Trusted Computing:

(Un)sicherheit für PC-Anwender?

Prof. Dr.–Ing. Damian Weber

Hochschule für Technik und Wirtschaft des Saarlandes

dweber@htw-saarland.de

http://www-crypto.htw-saarland.de/weber/

Hochschule für Technik und Wirtschaft, Saarbrücken

≈ 3000 Studierende, 110 Professoren

- Fachbereiche
  - Architektur
  - Bauingenieurwesen
  - Betriebswirtschaft
  - Elektrotechnik
  - Grundlagen/**Informatik**/Sensortechnik
  - Maschinenbau
  - Wirtschaftsingenieurwesen
- neue Studiengänge (Bachelor/Master)
  - **Kommunikationsinformatik** (B/M)
  - Internationale Betriebswirtschaft (B)
  - Maschinenbau (B)

Inhalte

1. Problematik
2. Untrusted Computing
3. Trusted Computing
   - Trusted Computing Group
   - Motivation
   - Technik
4. Plädoyer für freie Software

Was ist das Problem?

Bauen eines ,,sicheren" PCs.

Mit einem ,,sicheren" Betriebssystem.

Mit ,,sicheren" Applikationen.

Was bedeutet „sicher”?

Zuverlässigkeit: Mein PC funktioniert wie erwartet, trotz ...

- „zufälliger” Fehler (kaputte Festplatte $\rightsquigarrow$ Backup)
- gelegentlicher Softwarefehler (Applikation, Betriebssystem)
- provozierter Fehler (Attacken durch Hacker)

Für Netzwerke

- Vertraulichkeit
- Integrität
- Authentisierung

$\rightsquigarrow$ **Secure Computing** ist das, was wir brauchen ...

Wo ist das Problem?

Das PC–Design existiert seit $\approx$ 20 Jahren.

Mittlerweile müßte das Problem doch erledigt sein, oder?

PC–Sicherheit – neuere Sicherheitslücken

10.11.2003 Eudora Mailclient Version <6.0 Pufferüberlauf
21.10.2003 Internet Explorer: Liste von Sicherheitslücken
20.10.2003 JAVA Applets verletzen Sandbox-Restriktionen
16.10.2003 Windows Messenger Service Pufferüberlauf
15.10.2003 MS Exchange Server 2000 Pufferüberlauf
13.10.2003 FTP Server ProFTPd 1.2.7 - 1.2.9rc2 Pufferüberlauf
10.10.2003 Xsco OpenServer 5.0.7 Pufferüberlauf
01.10.2003 OpenSSL <0.9.7c, 0.9.6k Memory errors
18.09.2003 sendmail < 8.12.10 Pufferüberlauf
30.08.2003 Diverse Schwächen in SAP Transaction Server
28.08.2003 PAM SMB (Linux+WinNT Authentication): Pufferüberlauf
18.08.2003 P2P-Netzwerke basierend auf emule,lmule,xmule
11.08.2003 MSBLAST (Lovsan) Wurm basierend auf RPC-Lücke vom 20.07.
04.08.2003 Solaris dynamic linker Pufferüberlauf
31.07.2003 FTP Server wu-ftpd Pufferüberlauf
20.07.2003 Win2K RPC DCOM Denial of Service+Privileges, Port 135
09.07.2003 Acrobat Reader Verifikation signierter Plug-ins fehlerhaft
01.07.2003 Acrobat Reader bis V5.0.7 Pufferüberlauf

Warum existiert das Problem?

Komplexität von Systemen

- PC–Hardware
- Betriebssystem
- Applikationen
- Systeme interagieren

Internet Explorer + Outlook + EXE Attachments = Desaster

Beweis für die Korrektheit von Programmen schwierig!

- Windows 2000: $\approx$ 40 Mio Zeilen Code
- Linux 2.4.21: $\approx$ 3.5 Mio Zeilen Code

Untrusted Computing

Wem vertrauen wir bisher?

- Hardware
- BIOS
- Testlabors
- Betriebssystem
- Applikationen
- Compiler

The Untrusted User

. . . warum bisherige Kopierschutzmaßnahmen nicht ausreichen . . .

Maßnahme	Gegenmaßnahme
ändere Playerprogramm	System erzwingt Schreibschutz
füge Festplatte zu anderem System	verschlüssele Programm
finde Schlüssel (Debugger)	**Hardware unterbindet Debugging**

. . . Angriff auf die Hardware . . .

Maßnahme	Gegenmaßnahme
kopiere Datenstrom von Boxen	**Hardware verschlüsselt Datenstrom**

⇝Hardware–Erweiterung **TPM = Trusted Platform Module = nexus**

The Untrusted User – The Enemy

This is a new focus for the security community, [. . .]

The actual user of the PC

– someone who can do anything they want –

is the enemy.

David Aucsmith, security architect for Intel

Einschränkung durch Paragraphen

Microsoft End User License Agreement (Windows XP)

- you may *need to reactivate the Product*
- you may not *reverse engineer, decompile, or disassemble*
- you *acknowledge and agree that MS may* **automatically check** *the version of the Product and/or its components*
- you acknowledge and agree to upgrades or fixes *that will be* **automatically downloaded** *to your Workstation Computer*
- updates may *affect your ability to copy, display and/or play* content *through MS software that utilize DRM*
- you agree that MS *may collect and use technical information gathered in any manner*

Eine gute Idee...

Programmcode wird elektronisch unterschrieben

vor der Ausführung wird die Unterschrift geprüft

Verschlüsselte Dateien

[existiert schon: BSD UNIX, CryptFS]

...heimtückisch realisiert

PC–Besitzer hat keinen Zugriff auf eigenen Schlüssel

die Unterschrift wird durch Dritte[1] geprüft

⇝etablierte Konzerne können auf technischem Wege

- den Anwender an die Applikation fesseln
  Customer Lock–In
- kleine Softwarehäuser verdrängen
- freie Software unbrauchbar machen

[1] Content Anbieter, Softwarelieferanten

Trusted?

Trusted heißt, der Computer kann seine eigene Integrität beweisen.

Trusted heißt, der Content–Provider vertraut meinem Computer.

Merke:

es heißt *Trusted Computing* und nicht *Secure Computing*.

aber: Aktivierung von TC ist optional (can we trust the TCG?)

Einschränkung durch Technik

Trusted Computing Group TCG:

Microsoft, Intel, IBM, HP, AMD ...

TCPA: Trusted Computing Platform Alliance (Hardware)

Palladium: Windows–Unterstützung für TCPA–Features (Software)

TCPA$\rightsquigarrow$TCG

Palladium$\rightsquigarrow$NGSCB

trusted computing : IBM, ursprünglicher Oberbegriff

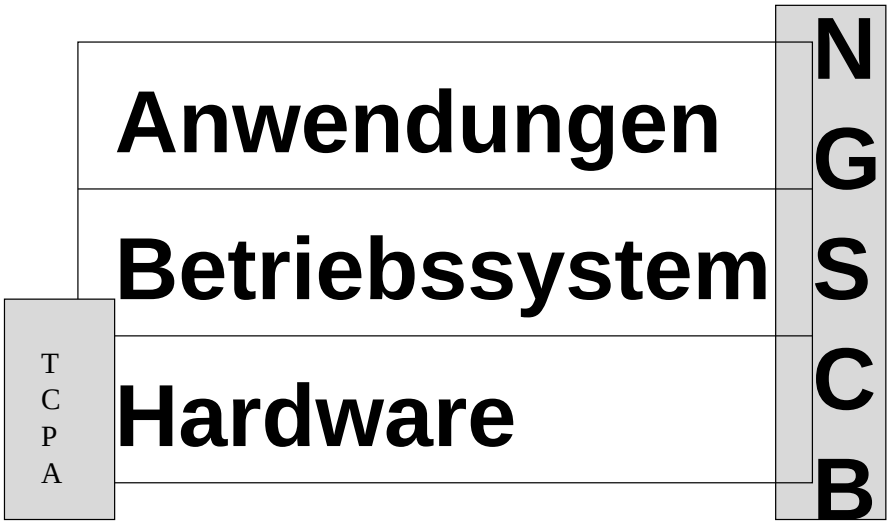
trustworthy computing: Microsoft

treacherous computing: Free Software Foundation

NGSCB

Next Generation Secure Computing Base (Palladium)

The Mickey Mouse Operating System. [Alan Cox].



Motivation

Intel/AMD:

- Home Entertainment Markt $\rightsquigarrow$Digital Rights Mgmt $\rightsquigarrow$PC

Microsoft:

- Raubkopien
- Geschäftsmodell: befristete Lizenzen
- Digital Rights Mgmt Applikationen (Musik, Filme,...)
- Erhöhung der Migrationskosten ($\longleftarrow$ Customer Lock–In)
  - verschlüsselte Dateien
  - Erlaubnis der Urheber von Dateien

Wert einer Software = Kosten der Migration zur Konkurrenz

Motivation

We came at this thinking about music,

but then we realized

that e-mail and documents

were far more interesting domains...

Bill Gates

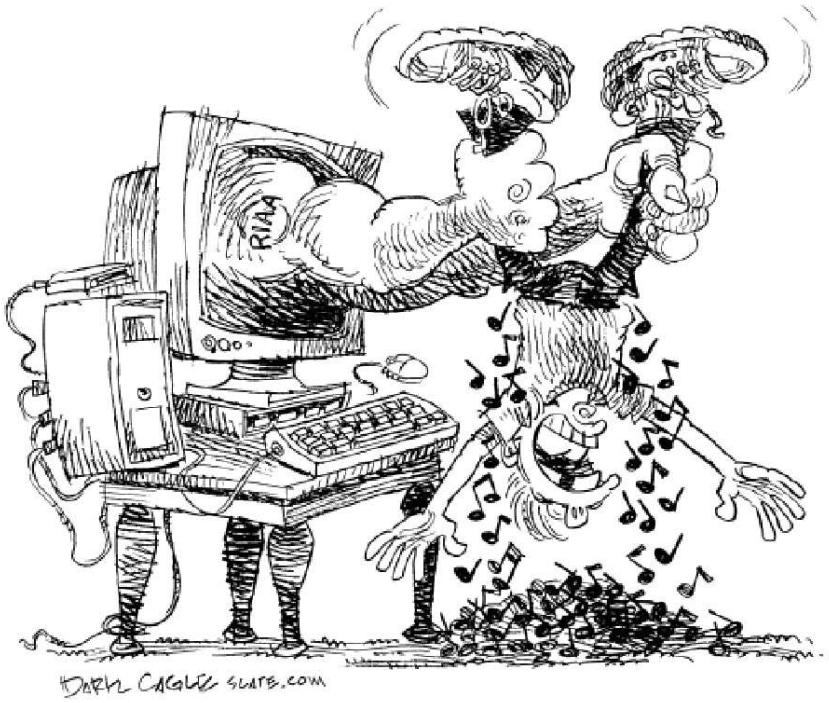
Remote Attestation

Vision des Digital Rights Management

- Server: Windows Rights Management Services
- PC: Windows Rights Management Client
- WWW: Rights Management Plug–In for Internet Explorer
- CDs, DVD–Filme, MP3: Windows Media DRM
- Office: Information Rights Management
  (Word, Excel, PowerPoint Outlook)

Digital ,,Restriction" Management

Kontrolle von Musik



Kontrolle von Dokumenten

Konfiguration kann ...

- Ablaufdatum setzen
- Drucken verbieten
- Leseberechtigung erteilen
- diese Rechte nachträglich verändern (Online–Kontrolle)

Mögliche Anwendungsszenarien:

- Tony Blair's Irak Dossier
- Fishman Affidavit (Scientology)
- Kriminelle Vereinigungen

Konsequenzen für journalistische Recherchen?

Trusted Computing und Integrität

Vertrauen ist gut, Kontrolle ist besser?

- **Hardware**
- **BIOS**
- Testlabors
- **Betriebssystem**
- **Applikationen**
- **Compiler**

$\rightsquigarrow$*Kontrolle des Zustands*

Trusted Computing stellt **Originalzustand** sicher. Eventuell.

Der Originalzustand ist per ,,Fernbedienung" überprüfbar.

Achtung: kein Beweis für eine fehlerfreie Applikation

Technische Umsetzung

Hardware Baustein: TPM = Trusted Platform Module

1. Prüfe Echtheit der Startkonfiguration
   - BIOS
   - optionale ROM–Bausteine
   - Bootsektor
   - DRM boot loader
   - DRM Modul
2. Lade Betriebssystem
   - Entschlüssele Betriebssystem
   - Lade Betriebssystem
3. Betriebssystem überprüft
   - HCL Hardware Check List
   - SRL Serial Number Revocation List

$\rightsquigarrow$**Daten werden an eine Plattform gebunden**

Bereits realisierte Systeme

IBM Thinkpad mit TCPA–Chip

BIOS

- American Megatrends Inc AMIBIOS8
- Transmeta TM5800

Anm.: NGSCB nicht vor 2005, API Anfang Nov. 2003 vorgestellt

Free Software

Eigenschaften:

- Kopieren
- Verteilen
- Öffentliches Review
- Erweitern, Verändern, Verbessern aktueller Versionen

Einschränkung dieser Aspekte ...

- Wissenschaft betroffen
- *freie Software* betroffen:
  - Linux, FreeBSD
  - Openoffice
  - OpenSSL

Copyleft–Lizenz

Grundsatz: Frei verfügbare Software bleibt frei auf Dauer.

GNU Public License

Copyleft anstatt Copyright

Source Code vorhanden – **Open Source**

- darf weitergegeben werden
- darf modifiziert werden
- meist kostenlos

Untrusted Computing und Open Source

Vertrauen ist gut, Kontrolle ist besser!

- Hardware
- **BIOS:** `www.linuxbios.org`
- Testlabors
- **Betriebssystem:** `www.kernel.org, www.freebsd.org`
- **Applikationen:** `www.sourceforge.net`
- **Compiler:** `www.gnu.org`

$\rightsquigarrow$*Kontrolle über Implementierung*

Trusted Computing und Open Source

Q: *Could Linux, FreeBSD or another open source operating system 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 NGSCB 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.

[Microsoft NGSCB FAQ]