Технічні науки

УДК 004.056.55:621.391

Kazachenko Olha

Student

National technical university of Ukraine

«Igor Sikorsky Kyiv Polytechnic Institute»

Казаченко Ольга Дмитрівна

Студентка

Національний технічний університет України

«Київський політехнічний інститут ім. Ігоря Сікорського»

Казаченко Ольга Дмитриевна

Студентка

Национальний технический университет Украины

«Киевский политехнический институт им. Игоря Сикорского»

SIDE CHANNEL ANALYSIS OF CRYPTOSYSTEMS

АНАЛІЗ КРИПТОСИСТЕМ ПО СТОРОННІХ КАНАЛАХ

АНАЛИЗ КРИПТОСИСТЕМ ПО СТОРОННИМ КАНАЛАМ

Summary. In this article described main types of SCA, their particularity and how they can be applied to modern, wide-used cryptosystems to break their security.

Keywords: SCA, encryption algorithm, hardware encryption, cryptosystem, side channel analysis, information security.

Анотація. У даній статті описано основні види SCA, їх особливості та як їх застосування до сучасних, широко розповсюджених криптосистем може негативно вплинути на безпеку.

Ключові слова: SCA, алгоритми шифрування, апаратне шифрування, криптосистема, side channel аналіз, інформаційна безпека.

Аннотация. В данной статье описано основные виды SCA, их особенности и как их применение к современным, широко распространенным криптосистемам может негативно сказаться на безопасности.

Ключевые слова: SCA, алгоритмы шифрования, аппаратное шифрование, криптосистема, side channel анализ, информационная безопасность.

1. Introduction

Side-channel attacks are easy-to-implement whilst powerful attacks against cryptographic implementations, and their targets range from primitives, protocols, modules, and devices to even systems. These attacks pose a serious threat to the security of cryptographic modules. In consequence, cryptographic implementations have to be evaluated for their resistivity against such attacks and the incorporation of different countermeasures has to be considered.

2. What SCA is?

Actually, in reality, cryptographic algorithms are always implemented in software or hardware on physical devices which interact with and are influenced by their environments. These physical interactions can be instigated and monitored by adversaries and may result in information useful in cryptanalysis. This type of information is called side-channel information, and the attacks exploiting side-channel information are called side-channel attacks. The underlying idea of SCA attacks is to look at the way cryptographic algorithms are implemented, rather than at the algorithm itself [1].

It is not difficult to see that conventional cryptanalysis treats cryptographic algorithms as purely mathematical objects, whilst side-channel

cryptanalysis also takes the implementations of the algorithms into account. Hence, SCA attacks are also called implementation attacks.

Side channels emerge because computation occurs on a non-ide-al system, composed of transistors, wires, power supplies, memory, and peripherals. Each component has characteristics that vary with the instructions and data being processed. When this variance is measurable by an attacker, a side channel is present [2].

3. Types of SCA

3.1 Timing analysis

One of the earliest and most easily understood side channel attacks is the timing attack. A timing attack occurs when side channel leakage is obtained by observing the amount of time an operation takes to occur [1].

The basic assumptions of timing analysis are:

- The run time of a cryptographic operation depends to some extent on the key. With present hardware this is likely to be the case, but note that there are various efficient hardware based proposals to make the timing attack less feasible through 'noise injection'. Software approaches to make the timing attack infeasible are based on the idea that the computations in two branches of a conditional should take the same amount of time ('branch equalisation').
- A sufficiently large number of encryptions can be carried out, during which time the key does not change. A challenge response protocol is ideal for timing attacks.
- Time can be measured with known error. The smaller the error, the fewer time measurements are required. This approach intersects with fault analysis.

3.2 Fault analysis

Most of the devices that perform various cryptographic operations are usually assumed to operate reliably when we use them, so we might not think to question if the security of such operations depend on the reliability of these devices that implement them. In spite of this assumption, hardware faults and errors occurring during the operation of a cryptographic module in fact have been demonstrated to seriously affect the security. These faulty behaviors or outputs may also become important side channels, and will even greatly increase a cipher's vulnerability to cryptanalysis sometimes. Fault attacks present practical and effective attacking against the cryptographic hardware devices such as smart cards.

There are two major kinds of fault side channels. The first ones are channels which are induced by computational faults occurring during cryptographic computation in an attacked module. These faults can be either random or intentional, caused, for instance, by a precise voltage manipulation. Having the ability to introduce computational faults, this kind of attack can be used on almost every kind of cryptographic mechanism and it is regarded as one of the most effective side channel attacks at all. The second kinds of fault side channels are those which are induced by sending an intentionally corrupted input data to the attacked module. For the module, this means a non-standard situation which must be handled in a special way. Usually the module has to use an error message to inform the user (the module can hardly know whether this is an ordinary user or an attacker) that the computation has been stopped due to some reasons [3].

3.3 Power analysis

The basic idea of this kind of attack is to reveal the key of a cryptographic device by analyzing its power consumption. Essentially, two dependencies of the power consumption are exploited: the data-dependency and the operation-dependency [1].

During the time the encryption is performed, the power consumption of the microcontroller is measured. For this purpose, resistor has been inserted in the ground wire of the power supply of the microcontroller. The voltage drop along this resistor is measured and recorded using a digital oscilloscope. The shape of a power trace strongly depends on the operations that are executed by the device and on the data it processes. An attacker can of course also zoom in closer on a power trace. When zooming in on a trace, the power consumption of individual clock cycles becomes visible [4]. Each peak that can be seen in this trace corresponds to the power consumption of the microcontroller in one clock cycle. Power analysis attacks work because the peaks look different for different operations and different data.

Attacks that exploit this property based on just one power trace are referred to as simple power analysis (SPA) attacks. It is a technique that involves directly interpreting power consumption measurements collected during cryptographic operations. In contrast to SPA attacks, differential power attacks (DPA) require a large number of power traces. The main advantage of DPA attacks compared to SPA is that no detailed knowledge about the cryptographic device is necessary. In fact, it is usually sufficient to know the cryptographic algorithm that is executed by the device. Another important difference between the two kinds of attacks is that the recorded traces are analyzed in a different way. In SPA attacks, the power consumption of a device is mainly analyzed along the time axis. The attacker tries to find patterns or tries to match templates in a single trace. In case of DPA attacks, the shape of the traces along the time axis is not so important [4]. DPA attacks analyze how the power consumption at fixed moments of time depends on the processed data. Hence, DPA attacks focus exclusively on the data dependency of the power traces.

3.4 Electromagnetic analysis

Electromagnetic analysis provides yet another means of side-channel attack. Instead of capturing the power consumption of a given device, the electromagnetic (EM) emanations are measured. Complementary metal oxide semiconductor (CMOS) devices, which include most semiconductor devices today, consume power during gate transitions from high to low levels. Additionally, the act of switching a gate causes a tiny short circuit and a small spike in current draw as the signal propagates through the gate's transistors [1]. All of these changes in flow of power alter the electromagnetic field surrounding the device, and these changes can be picked up by a special probe.

Capturing EM data requires a near-field probe which contains a simple coil of wire. This probe is placed very close to the device being analyzed. Current moving within the device induces small currents in the coil, which are then amplified by an attached low-noise amplifier (LNA) and captured by an oscilloscope. This captured data is analyzed in much the same manner as in power analysis attacks. Electromagnetic analysis has some advantages over power analysis [1]. Unlike DPA, it is a non-invasive attack, eliminating the need to modify the target. Second, the nature of using a movable probe results in the ability to perform localized captures. In other words, if the CPU component of the SoC is found to leak the most information, the probe is positioned directly over that area of the die to obtain the most signal and the least noise. Power analysis, on the other hand, is limited to the aggregate power consumption of the entire device. Finally, electromagnetic analysis (EMA) allows the observation of the charge and discharge cycles of a gate discretely, providing more detail on each gate's transitions than power analysis.

4. Conclusion

In this article was described general types of attacks that used recorded side-channel information while system done computations. They can be applied

to cryptosystem encryption/decryption process, if physical access to device, which comprise interested implementation of cipher algorithm, exists. Even if the system under investigation has strong security due to strong mathematic basis (AES and RSA algorithms for example), invalid implementation can annul are security they guarantee.

Finally, the most important conclusion from this paper is that it is not only a necessity but also a must, if you participate in cryptosystem`s embodiment, evaluate cryptographic modules for their resistivity against SCA attacks.

Reference:

1. YongBin Zhou, DengGuo Feng - Side-Channel Attacks: Ten Years After Its Publication and the Impacts on Cryptographic Module Security Testing, State Key Laboratory of Information Security, Institute of Software, Chinese Academy of Sciences, Beijing, China.
2. Peter Gutmann, David Naccache, Charles C. Palmer - Side Channel attacks on Cryptographic software, Copublished by the IEEE computer and reliability societies 1540-7993, November 2009.
3. Marc Joye, Michael Tunstall - Fault Analysis in Cryptography, Springer-Verlag Berlin Heidelberg, 2012.
4. Stefan Mangard, Elisabeth Oswald, Thomas Popp - Power Analysis Attacks: Revealing the Secrets of Smart Cards, 2007 Springer Science+Business Media, LLC.