Review on variants of Architecture against Cache-Based Side-Channel Attacks

Mr. Niketan G. Patel[1] Prof. Chirag A. Patel[2]
[1]P.G. Student [2]Associate Professor
[1,2] Department Of Computer Engineering
[1]Gujarat Technological University, Gandhinagar [2]Government Engineering College, Modasa City

Abstract— there are various types of caches. Cache components include data and instruction caches. There are various types of cache attacks also. In hardware cache attacks are performed using cache hit and miss, power traces, Monitoring memory of cache activity. In software caches attack are performed when derive secret key use in Cryptographic operation through legitimate. Cache attacks are reducing performance and also leakage information of virtual machine. In this paper we have presented variants of architecture which stop cache based side channel attacks.

I. INTRODUCTION

Side channel attack is any attack of information gained from the psychical implementation. In software cache attacks are performed on secret keys. There are various cryptographic techniques for encode the information decode by using the same key where at least one key is secret key. Size of secret key is depending on which cryptographic algorithm use for sharing key. If the key is long enough then its time consuming to decode information so that antagonist are use extra information power[1],time elapsed , electromagnetic radiation, acoustic, faults/error[2] in the program, cache access time etc. such attacks known side channel attacks [3][4].vary depending on the basis of attack.

A. *General classes of attacks*

1) *Timing attacks*: attack based on how much time take performed for process.
2) *Power monitoring attack:* Which make use of change of power consumption by hardware.
3) *Electromagnetic attack*: it based on leaked electromagnetic radiation which can directly provide plain text and other information.
4) *Data eminence:* In which data are after supposedly having been deleted. [1]
Also cache component share using cloud computing.

B. *Cloud computing has a three basic models*

1) *Public cloud model:* This cloud based on creates application for general public over internet.
2) *Private cloud model:* It is private or internal model using for single organization. It is managed by third party.
3) *Hybrid Cloud model:* Hybrid cloud is combination of public and private cloud. [5]

Using cloud computing virtualization enables to share multiple machines to single path. Resources are virtualized by virtual monitor. Virtual monitor machine give guarantee to provide effective resources. Attacks are possible in this technology using third party response. Investigation on side channel attack is very difficult to stop because of many results generate using internet. In cloud computing provide security is relatively poor. [6]

II. VARIANTS OF ARCHITECTURE AGAINST CACHE-BASED SIDE-CHANNEL ATTACKS

A. *Side channel attack reduce using Hardware/Software count measure*

In this paper to build a framework for exploited the vulnerability of first two phase of AES algorithm. In this algorithm founier and tunstall [6] which are trace driven cache attacks. Their attacks are power based attack using AES encryption and cache size 16 byte. Researcher tried to attack with cache line size containing a single element of SBOX such line reduce to zero [6].They are choose this attack because if attack fails then it’s also fails in time based attack also. Most of attacks are based on electromagnetic, radiation. Algorithm is failed if it couldn’t recover the cache traces. In proposed algorithm they are taking 16 bit of plain text and 16 bit of secret key. They are assigning random value (s) to the first element of plain text They are assign same value to next plain text and execute AES using secret key and record hit/miss pattern after AES phase1.After that they are check ideal AES hit or miss pattern and execute this steps until ideal pattern not get.

After achieve ideal pattern varying relative plain text logical relation of secret key with plain text. After that first element of plain text XOR with second secret key and generate resultant after that in second element XOR with second secret key and add initial value and varying with ideal pattern if its correct or not. They are find logical relation key bytes. They after passing a plaintext with secret key B and generate encrypted data. After that pass 256 key and encrypt this value with reference key. They are found out same value. Vulnerable part of AES system when XOR with sub byte substitution. They are stored this value on hardware in conventional system store into temporal and spatial locality nature of cache the attack can find this value and use statically methodology in this algorithm they are take an extra hardware so that processor which hold SBox value without communicating memory. It is communicating to hardware so that cache never SBox value. [6]

B. *Two- Stage mode detect cache based side channel attack*

In this algorithm detection approach is known as CSDA. They are use two detection mode guest detection and host detection mode. They are use cpu-utilization and memory utilization of guest. K-means clustering used for detection of result for the host detection they are used shape test for attack features of cache miss sequence. Shape test use the first order statics like mean, variance and entropy. When regularity test use second order higher statics for describe features. In detection they are used to various definitions for detection. [9]

Cache Miss Times: Cache Miss Time is defined for particular time where CMT refers to cache miss times refer between intervals of time. [9]

Cache Miss Sequence: cache miss sequence is defined as the sequence comprised several cache miss time ordered by time. Where cache miss time measured in particular time. [9]

Suspect attack: Suspect Attack sequence a special cache miss sequence. That may exist in CSMA. If cache misses sequence meets special condition like if cache miss time of any particular time in cache miss sequence is larger than cache minimum threshold. [9]

Suspect Attack Windows: The time window corresponding to suspect attack window is defined as suspect attack window.

Host detection doing using these steps

1) Organizing samples CMT to CMS.
2) Check miss sequence is suspect attack sequence
3) Checked cache miss sequence is not suspected attack sequence that there is no CSA in the host. If cache misses sequence is suspected attack sequence than is submitted to guest detection. [9]

Guest Detection: In guest detection they are organize virtual cpu utilization and attack features are proposed second attack detection strategy is complete the guest detection. Virtual CPU utilization Vcus= {(m_1, t1) .... (Mn, tn)} CPU utilization sequence order by time where m_n is CPU utilization measured in time same as virtual memory utilization also m_n measured memory utilization in particular time. They are used two type of utilization rate. One for virtual memory utilization and one for CPU utilization rate.

URI is calculated using following steps.[9]

1) First divide steps in Z into Y non-overlapping windows whose size is t which satisfies n= Y*T.
2) Calculate standard deviation of each window.
3) Calculate standard deviation of pair wise difference. [9]

Divide URI in two class using K-means clustering smaller and larger class. Also the memory utilization rate and virtual CPU utilization are divided in to smaller class and larger class. If compute and interaction of virtual memory and virtual CPU utilization is empty then host detection is false. [9]

C. Side channel attack stop using virtual Fire wall

This paper is mainly focus on the defense of vulnerability of side channel attack. This algorithm is combination of randomly decryption and virtual firewall appliance. They are using firewall as cloud computing backend and preventing extraction using randomly decryption. [10]

Virtual Firewall Appliance: Firewall is protecting from other user of network. In virtual cloud they are initiate intruders. They are create new VM targeted VM and extract confidential information in conventional Method. They are place VM to targeted VM so that it prevent in virtual appliances [10].

Randomly Encryption and Decryption: Virtual appliances implementation prevent from side channel but most of cloud service use now in e-commerce so that strict security provide to that services. They provide confusion and diffusion. Confusion making relationship between plaintext and cipher text. Diffusion refers to that the randomly in static of plain text is "dissipated" in statics. The plaintext should be redistributed in the non uniforminity and it is larger so that it difficult to decrypt. Which is much harder to detect. In this algorithm they are used to decrypt to using confusion algorithm. Randomly encryption algorithm each and every time they are change encryption algorithm so that it is secure. Attacking cloud through cache based side channel in virtualization environment. [10]

D. Using Preloading concept reduce side channel attack

In concept of preloading or cache they are load all security critical data. An ES lookup all the cache before crypto operation. For the security concern PL is not provide better security in initial loading. In this algorithm they are combine PL to initial security and also combine preloading concept. In this algorithm no correlation between the secret key and cache hit so that this algorithm also protect against to time driven attack for which data is sensible. It is not load so that ant ganister could not have that information. Also this algorithm switches back to process of lock tables. Lock cache line replacement is done using match with active Id of cache with lock cache Id. If it is the owner ID then its replace otherwise it is not replace. Preloading and reloading concept is done using hardware logic preloading state part of process context switched then hardware will reload all critical data. So that hardware complexity is increase. In software all preloading and locking is performed during protected process. In this algorithm they devise exception handler to load all the critical data using pure hardware based defense mechanism such as RP cache. It can be easily updated. Informing loads are special load instructions that "inform" the software when the load misses in the cache. There are three ways implementing informing loads [8]. In the proposed algorithm all the protected tables are load with informing load instruction. All load information loading without extra overhead When hit the cache when miss occurs exception will generate if exception handler all the tables in predetermined order than earlier tables have higher chances than later.[7]

E. PTP Technique

PTP technique is allowed to probing and target instance of some level of overlapping access to shared cache resource. This technique concentrate on reduce the cache overlapping. Attempts to isolate data in the cache based on the VM that using it. When using probing instance the cache would flush every time the probing context. In non-cloud mechanism it's typically insufficient for cache flushing .The cloud techniques to be much more efficient scheduling architecture. Cache flush occur when relevant data store in cache. Cache is useless until the data store in cache so that reduce the cache flush when relevant data in cache. This technique flush cache when cpu switch domains when proper isolation between VM then all the data of previous domain is not used to next domain then its flush otherwise its untouched for next domain. Another factor is to reduce overhead it's depended on hardware but cache flushes is done when context switch occurs so that it reduce the flushing. This algorithm use scheduling algorithm for when cache flush is needed. Flushing the cache is able to occur if cpu goes to domain1 to ideal domain there is no need to flush the cache side channel could have been implement. For that VM implement for when flush is necessary Xen scheduler operates represented operates on scheduling units VCPUS. VCPU is represented a virtual CPU and is associated with domain. VCPU is given new data field "faint" which indicates the origin of data currently reside in the cpu cache VCPU's taint value is assigned the identifier for domain and the result of algorithm cache and flush occur when context switch occur.

REFERENCES

[1] Paul Kocher, Joshua Jaffe, and Benjamin Jun. "Differential power analysis". In Michael Wiener, editor, Advances in Cryptology CRYPTO 99, volume 1666 of Lecture Notes in Computer Science, pages 789–789. Springer Berlin / Heidelberg, 1999.

[2] Eli Biham and Adi Shamir. "Differential fault analysis of secret key cryptosystems". In Burton Kaliski, editor, Advances in Cryptology CRYPTO '97, volume 1294 of Lecture Notes in Computer Science, pages 513–525. Springer Berlin / Heidelberg,1997

[3] N. Lawson. "Side-channel attacks on cryptographic software". Security Privacy, IEEE, 7(6):65 –68, 2009.

[4] JeaHoon Park, HoonJae Lee, and ManKi Ahn. "Side-channel attacks against aria on active rfid device". In Convergence Information Technology, 2007. International Conference on, pages 2163 –2168, 2007.

[5] http://en.wikipedia.org/wiki/Side_channel_attack.

[6] Ankita Arora, Sri Parameswaran," A Hardware / Software Countermeasure and a Testing Framework for Cache based Side Channel Attacks" IEEE 2011.

[7] Jingfei Kong, Onur Aciic¸ mez, Jean-Pierre Seifert, and Huiyang Zhou,"Architecting against Software Cache-Based Side-Channel Attacks",VOL. 62,, IEEE 2013

[8] M. Horowitz, M. Martonosi, T. Mowry, and M. Smith, "Informing Memory Operations: Providing Memory Performance Feedback in Modern Processors," Proc. Int'l Symp. Computer Architecture (ISCA), 1996.

[9] Si Yu, Xiaolin Gui, Jiancai Lin, "An Approach with Two-Stage Mode to Detect Cache based Side Channel Attacks" pp 186 - 191,,*IEEE 2013,* ISBN 978-1-4673-5741-8

[10] Bhrugu Sevak, "Security against Side Channel Attack in Cloud Computing", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-2, December 2012.

[11] Michael Godfrey & Mohammad Zulkernine," A Server-Side Solution to Cache-Based Side-Channel Attacks in the Cloud", ISBN 978-0-7695-5028-2,IEEE 2013