ISSN 2319-2720

Volume 3, No.1, January – March 2014

International Journal of Computing, Communications and Networking

Available Online at http://warse.org/pdfs/2014/ijccn033120143.pdf

Side Channel Attacks and its Impact on Symmetric Algorithms through Power Analysis

Hridoy Jyoti Mahanta[1] and Ajoy Kumar Khan[2]

[1]Department of IT, Assam University, Silchar, India, hridoy69@gmail.com

[2] Department of IT, Assam University, Silchar, India, ajoyiitg@gmail.com

ABSTRACT

Side channel attack is one of the most volatile fields of research in the domain of network security. With side channel attack, cryptanalysis is no more confined to its dependence on plain text or cipher text. Indeed the physical characteristics of the cryptographic device are the side channel information which is used to find the cryptographic algorithm used and also the secret key. It is one of the most efficient techniques and has successfully broken almost all the cryptographic algorithms today. This paper presents a brief idea introduction to various possible side channel attacks. Also, the impact of side channel attack on two most wide spread algorithm Data Encryption Standard (DES) and Advanced Encryption Standard (AES) has been briefly stated. Some of the general mitigation techniques available in the literature are also discussed in brief.

Key words: cryptographic device, AES, DES, Power Analysis, SPA, DPA.

1. INTRODUCTION

Classical attacks were based on knowing the plain text or the cipher text or both. Encryption devices were meant only to convert the plain text to cipher text and vice versa. But today it is known that these devices provides additional information, the side channel information [1], which can be used to break into the crypto system and get the required secured data. This information includes power, time of operation, electromagnetic field, faults, frequency etc. Side channel attack uses this additional information to attack a system. The main motive of such attack is recovery of the key [2]. Though the side channel information as mentioned above are mainly hardware related but some software based side channel information have become a subject of interest. Cache based software side channel vulnerabilities [3] for AES and RSA have already come up. Even the web applications [4] are not deprived of such attacks. Despite of HTTPS protection, sensitive information leak from the web during video streaming, voice-over-IP, web browsing and many more providing side channel information for attack.

The rest of the paper is organized in six sections. The next section gives a comparison of the traditional model of attack and side channel model of attack. Section 3 explains some of the classic side channel attacks in brief. Section 4 gives an idea of some of the recent side channel attacks that have come up. Section 5 gives a brief detail on the impact of differential power attack in DES and AES algorithms. Section 6 states some of the general mitigation techniques for such attacks and finally a conclusion is formulated.

2. MODELS OF ATTACK

Traditional model [5] for attack was based on that the attacker was aware of the encryption protocol or any of data that was exchanged between the sender and the receiver. Some mathematical theory then was used to decipher the secured data. Figure 1 shows the traditional model of attack.

But recent research shows a different view of attack through the side channel information which leaks out of the cryptographic device during its operation. A new model [5] has hence come up which utilizes this additional information for attack making it different from the traditional one as shown in figure 2.

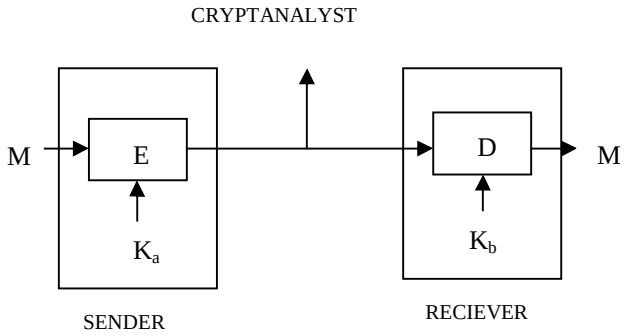

Figure 1: Traditional model of attack [5]

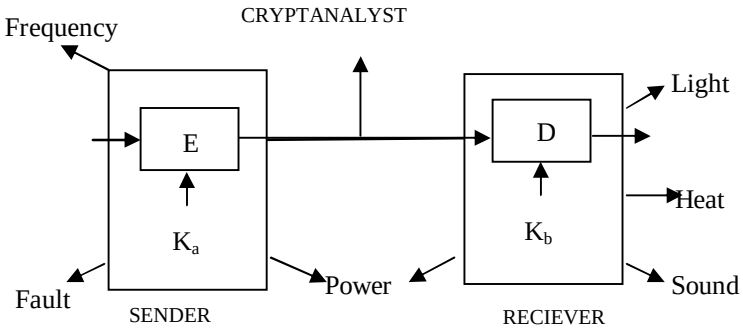

Figure 2: Side channel attack model [5]

3. CLASSIC SIDE CHANNEL ATTACKS

Side channel attack utilizes additional inputs and outputs from a cryptographic device. Some of this information is the classic inputs/outputs which have always come up. Based on this information side channel attack mainly occurs in the following ways as stated below.

3.1 Timing Attack

The timing attack is concerned with the time required to perform the cryptographic operations. This time to operate varies among the inputs as these operations may have unnecessary statements, conditional, branching statements etc. which have different time for execution. The attacker uses this difference in the time to make the exact guess of the key. The time samples are collected with different inputs and are fed into a statistical model which guesses the key with an extent to certainty. By measuring the amount of time required, the attacker can easily find out the fixed Diffie-Hellman exponents, factor RSA keys, and break other cryptosystems [6]. However, use of masking [6], Montgomery multiplication in RSA can prevent this attack to a large extent.

3.2 Electro Magnetic Attack

Flow of electric current carries an electromagnetic field with it. This field carries additional information with it like amount of power, time etc. If this information can be measured out, an attacker can break into the security system and find out the secret key. Electro Magnetic (EM) attack uses this information as side channel information to make an attack into the system. Quisquater and Samyde first showed the possibility to study the EM radiation from a smart card [7]. Quisquater also introduced the two ways to study the electro magnetic radiation: Simple EM Analysis (SEMA) and Differential EM Analysis (DEMA). SEMA used the information from one EM radiation measurement where as in DEMA statistical analysis of multiple information was done to find the secret key. Soon experiments of EM attack on DES, RSA and COMP-128 were performed which revealed that such attack was more feasible than other side channel attack as it could make measurements from a large distance even in a noisy environment [8]. As stated by Agarwal et al., radiation can be of two types: intentional and unintentional [9]. The earlier is a result of the direct flow of current where as the latter is the result of various coupling, modulations etc. Side channel attack explores the unintentional radiation. Indeed, EM leakage has multiple channels which can provide information for even a DPA resistant device. However, such attack can be counter measured by signal strength reduction and signal information reduction [5].

3.3 Fault Analysis Attack

Fault analysis attacks are based on the faults made by the cryptographic devices which may be intentional or naturally occurring. The faulty outputs of these devices are the side channel information for such attacks.

The faults can occur in two ways, first is computational faults occurring during the cryptographic computation. Second is when faulty input is fed into the device to get faulty outputs and analyze them to get the key [5]. Successful fault attack occurs in two steps, first is injection of the fault where the time of injection is of prime concern. Second is exploitation of these faults so that by analyzing them we can find the secret key [5].

Fault analysis can occur in two ways, simple fault analysis (SFA) and differential fault analysis (DFA). SFA [10] exploits one or few faults to recover the secret key. The implementation RSA algorithm can be easily be broken by inducing a fault into it and doing the calculations again [10]. Whereas, the same doesn't go for elliptic curve cryptography. Here a simple fault cannot easily predict the possible key. DFA on the other hand tries to find the key bit by bit. Here for every single bit faults are induced and the process is iterated till the entire key is found. Implementations of elliptic curve, hyper elliptic curve have been broken using DFA [10]. Indeed fault attack can break almost all the cryptographic algorithms. Counter measure for such attack is to restart whenever there is a fault result instead of carrying on with it.

3.4 Power Analysis Attack

Most of the cryptographic devices require external power supply to operate. Power analysis attack exploits the relation between power consumed and data to find the operation within the device and combining with other cryptanalysis techniques can find out the secret key of encryption [11].

To measure the power consumed a small resistor (50 ohm) is connected in series with the power or ground. The voltage difference across the resistor by the resistance gives the current [12].

The power analysis is done in two ways, simple power analysis (SPA) and differential power analysis (DPA). SPA analyses directly the power consumes measurements that can be directly acquired from visual representations. SPA can give information about the operation in the device as well as about the secret key. SPA uses a trace which is the power consumption measurement in a cryptographic operation. The trace depicts the operation going in the device. Figure 3 and 4 shows trace of DES algorithm [12].

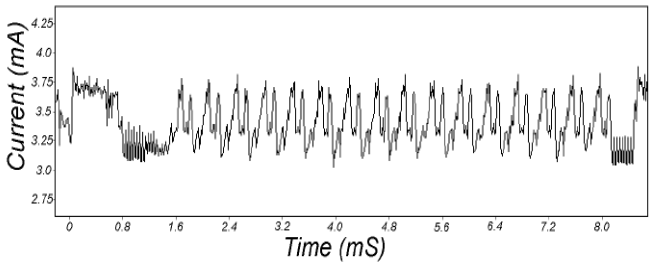

Figure 3: SPA showing traces of DES [12]

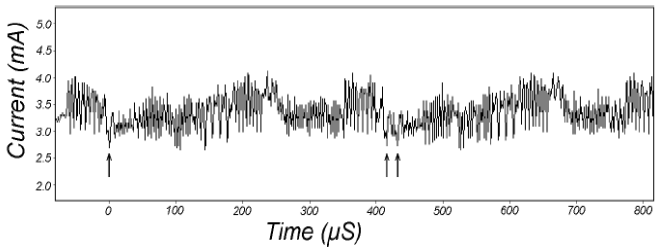

Figure 4: SPA showing traces of round 2 and 3 of DES[12]

From figure 3, the 16 rounds of DES are clearly visible. Figure 4 gives more details of the rounds in the DES.
As SPA gives details of the individual steps of the cryptographic operations so they can be easily broken up. SPA can be prevented by simply avoiding the operations involving the secret key. Using hardwired hardware can also reduce SPA as they consume very small amount of power [12].

Unlike SPA, DPA analyses the values through a statistical model. Often due to smaller variation in the power it is difficult to find the key through simple power analysis, we then need to collect a large number of samples and then feed them into some statistical model and find the correct key guess from them [12]. This approach is quite time consuming but provides accurate results most of the time. DPA defines some selection function which operates to a certain limit of values. If the guessed key is correct the computed value for the selection function is same as the actual value of target with probability 1. But if the guessed key is incorrect the value of the function differs for about half of the cipher text. This will be discussed in a later section. DPA can be prevented by reducing signal size, introducing much noise and designing cryptosystems relevant to hardware [12].

4. REVIEW OF RECENT SIDE CHANNEL ATTACKS

Apart from the classical techniques to attack a cryptographic system, many new techniques have come up in the recent time. These are in itself a new field of research in the side channel attack domain. Some of them are discussed below in brief.

4.1 Frequency Based Attack

This type of side channel attack is quite similar to Power attack just that instead of considering the time domain, frequency domain is considered for measurements. Personal digital assistants (PDA), cell phones, pagers are some of the devices which can be attacked by such side channel information. It is efficient even when the traces are misaligned where EM attack fails [5].

4.2 Online Application Leakage

As most of the activities today are software centered, a number of applications are delivered through the web. Some of these applications store a lot of sophisticated information of the user. As these information flows through the network, they often act as side channel information leading to a new paradigm of side channel attack [4]. In US, applications like Online Health, Online Tax etc are quite frequently used. The user needs to fill a lot of information in them. The key strokes in doing this, leaks the information they are feeding into it. It is well studied in [4].

4.3 Acoustic Attack

Though classic side channel attack have mainly concentrated on the power analysis, EM analysis, timing analysis etc, but one of the oldest eaves dropping viz. acoustic emanation is of vital interest [14]. That a co- relation exists between the sounds produced and computation of a processor has been well presented by Shamir et al [13]. An acoustic side channel attack on the printers has been studied by Michael Backes et al [14]

4.4 Visible Light Attack

The average luminosity of a CRT's diffuse reflection can be used to reconstruct the same signal displayed on the CRT. This was well demonstrated by Kuhn [15]. He also visualized that the same technique is even valid in case of LED. Besides, the advantage is that this type of attack doesn't even need any physical access.
The way radiation is emitted from a LED can be analyzed to infer the data processed, is well discussed by Loughry and Umphress [16].

4.5 Error Message Attack

In many communication methodologies there is a need to send an acknowledgement or an error message by the receiver to verify that the message has been received. Such error messages sent back by the receiver to the source can be used as side channel information in such attack.
Such an attack was described well by Vaudenay [17] on symmetric encryption technique with block cipher in CBC mode. He stated that in case of CBC the message either needs to be in form of blocks or padding. If such padding during decryption results to be invalid then some sort of error message is returned. If an attacker can find the padding error status, it can act as a side channel for chosen cipher text attack [17].

4.5 Cache Based Attack

The theoretical concept to use a cache memory is to speed up the processing. Data are stored in the cache and whenever they need to be fetched, it is done from the cache itself instead of the main memory. However, if the data is not in the cache it needs to be extracted from the main memory. This causes an unwanted delay. This delay acts as side channel information in case of cache based attack.

This kind of attack was first proposed by Kelsey et al [18]. Further work showed that this type of attack was good when software implemented ciphers are used. Osvik et al [19] later demonstrated that such attack is extremely strong as they are independent of the plain text or the cipher text, but only observation of the cryptographic operation on the cache.

4.6 Scan Based Attack

Scan based attack leads to recover secret keys from hardware implementation of encryption techniques. Scan based test which is mainly used for validating the function of hardware can be also provide side channel information for scan based attack.

A scan based attack on DES algorithm to recover the secret key is explained in [20].

4.7 Combination of Side Channel Attacks

Moreover, if two or more side channel attacks are combined then they can be a new theoretical attack. Besides, the specific countermeasures of individual attacks may also be overcome by such combination.

A combined power and timing attack was mentioned in [21].

5. DIFFERENTIAL POWER ANALYSIS ATTACK ON SYMMETRIC ALGORITHM

It is quite easy to make a SPA resistant device, but DPA is very complex and is very difficult to prevent a system from such attack. As stated before, with DPA almost all the cryptographic algorithm has been broken. In this section a brief overview of the way the two most common symmetric cryptographic algorithms DES and AES are given.

5.1 DPA Attack in DES

In previous section it has already been mentioned that with smaller variations of the power consumptions, it is impossible to find the key by just observing these variations. In such cases we use DPA, which uses a statistical model to find out the correct value from a large number of samples.

One of the most widely known symmetric algorithms, DES uses 16 rounds to encrypt a piece of information. The operation of the s-box to make 4 bits output from 6 input bits in 8 s-boxes so as to get 32 bits is the most crucial step in the algorithm. DPA uses a selection function D(C, b, K_s) [12] which computes the value of bit $0 \le b < 32$ of intermediate L at the beginning of the 16^{th} round for the cipher text C, where the 6 bit key input to the s-box corresponding to b is $0 \le K_s < 32$. There after m encryption operations are observed from where T[1....m] traces are capture having k samples in each. The cipher text $C_{1....m}$ is also recorded [12]. Once K_s is guessed, to measure its correctness the power consumption measurement is used. Of the *k* samples, the difference between those samples with average 1 and those with average 0 is calculated. At any point *j*, this calculated value gives average over C[1...m] of the effect due to the value represented by the selection function D on the power consumption measurements at point j. Mathematically,

$$\Delta_D[j] = \frac{\sum_{i=1}^{m} D(C_i, b, K_s)\mathbf{T}_i[j]}{\sum_{i=1}^{m} D(C_i, b, K_s)} - \frac{\sum_{i=1}^{m} (1 - D(C_i, b, K_s))\,\mathbf{T}_i[j]}{\sum_{i=1}^{m} (1 - D(C_i, b, K_s))} \approx 2\left(\frac{\sum_{i=1}^{m} D(C_i, b, K_s)\mathbf{T}_i[j]}{\sum_{i=1}^{m} D(C_i, b, K_s)} - \frac{\sum_{i=1}^{m} \mathbf{T}_i[j]}{m}\right) \quad [12]$$

If K_s is incorrect then the value of b using function D will differ from the actual target for about half of C where as if Ks is correct then the value of b using function D will exactly be same as the actual target bit b with probability 1. The correct value of K_s can thus be identified from the spikes in the differential trace. Finding all the 8 K_s will lead us to find the entire 48 bit sub key. This analysis was first done by Paul Kocher et. al. and is described in [12].

5.2 DPA Attack in AES

The AES algorithm operates on 128 bit data with a variable key size of 128, 192 or 256 bit. In block cipher, DPA attack is done separately on every block by guessing the key at first or last round [2]. The operations in AES are generally byte oriented so the key is guessed 8 bits per time. Like DES, the s-box operation is again a vital part of AES. The way the s-box in AES is attacked is given below in brief [2].

i) The attacker runs M number of random plain text denoted by I_1 to I_m in the cryptosystem with a common key K. For every input the power consumption curve C_{ij} is measured in discreet time. Index *i* corresponds to input I_i and *j* corresponds to the processing time.

ii) Based on the cryptographic algorithms and correlation with the key K, a selection function is chosen. An isolated target bit *a* is determined which depends on some bits of K.

iii) Using this selection function the attacker can find the value of *a* by I_i and partial guessed key. Based on this value the C_{ij} are separated to two sets such that,

$S_0 = \{C_{ij} \mid a=0\}$ and $S_1 = \{C_{ij} \mid a=1\}$ also $|S_0| + |S_1| = M$. [2]

iv) The average power trace of each set is then calculated and the difference between them (*say Dj*) is found. The selection function is selected for the intermediate bit *a.* But while calculating this data, the amount of power consumption changes a little say €, as the bit changes from 0 to 1. So, if computation of the bit occurs at j/ then for j= j,/

$E\{C_{ij} \mid a=0\} - E\{C_{ij} \mid a=1\} = €$ and if $j \neq j'$ then, $E\{C_{ij} \mid a=0\} - E\{C_{ij} \mid a=1\} = 0$. [2]

v) So, if the key guessed is correct the differential power signal will have significant peak else not show any biases. So, as the number of plain texts increases the differential power signal will converge to,

$\text{Lim } D_j = E\{C_{ij} \mid a = 0\} - E\{C_{ij} \mid a = 1\}$. [2]

With suitable number of measurements the differential power signal will be € at j/ and zero at all other times. So, in average a weak signal can be always recovered. These entire steps are well described in [2].

6. MITIGATING SIDE CHANNEL ATTACKS

As side channel attack doesn't make physical involvement in

implementation, so resisting it becomes quite a difficult task. For the classical attacks, mitigation techniques have been proposed to a great extent but they only make the attack difficult but not impossible. Some of these techniques are discussed below in brief.

Timing attack is confined to analyzing the difference in the time consumed for different operations in the encryption/decryption technique. Making this time constant for every operation such as multiplication and exponentiation by adding delays wherever required can resist such attack [1]. However, this may slow down the overall processing.

Power attack and EM attack can be mitigated using similar techniques most of the time. Making operations data independent or saturating the clock cycles for all the operations may prevent attacks from leakage of power or EM emanation [1]. Avoidance of conditional and branch statements can also put a major impact in resisting SPA and timing attack. Addition of noise or techniques which prevents reduction of noise [1] is also preferable in mitigating power and EM attacks.

For DPA or DEMA, masking technique, i.e. combining the input value with some random value making the actual input undistinguishable is very much proposed. Reducing the signal strength and signal information resists EM attack to a large extent [5].

In case of fault attack, doubling the encryption operation during a single round has proven to mitigate such kind of attack [5]. Enabling error checking techniques such as checksum has also been proposed in many research works.

For the recent side channel attacks that have been mentioned in section 4, mitigation techniques are yet to be proposed. It is presently a volatile field of research. However, some work on cache based attack have been done which has proposed some cache less system or techniques to reduce cache miss to avoid such attack [5].

7. CONCLUSION

With side channel attack, the cryptographic algorithm used in a device and the key used can be easily discovered. Research on many new physical specifications of the device is going on to break the system. Side channel attack being passive and non invasive makes it is very difficult to protect a system from such attack. In this paper we provided an overview of the various side channel attacks, its impact on DES and AES and also a few countermeasures.

REFERENCES

1. Hagai Bar-El. **Introduction to side channel attacks**, *Discretix technologies Ltd.*, 43, 2003.
2. Mohammad Zahiduf Rahaman and Mohammad Akram Hussain. **Side channel attack prevention for AES smart card**, *11th ICCIT*, IEEE, pp. 376-380, 2008.
3. E. Brickell, G. Graunke, M. Neve and J-P Seifert. **Software mitigations to hedge AES against cache- based software side channel vulnerabilities**, *IACR ePrint Archive Report*, 52, 2006.
4. S. Chen, R. Wang, X. Wang and K. Zhang. **Side-channel leaks in web applications: A reality today, a challenge tomorrow**, *IEEE Symposium in Security and Privacy*, pp. 191-206, 2010.
5. Y. Zhou and D. Feng. **Side-channel attacks: Ten years after its publication and the impacts on cryptographic module security testing**, *Information security Seminar, (WS 06/07)*, 2005.
6. P. Kocher. **Timing attacks on implementation of Deffie-Hellman, RSA, DSS and other systems**, *Advances in Cryptology-CRYPTO*, Springer-Verlag, pp. 104-113 ,August 1996.
7. J-J Quister and D. Samyde. **Electromagnetic analysis (ema): Measures and countermeasures for smart cards**, *Smart card programming and Security*, Springer-Verlag, pp. 200-210 , 2001.
8. E. De mueler et. al. **Electromagnetic analysis attack on an FPGA implementation of an elliptic curve cryptosystem**, *ICCT EUROCON*, IEEE, pp.1879-1882, 2005.
9. D. Agarwal, B. Archambeault, J. R. Rao and P. Rohatgi . **The EM side-channel(s)**, *CHES 2002*, IEEE, Springer-Verlag, pp.29-45, 2003.
10. R. M. Avanzi. **Side channel attacks on implementation of curve based cryptographic primitives**, *Cryptology ePrint Archive*, Report 2005/017, 2005.
11. J. Zhang, D. Gu, Z. Guo and L. Zhang. **Differential power cryptanalysis attacks against PRESENT implementation**, *ICACT*, IEEE, Vol. 6, pp.56-66, 2010.
12. P. Kocher, J. Jaffe and B. Jun. **Differential power analysis**, *Advances in Cryptology*, CRYPTO, Springer, Berlin/Heidelberg, 1999.
13. A. Shamir and E. Tramer. **Acoustic Cryptanalysis: on nosy people and noisy machines**, *EUROCRYPT* rump session, 2004.
14. M. Backes et. al. **Acoustic side-channel attacks on printers,** *USENIX Security Symposium*, 2010.
15. M. Kuhn. **Optical time domain eavesdropping risks of CRT displays**, *in proc of Symposium of Security and Privacy*, pp. 3-18, 2002.
16. J. Loughry and D. Umphress. **Information leakage from optical emanations**, *ACM Transactions on Information and System Security*, Vol. 5, pp.262-289, 2002.
17. S. Vaudenay. **Security flaws induced by CBC padding-Applications to SSL, IPSEC, WTLS**, *EUROCRYPT, LCNS 2332*, pp.534-545, 2002.
18. J. Kelsey, B. Scheneir, D. Wagner and C. Hall. **Side channel cryptanalysis of product ciphers**, *in Proc of 5th European Symposium on Research in Computer Society*, LCNS 1485, pp.97-110, 1998.
19. D. A. Osvik, A. Shamir and E. Tromer. **Cache attacks and countermeasures: the case of AES**, *Topics in Cryptology CT-RSA*, Springer Berlin Heidelberg, 2006.
20. B. Yang, K. Wu and R. Karri. **Scan based side channel attack on Data Encryption Standard**, *IACR Cryptology, ePrint Archive*, 83, 2004.
21. W. Schindler. **A combined timing and power attack**, *PKC*, LCNS 2274, pp. 263-279, 2002.