HOCHSCHULE DER MEDIEN

Trusted Computing mit Windows Vista

Thomas Müller, Hochschule der Medien, Stuttgart

Agenda

- Ziele und Konzepte des Trusted Computing
- Anforderungen an Trusted Operating Systems
- Sicherheitsfunktionen in Windows Vista
- Bewertung der Funktionen
- Bekannte Angriffe
- Mögliche Lösungsansätze
- Fazit

Was bedeutet Vertrauen?

- „Vertrauen ist die subjektive Überzeugung der Richtigkeit bzw. Wahrheit von Handlungen und Einsichten eines anderen oder von sich selbst“

- Bedeutung nur schwer auf die IT-Welt übertragbar
  - Software ist nicht vertrauenswürdig
  - Vertrauen basiert hier durchaus auf Beweisen!
  - Vertrauenswürdig bedeutet sich sicher sein zu können dass ein System wie erwartet arbeitet.
  - Attested (beglaubigtes) Computing evtl. der bessere Begriff?

Ziele des Trusted Computing

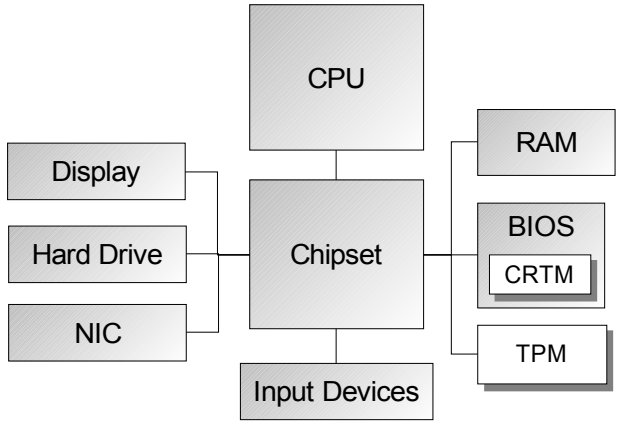
- Schaffung einer Plattform Identität
- Bereitstellung von sicherem Schlüsselspeicher
- **Bewertung der Systemintegrität anhand des Zustands eines Systems**
- Bereitstellung von abgeschirmten Ausführungsbereichen
- …

Kernkonzepte des Trusted Computing

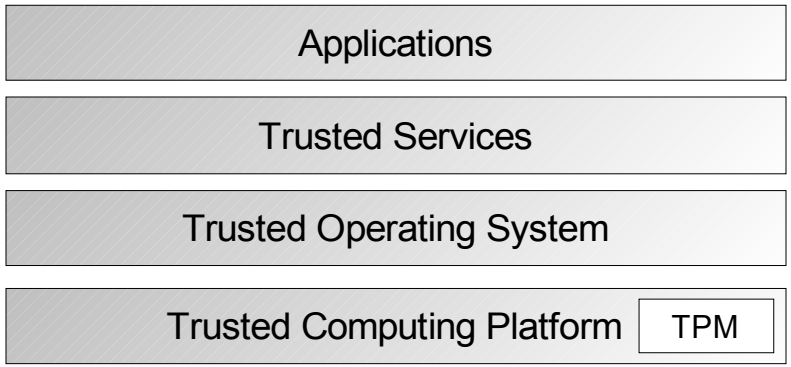
- Hardware als Vertrauensanker (Root of Trust)
  - Trusted Platform Module (TPM), Intel TET, ARM Trustzones …
- **Vertrauenskette (Chain of Trust)**
  - **Integritätsmessungen (Integrity Measurement)**
  - **Integritätsbewertung (Integrity Validation)**
- **Integritätsnachweis (Remote Attestation)**
- Isolation von Prozessen (Security Domains / Multilevel Security)
- …

Begriffsdefinitionen

- Trusted Computing Platform (TCP)[1]
  - Vertrauensanker (TPM)
  - Besteht aus Hardware und Firmware
  - Startet die Vertrauenskette



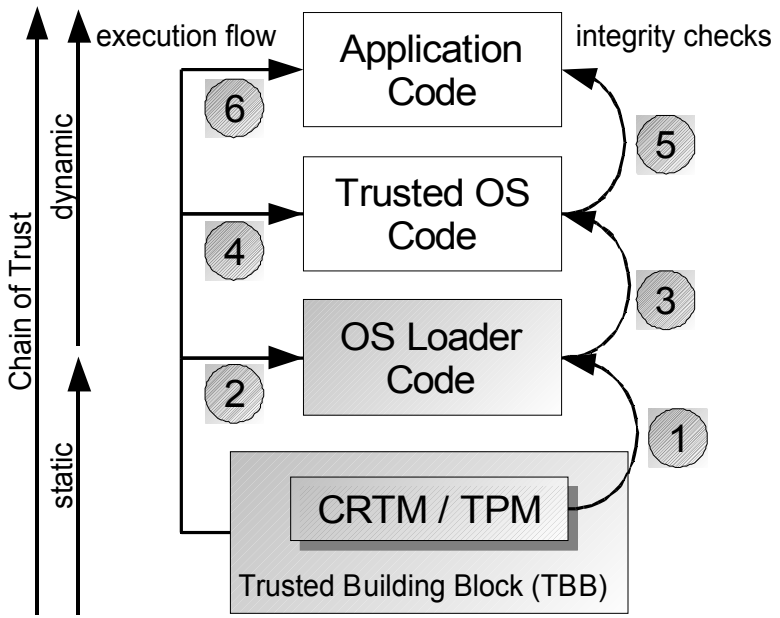
- Trusted Computing System (TCS)
  - TCP +
  - Betriebssystem +
  - Dienste +
  - Applikationen



1) Am Beispiel der TCP der Trusted Computing Group

Vertrauenskette (Chain of Trust)

- Jede Instanz der Ausführungskette wird zuerst gemessen und dann ausgeführt
- Messergebnisse werden in den 23 PCR[1] des TPM abgelegt
- TCP füllt PCR 0-7
  - (Static Chain of Trust)
- PCR 8-15 für Startvorgang des OS
  - (Static-OS Chain of Trust)
- Restliche PCR werden für Messungen zur Laufzeit verwendet
  - (Dynamic-OS Chain of Trust)



1) PCR = Platform Configuration Register

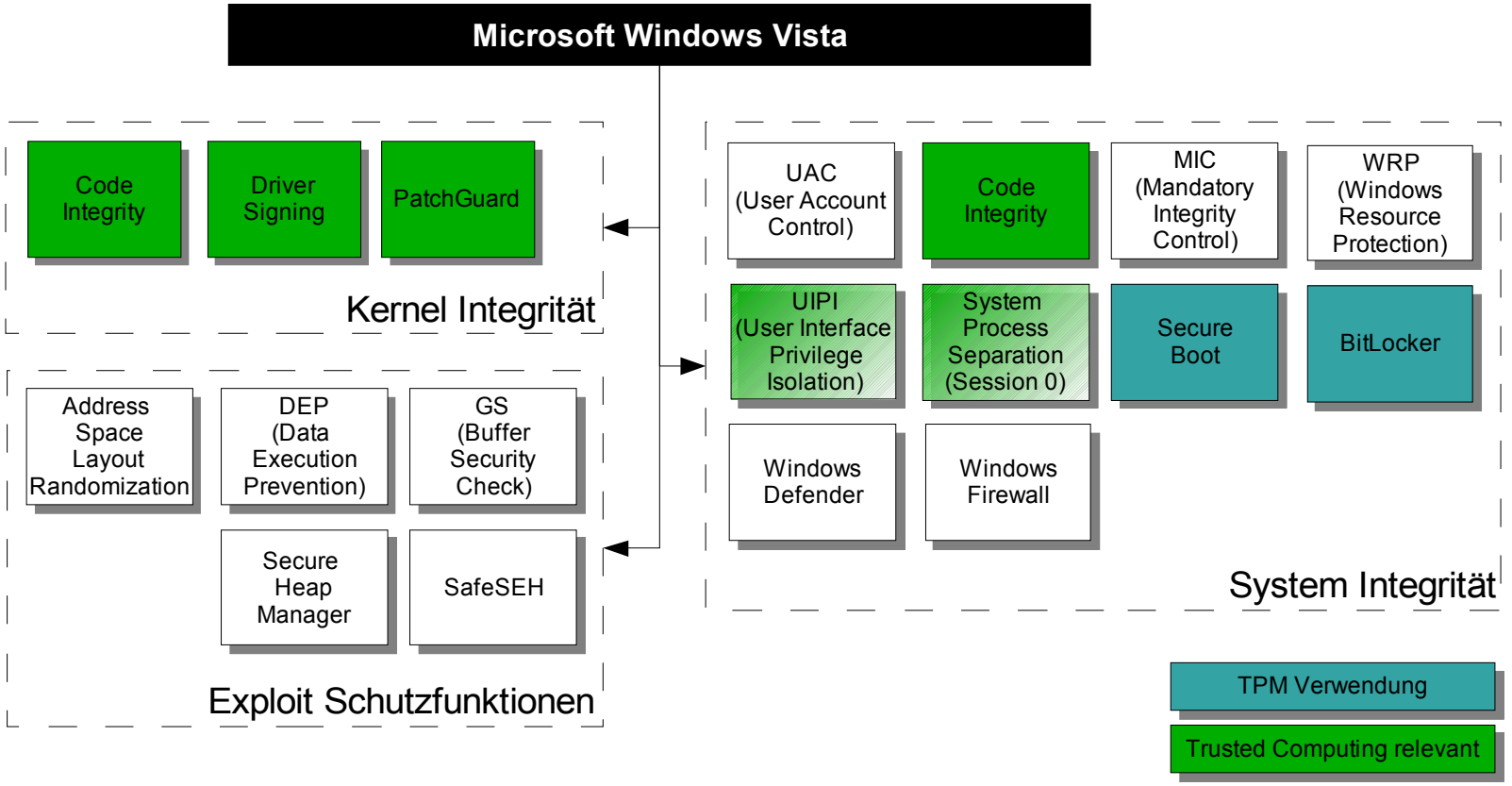
Integrity Validation / Remote Attestation

- Bewertung der Systemintegrität durch Vergleich der Prüfsummen mit Referenzwerten:
  - TPM schützt Prüfsummen durch Signatur – Keine Bewertung!
  - Auch ein „sicheres“ Betriebssystem ist nicht in der Lage seine Integrität selbst zu bewerten!
- Verwendung der „sealing“ Funktion des TPM
- Eine weitere Instanz ist notwendig
  - Ein entferntes Computersystem (Remote Attestation)
  - Ein geschlossenes System im System (z. B. Smartcard)

Anforderungskatalog für Trusted-OS

1. Fortsetzung der Vertrauenskette bis zum Ende des Startvorgangs
2. Erweiterung der Vertrauenskette zur Laufzeit
3. Bereitstellung einer Schnittstelle zur Abfrage der Vertrauenskette
4. (Bewertung der Systemintegrität)
5. …

Sicherheitsfunktionen in Vista



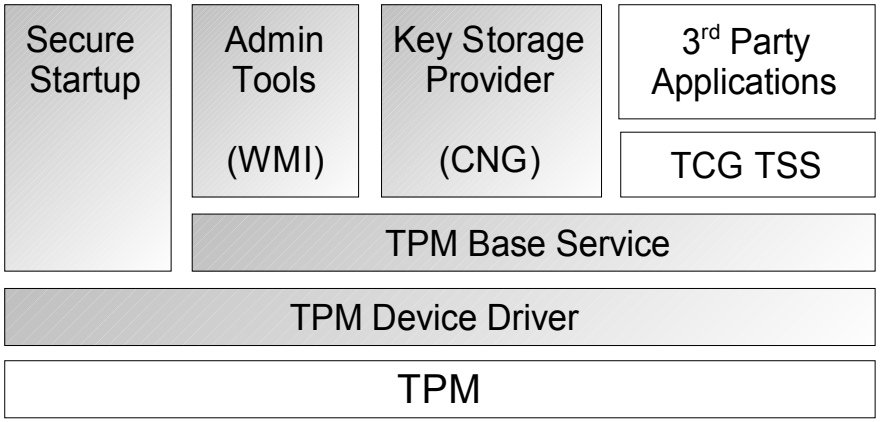
Windows Vista Integritätsschutz

- Secure Startup (Teil der BitLocker Festplattenverschlüsselung)

- Digital signierte Treiber (Driver Signing)
- Integritätstests (Kernel Integrity Checks)

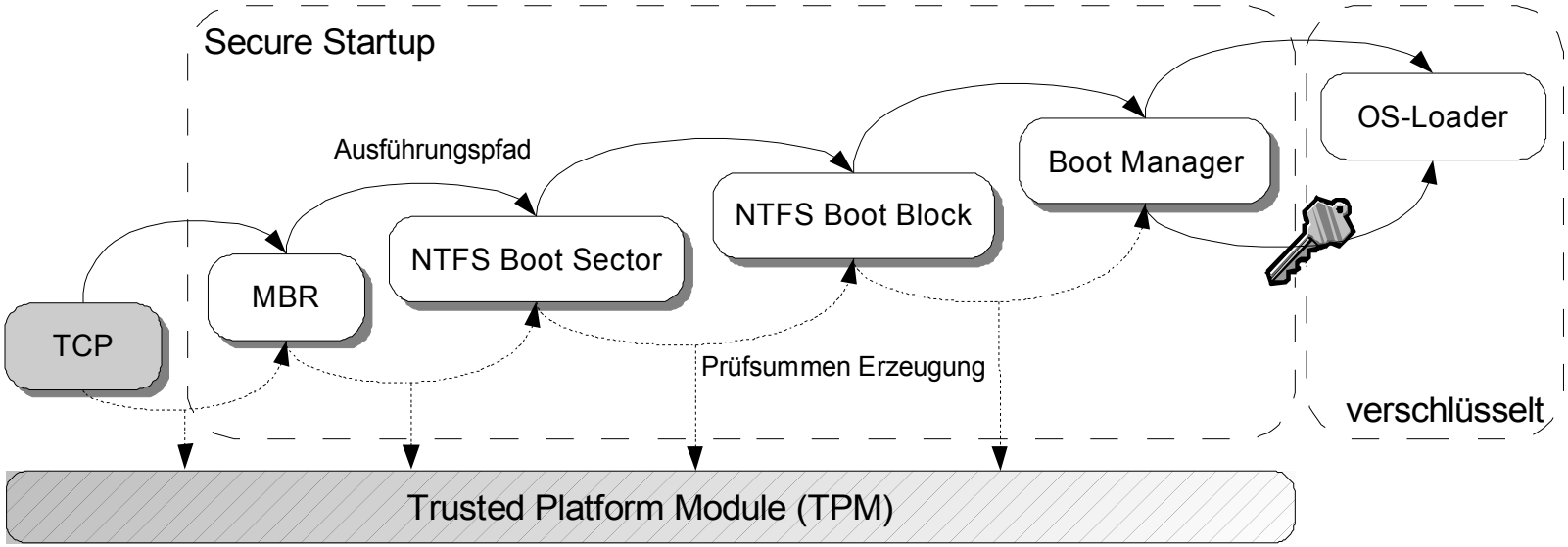
- Network Access Protection (NAP)

Verwendung des TPM in Windows Vista

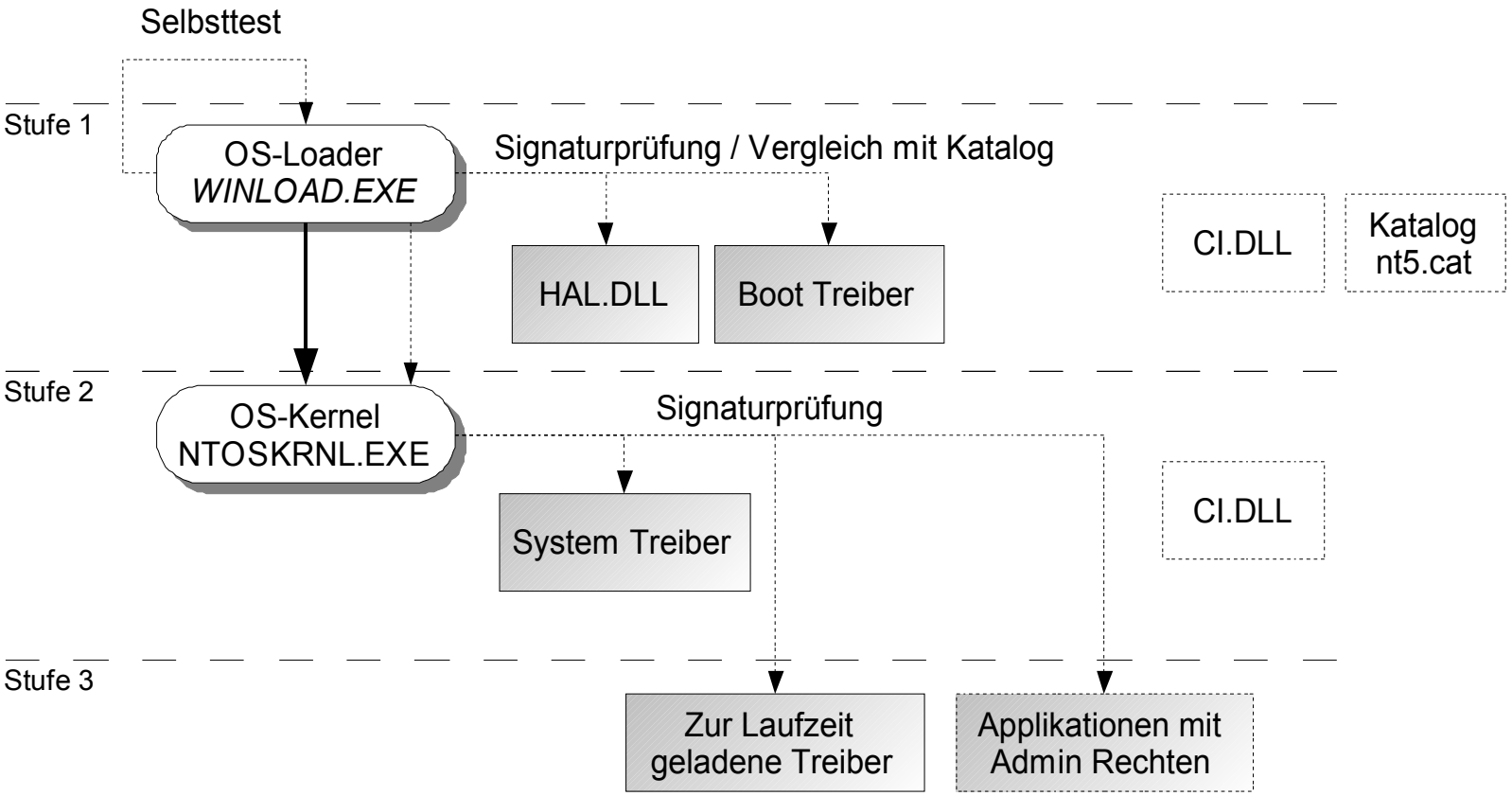


- Vista enthält keinen zur TCG Spezifikation konformen Trusted Software Stack
- Microsofts CNG bietet nur eine Untermenge der TPM Funktionen
- TSS von anderen Herstellern unterliegen TPM Base Service Kontrolle
- Secure Startup einzige direkte Verwendung des TPM

Microsoft Secure Startup (BitLocker)

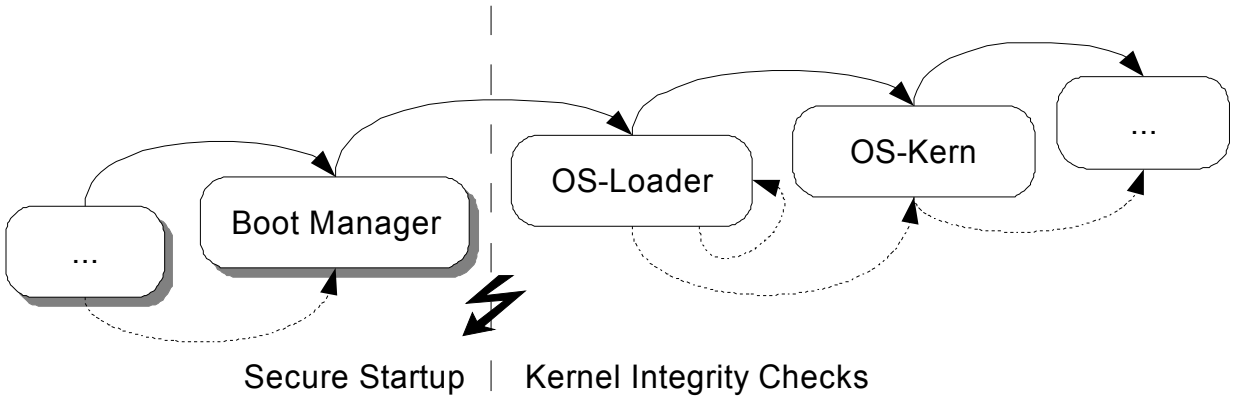


Treibersignaturen / Integritätstests



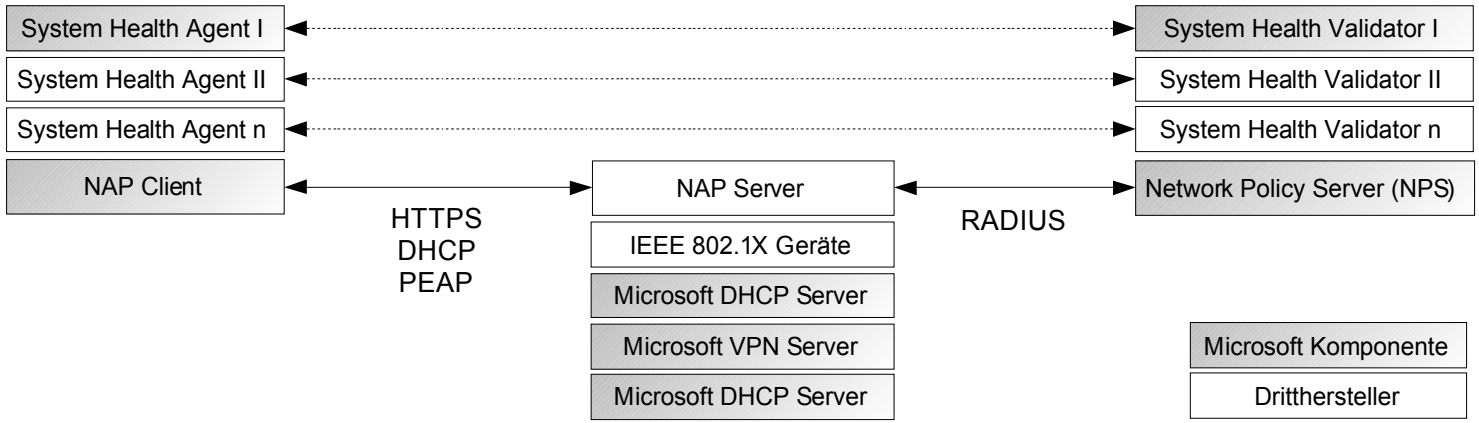
Bewertung des Integritätsschutzes

- Secure Boot / BitLocker
  - Schützt nur vor „offline“-Angriffen
  - Kein echter Integritätstest
- Driver Signing / Kernel Integrity Checks
  - Unterbrechung der Vertrauenskette
  - OS-Loader bildet neuen Vertrauensanker
  - Integritätprüfung des OS-Loader ist Selbsttest



Network Access Protection (vereinfacht)

- Netzwerkzugriffskontrolle basierend auf Systemzustand
- Systemzustand ermittelt durch System Health Agents
- Bewertung des Systemzustands durch System Health Validators
- NAP Server (z. B. WLAN-AP) blockt oder isoliert nicht konforme Systeme
- Erstellung eigener SHA/SHV Komponenten möglich



Bewertung NAP

- Bewertung des Systemzustands nur basierend auf Zustand von:
  - Firewall
  - Virusschutz
  - Spywareschutz
  - Automatische Updates
- Agenten-Systeme anfällig für lokale Manipulation[1]
- Integrität der Agenten kann nicht gewährleistet werden
- Keine Verwendung des TPM

1) Ciscos NAC Angriff (BlackHat 2007)

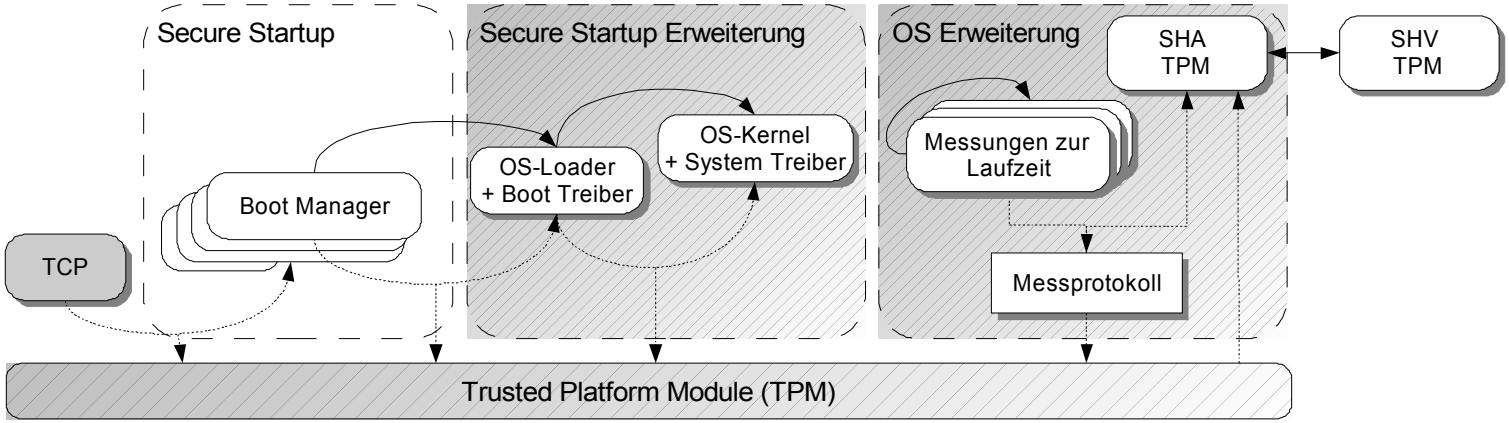
Bekannte Angriffe auf Vista Systemintegrität

- Pagefile Attack (Juli 2006) – Joanna Rutkowska
  - Manipulation von Code in ausgelagerten Treiber
  - Seit Vista RC2 teilweise behoben
- Blue Pill (Juli 2006) – Joanna Rutkowska
  - Verwendung von CPU Virtualisierungssupport (AMD SVM, INTEL VT)
  - OS wird zur Laufzeit in VM verschoben – volle Kontrolle von Systemevents
  - Keine zuverlässige Gegenmaßnahme vorhanden (nicht Vista spezifisch)
- **WINLOAD.EXE Patch (November 2006) - Symantec**
  - Deaktivierung der Selbsttestfunktion des OS-Loader
  - Erlaubt die Deaktivierung sämtlicher Integritätsschutzfunktionen
  - Trotz ungültiger Code-Signatur nur schwer zu erkennen
- **Vbootkit (März 2007) - NVLabs**
  - Platzierung von Schadcode im Kernelspeicher durch Verwendung von alternativem MBR (CD, USB-STICK, PXE) – Manipulation von OS-Loader und OS-Kernel
  - Keine Manipulation von Systemdateien erforderlich
  - **Schlägt fehl bei aktivem BitLocker (Secure Startup)!**

Vista als Trusted-OS (Konzept)

1. Erweiterung der Vertrauenskette bis zum OS-Kernel
   - Ermöglicht die Erkennung der WINLOAD.EXE Modifikation
   - Zusätzliches „sealing“ liefert Schutz vor Modifikation
2. Erweiterung der Vertrauenskette zur Laufzeit
   - Protokollierung „kritischer“ Events
   - Prüfsumme über Protokoll geschützt durch TPM
3. Erweiterung der NAP Architektur
   - SHA/SHV für die Überprüfung der beim Startvorgang erzeugten Prüfsummen
   - SHA/SHV für die Überprüfung des Applikationsprotokolls
   - Verifikation der TPM Signatur auf dem NPS

Vista als Trusted-OS (Konzept)



- Prüfsummen über OS-Loader und OS-Kernel werden im TPM abgelegt
- OS-Kernel protokolliert sicherheitskritische Events
  - Laden von Windows Diensten
  - Nachladen von Treibern
  - Start von Applikationen mit administrativen Rechten
- Prüfsummen des Startvorgangs und Laufzeit-Protokoll werden durch das TPM signiert und an den NPS übertragen

Fazit

- Windows Vista ist kein Trusted-OS
- Trusted Computing Einflüsse erkennbar:
  - Innerhalb des BitLocker Teams
  - Innerhalb des NAP Teams
  - Beide Umsetzungen sind nur Insellösungen
- Erstellung und Bewertung eines Laufzeit-Protokolls sehr komplex
  - Bisher nur als Proof-of-Concept für Linux verfügbar[1]
- Kein wirksames Konzept zur Isolation von Prozessen vorhanden
- Desktop Betriebssysteme wie Vista zu komplex für Trusted-OS
  - Neue OS-Architekturen und Hardware Support[2] notwendig

1) Integrity Measurement Architecture (IMA) von IBM
2) z. B. Intel TET

Fragen und Anregungen:

Thomas.Mueller@xnos.de

www.xing.com/profile/Thomas_Mueller224

Unterlagen auf xnos.org:

- Foliensatz
- Kurzfassung „Trusted Computing mit Windows Vista“
- Diplomarbeit „Konzepte und Anforderungen für Trusted Computing Systeme“ (ab 07/07)

Ressourcen

- Microsoft NAP
  - www.microsoft.com/technet/network/nap/default.mspx
- Integrity Measurement Architecture
  - domino.research.ibm.com/comm/research_projects.nsf/pages/ssd_ima.index.html
- Intel Trusted Execution Technologie
  - www.intel.com/technology/security/
- Vbootkit: Compromising Windows Vista Security
  - www.nvlabs.in/files/vbootkit_nitin_vipin_whitepaper.pdf
- Symantec: Winload.exe Patch
  - www.symantec.com/avcenter/reference/Security_Implications_of_Windows_Vista.pdf
  - http://www.symantec.com/avcenter/reference/Windows_Vista_Kernel_Mode_Security.pdf
- J. Rutkowska: Subverting Vista Kernel for Fun and Profit
  - www.blackhat.com/presentations/bh-usa-06/BH-US-06-Rutkowska.pdf

HOCHSCHULE DER MEDIEN

Hochschule der Medien

Nobelstraße 10
70569 Stuttgart

Tel. 0711 8923 10
Fax 0711 8932 11

info@hdm-stuttgart.de

www.hdm-stuttgart.de