Synergie 2006 Berlin

Quo Vadis Linux:

DRM Systeme und Trusted Computing

Prof. Dr. Rüdiger Weis

Technical University of Applied Sciences Berlin

Overview

- Trusted Computing Architecture
- Cryptographical Problems
- Lock-Out Problems
- Problems for Linux
- Workarround

TC und DRM Version 1

- Security Pipeline Magazine February 5, 2004
- Rob Enderle

  ” The group is laboring under the burden of a couple of misconceptions by the public: Despite misconceptions to the contrary, this group is not directed by either Microsoft or the U.S. government. They are not primarily focused on Digital Rights Management; any secure repository would be attractive to a DRM solution, but DRM is not the goal of this group. ”

TC und DRM Version 2

- Annual Computer Security Applications Conference ACSAC, December 6-10, 2004, Tucson, Arizona
- Workshop on Trusted Computing
- Chair: Dr. Harvey H. Rubinovitz, The MITRE Corporation
- ”One use of trusted computing is Digital Rights Management (DRM). DRM is a term used for technologies that control how digital content is used. Creators of documents and entertainment media (music, movies, etc.) can control what type of access (read-only, read for the next 10 days, copy, etc.) is allowed to their content, and prevent unauthorized access.”

$\mathbf{T} \in \{Trusted, Treacherous\}$

- 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, ACM Turing Award Winner 2002.

- ”(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.”

'Policy Neutral': DRM and censorship

DRM and censorship are Siamese twins.

'Policy Neutral'

- The same techniques which avoid copying music songs can be used to limit the access to all kinds of documents.
- The combination of **DRM and Observation Hardware** leads to very dangerous implications.

DRM and censorship are Siamese twins.

TCG and SHA-1

TCG Presentation, RSA 2005

- ”SHA-1 Computing Engine
  - Multiple uses: integrity, autohization, PCR extension, etc.”

!!!TCG architecture is builded on
a **broken** cryptographic function!!!

Why are SHA-1 collissions so harmfull?

TCG uses SHA-1 for allmost all operations.
The iterative structure of SHA1 makes attacks practical.

- Integrity messaments using SHA-1 are compromized.
- Digital signatures using SHA-1 are compromized.
- PKIs using SHA-1 are compromized.

We have warned the TCG to use SHA-1
e.g. in our CCCongress talks every year since 2002.

- Weis, R., Lucks, S.,"Hash-Funktionen gebrochen", Datenschutz & Datensicherheit (DuD) 04/05, 2005.

Verschärfte Blackboxprobleme

Neue Blackboxprobleme durch höhere Integration

- `www.heise.de/newsticker/meldung/print/51173`
  Heise-Ticker, 16.09.2004
- IBM Notebooks verwenden National Semiconductors PC8374T bzw. PC8392T.

Integration

Stellungnahme der Bundesregierung zu den Sicherheitsinitiativen TCG und NGSCB im Bereich Trusted Computing, S. 2 f., Absatz 2.2

- ” Um die Funktionen des Sicherheitsmodules eindeutig zuordnen zu können und eine eindeutige Prüffähigkeit zu gewährleisten, müssen sie Sicherheitsfunktionen an eine zentralen Stellle in einem seperaten Baustein (TPM) gebündelt werden. Eine Vermischung des Sicherheitsmoduduls mit anderen Funktionseiheiten (z.B. CPU, Chipsatz, etc.) führt zu Intransparenz und dazu, dass eine sicherheitstechnische Überprüfung nicht mehr einfach durchführbar ist. ”

Worried Contries

TCG on RSA 2005
”Integrated vs. Discrete”
...

- ”Some contries worry where they’re made:
  - Today: Taiwan, China, Germany, United States, others”

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...

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" ...

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`

Secure I/O Probleme

- Neue Patent-Probleme.
- Neue Kartell-Probleme.
- Neue Blackbox-Probleme.
- 'Orwellsche' Zensur-Möglichkeiten.

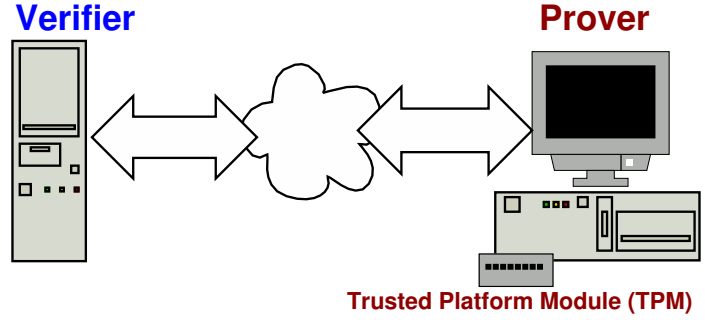
New in TCG 1.2

Nov 2003, Amsterdam: TCG 1.2

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

Improved Privacy

- Unique Enorsment Key ($\approx$ Device-ID)
- Linkability



TCG 1.2:
'Crypto Magic': Zero Knowledge Techniques

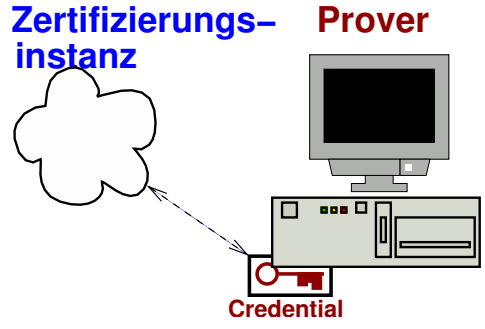
Direct Anonymous Attestation

- E. Brickell, J. Camenisch, L. Chen
  - ”Direct Anonymous Attestation”
  - Manuscript 2004.

  We thank the authors for providing an early version for scientific discussion.
- R. Weis, S. Lucks, A. Bogk
  - ”TCG 1.2 - Play fair with the Fritz-Chip?”
  - SANE 2004.

DAA Protocol

- TPM chooses a secret f,
- the secret f is blindly signed by the CA, with a CL-signature (Camenisch/Lysyanskaya)
- Pseudonym $N_V = \zeta^{\mathrm{f}} \bmod \Gamma$



Widerufbarer Schutz

Widerufbarer Schutz der Privatssphähre

$$N_V = \zeta^{\mathbf{f}} \bmod \Gamma$$

- Variante I: Benutzer wählt ζ.
- Variante II: Überprüfer wählt ζ.
  $\Longrightarrow$ Schutz beliebig reduzierbar.

Chaos Computer Club

- Chaos Computer Club, Old Europe

  - TCPA - Whom do we have to trust today?
  - http://www.ccc.de/digital-rights/forderungen
  - Full User Control over all keys.

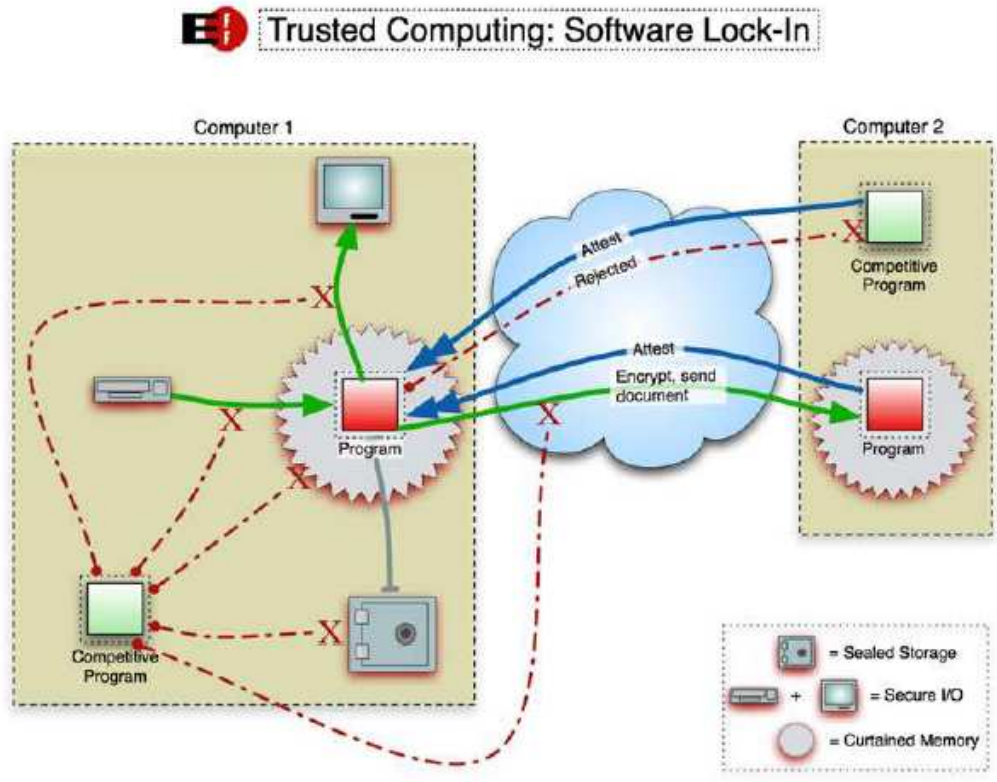
EFF: Promise and Risk

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

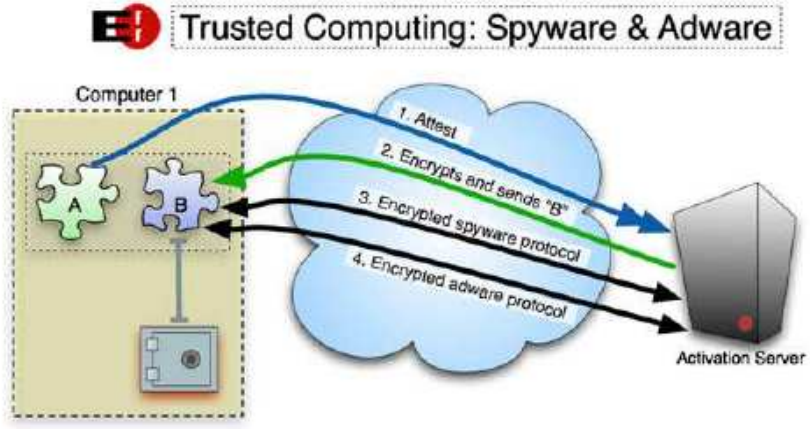
`http://www.eff.org/Infra/trusted_computing/`

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

Software Lock-In



Spyware

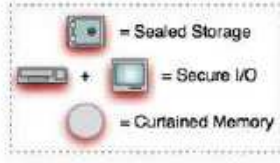


SPYWARE PROTOCOL:

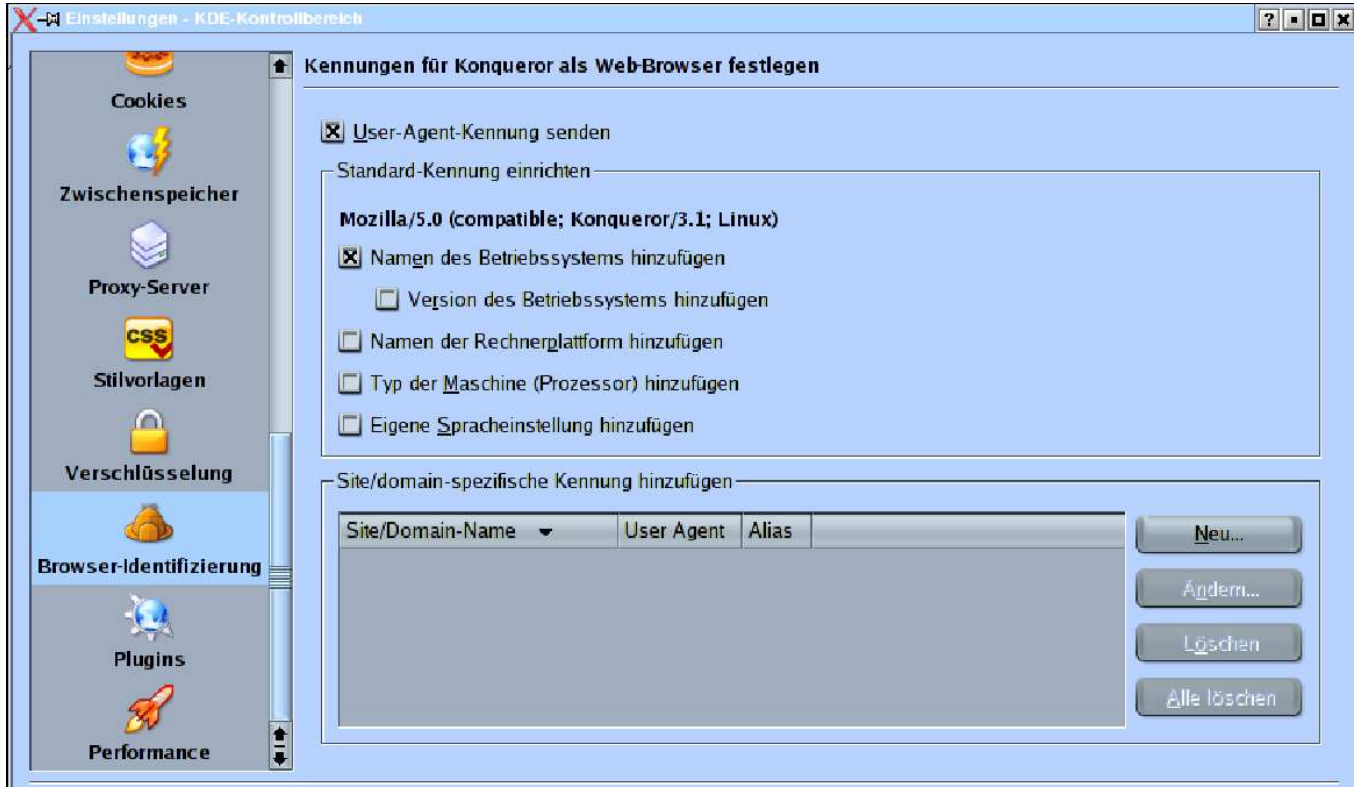
CLIENT: OK TO PROCEED?
SERVER: SEND USER INPUT EVENTS 0-255.
CLIENT: RECENT USER ACTIONS 0-255 FOLLOW.
SERVER: RECEIVED ACTIONS 0-255. YOU MAY PROCEED.

ADWARE PROTOCOL:

CLIENT: OK TO PROCEED?
SERVER: AD DATA FOLLOWS.
CLIENT: AD DISPLAYED.
OK TO PROCEED?
SERVER: YOU MAY PROCEED.



Real World Example



Owner Override

- Seth Schoen (EFF):
  ”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.

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`

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.

IBM gesteht 'Einsperren' ein

"

David Safford vom IBM Research gestand ein, dass derartige Mechanismen zum Einsperren der Nutzer in proprietären Softwarewelten mit Trusted-Computing-Systemen denkbar seien.

"

www.heise.de/newsticker/meldung/print/46789

’Niemals mit Open-Source kompatibel’

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

- Ich kenne viele Installationen, die Dual-Boot-Systeme sind. Mal wird Linux, mal Windows geladen. Ist Windows geladen, kann Palladium gestartet werden. Wer soll da bitte wen behindern? ” 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.”

Resistance helps

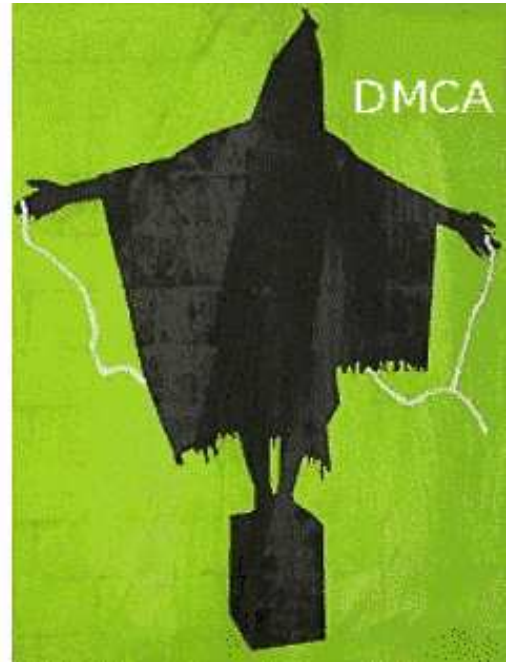
- Intel has redrawn the plans for a **Processor-ID** because of the user resistance.
- TCG1.2 has fixed *some* problems.
- 'We are important customers!'
- Fight Digital Restrictions Management!
- GPL 3.0

The OS War is over

- Windows means slavery.
- Apple usese TPMs inside the Intel Macs.

"We are stunned that [...] has adopted the **tactics and ethics of a hacker** to break into the iPod and we are investigating the implications of its actions under the **DMCA and other laws**."

Do Not Think Different.



Ballmer Junior

www.heise.de/newsticker/meldung/51814

- Allerdings gebe es neben jenen, die aus finanziellen Gründen "Raubkopien" nutzten auch jene, die Probleme mit aktuellen DRM-Techniken hätten die bei Windows schon seit Jahren eingesetzt werde. Dazu zählt Ballmer auch seinen eigenen zwölfjährigen Sohn.

Keine Panik!

- ” Er [David Stafford, IBM Research] forderte die versammelte Gemeinde von Bürgerrechtlern, Programmierern und Hackern allerdings auf,

  ”nicht über mögliche Attacken auf die Offenheit in Panik zu geraten”

  Der Markt verlange überall nach offenen, interoperablen Lösungen, so dass diese sich – zumindest langfristig – durchsetzen würden.”
  ”

www.heise.de/newsticker/meldung/print/46789

The OS War is over

- Life free:
  - GNU/Linux
  - BSD
  - Minix

- **Write Your own and put it under GPL!**

Acknowledgements

Andy Tanenbaum, Jan Mark Wams, Richard Stallman