”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

TCG
Die ‚Trusted Computing Group' misstraut ihren Kunden – ohne Kontrolle des Benutzers soll ein Cryptochip in vielen elektronischen Geräten verhindern, dass dieser bestimmte Funktionen ausführt. Die in Silizium gegossene orwellsche Vision eines entmündigten Rechtekonsumenten, der nur mit digitalem Offenbarungseid weiter konsumieren darf.

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”**

’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**

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.”

’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.
(≈ Nobel Price for Computer Science)

Enforcement

- ”Microsoft Lizenzen lächerlich”?
- Enforcement by
  - TPM Chip
  - DMCA
- Forced ’updates’

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.

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`

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."

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.

New in TCG 1.2

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

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

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

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.

Angenehmes Abhören

Bemerkenswert ist, dass nur

- eine kleine Anzahl
- von zeitlich nicht notwendigerweise zusammenhängenden Ciphertexten
- passiv abgehört

werden muss.

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

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

- und nutzte

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

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...

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.

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" ...

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.

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.

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."

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!

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`

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?

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.