Side channel cryptanalysis

J-J. Quisquater & D. Samyde

Université catholique de Louvain
Groupe Crypto
3 Place du Levant
B-1348 Louvain la Neuve, Belgium
jjq@dice.ucl.ac.be
samyde@dice.ucl.ac.be

Abstract

Cryptology includes cryptography and cryptanalysis technics. Cryptography is managed by Kerckhoffs principles, so any information related to a cryptosystem can be public except the keys. The cryptanalysis is the sum of a lot of very advanced technics in order to find these keys. The controversy about the Data Encryption Standard security has highly contributed to the development of new cryptanalysis methods based on mathematics. The linear and differentials analysis are the most convincing examples. Although these techniques often require great quantities of plain texts and ciphered texts, there are other very powerful methods based on the involuntary "information leakage". Indeed a cryptosystem can leak information in various manners, thus significant data can be extracted from physical signals emitted by the ciphering device. Temperature, acoustic waves, electromagnetic radiations, time or light (radiated, laser, infrared, …) signs which can be extremely dangerous. It is then possible to define side channel. The side channel cryptanalysis has been the speciality of secret services for a long time, but ten years ago, the scientific world started contributing to develop new side channel very effective technics.

Keywords Side channel cryptanalysis, Tempest, Timing attack, Power & ElectroMagnetic Analysis, Fault Analysis

Introduction

The history of the conventional cryptanalysis and the development of the most powerful computers are closely dependent. The undeniable proof is the brilliant cryptanalysis of the naval Enigma by A. Turing and both GHCQ's Colossus at Bletchley Park during the World War II. As conventional cryptanalysis side channel's power can really be frightening, their successes remained in the shadow for a long time.

In the past, the most advanced automats were based on mechanical principles that are well known today. But with the evolution of sciences, electricity become stronger and stronger, so electromechanic appeared and then electronic. Although the desired physical effects were advisely used as the principal component of a device, other parasitic effects can sometimes be neglected. In this case it is sometimes possible to extract significant information from the handled data [1].

As a current runs through a wire, it creates an electric field, a magnetic field as well as a heating. These effects are known and described by the Maxwell's equations and the Joules's law. But when some of these existing physical effects are not desired by the designer of the automata, they can create leakages. It is possible to remotely collect the electromagnetic field with an adapted antenna, to reamplify it, and to do a demodulation in order to obtain information. In the case of a cathode ray tube or a computer screen, the pixel of the screen is obtained thanks to the projection of an electron beam on sensitive molecules. But the position of the electron beam is controlled by coils. If the radiated field is collected, amplified and then introduced at the input of other coils, it makes possible to copy the image of the remote screen.

Concerning heat, some thermal cameras have a good resolution, they permit to construct a signature. These signature characterizes the device. The manufacturers of cryptoprocessors also try to limit the heat to reveal information on calculation in progress into their chip. The exhaustive list of the undesirable edge effects during the processing of a device can not be given here, however this article tries to point out the importance of side channel cryptanalysis and to draw up a list of the attacks most currently used against the cryptographic implementations.

People often forget to underline the important part played by the side channel in successful cryptanalyses. There are several manners to conceive cryptanalysis. The most conventional one consists in looking at the cryptographic primitives as a mathematical objects or an algorithm. Another one is interested in the implementation of the primitive in a ciphering device. It is then interesting to analyze the side channel obtained. A good side channel source is then inherent to the structure of the physical implementation. It is important to notice that it can considerably facilitate the work of a possible attacker.

History

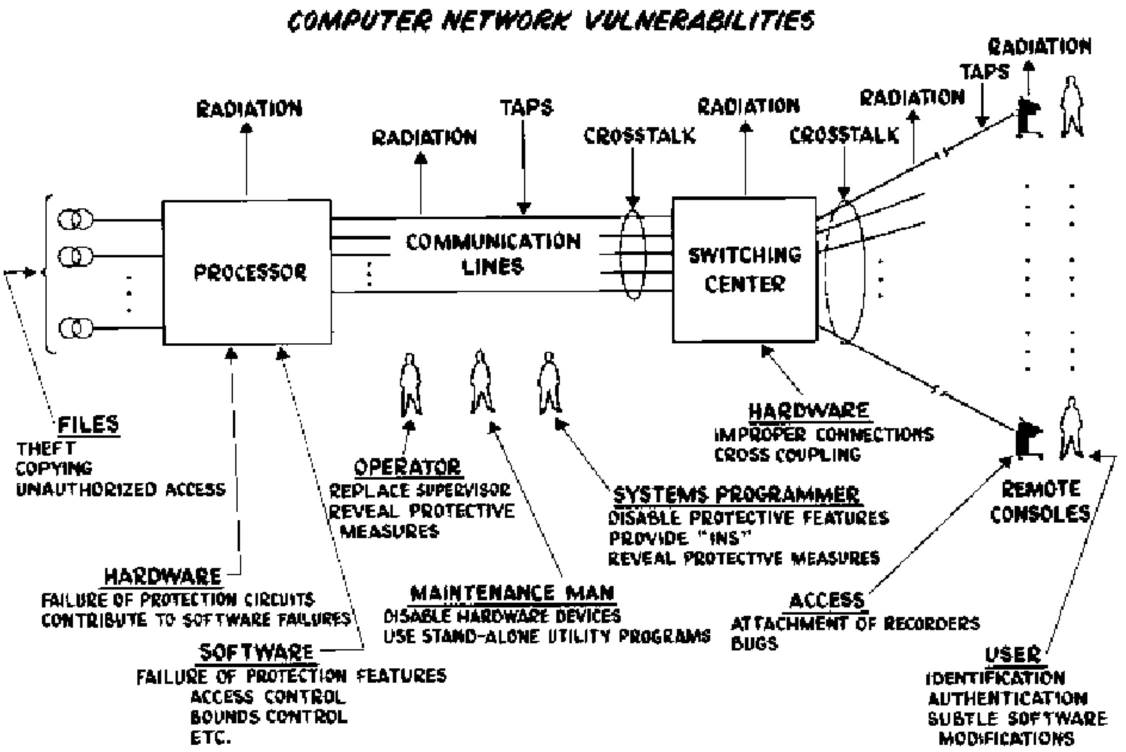

Figure 1 : Information leakage by one of the designers of Arpanet

It is quite difficult to fix with precision the birth of the side channel cryptanalysis. But it would be false to think it was at the end of XXth century. It even seems this date is rather at the end of XIXth century or the whole beginning of XXth. The discovery of the existence of side channel obviously did not give place to publications and international communications.

J. Maxwell establishes its theory on electromagnetic waves in 1873. But at the end of the 19th century some cross talk problems in telephone links were mentioned. During the First World War, these coupling problems were used to spy communications. Information obtained was only copied on another media and then listened. The signal processing was non-existent in such interceptions.

But in 1918, H. Yardley and its team discovered that classified information could leak from electric materials. But this knowledge make it possible to find the handled secrets. The data contained in a cryptographic device modulated a signal on the tape of a close recording source. In the middle of the thirties, the study of the IBM typewriter indicated that the leakage of information was important and must be considered.

Military people started to seriously consider this kind of leakage; and the various western armies paid great attention to limit the radiations on their sensitive devices at the time of the Second World War, particularly for the embedded oscillators. That did not prevent the communist's Teletype from "being intercepted" in Berlin. Reception antennas were placed in close tunnels. During the fifties, the Chinese authorities also used acoustic techniques to spy embassies, whereas Russian sent microwaves on metal bars contained in statues, in order to recover the acoustic waves of an American embassy. The creation of the NSA in 1953 immediately gave a crucial importance to the recovery of the compromising signals. The word SIGINT which is the acronym of SIGnal INTelligence took all its meaning then. Using telephone wire as an antenna carried one of the first interceptions of electromagnetic radiations out. In the future, this kind of technique continued to be applied successfully for data interceptions of some computer screens. It worked for at least a distance of several hundreds of kilometers. These first experiments were carried out with the M.I.T.

The beginning of the great series of the American & NATO military standards for the limitation of the compromising electromagnetic radiations and the use of shield appeared in the middle of the fifties. The American armies worried about this new threat and initiated the tempest program. At the beginning of the sixties, the Russian embassy and some French devices were spied in London, thanks to their electromagnetic radiations. While demodulating the recovered signal correctly, English people managed to find classified information. This time the signal processing was introduced and continuously took an increasingly place in the future. One example is related to the cryptanalysis of a Russian code during the crisis of Cuba. The American Oxford interceptor succeeded in recovering the electromagnetic radiations emitted by a Soviet ciphering device located on the island. Moreover the American marine carried out that the measurement of the radiated noise make it possible to know the position of the rotors inside some cryptographic devices.

The civils did not yet know a lot about the interception possibilities, as this kind of methods was still confidential. But quickly, at the beginning of the seventies, people mentioned cases of interferences between some of their electronic materials. And the cases of young researchers playing music with their screen or their printer into a radio receiver or a device including a demodulation, were not isolated.

However the uses of the side channel analysis continued to exist and the Kilderkin operation which consisted in the interception of the electromagnetic emanations of the Russian embassy in Canada took place in the middle of the seventies. Quite at the same time, the Polish services were surprised spying Soviet military material; once more time, the electromagnetic radiations were blamed. This time, in fact, it was the power wire that was listened. In 1984 the NSA introduced the new concept of safety zone around a measurement point and it is the next year that IBM builded its first armored PC [2]. At the end of twenties, I. Murphy a.k.a Captain Zap published the first plans of tempest receivers, just after British television showed demonstrations on this subject. At this time, the French army started to be very interested in the development of a tempest chain, and the Bulgarian services used equipped trucks with hidden antennas to spy and to intercept military communications in Western countries. In nineties R. Anderson and M. Kuhn worked on the reduction of radiations and published new fonts. For healthy reasons, the manufacturers had to drastically reduce screen radiations. In 1996 P. Kocher published his work based on timing measurement. Using the processing time of a cryptosystem, his timing attack, exploited by F. Koeune, make it possible to recover a 512 bits RSA private key with a few hundreds of thousands of samples in a few minutes, whereas the factorization of an equivalent number required several intensive months of processing. The work of P. Kocher and its team then concentrated on power and consumption analysis. He unleashed the full of differential measurements. Then the large banking accounts asked silicon founders to quickly find fast and effective solutions to solve this problem. During the last ten years, another analysis appeared, based on fault injection. The idea was very simple: if it was not possible to extract keys from the leakage, maybe was possible to disturb the processor during a critic processing.

The history reports even cases where the sides channels were voluntary introduced in order to be able to recover the significant data easier thereafter. Finally, the cryptanalysis using side channel has developed more and more to become today one of the serious components for intelligence collection.

Electromagnetic leakage

The electromagnetic radiations can still be used nowadays against recent systems. The quality of the antennas is very important, and it is possible to find several kinds (logarithmic, planar...) of them. In the same way, the frequency stability of the local oscillators are necessary to obtain a good result; the best receivers authorize a precision of 10^{-6} Hz, using phase locked loop.

The level of classical countermeasures has been improved in a significant manner since few years. In the case of a cathode ray tube, it is difficult to obtain a valid interception farther than ten meters, using an old material. This distance and this level of radiations must be compared to the distances obtained by the satellites who listen two aligned antenna from the space.

Nowadays, some information is public because it has been declassified. But the simple presence, or not, of electromagnetic radiations is often enough to provide useful information to an attacker. Some systems recreate a false magnetic field around them, in order to mask their presence or their radiations. However, the theorem of C. Shannon indicates that by repeating measurement, it becomes possible to remove the noise and to obtain a signal noise ratio as high as desired.

Devices as smart cards use operative countermeasures to limit the number of executions. In the large majority of cases, the designers try to limit the level of radiations or to define a protection area in order to reduce the power of the signal. But some applications very often require a Faraday cage to be protected, and it is not always simple and possible to use one.

Some recommendations, related to the level of attenuation of the Faraday screen rooms, seemed unexplainable in the past. Recent work of Mr. Kuhn, and other academics, seem to be able to explain the differences between the attenuations required by the military and the civilians. Indeed, the military attenuations do not seem to leave any chance of interception, even with recent material, whereas the civil levels did not ensure this shielding quality.

It is also important to notice that the light emitted by a screen, contains useful information which is the video signal. M. Kuhn recently published it is possible to reconstruct a video image starting from the luminosity of a distant screen.

Timing attack

One of the first attacks by measurement of the response time of a system, made it possible to reduce the number of tests, in order to find a password. This attack was particularly effective against the implementations of Unix. Indeed, if the comparison between the password recorded and the password seized is carried out byte by byte on the basis of the first bit, and if the machine response was available at the first error, it was then possible to test all the bytes located in first position and to choose the one which had the longest response time. Indeed, this last was inevitably the good, since the response time lengthened corresponded to the time of comparison and erroneous response of the second byte. According to R. Moreno, this kind of analysis also functioned at the time of the bearing of a banking application since a Motorola processor, on a smart card including a processor Thomson. This attack has been applied by F Grieu. It is also possible to use the measurement of the response time, in order to know the contents of the mask of a distant data-processing waiter. Indeed, if the information is already present in the memory cache of the computer, and if it has to be load the response time is different.

In 1996, P. Kocher published a rather theoretical article, on the use of the measurement of time, to try to find cryptographic keys. Two years later, F. Koeune applied this analysis and showed how it was possible to defeat a naive implementation of the algorithm Square & Multiply for the modular exponentiation. There are only two possibilities of connection inside the code carried out for its demonstration, but these two connections do not take the same time. It is then possible to know rather quickly the cryptographic keys [3], with a few hundreds of thousands samples.

Countermeasures against timing attacks may seem to be trivial, but a constant time answer is not always possible: sometimes it is necessary to consider the worst case of an algorithm, or to insert much more subtle countermeasures, modifying the temporal properties.

Thermal analysis

The thermal analysis is not used a lot against cryptographic devices; it is more current for satellite or space image analysis. In many cases, the materials stationed at a place has modified the temperature or the illumination of the storage place. Even a long time after their departure, it is always possible to carry out a measurement revealing their very last presence.

Concerning processors, the limiting factor is the diffusion of heat. The equation of propagation is well-known, but the propagation times are crippling. However, it is important not to obtain hot points on the chip, in order not to reveal a specific activity [4]. In the past, the security components verifiers used liquid crystals to reveal the activity areas of the component. But actually this method is too slow.

Power analysis

A small antenna inserted in a perforated condenser can provide a lot of information on the activity of an electronic card. This old technic is well known and has been used for a long time. An electronic card often contains few very interesting elements to analyze, by measuring their consumption. Inserting a low value resistance between the ground pin and the general ground of the card, is enough to track the specific consumption of a chip. In the past, some people had already noticed that the power analysis of a cryptoprocessor could provide information on the handled keys. In 1998, P. Kocher [5] introduced the concept of differential power analysis; it is the intercorrelation value of two random variables. This method called DPA is very powerful against smart cards and recent processors. Moreover, it is possible to improve the resolution, using a coil located in the close field of the processor [6,7]. The signal noise ratio can be greatly improved by 30 to $40db$. IBM recently used this method to defeat GSM card security. The algorithm used is simple in both cases: the idea is to quantify the influence of a bit of the key and to separate the traces obtained in two sets. These sets are built according to the value of one bit of the key. Then checking the assumption on the value of the key bit, the real value can be recovered.

Conclusion

In conclusion, side channel cryptanalysis is a powerful tool and can defeat some implementations of very robust and well suited algorithms. Perhaps in the future, others side channels will be discovered; but the real cost of the these attacks is increasing. In order to be immunated to a high number of cryptanalysis, implementations must now integrate a very high level of expertise. The countermeasures are always possible and available, but they must be well thought. It is easy to believe avoiding a side channel and in fact to become weaker from another one [8,9].

It is an eternal game between robbers and policemen; for the moment cryptanalysts seems to be better [10] than designers, but in the future it will undoubtedly quickly evolve.

References

[1] NACSIM 5000: *Tempest Fundamentals*, National Security Agency, Fort George G.Meade, Maryland. Feb 1982. Partially declassified also available at `http://cryptome.org/nacsim-5000.htm`.

[2] M. Kuhn and R. Anderson, Soft tempest: *Hidden data transmission using electromagnetic emanations*, In D. Aucsmith, editor, Information Hiding, vol 1525 of Lecture Notes in Computer Science, pp 124-142. Springer-Verlag, 1998.

[3] J. Kelsey, B. Schneier, D. Wagner, and C. Hall, *Side Channel Cryptanalysis of Product Ciphers*, in Proc. of ESORICS'98, Springer-Verlag, September 1998, pp. 97-110.

[4] J-S. Coron, P. Kocher, and D. Naccache, *Statistics and Secret Leakage*, Financial Cryptography 2000 (FC'00), Lecture Notes in Computer Science, Springer-Verlag.

[5] P. Kocher, J. Jaffe and B. Jun, *Differential Power Analysis*, In M. Wiener, editor, Advances in Cryptology - CRYPTO'99, vol. 1666 of Lecture Notes in Computer Science, pp. 388-397, Springer-Verlag, 1999. Also available at `http://www.cryptography.com/dpa/Dpa.pdf`.

[6] K. Gandolfi, C. Mourtel and F. Olivier, *Electromagnetic analysis : concrete results*, In Koç, Naccache, Paar editors, Cryptographic Hardware and Embedded Systems, vol. 2162 of Lecture Notes in Computer Science, pp. 251-261, Springer-Verlag, 2001.

[7] J.-J. Quisquater and D. Samyde, *ElectroMagnetic Analysis (EMA) Measures and Counter-Measures for Smart Cards*, in I. Attali and T. Jensen, editors, E-Smart Smartcard Programming and Security, vol. 2140 of Lecture Notes in Computer Science, pp. 200-210, Springer-Verlag 2001.

[8] R. Anderson, M.Kuhn, *Tamper Resistance - A Cautionary Note*, Proc. of the Second USENIX Workshop on Electronic Commerce, USENIX Association, 1996.

[9] O. Kommerling and M. Kuhn, *Design principles for tamper-resistant smartcard processors*, In Proc. of the USENIX Workshop on Smartcard Technology (Smartcard'99), pp. 9–20. USENIX Association, 1999.

[10] E. Biham and A. Shamir, *Power Analysis of the Key Scheduling of the AES Canditates*, in Second Advanced Encryption Standard Candidate Conference, Rome, March 1999.