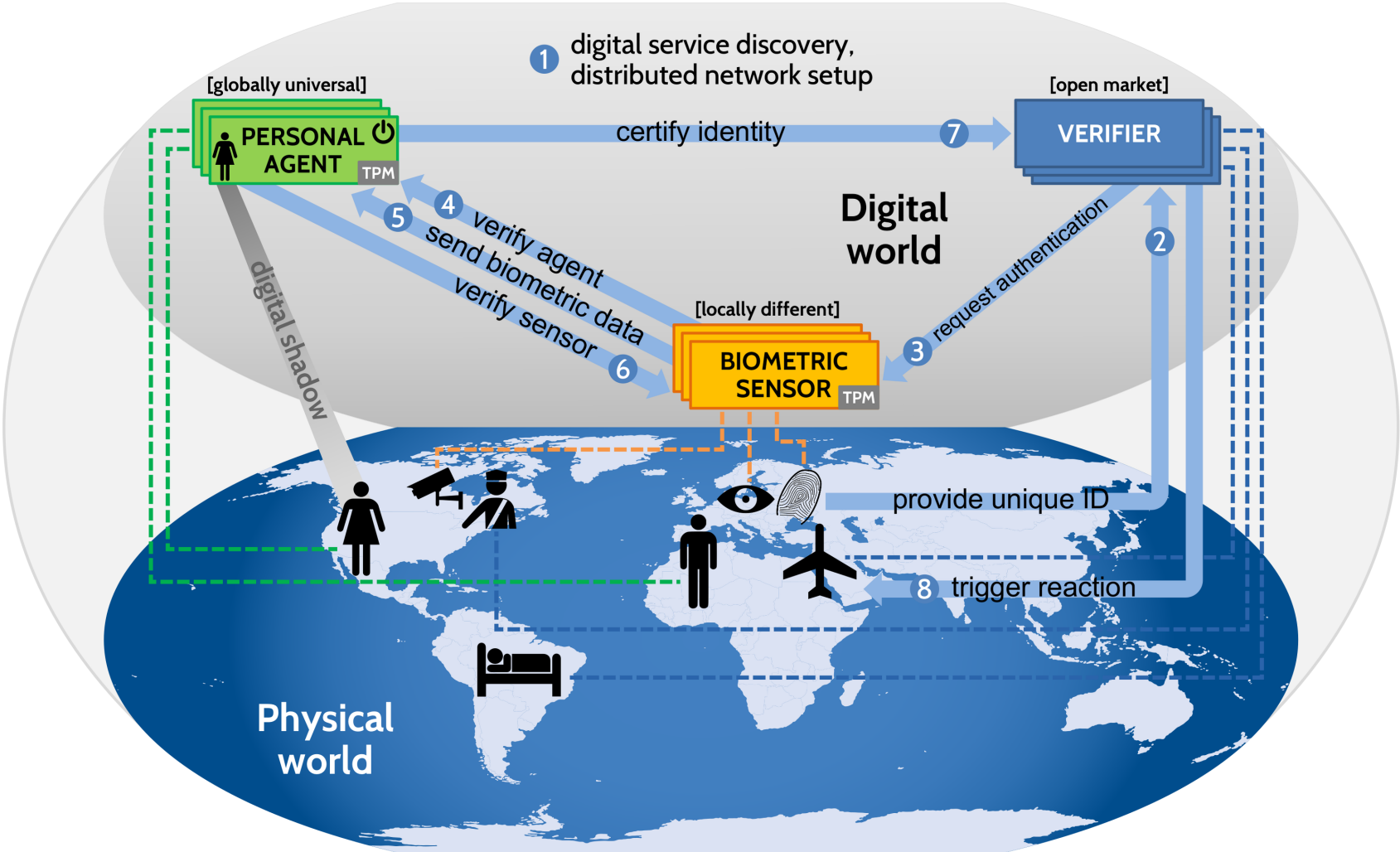
Digital Shadow: Biometric Sensor

Master's Thesis Seminar

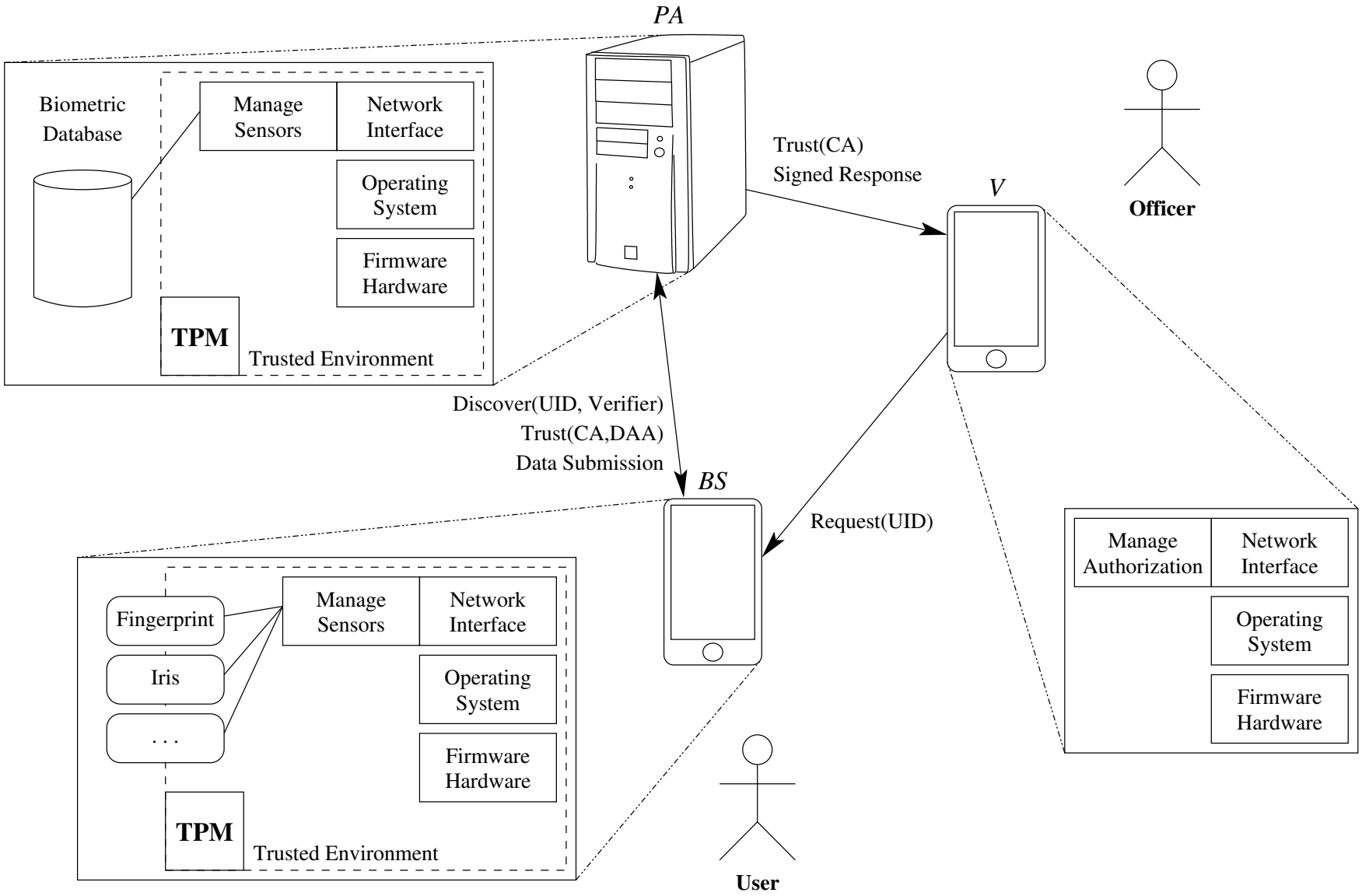
Michael Preisach

January 15, 2019

Project Overview Digital Shadow



Physical Overview



TPM2: Platform Configuration Registers (PCR)[1]

- 24 Registers (for the PC)
- represents state of measured unit
- reset only by power cycle
- SHA1 or SHA256
- modify by *Extend()*:

```
newPCR = Digest(oldPCR || data)
```

- extension chain possible

PCR	Allocation
0	BIOS
1	BIOS Config
2	Option ROM
3	Option ROM Config
4	MBR
5	MBR Config
6	State transition and wake events
7	Platform specific measurements
8-15	Static OS
16	Debug
17-22	General Purpose
23	Application Support

[1] Arthur, Challener: *A Practical Guide to TPM 2.0*

TPM2: Platform Configuration Registers (PCR)[2]

Component	measured by
BIOS	CRTM
TrustedGRUB MBR bootcode	BIOS
TrustedGRUB kernel (`diskboot.img`)	TrustedGRUB MBR bootcode
TrustedGRUB kernel (`core.img`)	`diskboot.img`
GRUB modules + OS	TrustedGRUB kernel
Applications	OS (e.g. Linux IMA)

[2] `https://github.com/Rohde-Schwarz-Cybersecurity/TrustedGRUB2`

Linux Integrity Measurement Architecture (IMA) [3] [4]

- Kernel extension for measuring accessed files
- configurable via policies (access mode, files, users, . . .)
- standardized log file entries
- extend PCR and create log file entry

[3] https://wiki.strongswan.org/projects/strongswan/wiki/IMA
[4] https://sourceforge.net/p/linux-ima/wiki/Home/

Attestation

1. hash a number of PCR values (= *Quote*)
2. sign hash with TPM key
3. remote party validates signing key
4. remote party validates values of PCRs
5. remote party validates values of (IMA-)Event log

State of the Project: What is Done

- small PC with dedicated TPM2 device
- installed GRUB-TPM2
- installed TPM2-ESAPI and development environment
- read most parts of the book *Trusted Computing Platforms - TPM2.0 in Context* and implemented basic examples

State of the Project: What is next

- solve remaining problems with GRUB-TPM2
- implementing more complex tasks with the TPM2
- understanding *Direct Anonymous Attestation* (DAA)
- define and develop a trusted environment between BS and PA

Questions

- IMA also works for other system calls?
- Details about CRTM