University of BRISTOL

Systems & Software Security

COMSM0050

2020/2021

University of BRISTOL

Trusted Platform Module

bristol.ac.uk

TPM (Trusted Platform Module)

- Trusted Computing Group
  - Microsoft, Intel, IBM etc…
- Promoting standard for more trusted computing
  - Additional chip on the motherboard
  - … called TPM
- Used for
  - Disk encryption
  - System Integrity
  - Password protection
  - … and more

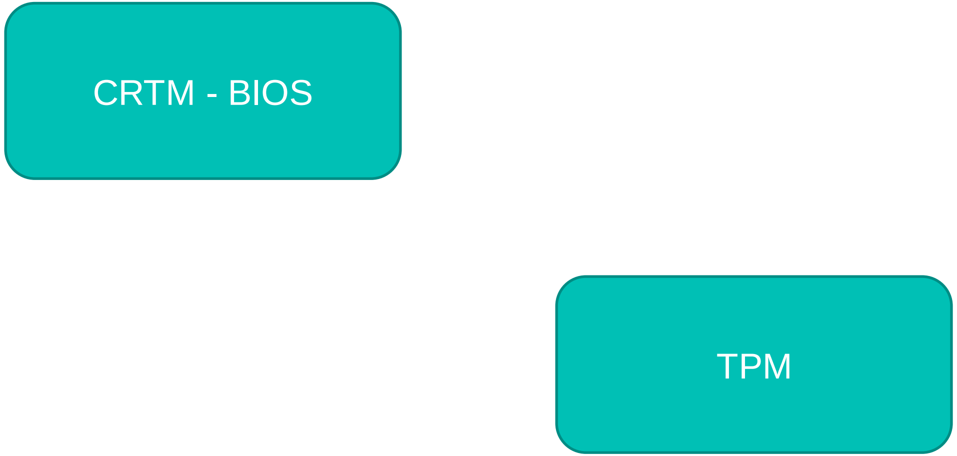
TPM (Trusted Platform Module)

- Trusted Computing Group
  - Microsoft, Intel, IBM etc…
- Promoting standard for more trusted computing
  - Additional chip on the motherboard
  - … called TPM
- Used for
  - Disk encryption
  - **System Integrity**
  - Password protection
  - … and more

Requirements

- We can achieve trust if we can verify the system has booted correctly
- We assume the PC hardware has not been modified
  - Key function is in the hardware TPM
- We need to monitor the boot process
  - Initial boot measure by the "Core Root of Trust" (ROM)
  - Hash the BIOS, store results in TPM, start the BIOS
  - BIOS do its job, load the next stage, hash it store in TPM etc…

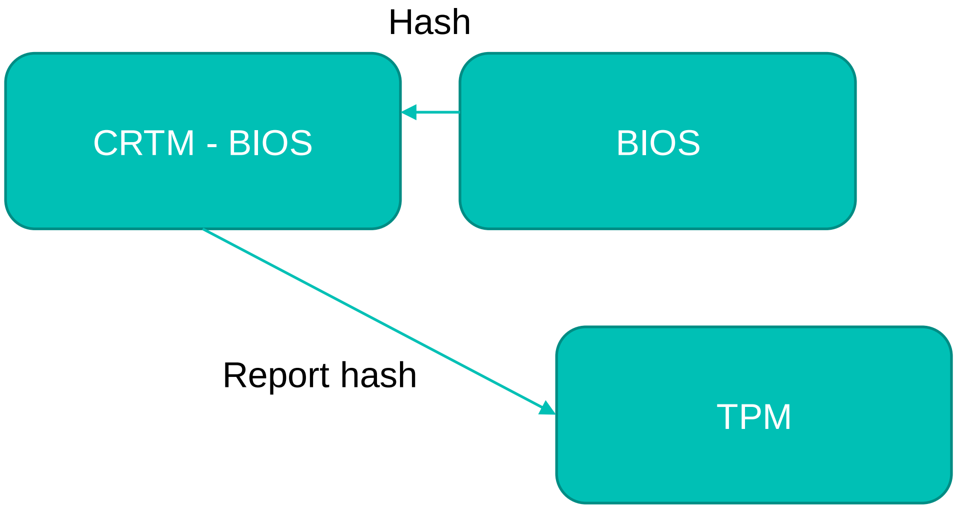
Authenticated Boot



CRTM - BIOS

TPM

Authenticated Boot



Hash

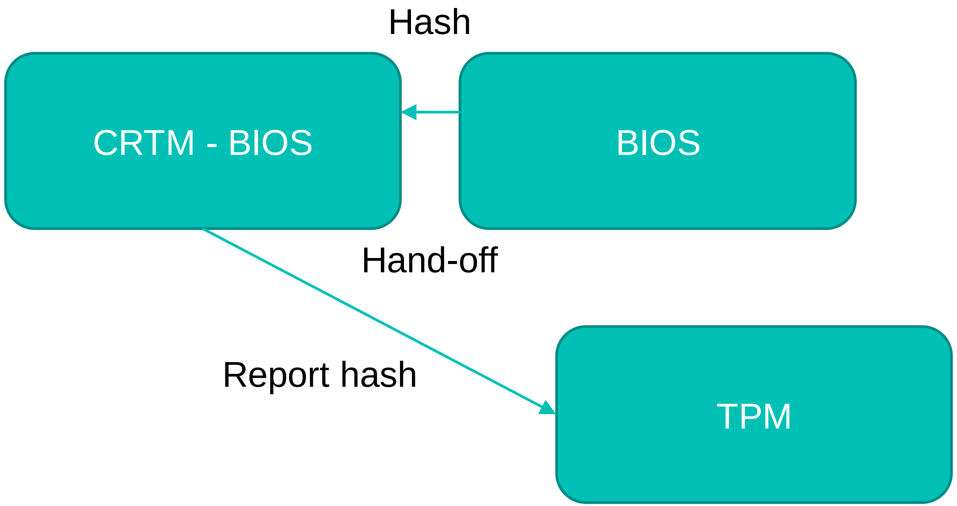
CRTM - BIOS

BIOS

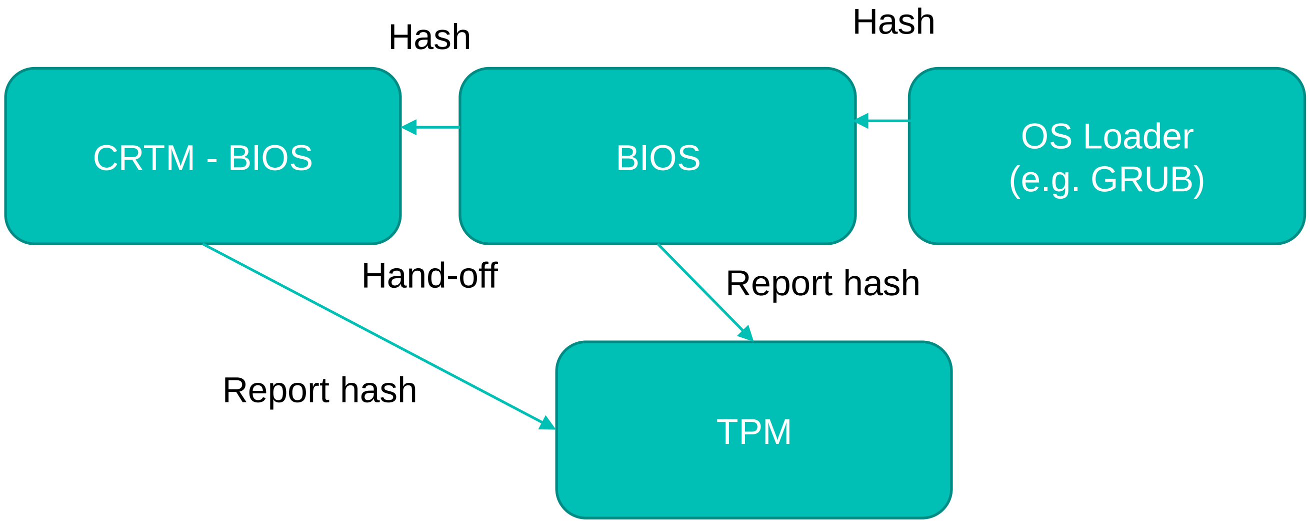
Report hash

TPM

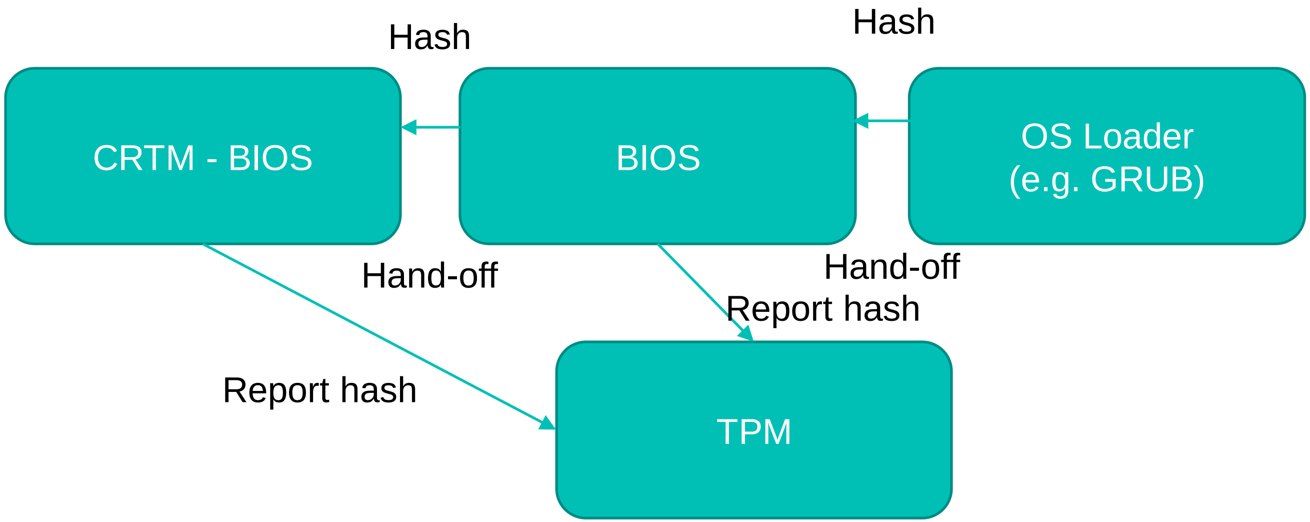
Authenticated Boot



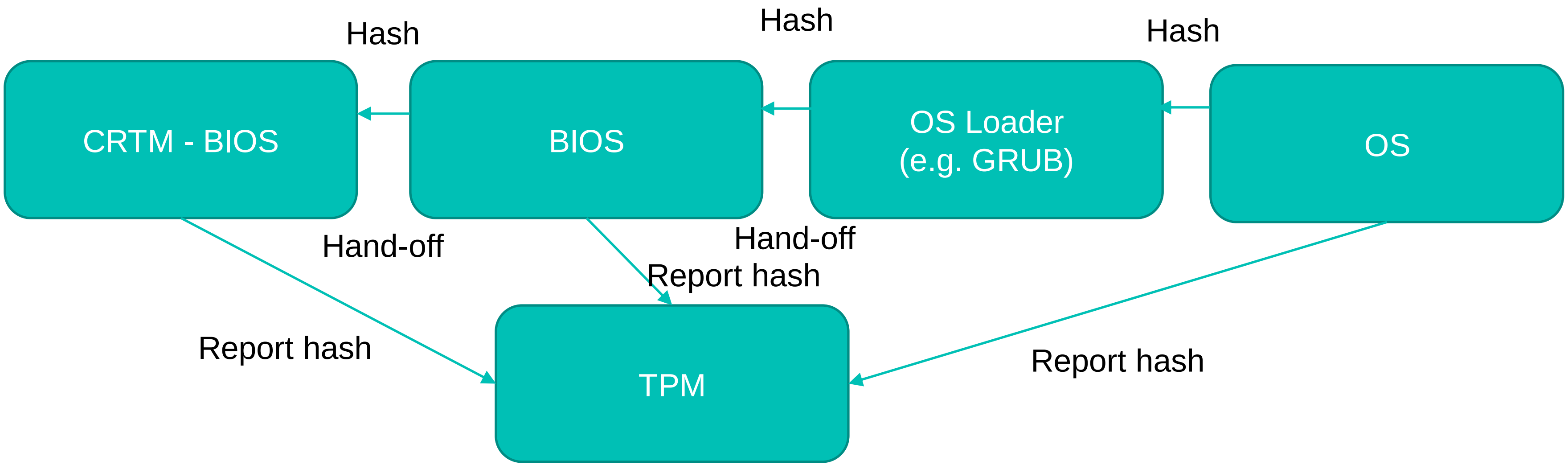
Authenticated Boot



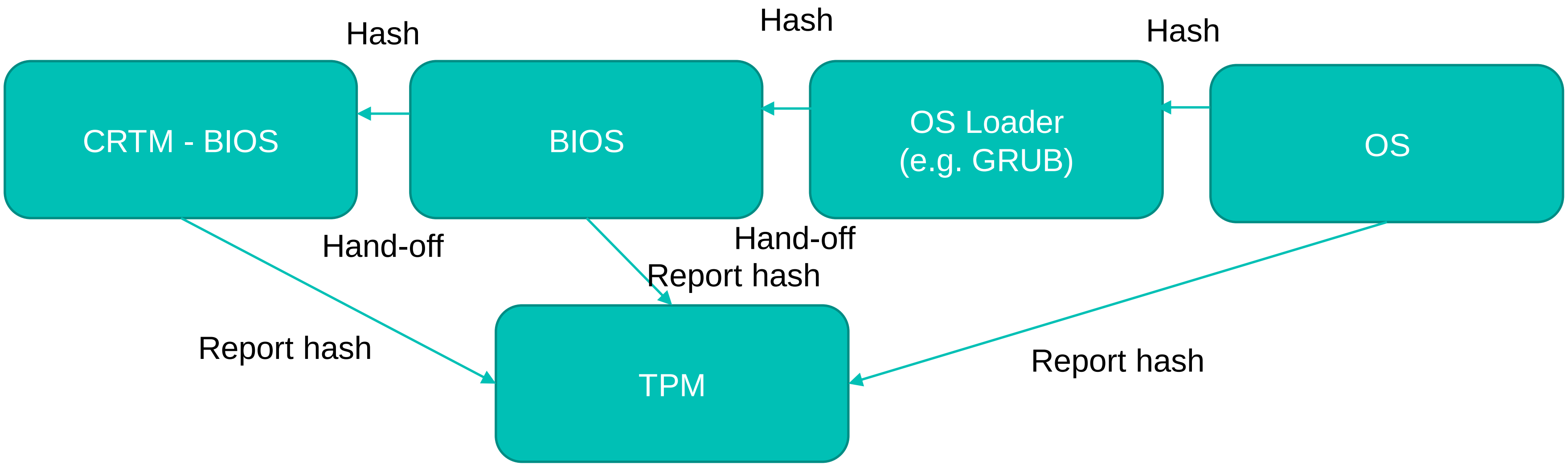
Authenticated Boot



Authenticated Boot



Authenticated Boot (simplified)

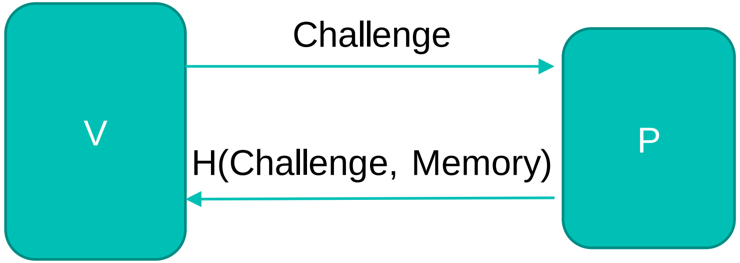


TPM registers

- Platform configuration registers (PCRs)
  - Used to store platform integrity metrics
- A PCR hold a summary of a series of value
  - Not the entire chain of hash
  - The chain can be infinite
- A PCR register is extended
  - PCR = HASH(PCR | new measurement)
  - Shielded TPM location (i.e. cannot be modified from outside)
  - Measurement are provided by software

Remote attestation

- Untrusted prover “P” and trusted verifier V
- V knows P expected memory content
- V send challenge with a nonce to P
- P compute a measurement
- V verify the measurement



What remote attestation tells you

- Positive result
  - Correct memory content
  - Good device
- Negative result
  - Malfunctioning device
  - Malicious device
- No response
  - Malfunctioning device
  - Malicious device

TPM and Remote Attestation

- PCR cannot be modified
  - Only reset at reboot
- TPM contains a key used to sign the attestation
- Verifier
  - Verify the TPM certificate/key
  - Verify the PCRs
- Attestation
  - PCRs value
  - sign(PCRs, challenge[nonce])

TPM and Remote Attestation

- You need not to stop at the OS
  - Can attest kernel modules (e.g. drivers)
  - Applications?
  - Configurations?
  - Scripts?
  - Where to stop?
  - Problem with load order? (remember it is a chain)
- Check IMA paper on course website
  - Linux implementation by IBM

University of BRISTOL

Limitations?

Static Root of Trust problem

- Verifies only static information
  - Code at loading time
- Long running application
  - Do we reboot the system to do a sensitive operation?
- Runtime status of a device is not known
  - Attacker can compromise a system during execution
- Reboot not sufficient
  - iPhone has secure boot
  - … so only safe code is executed
  - yet permanent jailbreak
  - Configuration file loaded during boot exploit a vulnerability…
  - … solution verify configuration? Then configuration cannot change?