Agenda

- Introduction to Hardware Security
- History of Hardware Security
- Why do we need it?
- Types of Conventional Hardware Security
  - Cryptoprocessors
  - Hardware Security Modules
- What does hardware security actually do?
- Hardware Security Modules (HSMs)
Introduction to Hardware Security

- Physical device that provides a layer of security.
- Protects data from unwanted accesses.
- Helps prevent exploits of specific vulnerabilities.
- Provides some advantages over security via software.
  - Actual degree of security
  - Speed
  - Tampering
History of Hardware Security

- **Literal Hardware Security**
  - 1853 - First patent on an electro-magnetic alarm.
  - Late 1800s - Electronically controlled vaults.
- **Conventional Hardware Security started with Military Applications**
  - Weapons arming, communications.
- First civilian use in the 1980’s, primarily in the financial industry with ATMs and mainframe computers.
- Now used in numerous consumer level applications
  - sim cards, smart cards, game controllers, cars, and various other consumer electronics.
- **Recent standards created for cryptoprocessors**
  - Trusted Platform Module (TPM) - 2009
Why do we need it?

- Modern security work is largely focused on either protecting or attacking target operating systems.
- Software is not enough to fully protect a system.
- Security in hardware offers performance and power consumption advantages over its software equivalents.
  - Increasing amounts of data being processed and the complexity of encryption algorithms slows down security implementations severely.
  - Often times these same encryption algorithms can be implemented in hardware.
Types of Hardware Security

- Cryptoprocessors
- Hardware Security Modules
Cryptoprocessors

- Dedicated processor for cryptographic operations.
- Has some degree of tamper resistance.
- Limits the amount of physical security needed via compartmentalizing secure portions of the system.
What does Hardware Security Do?

- Implements encryption algorithms to secure data.
- Store encrypted data in a difficult to access fashion.
- Prevents unencrypted data from existing in an idle state on the system.
- In the US, Hardware security conforms to the Federal Information Processing Standards (FIPS).
- In general, it works just like any other processing hardware only its optimized for encryption algorithms and secured more thoroughly.
Trusted Platform Module Standard

- Cryptographic processor
  - random number generator
  - RSA key generator
  - SHA-1 hash generator
  - encryption-decryption-signature engine

- Persistent memory
  - Endorsement Key (EK)
  - Storage Root Key (SRK)

- Versatile memory
  - Platform Configuration Registers (PCR)
  - Attestation Identity Keys (AIK)
  - storage keys
Processor with Double Encryption
Hardware Security Modules

- HSM’s provide both logical and physical protection of data
- Possess tools to protect against tampering
- Contains one or more cryptoprocessors
- Can have multiple levels of security
- Often operates within a lock safe or chest to further prevent hardware tampering
Concerns

- What are the concerns if Hardware security protects against remote attacks?
  - Physical Access to the Hardware Module
    - Drill into module, probe components
    - Power Analysis of Module
    - UV Light Memory Reading
    - Setting/Resetting SRAM via light injection
    - Fault Injection
  - “Remote Analysis of Module”
    - Listening on the network for server based HSMs.
Solutions

- Hardware security components must provide some tamper resistance.
  - Sensors for tampering detection
    - Tampering results in zeroizing of data (keys and hashes)
    - Self-destruction?
  - UV Light Protection
- Limit physical access to systems
- Active vs Passive Modules
  - Active, “full-sized” processors have an ability to recognize tampering.
  - Passive modules such as smartcards won’t know and thus need different tampering resistance.
Sources

- http://perspecsys.com/history/
- http://www.princeton.edu/~achaney/tmve/wiki100k/docs/Secure_cryptoprocessor.htm
- http://www.engr.uconn.edu/~tehrani/teaching/hst/
- http://www.cren.net/crenca/onepagers/hsm2.html
Questions?