The Trusted Platform Module (TPM)

Architecture and Applications

Egil Martinsen
www.nsm.stat.no

The TCG and the TPM

- What is a Trusted Platform Module (TPM)?
  - Tamper resistant device used to provide a basis of a secure computing environment
  - Many manufacturers: Broadcom, Infineon, Atmel...
- Who makes the specification?
  - The Trusted Computing Group (TCG)
- Assurance requirement 6 in Orange book:
  - The trusted mechanisms that enforce the basic requirements must be continuously protected against tampering and/or unauthorized changes.

TPM Architecture basics

- Three basic features provided by the trusted platform [1]:

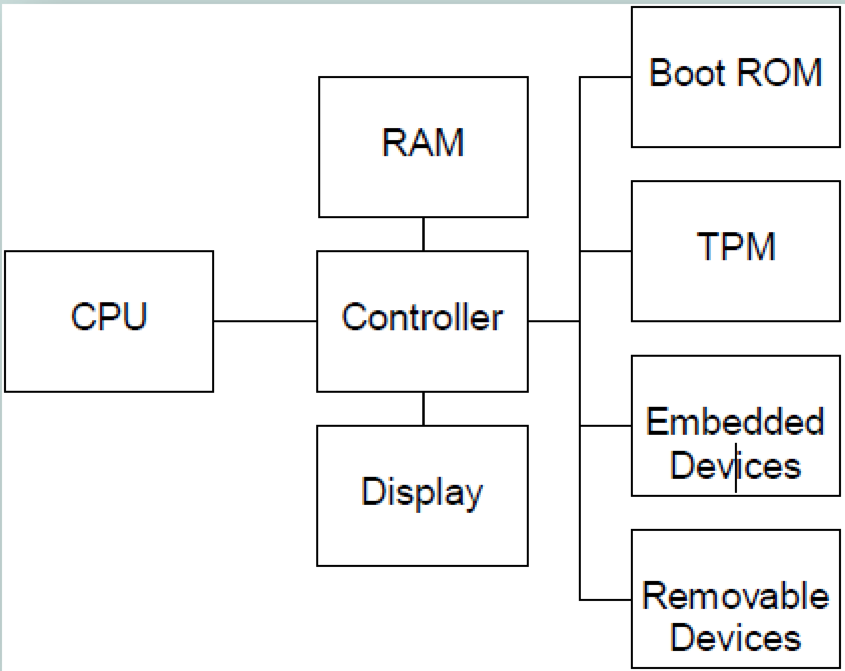
1. Protected Capabilities
    - *”Set of commands with exclusive permission to access shielded locations”*
        - Relates to Orange book’s ”System Architecture” requirement (C2)
2. Integrity Measurement, Logging and Reporting
    - *”Measurement is the process of obtaining metrics of platform characteristics that affect the integrity”*
        - Relates to Orange book’s ”System Integrity” requirement (C2)
    - *”Logging is storing of integrity metrics in a log for later use”*
        - Relates to Orange book’s ”Audit” requirement (C2)
    - *”Integrity reporting is the process of attesting to integrity measurements”*
        - Relates to Orange book’s ”System Architecture” requirement (C2)
3. Attestation
    - *”Attestation is the process of vouching for the accuracy of information”*
        - Relates to Orange book’s “Identification and Authentication” requirement (C2)

TCG Platform Specifications

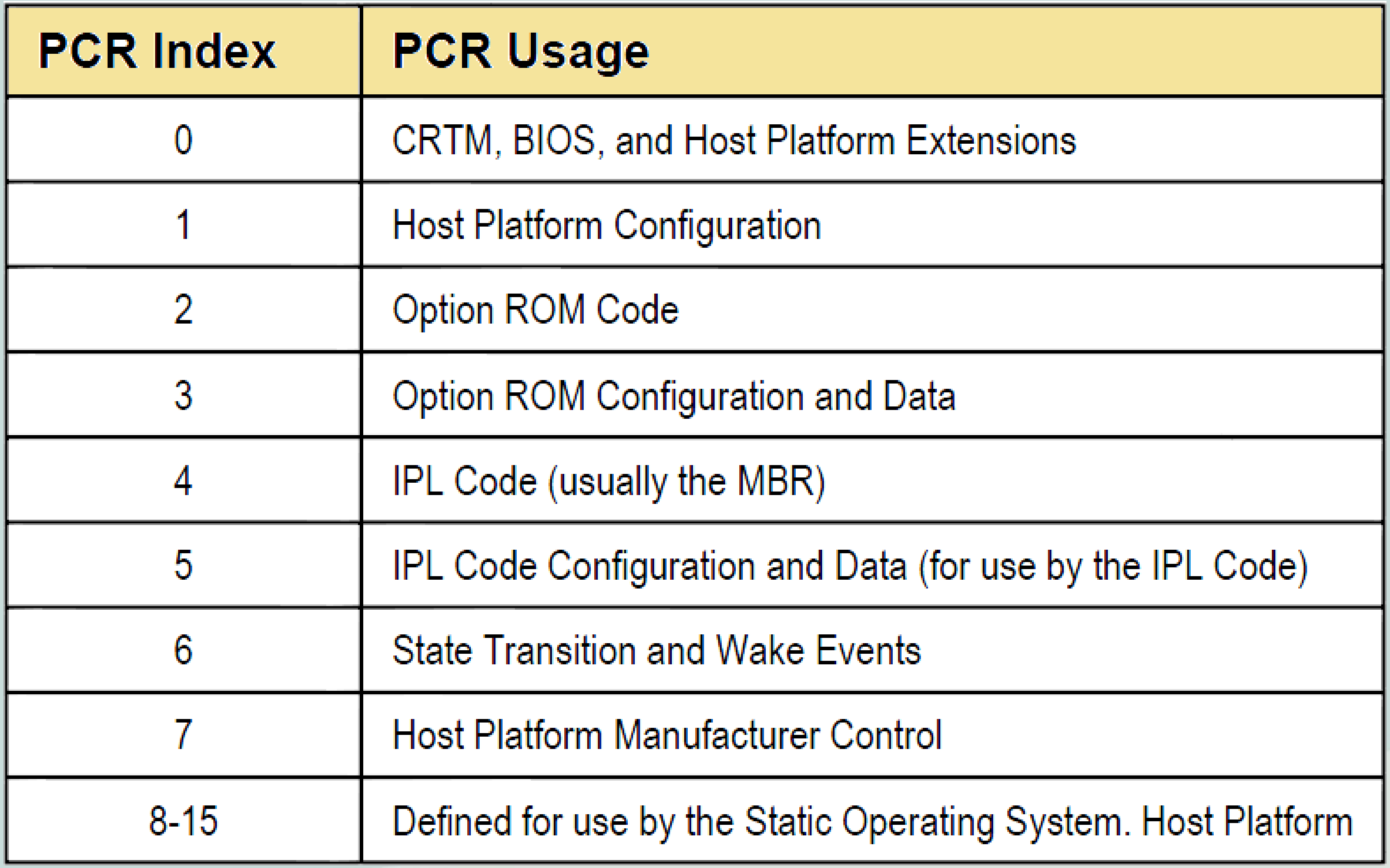
- Mobile phones and PDA’s
- Servers
- Storage
- PC Clients

TPM in PC Clients

- The TCG referance architecture for PC Clients

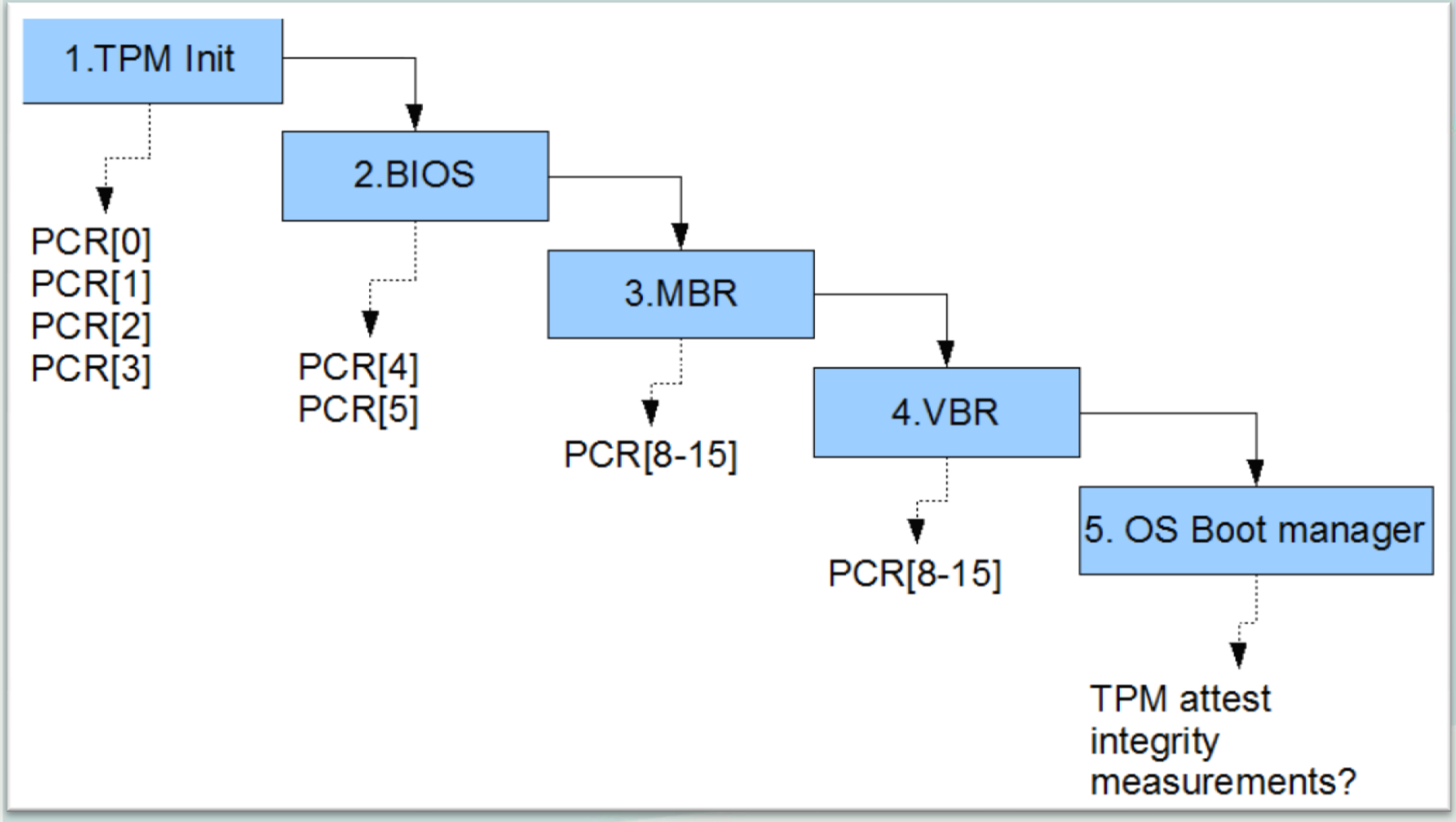


TPM Registers used in Integrity Measurement



PCR Index	PCR Usage
0	CRTM, BIOS, and Host Platform Extensions
1	Host Platform Configuration
2	Option ROM Code
3	Option ROM Configuration and Data
4	IPL Code (usually the MBR)
5	IPL Code Configuration and Data (for use by the IPL Code)
6	State Transition and Wake Events
7	Host Platform Manufacturer Control
8-15	Defined for use by the Static Operating System. Host Platform

Secure Boot with the TPM



TPM Sealing

- Sealing = Access to data is controlled by the state of the platform
- Definitions
  - PK = TPM public key
  - SK = TPM private key
  - DK = Drive encryption key
- After ”fresh” OS install:
  1. Encrypt drive using symmetric algorithm with key DK
  2. *TPM_Seal* (DK, state of PCR registers) -> Creates a datablob encrypted with PK. Datablob stored on harddrive
- At **5. OS Boot manager**:
  - *TPM_Unseal*(datablob) -> Pseudocode executed inside TPM:
    1. Decrypt datablob using SK
    2. If (state of PCR registers == state of PCR registers in datablob), release DK to OS Boot manager

References

- [1] – TCG Architectural Overview
  https://www.trustedcomputinggroup.org/groups/TCG_1_4_Architecture_Overview.pdf
- [2] – TCG PC Client Specific TPM Implementation Specification for Conventional BIOS
  https://www.trustedcomputinggroup.org/groups/pc_client/TCG_PCClientTPMSpecification_1-20_1-00_FINAL.pdf
- [3] - TCG Glossary of Technical Terms
  https://www.trustedcomputinggroup.org/groups/glossary/
- [4] – Bitlocker Drive Encryption, Powerpoint presentation by Jean Gautier @ Microsoft

- TPM Chip picture on slide 2: http://www.infineon.com/cms/media/press/Image/press_photo/TPM_SLB9635TT.jpg
- Specifications pictures on slide 4: https://www.trustedcomputinggroup.org
- Architectural picture on slide 5 and PCR usage picture on slide 6: [2]