(Physical Attacks Basics)

Physical Attacks

- All the physical attacks exhibit two common things.
- **Requirements:**
  - Direct access to the chip
  - Connection to signal wires (measurement)
  - Equipment, tools, skills, and knowledge (hardware, cryptographic algorithms, data analysis)
- **Have Two Phases:**
  - **Interaction:** attacker exploits some physical characteristics of the device (collect data by interacting with some physical characteristics of the device)
  - **Exploitation:** analyzing the gathered information to reveal the secret and break the security

Physical Attacks and Hardware Security

- Compared to attacks at network level or software level
  - Physical attacks have higher requirements because they require
    - Physical access to the system
    - Specialized equipment, tools, and knowledge
  - Thus, Physical attacks are harder to launch

- **Building security at hardware**
  - **Pro:** The same costs and efforts investing on protection from hardware will most likely make the system more secure than adding security from network and software layers
  - **Con:** But it add a new attacking surface
  - Thus, we should consider the vulnerabilities of hardware design and implementations.

Physical Attacks: Attackers

- **Class I:** clever outsiders
  - Very intelligent but have Insufficient knowledge of the system
  - Limited access or do not have access to equipment and tools to break the system
- **Class II:** knowledgeable insiders
  - Knowledge of the system
  - Access to tools and equipment
- **Class III:** funded organizations
  - Access to all resources
  - Have a team of expert with all the necessary skills, tools, knowledge, and equipment to invent new attacks if necessary to break the target system.

Physical Attacks: Motivations

Based on how money can be made from successful physical attacks, the motivation can be further partitioned for physical attacks into several groups.

- **Direct theft of service or money**
  - **Example:** Breaking smart cards and making bogus deposit or breaking the TV set top box to watch programs without subscribing. Breaking game consoles to play games without paying.

- **Sell/re-sell of products illegally**
  - **Example:** IP piracy, cloning, overbuilding, and counterfeiting

- **Interrupting** damaging the service provided by the competitors **(denial of service) for** posting their own sales
  - **Example:** An attacker can insert malicious updates, patches or hardware Trojan to make competitors device or system malfunction or suffer bad performance. This will give their own product an end, an unfair competitive edge.

Physical Attacks: Goals

- When we say breaking a system, we do not mean physically destroying the system. Instead, the attackers want to learn information about the system that he doesn't have access. In the case of cryptosystems, such information could be the secret key, or the secret data.

- **Goal:** “breaking” the (crypto)system Learn information without authorization
  - Example: secret key/data (cryptosystem), detailed design info (system/chip/IP).

- **Physical Attacks vs. Cryptanalysis**
  - Both have the goal of breaking the security
  - **Cryptanalysis**: mathematical analysis to find the theoretical weakness
    - **Example**, the birthday attack and the differential Cryptanalysis. Modern crypto systems are theoretically sound and unbreakable
  - **Physical attacks**: exploit weakness in the implementation of the cryptographic algorithms. Physical attacks attempts to find existed flaws and break the system. Based on whether the targeted system or device will be damaged during or after the attack.

Physical Attacks: Classification

- **Invasive attacks**
    - Requires direct access to inside of the chip/device
    - Can be Reversible or irreversible (after attack, whether the system can be reassembled), irreversible cannot be repeated.
    - Device will be damaged, or tamper evidence left after the attack
    - Cost and required skills vary based on attack and system, but normally it is high.

- **Non-invasive attacks**
    - Attacker interacts with the device/chip via its interface (voltage, current, clock, I/O, etc.)
    - Attack can also be Passive or active depending on whether the attacker only monitors and measures the physical characteristics or injects input to the system to cause the system malfunction.
    - Normally, such attacks do not damage device and do not leave any tamper evidence.
    - Most of these attacks are low cost and are repeatable.

Physical Attacks: Classification

- Invasive attacks

- Non-invasive attacks

- Semi-invasive attacks
  - Require access to the surface of the chip, but not need to create contacts with internal wires
  - Normally, does not damage the system and depends on the attack
  - They may or may not leave tamper evidence
  - The cost of this attack depends on what kind of surface, what kind of interact they will have with the system. Moderate cost, always lower than the invasive attacks.
  - They require some special skills
  - Repeatable (cyber invasive attacks)

Physical Attacks: Classification

There are a different ways to perform physical attacks. And based on how physical attacks are performed, it can also be put into several different categories.

- **Reverse engineering (invasive)**
  - This type attack study chip’s inner structure and try to determine functionality of the system.
  - Exhibit very high cost, and attacker have similar capability of the designer like, manufacturing.
- **Micro probing (invasive)**
  - It requires directly access the chip surface to observe, manipulate, and interact with the chip
  - It observes, manipulates, interferes with the chip
- **Fault generation (semi- or non-invasive)**
  - Attacker generate/create fault, normally faulty input or make the chip run in abnormal environmental conditions
  - It cause chip to malfunction, to leak information,
  - It can also give additional access to system
  - Depending on how the fault is generated, the attack can be either be semi-invasive or non-invasive.

Physical Attacks: Classification

- **Side-channel attacks (non-invasive)**
  - Attacker monitor/measure chip’s physical characteristics (power, current, timing, EM radiation, etc.) during its normal operation.
  - Attacker perform data analysis to learn information.

- **Software attacks (non-invasive)**
  - The attacker will use normal I/O interface
  - The Attacker exploit known security vulnerabilities in protocols, algorithms and their software implementation to perform attack

(Physical Attacks and Countermeasures)

Physical Attacks

- **Invasive**
- **Semi-invasive**
- **Non-Invasive**

Invasive Attacks

- **Decapsulation and deprocessing**
  - Remove the package (i.e., depackaging) to expose the silicon die
  - The deep processing removes layer by layer and allows attackers to study features in each layer.
- **Reverse engineering (RE)**
  - Once the chip is opened, the RE can be performed to reveal chip inner structure and functionality.
- **Depassivation and microprobing**
  - RE can be done using an optical microscope with digital camera to capture high resolution image of the chip's surface in each layer.
  - More detailed information can be obtained by monitoring on-chip bus activity, at submicron precision.
  - Secret keys with sensitive data can be extracted from memory by this method
- **Chip modification**
  - With all detailed information, the attackers will be able to rebuild or modify the chip.
  - Attacker can cut certain internal interconnections (wire), disable on-chip components such as encryption blocks.
- **Cost varies but is increasing very fast** for modern chips as they requires expensive equipment and a very skilful attacking team.

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

- **Decapsulation and deprocessing**
  - Remove the package (depackage) to expose the silicon die
  - Not need any contact with internal signals or bus lines, thus, the expensive microprobing station and the other equipment may not be required.
- **Launching attacks:** Attackers will have to use other equipment to launch different semi-invasive attacks
  - **Imaging:** Attacker use optical and laser techniques (special cameras), active photon probing, backside infrared imaging to read chip layout, localize the active regions, or read the logical state of certain CMOS transistors.
  - **Fault injection:** Ultraviolet (UV) light attacks, optical fault injection, local heating, memory masking (change memory contents or disable write operation in flash)
  - **Side channel analysis:** optical emission, optically enhanced position-locked power analysis

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

Non-invasive Attacks

- **Side channel analysis (passive)**
  - It monitors the chip's execution and it collects some measurement, *i.e. Timing*, power, EM emission, acoustics, NFC.
- **Brute force (active):**
  - Strategy for organized (instead of random) search information on the chip
  - Attacker can search for keys and passwords if they are not sufficiently long.
  - Recover design (black-box attack) from the input or output pairs
  - Find backdoor access to factory test or programming mode by injecting random signals or commands applying high voltage
- **Data remanence (active)**
- **Fault injection (active)**

Both these attacks need interaction with the chip, therefore they are all active attacks. If secret keys or data are stored in SRAM, they may leak in several ways because of the physical characteristics of SRAM.

Data Remanence

- **Data remanence in SRAM:** After power is down, SRAM will still retain the data for a short period of time.
  - After power is down, SRAM still retain the data for a short period of time.
    - Attacker can try to steal or retrieve data during this period.
  - Data “burned-in” (stored) at same location for long time, it may appear after the chip is powered up again
    - Attacker can view or retrieve data right after power up
  - Data can also be “frozen” in SRAM at low temperature (-20^{o}C), data can also be freeze at higher temperature
    - Attacker can freeze data and read it

- **Data remanence in EEPROM and Flash**
  - Vth changes after after each write and then erase in such memory
    - Attacker may extract data after multiple write/erase cycles

Fault Injection Attacks

- **Idea:**
  - The idea is to manage the chip/system execute with faulty or unexpected input or command/instruction
  - Observe chip/system execution to gain unauthorized access to systems or learn secret data
- Possible to input faulty signal directly from the input/output interface. But secure systems can easily detect such faulty input before the execution starts.
- **Fault generation techniques:** How can attackers inject faults?
  - Glitches (clock, power)
  - Temperature
  - White light, laser
  - X-ray and ion beams
  - Electromagnetic flux

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

Fault Injection Attacks: Glitch

- **Glitch is a fast change in chip's supply signals (power/voltage and clock).**
  - It may affect some transistors or flip-flops.
  - Although attacker may not have control on which transistor or flip-flop will change, attacker can find security holes by a systematic search.

- **Clock glitch**
  - A shorter clock pulse cause *incorrect instruction fetch* in Motorola controllers
- **Power glitches**
  - Break AES on secure microcontroller, the careful selection of time slot can reduce the number of attempts.
  - Corrupted EEPROM data read

Countermeasures: Fault Injection

- Fault-tolerant computing techniques can be used to defend both at software level and hardware level.
- **Software approach**
  - Execution redundancy
  - Checksums on data transfers
  - Randomized execution
- **Hardware approach**
  - Redundancy (e.g., fault tolerant computing)
  - Fault detector
- Defending does come with overhead in hardware and performance.
- Detecting fault injection attacks after the attack might be too late, the damage may have already been made. For example, attackers may have already learned information about sensitive data. It is preferred to detect the faulted condition before the system executes under such conditions.

Countermeasures: Invasive Attacks

- **Bus scrambling**
  - All the databases that connect the CPU and the memory are either in the increasing order (zero page to highest page), or in the opposite order(highest to zero). This makes it easy for the attackers to locate the baseline they want to probe.
  - We can do bus scrambling (change the order/connection of data to confuse the attacker).

- **Data encryption**
  - Encrypt data and decrypt in a trusted zone: We can also encrypt sensitive data to prevent an attacker from probing it.
  - The data of the encryption needs to be decrypted in a trusted zone before it can be used.

Countermeasures: Invasive Attacks

- **Glue logic design**
  - Hide the data bus: Standard building blocks such as register files, instruction decoders, arithmetic and logical units, and input/output circuits are glued together like a ASIC instead of individual components.
  - This hides the data, the data bus, which makes impossible for attackers to find the signal to attack.

- **Sensor mesh at top metal layer**
  - Continuous monitor of all paths in the mesh: To protect from invasive attacks, most of the smart card, smart cards have a sensor mesh implemented in the top metal layer. All the paths in the mesh are monitored continuously.
  - Microprobing attempts will cause short circuits.
  - This will trigger an alarm and the memory contents will be reset to protect sensitive data.

Thank You