A Study on the Side Channel Attacks in Cloud Data Centers

[1]Basel Hashem Ghallab Abdulsafi, [2]R Suchithra
[1]*Keisie International University, South Korea.*
[2]*Jain University, Bangalore*

ABSTRACT

Side-channel analysis is a powerful technique that the principle comprises in monitoring some side-channel information like the running time, the power consumption, or the electromagnetic radiation. Side-channel attacks are easy-to-implement while capable attacks against cryptographic implementation and their objectives run from primitives, protocols, modules, and devices to even systems. These attacks represent a genuine risk to the security of cryptographic modules. Processor micro architectural side and covert channel attacks have risen as the absolute most sharp attacks and ones which are difficult to manage, without affecting framework performance. Not at all like electromagnetic or power-based channels, micro architectural side and covert channel don't require physical proximity to the physical proximity. These attacks are non-obtrusive in which an attacker can get private information, for example, secret keys by basically watching the side channel information leakage. (such as the power consumption, timing, and electromagnetic emanations). This survey gives an overview of the side channel attacks, extricates the key elements of the processor's micro architectural functional units ,surveys the methods and techniques utilized in these attacks and is expected to anayse the execution of elliptic bend cryptosystem under side channel attacks.

I. INTRODUCTION

Security has for quite some time been a concern in computing and communications systems, and significant research exertion has been dedicated to tending to it. Cryptographic algorithms, including symmetric ciphers, public-key ciphers, and hash functions, frame an arrangement of primitives that can be utilized as building pieces to develop security components that objective particular objectives[1]. For example, network security protocols, such as SSH and TLS, consolidate these primitives to give validation between communicating substances, and guarantee the privacy and respectability of communicated data. In practice, these security mechanisms just determine what functions are to be performed, regardless of how these functions are implemented. Provable security turns out to be increasingly famous in the cryptographic community. It is currently basic to consider it to be a property of a cryptosystem. Provable security is at the protocol level, a harder assignment might be to assess the security of a cryptosystem at the implementation level.

Wireless Sensor Networks (WSN) have been broadly considered as a standout amongst the most vital technologies[5]. They principally comprise of a few autonomous sensors to collaboratively monitor physical and environmental conditions[4]. These sensor hubs are little in estimate and outfitted with sensors, embedded microcontrollers, and radio transceivers. They don't as it were have sensing capacities yet in addition data processing and communicating capacities. They are likewise application subordinate and essentially intended for real-time gathering also, analysis of low level data in hostile environments[6]. WSNs are especially powerless against side channel information assaults. Side channel information will be information that is spilled while a cryptographic device is performing cryptographic calculations, for example, encryption/decryption and of generation of certificates.

II. Scope of the Survey

This survey concentrates on side and undercover channels which may exist inside a modern processor. This incorporates processor cores and any practical units inside a multi-core multi-threaded processor such as caches, memory controller, or interconnection network. This work does no take a gander at different segments of a computer, e.g. hard drives and related timing secret channels due hard drive disk head development[2]. Likewise, concentrate is on software attacks on hardware where an attacker process can take in some information about casualty process, or coordinating attacker processes can send information between each other. Hardware attacks, for example, power examination side channels [8] or electromagnetic side channels [7] are not in the extension.

III. MODELS OF SIDE CHANNEL EFFECT

A cryptographic primitive can be considered from no less than two purposes of perspectives: from one viewpoint, it can be seen as an abstract

mathematical object then again, this primitive will in fine must be implemented in a program that will keep running on a given processor, in a given environment, and will subsequently show particular attributes. The principal perspective is that of classical cryptanalysis; the second one is that of side-channel cryptanalysis. Side-channel cryptanalysis exploits implementation-particular attributes to recuperate the mystery parameters associated with the calculation. It is in this manner significantly less broad — since it is particular to a given usage however frequently substantially more intense than classical cryptanalysis, and is viewed as genuinely by cryptographic devices' implementers. In traditional cryptanalysis, while evaluating the security of a cryptographic protocol, one more often than not accept that the advisory has an entire depiction of the protocol, is in control of all public keys, and is just inadequate with regards to learning of the secret keys.

Likewise, the adversary may have intercepted a few data traded between the legitimate participants, and may even have some control over the idea of this data (e.g., by choosing the messages in a picked message assault on a mark conspire, or by choosing the cipher text in a picked cipher text assault on an open key encryption plot). The adversary at that point endeavors to bargain the protocol objectives by either taking care of a fundamental issue thought to be unmanageable, or by misusing some plan imperfection in the protocol.

IV. SIDES CHANNEL ATTACKS

The objective of side channel attacks is to extricate private data, i.e., a secret key or even the implemented algorithm, from the physical conduct of the objective gadget [3]. The aggressor can utilize distinctive variations of side channel attacks to reason the internal workings of the software or the hardware of the hub [9].

The attacker may utilize techniques for example, power analysis (straightforward power analysis and differential power analysis), execution cycle frequency analysis, timing data analysis (on information development into furthermore, out of the CPU), electromagnetic radiation analysis, acoustic emission analysis, and so forth [9].

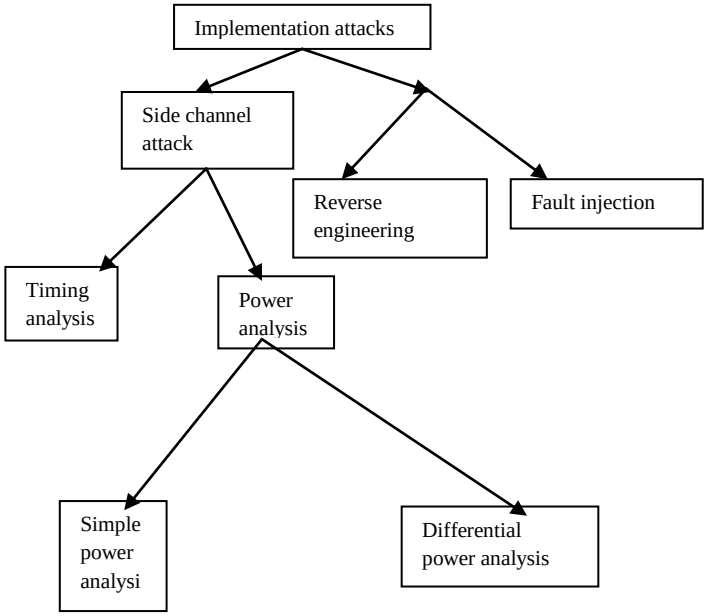

FIGURE 1: CLASSIFICATION OF ATTACKS

Figure 1 presents a classification of the attacks. In principle, any of the above side channels can be considered for an attack.

V. POWER ANALYSIS ATTACKS

There two fundamental variants attacks (simple power analysis and differential power analysis attacks). A simple power analysis (SPA) assault is a technique used to straightforwardly and outwardly review the power utilization flag estimations gathered while a device is performing cryptographic operations. Differential Power Analysis (DPA) assault utilizes factual analysis and mistake revision techniques to separate data associated to mystery keys of a cryptographic device [10]. In SPA, the data of a single power consumption estimation can be utilized for an attack. Be that as it may, the attack must be fruitful if the flag which the attacker needs to misuse is completely present in the got power follow. In the event that the flag which the attacker needs to misuse is secured with a considerable measure of commotion, at that point a few power consumption follows can be gathered and measurable systems can be utilized for flag investigation, which is referred to as DPA. Side channel attacks shouldn't interrupt the ordinary operation of a device. In any case, these attacks may not stay unnoticed when executed to sensor nodes [11].

VI. CONCLUSION

According to the perceptions made here it has been appeared how powerful power examination

attacks are and that they are generally simple to execute, along these lines making unprotected wireless sensor systems vulnerable to these attacks. This is since the sensor hubs are conveyed in unguarded environments without legitimate physical shielding. side and incognito channel look into has indicated assortment of, regularly extremely sharp, methods for extracting data for a computer system. Processor micro architectural side and incognito channel assaults have developed as a few of the most cunning assaults, and ones which are difficult to manage, without affecting system performance. Cryptology might be viewed as a continuous struggle amongst cryptographers and cryptanalysts. Assaults on cryptography have a similarly long history. The security of cryptographic modules for giving a reasonable level of assurance against white-box assaults ought to be analyzed in an absolutely un-put stock in execution environment.

VII. REFERENCES

[1] A. J. Menezes, P. C. Oorschot, S. A. Vanstone. Handbood of applied cryptography(5th edition). CRC Press, 2001.

[2] Gold, B., Linde, R., Cudney, P.: Kvm/370 in retrospect. In: Security and Privacy,1984 IEEE Symposium on. pp. 13{13. IEEE (1984)

[3] Schellenbrg, F., "Comparing Power and Electromagnetic Analysis of Embedded Devices," Ruhr-Universitat Bochum, Bachelor Thesis 2006

[4] Pongaliur, K., Abraham, Z., Liu, A., Hiao, L. and Kempel, L., "Securing Sensor Nodes Against Side Channel Attacks," in High Assurance Systems Engineering Symposium, 2008. HASE 2008. 11th IEEE, 3-5 December 2008, 2008, pp. 353-361.

[5] Zheng , J. and Jamalipour, A., "Introduction to Wireless Sensor Networks," in Wireless Sensor Networks: A Networking Perspective. 1, Zheng J. and Jamalipour A., Ed.: Wiley-IEEE Press, 2009, pp. pp.1-18.

[6] Padmavathi , G. and Shanmugapryiya, D., "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks," International Journal of Computer Science and Information Security (IJCSIS),vol. 4, no. 1&2, pp. 1-9, 2009.

[7] Gandol_, K., Mourtel, C., Olivier, F.: Electromagnetic analysis: Concrete results.In: Cryptographic Hardware and Embedded SystemsCHES 2001. pp. 251{261.Springer (2001)

[8]. Kocher, P., Ja_e, J., Jun, B.: Di_erential power analysis. In: Advances in CryptologyCRYPTO99. pp. 388{397. Springer (1999)

[9] Han , Y., Zou, X., Liu, Z. and Chen, Y., "Improved Differential Power Analysis Attacks on AES Hardware Implementations," in International Conference on Wireless Communications, Networking and Mobile Computing (WiCom'07), 2007, pp. 2230-2233.

[10] Kocher , P., Jaffe, J. and Jun, B.. (1998) Cryptography Research. [Online]. HYPERLINK " http://www.cryptography.com/dpa/technical"http://www.cryptography.com/dpa/technical

[11] Meulenaer , G., and Standaer, F., "Stealthy Compromise of Wireless Sensor Nodes with Power Analysis Attacks," in MOBILIGHT2010, 2010, pp.229-242.