



# HSB

Hochschule Bremen  
City University of Applied Sciences

## Trusted Monitoring mit Hilfe eines TPMs durch das Trusted Attestation Protocol

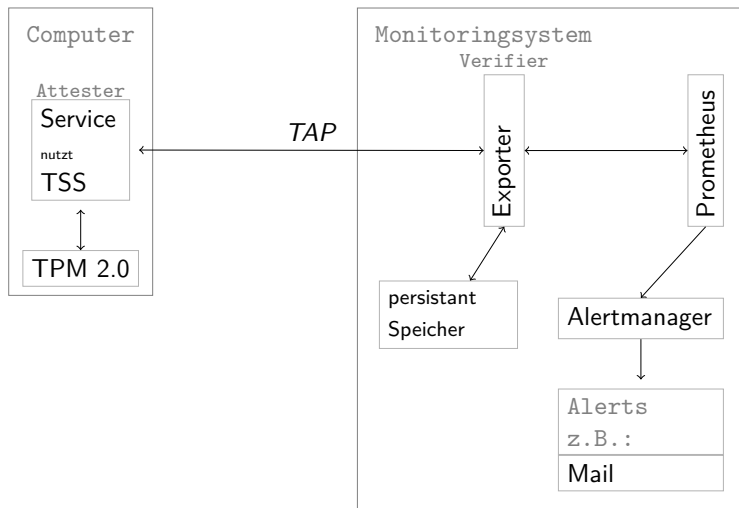
Martin Müller  
Matrikelnr.:358740  
29. Juni 2020

Masterseminar - Finalvortrag

# Inhaltsverzeichnis

- ① Trusted Platform Modul (TPM)
- ② Trusted Attestation Protokoll (TAP)
- ③ Monitoringsystem
  - Grundlagen
  - Trusted Monitoring

# Trusted Monitoring



# Idee vom TPM

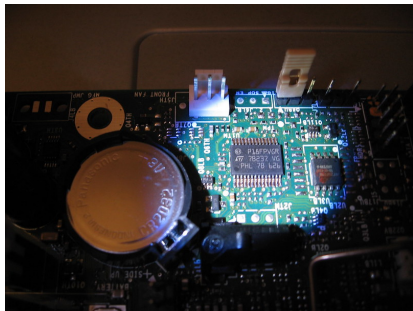
## Hardware Security Modul (HSM):

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

## Besonderheit für TPM

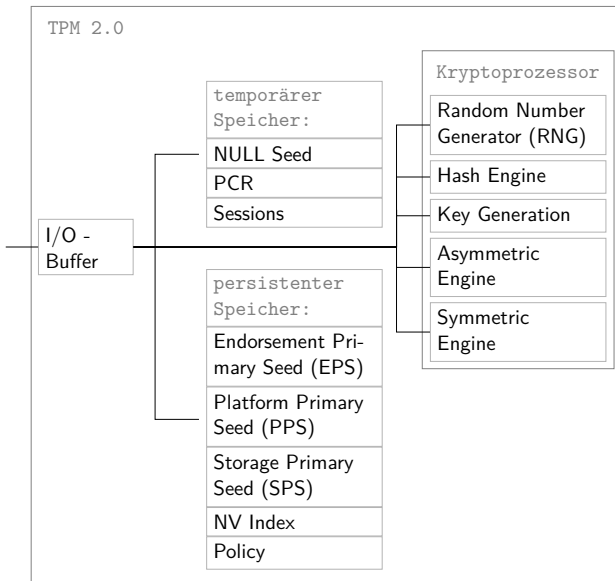
- Smartcard dauerhaft im PC gelassen
- Security per Computer  
vs. per Person

# Verbreitung des TPMs

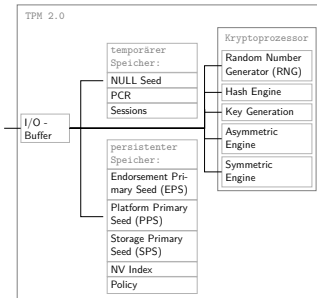


- Dank Microsoft und UEFI nun in fast allen Computern

# Aufbau des TPMs



# Aufbau des TPMs



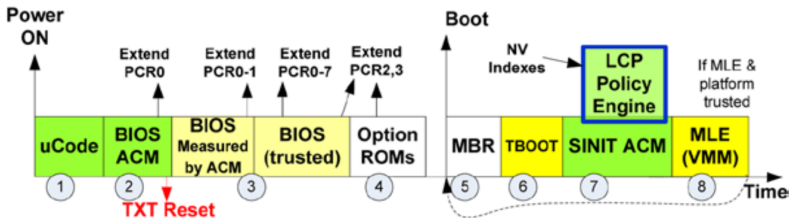
PCR-Bänke nur Extends oder Clean:

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

Quote PCR-Values + Nonce  
signiert

# Einsatzmöglichkeiten

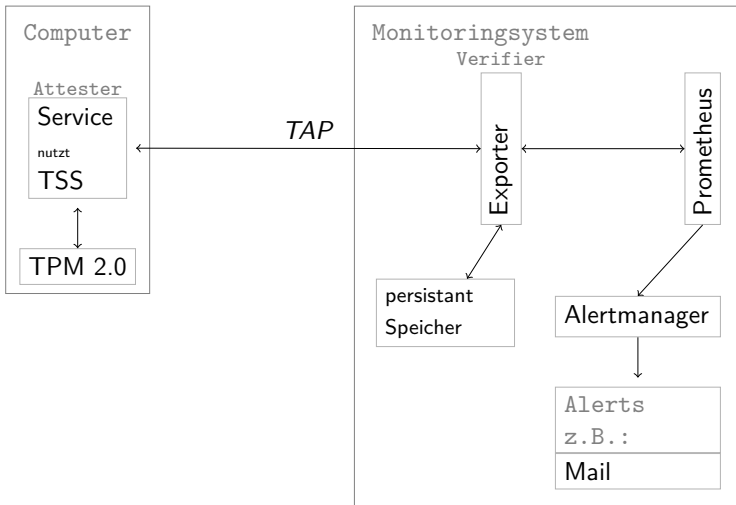
## Measured Boot





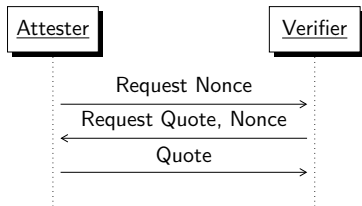
# Trusted Monitoring

## Trusted Attestation Protokoll (TAP)



# Trusted Attestation Protokoll (TAP)

## Einsatzmöglichkeiten



- Zugang (zum Netzwerk)
- **Remeasurement**
- Unidirektional
- Sitzungloses

# Monitoringsystem

## Grundlagen

Datenerhebung Push vs. Pull

Speicher der Daten Dauer, Granularität

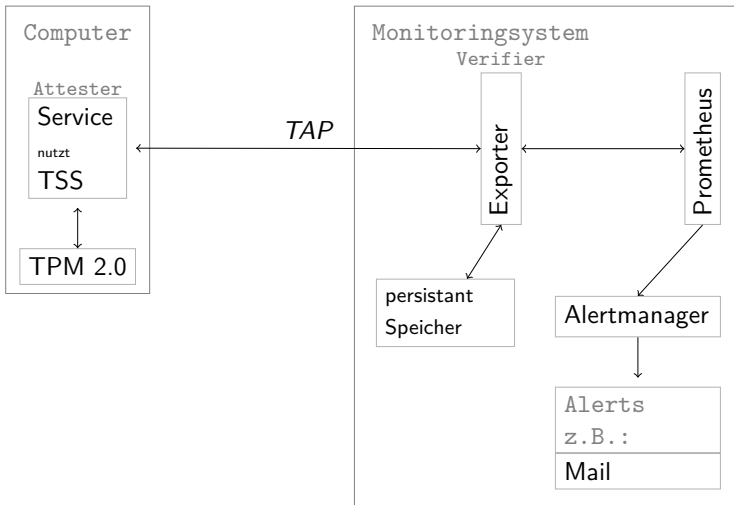
Visualisierung Diagramme, Charts, Dashboards

Analytik und Reporting KPIs und andere Businessfragen

Alerting Kategorisieren von Alerts, Schwellwerte

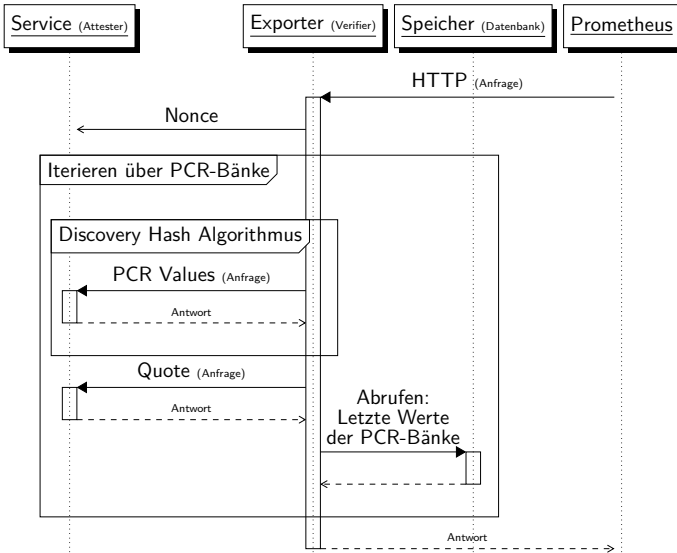
# Monitoringsystem

## Komponenten



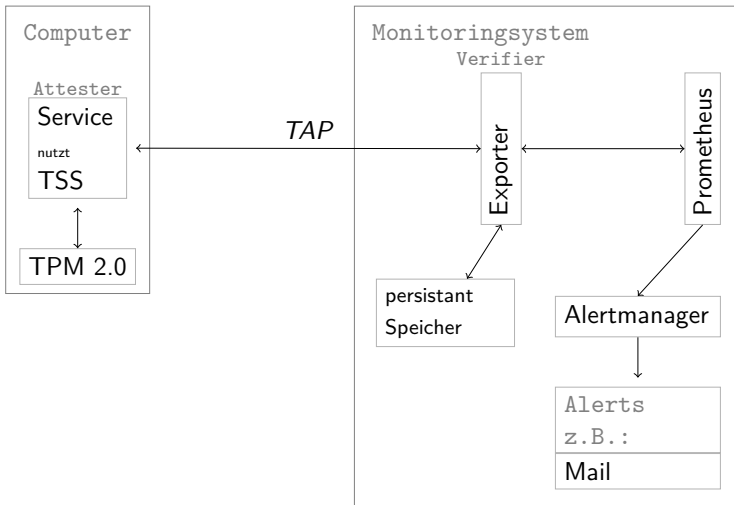
# Monitoringsystem

## Ablauf



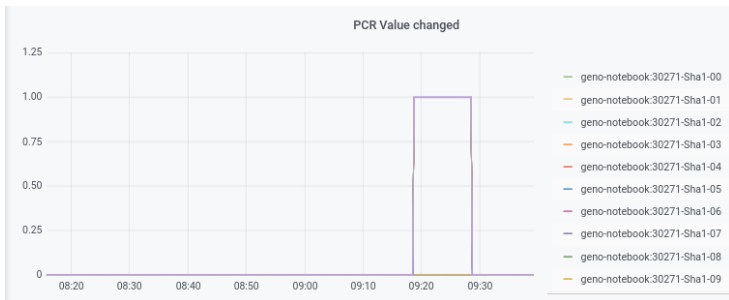
# Monitoringsystem

## Komponenten



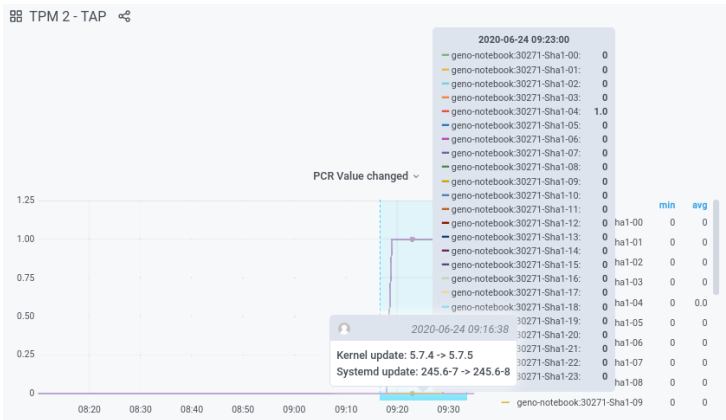
# Monitoringsystem

Hilfe der Computer verhält sich anders



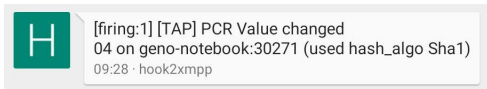
# Monitoringsystem

Es war ein Betriebssystemupdate





# Trusted Monitoring mit Hilfe eines TPMs durch das Trusted Attestation Protocol



Vielen Dank für Ihre Aufmerksamkeit

**Fragen?**

TPM im Browser zum Experimentieren:

<https://google.github.io/tpm-js/>

“Hacking (with) a TPM” von Andreas Fuchs:

[https://media.ccc.de/v/36c3-10564-hacking\\_with\\_a\\_tpm](https://media.ccc.de/v/36c3-10564-hacking_with_a_tpm)

# Quellen

## Trusted Computing Group

<https://trustedcomputinggroup.org/resources/>

## A Practical Guide to TPM 2.0

*Will Arthur, David Challener und Kenneth Goldman*

<https://rd.springer.com/book/10.1007/978-1-4302-6584-9>

## OSS implementation of the TCG TPM2 Software Stack (TSS)

<https://tpm2-software.github.io/>