Side Channel Attacks in IaaS and Its Defense Mechanisms

R. Vanathi, SP. Chokkalingam

ABSTRACT--- The Cloud Computing (CC) consumes monetarily prominent for collective assets of another third party applications. A cloud stage empowers to part assets between commonly doubting CC customers and provides financially savvy, on-request mounting. With the exponential development of Cloud Computing condition, vulnerabilities and their relating misuse of the overall cloud assets may possibly increment. In spite of the fact that CC gives various advantages to the distributed computing inhabitant, Be that as it may, includes specifically asset allocation and Virtual Machine (VM) physical residing in the likely for touchy data spillages, for example, Side Channel (SC) attacks. In this paper various side channel attacks, its defence mechanisms has been discussed and also a comparison is made among those attacks.

Keywords – VM, SEMA, DEMA, CRT, AES.

I. INTRODUCTION

The Side channel attack is in contrast to encryption, which shields data from being interpreted by unapproved people, Side Channel attacks mean to abuse the encryption frameworks and to shroud the event of correspondence. SC outbreaks were at first recognized as the primary danger on staggered secure frameworks for example OS, database, and systems. All the more as of late, the focal point of the analysts has moved nearby Side Channel attacks in Cloud Computing. From the previous dimension store (L2 or L3) is constantly mutual between VM, is the most focusing on device for these outbreaks. Accordingly, the point of this article is to investigate cross-VM SC attacks including the CPU reserve and their countermeasures in CC and to contrast and the customary SC attacks and countermeasures [1]. We sorted the SC attacks as indicated by the equipment intermediate they aim and endeavour manners in which they get the module and the technique they use to extricate private data. The cross VM side channel attack is the major attack on Infrastructure as a Service (IaaS).

Distributed computing gives a compelling plan of action to the organization of IT foundation, stage, and programming administrations. Regularly, offices are redistributed to cloud suppliers and this offers the administration shopper virtualization advancements without the additional cost weight of improvement. Notwithstanding, virtualization acquaints genuine dangers with administration conveyance, for example, DoS attacks, Cross-VM Side Channel attacks, Hypervisor Escape and Hyper-jacking. A standout amongst the most modern types of attack is the cross-VM store side channel attack that misuses shared reserve memory between VMs. A reserve side direct attack results in side channel data spillage, for example, cryptographic keys.

In this paper the side channel attacks types are discussed in section II and the defence methods are compared in section III and the conclusion is discussed in section IV.

II. SIDE CHANNEL ATTACK

Different strategies utilized by the aggressors to dispatch reserve side channel attack are exhibited, similar to a basic examination of countermeasures against store side channel attacks as shown in figure 1.

- Cache based side channel Attack
- Timing Attack
- Power-Monitoring Attack
- Electro-magnetic Attack
- Acoustic and Eaves Dropping Cryptanalysis
- Differential Fault Analysis
- Data Ruminate

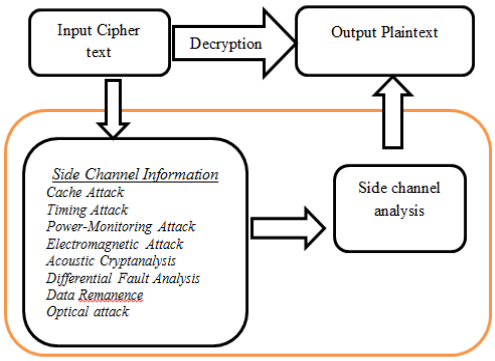

Fig 1: Side Channel Attack

2.1 Cache Based Attack

Cache based side channel attack uses application behaviour of cache memory to leak data about the encryption algorithm to the attacker. The Cache-based Side Channel Attack (CSCA) is copied by the government operative procedure by checking the mutual store of the VM and if the assailant associates any entrance with data by the unfortunate casualty the data loses its security as the programmer will attempt to break the cryptographic encryption calculation to take the key utilized for encryption. One of the significant attacks in the Infrastructure as a Service of cloud is cross VM attack, which has a more serious danger of aggressor's virtual machine trading off the injured individual's virtual machine

Revised Manuscript Received on February 14, 2019.

R. Vanathi, Research Scholar Saveetha School of Engineering, Saveetha University, Chennai, Tamil Nadu, India. (vanathisriram@gmail.com)

SP.Chokkalingam, Department of Information Technology
Saveetha School of Engineering, Saveetha University, Chennai, Tamil Nadu, India. (Cho_mas@yahoo.com)

to take the encryption key [2]. Reserve based attack happens for the most part in the for all intents and purposes isolated condition, where the assailant's virtual machine and the unfortunate casualty's virtual machine should keep running on the equivalent physical condition, having a similar primary memory and store. The different dimensions of store are L1, L2 and L3 (Highest-Level)[15].

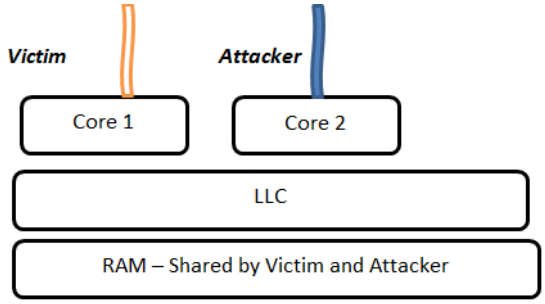

Fig 2: Cache based attack

The LLC, shown in figure 2, is shared among every one of the centers of a multicore crumb and is a brought together store, i.e., it holds the two data. LLC dimensions amount in megabytes, and get to latencies are of the request of 40 cycles [16]. Bolster centre private, brought together L2 reserves of middle of the road size and inactivity. Any memory get to first gets to the L1 reserve, and on a miss, the demand is sent down the pecking order until it hits in a reserve or gets to primary memory. The L1 is ordinarily listed by virtual location, while every other store is filed by physical location.

2.2 Timing Attack

In timing attack the attacker monitors/analyse the amount of time taken by the system to respond to the input fed into the computer. The time taken to produce the output varies depending on the encryption algorithm, system performance, optimization techniques, Ram, cache hits and so on. The statistical analysis is used to find out the decryption key to break the encryption algorithm. Timing attack mainly target the application that uses OpenSSL like smart cards and web servers. However the attack on web servers is not really successful because the time taken for accessing the web server might be deviated due to the network condition as well. Mainly the timing attack is being implemented on smart cards [29].

Vulnerability

Host based Security: If host based security is provided by encrypting the data on the smart card still vulnerability happens during the transmission data between the card and the computer. Physical vulnerability: The attackers can try physical attack through physical tampering of the smart card which is a technique used to remove the small chip from the smart card and through series of techniques the data and the metal line tracing on the chip can be identified by the attacker.

Properties of timing attack

In the above attack, unfailingly, the attacker can just derive whether a web asset is stored, among countless assets that may uncover clients' security. At the end of the day, the "data rate" of spilled data in such testing attacks is exceptionally low. Attributable to the constrained data available through testing, assailants/malevolent sites need a substantial number of dull activities to remove enough data for deducing few clients' protection. For instance, to test clients' perusing history, the attacker must set up a rundown of URLs and check every one of them over and over . Likewise, the consequence of a functional planning put together testing will contrast depending with respect to the speed of the equipment on which the program is running. To accomplish exact time sensitive estimation results, attackers must recurrent time estimation tasks to accomplish the ideal alignment.

2.3 Power-Monitoring Attack

Power monitoring attack is one form of side channel attack in which the attacker will monitor the power consumption of the hardware devices like, IC(Integrated Circuits), smart card and temper resistant. Through this technique the sensitive details like encryption key and other private details from the device[4].

Simple Power Analysis(SPA) includes outwardly translating force follows, or charts of electrical action after some time. Differential Power Analysis (DPA) is a further developed type of intensity examination, which can enable an aggressor to process the halfway qualities inside cryptographic intentions through factual examination of data gathered from numerous cryptographic tasks[5].

The fast increment in the utilization of inserted frameworks for performing secure exchanges, has relatively expanded the security dangers which are looked by such gadgets. Side channel attack, a modern security danger to implanted gadgets like smartcards, cell phones and PDAs, abuses the outer signs like preparing time, control utilization and electromagnetic discharge to recognize the interior calculations. Power investigation attack, presented by Kocher in 1998, is utilized by enemies to listen stealthily on confidential data while the gadget is executing a safe exchange. The enemy watches the power follow scattered/devoured by the chip amid the encryption/decoding of the AES cryptographic program and predicts the mystery key utilized for encryption by extricating important data from the power flow.

Countermeasures proposed to beat control examination are data screening, table screening, current flattening, hardware level arrangements, sham guidance inclusions, adjusting bit-flips, and so on. Every one of these strategies are either helpless to multi-request side channel attacks, not sufficiently conventional to cover all encryption calculations, or weight the framework with high region cost, run-time or vitality utilization.

2.4 Electro-magnetic Attack

Electro-magnetic attacks are attacks caused by releasing the electromagnetic emission liquidated from gadget and carries out signal examination on the same. This kind of attack are a progressively explicit kind of attack in which the attack generation in known explicitly [24]. Electromagnetic attacks are commonly non-obtrusive and

aloof, implying that these attacks can be performed by watching the typical working of the objective gadget without causing physical damage. However, an assailant may improve motion with fewer clamours by repackaging the chip and gathering the flag nearer to the source. These attacks are effective against cryptographic usage that perform distinctive tasks dependent on the data at present being handled, for example, the square-and-increase execution of RSA. Diverse activities discharge distinctive measures of radiation and an electromagnetic hint of encryption may demonstrate the precise tasks being performed, enabling an aggressor to recover full or fractional private keys [18].

Attack methods

Two types of Electromagnetic attacks are:

Simple Electro Magnetic Analysis (SEMA) attacks and Differential Electro Magnetic Analysis (DEMA) attacks.

Simple electromagnetic analysis - In straightforward electromagnetic examination (SEMA) assaults, the assailant reasons the key specifically by watching the follow. It is extremely successful against deviated cryptography implementations. Typically, just a couple of follows are required; however the aggressor needs a solid understanding of cryptographic gadget and the execution of its computation. An execution defenceless against SEMA assaults will play out an alternate task contingent upon the bit of the key, which is 0 or 1, which will utilize distinctive measures of intensity and additionally extraordinary chip segments.

Differential electromagnetic analysis - Sometimes, straightforward electromagnetic examination is preposterous or does not give enough data. Differential electromagnetic investigation (DEMA) assaults are progressively perplexing, yet are powerful against symmetric cryptography usage, against which SEMA assaults are not. Additionally not at all like SEMA, DEMA assaults don't require much learning about the gadget being assaulted.

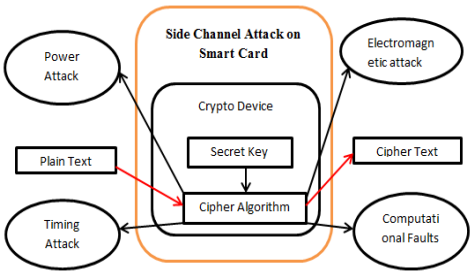

Fig 3: Side Channel Attack on Smart Cards

2.5 Acoustic and Eavesdropping cryptanalysis

Audio cryptanalysis is a sort of side channel assault that abuses sounds transmitted by PCs or different gadgets. A large portion of the cutting edge acoustic cryptanalysis centres around the sounds delivered by PC consoles and interior PC parts, however generally it has additionally been connected to affect printers, and electromechanical disentangling machines.

Numerous PCs transmit a piercing clamour amid task, because of the tremor in part of their electronic components. The acoustic radiations in excess of a worsening can permit on data about the product successively executed on the PC and precisely deliver delicate data about security-related calculations. In a fundamental introduction, we have appeared changed RSA keys instigate diverse sound examples, yet it was not clear how to extricate singular key bits. The fundamental issue was the extremely low transfer speed of the acoustic side channel [6].

Past audibility, demonstrates a comparative low-data transfer capacity assault can be performed by estimating the electric capability of a PC body. An appropriately prepared assailant need simply contact the objective PC with his exposed hand, or get the required leakage data from the commencement at the remote end of VGA, Ethernet links or USB [13].

A side channel is an assault vector that is non-immediate and flighty, and therefore hasn't been legitimately verified. For instance, your pass code keeps me from straightforwardly assaulting your telephone — however in the event that I could work out your pass code by taking a gander at the oily smirches on your screen, that would be a side station assault. For this situation, the security specialists tune in to the shrill (10 to 150 KHz) sounds delivered by your PC as it unscrambles data[14].

2.6 Differential Fault Analysis

Differential fault analysis (DFA) side channel attack is an attack generated in the cryptanalysis field. The logic behind this attack is to generate or inject faults in sudden environmental conditions—into cryptographic implementations, to disclose internal states of the hardware implementations. For example, the embedded processor in the smart card may be prone to high temperature, unconfirmed supply voltage or current, extremely high overclocking, robust electric or magnetic fields, or even ionizing radiation to affect the processor operations. Due to which the processor will produce improper outcomes due to physical data corruption, out of which the attacker may read the instructions executed by the processor. Almost around 200 single-flipped bits are needed to get a secret key in DES and Triple DES[23].

Blaming an ongoing smartcard is troublesome, with a high hazard to make the chip self-destruct in the event that it distinguishes an assault; that is the reason late DFA inquire about endeavor to limit the prerequisites on the quantity of flaws. It is straightforward, which a very convincing property is given that we need to execute it independent from anyone else and surmise some missing parts in its depiction.

2.7 Data Reminisce

Data reminisce is the lingering physical portrayal of data that has been deleted or overwritten. In non-unpredictable programmable gadgets, for example, UV EPROM, EEPROM or Flash, bits are put away as charge in the coasting door of a transistor. After each eradicate task, a portion of this charge remains. Security assurance in microcontrollers and smartcards with EEPROM/Flash recollections depends on the presumption that data from the memory vanishes totally in the wake of eradicating. While microcontroller makers effectively solidified as of now their

structures against a scope of assaults, regardless they have a typical issue with data remanence in drifting door transistors. Indeed, even after an eradicate activity, the transistor does not return completely to its underlying state, in this manner enabling the aggressor to recognize recently modified and not customized transistors, and in this manner re-establish data from deleted memory[17].

The examination toward this path is condensed here and it is appeared much data can be removed from some microcontrollers after their memory has been 'deleted'.

2.8 Results & Discussions

The optical attack is based on the visual capturing of the sensitive information. The Cathod Ray Tube could be used as a monitoring method to view the contents from a distance. The concentration of light released from the raster-scan screen as operation of time belongs to the video indication convolved with the urge reaction of the phosphors. Hackers of this type of attack will try their level best to monitor the data emitted from the light of CRT. The text can be converted into the readable format through photo sensors [8]. In these type of eaves dropping attack the motive of the hacker/attacker is to monitor the data to steal the sensitive information's like password, decryption key and other sensitive content. It is just a passive method in which the information is just stolen without modifying the data.

If the photon reaches the metal plate with 1.1eV of strength, an electron-hole pair will be generated. The unique photon will be consumed by the electrons and then separate through atomic binding. An eletric field like in a transistor can detach the pair, which results in current. This is termed photovoltaic effect. The encouraged current may affect SRAM cells to switch. To initiate the signal for the light diode, output port of the microcontroller has been used. It is also possible to activate physically using an on/off-switch [11].

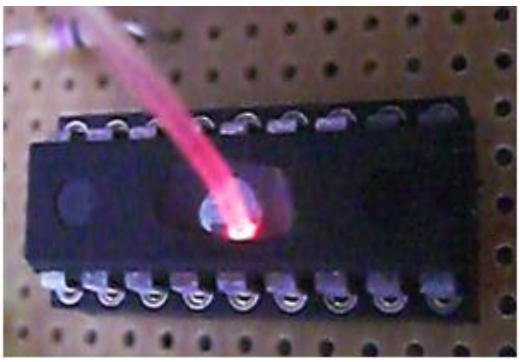

Fig 4: Laser light attack on a micro-controller using a fibre-optic light guide

III. III COMPARISON ON VARIOUS SIDE CHANNEL ATTACKS

Table 1
A Comparison on various side channel attacks, behavior and defense mechanism

Attack Type	Behaviour	Physical Security Attack	Defending Mechanism
Cache Attack	Shared cache memory will be monitored by the attacker to steal the sensitive information.	Non-invasive, Passive	Sandbox (Dynamic binary translation)[16]
Timing Attack	Keep track of computation time to detect the strength of the algorithm.	Non-invasive, Passive	StopWatch, to modify timings observed by the attacker VM[21]
Power-Monitoring Attack	Examines the power consumption by the hardware devices.	Non-invasive, Passive	Game theoretic approach[20]
Electromagnetic Attack	Monitoring the electromagnetic radiations, leaked to steal the sensitive information like decryption key.	Non-invasive, Passive	new ROM is used to design the AES cryptographic circuit[18]
Acoustic Cryptanalysis	Examines the sound produced by the hardware device including the key press.	Non-invasive, Passive	Using Sensor nodes and SecureVibe[15]
Differential Fault Analysis	Faults or Errors will be introduced in the system to monitor the original sensitive data.	Non-invasive, Passive	New AES with pipeline structure and Silicon-Level Countermeasure[19]
Data Reminisce	Sensitive data will be revoked even after deleting it from primary memory.	Invasive, Passive	Safe circuits are used to integrate erased data into conventional SRAM[17]
Optical attack	Through visual recording the sensitive data will be hacked.	Non-invasive, Passive	Public-key cryptography scheme.

The various side channel attacks have been compared and its defence mechanisms are discussed in table 1.

IV. CONCLUSION AND FUTURE WORK

The various attacks generated by the side channel attack have been discussed. Each and every attack has its own ways of attack generation, detection techniques and defence mechanisms against the various securing cryptographic algorithms. Because of the numerous profits and on demand services of the cloud there are so many organisations and end users who make use of the cloud services. The users should know about the issues in cloud computing to avail the cloud computing services in a secured way. In this paper we have discussed about various side channel attacks. The tabulation explains about the various side channel attacks and its effects. To prolong the survey of this paper, various attack generation and defence mechanisms of the side channel attacks can be concentrated individually.

REFERENCES

1. Minhaj Ahmad Khan, "A Survey of Security Issues for Cloud Computing", Journal of Network and Computer Applications, 2016.
2. Jiming Xu and Howard M. Heys,"Template Attacks of a Masked S-Box Circuit: A Comparison Between Static and Dynamic Power Analyses", IEEE, 2018, pp 277-281.
3. Hasindu Gamaarachchi Harsha Ganegoda," Power Analysis Based Side Channel Attack",http://www.ce.pdn.ac.lk.
4. Marc Witteman Riscure The Netherlands
5. Marc Witteman, Riscure The Netherlands,"Secure Application Programming in the presence of Side Channel Attacks", www.riscure.com.
6. Franc¸ois-Xavier Standaert, "Introduction to Side-Channel Attacks", Secure Integrated Circuits and Systems, Springer 2010, pp 27-42.
7. Ashish Singh and Kakali Chatterjee , "Cloud security issues and challenges: a survey", Journal of Network and Computer Applications, 2016.
8. Andrey Leshenko, "Emission Security and Side-channel Attacks",Comp Sec Seminar 2017.
9. Arti Ochani , Ramrao Adik , "Security Issues In Cloud Computing", International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2017), pp 783-787. VMM
10. Yiwen GAO1,2, Wei CHENG1, Hailong ZHANG1, Yongbin ZHOU, "Cache-Collision Attacks on GPU-based AES Implementation with Electro-Magnetic Leakages", 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications,2018, pp 300-306.
11. Jörn-Marc Schmidt and Michael Hutter,"Optical and EM Fault-Attacks on CRT-based RSA: Concrete Results", Secure Business Austria (SBA), Graz University of Technology, Inffeldgasse 16a, 8010 Graz, Austria
12. R.Barona , E.A.Mary Anita, "A Survey on Data Breach Challenges in Cloud Computing Security: Issues and Threats", 2017 International Conference on circuits Power and Computing Technologies [ICCPCT].
13. Asif Raza Kazmi, Mehreen Afzal, Muhammad Faisal Amjad, Adnan Rashdi, "Combining Algebraic and Side Channel Attacks on Stream Ciphers", 2017 International Conference on Communication Technologies (ComTech), IEEE, pp 138-142.
14. Younghyun Kim, Woo Suk Lee, Vijay Raghunathan1 , Niraj K. Jha and Anand Raghunathan, "Vibration-based Secure Side Channel for Medical Devices", June 7–11, 2015, San Francisco, CA, USA, ACM.
15. Kanthakumar Pongaliur, Zubin Abraham1, Alex X. Liu, Li Xiao, Leo Kempel, "Securing Sensor Nodes Against Side Channel Attacks", 2008 11th IEEE High Assurance Systems Engineering Symposium,pp 353-361.
16. Mengjia Yan, Read Sprabery, Bhargava Gopireddy, Christopher Fletcher, Roy Campbell, Josep Torrellas, "Attack Directories, Not Caches: Side-Channel Attacks in a Non-Inclusive World", IEEE.
17. He Yuemei, Guan Haibing, Chen Kai, Liang Alei, "A New Software Approach to defend against Cache-based Timing Attacks", 2009, IEEE.
18. Kang Wenjing, Yu Kai, Yu Guoyi*, and Zou Xuechen, "Novel Security Strategies for SRAM in Powered-off State to Resist Physical Attack", ISIC, 2009, PP 296-301.
19. Tsunato Nakai, Megumi Shibatani, Mitsuru Shiozaki, Takaya Kubota, Takeshi Fujino, "Side-Channel Attack Resistant AES Cryptographic Circuits with ROM reducing Address-Dependent EM Leaks", 2014 IEEE, pp 2547-2550.
20. Sho Endo, Yang Li, Naofumi Homma, Member, IEEE, Kazuo Sakiyama, Member, "A Silicon-Level Countermeasure Against Fault Sensitivity Analysis and Its Evaluation", IEEE TRANSACTIONS ON VERY LARGE SCALE INTEGRATION (VLSI) SYSTEMS, 2014.
21. Longfei Wei, Amir Hasan Moghadasi, Aditya Sundararajan and Arif I. Sarwat, "Defending Mechanisms for Protecting Power Systems against Intelligent Attacks", 2015 10th System of Systems Engineering Conference (SoSE), 2015 IEEE, pp 12-17.
22. Peng Li , Debin Gao, Michael K. Reiter , "Mitigating Access-Driven Timing Channels in Clouds using StopWatch", 2013 IEEE.
23. Ziqi Wang; Rui Yang; Xiao Fu; Xiaojiang Du; Bin Luo, "A shared memory based cross-VM side channel attacks in IaaS cloud", 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Year: 2016, pp 181 – 186.
24. Geetanjali Nenvani, Huma Gupta, "A Survey on Attack Detection on Cloud using Supervised Learning Techniques", 2016 Symposium on Colossal Data Analysis and Networking (CDAN). VM escape
25. Asma A. Shaikh , "Attacks on Cloud Computing and its Countermeasures", International conference on Signal Processing, Communication, Power and Embedded System (SCOPES)-2016, pp 748 – 752. Malware injection attack
26. Xiangyu Li, Member, IEEE, Chaoqun Yang, Jiangsha Ma, Yongchang Liu, and Shujuan Yin, "Energy-Efficient Side-Channel Attack Countermeasure With Awareness and Hybrid Configuration Based on It", IEEE Transactions on Very Large Scale Integration (VLSI) Systems, 2017, pp 1-14.
27. B.Sumitra, C.R. Pethuru, M.Misbahuddin, "A Survey of Cloud Authentication Attacks and Solution Approaches", International Journal of Innovative Research in Computer and Communication Engineering, oct 2014, pp: 6245-6253.
28. Yongle Wang, JunZHang Chen, "Hijacking spoofing attack and defense strategy based on Internet TCP sessions", 2013 2nd International Symposium on Instrumentation and Measurement, Sensor Network and Automation (IMSNA), pp: 507 – 509.

29. Balasubramani S, S.K. Rani, K. Suja Rajeswari "Review on Security Attacks and Mechanism in VANET and MANET" Artificial Intelligence and Evolutionary Computations in Engineering Systems, pp. 655–666, 2016.
30. Alxander E, Sathyalakshmi, "Privacy-aware set-valued data publishing on cloud for personal healthcare records", International Conference on Artificial Intelligence and Evolutionary Computations in Engineering Systems, ICAIECES, 19 May 2016, pp 323-344.