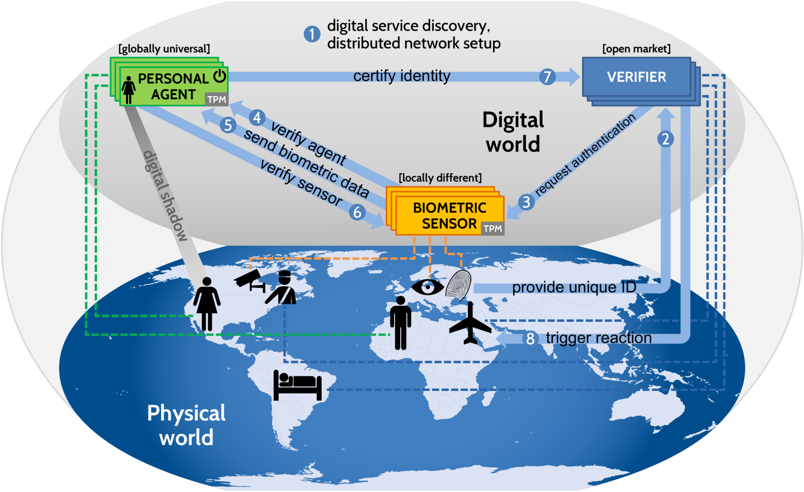
Digital Shadow: Biometric Sensor

Master's Thesis Seminar

Michael Preisach

April 21, 2020

Biometric Sensor as Part of Digidow



Threat Model

- Biometric Sensor (BS) point of view
  - Rogue Personal Identity Agent (PIA)
  - Metadata/Attribute Extraction on Network
  - Defects on Network - Discovery not working
  - Sensor data modification at sensor hardware (e. g. camera)
  - Physical manipulation of hardware
- Network/PIA point of view
  - Retransmission of sensor data
  - Blocking data transmission
  - Sensor data aggregation
  - Sensor data modification before transmission

Trusted Platform Module (TPM)

- Dedicated Cryptocoprocessor in the PC
- Toolset available for measurement, attestation, key management, ...
- Available Hierarchies: Storage, Endorsement, Platform, Null
- Platform Configuration Registers (PCR) for the state of the system[1]

PCR	Usage
0	UEFI boot and runtime services
1	SMBIOS, ACPI, ...
4	UEFI OS Loader
5	ESP, GPT
7	Unified Kernel
10	Integrity Measurements (by Kernel)

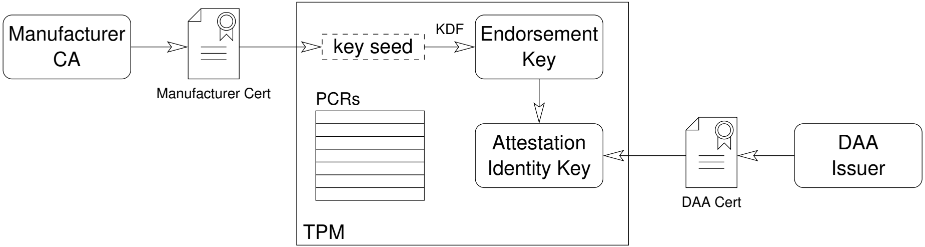
[1] https://www.trustedcomputinggroup.org/wp-content/uploads/PC-ClientSpecific_Platform_Profile_for_TPM_2p0_Systems_v21.pdf

Integrity Measurement Architecture[2]

- Compile options within the Linux Kernel
- When the Kernel starts, a large set of resources can be measured
  - files accessed by root
  - all executables run
  - shared libs and all other files held in memory
  - ...
- Based on policies, cooperates with selinux
- Creates Hash chain in PCR 10 (default)
  - new_hash = hash(old_hash | resource)
- integrity log lists measured resources, different file formats possible
- Attestation
  1. Create Attestation Identity Key (AIK) from the Endorsement Key
  2. Sign the current PCR value and the log with the AIK

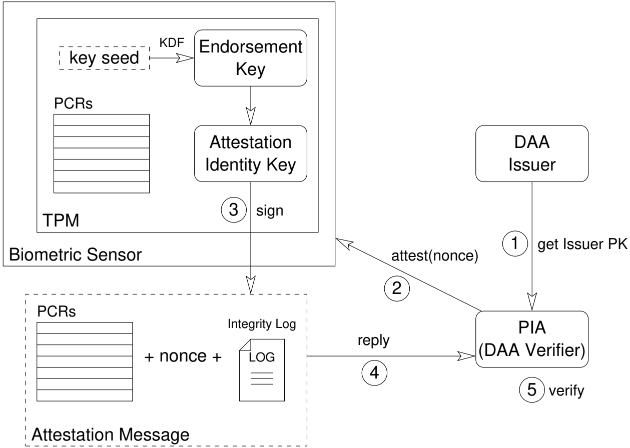
[2] https://wiki.gentoo.org/wiki/Integrity_Measurement_Architecture

TPM environment for DAA



- TPM can sign messages with the AIK
- The signature is proofable with the Issuer Public Key (zero knowledge proof)

DAA Verification



- Issuer Public Key is assumed known to any PIA
- Verifier (PIA) can only check validity of BS
- Only communication between PIA and BS
- Revocation lists manage termination of subscription

Mitigated Threats

- Biometric Sensor point of view
  - Rogue PIA Two way DAA? TBD
  - Metadata/Attribute Extraction on Network Cert based channel encryption? TBD
  - Defects on Network - Discovery not working Denial of Service
  - Sensor data modification at sensor hardware Firmware/Driver trust/attestation
  - Physical manipulation of hardware Trusted Bootchain
- Network/PIA point of view
  - Retransmission of sensor data Integrity Measurement/Trusted Software
  - Blocking data transmission Integrity Measurement/Trusted Software
  - Sensor data aggregation Integrity Measurement/Trusted Software
  - Sensor data modification before transmission Integrity Measurement/Trusted Software

State of the project

- Trusted Boot: ready, different flavors tested
- DAA: Basically working, Attestation Key not yet in TPM
- Integrity Measurement: ongoing, not running, policy design necessary
- Put above parts together
- Thesis: Theoretical concepts need to be written down
- Future work: minimize system, hardening on OS level