Physical Attacks

-- Attacks & Countermeasures

Cybersecurity Specialization
-- Hardware Security

Invasive Attacks

- Decapsulation and deprocessing
  - Remove the package to expose the silicon die
- Reverse engineering
  - Reveal chip inner structure and functionality
- Depassivation and microprobing
  - Probe single bus activity, submicron precision
- Chip modification
  - Disable chip component (cut wire)
- Cost varies, but is increasing very fast.

Invasive Attacks: Tools

- IC soldering/desoldering station
- Simple chemical lab
- High-resolution optical microscope
- Oscilloscope, logic analyser, signal generator
- Wire bonding machine, laser cutting system, microprobing station
- Scanning electron microscope
- Focused ion beam (FIB) station

Semi-invasive Attacks: Tools

- IC soldering/desoldering station
- Simple chemical lab
- High-resolution optical microscope
- Oscilloscope, logic analyser, signal generator
- UV light sources, lasers
- Microscopes (laser scanning, infrared etc)
- PC with data acquisition board, FPGA boards, prototyping boards

Semi-invasive Attacks

- Decapsulation and deprocessing
  - Remove the package to expose the silicon die
  - But will not contact internal bus lines
- Launching attacks
  - Imaging: optical and laser techniques, active photon probing, backside infrared imaging
  - Fault injection: Ultraviolet (UV) light attacks, optical fault injection, local heating, memory masking
  - Side channel analysis: optical emission, optically enhanced position-locked power analysis

Non-invasive Attacks: Tools

- IC soldering/desoldering station
- Oscilloscope, logic analyser, signal generator
- PC with data acquisition board, FPGA boards, prototyping boards
- Digital multimeter
- Universal programmer and IC tester
- Programmer power supplies

Non-invasive Attacks

- Side channel analysis (passive)
  - Timing, power, EM emission, acoustics, NFC
- Brute force (active)
  - Search for keys and passwords
  - Recover design (black-box attack)
  - Find backdoor access to factory test or programming mode
- Data remanence (active)
- Fault injection (active)

Data Remanence

- Data remanence in SRAM
  - Retaining data after power down
    - Retrieve data after power down
  - Data "burned-in" after long time storage
    - Retrieve data right after power up
  - Data "frozen" at low temperature (-20°C)
    - Freeze data and read it
- Data remanence in EEPROM and Flash
  - V_{th} changes after write/erase
    - Extract data after multiple write/erase cycles

Fault Injection Attacks

- Idea
  - Have the chip/system execute with faulty or unexpected input/command
  - Observe chip/system execution
- Fault generation techniques
  - Glitches (clock, power)
  - Temperature
  - White light, laser
  - X-ray and ion beams
  - Electromagnetic flux

Fault Injection Attacks: Glitch

- Glitch is a fast change in chip's supply signals (power and clock).
  - Affect some transistors or flip-flops
  - Attack by a systematic search
- Clock glitch
  - Incorrect instruction fetch
- Power glitches
  - Corrupted EEPROM data read
  - Break AES on secure microcontroller

Countermeasures: Fault Injection

- Software approach
  - Execution redundancy
  - Checksums on data transfers
  - Randomized execution
- Hardware approach
  - Redundancy (e.g. fault tolerant computing)
  - Fault detector

Countermeasures: Invasive Attacks

- Bus scrambling
  - Change the order/connection of data bus
- Data encryption
  - Encrypt data and decrypt in a trusted zone
- Glue logic design
  - Hide the data bus
- Sensor mesh at top metal layer
  - Continuous monitor of all paths in the mesh
  - Microprobing will cause short circuits
  - Reset memory to preserve data