Microsoft Lizenzen lächerlich"?
- Enforcement by
  - ▶ TPM Chip
  - ▶ DMCA
- Forced 'updates'

# Forced 'Updates'

---

- heise online News, 12.09.2003,  
Xbox Live schließt ''Sicherheitslücke''
- heise online News, 19.08.2003,  
Microsoft will automatische  
Updatefunktion für nächstes Windows
- heise online News, 03.09.2003,  
Bill Gates setzt auf automatische Updates

# Black Box Crypto

---

Hidden Channels are so easy - also "provable" secure:

- Ruediger Weis, cryptolabs Amsterdam  
Stefan Lucks, Universität Mannheim

**"All Your Keybit are belong to us -  
The Truth about Blackbox Cryptography",**

SANE 2002, Maastricht 2002.

# Official TCG Statement

---

Answer of the TCG resp. CCC questions (Juni 2003)

- "Es ist natürlich nicht völlig auszuschliessen, dass ein Chip-Hersteller ein TPMs mit Funktionen baut, die von der Spezifikation abweichen und einen Zugriff auf gespeicherte Schlüssel erlauben."

International and Independent Control needed.

Processor Integration...



# External Key Generation

---

- The keys are often generated **outside** the chip to save money.
  - ▶ Producer has easy access to the private key of the user device.

International and Independent Control needed.

# NSA and Backdoors

---

- heise online News, 09.08.2003,  
NSA will gegen Hintertüren vorgehen

*"In seiner Aussage wies Wolf ebenfalls darauf hin, dass "untrustworthy hardware" (nicht vertrauenswürdige Hardware) ein Problem ähnlicher Tragweite werden kann."*

# Microsoft and Backdoors

---

- **Q: Won't the FBI, CIA, NSA, etc. want a back door?**
- **A:** Microsoft will never voluntarily place a back door in any of its products and would fiercely resist any government attempt to require back doors in products. From a security perspective, such back doors are an unacceptable security risk because they would permit unscrupulous individuals to compromise the confidentiality, integrity, and availability of our customers' data and systems. [...]

*... "never voluntarily" ...*

# MS: Lawful Interception

---

- **Q: How could a law enforcement agency access data protected by the NGSCB architecture?**
- **A: Just as with other commercial-grade cryptographic hardware, law enforcement agencies could conceivably "break" the SSC in the hardware of a seized machine to obtain machine secrets.**

# Intel and Backdoors

---

- July 2003: Hearing Ministry of Economy:  
1 min of silence
- Streams:  
Bundesministerium für Wirtschaft und Arbeit

Symposium:

"Trusted Computing Group (TCG)"

am 2. und 3. Juli 2003 (Berlin),

<http://www.webpk.de/bmwa/willkommen.php>

# Intel has learned

---

## Processor-ID failed.

- Oct 2003: IDF:
  - ▶ Own Endorsement Key
  - ▶ FIPS certification
  - ▶ Zero-Knowledge
  - ▶ No Backdoors ('naive')

... but still there are a lot of problems.

# Real-World Key-Management

---

- 2001: Microsoft server certificate expired (MSN, Passport,...).
- Microsoft seems to be still looking for a "lost" certificate from 2001.
- nsa\_key

# TCPA Certificate expired

The screenshot shows a Mozilla browser window with the address bar displaying `https://www.trustedcomputing.org/tcpaasp4/index.asp`. The page content includes a banner for the TCPA (Trusted Computing Platform Alliance) and a security warning dialog box. The dialog box contains the following text:

**Trusted Computing**  
"www.trustedcomputing.org" is a site that uses a security certificate to encrypt data during transmission, but its certificate expired on 02/26/2003 07:31 PM.

You should check to make sure that your computer's time (currently set to Tue 06 May 2003 06:30:48 PM CEST) is correct.

Would you like to continue anyway?

The background page shows the TCPA logo and a banner that reads "WELCOME TCPA TRUSTED COMPUTING PLATFORM ALLIANCE". Below the banner, there are sections for "About TCPA" and "Mission". The "Mission" section states: "Through the collaboration of HW, SW, communications, and technologies for an enhanced security environment, TCPA implements trust in platforms."

A security warning dialog box is open, displaying the following information:

**Could not verify this certificate because it has expired.**

**Issued To**

Common Name (CN)	www.trustedcomputing.org
Organization (O)	Intel Corporation
Organizational Unit (OU)	Trusted Computing Platform Alliance
Serial Number	08:A5:99

**Issued By**

Common Name (CN)	Thawte Server CA
Organization (O)	Thawte Consulting cc
Organizational Unit (OU)	Certification Services Division

**Validity**

Issued On	02/26/2002
Expires On	02/26/2003

**Fingerprints**

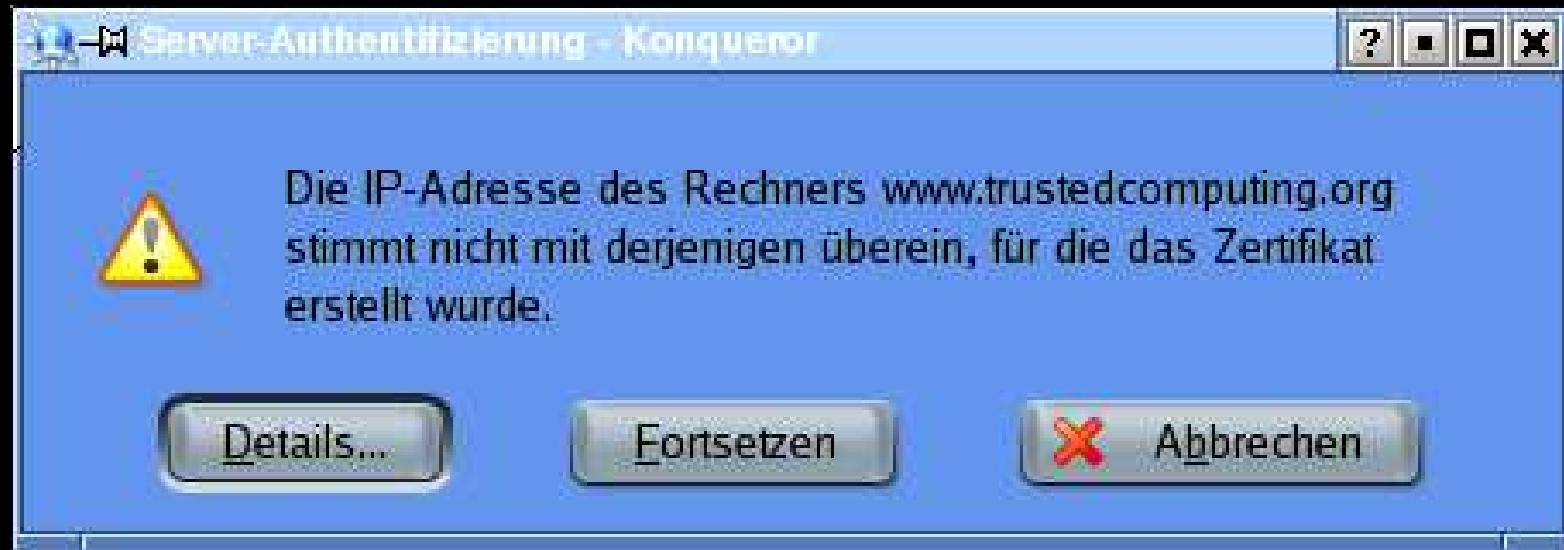
SHA1 Fingerprint	5E:E3:51:89:F9:DE:9C:C2:58:F5:90:D2:75:C3:24:65:D4:EA:AC:3
MD5 Fingerprint	D8:4C:E7:8C:70:DA:A9:0A:75:B7:F0:18:6A:AC:72:D4



# For a long, long time!



# Digital Identity Crises



# 'Niemals kompatibel'

---

**Peter N. Biddle**, Microsoft Product Unit Manager Palladium, Comdex 2002

- " Grundsätzlich könnte die gesamte Palladium-Architektur auch nach Linux portiert werden, wenn die Lizenzvorbehalte im Stil der GPL nicht wären. Jeder Code für ein TPM wird von der TCPA signiert und verschlüsselt. Wird irgendetwas weitergeben, verändert und neu kompiliert, so ist eine neue TCPA-Lizenz erforderlich. So gesehen wird das Trustworthy Computing niemals mit einer Open-Source-Lizenz kompatibel sein."

# Microsoft: Open Source OS

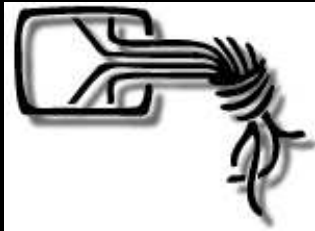
---

- **Q: Could Linux, FreeBSD, or another open source OS create a similar trust architecture?**
- **A:** From a technology perspective, it will be possible to develop a nexus that interoperates with other operating systems on the hardware of a nexus-aware PC. Much of the next-generation secure computing base architecture design is covered by patents, and there will be intellectual property issues to be resolved. It is too early to speculate on how those issues might be addressed.

# Demands

---

- Chaos Computer Club



- ▶ TCPA - Whom do we have to trust today?
- ▶ <http://www.ccc.de/digital-rights/forderungen>
- ▶ u.a. **volle Schlüssel-Kontrolle**

# CEBIT 2003 Forderungen

---

Die Chaos Computer Club an IBM überreichten Forderungen zu TCPA:

- 1. Vollständige Kontrolle des Anwenders über sämtliche gespeicherten Schlüssel
- 2. Sicherstellung, dass keine verborgenen Kanäle existieren, über die geheime Schlüssel des Anwenders übertragen werden.
- 3. Übertragung von Schlüsseln auf einen anderen Rechner muss ermöglicht werden.
- 4. Transparenz über die Zertifizierungs-Mechanismen

# A New Idea from the EFF

---

- Egg of Columbus?!



CRYPTOLABS

# EFF: Promise and Risk

---

- Seth Schoen
  - ▶ Trusted Computing: Promise and Risk
  - ▶ Comments LT policy



[http://www.eff.org/Infra/trusted\\_computing/](http://www.eff.org/Infra/trusted_computing/)



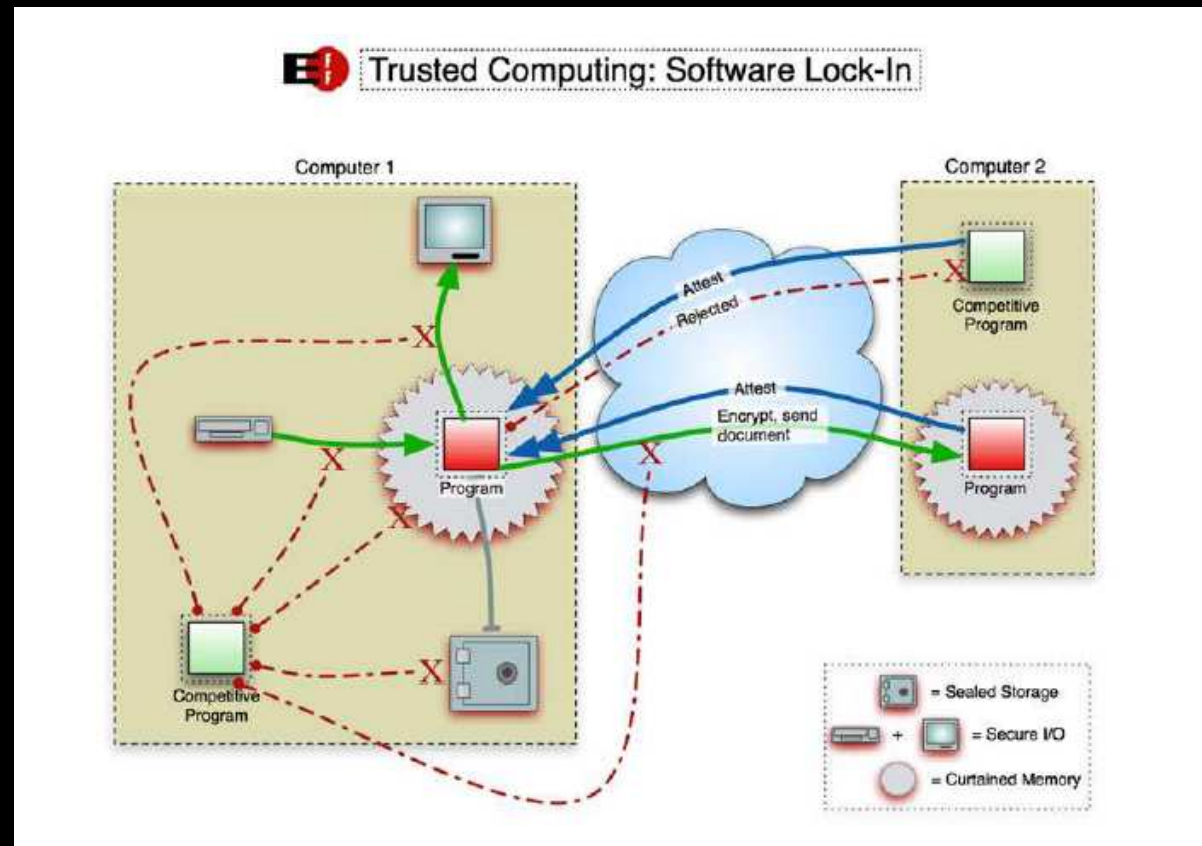
# Problem Remote Attestation

---

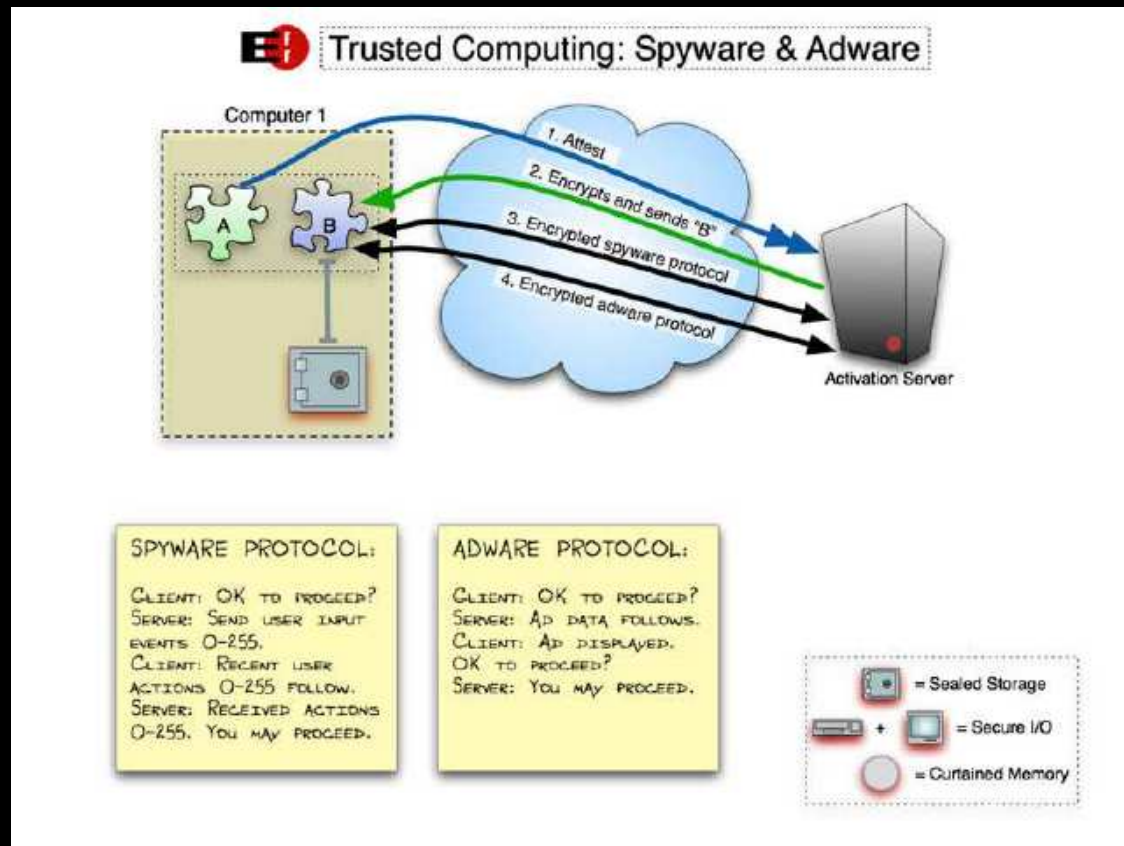
Third parties can enforce policies **against** computer owner – for example:

- Digital Restrictions Management (DRM)
- application lock-in
- migration and back-up restrictions
- forced upgrades and downgrades
- application-specific spyware
- preventing reverse engineering

# Software Lock-In



# Spyware



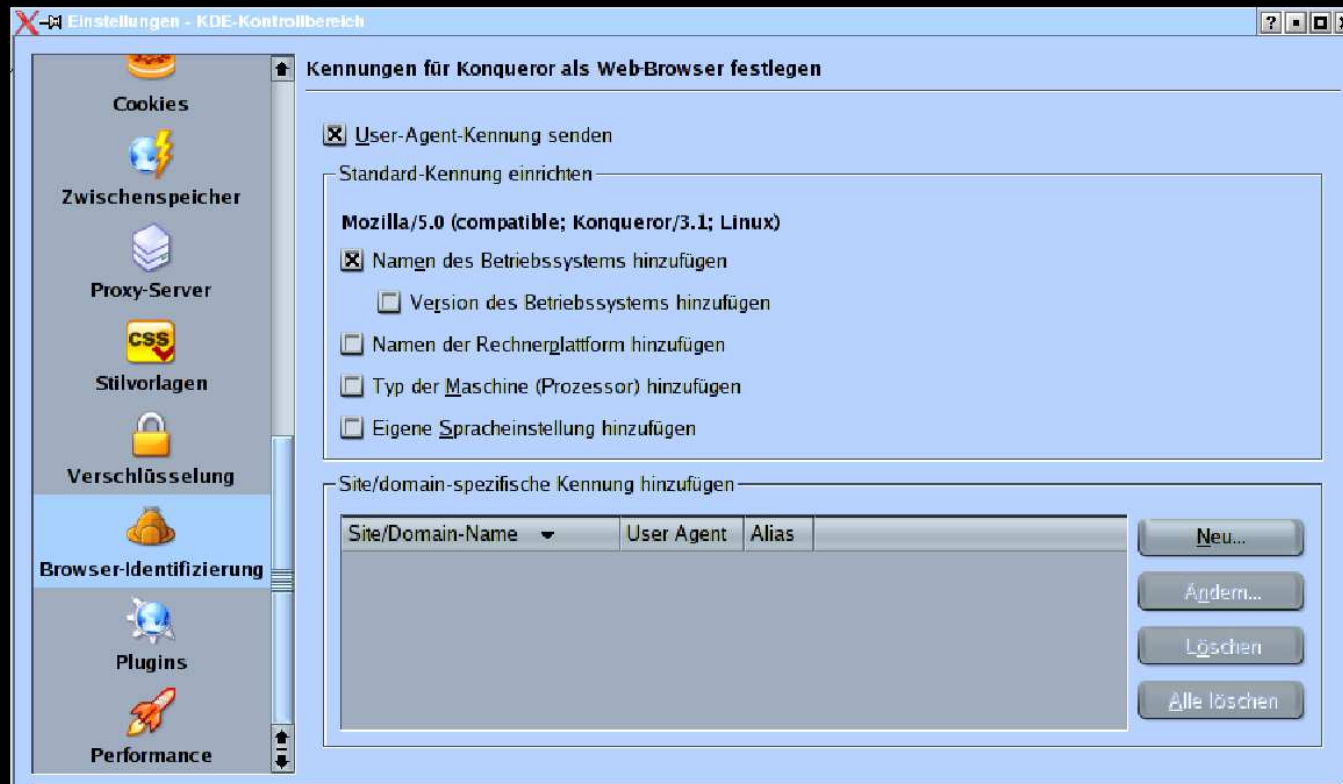
# Speaking to Big Brothers

---

**” Third-party uncertainty about your software environment is normally a feature, not a bug. ”**

- Samba ...

# Real World Example



# Owner Override

---

”Owner Override works by empowering a computer owner, when physically present at the computer in question, deliberately to choose to generate an attestation [...] to present the picture of her choice of her computer’s operating system, application software or drivers.”

# Attestation + Owner Override

---

- Compromise of software can still be made detectable by a remote party
- Computer owners retain substantial control over local software
- Competition, interoperability, user control and choice are preserved

# Company Policy

---

- An organization can more effectively enforce policies against its own members,
  - ▶ so long as they are using computers owned by the organization



# Resistance helps

---

- Intel has redrawn the plans for a **Processor-ID** because of the user resistance.
- TCG1.2 has fixed *some* problems.
- **'We are important customers!'**

# Acknowledgments

© cryptolabs Amsterdam 2003 under the GNU Free Document License.

Produced with Free Software under GNU/Linux.



"Licht ins Dunkel", Spiegel Online 08/03

**Big thanks to:**

Rop Gonggrijp, Carla van Rijsbergen, Andreas Bogk, Lucky Green, Ross Anderson

Andy Tanenbaum, Guido v. Noordende, Kees Bot, Philip Homburg, Jan-Mark Wams

**CRYPTOLABS**