# Ist trusted computing wirklich vertrauenswürdig?

## *Konzeptionelle Schwächen und Risiken*

Ruediger Weis

cryptolabs Amsterdam &
Computer Systems Group, Vrije Universiteit Amsterdam
(Old Europe)



# Outline

- TCPA und Palladium
- Kryptographische Probleme
  - Schlüssel Management
  - Verdeckte Kanäle
  - Backdoor Problematik
- Gefährdung der Wissensgesellschaft
- Konsequenzen

# Rücktritte und Namensänderungen

- 18.01.2003:
  **Richard Purcell**, oberster Datenschutzbeauftragte von Microsoft, tritt zurück.
- 21.01.2003:
  **Palladium** heisst jetzt: NGSCB und der **Fritz-Chip** SSC.
- 08.04.2003:
  **Trusted Computing Group** gründet sich.
- 22.04.2003:
  **Howard Schmidt** , ehemalige Chef für Produktsicherheit bei Microsoft, tritt als Berater der US-Regierung für Netzsicherheit zurück.



# 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

# Schon in der Praxis

"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



# Fussnote: 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 alternative Betriebssysteme wie GNU/Linux.

- "I expect TCPA to become irrelevant, since Microsoft is a monopoly player in the OS market"

Bruce Schneier, CEO counterpane [a]

[a] Autor des Standarwerkes: “Applied Cryptography”



# Trusted Computing Platform Alliance

Die TCPA wurde 1999 gründet von Intel, Microsoft, HP, Compaq und IBM. Die Liste der Mitglieder war lange Zeit *nicht* öffentlich.

- Momentan sehen viele Experten *Auflösungserscheinungen*.
- Microsoft Q& A, Februar 203:
  - **Q:** Is NGSCB (Palladium - RW) base Microsoft’s implementation of the Trusted Computing Platform Alliance (TCPA) specification?
  - **A:** No, the next-generation secure computing base is not an implementation of the TCPA spec. . . .

# TCPA Übersicht

Ermöglicht Fremdkontrolle über den persönlichen Computer

> *"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 2003.

($\approx$ Nobelpreis für Informatik)



# Keymanagement

- **Endorsement Key**:
  Eindeutiger RSA Schlüssel erzeugt vom **Hersteller.**
  Gefahr der Aufzeichnung!!!
  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" .

# 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 von Ron Rivest.
- Erste SHA Version bot nicht die erwartete Sicherheit.
- Änderung ohne genaue Begründung.
- Wir ahnen inzwischen warum.

# 160 bit Hash ist nicht mehr zeitgenäss

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 Microsoft 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.
- In mehreren Windows-Versionen wurde ein zusätzlicher kryptographischer Schlüssel mit dem schönen Namen `nsa_key` [a] gefunden. Es wurden hierzu verschiedene widersprüchliche und zum Teil schwerlich nachzuvollziehbare Erklärungen abgegeben.

[a] NSA=National Security Agency, US Geheimdienst, www.nsa.gov

# Meinung Führender Cryptographen

Stamtements von der RSA Conference, San Francisco, April 2003.

**Whitfield Diffie** [a]

- ”(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”**

[a]Whitfield Diffie ist einer der Entdecker der Public-Key Cryptographie.



# Turing-Preisträger Ron Rivest

**Prof. Ron Rivest** [a]

- ”We should be watching this to make sure there are the proper levels of support we really do want”
- ”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."
- ”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.”

[a]Ron Rivest ist unter anderem auch bekannt als einer der Autoren des RSA Algorithmus und der Designer der MD4-Hash-Funktionen Famile.

# Trusted Plattform Module (TPM)

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



# Black Box Crypto

*Verdeckte Kanäle leicht zu implementieren.*

Sogar beweisbar sicher:

- 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" herrauszuschmuggeln.
- Selbst eine Hardwareanalyse kann nicht aufdecken, welche Informationen durchgesickert wurden.



# Sophisticated Bit Smuggeling

**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

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

# Sophisticated Bit Smuggeling 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
$$p = \bigoplus_{1 \le i \le m} z_i y_i$$
- 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 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.



# Hardware Analyse

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

# Weitere Manipulationsmöglichkeiten

- Zufallszahlenquelle
- Schlüsselerzeugung
- . . .



# Q& A von Microsoft zu 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" ...

# 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?



# Q& A von Microsoft zu Lawful Interseption

- **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. . . .

Bedeutet dies, dass:

- die Crypto-Chips durch Hardwareanalyse leicht zu brechen sind?
- US Sicherheitsbehörden sich Zugriff zu Computerhardware im Ausland [a] erzwingen?

[a] Zumindestens in Schurkenstaaten, wie Lybien, Kuba und Deutschland.

# GNU/Linux und TCPA

- Mindestens zwei Firmen arbeiten einer ”TCPA-enhanced” version von GNU/Linux.
- Nach einer kostspieligen Evaluation wird *eine* Version unterzeichnet.
- Dieses 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’led software can be hijacked for commercial purposes, idealistic young programmers will be much less motivated to write free software.”

Ross Anderson



# Niemals mit Open-Source kompatibel

Peter N. Biddle, Microsoft, 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.”

# Q& A Microsoft zu konkurrierenden BS

- 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.



# Interoperabilität

- XML Office Initiative.
- MS blockiert.
- Palladium Container behindern Datenaustausch.

Wissensverlust droht.

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

Steven Levy, MSNBC/Newsweek
Gut für betrügerische Unternehmen,

schlecht für die Wissensgesellschaft.

# Conclusion

- Offene Netzte haben eine Wissensexploxion ausgelöst.
- TCPA bedoht die Wissensgesellschaft.
- Archivierung von Wissen wird schwierig bis unmöglich.
- Es drohen zwei Welten zu entstehen, welche Schwierigkeiten haben werden Informationen auszutauschen.
- Die Fremdkontrolle von kryptographischen Schlüsseln, welche eine gewichtige Rolle in der zukünftigen IT Infrastruktur spielen, durch eine privatwirtschaftliche Firma, welche unter der Rechtsaufsicht einer ausländischen Regierung stehen, bringt auch interessante wirtschaftspolitische und juristische Fragestellungen mit sich.



# 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 Programmkomittee-Mailingliste USENIX/CARDIS2002



# Kontakt

Dr. rer. nat. Ruediger Weis,
Diplom-Mathematiker
cryptolabs Amsterdam

- ruedi@cryptolabs.org
- www.cryptolabs.org


Folieb erhältlich unter: http://cryptolabs.org/tcpa

Produced with Free Software under GNU/Linux. Typesettig: LaTeX.

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