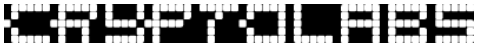
Trusted Computing 2004 - eine unendliche Geschichte

Ruediger Weis & Andreas Bogk

cryptolabs Amsterdam & CCC Berlin



Overview

- T* computing in 2004
- Neue Blackboxprobleme durch Integration
- Widerufbarer Direct Anonymous Attestation
- Owner Control
- TPM Hacking

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`

Kostenlose TCG-Mitgliedschaft

Business Community Day Frankfurt, Juni 2004

”Industry Liaison Program”

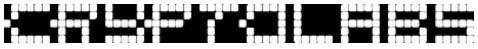
Lobenswert, aber:

- **- NDA.**
- **- Kein Stimmrecht.**

Advisory Council

- David Farber, Telecommunications Systems Professor Universität von Pennsylvania, EFF
- Moira Gunn, ”Tech Nation”
- Gary Roboff, ISTPA (International Security, Trust & Privacy Alliance)
- Rigo Wenning, W3C, P3P
- Rob Enderle, EDV-Analyst

Nur beratend.



Rob Enderle, 1999

”Bill Gates auf dem Weg zur Herrschaft über das Internet”

- Rob Enderle:

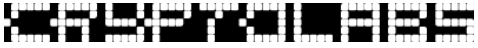
  ”Microsoft, weltweit größter Softwarehersteller und gemessen am Börsenwert das wertvollste Unternehmen überhaupt, will das Internet total beherrschen”

Zitiert nach: Christiane Schulzki-Haddouti, telepolis 18.05.1999,

Rob Enderle, 2004

Trusted Computing: Maligned by Misrepresentations and Creative Fabrications,

- Security Pipeline Magazine February 5, 2004
- ”One of the critical roles IBM, HP, and Sun play with this group is ensuring that the platform is open and cross-platform. Sun in particular has no interest in a Microsoft-only solution, and Sun, IBM and AMD don’t want an Intel-only solution either. The participation of these companies will likely mitigate the risk of hardware or software lock-in.
  And the international membership is designed to ensure the result doesn’t favor US companies or is in any way compromised by the U.S. government.”



Rob Enderle, 2004

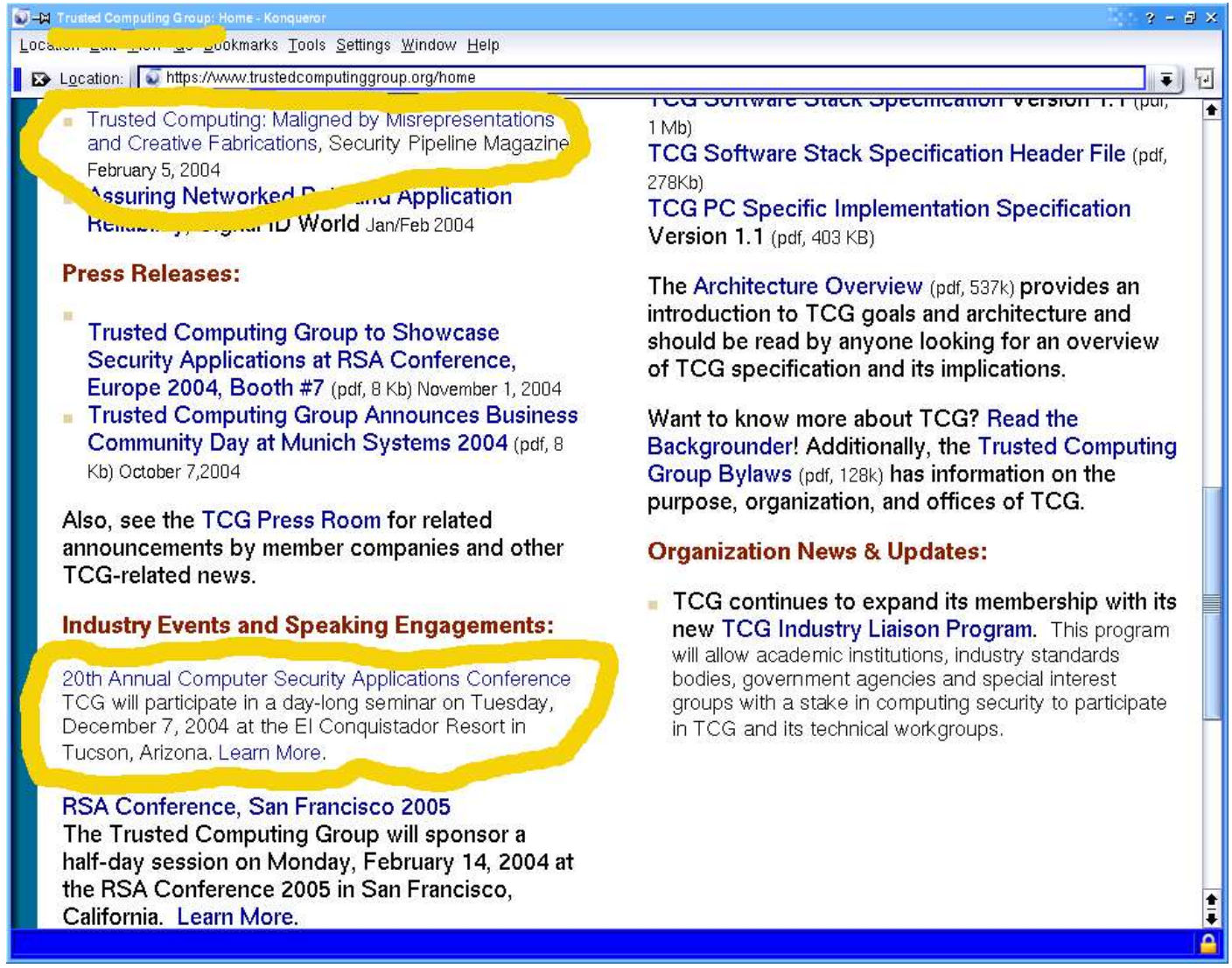
SCO Keynote, Rob Enderle:

Free Software and the Idiots who Buy It

- ”I actually am Bill Gates Love slave”

www.sco.com/2004forum/agenda/Enderle_keynote_SCO-Forum2004.html

TCG Homepage



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.”

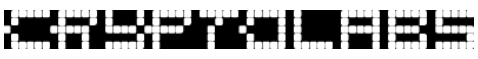
$\mathbf{T} \in \{Trusted, Treacherous\}$

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

Planed Hardware Changes

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

'One chip to rule them all'



'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.”

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 by hardware

'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.

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.

Super-I/O Baustein

National Semiconductors Super-I/O-Bausteine

- Tastaur
- Maus
- Drucker
- Floppy-Laufwerk
- RS-232-Schnittstellen
- **TCG-1.1b**-Trusted Platform Module

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. ”

IBM: Mehr als 16 Mio alte TPMs

Nach eigenen Angaben hat IBM weltweit bereits mehr als 16 Millionen PCs mit altem TPM abgesetzt.

- Embedded Security Subsystem 2.0
- **TCG-1.1b** Trusted Platform Module

Alte Standardversion ohne verbesserten Schutz der Privatspähre!

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`

Sichere I/O

- Heise Ticker, 14.09.2004,
- Der **Trusted-Mode Keyboard Controller** (TMKBC) soll einen sicheren Kanal zum dem sicheren Teil des Kernel. ermöglichen.
- Geplant für 2005.

Secure USB

- Intel & Microsoft: USB-Security-Extension-Schema (USB SE)
- Geplant für Herbst 2005.

Mit einem sicherem USB Kanal bieten

USB Smart-Card/Leser Systeme

einen noch besseren Ersatz für die festgelöteten TPMs.

Secure I/O Probleme

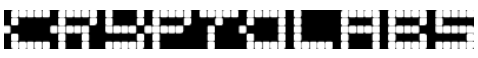
- Neue Patent-Probleme.
- Neue Kartell-Probleme.
- Neue Blackbox-Probleme.
- 'Orwellsche' Zensur-Möglichkeiten.

Kein Staatsexamen!

New in TCG 1.2

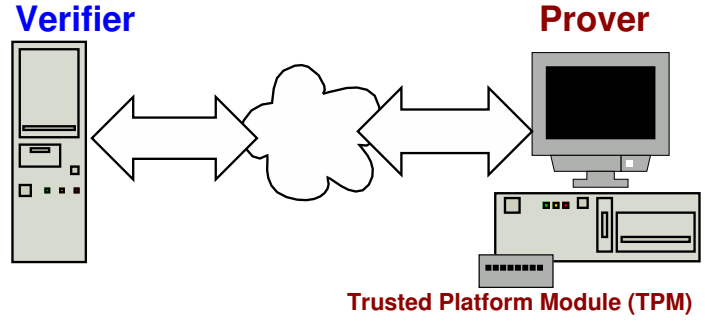
Nov 2003, Amsterdam: TCG 1.2

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



Improved Privacy

- Unique Enorsment Key (≈ Device-ID)
- Linkability



TCG 1.2:
'Crypto Magic': Zero Knowledge Techniques

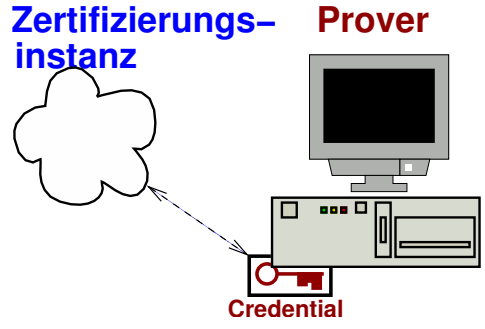
Direct Anonymous Attestation

- 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.

Cryptograghical Remarks

- !!!Many mathematical errors in the standard documents!!!
- !!!Use better Hash!!!

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.

A Brilliant Idea from our US friends

- Owner Override = Egg of Columbus?!

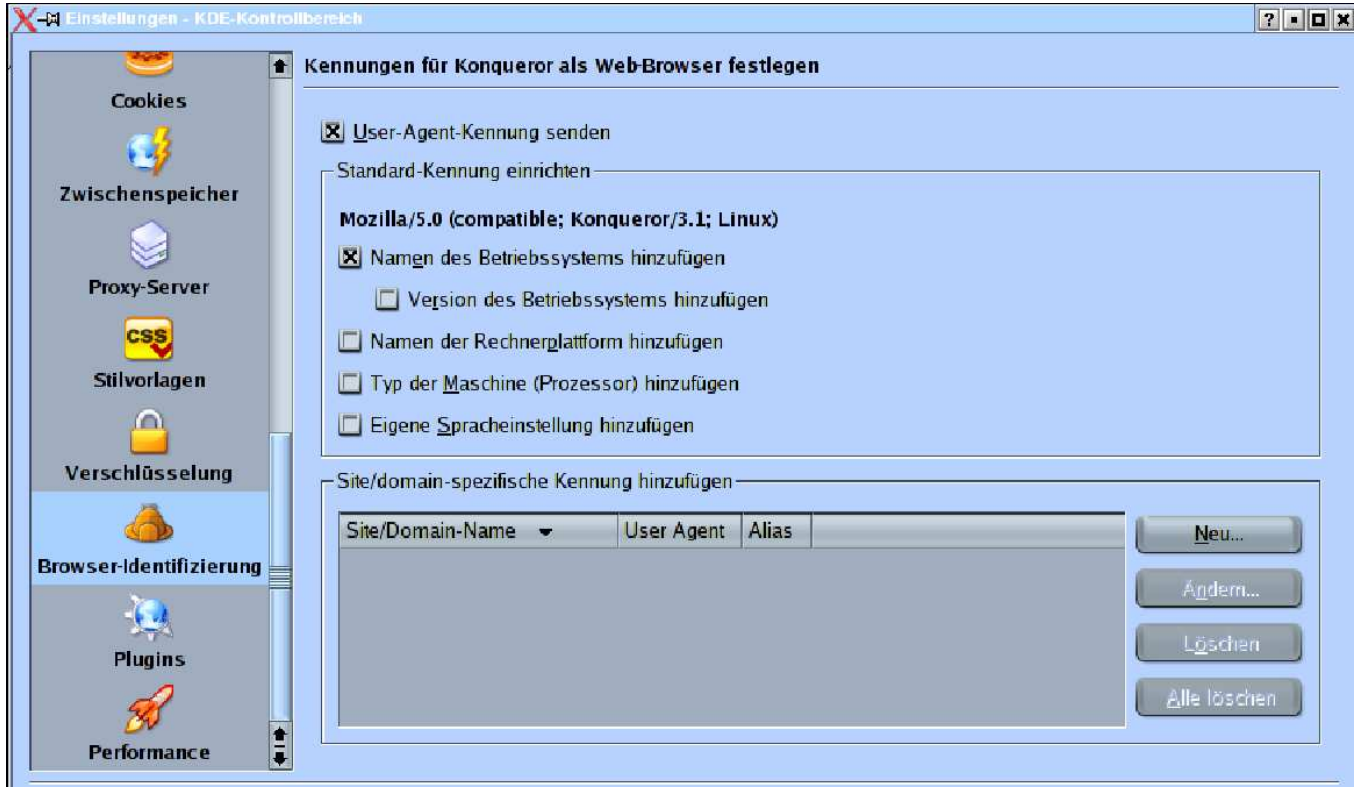
EFF: Promise and Risk

- 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. ”

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.

CFP 23.4.2004

- 23.04.2004
- Conference:

Computers, Freedom & Privacy

Heise Ticker:
Trusted Computing als Paradies für Spyware?

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

Golem interviewed IBM

- Golem.de

  dyn1.golem.de/cgi-bin/usisapi.dll/forprint?id=28464

  Interview: Trusted Computing - Problem oder Notwendigkeit?
  TC - Trusted-, Trustworthy- oder doch eher Treacherous-Computing?

- Herr S.,
  ThinkVantage Consultant bei IBM für Europa, den Mittleren Osten und Afrika

Remote Attestation?

- **Golem.de :** Ein weiterer zentraler Kritikpunkt an TCG ist die vorgesehene "Remote Attestation", da diese auch die Möglichkeiten des Nutzers einschränkt, das eigene System bewusst zu modifizieren.

Owner Override?

- [Golem.de] Die Electronic Frontier Foundation schlägt in dieser Hinsicht beispielsweise mit Owner Override ein Konstrukt vor, das genau diese Problematik umgehen soll. Inwiefern haben solche Vorschläge eine Chance, im Rahmen der TCG umgesetzt zu werden?

IBM zu Owner Override

- **Herr S., IBM**: Der Owner hat die freie Wahl, ob das TPM überhaupt aktiviert wird. Die Spezifikationen der TCG sehen keinen Owner Override im von der EFF beschriebenen Sinne vor, da dieser Owner Override negative Konsequenzen für den Endanwender hat.

Seltsame Banken??

- [**Herr S., IBM**] Die Überprüfung eines Bankrechners wäre zum Beispiel nicht mehr möglich und der Benutzer müsste wieder auf blindes Vertrauen zurückgreifen. Dementsprechend ist die Frage des Owner Override kein Diskussionspunkt in der TCG.

Wie bitte???

- **Golem.de:** Welche negativen Konsequenzen könnten dies konkret sein? Inwiefern wäre die Überprüfung eines Bankrechners nicht mehr möglich?

Ganz Seltsame Banken!!!

- **Herr S., IBM:** Ein Owner Override könnte der Bank ermöglichen, ein fehlerhaftes System als korrekt zu attestieren. Somit kann ein Benutzer während der Transaktion nicht sicher feststellen, ob die Bank wirklich korrekt ist oder ob sie den Owner Override verwendet hat.

Useful Things

- TPM $\approx$ Hardwired Smart Card
- First realizations: LPC Bus
- Secure Storage for Cryptographic Key
- Secure Booting

Owner Controled Trusted Enviroment

- Own Endorsment Key
  - Owner Controled Trusted Infrastructure
  - On Chip Key Generation
  - Credidals

Identity Management

- DAA
- Pseudonymity Control

Cryptolabs Smart Card Stuff

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

Portation blockated by patent problems.

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.

Resistance helps

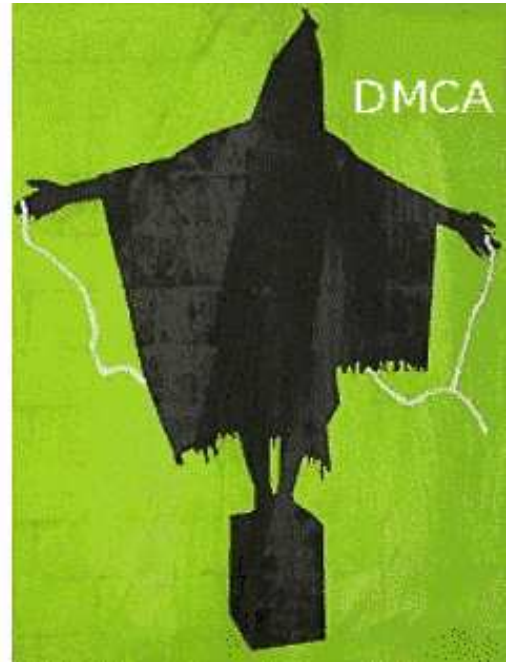
- Intel has redrawn the plans for a **Processor-ID** because of the user resistance.
- TCG1.2 has fixed *some* problems.
- 'We are important customers!'
- Fight Digital Restrictions Management!

The OS War is over

- Windows means slavery.
- Apple is a company under US Law.

"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!**

Acknowledgments

Produced with Free Software under GNU/Linux.

”Licht ins Dunkel”,Spiegel Online 08/03

Big thanks to:

Rop Gonggrijp, Carla, Lucky Green, Ross Anderson, Volker Grassmuck

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