Physical Security Attacks and Defenses for Computing Systems

Steve Weingart
Senior Engineer
c1shw@us.ibm.com
(561) 392 6100

Secure Systems and Smart Cards

IBM T.J. Watson Research Center
Hawthorne, NY

Physical Security Attacks & Defenses

Outline

- Definition
- Attacks
- Defenses
- Standards

Definition:

Physical Security,

A barrier placed around a computing system to deter unauthorized physical access to that computing system. In the event of an attack, there should be a low probability of success; and a high probability of the attack being detected either during the attack, or subsequent to penetration.

Physical Security Attacks & Defenses

Attacks

- Low Tech
  - Theft
  - Mis-use

- High Tech
  - Machining
    - Mechanical
    - Water
    - Laser
    - Chemical
    - Shaped Charge
  - Probes
    - Passive/Active
    - Mechanical
    - Energy
      - E-beam/Ion Beam
      - X-Ray
      - IR Laser
  - Energy
    - Imprinting
      - Temperature
      - Voltage
      - Radiation
    - Disruption
  - Tempest
    - EM Emanations
    - Power/Current Profile

Defenses (High & Low Tech)

- Tamper Resistance
  - Guards
  - Weight, Size, Material
  - Complexity
  - Inaccessibility
    - Chip Coatings
    - Substrates

- Tamper Evidence
  - Holographic Seals
  - ‘Bleeding’ Paint
  - Crazed Materials

- Tamper Detection
  - Membranes
    - Metallic
    - Organic
    - Other
  - Sensors
    - Temperature
    - Radiation
    - Voltage

- Tamper Response
  - Zeroization

The Operating Envelope

The range of all conditions that are required for correct operation of all components.

Note: For Tamper Responding systems that use erasure as a means of protecting secret data, correct operation includes the ability to guarantee the removal of memory contents when desired.

- Voltage
- Temperature
- Radiation

Standards

- Not Many!
  - In commercial sector
- FIPS 140-1
  - Seems to be the emerging commercial standard
  - Reasonable, but needs updating now
- ANSI 9.66
  - Had been different than FIPS 140-1
  - Probably will not be in the future
- TNO (Delft Holland)
  - Not really a standard, an Authority
- ITSEC
  - Not Really Focused on Hardware
- Common Criteria
  - Not Really Focused on Hardware

An Example of a Physically Secure Coprocessor