”Trusted Computing”
Vertrauen für die grossen Brüder?

Ruediger Weis

cryptolabs Amsterdam

Overview

- TCG and Microsoft
- TCG 1.2
  - Backdoors and Hardware Security
  - Removing Endorsement Key
  - Direct Anonymous Attestation
- New Idea: Owner Override

Planed Hardware Changes

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

CCC Fahndungsplakat 0.2

’One chip to rule them all’

- Richard Stallman:
  - *”Treacherous computing is a major threat to our freedom”.*
- CHIP:
  CeBIT-Highlights 2003: Die besten Produkte
  - **”Bremse des Jahres”: IT-Allianz TCPA**

’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`

New in TCG 1.2

- + DAA
- + FIPS 140-2
- (+) Removable Endorsement Key
- + AES192, AES256, Triple-DES
- - SHA1
- - Openness

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.

Hauptergebnisse

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

Sophisticated Bit Smuggeling

Beispiel: Nutze den IV von Block Cipher Modis.
Seien E_{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

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

Sophisticated Bit Smuggeling II

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

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

- und nutzte

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

Verdeckter Kanal

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

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

  durch die Lösung eines Linearen Gleichungssytems 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.

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.

TCG 1.2

Nov 2003: RSA Amsterdam: TCG 1.2

- FIPS140-2
  - Who does the evaluation?
- Removable Endorsement Key
  - Fine for big companies and 3 letter organizations.
- Direct Anonymous Attestation
  - Good idea!

MUST 2048 bit or greater

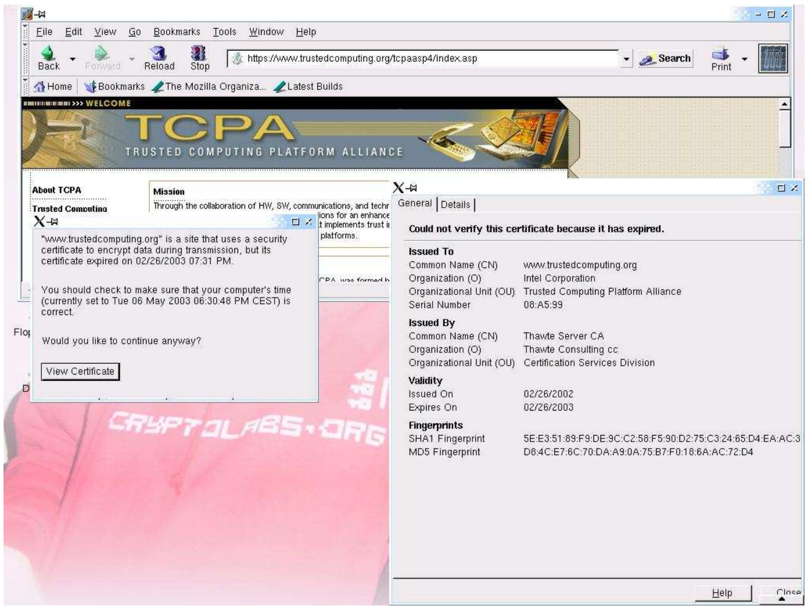
TCG1.2 (Part 1, P.12 f.)

- ”All Storage keys MUST be of strength equivalent to a 2048 bit RSA key or greater.”
- ”The minimum RECOMMENDED key size is 2048 bits.”
  - Why support for 512, 768 and 1024?
  - Why SHA-1 with only 160 bit output?

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



’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

A New Idea from the EFF

- Egg of Columbus?!

EFF: Promise and Risk

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

Electronic Frontier Foundation
Defending Freedom in the Digital World

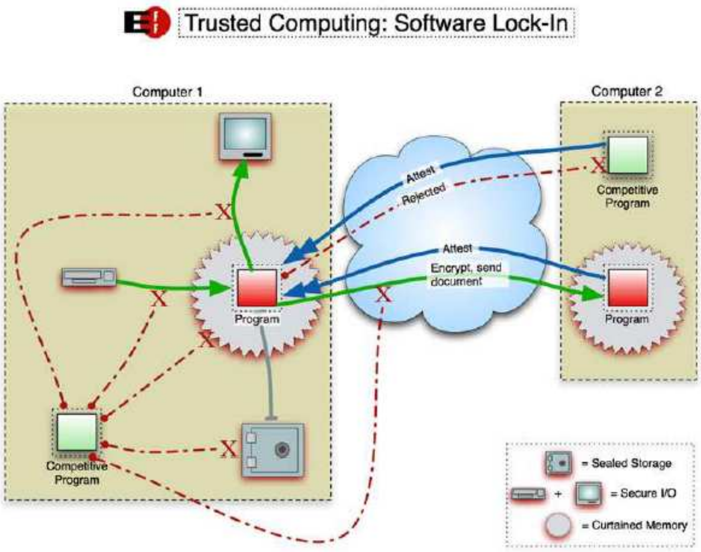
http://www.eff.org/Infra/trusted_computing/

Problem Remote Attestation

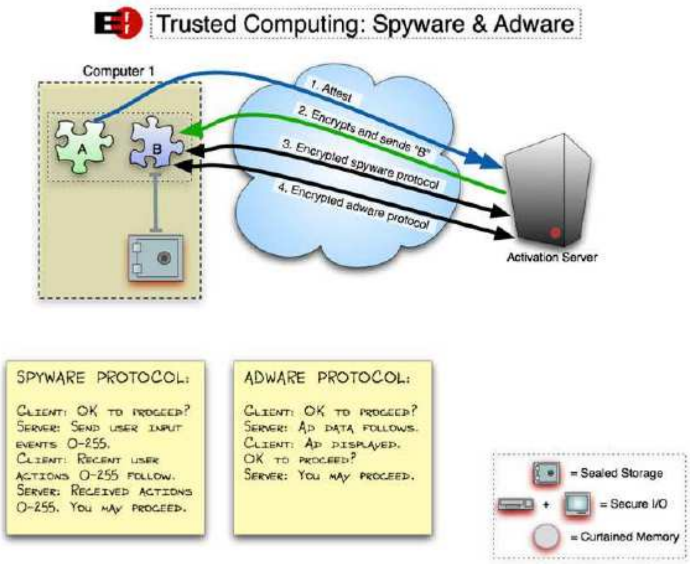
Third parties can enforce policies
against computer owner – for example:

- 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

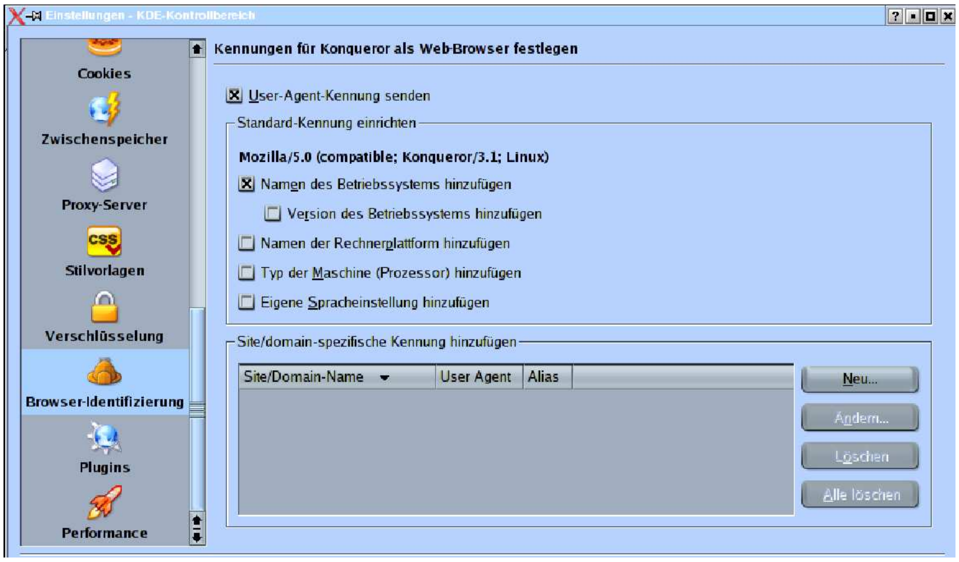


Speaking to Big Brothers

” 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

TPM and Smart Cards

- TPM $\approx$ Hardwired Smart Card
- First realizations: LPC Bus

Cryptolabs Smart Card Stuff

- File Encryption with KDE GUI
- PGP and GPG
- FreeS/WAN
  (with Bastiaan Bakker and Stefan Lucks)

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!'
- Fight Digital Restrictions Management!

The OS War is over

- Windows means slavery.
- Apple is a company under US Law.
- Life free:
  - GNU/Linux
  - BSD
  - Minix
  - **Write Your own and put it under GPL!**

German Government on TCG

Federal Government's Comments on the TCG and NGSCB in the Field of Trusted Computing

`www.bsi.de/trustcomp/stellung/`

`StellungnahmeTCG1_2a_e.pdf`

EU on TCG

23.01.2004:
Datenschutzgruppe der Europäischen Union
Arbeitspapier über vertrauenswürdige
Rechnerplattformen und insbesondere die
Tätigkeit der Trusted Computing Group (TCG)

`www.europa.eu.int/comm/internal_market/`
`privacy/docs/wpdocs/2004/wp86_en.pdf`

Acknowledgments

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

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