HSB
Hochschule Bremen
City University of Applied Sciences

Trusted Monitoring mit Hilfe eines TPMs durch das Trusted Attestation Protocol

Martin Müller
Matrikelnr.:358740
2. Oktober 2020

Kolloquium

Inhaltsverzeichnis

Aufgabenstellung

und Motivation

- TPMs überall verbaut
- Manipulationssicher
- kein Überblick über mehrere Geräte

$\Rightarrow$ Monitoring über der TPM mittels Remote Attestation

HSB
Hochschule Bremen
City University of Applied Sciences

Grundlagen

Trusted Platform Modul (TPM)

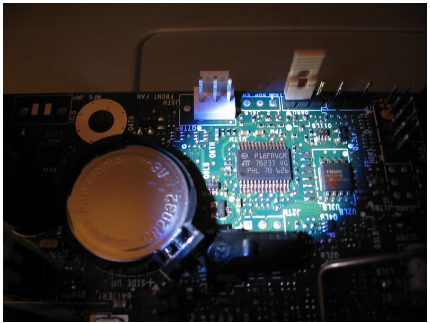


Figure: TPM on a DQ965GF Motherboard (flickr: Tyler Oderkirk)

Hardware Security Modul (HSM):

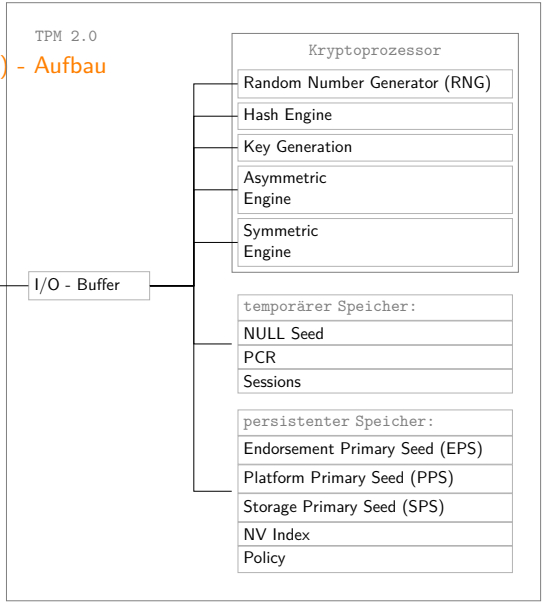
- Schlüsseln sicher vor Software aufbewahren
  z.B. Dateisystem, Memory-Dump

Besonderheit für TPM

- Smartcard dauerhaft im PC gelassen
- Security per Computer
  vs. per Person

Grundlagen

Trusted Platform Modul (TPM) - Aufbau



Grundlagen

Trusted Platform Modul (TPM) - Measured Boot

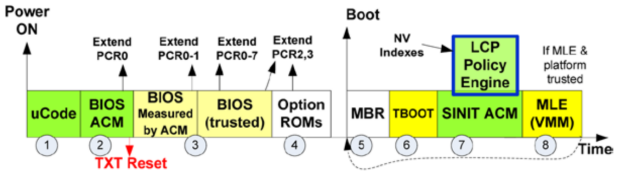


Figure: Intel TXT boot timeline (Figure 22-1 aus [ACG15, S. 336])

PCR-Bänke nur Extends oder Clean:

$$PCR_{new\_value} = Hash(PCR_{old\_value} || data)$$

Quote Nonce, Hash ausgewählten PCR-Werte und Signature

Grundlagen

Trusted Attestation Protokoll (TAP) - Einsatzmöglichkeiten

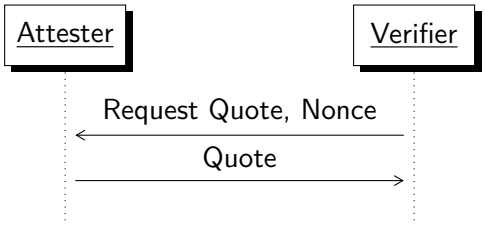


Figure: Sequenzdiagramm für Nonce vom Verifier (gekürzte Figure 1 aus [TCG-TAP1, S. 9])

- Zugang zum Netzwerk
- **Remeasurement**
- Unidirektion
- Sitzungloses

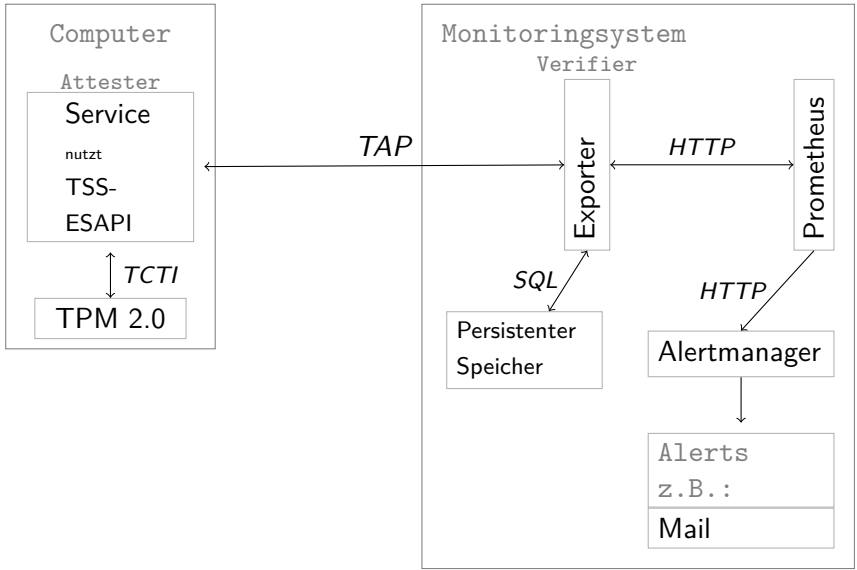
Grundlagen

Monitoringsystem

Datenerhebung	Push vs. Pull
Speicher der Daten	Dauer, Granularität
Visualisierung	Diagramme, Charts, Dashboards
Analytik und Reporting	KPIs und andere Businessfragen
Alerting	Kategorisieren von Alerts, Schwellwerte

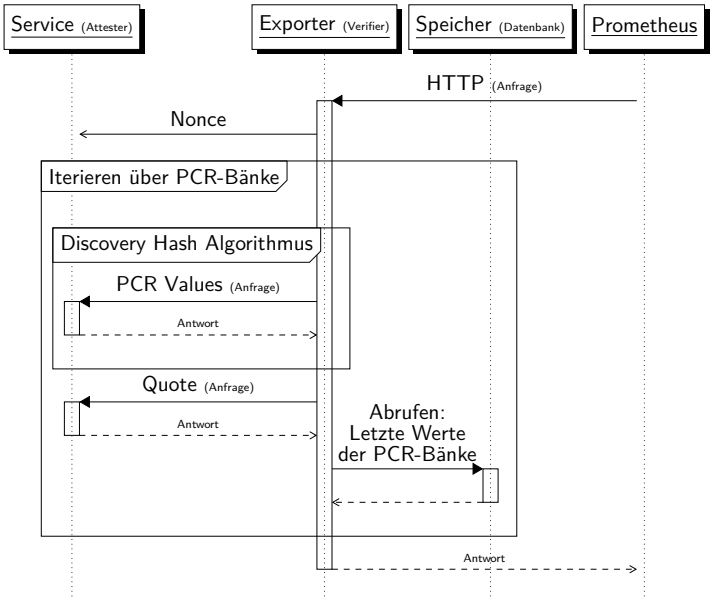
Konzept

Komponenten



Konzept

Ablauf



Konzept

Vorteile, Nachteile und Alternativen

Vorteile:

- hohe Datensparsamkeit
- Kontrolle über zeitliches Verhalten
- einfacher Attester

Alternativen für Nachteile:

Unidirektion und Sitzungloses
: bekannte Algorithmen und 3rd-Party Nonces

Algorithmus Discovery
: kleinester Nenner an Algorithmen

offenen Ports bei Attester
: Push-Monitoring

Implementierung

- TAP-Bibliothek mit Rust TSS ESAPI wrapper
- Folgende Komponenten:
  - TAP-Attester-Service
  - TAP-Verifier-Client (für Tests)
  - TAP-Verifier-Exporter

Zusammenfassung

- verbindungsorientiertes Netzwerkprotokoll
- vertrauenswürdiger Zufallszahlengenerator
- persistenter Speicher
- keine definitiertes Verhalten bei Fehlern

Fazit

und Ausblick

- optimieren des TAP-Attester-Service nach Performance
- TAP auch nutzen um Public Key des Attesters abzufragen.
- Sicherheitseinschätzung von Push- gegenüber Pull-Monitoring

Trusted Monitoring mit Hilfe eines TPMs
durch das Trusted Attestation Protocol

Vorführung

Trusted Monitoring mit Hilfe eines TPMs
durch das Trusted Attestation Protocol

Vielen Dank für Ihre Aufmerksamkeit

Fragen?

Quellen

Will Arthur, David Challener, and Kenneth Goldman. *A practical guide to TPM 2.0 : using the trusted platform module in the new age of security*. Berkeley, CA: ApressOpen, 2015. ISBN: 978-1-4302-6583-2. URL: https://link.springer.com/book/10.1007/978-1-4302-6584-9.

TCG. *Trusted Attestation Protocol (TAP) Use Cases - for TPM Families 1.2 and 2.0 and DICE*. Tech. rep. Version v1.00-r0.35. Nov. 5, 2019. URL: https://trustedcomputinggroup.org/wp-content/uploads/TCG_TNC_TAP_Use_Cases_v1r0p35_published.pdf (visited on 02/14/2020).