Side Channel Attack-Survey

[1]JOY PERSIAL G, [2]PRABHU M, [3]SHANMUGALAKSHMI R.

[1]PG Scholor Dept of CSE, Adhiyamaan College of Engineering, Hosur, TamilNadu, India.
[2&3]Assoc. Prof. Dept of CSE, Adhiyamaan College of Engineering, Hosur, TamilNadu, India.

ABSTRACT
The need for security has gained more importance in this information intense society. Cryptography is the design and analysis of mathematical structures that enable secure communications in the presence of malicious adversaries. Side channel attacks are a recent class of attacks that is very powerful in practice. By measuring side channel information, the attacker is able to recover very sensitive information. This paper shows the survey on different possible side channel attacks and the possible measure to overcome the attack.

KEYWORDS**:** *Side channel Attack, Cryptography, Mathematical Function, Sensitive Information*

I. INTRODUCTION

Security is as strong as the weakest link. We live in an age in which almost all sensitive information is controlled and distributed via computer networks. We have come a long way in protecting this information with a wide array of cryptographic schemes and protocols, but there are still many concerns for systems in which the physical implementations can be accessed. Systems which make use of crypto- graphic protocols that we use everyday such as ATM's is vulnerable to implementation attacks. Given physical access to the targeted device, an attacker can recover sensitive information which is otherwise supposed to be hidden, such as the devices key used for encryption. These devices being readily available for physical access and an increasing number of individuals are deploying these attacks for personal gain therefore there is an evident need for raising the robustness of our current cryptographic implementations by introducing countermeasures in both hardware and software.

Physical attacks on cryptographic devices take advantage of implementation-specific characteristics to recover the secret parameters involved in the computation. The side-channel attacks are a class of physical attacks in which an adversary tries to exploit physical information leakages [9]. The rapid increase in the use of embedded systems for performing secure transactions has proportionally increased the security threats which are faced by such devices. Side channel attack is a sophisticated security threat to embedded devices. Side-channel attacks derive information about the functional behavior of a system, without utilizing the intended interface to the system. In other words SCA is a method for extracting information from electronic devices through analyzing their physical characteristics. Side channel attack exploits the external manifestations like processing time, power consumption and electromagnetic emission to identify the internal computations [8]. The analysis is often applied to cryptographic devices in order to investigate the leakage of secret data, such as keys and PIN codes [10]. The results are used to identify weaknesses in the implementation of hardware and software. Side-channel analysis is an important instrument in the product development and evaluation cycle of secure devices and contributes to reaching a high level of security.

This paper provides a brief discussion about different Side Channel Attacks and the possible countermeasures. The next section provides gives a detailed description about related work and the tools that were used to measure attacks. Section 3 presents the different possible Side Channel Attacks. Section 4 provides the possible countermeasures and finally section 5 provides conclusion.

II. RELATED WORK

Since the beginning of 2005, Riscure has offered companies a software tool to perform side channel analysis (e.g. Power Analysis). It is the first side-channel analysis tool on the market with a fully graphical user interface. Evaluation labs and manufacturers can use the tool to test the system against susceptibility to side-channel attacks and to rapidly implement their own new side channel analysis techniques. Manufacturers and evaluation labs spend therefore each year considerable research efforts to ensure that the systems are not vulnerable to the latest side-channel attacks. Each manufacturer and evaluation lab develops its own proprietary side channel analysis testing software. These existing tools have several problems. First of all, they show a lack of flexibility to implement new side-channel attacks. Second, development and maintenance can be expensive for relatively small manufacturers and labs. Third, these tools are usually not very user-friendly as they are command-line driven. Fourth and final, effective operation is usually limited to the one or two experts that were involved with coding the tool from the beginning. So, although in the last couple of years, side-channel analysis has moved from an experimental and exotic attack class to an accepted and relatively mature one, the development of tools has lagged behind. In addition, the importance of protection against side-channel attacks has become paramount and sole dependence on an external lab which gives the manufacturer understandably an uneasy feeling.

III. BACKGROUND

Side-channel cryptanalysis is a branch of cryptography in which sensitive information is gained from the physical implementation of a target cryptosystem [15]. This is in contrast with other forms of cryptanalysis where the algorithms and their underlying computational problems are attacked. All electronic devices leak information in a multitude of ways [4]. Side Channel Attacks look for information through other unintended channels from the target device. These could be timing or power traces of inner operations of the device, or faulty outputs produced by it [5]. Cryptanalysis side channel attacks don't attack the mathematical basis of an algorithm but a physical implementation [6].
Attacks that use a few observations are referred to as simple side channel attacks. The 'simple' refers to the number of measurements used and not to the simplicity of the attacks. In fact, they require a precise knowledge of the architecture and implementation of both the device and the algorithm and their effect on the observed measurement sample. As a result, they are relatively easy to protect from.
Attacks that use many observations are referred to as differential side-channel attacks. The timing attacks typically target variable instruction flow. Their focus is on public key ciphers as symmetric ciphers, which always perform the same operations, can easily aside from the cache effects be made constant time. The public key ciphers can be effectively protected using masking or blinding techniques that prevent collecting multiple measurements of the same operation on different data.
The different possible side channel attacks are: Timing Attacks, Power Analysis Attacks, Electromagnetic Analysis Attacks, Fault Induction Attacks, Optical Side Channel Attacks, Traffic analysis attack, Acoustic attacks, and Thermal Imaging attacks.

3.1 Timing attack

The running time of a cryptographic device can constitute an information channel, providing the attacker with invaluable information on the secret parameters involved. In timing attack, the information at the disposal of the attacker is a set of messages that have been processed by the cryptographic device and, for each of them; the corresponding running time is analyzed.[1] The goal is to recover the secret parameters.

3.2 Power analysis attack

The power consumption of a cryptographic device may provide much information about the operations that take place and the involved parameters [13].

Simple power analysis

Simple power analysis (SPA) is the simplest of the side channel power analysis attacks, where the power traces of cryptosystem device are recorded and examined to identify weaknesses or visible

characteristics that could be used to break the cryptosystem and retrieve the secret key. A trace refers to a set of power consumption measurements taken across a cryptographic operation.

Differential Power Analysis

The more popular and powerful side channel power attack is the Differential Power Analysis (DPA) attack [3] [5].

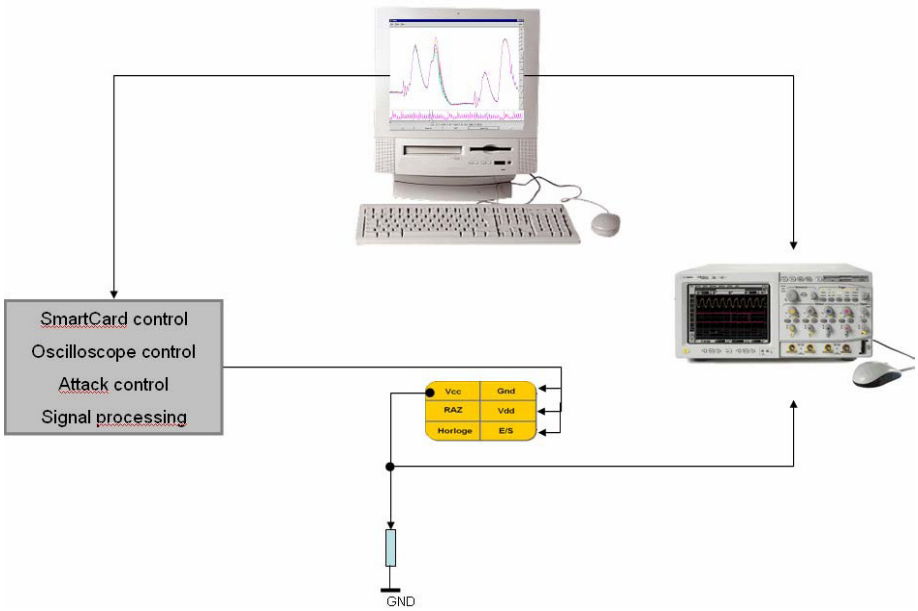

Figure 1 - A DPA attack platform

DPA requires no kind of physical intrusion into the cryptographic hardware and can he carried out by any attacker who has sufficient knowledge of the internal workings i.e., cryptographic algorithm of the cryptosystem, with little or no information on the implementation. DPA attacks attempt to extract micro-patterns and use statistical correlations between power consumed by the cryptosystem and the input data. An example for Differential Power Analysis is shown in Figure 1.

Higher-Order Differential Power Analysis

Higher-Order Differential Power Analysis (HODPA) is a combination of DPA attacks, timing attacks and traditional cryptanalysis [7]. It combines several data sources, different time offsets, and higher forms of signal processing to break the cryptosystem.

Correlation Power Analysis

Correlation approaches are based on the relation between the actual power consumption of a circuit and a power consumption model e.g., the Hamming weight model. The relationship between the power consumption and the Hamming distance is linear and the correct key is the one which maximizes their correlation factor [11] [12].

Template attack

A new variant of power analysis attack, named template attack, was proposed by Chari et al. In theoretical sense this is the strongest form of side channel attack. This attack requires that an adversary has access to an identical experimental device that he can program to his choosing.

3.3 Electromagnetic attack

Any movement of electric charges is accompanied by an electromagnetic field. The currents going through a processor can characterize it according to its spectral signature. The information measured can be analyzed in the same way as power consumption as simple and differential electromagnetic analysis (SEMA and DEMA), but may also provide much more information and are therefore very useful, even when power consumption is available. EMA is a non-invasive attack, as it consists in measuring the near field.

3.4 Fault induction attack

Faulty computations are sometimes the easiest way to discover a secret key. A recent and more powerful cryptanalysis technique consists of tampering with a device in order to have it perform some erroneous operations, hoping that the result of that erroneous behavior will leak information about the secret parameters involved [12]. The fault can be characterized from several aspects [1].
Permanent and transient:
A permanent fault damages the cryptographic device in a permanent way, so that it will behave incorrectly in all future computations; such damage includes freezing a memory cell to a constant value, cutting a data bus wire, etc.
In transient fault, the device is disturbed during its processing, so that it will perform faults in that specific computation. Examples of such disturbances are radioactive bombing, abnormally high or low clock frequency, abnormal voltage in power supply, etc.
Error location:
Some attacks require the ability to induce the fault in a very specific location such as memory cell.
Time of occurrence:
Some attacks require being able to induce the fault at a specific time during the computation, while others do not.

3.5 Optical Side Channel Attacks

The intensity of light emissions from a monitor or liquid crystal display is used to study the contents of the last displayed screen. Given the form-factor optical side channel attacks on sensor nodes are formulated differently from the attacks on devices that use a visual display to output the information. The sensor nodes have light emitting diodes (LED), which have two primary purposes. The first purpose is in debugging the application program while programming the node and the second use is for the purpose of signaling. LEDs are externally visible to both the user as well as an adversary, unless the node is used for an application in which they are not in the line of sight [14].

3.6 Traffic Analysis Attacks

Traffic analysis attacks are attacks that analyze traffic flow to gather topological information. This traffic flow could get information about critical nodes in a sensor network. Due to the limited energy capacity of nodes and the fact that the transceiver component of a node consumes the most power, the nodes in a sensor network limit the use of the transceiver to transmit or receive information either at a regulated time interval or only when an event has been detected.

3.7 Acoustic attacks

Acoustic attacks are classified into acoustic emissions from keyboards and acoustic emissions from computing components such as CPU and memory. Acoustic emissions are produced by a keyboard when different keys are pressed and can be used to identify the keys being pressed with extra triangulation information [14]. Acoustic emissions from computing components are exploitable.

3.8 Thermal Imaging attacks

Thermal imaging attacks differ from acoustic attacks in that the emission being exploited is heat instead of sound. Such attacks often exploit the infrared images emanating from CPUs.

IV. DISCUSSION AND RESULTS

Timing attacks can be prevented by hiding variations or blinding [1]. The simplest way to hide variation is to make the computation strictly constant time, for all possible secret exponents. Another possibility is to modify the Montgomery algorithm so that an additional subtraction is always carried out, even if its result is simply discarded afterwards. This modification is easy to carry out, does not decrease performance very much and clearly defeats the attack. The other type consists in hiding internal state, so that the attacker cannot simulate internal computations any more.
Power consumption is reduced with masking and elimination techniques. Masking randomizes the signal values at the internal circuit nodes while still producing the correct cipher text. This can be done at the algorithmic level where a random mask is added to the data prior to the encryption and

removed afterwards without changing the encryption result or at the circuit level where a random mask-bit equalizes the output transition probabilities of each logic gate. The key notion behind elimination (hiding) is to remove power variation information available to the attacker. Provide aggressive physical shielding to hide data [2].

Electromagnetic information leakage is prevented by encompassing the node with a casing so as to prevent access to individual components. The measure is to use secret shares in which the original computation is divided probabilistically such that the power subset of shares is statistically independent. Another technique called Masking in which the intermediate variable is not dependent on an easily accessible subset of secret key. This result in making it impossible to deduce the secret key with partial information gathered through EM leakage.

The most common way to protect against Fault induction attack is to check the computation [1]. Another way to check for the presence of faults is to verify the signature. The best way is to double check the calculation [2].

One practical and effective measure for acoustic attacks is to encapsulate a node in sound absorbing material. Another measure is to introduce random acoustic noise of similar frequency to obfuscate acoustic emissions from nodes.

To counter thermal imaging attacks, one approach is to use a dual layered case with the inner layer a highly conducting surface and the outer layer made of a non-conducting material. When heat is generated from internal computing components, the inner, highly conducting surface will quickly dissipate the heat around. The outer layer prevents accesses to the temporary hot spots formed on the inner layer.

V. CONCLUSION

Side Channel Attacks continue to be a challenge for cryptographic system designers. It is not possible to design a general framework to counter them and also there is no perfect measure against them. At best we can limit the threat to more skilled, more resourceful, better trained adversaries. As always, security must be considered from an economical point of view. The study of side channel attacks is seeing a surge in interest.

REFERENCES

[1] Prof. Jean-Jacques Quisquater, Math Rizk, Side Channel Attack - State of the art, October 2002.

[2] Surinderjeet Singh, Side Channel Attacks Department of Computer Science, Indian Institute of Technology Bombay, April 14, 2009.

[3] , Daniel Mesquita, Benoît Badrignan, Lionel Torres, Gilles Sassattell, Michel Robert, Jean-Claude Bajard, Fernando Moraes, A Leak Resistant Architecture against Side Channel Attacks.

[4] Katsuyuki Okeya, Kouichi Sakurai, A Multiple Power Analysis Breaks the Advanced Version of the Randomized Addition-Subtraction Chains Countermeasure against Side Channel Attacks, ITW2003, Paris, France, March 31 -April 4, 2003.

[5] You-Seok Lee, Yong Je Choi, Dong-Guk Han, Ho Won Kim, Hyoung-Nam Kim, A Nobel Key-Search Method for Side Channel Attacks based on Pattern Recognition, ICASSP 2008.

[6] Jens R¨udinger, Adolf Finger, Algorithm Design and Side Channel Vulnerability on the Example of DPA Attack, Proceedings of the Sixth International Conference on Networking (ICN'07).

[7] Vijay Sundaresan, Srividhya Rammohan and Ranga Vemuri, Defense against Side-Channel Power Analysis Attacks on M:icroelectronic Systems,.

[8] Jingfei Kong, Onur Acıiçmez, Jean-Pierre Seifert and Huiyang Zhou, Hardware-Software Integrated Approaches to Defend Against Software Cache-based Side Channel Attacks, 2008 IEEE.

[9] Thanh-Ha Le, Jessy Clediere, Christine Serviere, Jean-Louis Lacoume, How can Signal Processing benefit Side Channel Attacks, 2007 IEEE.

[10] Jens R¨udinger, Adolf Finger, Key Dependent Operation and Algorithm Specific Complexity of Statistical Side Channel Attacks, 2009 IEEE.

[11] Thanh-Ha Le, Jessy Clédière, Christine Servière, and Jean-Louis Lacoume, Senior Member, IEEE, Noise Reduction in Side Channel Attack Using Fourth-Order Cumulant, IEEE Transactions on Information Forensics and Security, Vol. 2, No. 4, December 2007.

[12] Christophe Clavier, Passive and Active Combined Attacks on AES - Combining Fault Attacks and Side Channel Analysis, 2010 Workshop on Fault Diagnosis and Tolerance in Cryptography.

[13] Frederic Amiel, Karine Villegas, Passive and Active Combined Attacks –Combining Fault Attacks and Side Channel Analysis, 2007 Workshop on Fault Diagnosis and Tolerance in Cryptography.
[14] Kanthakumar Pongaliur1 Zubin Abraham1 Alex X. Liu1 Li Xiao1 Leo Kempel, Securing Sensor Nodes Against Side Channel Attacks, 2008 11th IEEE High Assurance Systems Engineering Symposium.
[15] Mohammad Zahiduf Rahaman and Mohammad Akram Hossain, Side Channel Attack Prevention for AES Smart Card, Proceedings of 11 th International Conference on Computer and Information Technology (ICCIT 2008) 25-27 December, 2008, Khulna, Bangladesh.

Authors Biographies

Joy persial G received her B.E degree in Information Technology from Karunya University in the year 2010. She is currently a post graduate student in the Computer Science and Engineering Department of Adhiyamaan College of Engineering, Hosur, TamilNadu. Her area of interest is Network Security and Cryptography. This paper is the work of her academic project.

Prabu M is working as a Lecturer in the Department of Computer Science and Engineering in Adhiyamaan college of Engineering, Hosur, Tamil Nadu, India. He has published more than 15 International/National journals and presented the 15 International/ National Conferences.He is presently doing his Ph.D in Anna University, Coimbatore, India. His area of interest are computer Networks, Information Security and Cryptography. He is life member of ISTE.

Dr. Shanmugalakshmi R is working as an Assistant Professor in the Department of Computer Science and Engineering in Government College of Technology, Coimbatore, India. She has published more than 50 International/National journals. Her research area includes Image Processing, Neural Networks, Information Security and Cryptography. She has received Vijya Ratna Award from India International Friendship Society in the year of 1996, she has received Mahila Jyothi Award from Integrated Council for Socio-Economic Progress in the year of 2001 and she has received Eminent Educationalist Award from International Institute of Management, New Delhi in the year of 2008.She is member of Computer Society of India, ISTE and FIE