ISEL
INSTITUTO SUPERIOR DE
ENGENHARIA DE LISBOA

Cibersegurança

- Trusted Computing
- Trusted Platform Module (TPM)

ISEL – Instituto Superior de Engenharia de Lisboa
Rua Conselheiro Emídio Navarro, 1 | 1959-007 Lisboa

Computer security

Branches

- Protection of systems against external attacks
  - Includes all methods that are used by system owners against external attackers (e.g. Firewalls, IDS, IPS etc).
  - The system owner installs software that uses its own means to determine if a remote user is malicious and (hopefully) terminates the attack

Computer security

Branches

- Protection by the system owner against internal users
  - Includes prevention of users to read each other’s data, use more than their allotted share of resources, etc.
  - All password protection and used management software are included in this branch. Also, to some extent, anti-virus/anti-spam software is included here.

Computer security

Branches

- Protection against the current owner (or possessor) of the machine
    - Involves the verification of a remote host that the user machine will behave in a certain predictable way.
    - Also, ensuring that the system is not inspected nor that the software running on it neither the data that it holds are stolen.
    - The “attacker” is not limited to some attack surface that was exposed to him but can also use a soldering iron to tap into busses, replace chips and other system parts, etc.

Computer security

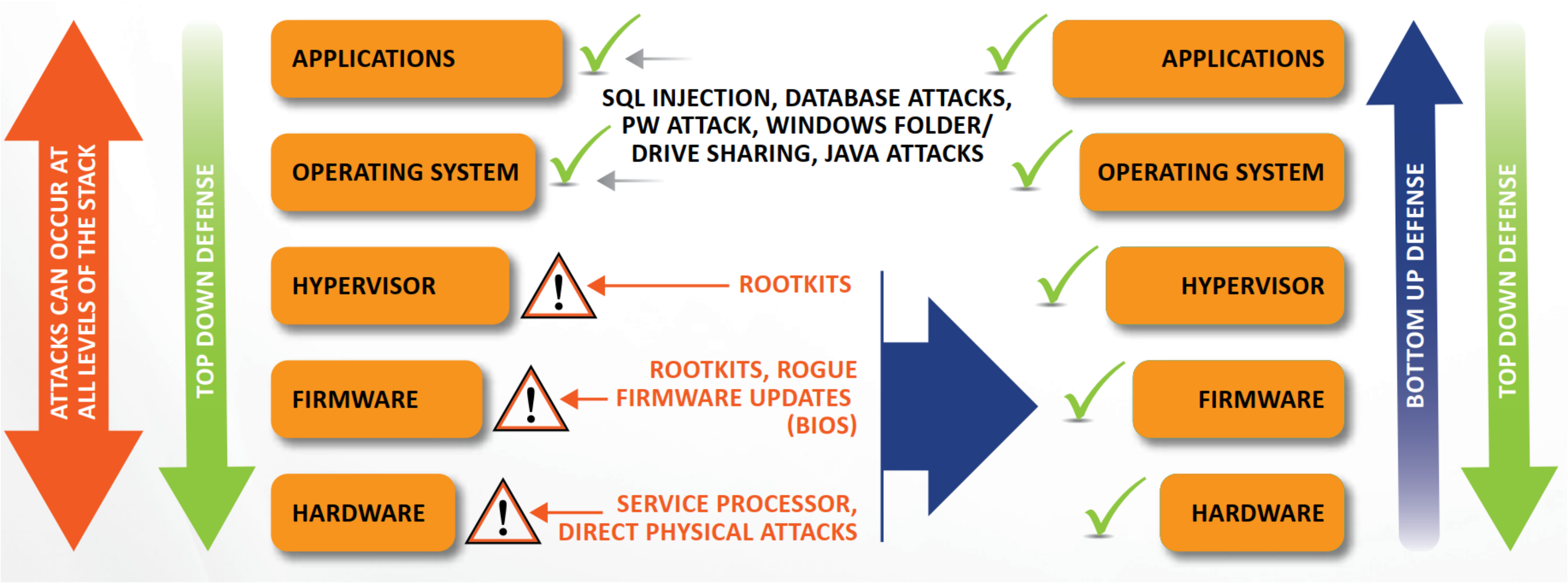
Trusted computing

- Aims to the development of technologies that give users guarantees about the behavior of the software running on their devices.
  - This means that even when an attacker gains control of the system, he cannot make it misbehave.
- No software-only solution can provide such guarantees, as an attacker can always manipulate software if the OS is not trusted.
- It is much harder for an attacker to modify hardware functionality, which is why a user’s trust is said to be rooted in the hardware.
  - To some extent, hardware can be considered immutable.

Computer security

Trusted computing

- Bottom-up security approach


ATTACKS CAN OCCUR AT ALL LEVELS OF THE STACK
TOP DOWN DEFENSE
APPLICATIONS
OPERATING SYSTEM
HYPERVISOR
FIRMWARE
HARDWARE
SQL INJECTION, DATABASE ATTACKS, PW ATTACK, WINDOWS FOLDER/ DRIVE SHARING, JAVA ATTACKS
ROOTKITS
ROOTKITS, ROGUE FIRMWARE UPDATES (BIOS)
SERVICE PROCESSOR, DIRECT PHYSICAL ATTACKS
APPLICATIONS
OPERATING SYSTEM
HYPERVISOR
FIRMWARE
HARDWARE
BOTTOM UP DEFENSE
TOP DOWN DEFENSE

Computer security

Trusted computing vocabulary

- Trust (*Trusted Computing Group*'s working definition)
  - "An entity can be trusted if it always behaves in the expected manner for the intended purpose."

Computer security

Trust

- Is about how you use something.
- A system can be trusted if it always behaves in the expected manner for the intended purpose.

  Even when an attacker gains control of the system (it cannot misbehave).
- Users are given no guarantees that the trusted components will not breach their security policies.

Trustworthy

- Is about whether it is safe to use something.
- Users are asked to trust a set of components, and the security of the system is no longer guaranteed if any of its components are breached.
- Provides users with proof that its trusted componentes will not violate security.

Computer security

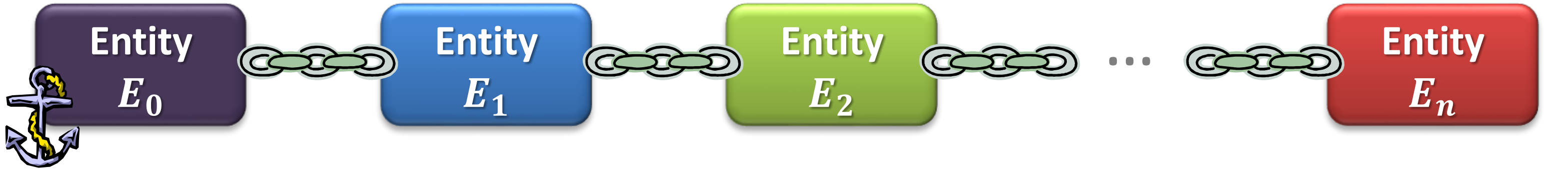
Trusted computing vocabulary

- Trusted Computing Bases (TCBs)
    - The sets of hardware and software components which are critical to the architecture’s security.
    - The components of the TCB are designed so that, when other parts of the system are exploited, they cannot make the device misbehave.
    - Ideally, a TCB should be as small as possible in order to guarantee its correctness.
        - To keep the TCB as small as possible, most trusted computing technologies build trust chains.

Computer security

Trusted computing vocabulary

- Trust Chains
  - Are formed by verifying each component's (E_i) validity from the bottom up.
    - For software, this can be done by measuring each component in the chain before its execution.
    - For hardware, this can involve checking whether the signature of the platform components has changed, i.e. whether one of the components has been modified or even removed or replaced.
  - Always need to be anchored in a component that is inherently trusted (E_0), which is referred to as Root of Trust (RoT).



Computer security

Trusted computing vocabulary

- Measuring
  - Used to verify the authenticity of software components.
  - This is done by calculating a hash or Message Authentication Code (MAC) of its code and data.
    - Some designs also include other identifying information, like the memory layout.
  - The measurement result is used to attest the component’s state.
  - Since a hash or MAC value for a given input is probabilistically unique, it also identifies the state of the software component at that time.
  - Who measures E0?
    - Must be trusted, because there is no mechanism to measure the RoT!

Computer security

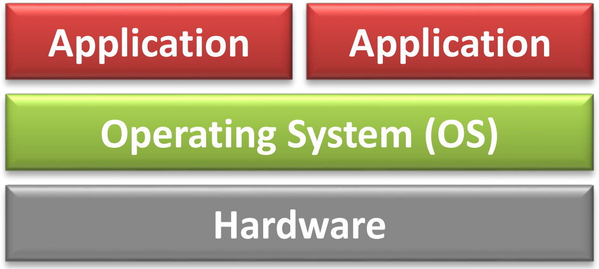
Trusted computing vocabulary

- Attestation
  - The process of proving to an authorized party that a specific entity is in a certain state.
  - In order to give strong security guarantees, an architecture which supports attestation should guarantee integrity of the attested state as well.
  - Trusted computing architectures may provide local and remote attestation:
    - Local refers to one software module attesting its state to another running on the same platform;
    - Remote refers to attesting to a remote party residing outside the trusted system.
  - A common way to implement attestation is to measure software modules during their initialization, while preventing later modifications by means of isolation.

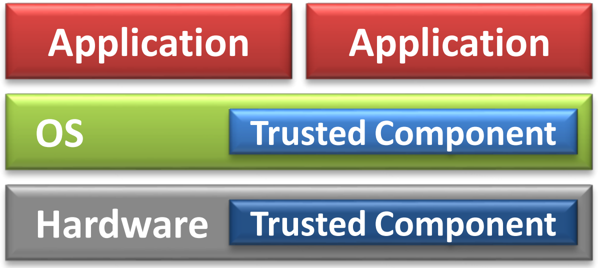
Computer security

Trusted platform :: Basic idea

- Trusted components in hardware and software
- Provides a variety of trusted functions
  - Set of cryptographic and security functions
  - Creates a foundation of trust for software
- Provides hardware protection for sensitive data
  - Keys, counters, random number generators, etc.
- Desired goals in practice
  - Trusted Computing Base (TCB) should be minimized
  - Compatibility to commodity systems



Conventional Platform



Trusted Platform

Computer security

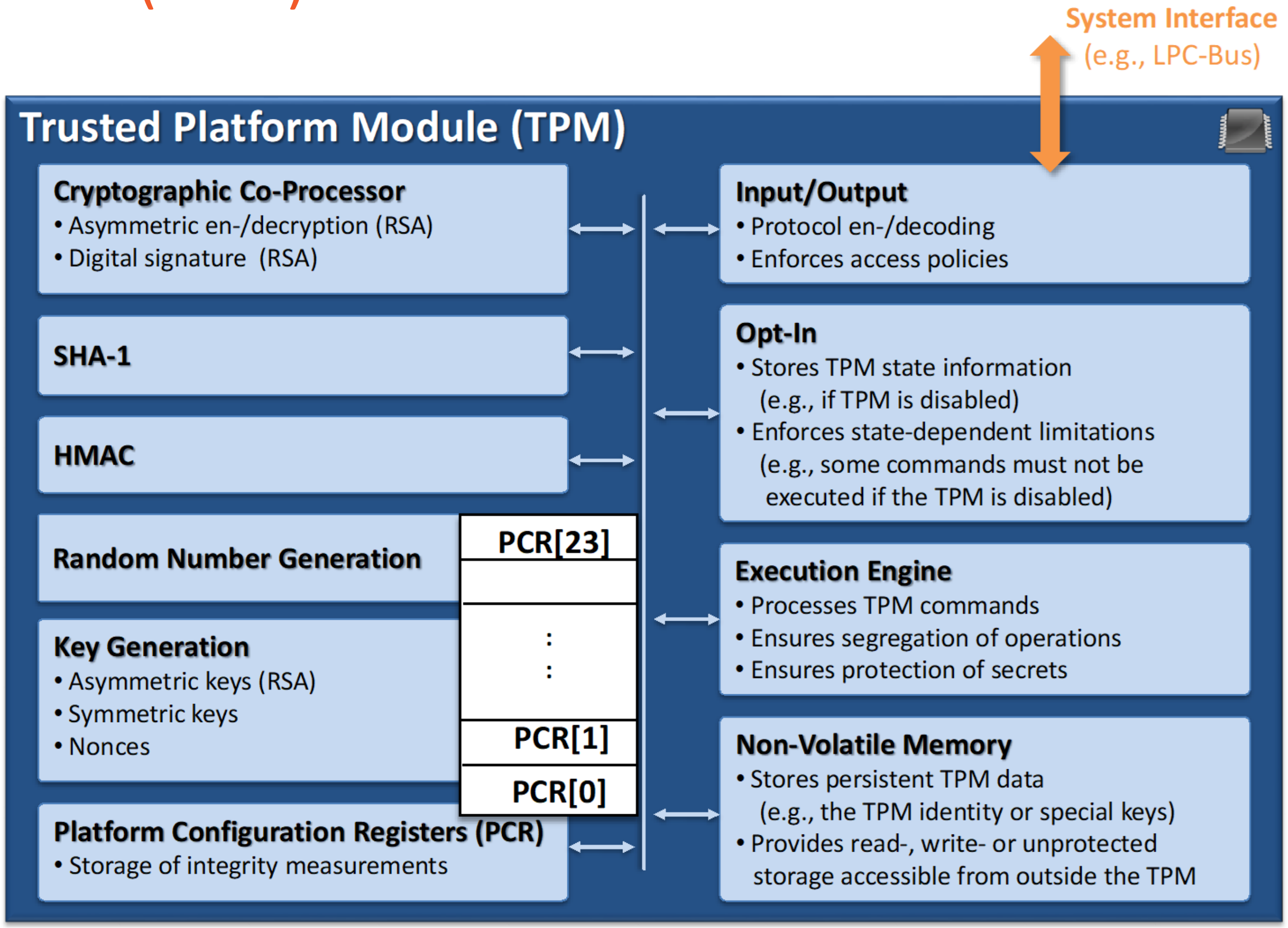
Trusted Platform Module (TPM)

- Specified by the Trusted Computing Group (TCG) in 2011 (v1.2)
- A cryptographic coprocessor capable of
  - Computing several cryptographic functions
  - Generating and storing keys
  - Performing attestation.
- Added to the computer motherboard and connected to the CPU using the Low Pin Count (LPC) Bus
- Provides limited protection against physical attacks
  - The CPU package, the TPM chip and all connecting buses are part of the TCB

Computer security

Trusted Platform Module (TPM)

- Architecture



System Interface
(e.g., LPC-Bus)

Trusted Platform Module (TPM)

Cryptographic Co-Processor

- Asymmetric en-/decryption (RSA)
- Digital signature (RSA)

SHA-1

HMAC

Random Number Generation

Key Generation

- Asymmetric keys (RSA)
- Symmetric keys
- Nonces

PCR[23]

:
:

PCR[1]

PCR[0]

Platform Configuration Registers (PCR)

- Storage of integrity measurements

Input/Output

- Protocol en-/decoding
- Enforces access policies

Opt-In

- Stores TPM state information (e.g., if TPM is disabled)
- Enforces state-dependent limitations (e.g., some commands must not be executed if the TPM is disabled)

Execution Engine

- Processes TPM commands
- Ensures segregation of operations
- Ensures protection of secrets

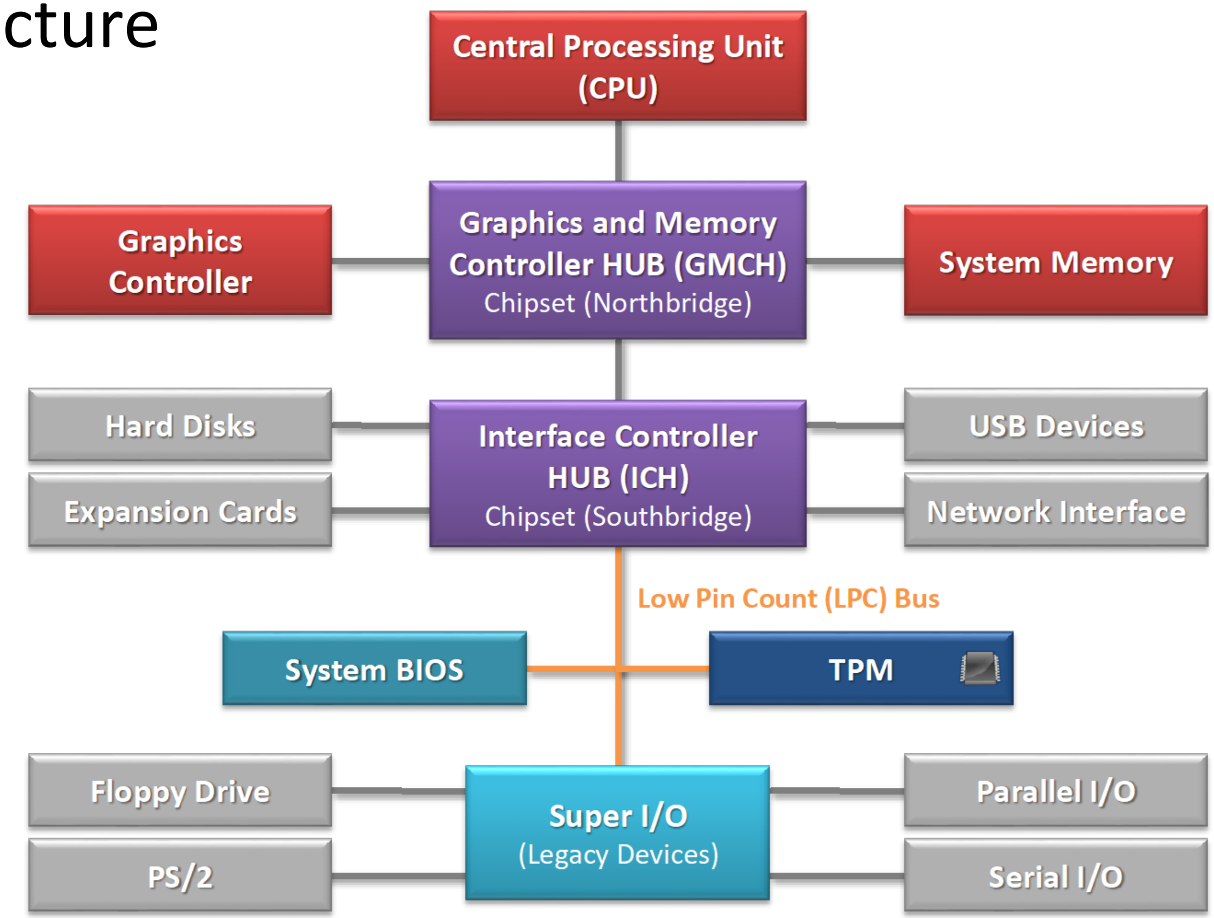
Non-Volatile Memory

- Stores persistent TPM data (e.g., the TPM identity or special keys)
- Provides read-, write- or unprotected storage accessible from outside the TPM

Computer security

Trusted Platform Module (TPM)

- Integration into the PC architecture



Computer security

Trusted Platform Module (TPM)

- Provides three RoTs
  - Root of trust for measurement (RTM)
    - A trusted implementation of a hash algorithm, responsible for the first measurement on the platform - whether at boot time, or in order to put the platform into a special, trusted state;
  - Root of trust for storage (RTS)
    - A trusted implementation of a shielded location for one or more secret keys - probably just one, the storage root key (SRK);
  - Root of trust for reporting (RTR)
    - A trusted implementation of shielded location to hold a secret key representing a unique platform identity, the endorsement key (EK)

Computer security

Trusted Platform Module (TPM)

- Provides 9 different types of keys
  - 3 special TPM key types
    - Endorsement Key, Storage Root Key, Attestation Identity Keys
  - 6 general key types
    - Storage, signing, binding, migration, legacy and "authchange" keys
  - Each key may have additional properties, the most important ones are
    - Migratable, non-migratable or certified migratable (i.e. whether the key is allowed to be migrated to another TPM)
    - Whether the key is allowed only to be used when the platform is in a specific (potentially secure) configuration

Computer security

Trusted Platform Module (TPM)

- Endorsement Key
  - TPM identity represented as Endorsement Key (EK)
    - Unique en-/decryption key pair
    - Private key does not leave TPM
    - Public key is privacy-sensitive (since it identifies a TPM/platform)
  - Generated during manufacturing process of TPM
    - Either in TPM or externally and then embedded into the TPM
  - Must be certified by EK-generating entity (e.g. by the TPM manufacturer)
  - Can be deleted (revoked) and re-generated by a TPM user
    - Revocation must be enabled during creation of the EK
    - Deletion must be authorized by a secret defined during EK creation
    - EK-recreation invalidates Endorsement Credential (EC)

Computer security

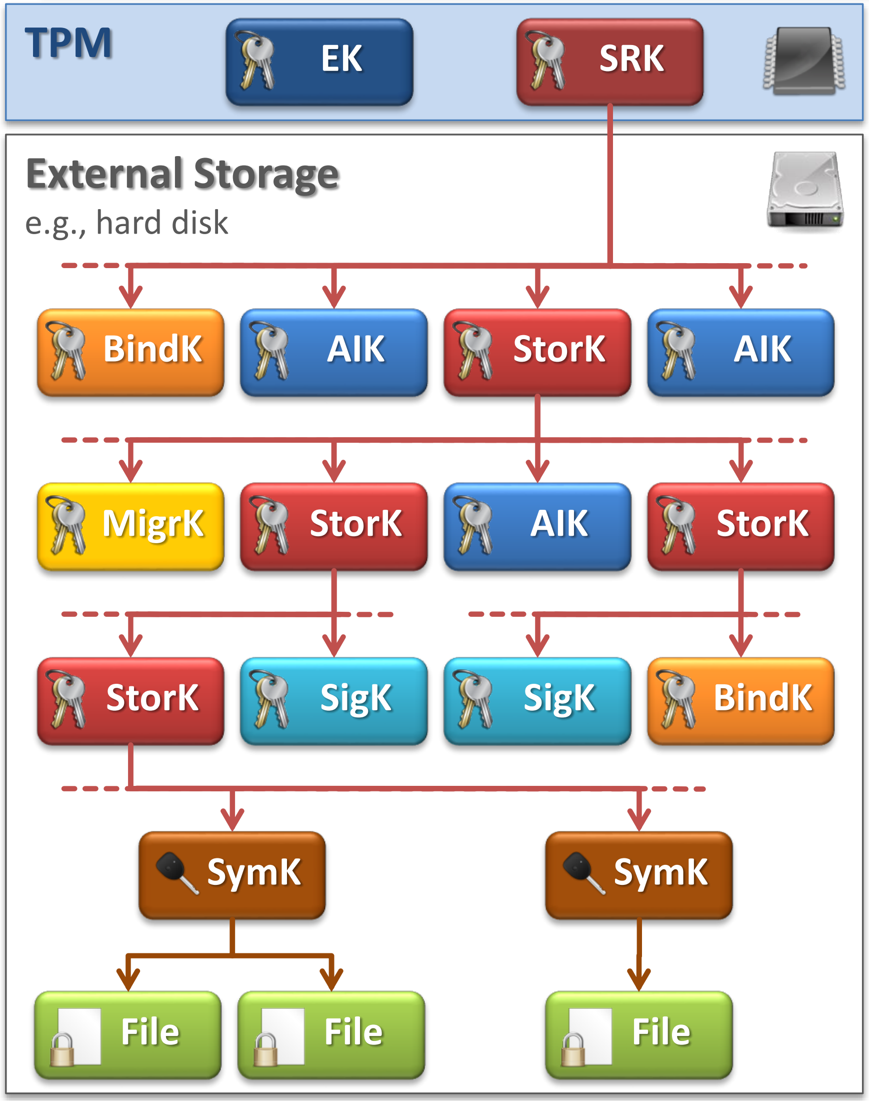
Trusted Platform Module (TPM)

- Storage Root Key (SRK)
    - Represents the Root of Trust for Storage (RTS)
    - RSA en-/decryption key pair
        - Must at least have 2048-bit key length
        - Private SRK must not leave TPM
    - Generated by TPM during process of installing TPM Owner
    - Deleted when the TPM Owner is deleted
        - This makes key hierarchy inaccessible and thus destroys all data encrypted with keys in that hierarchy

Computer security

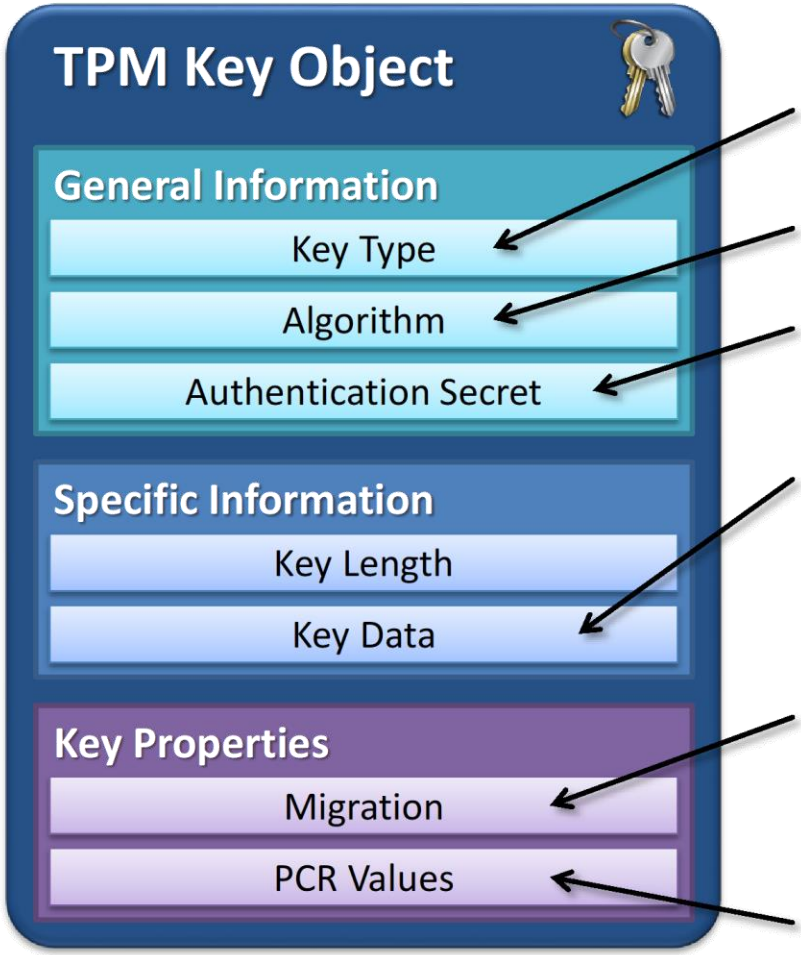
Trusted Platform Module (TPM)

- TPM Key Hierarchy
  - Depth of hierarchy and number of TPM-protected keys only limited by size of external storage
  - Storage keys (StorK) protect all other key types
    - Attestation ID keys (AIK)
    - Signing keys (SigK)
    - Binding keys (BindK)
    - Migration Keys (MigrK)
    - Symmetric keys (SymK)
  - Transitive protection
    - SRK indirectly protects arbitrary data (e.g., files)



Computer security

Trusted Platform Module (TPM)



e.g., signing key, binding key, storage key, ...

e.g., RSA, DSA, HMAC, AES, ...

Authentication secret required to use the key

Public and private key, asymmetric key. Secret key data is encrypted with the corresponding parent key.

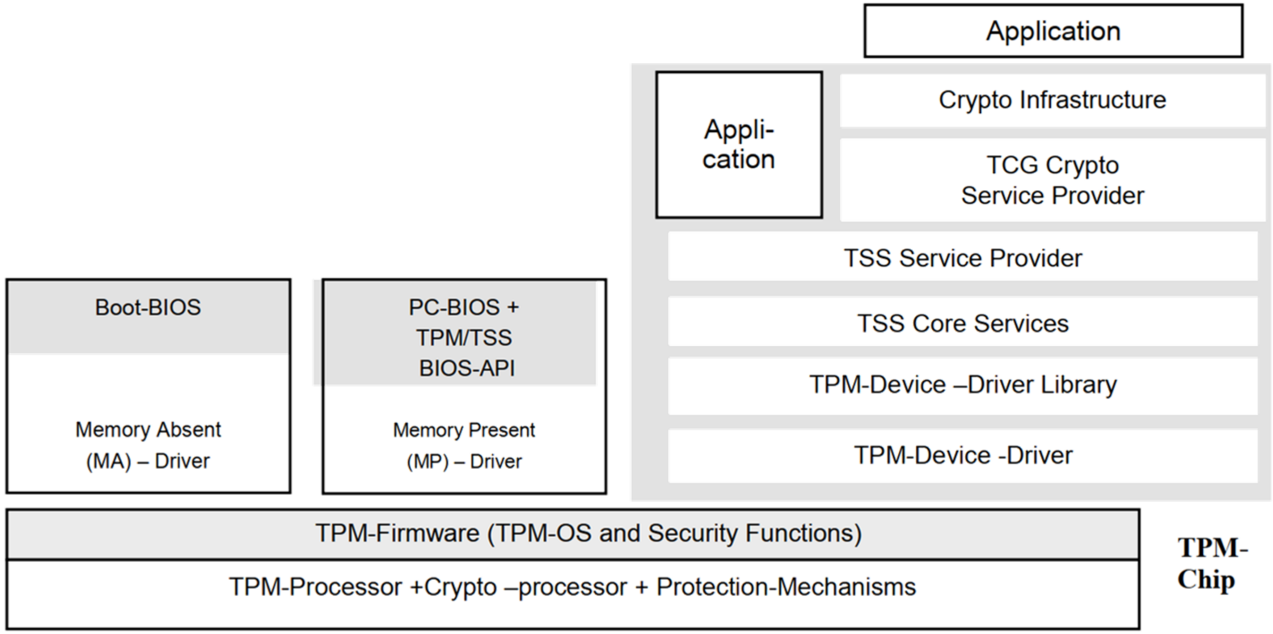
Information about the migratability of the key:
- migratable
- certified mitgratable
- non-migratable

A key can be sealed to specific PCR values. This means that such a key can only be used when the platform is in a specific (trusted) state.

Computer security

Trusted Platform Module (TPM)

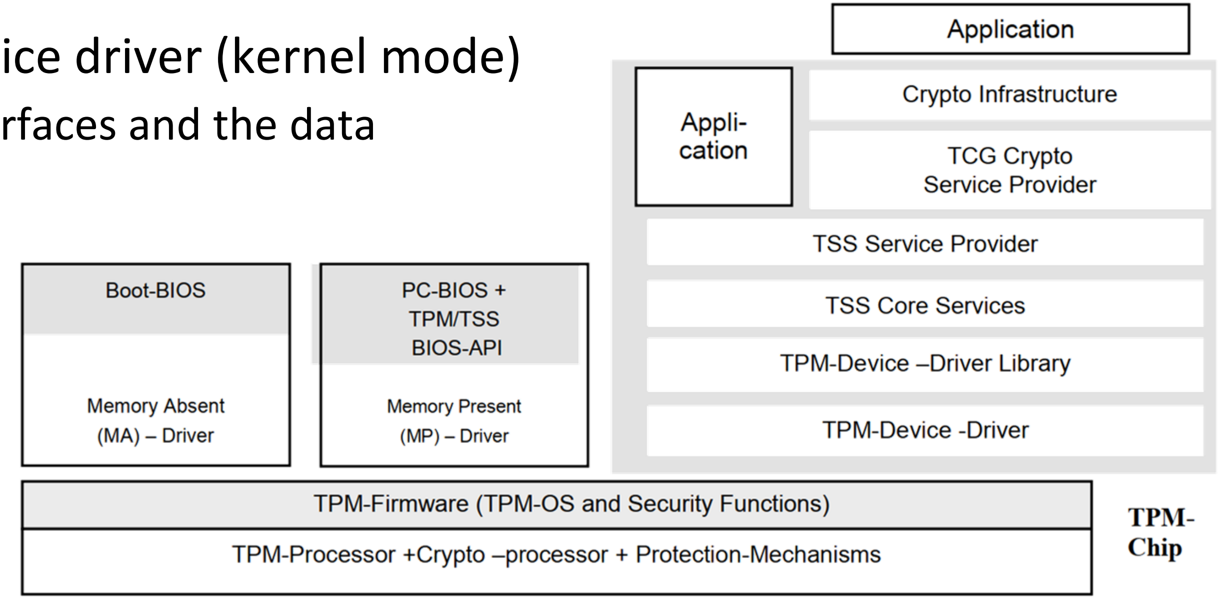
- Trusted Platform Support Service (TSS)
  - A security API which provides the TPM functions for the relevant operating system.
  - Normally the TPM manufacturer also supplies the TSS required for the relevant OS.
  - TSS consists of


Application
Appli-cation
Crypto Infrastructure
TCG Crypto Service Provider
TSS Service Provider
TSS Core Services
TPM-Device –Driver Library
TPM-Device -Driver
Boot-BIOS
Memory Absent (MA) – Driver
PC-BIOS + TPM/TSS BIOS-API
Memory Present (MP) – Driver
TPM-Firmware (TPM-OS and Security Functions)
TPM-Processor +Crypto –processor + Protection-Mechanisms
TPM-Chip

Computer security

Trusted Platform Module (TPM)

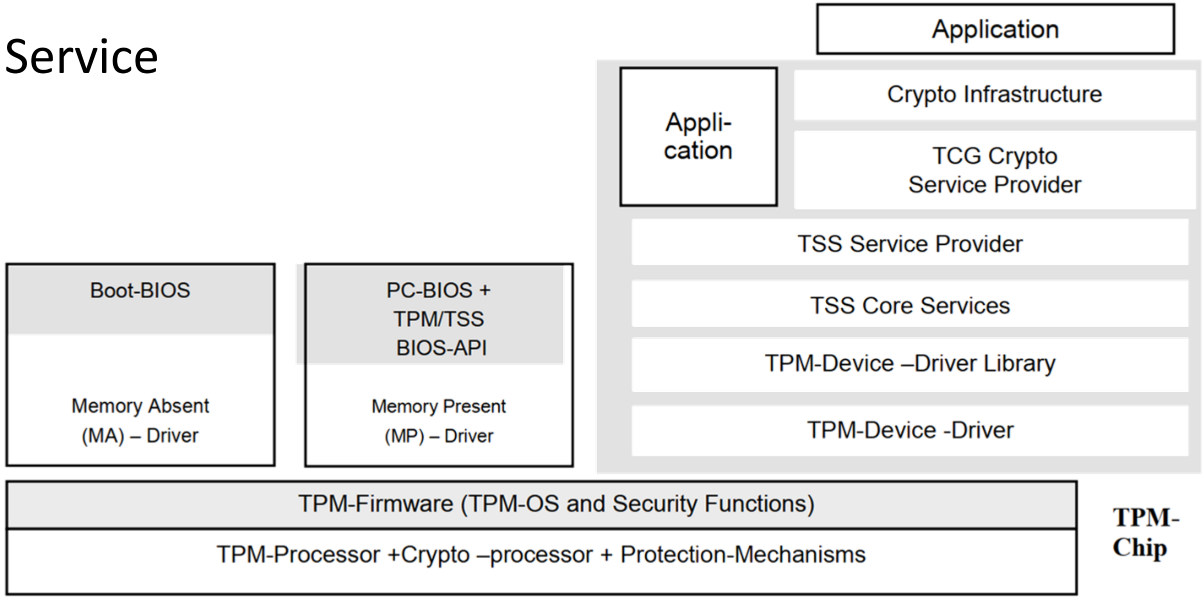
- Trusted Platform Support Service (TSS)
  - A security API which provides the TPM functions for the relevant operating system.
  - Normally the TPM manufacturer also supplies the TSS required for the relevant OS.
  - TSS consists of
    - At the lower level, the hardware-based device driver (kernel mode)
      - Responsible for the initialization of the interfaces and the data exchange with the TPM via the LPC bus.


Application
Appli-cation
Crypto Infrastructure
TCG Crypto Service Provider
TSS Service Provider
TSS Core Services
TPM-Device –Driver Library
TPM-Device -Driver
Boot-BIOS
Memory Absent (MA) – Driver
PC-BIOS + TPM/TSS BIOS-API
Memory Present (MP) – Driver
TPM-Firmware (TPM-OS and Security Functions)
TPM-Processor +Crypto –processor + Protection-Mechanisms
TPM-Chip

Computer security

Trusted Platform Module (TPM)

- Trusted Platform Support Service (TSS)
  - A security API which provides the TPM functions for the relevant operating system.
  - Normally the TPM manufacturer also supplies the TSS required for the relevant OS.
  - TSS consists of
    - The next higher level consists of the System Service
      - TPM Device Driver Library
      - TSS Core Services
      - TSS Service Provider



Application
Appli-cation
Crypto Infrastructure
TCG Crypto Service Provider
TSS Service Provider
TSS Core Services
TPM-Device –Driver Library
TPM-Device -Driver
Boot-BIOS
Memory Absent (MA) – Driver
PC-BIOS + TPM/TSS BIOS-API
Memory Present (MP) – Driver
TPM-Firmware (TPM-OS and Security Functions)
TPM-Processor +Crypto –processor + Protection-Mechanisms
TPM-Chip

Computer security

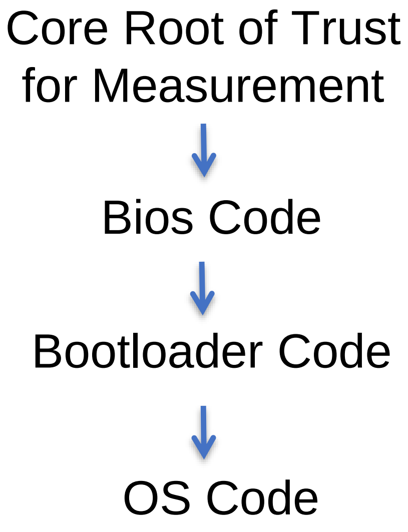
Trusted Platform Module (TPM)

- Applications
  - Trusted boot
  - Machine Authentication
  - Remote Attestation
  - Data Protection

Computer security

Trusted Platform Module (TPM)

- Applications :: Trusted boot
  - Creates record of the software booting on the machine
  - Hash chain of the booted software stored inside TPM registers
  - Example of hypothetical chain of measurements



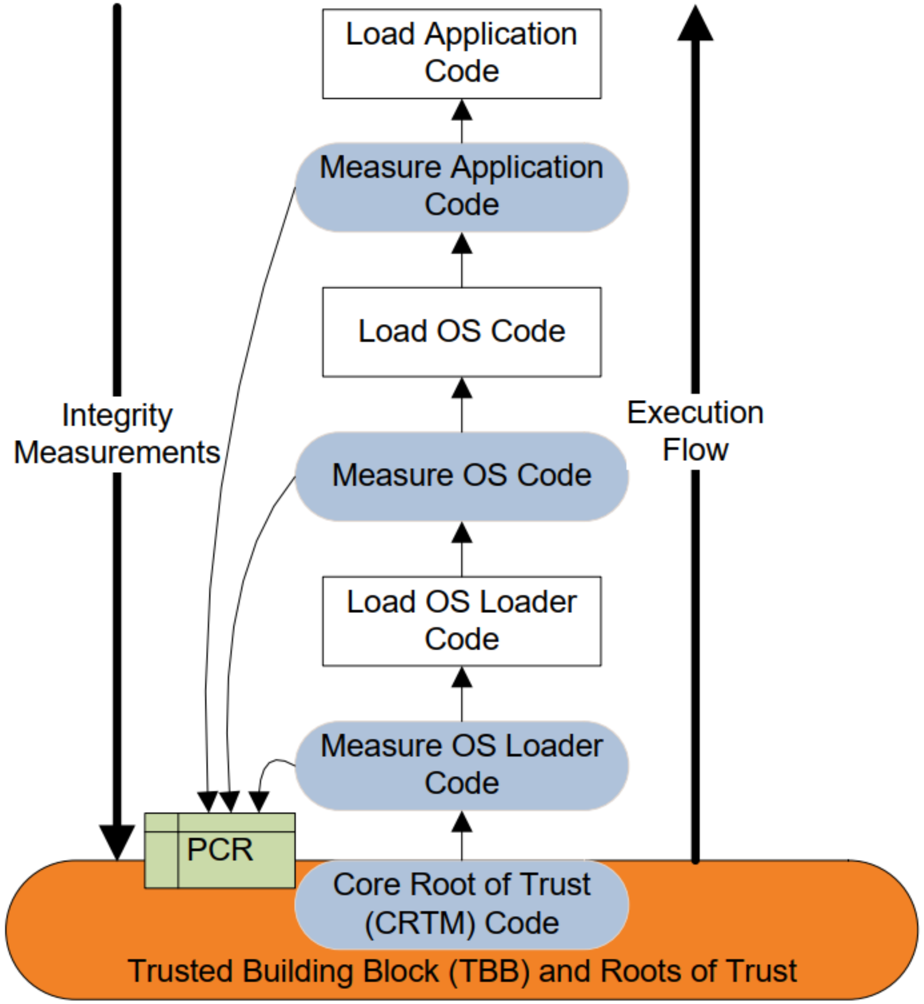
Platform Configuration Registers
(PCRs)

PCR0	hash(BIOS)
PCR1	hash(PCR0||BLoader)
PCR2	hash(PCR1||OS)
PCR3	…

Computer security

Trusted Platform Module (TPM)

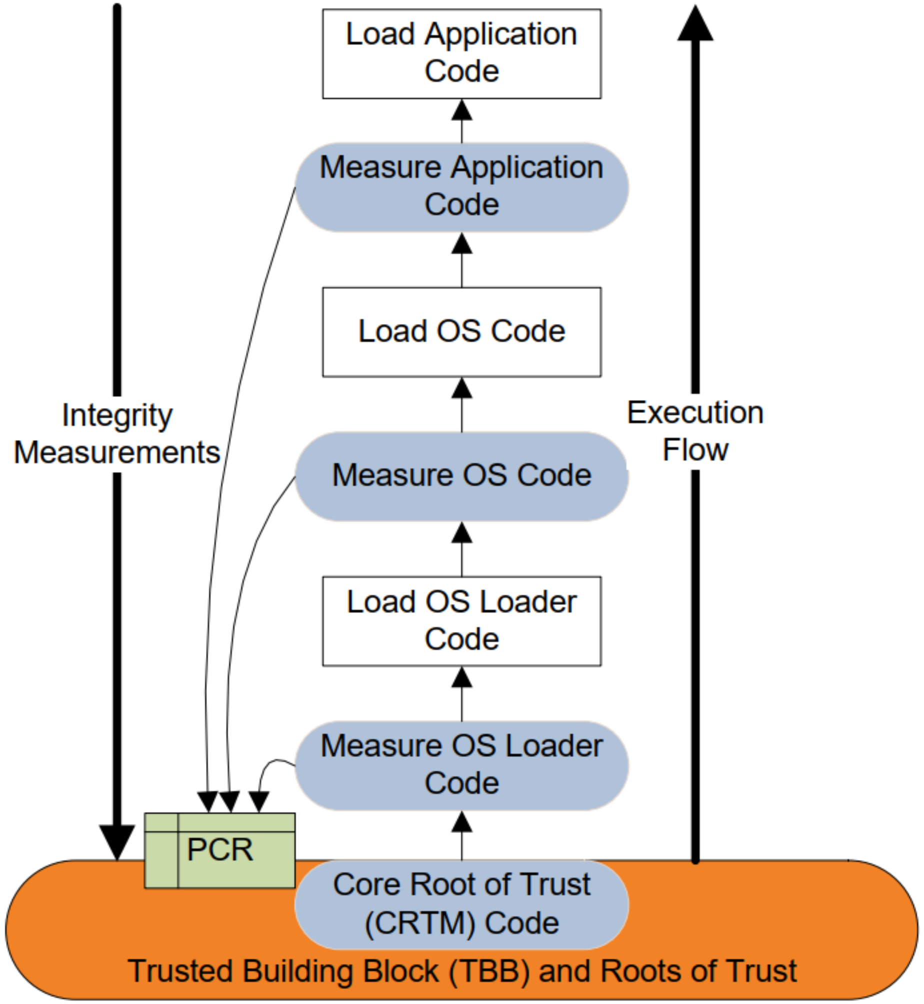
- Applications :: Trusted boot
  - The first component to power up is the system BIOS (Basic Input/Output System).
  - The boot sequence is initiated by the Core BIOS (i.e. CRTM: Core Root of Trust Measurement), which first measures its own integrity.
  - This measurement is stored in PCR01 and later it is extended to include the integrity measurement of the rest of the BIOS.



Computer security

Trusted Platform Module (TPM)

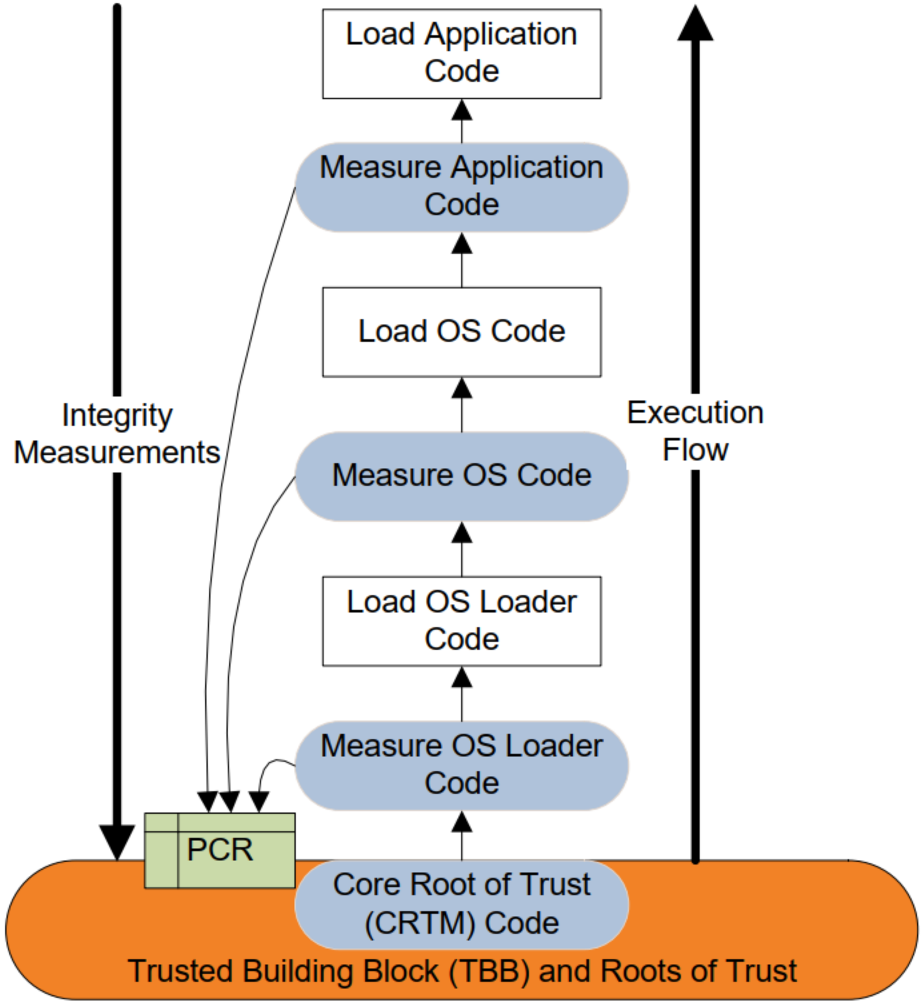
- Applications :: Trusted boot
  - The Core BIOS then measures the motherboard configuration setting, and this value is stored in PCR1.
  - After these measurements, the Core BIOS will load the rest of the code of the BIOS.
  - The BIOS will subsequently measure the integrity of the ROM firmware and the ROM firmware configuration, storing them in PCR2 and PCR3, respectively.
  - At this stage, the Trusted Building Block (TBB) is established.



Computer security

Trusted Platform Module (TPM)

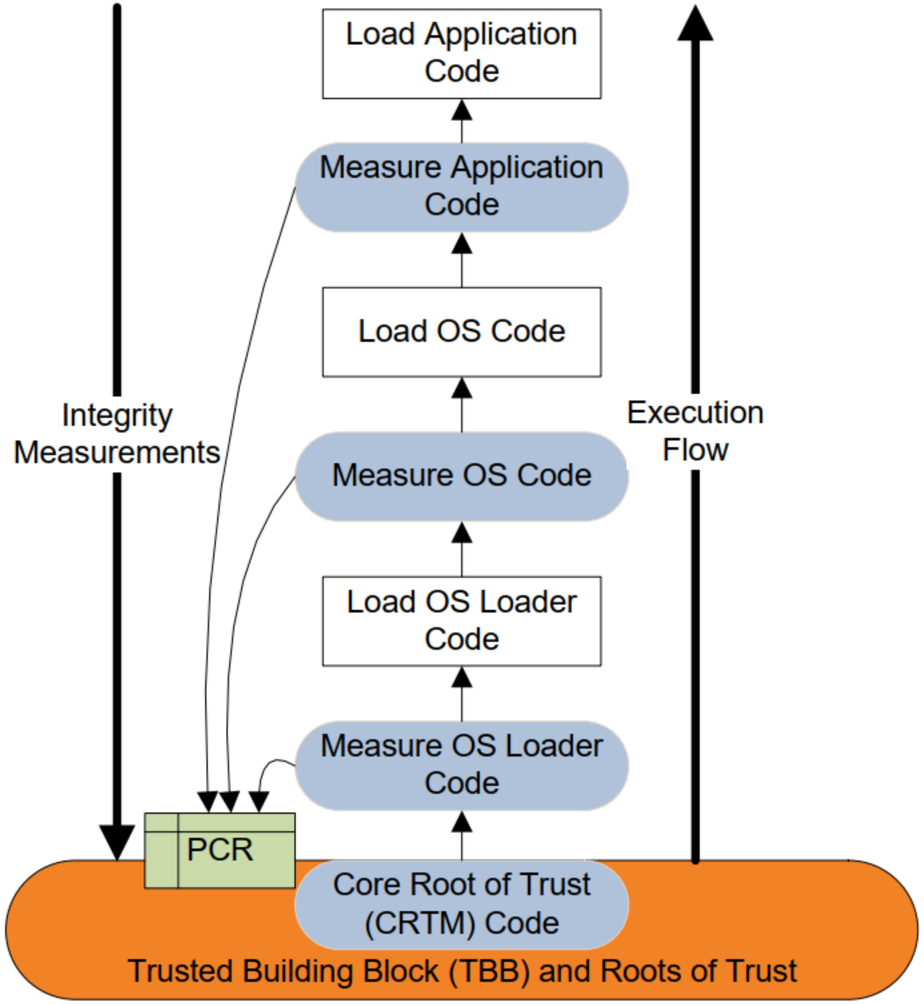
- Applications :: Trusted boot
  - The CRTM will proceed with integrity measurement and loading of the Operating System (OS).
  - The CRTM measures the integrity of the OS loader code, also termed the Initial Program Loader (IPL), and stores the measurement in the PCR. The designated PCR index is left to the discretion of the OS.
  - Subsequently, it will execute the OS Loader Code and on its successful execution, the TPM will measure the integrity of the OS code. After measurement is made and stored, the OS code executes.



Computer security

Trusted Platform Module (TPM)

- Applications :: Trusted boot
  - Then, the relevant software that initiates its execution will be subjected to an integrity measurement, and values will be stored in a PCR.
  - Finally, the software will be sanctioned to execute.



Computer security

Trusted Platform Module (TPM)

- Applications :: Machine Authentication
  - TPM keys can be used to reliably identify a machine
    - TPM soldered to motherboard
    - Keys cryptographically bound to a particular TPM
  - Signing-based authentication
    - This data passed through machine X, because origin can’t be proven with just a signature
    - Decryption-based authentication
      - Only machine X can read this data
    - One of the simplest TPM applications

Computer security

Trusted Platform Module (TPM)

- Applications :: Remote Attestation
  - Based on the concept of Quotes:
    - Signed report of current PCR contents
    - Many PCR constraints (e.g., keys) can be used for attestation also
  - Remote verifier can check boot state of machine
  - Potentially very powerful!
    - Is this machine running the right image? Is the software trustworthy?
  - Easier said than done:
    - Interpreting PCR values is hard
    - Work to regularize them is ongoing
    - Values are very fragile and hard to predict!

Trusted Platform Module (TPM)

- Applications :: Data Protection
  - Provide hardware protection, tamper resistance to sensitive data
  - Use to encrypt small, high-value data; for example:
    - Software-held private keys (e.g. user identities)
    - Symmetric keys usable for bulk encryption
    - Password stores
  - Can be used for hard drive encryption (if supported)
    - TPM-sealed symmetric key encrypts drive (e.g. Bitlocker option in Windows)
  - Not suitable for bulk data encryption
    - Too slow! Public key encryption only, cheap processor
    - No fast symmetric ciphers due to export regulations

Computer security

References

- Correia, M. P. & Sousa, P. J. (2017). Segurança no Software (2ª Edição). Lisboa: FCA.
- Coppolino, L. & D'Antonio, S. & Mazzeo, G. (2019). A Comprehensive Survey of Hardware-assisted Security: from the Edge to the Cloud. Internet of Things. 100055. 10.1016/j.iot.2019.100055.
- Martin, A. (2008). The ten-page introduction to Trusted Computing (Report number CS-RR-08-11). Oxfordshire: Oxford University Computing Laboratory.
- Brandl, H. & Rosteck, T. (2004). Technology, Implementation and Application of the Trusted Computing Group Standard (TCG) - Secure platforms provide new levels of security. Datenschutz und Datensicherheit, Vieweg.