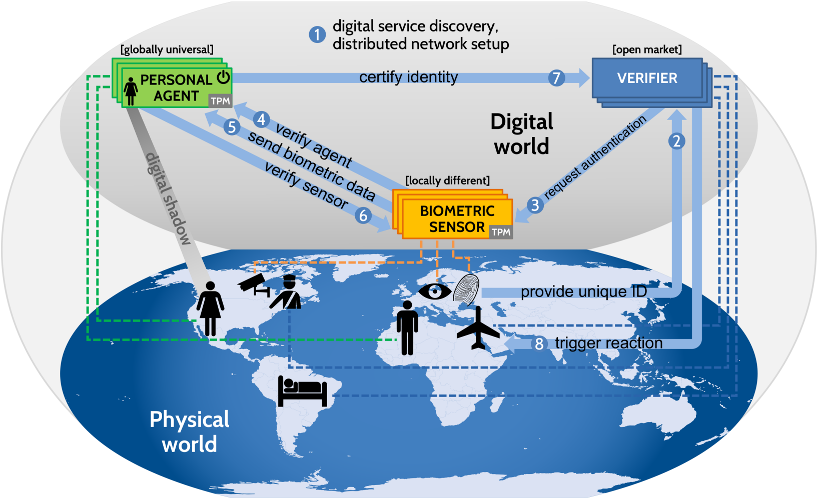
Digital Shadow: Biometric Sensor

Master's Thesis Seminar

Michael Preisach

November 19, 2019

Project Overview Digital Shadow



Recap: Trust inside Biometric Sensor

- manufacturer of TPM holds certificate
- TPM holds measurements of boot chain in PCR
  - CRTM measures BIOS
  - BIOS measures MBR/EFI Bootloader
  - bootloader measures Kernel (Grub 2.04 supports TPM2)
  - Kernel measures libs, executables, . . .
- TPM Quote: summarize the PCR state and sign it with TPM Endorsement Key (EK)

Problem: Create trust beween BS and PA

- network discovery
- **no Knowledge about BS**
  - **Hardware**
  - **Software**
  - **Am I talking to a valid BS**
  - Correct client to certify identity for given biometric data
- **BS faces same problem with PA**
- establish a secure channel to submit sensitive data

Solution: Direct Anonymous Attestation (DAA)

- based on group signatures
- Zero Knowledge Proof to verify group membership
- defines 3 Parties
  - Issuer: provides public key for a group (e.g. all Biometric Sensors) and manages group memberships
  - Member: holds a group private key to sign messages (e.g. a Biometric Sensor)
  - Verifier: knows the group public key and is able to verify correctness of signature (e.g. Personal Agent)
- used DAA is based on Elliptic Curves (ECDAA)