David Murillo Santiago
Dr. Pugh
IS-3513
26 September 2023

Case Study #2 Questions

1. What are the seven main types of Side Channel Attacks (SCA)?

Side Channel Attacks represent a significant concern in the realm of home security, particularly in the context of smart homes. SCA attacks exploit the unintended data leakage from various smart devices, such as sensors and appliances, within the home environment. There are seven types of SCA attacks: Timing analysis, traffic analysis, electromagnetic analysis, simple power analysis, differential power analysis, fault analysis, acoustic analysis.

Timing Analysis

Timing analysis involves examining timestamps associated with various operations in a system. These attacks capitalize on the observation that each operation in a computer consumes a specific amount of execution time, depending on the input it receives. By measuring the time spent on operations, an attacker could deduce confidential system information. This attack is useful for global eavesdroppers when they are looking for contextual information of a wireless network.

Traffic Analysis

Traffic analysis is a type of attack that centers on monitoring and analyzing network traffic patterns to extract information about a system. Attackers monitor, track, count, and record packets and their transmission intervals. Through the analysis of this data, attackers can determine the source and destination of the packets.

Electromagnetic Analysis

Electromagnetic analysis is a technique employed to compromise cryptographic systems. As cryptographic devices perform encryption or decryption, they emit radiation that attackers could exploit to identify correlations between the leaked radiation and encrypted data.

Simple Power Analysis

Simple power analysis aims to uncover sensitive information by visually observing power consumption fluctuations during the execution of cryptographic algorithms. By monitoring these fluctuations, attackers could discern which encryption method is being applied on the signal.

Differential Power Analysis

Differential power analysis, similar to simple power analysis, aims to uncover encryption keys by analyzing power consumption fluctuations. However, it distinguishes itself by examining both non-cryptographic and cryptographic operations, then comparing their power consumptions patterns.

Fault Analysis

Fault analysis intentionally introduces errors into a cryptographic device or system to analyze its behavior. These errors or faults are deliberately injected into cryptographic system through tactics like altering the temperature, applying laser beams at special frequencies, or injecting fake packets to raise likelihood of collision. The goal is to create discrepancies in the device's regular operation and observe its responses.

Acoustic Analysis

Acoustic analysis extracts sensitive information by analyzing the sound emissions produced by electronic devices during their operation. This process exploits the unique sound patterns generated by these devices, and trained model can be used to distinguish subtle sound variations.

2. What are three classes of SCA?

Side-Channel Attacks are categorized into three classes based on their level of intrusion: invasive, semi-invasive, and non-invasive attacks:

Invasive Attacks

Invasive attacks represent the most intrusive form of Side-Channel Attack, necessitating physical engagement with the target device, which often results in the device's destruction. These attacks are typically conducted when the attacker has direct physical access to the device. Fault analysis falls under the category of invasive attacks because tampering with the devices often results in the destruction of the device.

Semi-Invasive Attacks

Semi-invasive attacks require physical modification to the target device, but they do not destroy it. These attacks are conducted when an attacked aims to gain insights into the device's operation. Simple and differential power analysis, as well as acoustic analysis, are classified as semi-invasive attacks because they require physical access or proximity to the target device but do not lead to the destruction of the device.

Non-Invasive Attacks

Non-invasive attacks are characterized by their lack of physical contact with the target device. Instead, they rely on externally accessible information such as monitoring power consumption or observing network traffic. Timing, traffic, and electromagnetic analysis fall under the category of non-invasive attacks because they do not require physical access to the target device and can often be performed remotely.

3. What are the two types of SCA behavior?

There are two-types of SCA behavior based on how attackers interact with a system: passive and active attacks.

Passive Attacks

Passive attacks only exploit the output of a system.

Active Attacks

Active attacks involve manipulating system inputs and collecting and studying the subsequent outputs.

4. SCA always assume what?

Depending on the type of Side-Channel Attack, SCA makes various assumptions, with one fundamental assumption being that data constantly leaks from the target device. This constant leakage from target devices offers attackers the opportunity to exploit data leakage and discover meaningful patterns within the data.

5. The authors emphasize the vulnerabilities within what? Give two examples of devices with potential vulnerabilities.

The author emphasizes vulnerabilities within smart home systems due to the modern rise of the Internet of Things. Two examples of devices with potential vulnerabilities in smart home systems are Smart TVs and Smart Locks.

Smart TVs

Potential risks associated with smart TVs include firmware modification and content recognition. Attackers may exploit firmware modification to gain unauthorized access or manipulate the TVs behavior. On the other hand, content recognition exploits discern the content being watched on a smart TV, thus compromising user privacy.

Smart Locks

Potential risks associated with smart locks include revocation evasion attacks and access log evasion attacks. Revocation evasion attacks target the feature in smart locks that allows owners to revoke access for other users, enabling attackers to maintain access even after owners has revoked it. Access log evasion attacks allow hackers to circumvent the log recording security measures to conceal their unauthorized entries.