Grobe Skizzierungen

Sicherheitstechnische Forderungen

an TCG* und Palladium*

Andy Müller-Maguhn,

andy@ccc.de

Symposium "Trusted Computering Group"

Berlin, 3. Juli 2003

(A)ll rights reversed. Reprint what you like.

* oder wie das diese Woche auch immer genannt wird

Forderung 1: Kontrolle des Anwenders über die Schlüssel

- Vollständige Kontrolle des Anwenders über sämtliche gespeicherten Schlüssel
  - Sicherheit bei externer Generierung, möglicher Verwahrung und zumindest partieller Verwaltung (CA) fragwürdig
  - Gefahr der Fremdkontrolle über die Schlüssel = Gefahr der Fremdkontrolle über den Rechner
  - Schlüsselkontrolle durch den Anwender verhindert nicht zwangsläufig Mißbrauch, aber spezifische Mißbrauchsoptionen
  - Schlüsselkontrolle durch den Anwender entlastet somit auch die TCG vom Verdacht, Mißbrauchspotentiale zu schaffen
  - Vollständige Schlüsselkontrolle heißt deswegen vollständig, weil damit auch der Endorsement Key des TPM gemeint ist

"The right way to look at this is you are putting a virtual set-top box inside your PC.

You are esentially renting out part of your PC to people you may not trust."

Prof. Ron Rivest [1]

(A)ll rights reversed. Reprint what you like.

[1] http://theory.lcs.mit.edu/~rivest/

Forderung 2: Ausschluss von verborgenen Kanälen

- Sicherstellen, dass keine verborgenen Kanäle existieren, über die geheime Schlüssel des Anwenders übertragen werden.
  - Gefahr der Übertragung (des Leakens) besteht sowohl bei Erzeugung, als auch bei der anschließenden "sicheren" Verwahrung
  - TCG gesteht ein: "Es ist natürlich nicht völlig auszuschließen, dass ein Chip-Hersteller ein TMP mit Funktionen baut, die von der Spezifikation abweichen und einen Zugriff auf gespeicherte Schlüssel erlauben."
  - Zertifizierung wirft Fragen nach Verfahren, Transparenz und Überprüfbarkeit auf (um nicht zu sagen: vertrauenswürdigkeit)
  - TPM sind ausdrücklich **nicht** vor Hardwareangriffen geschützt, d.h. zerstörungsfreies Auslesen ist technisch möglich
  - Kontrollierbarkeit sinkt mit steigender Komplexität, d.h. bei Integration des TPM in den Prozessor steigt Potential nicht erkannter Probleme

(A)ll rights reversed. Reprint what you like.

Forderung 3: Übertragbarkeit der Schlüssel

- Übertragung der Schlüssel auf einen anderen Rechner muss ermöglicht werden.
  - Beugt Mißbrauchspotentialen im Bezug auf Lizensierungspraktiken vor.
  - Stellt Anwenderautonomie im Bezug auf Kontrolle über Hardware (auch Ausfallsicherheit) sicher

"I say you need to hold the keys to your own computer."

Whitfield Diffie [2]

(A)ll rights reversed. Reprint what you like.

[2] http://research.sun.com/people/diffie/

Forderung 4: Transparenz über die Zertifizierung

- Vollständige Transparenz über die Zertifizierungs-Mechanismen
  - Vollständig heißt nicht nur Benennung der Zertifikate, sondern auch der Mechanismen und untauschbarkeit des geprüften Codes
  - Derzeitige Zertifizierung rein konzeptionell, weder Zertifizierung der TMP noch CA derzeit noch nicht geklärt
    Zitat TCG: "Die TCG hat keine Pläne, selber eine Zertifizierung der TPMs durchzuführen"
  - Zitat: TCG:"Ein Missbrauch der TCPA-Spezifikationen oder die Modifikation des Designs kann daher von Seiten der TCG nicht endgültig ausgeschlossen werden. Darüber hinaus können die Spezifikationen nicht verhindern, dass ein Betriebssystem oder eine Applikation die Zertifizierung von Software verlangt. Es ist nicht das Ziel der TCG, die Rechte der Nutzer oder die Freiheit der Anwendungsprogrammierer zu beschränken."
    - Vielleicht ist es nicht Ziel der TCG, vielleicht es aber Ziel von einzelnden Mitgliedern der TCG
  - Zitat TCG: "Die TCPA-Spezifikationen sehen nicht vor, irgendwelche Software zu zertifizieren oder in der Lauffähigkeit einzuschränken. Ein derartiger Schritt würde eine sehr viel weiterreichende Sicherheitslösung unter Einbezug des Betriebssystems erfordern."

Sicherheit ist die Sicherheit des schwächsten Punktes.

(A)ll rights reversed. Reprint what you like.

Weitere Informationen

http://www.ccc.de/

http://www.ccc.de/digital-rights/

mail@ccc.de

(A)ll rights reversed. Reprint what you like.