Trusted Computing

Von
Michael Niehenke
und Marcus Proest

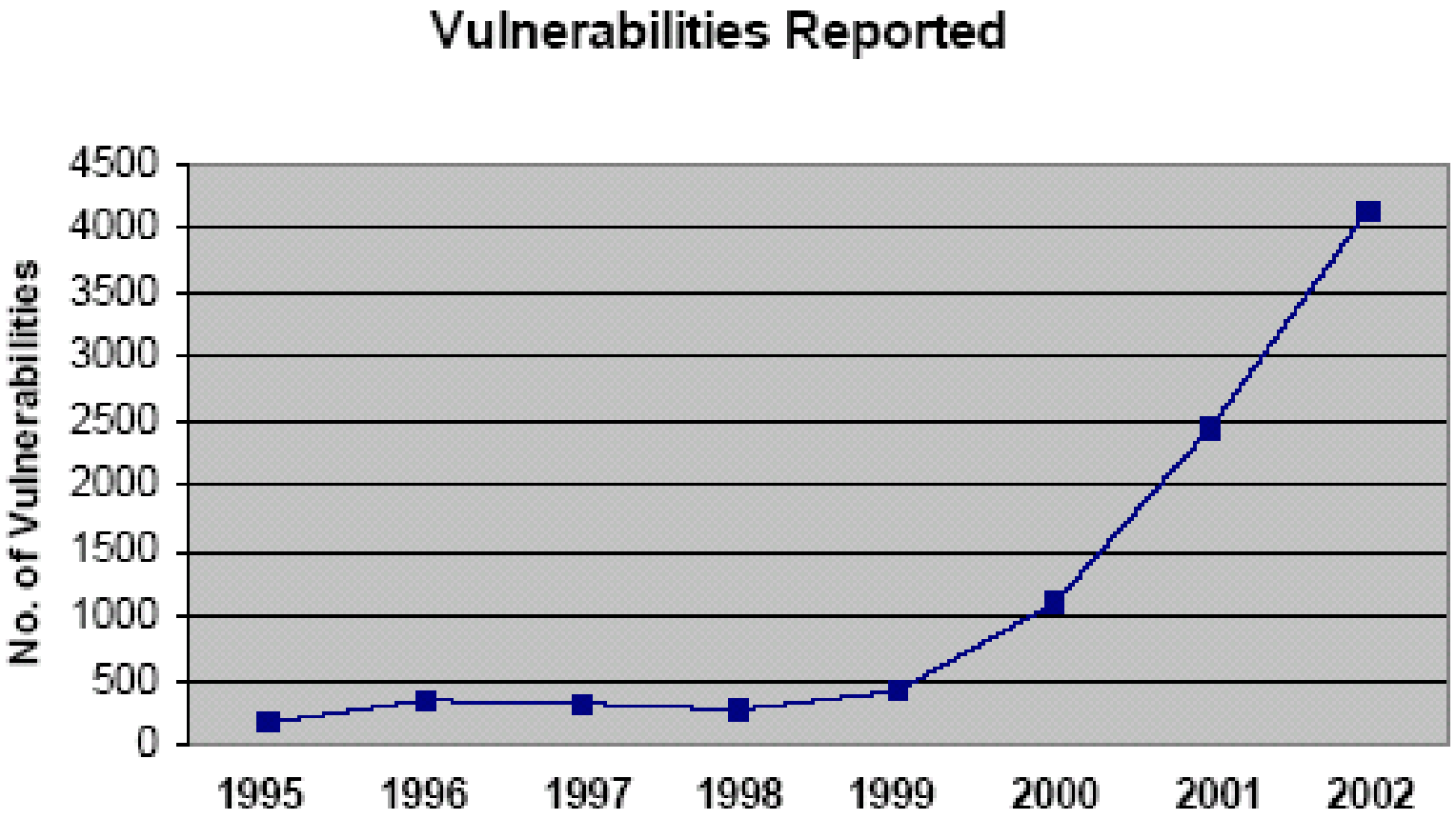
Gliederung

- Einleitung
- Die Trusted Computing Group
- Das Trusted Platform Module
- Anwendungen und Szenarien
- Kritik
- Ausblick
- Quellen

Einleitung (1/2)

- Problem
  - Anforderungen an Sicherheit werden größer
  - Bestehende Systeme sind unsicher
  - Hackerangriffe werden häufiger
- Lösung
  - Zusammenschluss von internationalen Konzernen
    → Trusted Computing Group (TCG)
  - Sicherheit in Hardware

Einleitung (2/2)



Die Trusted Computing Group (1/5)

- Trusted Computing Platform Alliance (TCPA)
  - Gegründet 11.10.1999
  - Microsoft, HP, Compaq, IBM, Intel
  - Spezifikation sicherer Technologien
  - Erhöhung des Vertrauens bei B2B
  - Bis April 2003 über 200 Mitglieder
  - 30.01.2001: erste TCPA Spezifikation (1.0)
  - Mai 2002: TCPA Spezifikation 1.1b

Die Trusted Computing Group (2/5)

- Trusted Computing Group (TCG)
  - Gegründet 08.04.2003 durch Gründungsmitglieder der TCPA
  - Grund: Wahrscheinlich Schwierigkeiten in der Konsensfindung
  - Heute 7 Hauptmitglieder: AMD, HP, IBM, Intel, Microsoft, Sony, Sun
  - ca. 40 weitere Mitglieder

Die Trusted Computing Group (3/5)

- Organisation
  - Ähnelt anderen Standardisierungsgremien
  - 3 Level der Mitgliedschaft
    - Promoter (50.000$ p.a.)
    - Contributor (15.000$ p.a.)
    - Adopter (7.500$ p.a.)
  - Promoter und Contributors bilden Board of Directors
  - Nur Promoter haben dauerhaften Sitz im BoD
  - Adopter kein Stimmrecht, nur Zugriff auf Ergebnisse

Die Trusted Computing Group (4/5)

- Arbeitsweise
  - TCPA erkennt TCG als offiziellen Nachfolger an
  - TCG führt TCPA Spezifikationen weiter
  - 05.11.2003: TPM Spezifikation 1.2
  - Erste Implementierungen für Anfang 2004 erwartet
  - Teile der Spezifikationen stehen zunächst nur den Mitgliedern zur Verfügung
  - Veröffentlichung unter RAND Lizenz

Die Trusted Computing Group (5/5)

- Development Policies
  - Open Platform Development Model
    - Plattformunabhängig
  - Platform Owner and User Control
    - Benutzer soll vollständige Kontrolle behalten
    - Alle Features deaktivierbar
  - Privacy Effect of TCG Specifications
    - Sicherheit der persönlichen Identifizierbarkeit

Das Trusted Platform Module (1/8)

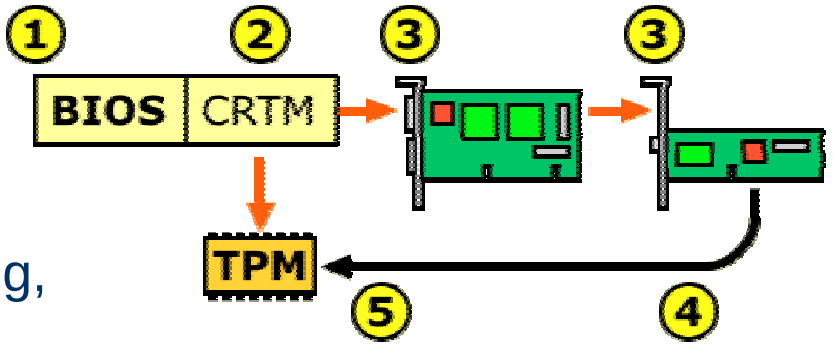
- Zentrale Hardwarekomponente
- Sicherheit soll auf Hardwareebene garantiert werden
- Bei PC: Chip auf Motherboard

Das Trusted Platform Module (2/8)

- Hauptfunktionen
  - Schlüsselgenerierung, Ver- und Entschlüsselung
    - Kann asymmetrische Schlüssel unter Verwendung eines sicheren Zufallszahlengenerators generieren
    - Mechanismus zur sicheren persistenten Datenspeicherung
    - Sichere Schlüsselspeicherung
  - Platform Control Registers (PCR)
    - Speicherung der aktuellen Konfiguration von Soft- und Hardware durch Hash- Werte
    - Aufbau einer Chain of Trust beim Bootvorgang

Das Trusted Platform Module (3/8)

- Hauptfunktionen
  - Platform Control Registers (PCR)
    - Boot: BIOS lädt CRTM (Core Root of Trust Measurement)
    - CRTM kontaktiert TPM
      TPM aus: Fehlermeldung, Bootvorgang fortsetzen
    - TPM an: Analyse der Komponenten
    - Berechnung der Rechnerkonfiguration
    - Sicherung eines SHA-1 Wertes der Konfiguration in PCR



Das Trusted Platform Module (4/8)

- Hauptfunktionen
  - Endorsement Key
    - Für jeden Chip einzigartig
    - Vom Hersteller in TPM geschrieben
    - Privater EK und öffentlicher EK
    - Private Key verlässt nie das TPM
    - Von Zertifizierungsstelle zertifiziert
    - Basis für weitere Schlüssel → Anonymität der Plattform durch AIK Schlüssel

Das Trusted Platform Module (5/8)

- Hauptfunktionen
  - Initialisierungs- und Management Funktionen
    - Managen von Features des TPM Chips
    - Möglichkeit den Chip zu deaktivieren

Das Trusted Platform Module (6/8)

- Allgemeine Nutzungsbeispiele

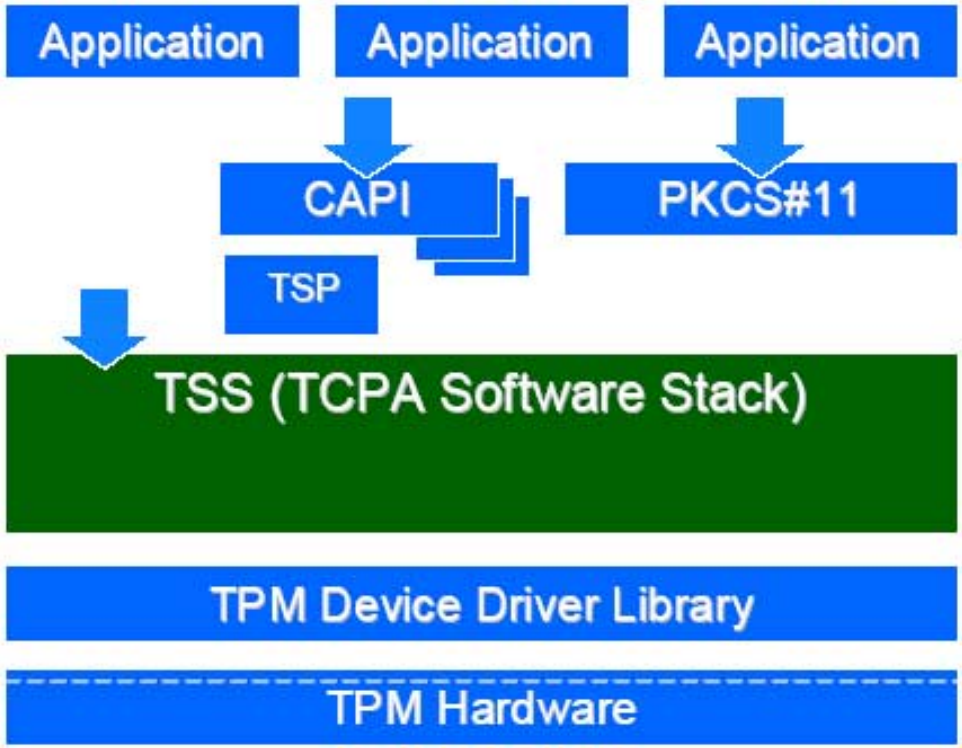
Bedrohung	Momentane Lösungen	Schwachstellen	TPM- Lösungen
Datendiebstahl	Datenverschlüsselung (EFS, VPN, verschlüsselte eMail, etc)	Schlüssel liegen auf der Harddisk und können manipuliert werden	Sichere Speicherung von Schlüsseln durch Hardware
Unerlaubter Zugriff auf die Plattform	Username / Passwort Biometrische Verfahren oder Hardware Tokens	Dictionary Attacks Manipulierte Biometrische Daten Authentifizierungsdaten sind nicht mit der Plattform verknüpft	Authentifizierungsdaten mit Plattform verknüpft
Unerlaubter Netzwerkzugriff	Windows Netzwerk Logon, IEEE 802.1x	Kann umgangen werden Zertifikate können gefälscht werden Daten werden auf der Festplatte gespeichert und können manipuliert werden	PKI Methode zur Plattform Authentifikation Hardware Schutz der Authentisierungsdaten

Das Trusted Platform Module (7/8)

- TCG Software Stack (TSS)
  - API zum Zugriff auf TPM Funktionen
  - Spezielle Funktionen zu bereits bestehenden CryptoAPIs
    - MS CAPI
    - CDSA
    - PKCS#11
  - Fehlende Funktionen in CryptoAPI nur mittels Direktzugriff auf TSS möglich

Das Trusted Platform Module (8/8)

- TCG Software Stack (TSS)



Anwendungen und Szenarien (1/6)

- Palladium / NGSCB
  - Palladium umbenannt in Next Generation Secure Computing Base (vermutlich wegen schlechter Presse)
  - Vertrauenswürdige Computerumgebung in MS OS
  - Sicheres Betriebssystemmodul: Nexus
    - Sichere Kommunikation mit Anwendungen, Peripherie, primären und sekundären Speicher

Anwendungen und Szenarien (2/6)

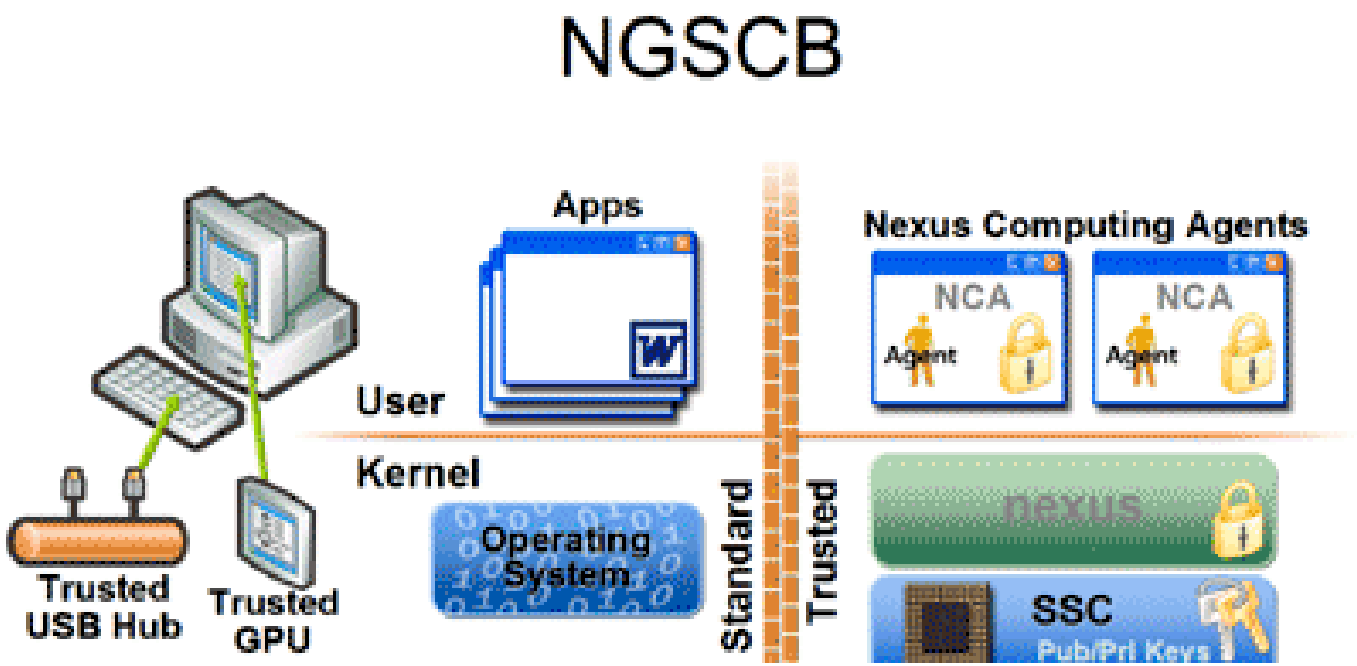
- Palladium / NGSCB
  - Sicherheitsmerkmale
    - Geschützter Speicher
    - Sichere Speicherung
    - Digitale Signatur
    - Sichere E/A

Anwendungen und Szenarien (3/6)

- Palladium / NGSCB
  - Nexus
    - Verwaltet Funktionalität für vertrauenswürdige Operationen
      - Prozesserzeugung
      - Signatur-Handling
      - Ver- und Entschlüsselung
  - Trusted Agents (Nexus Computing Agents)
    - Programm/-teil in geschütztem Speicherbereich
    - Greift auf Nexus zu um gesicherte Operationen durchzuführen

Anwendungen und Szenarien (4/6)

- Palladium / NGSCB



Anwendungen und Szenarien (5/6)

- Palladium / NGSCB
  - Ungelöste Probleme
    - Fernwartung
    - Behindertengerechte Nutzung
    - Versiegelter Speicher
    - Auslagerung des sicheren Speichers
    - Zertifizierung

Anwendungen und Szenarien (6/6)

- IBM Embedded Security Subsystem (ESS)
  - Erste TCG Implementierung
  - Besteht aus TPM und Client Security Software
  - Sicherheit kann auf persönliche Bedürfnisse zugeschnitten werden
    - IBM Client Security Password Manager
    - IBM Client Security Software Assistent

Kritik (1/4)

- viele „ANTI-TCPA“ Communities/ Vereinigungen entstanden
- Information auf „Anti-Websites“ sollten mit Vorsicht betrachtet werden
- Aber Risiken erkennbar

Kritik (2/4)

- Digital Rights Management (DRM)
  - DRM soll die Verbreitung von digitalen Medien kontrollieren
  - Palladium als DRM-System vermutet
    - DRM Überlegungen als Ursprung von Palladium
    - Laut Microsoft hat sich Ziel verändert
  - Nicht Schutz des Nutzers, sondern Schutz vor dem Nutzer
  - DRM Mechanismen nicht Teil der TPM Spezifikation

Kritik (3/4)

- **Black- und Whitelists**
  - Listen von (un)erlaubten Komponenten bzw. Software
  - In TPM Spezifikation nicht vorgesehen
  - In Palladium leicht zu implementieren
- **Zertifizierung von Code**
  - Code muss zertifiziert werden, um mit Nexus kommunizieren zu dürfen
  - Kosten für Zertifizierung unklar
  - Problem für OpenSource und kleinere Unternehmen

Kritik (4/4)

- Wahrheiten und Gerüchte
  - TPM soll in den USA Pflicht werden
    → Unwahrscheinlich, Bemühungen vorhanden
  - Nicht ohne weiteres zu Linux kompatibel
    → Falsch, Linux Treiber bereits vorhanden
  - Abschaltbar
    → Richtig, defaultmässig deaktiviert (Opt-In)
  - Enthält eindeutige Rechneridentifikation
    → Richtig

Ausblick

- Verschiedene Implementierungen
  → sowohl Chancen als auch Risken
- TPM Chip kann Sicherheit erhöhen
- Aber auch Nutzerrechte einschränken

Quellen

- http://www.trustedcomputing.org
- http://www.trustedcomputinggroup.org
- http://www.heise.de/ct/Redaktion/ghi/tc/linuxtagTC.html
- http://www.againsttcpa.com
- http://www.intel.com
- http://www.ibm.com
- http://www.microsoft.com
- http://www.chip.de
- c’t 12/2003
- c’t 11/2003
- c’t 09/2003
- c’t 06/2003
- c’t 26/2002
- c’t 24/2002
- c’t 22/2002
- c’t 15/2002