Hardware Assurance Best Practices

Chapter 10

Episode 10.01

Trusted Hardware

Objective 2.3 Explain hardware assurance best practices.
• Hardware root of trust
- Trusted platform module (TPM)
- Hardware security module (HSM)
• eFuse
• Unified Extensible Firmware Interface (UEFI)
• Trusted firmware updates
• Measured boot and attestation

Trusted Platform Module (TPM)

- TPM chip
  - System-on-chip (SoC)
  - Stores cryptographic keys and the functionality to deal with them
- Persistent memory
  - Endorsement key (EK)
  - Storage root key (SRK)
- Versatile memory
  - Platform Configuration Registers (PCRs)
  - Attestation Identity Keys (AIKs)
  - Storage keys

Hardware Security Module (HSM)

- Not bound to a motherboard
- Removable card or device

eFuse

- Nonvolatile bit
  - Once set to 1, cannot be changed
- Useful to permanently disable functionality
  - Manufacturing tests
- Useful to permanently store data
  - Cryptographic keys

Firmware

- Software that's burned into hardware (chip)
- Difficult to change
- Unified Extensible Firmware Interface (UEFI)
  - Security Phase (SEC)
  - Pre-EFI Initialization (PEI)
  - Driver Execution Environment (DXE)
  - Boot Device Select (BDS)
  - Transient System Load (TSL)
  - Runtime (RT)

Firmware Security

- Measured boot and attestation
  - Instead of verifying digital signatures of code
    - Calculates code hashes
    - Stores hashes of programs that have been run
    - Securely sends hashes to management station
- Trusted firmware updates
  - Built-in capability to download, verify, and swap firmware images
  - Avoids overwrite failures that result in unbootable devices

Episode 10.02

Hardware Encryption

Objective 2.3 Explain hardware assurance best practices.
- Self-encrypting drive
- Bus encryption

Storage Encryption

- Full-disk encryption (FDE)
  - Software
  - Hardware

Hardware Encryption

- Self-encrypting drive (SED)
  - User provides password
    - Password gets used to encrypt key
    - Encrypted key is stored in nonvolatile memory of the disk controller

Bus Encryption

- SED still exposes plaintext once data gets read from the disk
- Moving crypto module from the disk controller to the CPU
  - Keeps data on the bus as ciphertext
  - Requires a dedicated chip (cryptoprocessor)
- Bus encryption is not suitable for general purpose computers
  - Expensive
  - Complex
  - Functional limitations

Episode 10.03

Hardware Security

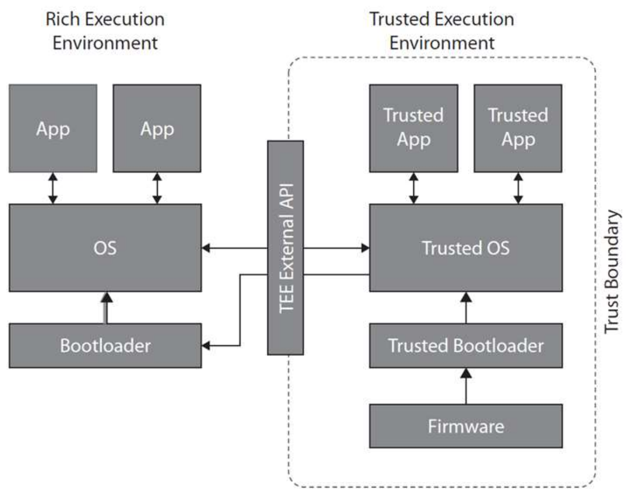
Objective 2.3 Explain hardware assurance best practices.
• Trusted foundry
• Secure processing
- Trusted execution
- Secure enclave
- Processor security extensions
- Atomic execution
• Anti-tamper

Secure Processing

- Trusted execution environment (TEE)
  - Rigorous assessment prior to certification
  - Secure enclave
    - Runtime environment that limits how programs interact with one another and the outside world

TEE and REE

- Processor security extensions
  - CPU instructions that support TEE functionality



Source: Chapman, B., & Maymí, F. (2020). *CompTIA CySA+™ Cybersecurity Analyst Certification All-in-One Exam Guide, Second Edition (Exam CS0-002)*, 248.

Secure Processing

- Atomic execution
  - Anti-interruption guarantee
  - Helps to protect from TOCTOU attacks

Trusted Foundry

- US DoD program
- Ensures that the supply chain for all DoD mission-critical systems is hardened
- Fewer than 100 companies have passed the rigorous certification process to be designated as trusted foundries

Anti-Tamper Techniques

- Chip attacks
  - Microprobing
    - Apply voltage to various conductors and recording the results
  - Visual analysis
    - Carefully removing the chip’s covering, layer by layer

Anti-Tamper Techniques

- Chip manufacturers employ techniques to thwart tampering
  - Random signals to confuse microprobing
  - Chip casing compromise detection
    - If compromised, place zeros in nonvolatile memory