A SURVEY ON CROSS VM SIDE CHANNEL ATTACK IN CLOUD COMPUTING

Ajay Kaarthic J[1] and Sangeetha G [2]
[1]B.Tech(IT)Student , Sri Venkateswara College of Engineering,
[2]Assistant professor, Sri Venkateswara College of Engineering,

ABSTRACT : Clouds are a large volume of virtualized resources which are easy to use and access. Multi tenancy is the biggest advantage of computing, where physical resources are shared among multiple clients. Virtualization facilitates multi tenancy with the help of the hypervisor. In a virtualization environment, many virtual machines (VMs) can run on the same core with the help of the hypervisor by sharing the resources. The virtual machines (VMs) running on the same core are the target for the malicious or abnormal attacks like side-channel attacks. Cache-based attack in the cloud is one of the side-channel attacks. More recently, the focus of the researchers has shifted toward side-channel attacks in Cloud Computing. Since the last level cache (L2 or L3) is always shared between VM, is the most targeting device for these attacks. Therefore, the aim of this paper to explore cache side chain attacks and their counter measures in Cloud Computing.

Keywords: Cloud computing, Cache based side chain attacks, Virtualization

1. INTRODUCTION

Cloud Computing (CC) is an Information technology paradigm that enables pervasive access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort, often over the Internet. It is a platform providing dynamic pool resources and virtualization. Based on a pay-as-you-go model, it enables hosting of pervasive applications from consumer, scientific and business domains. Cloud providers virtualize the resources like CPU, network interfaces, peripherals, hard drives, and memory using hypervisor. Cloud computing relies on sharing of resources to achieve coherence and economies of sales, similar to public utility . The top benefits of cloud computing are it eliminates the capital expense of buying hardware and software and setting up and running on site datacentres and vast amount of computing resources can be provisioned in minutes and power is saved and cloud computing is very much reliable. CC is a shared open environment, which has its own characteristics and features such as on-demand services and multi-tenancy. Specifically, it introduces multi-tenancy to facilitate the users to share computing physical resources provisioned over the Internet on-demand scaling.

1.1Types of Clouds Public Clouds : A Cloud in which service providers offer their resources as services to the general public, Public clouds offer several key benefits to service providers, including no initial capital investment on infrastructure and shifting of risks to infrastructure providers. However, public clouds lack fine-grained control over data, network and security settings, which hampers their effectiveness in many business scenarios.

Private Clouds : A Private Cloud Also known as internal clouds, private clouds are designed for exclusive use by a single organization. A private cloud may be built and managed by the organization or by external providers. A private cloud offers the highest degree of control over performance, reliability and security. However, they are often criticized for being similar to traditional proprietary server farms and do not provide benefits such as no up-front capital costs.

Hybrid CloudS : A Hybrid Cloud is a combination of public and private cloud models that tries to address the limitations of each approach. In a hybrid cloud, part of the service infrastructure runs in private clouds while the remaining part runs in public clouds. Hybrid clouds offer more flexibility than both public and private clouds.

1.2 Cloud services : Cloud offers services which can be grouped into three categories : software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). This paper provides cloud services at lower cost

Infrastructure as a Service : IaaS refers to on-demand provisioning of infrastructural resources, usually in terms of VMs. The cloud owner who offers IaaS is called an IaaS provider. Examples of IaaS providers include Amazon EC2 , GoGrid .

Platform as a Service : PaaS refers to providing platform layer resources, including operating system support and software development frameworks. Examples of PaaS providers include Google App Engine , Microsoft Windows Azure .

Software as a Service : SaaS refers to providing ondemand applications over the Internet. Examples of SaaS providers include Salesforce.com .

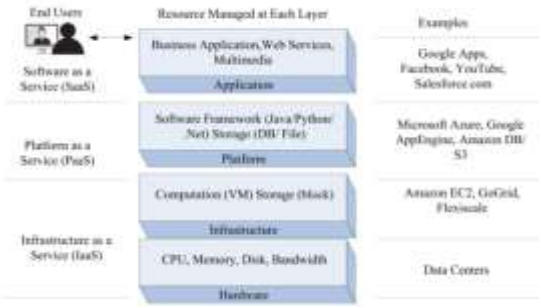

Fig.1: Layered model of cloud computing [1]

1.3Virtualization : Virtualization is a technique, which allows to share a single physical instance of a resource or an application among multiple customers and organizations. It does by assigning a logical name to a physical storage and providing a pointer to that physical resource when demanded ,Virtualization is the creation of a virtual rather than actual version of something, such as a server, a desktop, a storage device, an operating system or network resources.[2] virtualization involves using specialized software to create a virtual or software-created version of a computing resource rather than the actual version of the same resource. With the help of Virtualization multiple operating systems and applications can run on same Machine at the same time increasing the utilization and flexibility of hardware.

Types of Virtualization

Application Virtualization : Application virtualization helps user to use an application remotely from a server. The server stores all personal information and other characteristics of the application, but can still run on a local workstation. example, used in the case where user wants to run various version of same software.

Network Virtualization : The ability to run multiple virtual networks that each has a separate control and data plane. It coexist together on top of one physical network.[3] network virtualization provides flexibility, promotes diversity, and promises security and increased manageability. However, many technical issues stand in the way of its successful realization

Desktop Virtualization : Desktop virtualization is a practical research focus on the virtualization technology [4]. The purpose of desktop virtualization is to make the desktop virtual, so that users can log in to get their personal desktops through the network with any devices at any time and any place. This technology has a lot of advantages such as mobile computing, security, easier management and cost reduction, to greatly facilitate people's lives, Desktop virtualization allows the users' OS to be remotely stored on a server in the data center, allowing the user to then access their desktop virtually, from any location.

Storage Virtualization : Storage virtualization is an array of servers that are managed by a virtual storage system. The servers aren't aware of exactly where their data is, and instead function more like worker bees in a hive. It makes managing storage from multiple sources to be managed and utilized as a single repository. storage virtualization software maintains smooth operations, consistent performance and a perpetual suite of advanced functions despite changes, disruptions and differences in the underlying equipment.

2. Cross VM Cache Based Side Channel Attacks : Cache memory is located between RAM and CPU cores to remove the delay added by the accessing the data. The main objective of the cache memory is to decrease the required time for accessing data from the main memory. The cache is divided into L1, L2, and L3 level. Each VM has its own L1,L2 cache where L3 is a sharable cache. Although Side Channel (SC) attacks existed in the past in multilevel systems including database, operating system, and networking , the co-residency feature of the Cloud Computing(CC) makes cross-VM cache-based SC attacks more effective in this paradigm .It was very difficult to gain physical access to the system in the past, but with shared resources, in the cloud, physical access can be easily accomplished .Cross-VM Cache attacks are purely software based, and they extract the full encryption key of the well-known cryptographic algorithms including RSA, AES without any direct or physical interaction with the cryptographic devices .

These attacks are deployed very easily and are efficient as they require a short time to break the well-secured systems. Moreover, these attacks use the spying process to collect information about the accessed cache line for extracting the cryptographic key from Linux encrypted partition. The cross-VM cache-based SC attacks are also called remote attacks involving faraway observation of the normal input and output data of the device. Timing observation, cryptanalysis, analysis of the protocol, and SC attacks on the programming interfaces of applications are examples of remote timing attacks.

Cross VM cache based side channel attacks are due to the sharable L3 cache among variousVM's.

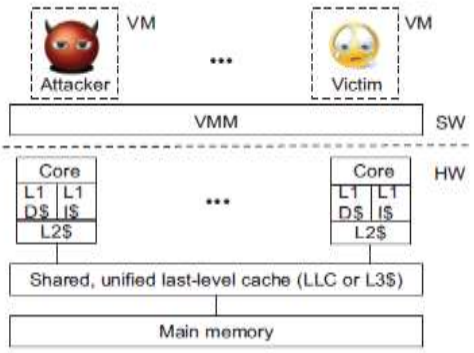

Fig.2:System model for a multi-core processor [15]

2.1 Categories of cross VM Cache based side channel attacks : The cross-VM cache based SC attacks are further categorized into time-driven, access-driven, and trace-driven attacks.

Time-driven side channel attacks : The cache is a processor component that stores recently used data in a fast memory block close to the microprocessor. Whenever the processor tries to retrieve data from the main memory, it can be delivered more quickly if this data is already stored in the cache (a.k.a. cache hit). On the other hand, if the data is not available in the cache (a.k.a. cache miss), it has to be fetched from the main memory (or a higher level of cache), which has a much larger latency compared to the cache. The difference between both cache access events, i.e. a cache hit and a cache miss, is measurable and provides the attacker with information on the state and the execution of the algorithm to extract secret key material. [5]Observing each single cache access event, however, is extremely hard when performing a local attack and even impossible for remote attacks. Hence in a time-driven cache attack, the adversary observes the aggregated effect of all the memory accesses in a cryptographic operation, i.e. the total number of cache misses and hits or at least its effect on the execution time of the operation. To infer key material, she then analyses cache collisions in a lookup table of interest. The main challenges [6] in the measurements of timings in the time-driven attacks are the increased level of noise (such as network latency and increased access time) and unpredictability of correlation of timings. Many cryptographic algorithms lack a proper defensive mechanism for cache based timing attacks. Therefore, the timing attacks can easily be implemented on any cryptosystem. For instance, libgcrypt (used in GNUTLS and GPG) and Cryptlib are not secure from the timing attacks. A defensive mechanism against the timing attacks is present in the OpenSSL 0.9.7 as an option. Nevertheless, this option is not enabled in common applications such as the Apache SSL module and mod SSL and therefore they are vulnerable to time-driven attacks.

Trace-driven side channel attacks : In these attacks, the attacker's process has the ability to capture a profile of the cache activity during the execution of the cryptographic algorithms. To launch this attack, the attackers need to access the profile in which they observe and extract the profile of the cache activity from other profile content.[7] A cache based power attack that exploits external collisions between different processes. Their attack requires 256 power traces to reveal the secret AES key. Lauradoux's power attack exploits the internal collisions inside the cipher but only considers the first round AES accesses and can reduce the exhaustive search space of a 128-bit AES key to 80 bits. We define a trace as a sequence of cache hits and misses. For example, MHHM, HMHM, MMHM, HHMH, MMMM, HHHH are examples of a trace of length 4. Here H and M represents a cache hit and miss respectively. The first one in the first example is a miss, second one is a hit, and so on. On tracing the pattern adversary can determine whether a particular access during an encryption is a hit or a miss. The trace of an encryption can be captured by the use of power consumption measurements. These attacks became powerful by the ability to continuously monitor the processor computation. Evict + Time attack, the cache is evicted before the encryption and then the cache access is investigated in term of a cache hit and cache miss. While in the Prime + Probe procedure, the cache is filled prior to encryption and after it has checked which cache line has or has not been accessed. The information can be further used to extract the encryption key. By using these attacks some features of the device are continuously monitored throughout the cryptographic operation, for example, a processor leaks information by analysing electromagnetic radiation [8].

Access-driven side channel attacks : Access driven side channel attacks provides logical access to the target computer system, An access-driven attack is a class of cache-based side channel analysis. Like the time-driven attack, the cache's timings are under inspection as a source of information leakage. Access-driven attacks scrutinize the cache behaviour with a finer granularity, rather than evaluating the overall execution time. Access-driven attacks leverage the ability to detect whether a cache line has been evicted, or not, as the primary mechanism for mounting an attack.Gullasch et al. [9] implemented a Flush + Reload SC attack that accessed specific memory lines in the AES memory by utilizing cache behaviour.

3. Countermeasures : The Countermeasures for Cache based side channel attacks are divided into Hardware-based , Software-based, Hypervisor-based.

3.1 Hardware-based countermeasure : The literature shows that cache-based SC attacks are mostly prevented by a hardware-based solution that mainly focuses on altering the replacement policies of cache [10].Though some of these solutions are effective

, existing processors are unable to employ this because they need a special support of hardware.[11] suggests avoiding memory accesses because attacks exploit the effect of memory access on the cache, and would thus be completely mitigated by an implementation that does not perform any table lookups. Instead of avoiding table lookup, one could employ them but ensure that the pattern of accesses to the memory is completely oblivious to the data passing through the algorithm.[12] suggested that instead of hidingaccess pattern dynamic table storage can be used.. In addition, the hardware-based solution proposed [13], included coming up with new designs for a shared cache. Hardware AES Support Several major vendors (including Intel, AMD, Sun, and Via) have recently announced or implemented specialized AES hardware support in their chips.

Assuming that the hardware executes the basic AES operation with constant resource consumption, this allows for efficient AES execution that is invulnerable to our attacks. However, these existing prevention mechanisms would require either modify the source code, altering the cryptographic algorithm, changing the hardware, e.g., changing cache design, or creating high computation cost in term of high overhead. Designing new caches will take longer time and during this time the SC attacks do a lot of damage. Therefore, there is a need for software-based prevention mechanisms for the quick mitigation of cache-based SC attacks.

3.2 Software-based countermeasure : Most of the existing prevention mechanisms for cache-based SC attacks are software-based and are associated to a specificcryptosystem. The basic phenomenon of this prevention mechanism is to edit the software in a new method that the SC attacks cannot be established.to prevent SC attacks on AES, many types of mechanisms have been proposed [14], such as The AES tables must be loaded into the cache prior to executing an encryption so that all accesses to AES create cache hit and hence have constant encryption time, During the AES execution, only mathematical operations should be used instead of table lookups. flushing the cache memory, cache partition using cache colouring and masking addresses, construct a new implementation of cryptographic algorithm that resists side-channel attacks,Limiting cache-based side-channel in multi-tenant cloud using dynamic page coloring. use dynamic software diversification to change the observable execution features while preservingsemantic of program and just changing the replica at the machine level instructionTo proposed CacheBar approach which automatically detects the concurrent access to shared pages and prevents them from evicting memory contents.

3.3 Hypervisor-based countermeasure : Hypervisor of a cloud system, does not interfere with the cloud's methods of operation. i.e cloud model (require no changes to the client-side code, nor to the underlying hardware) it is one of the preferred countermeasures for some cases. In terms of parallel side-channels, hypervisor can effectively prevent parallel cache-based side-channels while generating overhead that is highly dependent on the number of partitions needed. If fewer partitions are needed, the solution can run as fast, or possibly faster, than the insecure hypervisor. If more partitions are needed, then the solution will run with overhead up to 20-30 percent, though highly depending on workload.

4. CONCLUSION

While multi-tenancy has many benefits, clients co-residence and VMs physical co-residency arise security vulnerabilities to CC and enables a new form of sensitive information leakage known as SC attacks. Although there are many benefits to adopting CC, however, security is the most significant barrier. In this paper different hardware ,software, hypervisor based, specifically CPU cache-based SC attacks in the cloud environment and their countermeasures have been discussed. Several methods have been described by which the attacker can observe the memory pattern and access time variation of a cache of the victim process, e.g., one that executes encryption algorithm with an unknown private key. These methods are categorized into various type based on cache state.

In one method, the effect of the cache state is observed and then measure and analyses the consequence on the encryption algorithm running time, and in second methods the state of the cache is investigated after or during encryption. The second method is found to be noise-resistant and particularly effective. For 10 years it is a known problem in a virtualization environment. The most past attacks applied on the L1 cache which exploits the hyper threading or scheduler weaknesses. The existing last level cache attacks (L3) by using the prime probe and flush reload technique require memory deduplication and usage of huge pages. Some attacks do not have restrictions such as hyper-threading and memory sharing. There is a need for prevention mechanisms which is hypervisor-based and does not need any software by the client such as encryption algorithms or the changing of the underlying hardware. The hardware based solution is very expensive. Conversely, the software-based solutions need clients to change their software that does not comply with the cloud model. Therefore, a hypervisor-based software solution for these type of SC attacks including cache flushing, cache partitioning, and cache warming are required. However, during hypervisor-based solution, we have to keep in consideration the performance degradation of the system in term of CPU speed and load.

REFERENCES

[1] Qi Zhang, Lu Cheng, Raouf Boutaba, "Cloud computing: state-of-the-art and research challenges", J Internet ServAppl (2010) 1: 7–18.

[2]geeks for geeks, https ://www. Geeks for geeks .org/virtualization-cloud-computing -types/

[3]N.M Mosharaf Kabir "Network Virtualization: state of the art and research challenges" IEEE Communications Magazine, 2009 IEEE.

[4] Li Yan " Development and application of desktop virtualization technology" 2011 IEEE 3rd International Conference on Communication Software and Networks (ICCSN).
[5] Kris Tiri,Onur Acıı ̧cmez, Michael Neve, and Flemming Andersen, "Analytical Model for Time driven Cache attacks"https://iacr.org/archive/fse2007/45930404/45930404.pdf
[6] ShahidAnwar,ZakiraInayat,Mohamad FadliZolkipli,Jasni Mohamad Zain, Abdullah Gani, Nor Badrul Anuar, Muhammad Khurram Khan, Victor Chang ,"Cross-VM cache-based side channel attacks and proposed prevention mechanisms: A survey" Journal of Network and Computer Applications, Volume 93, 1 September 2017, Pages 259-279.
[7] Onur Acıçmez, Cetin Koc,"Trace driven cache attacks on AES" Conference: Information and Communications Security, 8th International Conference, ICICS 2006, Raleigh, NC, USA, December 4-7, 2006
[8]Karine Gandolfi,Christophe Mourtel, Francis Olivier,"Electromagnetic analysis: Concrete Results" Conference paper,First Online: 20 September 2001. https://link.springer.com/chapter/10.1007%2F3-540-44709-1_21
[9] David Gullasch and Endre Bangerter, "Advances on Access driven cache attacks" © Springer-Verlag Berlin Heidelberg 2007. https://ieeexplore .ieee. org/document/5958048/
[10] Percival large page performance,https://www.vmware.com/techpapers/2008/large-page-performance-1039.html
[11] Cache attacks and countermeasures ,https://link.springer.com/chapter/10.1007%2F11605805_1
[12] Efficient cache attacks on AES and countermeasures,https://link.springer.com/article/10.1007%2Fs00145-009-9049-y
[13] Zhang Y., Reiter M.K., 2013. Düppel: retrofitting commodity operating systems tomitigate cache side channels in the cloud. In: Proceedings of the 2013 ACM SIGSACConference on Computer & Communications Security. ACM. p. 827–838
[14] Micheal Godfrey,"Preventing cache based side channel attacks on cloud environment" IEEE Transactions on Cloud Computing (Volume: 2, Issue: 4, Oct.-Dec. 1 2014) https://ieeexplore.ieee.org/document/6899633/?part=undefined%7Csec5.3#sec5.3
[15] FangfeiLiu,YuvalYarom,Qian Ge, Gernot Heiser, Ruby B. Lee, "Last-Level Cache Side-Channel Attacks are Practical" 2015 IEEE Symposium on Security and Privacy, DOI 10.1109/SP.2015.43.