Hochschule Konstanz
Fakultät Informatik

Introduction to IT Security

WIN+AIN

Hanno Langweg

04b Secure Operating Environments - Trusted Computing

Secure Operating Environments

- Security of operating systems
- Trusted Computing
- Access control
- Malware

Trusted Computing

Trusted Platform Module (TPM)

- Concept from Trusted Computing Group
- Hardware module at heart of hardware/software approach to trusted computing (TC)
- Uses a TPM chip
  - Motherboard, smart card, processor
  - Working with approved hardware/software
  - Generating and using crypto keys
- 3 basic services
  - Authenticated boot
  - Certification
  - Encryption

https://www.infineon.com/export/sites/default/_images/SLB_9665_TT_2.0.png_184029107.png

Authenticated Boot Service

- Responsible for booting entire OS in stages, ensuring each is valid and approved for use
  - At each stage digital signature associated with code is verified
  - TPM keeps tamper-evident log of loading process
- Log records versions of all code running
  - Can then expand trust boundary to include additional hardware and application software
  - Confirms component is on the approved list, is digitally signed, and that serial number hasn’t been revoked.
- Result: Well-defined config with approved components

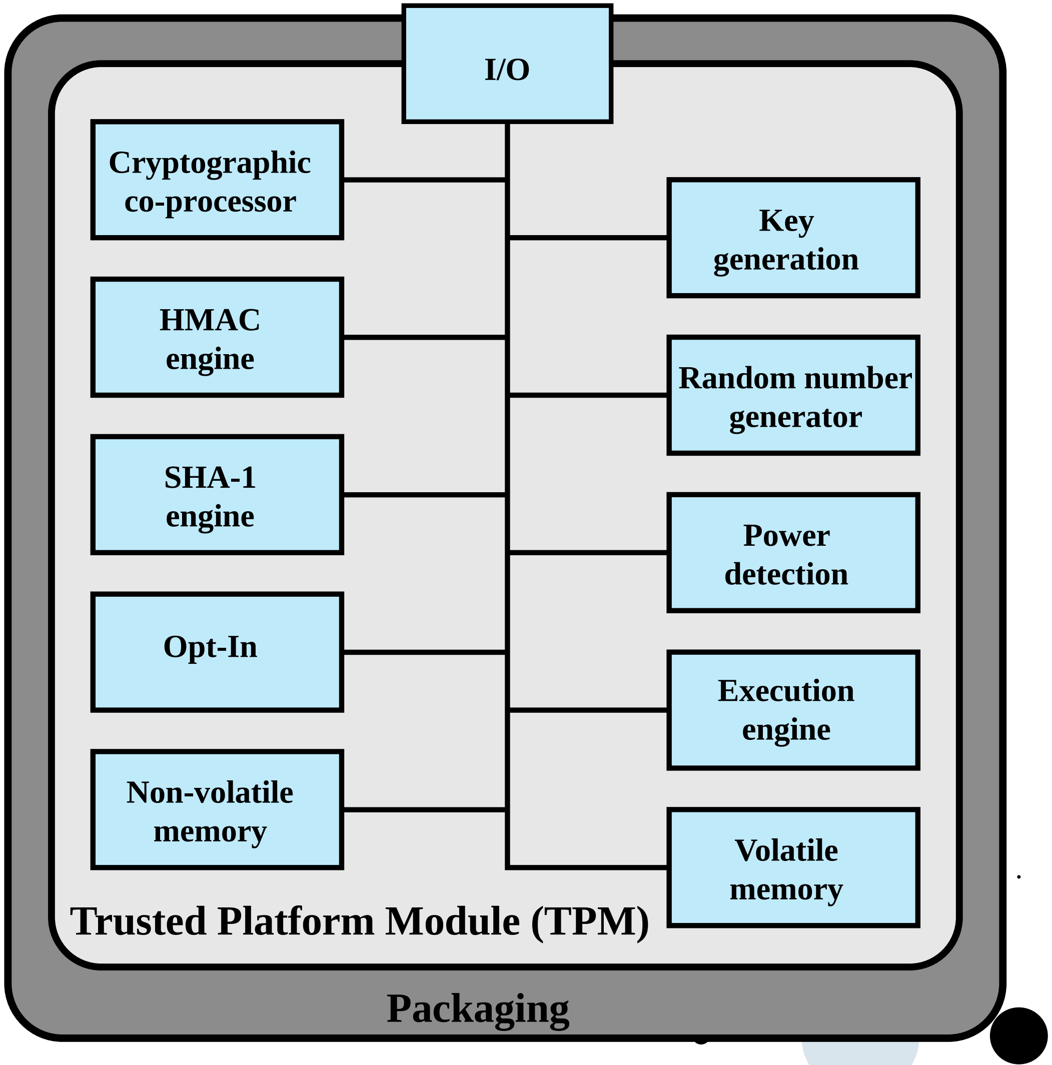
Certification Service

- Once a configuration is achieved and logged the TPM can certify configuration to others
  - Can produce a digital certificate
- Confidence that configuration is unaltered because:
  - TPM is considered trustworthy
  - Only the TPM possesses this TPM’s private key
- Challenge value in certificate to ensure timeliness
- Provides a hierarchical certification approach
  - Hardware/OS configuration
  - OS certifies application programs
  - User has confidence in application configuration

Encryption Service

- Encrypts data so that it can only be decrypted by a machine with a certain configuration
- TPM maintains master secret key unique to machine
  - Used to generate secret encryption key for every possible configuration of that machine
- Can extend scheme upward
  - Provide encryption key to application so that decryption can only be done by desired version of application running on desired version of the desired OS
  - Encrypted data can be stored locally or transmitted to a peer application on a remote machine

Block diagram of TPM functional components



Stallings/Brown figure 13.11