Physical Attacks

-- Building Secure Systems

Cybersecurity Specialization
-- Hardware Security

Tamper Protection Levels

DG. Abraham et al, "Transaction Security System", IBM System Journal, 1991.

- ZERO
  - No security feature, open access
  - Example: microcontroller, FPGA with external memory
  - No special equipment/tools, minutes to hours
- LOW
  - Basic security features, easy to break
  - Example: microcontroller with unprotected internal memory but proprietary access
  - Low cost tools, $1000/$500, hours to days

Tamper Protection Levels

- MODL
  - security features against low cost attacks
  - Example: microcontroller w protection, but sensitive to power analysis or power glitches
  - Some tools/skills, $10K/$5K, days to weeks
- MOD
  - Example: microcontroller with protection against UV light attack, ASICs, secure memory chips, smartcards
  - special tools/equipment/skills/knowledge, $100K/$50K, weeks to months

Tamper Protection Levels

- MODH
  - Application specific security features
  - Example: secure FPGA, modern smartcard, complex ASICs
  - Group of attackers, $1M/$200K, months
- HIGH
  - Protection against all known attacks
  - Example: secure crypto modules for certification authority, military, banking application
  - Team of specialists, design new tools, years

FIPS Security Levels

1. Specifies basic security requirements for a cryptographic module
2. Adds physical security: tamper evident coating or seals, pick-resistant locks
3. Enhances physical security to prevent unauthorized access to critical data
4. Detects penetrations to the cryptographic module/device from all directions

Federal information Processing Standards 140
"Security Requirements for Cryptographic Modules".

Known Security Failures

- Microchip PIC microcontroller
  - Security fuse bug.
- Hitachi smartcard
  - Information leakage on a product CD
- Actel secure FPGA
  - Programming software bug
- Xilinx secure CPLD
  - Programming software bug
- Dallas SHA-1 secure memory
  - Factory initialization bug

Understanding the Attacks

- Understand the attacker's motivations
  - Theft, access, DoS, IP piracy
- Understand the attackers
  - Outsiders, insiders, funded organizations
- Attacking categories
  - Invasive, semi-invasive, non-invasive
- Attacking methods
  - Reverse engineering, probing, fault, side channel, software

Securing your System

- Threat estimation
- System security evaluation
- Locating weak points
- Enhancing system security
  - Choose/upgrade secure components
  - Redesign for security
- System engineering approach
  - Security has to be built into the system, not onto a given system.