

D.7 Trusted Computing

1 Motivation

- Verschlüsselte Dateisysteme schützen nur statische Daten
 - Schwachstelle: Software zur Laufzeit
 - Betriebssystem, Anwendungen
- Sicherheitskonzepte zur Laufzeit ebenfalls unzureichend
Basis: Speicherschutz, Adressräume
 - Schwachstelle: Betriebssystem - vor allem Treiber
 - woher kommt Software, ist sie vertrauenswürdig?
 - Auslagerung von Treibern in eigene Adressräume bringt wenig
 - DMA-Geräte können direkt auf Speicher zugreifen
 - Signieren von Software kann helfen
 - ABER: wer überprüft die Signatur?
 - ist diese Einheit angreifbar?

2 Fazit: Sicherheitsarchitektur

- Viele Schutzmechanismen sind zu grob-granular
- Es wird eine durchgängig Kette vertrauenswürdiger Einheiten vom Systemstart bis hin zu jeder Anwendung benötigt
- ➔ Vertrauenswürdige Sicherheitsarchitektur benötigt ineinander greifende, wirksame Hardware-, Firmware und Software-Sicherheitskonzepte
 - ◆ Hardware: stellt vertrauenswürdige, nicht umgehbare Basisfunktionen zur Verfügung
 - ➔ Beispiel: sichere Erzeugung und Speicherung von Schlüsseln
 - Nutzung über einheitliche Schnittstelle durch Betriebssystem und Anwendungen
 - ◆ BS und Anwendungen bieten darauf aufbauend komplexere Dienste an
 - ➔ Beispiel: Verschlüsselnder Objektspeicher
 - ◆ Strategien (Policies) werden von den Mechanismen strikt getrennt.
 - Policies können Betriebssystem- oder Anwendungs-abhängig sein
 - Mechanismen sind einheitliche Basis

3 TCPA und TCG

- Trusted Computing Platform Alliance (TCPA)
 - 1999: Microsoft, Intel, IBM, Compaq, HP
 - 2003: > 200 Mitglieder
 - ➔ handlungsunfähig (Beschlüsse nur einstimmig möglich)
- TCPA-Ziele
 - Hard- und Softwarestandards für vertrauenswürdigerer Rechner-Plattformen (→ E-Business-Transaktionen)
 - Plattform = Motherboard, CPU, E/A-Geräte, BIOS, ...
- TCPA-Funktionen
 - sicheres Booten
 - *Attestation* (Bestätigung der Integrität der Systemkonfiguration einer Plattform gegenüber Kommunikationspartnern)
 - sichere Generierung und Aufbewahrung von Schlüsseln
- Trusted Computing Group (TCG)
 - 2003: AMD, HP, Intel, Microsoft (Beschlüsse mit 2/3-Mehrheit)

4 TCG-Architektur

- **Trusted Platform Module (TPM)**
= Hardware-Teil (TCG-Chip)
- **Root of Trust for Measuring Integrity Metrics (RTM)**
= Hardware / Firmware-Teil
(entweder in TPM integriert oder im BIOS implementiert)
- **Trusted Software Stack (TSS)**
= Software-Teil
- TPM + RTM + TSS = **TCG-Subsystem**
 - vertrauenswürdige Basisdienste als Bausteine für Betriebssysteme
 - OpenTC-Projekt (www.opentc.net) entwickelt Software-Framework für Trusted Computing – u. a. Betriebssystem auf Basis von Xen und L4

5 TCG-Subsystem

- TPM: Fest eingelöteter Smartcard-Prozessor
 - ◆ bietet kryptografische Operationen in Hardware
 - Zufallszahlen
 - Schlüsselgenerierung mit privatem Schlüssel der Chip nicht verlässt
 - Signieren und Signaturprüfung
 - Ver- und Entschlüsseln
- RTM "misst" in speziellen Registern den Systemzustand
 - bildet Hash über ausgeführte Befehlsfolge
 - damit können Modifikationen an Code festgestellt werden
- Sicheres Booten über eine BIOS Erweiterung (CRTM = Core RTM)
 - Spezielle Register "messen" den Bootvorgang vom BIOS über Bootloader zum Systemkern.
 - Softwareschicht kann aufgrund von Messwerten Rückschlüsse auf Systemintegrität ziehen

5 TCG-Subsystem (2)

- Integritäts-Messwerte werden in sicherem Speicher (auf TPM) abgelegt
 - *Attestierung* über eine Systemkonfiguration (=Messwert-Report)
 - Änderungen können durch Vergleich mit den ursprünglichen Messwerten entdeckt werden
- Anwendungen und Kommunikationspartner können Attestierungen abfragen
 - Gewissheit über Authentizität einer Plattform
 - Nachweis enthält Identität der Plattform + Angaben über konkrete Konfiguration
- TSS definiert Standard-API für Zugriff auf TPM
 - Ex- und Import von Kommunikationsschlüsseln
 - Erstellung Hashwerten und Integritätsbescheinigungen
 - Basis für Schnittstellen zu existierenden Krypto-APIs

6 Eindeutige Identität und Besitzerkonzept

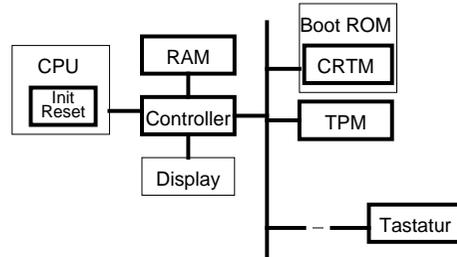
- TPM eindeutig identifizierbar
 - *Endorsement Key* und Zertifikat
 - Integration bei der Chip-Herstellung
 - Privacy-Problem → Endorsement Key gegenüber Dritten verschleiern
→ *Attestation Identity Keys* (AIK)
- Besitzer muss TCG-Plattform explizit übernehmen
 - Festlegung eines Passworts
 - Basis für Aktivierung und Deaktivierung
 - Basis für Zugriff auf geschützte Objekte im TPM-Speicher
- Zurücksetzen des TPM durch Jumper auf dem Board möglich
 - Löscht das Besitzer-Passwort
 - Verlust aller Schlüssel auf dem TPM

7 Roots of Trust

- "Vertrauenswurzeln" = Ausgangspunkte für den Aufbau einer vertrauenswürdigen Systemkonfiguration
 - den Roots of Trust muss vertraut werden - Fehlverhalten ist nicht aufdeckbar
- *Root of Trust for Measurement* (RTM)
 - Funktionen, die Integrität einer Konfiguration beim Booten, bei Reset und nach Suspend prüfen können
 - teilweise auf TPM, teilweise BIOS-Komponente (nicht ersetzbar!)
- *Root of Trust for Storage* (RTS)
 - schützt Schlüssel und vertrauenswürdige Daten
 - hierarchische Schlüsselverwaltung - Elternknoten verschlüsselt darunter liegende Schlüssel, Wurzel = Storage Root Key (SRK)
 - SRK wird bei Plattform-Inbesitznahme generiert und verlässt TPM nie
- *Root of Trust for Reporting* (RTR)

8 Trusted Building Blocks

- Komponenten und Verbindungswege, die sicherheitskritisch sind



- ★ häufige Schwachstelle: Verbindung zwischen Tastatur und System

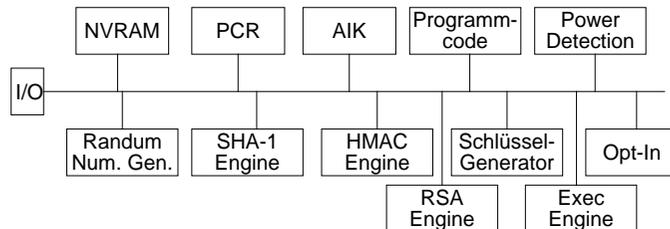
9 TPM im Detail

- Aufgaben

- ▶ Generierung von symmetrischen und asymmetrischen Schlüsseln (Hardware-basierter Zufallszahlengenerator), Signaturerstellung, Hashwertberechnungen, Chip-interne Verschlüsselung
- ▶ Verschlüsseln von kryptographischen Schlüsseln (Wrapping) (zur Verwaltung der Schlüssel außerhalb des TPM)
- ▶ sichere Speicherung von (kleinen) Objekten und Hashwerten
→ shielded Register,
Zugriff nur über bestimmte Sicherheitsdienste (Signieren, Verschlüsseln)
- ▶ Erstellen von signierten Reports über gespeicherte Werte (nur nach Autorisierung durch den Plattformbesitzer)
- ▶ Endorsement-Key und Generierung/Bestätigung von AIKs
- ▶ Vertrauenswürdiger Timer für Zertifikate mit Gültigkeitsdauer

9 TPM im Detail (2)

- Architektur



10 Sicheres Booten

- normaler Botvorgang:
Power-on → ROM → BIOS → MBR → Boot-Block → BS-Kern → ...
- Sicherheitprobleme
 - ◆ MBR (Master Boot Record) modifiziert (Boot-Sektor-Virus)
 - ▶ wird ungeschützt in den nackten Speicher geladen
 - ◆ Boot-Block manipuliert
 - ▶ kann modifiziertes Betriebssystem laden
 - ▶ Modifizierter Betriebssystemkern
 - ▶ kann überall zugreifen
 - ▶ kann Anwendungen falsche Tatsachen vorspiegeln
 - ▶ ...

10 Sicheres Booten

- sicheres Booten und TCG
 - Aufbau einer Vertrauenskette vom Einschalten bis zu den Anwendungen
- Power-on → CRTM
 - ◆ CRTM berechnet Hash-Werte und speichert sie in Register PCR₀ auf TPM
 1. HASH(CRTM) → PCR₀ – bevor CRTM in Speicher geladen wird
 2. HASH(BIOS) → PCR₁
- BIOS laden und starten
 3. HASH(Motherboard-Firmware | PCR₁) → PCR₁
 4. HASH(Hardware-Konfiguration | PCR₁) → PCR₁
 5. HASH(Option ROMS) → PCR_{2/3}
 6. HASH(MBR) → PCR₄
- MBR laden
 7. HASH(Boot-Block | PCR₄) → PCR₄

10 Sicheres Booten (2)

- Boot-Loader ausführen
 8. HASH(Betriebssystem-Kern | PCR₄) → PCR₄
- Betriebssystem laden und ausführen
 - ◆ BS kann verschlüsselt auf Platte abgelegt sein
 - TPM übernimmt sichere Speicherung des Schlüssels und Entschlüsselung
 - BS kann Hashwerte über Anwendungen erstellen
- Referenzwerte für gemessene Hash-Werte müssen über vertrauenswürdigen Kanal zugeführt werden
 - Vergleich mit aktuellen Werten führt zur Erkennung von Manipulationen

11 Zertifikate (Credentials)

- Ziel: Attestieren der Identität einer Plattform oder eines AIK einer Plattform
- Fünf Zertifikattypen für unterschiedliche Anwendungsbereiche
 - es werden nur die jeweils benötigten Informationen bereitgestellt
 - ◆ Endorsement (EK)
 - von TPM-Hersteller ausgestellt und signiert
 - erlaubt eindeutige Identifikation einer Plattform
 - ◆ Conformance
 - bestätigt, dass TBB des TPM die Spezifikation erfüllen
 - ◆ Platform
 - identifiziert Hersteller der Plattform und einige Eigenschaften der Plattform
 - ◆ Validation
 - attestiert Vertrauenswürdigkeit von einzelnen Komponenten

11 Zertifikate (Credentials) (2)

- ◆ Attestation Identity
 - beglaubigt private AIK-Schlüssel, die zum Signieren von TPM-Werten verwendet werden können
- ➔ Entkopplung der Informationen über die TPM-Plattform von den Informationen über die Eigenschaften der Plattform
 - Nutzung der mit dem Endorsement-Zertifikat verbundenen Schlüssel gibt automatisch Informationen über die konkrete Plattform und damit über den Benutzer preis
 - AI-Zertifikate nutzen Trusted Third Party (Privacy CA) zur Anonymisierung

11 Zertifikate (Credentials) (3)

- Erzeugung von AI-Credentials und AIK-Schlüsseln
- (1) Kommando TPM-MakeIdentity an TPM
 - erzeugt Schlüsselpaar (-AIK, +AIK)
 - erzeugt Identity-Binding und signiert dieses mit dem AIK → AIK-Request
 - $AR = (+AIK, EK-Cred, Platform-Cred, Conformance-Cred)$
 - $c = \{AR\}^{-AIK}$
- (2) Request an CA
 - TPM → CA: $\{(+AIK, c, EK-Cred, Platform-Cred, Conformance-Cred)\}^{+CA}$
- (3) CA prüft Credentials, extrahiert AR, erzeugt Session-Schlüssel K und erstellt AIK-Credential
 - $KC = \{K\}^{+EK}$ $C-Cred = \{AIK-Cred\}^K$
 - CA → TPM: (C-Cred, KC)
- (4) TPM kennt -EK und kann damit K und damit AIK-Cred entschlüsseln

11 Zertifikate (Credentials) (4)

- Nutzung von AIK-Credentials bei Diensten
 - ◆ AIK-Schlüssel können zum Signieren von PCR-Registerinhalten genutzt werden
 - ◆ Ermittlung der PCR-Werte und Signieren laufen vollständig im TPM ab
 - wenn sichergestellt ist, dass der TPM vertrauenswürdig ist, ist der signierte PCR-Wert authentisch
 - CA kennt Zertifikate des TPM und kann bestätigen, dass ein AIK von einer Standard-konformen TPM-Plattform stammt

12 TCG für Digital Rights Management

- Idee: Software oder Daten (z. B. Musikstücke) sind mit Regeln verknüpft, die die Eigenschaften der Umgebung spezifizieren
 - Software läuft nur in bestimmter Umgebung
 - Daten können nur in bestimmter Umgebung genutzt werden
- ↪ Durchsetzung von Lizenzbestimmungen
- ↪ Schutz vor Raubkopien
- ▲ Konsequenz: private Rechner arbeiten unter der Policy eines Software- oder Content-Anbieters
- ▲ Verallgemeinerung:
 - ◆ Policy wird an Inhalte geknüpft um geistiges Eigentum zu schützen
 - Anwendungsszenarien in betrieblichen Geschäftsprozessen
 - Geschützter Austausch von Dokumenten (Schutz aber auch nur beschränkt möglich)