Physical Attacks and Tamper Resistance

Mohammad Tehranipoor

ECE6095: Hardware Security & Trust
University of Connecticut
ECE Department

What is Tamper Resistance?

- Resistance to tampering the device by either normal users or systems or others with physical access to it.
- It ranges from simple features like screws with special heads to complex devices which can zeroize the content in it or encrypt the information.

IBM’s Attacker Categories

- Class I (clever outsiders)
  - Clever but have insufficient knowledge of the system and equipment.
- Class II (knowledgeable insiders)
  - Generally have access to sophisticated equipment and tools.
- Class III (funded organizations)
  - They are funded by big organizations and have access all kind of resources.

Protection Levels

- **LEVEL ZERO**
  - No special security features. All of the parts of the device are free to access.

- **LEVEL LOW**
  - Some security features are used. It can be broken less than $500 of equipment.

- **LEVEL MODL**
  - Secure against most of the low cost attacks. Attackers need to have more expensive tools and special knowledge.

- **LEVEL MOD**
  - Special tools and equipment are required as well as special skills and knowledge. Equipment cost may range from $5000 to $50000.

- **LEVEL MODH**
  - Special design is considered for secure device. Equipment cost to attack ranges from $50000 to $200,000.

- **LEVEL HIGH**
  - It is resilient against all known attacks.

Classification Of Physical Attacks
Non-Invasive Attacks

- Do not require decapsulation of the device, so it is non-destructive.
- Do not require any initial preparation of the device under test.
  - They can be done by tapping on a wire or plugging the device in the test chip.
- Easely reproducible, so that they are not expensive.
- However, it can take a lot of time to find an attack on any particular device.

Invasive Attacks

- Penetrative attacks: expensive to perform
  - Require expensive equipment, knowledgeable attackers and time
  - Almost unlimited capabilities to extract information from chips and understand their functionality
  - Leave tamper evidence of the attack or even destroy the device
  - Getting more demanding as the device complexity increases and the size shrinks

Semi-Invasive Attacks

- Relatively new type of attack, it fills the gap between non-invasive and invasive attacks.
- Similar to the invasive attacks, they require depackaging of the device.
- But, the attacker do not need to have expensive tools such as FIB.
- Actually, these attacks are not entirely new since UV light is used to disable security fuses in EPROM for many years.
Invasive Attacks

Sample Preparation
- Decapsulation
- Deprocessing

Reverse Engineering
- Optical imaging for layout reconstruction
- Memory extraction

Microprobing
- Laser cutter
- FIB workstation

Chip Modification

Sample Preparation
- It starts with partial or full \textbf{decapsulation} of the chip to expose the chip die

- \textbf{Decapsulation} is the process of the removal of the chip package
  - It can be done easily by anyone who has high school chemistry knowledge
  - Only need to do some practice on a dozen of chip

Manual Decapsulation

Milling a hole on the Chip Package
- In this way the acid will affect the only desired area on the chip surface

Exposing the chip package to acid
- Fuming Nitric Acid or mixture of Fuming Nitric Acid and concentrated Sulphuric Acid can be used
- The acid is applied with a pipette to the hole in the chip, it should be preheated to 50-70 °C

Cleaning the chip from the reaction products
- After 10-30 second, the chip is sprayed with dry acetone several times
- Also, ultrasonic bath can be used to clean the chip die surface

Decapsulation can be done from the rear side of the chip
- Access to the chip die can be established without using any chemical
- It requires to mill down to the copper plate which can be then removed mechanically
Automated Decapsulation

For the large quantities, automated decapsulation systems can be used.
- Very little skill and experience is required to operate it.
- Such systems cost over $15,000 and so that generally relatively large labs buy them.
- Also, they consume ten times more acid than the manual decapsulation, so the disposal of the wastes should be done in a proper way.

Sample Preparation

- **Deprocessing** is the opposite process of the chip fabrication.
- It has two main applications:
  - Removing passivation layer to expose metal layers for microprobing attack
  - Gaining access to the deep layers to observe internal structure of the chip
- Three basic deprocessing methods are used:
  - Wet chemical etching
  - Plasma etching, also known as dry etching
  - Mechanical polishing

Deprocessing

- The same partial decapsulation can be applied to smart card.
- Not all of them may maintain their electrical integrity.
- Generally, smart cards are decapsulated completely.

Deprocessing

- **Wet Chemical Etching:**
  - Each layer is removed by specific chemicals
  - Its downside is its uniformity in all directions
  - Each type of material needs certain etchants to be used.
  - Nitrox wet etchant is one of the most effective etching agents for silicon nitride and silicon dioxide passivation layers which selectively removes the passivation layers of integrated circuits while preserving full device functionality.

Deprocessing

- **Plasma Etching** uses radicals created from gas inside a special chamber.
  - Only the surfaces hit by the ions are removed.
  - Similarly, each type of material needs certain enchant.
- **Mechanical polishing** performed with the use of abrasive materials.
  - Time-consuming and requires special machines.
Reverse Engineering

- Reverse engineering is a technique used for understanding of the structure of the device and its functioning.
- For ASIC, it means locations of all the transistors and interconnections.
- All the layers of the chip are removed one by one in reverse order and photographed to determine the internal structure of the chip.
- Eventually, by processing obtained information, standard netlist can be created and used to simulate the device.

Reverse Engineering: Imaging

- Optical Imaging:
  - For reverse engineering the silicon chips down to 0.18 µm feature size, an optical microscope with a digital camera can be used.
- SEM:
  - For semiconductor chips fabricated with 0.13 µm or smaller technology, images are created using a SEM which has a resolution better than 10 nm.
Reverse Engineering: Memory extraction

- Memory extraction from Mask ROMs
  - only possible for certain type of Mask ROM memory
  - For example; NOR Mask ROM with active layer programming used in Motorola MC68HC705P6A Microcontroller can be read by removing the top metal layer
  - But, same Microcontroller with newer technology requires deprocessing

Invasive Attacks: Microprobing

- Tools
  - The most important tool is microprobing station. It consists of five elements
    - a microscope, stage, device test socket, micromanipulators and probe tips.

Invasive Attacks: Microprobing

- Microprobing
  - eavesdropping on signals inside a chip
  - injection of test signals and observing the reaction
  - can be used for extraction of secret keys and memory contents
  - laser cutter can be used to remove passivation and cut metal wires
  - limited use for 0.35μm and smaller chips

Invasive Attacks: Microprobing

- Tools
  - The most important tool is microprobing station. It consists of five elements
    - a microscope, stage, device test socket, micromanipulators and probe tips.

Invasive Attacks: Microprobing

- Microprobing is applied to the internal CPU data bus
  - Difficult to observe whole data bus at a time
  - Two to four probes are used to observe data signals which are combined as a whole data trace later.
Microprobing: Laser Cutting

- It is used to remove passivation layer to observe the metal layer
- Laser Cutting Systems consist of:
  - laser head mounted on camera port of a microscope
  - submicron-precision stage to move the sample
- Carefully dosed laser flashes remove patches of the passivation layer with micrometer precision

Microprobing: FIB Workstation

- The devices fabricated with 0.5 µm or smaller technology need more sophisticated tools to establish contacts with the interconnect wires
- FIB stations can be used to create test point, imaging and repairing
- Also, FIB can mill holes and cut the wires

Invasive Attacks: Chip Modification

- It is used to disable security protection circuitry
  - By cutting one of the internal metal interconnection wires
  - by completely destroying the circuit associated with the security protection using a laser cutter
- For more sophisticated attacks FIB is used
  - connecting the wire that transmits the security state to either the ground or the supply line
- Chip modification always requires at least partial reverse engineering of the chip to find the point for possible attack
Countermeasures

- Bus Encryption
- Top-layer Sensor Meshes
- ASICs and custom ICs
- Internal Voltage and Clock Frequency Sensors
- Light Sensor

Countermeasures: Bus Encryption

- The bus encryption is used to protect the sensitive information from probing.
  - Basically, the memory content is encrypted and then sent to the CPU by data bus
  - Before the data used in CPU, it is decrypted

Countermeasure: Bus Scrambling

- Typical probing areas
  - Memory bus drivers
  - Data bus itself where lines are organized in proper CPU bus width
  - Bus order is 99.9% of the time in order (0..7 or 7..0)

Bus Scrambling

- Data bus scrambling is used to confuse attackers
  - Order of the data bus is changed to make it difficult to observe bus signals

Counterme.: Top-layer Sensor Meshes

- Additional metallization layers that
  - form a sensor mesh above the actual circuit
  - do not carry any critical signals
- All the paths in a sensor mesh are continuously monitored for interruptions and short-circuits while power is available
  - It prevents laser cutter or selective etching access to the bus lines.
- Also, mesh layer hides the lower layer which makes navigation on the chip surface for probing and FIB editing more tedious.
Countermeasures: Top-layer Sensor Meshes

Figure 9: Escape route for improved crypto logic. The ‘YES’ logic design was added to this redundant etching of the bus. The netlists were then added to the protected mask area, providing easy probing access.

Figure 11: A FIB was used here to drill a fine hole into a bus line through the gap between two sensor mesh lines, refill it with metal, and place a metal cross on top for easy micropointing access.

Countermeasures: ASICs and Custom ICs

- Types of ASIC design
  - Glue logic design from VHDL or logic level (Netlist)
  - Fully custom design with security requirements

Countermeasures: Sensors

- Different kind of sensors can be used to detect attack attempt
  - Voltage and frequency sensors for glitching attacks
  - Light sensor can be helpful against decapsulation of the device
- Special purpose sensors can be created to detect probing.
  - Ring oscillator based detector (Probing Attempt Detector)

Sensors: Probing Attempt Detector

- Exploits the fact that probing will change the capacitance in the bus line.
  - Place ring oscillators on the bus lines
  - When the probe touches the one or more bus lines, frequency of the ring oscillator changes
  - PAD observes the bus lines continuously, when they have significant difference, it sets a flag that there is a probing attempt on the one of the lines

Sensors: Probing Attempt Detector

- Sample Preparation
  - Decapsulation
- Imaging
  - Backside imaging techniques
- Perform the Attacks
  - UV light attacks
  - Active photon probing
  - Optical Fault injection attacks

Semi-Invasive Attacks

25 December 2012
Semi-Invasive Attacks: Sample Preparation

- Decapsulation of the chip to prepare it for attacks.
- For the modern chips, backside decapsulation is used
  - There is no need to use chemicals

Semi-Invasive Attacks: Imaging

- Down to 0.8 μm technology, it was possible to identify all the major elements of microcontrollers – ROM, EEPROM, SRAM, CPU
- Difficult to distinguish for newer technologies
- Can be observed with infrared light from rear side
- Backside imaging also is useful to extract the Mask ROM content

UV Attacks: Locating the Security Fuses

- Security fuse
  - Controls access to the information stored in on-chip memory
  - They are physically located in the chip die
  - They are the separate memory cells from the main memory array
  - If they are away from the main memory or next to it, the security is not very high as the fuses can be found and disabled.
  - Better protection can be achieved when the security fuses are located on the same memory array
UV Attacks

- If fuses are close the main memory, UV light can be used to locate them.
- After, finding the security fuses, five to ten minutes under UV light should give the proper result. Then, memory is ready to read.

Semi-Invasive Attacks: Active Photon Probing

- Laser radiation can ionize an IC's semiconductor regions if its photon energy exceeds the semiconductor band gap.
- In active photon probing, a scanned photon beam interacts with an IC.
- Laser scanning techniques (LST)
  - One is called optical beam induced current (OBIC) and is applied to an unbiased chip to find the active doped areas on its surface.
  - Another is called light-induced voltage alteration (LIVA), applied to a chip under operation.

Laser scanning techniques

- Red low power laser beams ionize active areas.
  - Power off imaging identifies active areas.
  - Power on imaging distinguishes between closed and opened transistor channels.

Semi-Invasive: Optical Fault injection attacks

- Illumination of a target transistor causes it to conduct, thereby inducing a transient fault.
- Such attacks
  - Practical
  - Do not require expensive laser equipment
  - Any individual bit of SRAM in microcontroller can be set or reset.

Fault injection attacks: Changing SRAM contents

- Figure 91: SRAM memory array with maximum magnification (500x).
- Figure 92: Allocation of data bits in SRAM memory array.
Non-volatile memory contents modification

- EPROM, EEPROM and Flash memory cells are even more sensitive to fault injection attacks.
- They can be changed by light
- This attacks can be used to disable security fuses
  - The light should be focused down to the security fuse
- These attacks do not work on modern chips built in smaller sizes

References

- Semi-invasive attacks A new approach to hardware security analysis, Sergei P. Skorobogatov
- Physical Attacks and Tamper Resistance Sergei Skorobogatov
- Wet and Dry Etching Avinash P. Nayak Logeeswaran VJ and M. Saif Islam
- Security Failures in Secure Devices, Christopher Tarnovsky Black Hat, DC

- www.flylogic.net/blog
- http://www.siliconzoo.org/
- Smart Card Handbook, by Wolfgang Ranki, Wolfgang Effing
- Detection of Probing Attempts in Secure ICs, Salvador Manich, Markus S. Wamser and Georg Sigl