# Trusted Computing

## Teil 2: Chancen und Risiken

# Übersicht

1. Das Herzstück (TPM)
2. TC und OpenSourceSoftware
3. TC = Digital Rights Management ?
4. Zum Thema „Trust“
5. Ausblick

# 1 Das Herzstück (TPM) (1/2)

„Ein PC, der sicher sein soll vor fremden Manipulationsversuchen, vor bösartigen Virenattacken und heimlichen Ausspähmanövern; ein PC, dem der Nutzer endlich vertrauen kann.“

# 1 Das Herzstück (TPM) (2/2)

- TPM ist passives Bauelement
- Enthält Schlüssel, sicheren Speicherbereich, kryptographische Funktionen,…
- Betriebssystem entscheidet über Reaktionen auf Parameter, die das TPM zurückliefert.
- Schlüssel zum Schutz sensitiver Daten (SRK)
- Schlüssel zur Authentifikation im Netzwerk (EK)
- Schlüssel zur Anonymisierung (AIK)

# 2 TC und OSS

- TCG-Standard offen und betriebssystem-unabhängig
- Zugang zu TCG teuer, daher Benachteiligung kleinerer Unternehmen und OSS-Entwickler
- MS gibt keine Einsicht in Schnittstellen zu TPM, entwickelt eigene Standards, die andere übernehmen müssen
- Transparenz erwünscht

# 3 TC = Digital Rights Management?

„Die Innovation von TCG besteht darin, nun auch externen Parteien die Durchsetzung ihrer Nutzungsbedingungen auf den Rechnern ihrer Transaktionspartner zu ermöglichen.“

# 3 TC = Digital Rights Management?

- DRM gilt als anwenderunfreundlich, Kritiker sprechen von der Entmündigung des Verbrauchers und dem Verzicht auf die informationelle Selbstbestimmung.
- MS hält Patente auf DRM-Betriebssysteme, die nicht unbedingt etwas mit TC zu tun haben müssen ;)
- Inhalte können an Systemzustände gekoppelt werden und dadurch unveränderbar werden
- Komplettes DRM-System braucht zusätzlich DRM-BIOS und erweitertes DRM-TPM
- Sukzessive Einführung sehr wahrscheinlich

# 4 Zum Thema „Trust“ (1/2)

“Trusted Computing has a tiny problem:
trust.

A lot of users don`t want to trust it.”

# 4 Zum Thema „Trust“ (2/2)

- Trustworthy = Verhalten wie erwartet
- Wer vertraut wem?
- Inhalteanbieter und Softwareindustrie erlangen Zugang zum PC
- Kontrolle wird dem Benutzer teilweise entzogen
- Für Firmennetzwerke (B2B) vorteilhaft
- TPM deaktivierbar, Computer wird in 2 Bereiche unterteilt

# 5 Ausblick (1/3)

„Es ist, als seien unsere Gebete erhört worden. Nun wird es Zeit, sich über die Kosten zu unterhalten.“

# 5 Ausblick (2/3)

Risiken

- DRM
- Ausbau von Monopolstellungen
- Freie Meinungsäußerung und informationelle Selbstbestimmung ?
- Zensur
- Stellung der ACs

# 5 Ausblick (3/3)

Chancen

- Neue Stufe der IT-Sicherheit
- Neue Absatzmärkte
- B2B und B2C

Liste von bisher ausgelieferten TPM-Plattformen

http://www.tonymcfadden.net/tpmvendors.htm