Case Study on Various Countermeasures to Avoid Side Channel Attacks

P. G. V. Suresh Kumar

Associate Professor, Department of IT & SC, AAiT, Addis Ababa University
Addis Ababa, Ethiopia

Abstract -- *Side Channel Attacks is relatively a new area in cryptography that has gained more and more interest in early nineties. The side channel attacks are implemented on the physical domain exploiting the characteristics of the physical objects used in the cryptography. These implementations attacks sometimes turn out to be much more efficient than the best known cryptanalytic attacks. This paper aims to give an introduction to various types of side channel attacks and provides various countermeasures to avoid them.*

Keywords *– Side Channel Attacks, Timing Attacks, Fault attacks*

I. INTRODUCTION

Cryptography is a technique of prohibiting a message from being accessed even if the message is being possessed by a person for whom the message was not intended to. The motive or the main aim of cryptography itself arouses the curiosity of the unintended user to access the message. For satisfying this urge several approaches have been adopted by the unintended user to access the message. The traditional approach was the mathematical abstraction. A new approach that has paved a very significant path in cryptanalysis during the recent years is the Side Channel Analysis **[4]**.

Side channel attacks exploit the possibility of attacks that utilizes the information leaked during the implementation, operation and implementation environment of the message protocol's execution. The safeguard of this information was not considered in the traditional security models. But as the advancements in the side channel attacks are being made, the focus is being transferred to secure the protocol of the side channel attacks.

The side channel attacks are implemented on the physical domain exploiting the characteristics of the physical objects used in the cryptography. Thus for the implementation of side channel attacks the attacker has to know the internal functioning of the system. The side channel attacks are different from the brute force attacks and are certainly does not the focuses on attempts to break a cryptosystem by deceiving or coercing people with legitimate access. The side channel techniques are of concern because they can be easily mounted on the system and can be implemented using existing hardware.

Section II of this paper covers the various classifications of side channel attacks. Section III describes the various types of side channel attacks. It also covers some of the recent approaches adopted by the cryptanalysts for side channel analysis. Section IV describes the counter measures to avoid the side channel attacks. Section V includes conclusion of this paper. And the last section includes references used for making this paper.

II. CLASSIFICATION OF SIDE CHANNEL ATTACKS

Side channel attacks can be classified into two main classes [4]:-

- Classifications depending the control over computation process
- Classifications depending on the way of accessing the module

A. DEPENDING ON THE CONTROL OVER THE COMPUTATION PROCESS

This classification deals with the control over the computation process by the attackers and is divided into two main categories, viz, the active attacks and the passive attacks **[1]**.

The passive attacks don't interfere with the functioning of the target system but rather they just monitor the system during functioning and in the process will not disturb the device's functioning. These attacks are usually difficult to detect as there

is no modification in the functioning of the system which can be detected later on.

The active attacks on the other hand interfere with the functioning of the system and they exert some influence on the behavior of the attacked system. In the process neither the system nor the attacked party knows of the attack. But however an outside observer would be able to note the difference in the operation of the system.

The difference between the two types of attacks lies in the nature of the two attacks than the implementation of the attacks.

B. DEPENDING ON THE WAY OF ACCESSING THE MODULE [4], [7]

This classification deals with the type of control over the attacked surface, i.e., the physical, electrical and the logical interfaces that are exposed to the attacker. Thus Anderson et al made a classification of this as the invasive attacks, semi-invasive attacks and the non-invasive attacks.

INVASIVE ATTACKS

The invasive attack involves disassembling the cryptographic devices to get access to the internal components of the devices. This can be like the tapping on the conversation between two parties by gaining access to the wire between the two parties by sabotaging the wire.

NON-INVASIVE ATTACKS

The non invasive attack involves the close observation or the manipulation of the device's operation. This Exploit's the externally available information that is unintentionally leaked. This can be like having access to the conversation between two parties by the degradation of the wire and the leakage of the signal carried by the wire.

SEMI-INVASIVE ATTACKS

The semi-invasive attacks were introduced later than the invasive or the non-invasive attacks. This classification was given by Skorbogatov and Anderson. The semi-invasive attacks involve the gaining of access to the device but without making electrical contact other than with the authorized surface. This can be like tapping the conversation between two parties by the telephone company persons.

Out of the three classifications of these attacks the non-invasive attacks is completely undetectable. This is because there is no way of identifying if the attack has been made or not. On the other hand, the invasive attack requires processing of the individual device the non invasive attack are low cost and don't require much of the processing on the hardware. Thus the non-invasive attacks are much of a hurdle to the industry.

.

III. DIFFERENT TYPES OF SIDE CHANNEL ATTACKS

3.1. TIMING ATTACKS [3]

Are based on measuring the time it takes for a unit to perform operations. This information can lead to information about the secret keys. For example: By carefully measuring the amount of time required to perform private key operations, an attacker might fixed Diffie-Hellman exponents, factor RSA keys , and break other cryptosystems. If a unit is vulnerable, the attack is computationally simple and often requires only known cipher text.

Cryptosystems often take slightly different amounts of time to process different inputs. Timing measurements are fed into a statistical model that can provide the guessed key bit with some degree of certainty (by checking correlations between time measurements).

3.2. POWER CONSUMPTION ATTACKS

These attacks are based on analyzing the power consumption of the unit while it performs the encryption operation. By either simple or differential analysis of the power the unit consumes , an attacker can learn about the processes that are occurring inside the unit and gain some information that, when combined with other cryptanalysis techniques , can assist in the recovery of the secret key.

3.2.1. SIMPLE POWER ANALYSIS ATTACKS

It is generally based on looking at the visual representation of the power consumption of a unit while an encryption operation is being performed. Simple power analysis is a technique that involves direct interpretation of power consumption measurements collected during cryptographic operations. SPA can yield information bout a device's operation as well as key material. The attacker directly observes a system's power consumption. The amount of power consumed varies

depending on the microprocessor instruction performed. SPA analysis can for example , be used to break RSA implementations by revealing differences between multiplication and squaring operations. Similarly, many DES implementations have visible differences within permutations and shifts , and can thus be broken using SPA.

3.2.2. DIFFERENTIAL POWER ANALYSIS ATTACKS

These attacks are harder to prevent. They consist not only of visual but also statistical analysis and error-corrections statistical methods, to obtain information about the keys. DPA usually consists of data collection and data analysis stages that make extensive use of statistical functions for noise filtering as well as for gaining additional information about the processes that a unit is performing.

3.3. DIFFERENTIAL FAULT ANALYSIS ATTACKS

Fault analysis relates the ability to investigate ciphers and extract keys by generating faults in a system that is in the possession of the attacker, or by natural faults that occur. Faults are the most often caused by changing the voltage, tampering with the clock, or by applying radiation of various types. These attacks are based on encrypting the same piece of data twice and comparing the results. A one bit difference indicates a fault in one of the operations. Another type of fault analysis is the Non-Differential Fault Analysis Attacks but this is based on causing permanent damage to devices for the purpose of extracting symmetric keys. It must be mentioned that a trait of such attacks is that they do not require correct cipher texts. This leads to the attacker being able to make use of natural faulty units, without himself tampering with them

3.4. ACOUSTIC ATTACKS

Acoustic emanations are one of the oldest eavesdropping channels. Acoustic cryptanalysis is a type of side channel attack which extracts information unintentionally exploited from sounds produced during a computation or input-output operation. Eg: computer and keyboards and keypads used on telephones and Automated Teller Machines (ATMs) are vulnerable to attacks based on differentiating the sound produced by different keys.

3.5. CACHE ATTACKS

The main source of leakage in a cryptographic algorithm is from the cache memory. Cache memory is present on almost every computing system and makes use of the temporal and spatial locality of the code to improve the overall execution time of the program. The time required to access data present in the cache is much lesser than the time required to access data stored in memory. Thus the cache memory is used to provide access to the data at a much faster rate. The cache is a memory present between the CPU and the Main Memory and is used to speed program on the run time on an average. If the data accessed by the CPU is found in the cache then it is known as a hit. If it is not found in the cache memory it is referred to a miss. If a miss occurs then the CPU will look for the data in the main memory. This will, however, cause a delay, as the target data will be loaded from the main memory to the cache memory. This differential timing for memory access is used by attackers to gain knowledge of the secret key of a cryptographic algorithm and these types of attacks are known as cache attacks.

3.6. ELECTROMAGNETIC ANALYSIS

The electromagnetic attacks are based on the electromagnetic signals due to the current flowing in microelectronics. The components of the computer often generate electromagnetic radiation in their operation. This side channel information is used in the electromagnetic attacks. The measurement once acquired can be classified as the Simple Electro-Magnetic Analysis (SEMA) and Differential Electro-Magnetic Analysis (DEMA) similar to the Power Attacks. Electromagnetic analysis is not limited to measurements of overall device power consumption; electromagnetic analysis can target specific areas of the chip by positioning a small antenna. EM attacks can also be implemented by an attacker situated away from the hardware thus not requiring the physical access of the attacker. For example early attacks could use simple AM demodulators even a few meters away from the chip. This also causes the EM attacks to suffer complications due to noise, RF interference, and measurement error.

IV. PREVENTION OF SIDE CHANNEL ATTACKS

This section of the paper brings forth the techniques, the execution of which can prevent the side channel attack to be implemented. These techniques are

implemented by the designers to provide security from the attackers.

4.1. GENEARL COUNTERMEASURES AGAINST ALL ATTACKS

4.1.1. GENERAL DATA INDEPENDENT CALULATIONS

A general approach is that whole of the module operations should be data independent in their time consumption, i.e., the input data should be of uniform length. This makes the clock cycles the same in number in each of the operations. This approach prevents the occurrence of timing attacks as the timing attacks exploit the variation of the computation time of the input data. When the input data is of uniform length then the attacker cannot make any meaningful deductions in the time domain.

4.1.2. BLINDING

Blinding is a technique to prevent the attacker from knowing the exponentiation function or the data input. It is a technique by which an agent can compute a function for a client in an encoded form without knowing either the real input or the real output. Blinding prevents against all of the side channel attacks.

4.1.3. ADDING DELAYS

In this approach all the operations take equal amount of time to execute. This is by adding the delays in the program. The delays can be either fixed or be randomized. In case of fixed delays the delays are fixed to the slowest operations i.e. all operations take time as much as the slowest of the operations. In case of adding random delays the power analysis can be performed. Although the number of computations would be very large for power analysis but still it can be performed.

4.1.4. TIME EQUALIZATION OF MULTIPLICATION AND SQUARING

In this approach the time taken for performing the multiplication and the exponentiation actions is set to be similar. Thus the attacker is unable to learn the number of multiplications or exponentiations performed. In this, both the multiplication and exponentiation operations are performed where in normal operation only one would be performed. This thus safeguards the system against the timing attacks.

V. CONCLUSION

For many years, cryptology may have been a struggle between cryptographers and cryptanalysts. From past years, there have been many attacks on them. In this paper, we surveyed what are the different types of Side Channel Attacks and various countermeasures against them.

ACKNOWLEDGEMENT

We would like to convey our gratitude to Sri. P. Bhaskara Rao, Retd. Teacher, India, Nune Srinivas, faculty of SECE, Mrs. Pendem Padmaja, India, and a special thanks to Mr. P.V. Subrahmanyeswara Rao, before their technical support to realize the this proposal discussed in this paper.

REFERENCES

[1] Elisabeth Oswald Bart Preneel “A Survey on Passive Side-Channel Attacks and their Countermeasures for the NESSIE Public-Key Cryptosystems”.

[2] Jem Berkes, University of Waterloo ‘Hardware Attacks on Cryptographic Devices & Implementation Attacks on Embedded Systems and Other Portable Hardware”.

[3] Chester Rebeiro, Mainack Mondal, and Debdeep Mukhopadhyay “Pinpointing Cache Timing Attacks on AES”, Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur, India.

[4] Francios-Xavier Standaert, “Introduction to Side channel attacks” , UCL Crypto Group, Place du Levant 3, B-1348 Louvain-la-Neuve, Belgium.

[5] Hagai Bar-El ,”Intoduction to side channel attacks”, White paper.

[6] YoungBin Zhou, DengGuo Feng ,“Side-Channel Attacks: Ten Years After Its Publication And the Impacts on Cryptographic Module Security Testing” The work of this paper is funded by the National Natural Science Foundation of P.R. China under the Grant No. 60503014 & No. 60273027 & No. 60373039.