



## *„Wenn mein Aldi-PC zum Spion wird“*

*TCPA, Palladium, Digital Rights Management (DRM), DMCA, LaGrande usw. hört man in letzter Zeit immer öfter im Computerbereich. Doch was wirklich dahinter steckt, weiss kaum jemand. Zukünftig könnte die Industrie durch einen eingebauten Chip Computer kontrollieren.*

Chaos Computer Club Düsseldorf /  
Chaosdorf e.V. <[mail@chaosdorf.de](mailto:mail@chaosdorf.de)>

8. April 2003



# *Denkbare Probleme des Status Quo und bestehende Lösungsansätze*

## *Hardware*

gefälschte oder fehlerhafte Hardware

## *Betriebssystem*

mangelnde Rechteverwaltung → Verwendung eines OS mit  
Rechteverwaltung

Hintertüren → Verwendung eines vertrauenswürdigen OS

nicht eingebaute Verschlüsselung → Verwendung von  
Verschlüsselungssoftware (z.B. fuer verschlüsselte Dateisysteme)

nicht lizenziert → Freie Software, Erwerb einer Lizenz evtl. mit  
Seriennummer, Hologramm



## *Anwendungen*

Ausführen nicht gewünschter Aktionen, Viren, Ausspionieren des Anwenders

→ Verwendung vertrauenswürdiger Anwendungen, Überprüfen der Konfiguration, Virens Scanner

Sicherheitslücken, Hintertüren → Verwendung vertrauenswürdiger Anwendungen, Überprüfen der Konfiguration, Update bei Bekanntwerden von Sicherheitslücken

nicht lizenziert → Freie Software, Erwerb einer Lizenz evtl. mit Seriennummer, Hologramm, Dongle

## *Daten*

illegal, nicht lizenziert → Sicherstellung der Legalität

Spam → Spam-Filter, Verwendung unterschiedlicher E-Mail-Adressen



## *Über TCPA*

- ▷ Trusted Computing Platform Alliance
- ▷ Oktober 1999 von Compaq, HP, Intel, IBM und Microsoft gegründet
- ▷ mittlerweile über 200 Mitglieder, fast alle namhaften Hardware-Hersteller
- ▷ Microsoft: „Verbesserung der Vertrauenswürdigkeit und Sicherheit von Computer-Plattformen“
- ▷ Standardisierungsgremium für Hard- und Software



## *Mögliches Szenario für zukünftige Systeme*

### *Hardware*

- ▷ TPM-Chip (Trusted Platform Module), Fritz-Chip
  - eigenständiger Chip auf dem Mainboard, integriert im Chipsatz, integriert in CPU
  
- ▷ TPM-Chip kontrolliert Bootvorgang
  - Überprüfung des BIOS → BIOS übernimmt Kontrolle → TPM-Chip kontrolliert Status
  - Überprüfung sämtlicher Software-Komponenten, die zum Starten des OS notwendig sind → TCGA-konformes OS übernimmt Kontrolle
  - eine Überprüfung schlägt fehl → verlassen des trusted Modus → kein Zugriff auf TCGA-OS, TCGA-Anwendungen, TCGA-Daten etc.



## *Betriebssystem*

- ▷ Palladium, vor kurzem umbenannt in “next-generation secure computing base for Windows”
- ▷ Palladium ist das Gegenstück zu TCPA in Software spezifiziert, wie Anwendungen und Daten TCPA-konform geschützt werden können
- ▷ Nexus wird Teil eines neuen Windows-OS sein und verwaltet Zugriffe von “Palladium enhanced“-Anwendungen auf geschützte Daten
- ▷ Nexus gewährt oder verweigert Anwendungen den Zugriff nach Prüfung von Zertifikaten und kommuniziert dafür mit dem TPM
- ▷ Nexus isoliert Anwendungen voneinander aber ermöglicht einen parallelen Betrieb von trusted- und non-trusted-Anwendungen
- ▷ non-trusted-Anwendungen dürfen niemals auf trusted-Daten zugreifen



## *Anwendungen*

- ▷ Anwendungen müssen mit einem “trusted agent” ausgestattet werden, um auf geschützte Daten zugreifen zu können
- ▷ der “trusted agent” kommuniziert mit Nexus, welches letztendlich den Zugriff gestattet oder verweigert
- ▷ bestehende Anwendungen ohne “trusted agent” können weiterhin ausgeführt werden, aber keinen Zugriff auf geschützte Daten erlangen

## *Daten*

- ▷ Daten können durch Verschlüsselung vor unberechtigtem Zugriff geschützt werden
- ▷ Daten können durch Signaturen vor unberechtigten Änderungen geschützt werden



- ▷ Daten können mit einem “Verfallsdatum” versehen werden; danach verweigert die “Palladium enhanced”-Anwendung das Verwenden der Daten
- ▷ “Palladium enhanced”-Anwendungen können nach Abgleich mit Blacklists von zentralen Servern den Zugang zu bestimmten Daten verhindern
- ▷ Daten können benutzerbezogen freigeschaltet werden



## Probleme

- ▷ Sicherheit nicht für den Anwender, sondern Sicherheit vor dem Anwender
- ▷ Zertifizierungs-Mechanismen völlig unklar <sup>a</sup>
- ▷ unbequeme Dokumente können gezielt unlesbar gemacht werden
- ▷ DoS-Angriffe auf die zentralen Server können wichtige Rechner praktisch unbrauchbar machen (NTP-Server, Blacklist-Server) <sup>b</sup>
- ▷ zukünftiger Status von alternativen Betriebssystemen und Anwendungen unklar (zertifiziertes Linux, Freie Software)
- ▷ TPM defekt, Daten weg? <sup>c</sup>

---

<sup>a</sup>Kosten, wer, wann

<sup>b</sup>muss jeder Rechner online sein?

<sup>c</sup>Export von Schlüsseln



- ▷ eindeutige Zuordnung Hardware ↔ Anwender und Hardware ↔ Daten <sup>d</sup>
- ▷ versehentlich zertifizierter Virus/Backdoor <sup>e</sup>
- ▷ Schutz des Monopols und der kommerziellen Interessen statt den Bedürfnissen der Anwender
- ▷ Einsatz von TCPA/Palladium gesetzlich verpflichtend <sup>f</sup>
- ▷ einmal geschaffene Möglichkeiten können leicht missbraucht werden <sup>g</sup>

---

<sup>d</sup> nachvollziehbar, wer welche Daten wo veröffentlicht hat

<sup>e</sup> Code-Audit kaum möglich

<sup>f</sup> erste Bestrebungen in den USA

<sup>g</sup> Telekommunikations-Überwachung



## *Forderungen des CCC zu TCPA*



An IBM anlässlich der CeBIT am 18. März 2003 überreichte Forderungen:

1. Vollständige Kontrolle des Anwenders über sämtliche gespeicherten Schlüssel
2. Sicherstellung, dass keine verborgenen Kanäle existieren, über die geheime Schlüssel des Anwenders übertragen werden
3. Übertragung von Schlüsseln auf einen anderen Rechner muss ermöglicht werden
4. Transparenz über die Zertifizierungs-Mechanismen



# *Weitere Informationen*

Diese Folien im Netz:

<http://www.chaosdorf.de/files/TCPA.pdf>

- ▷ Trusted Computing Platform Alliance
- ▷ Ross Anderson's TCPA / Palladium FAQ
- ▷ CCC: Digitaler Maulkorb? Kritische Auseinandersetzung mit neuen Technologien und Gesetzen