ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(43), DOI: 10.17485/ijst/2016/v9i43/104390, November 2016* ISSN (Online) : 0974-5645

A Review on Cloud Security Challenges and Issues

K.Balaji*[*] and P. Sai Kiran

Department of CSE,KL University, Vijayawada – 520001, Andhra Pradesh, India
balajikcse@gmail.com, psaikiran@kluniversity.in

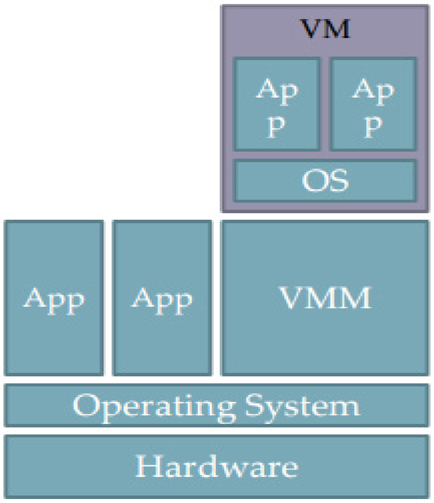
Abstract

Background/Objectives: Cloud computing offers various services with minimum management effort while provisioning resources via internet. Cloud clients are allowed to store their personal data at data centers, it will minimize storage maintenance in local systems**. Methods/Statistical Analysis:** Cloud computing environment facing huge issues with hardware and software vulnerabilities in maintenance and resources provisioning process. These vulnerabilities pose huge loss of data, confidentiality, privacy and availability. **Findings:** In this paper, we studied and concentrated on various attacks in Virtualization environment and the possible attack scenarios in each platform**. Application/Improvements:** In the final section, we studied and described all types of attacks.

Keywords: Confidentiality, Integrity, Privacy, Provisioning, Virtualization.

1. Introduction

Cloud computing has been defined by National Institute of Standards and Technology (NIST) as "a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction". Cloud computing integrates various technologies to provide effective and efficient services to the cloud clients[1]. The NIST cloud computing definition is most widely accepted. The NIST cloud computing model provides the three parts of cloud services such as (i) Essential characteristics (ii) Service models (iii) Deployment models. In this paper we concentrated on cloud virtual environment and its vulnerabilities. Virtualization is a promising technology which enable us to virtualize various resources in cloud environment. Virtualization provides an isolation environment, resource on-demand sharing among multiple users and scalability i.e., Content Security Policy (CSP) can increase or decrease Virtual Machine (VM's) in dynamic environment[3].



a) Para Virtualization

[*] *Author for correspondence*

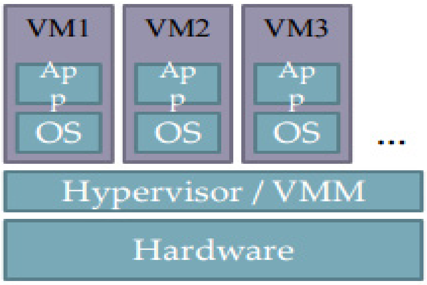


Figure 1.b) Full Virtualization

The full virtualization is a process of hosting guest operating system's on Virtual Machine Monitor (VMM) or hypervisor. Through hypervisor any guest VM can access the physical resources in cloud computing environment[2,4]. The VMM contains a special domain that acts as a root level or host operating system to control other operating system's ie. , domain's. Figure 1 a) gives a brief idea about the Para virtualization and it prevents users to execute some dangerous system calls on physical resources. This leads to prevention of denial of service attacks on physical resources. The full virtualization provides an infrastructure to run VM's with full access of physical resources in virtual environment. Figure 1 b) shows, virtualization technique provides a direct access to the physical resources so that it can execute any instruction without any involvement of host Operating System (OS). It leads to denial of service attacks on physical machine[5-7]. The benefits of virtualization are resource sharing, dynamic and scalability, cost effective, reduces power consumption, isolation and it helps CSP to manage resource in effective manner.

The paper organized as follows: section 2, gives the details of vulnerability in various hardware platforms that describes Trusted computing Failures in cloud environment and section 3 described about possible security vulnerability in software which is actually located at cloud infrastructure. In section 4, we described possible attacks while execution live migration of VM from one cloud environment and finally concluded about the paper in the conclusion.

2. Security Issues in Cloud Infrastructure

The entire state of the virtual machine is exposed to the device module or the hypervisor and if in case the attacker gains access of the hypervisor all the data of the virtual machine including the kernel states as well as the inputs from the keyboard will be compromised[8,9].

2.1Unauthorized Access to Hardware

A ring0 authorized domain or administrator gives a privileged access to lower level domains in the virtual environment in improper way. It leads to vulnerability of entire system and access granted system can directly utilize the hardware resources of host OS or hypervisor. It leads to a system failure and denial of service attacks. These attacks are entitled as "confused deputy attack"[10]. An example of this attacks are [CVE-2005-0204], [CVE-2007-5633] states that OS or hypervisor wrongly grants the access permissions to unauthorized domains in the virtual environment and provides an open access to hardware access such as Port I/O,MSR, etc[10].

2.2Hardware Reflected Injection Attack

A cloud user may store malicious data (worm, virus, etc) on store location of cloud service provider side. When it traverses from client to storage media it does nothing, later when it is accessed by higher privileged user it causes a vulnerability in data processing. It targets specific software on CSP side and performs malicious activities once it gets triggered. These attacks pose great risk to CSP such as data breach, data corruption and denial of service attacks. An example of these attacks is: [CVE-2010-4530].

2.3 Access by a Parallel Executing Entity

The cloud provider contains many platforms to make it characteristics to possible to client and resources are executed in parallel and/or independent manner. Some resources, like servers having a possibility of parallel execution with multiple core CPU's by using hardware assisted threads. A server shares features like memory, CPU, etc. In this regards, we are considering memory as a major component for implementing these attacks. Suppose client wants to execute or access memory location, CSP has to ensure that all other clients are passive for that memory location when legitimate client is trying to access. All other client usages are temporarily blocked by CSP to prevent illegal access of memory location. An attack [CVE-2005-0109] specifies how it is possible to access high privileged resources with least privileged clients on their locations using parallel execution of resources on cloud infrastructure. All the security codes, hardware failure, reasons & loses are mentioned in below Table 1.

Table 1. Hardware vulnerabilities

Code	Hardware failure	Reasons	Impact (10)	Loses
CVE-2007-5633	Confused Deputy	Assigning of root access rights to cloud client to pooled resources	7.8	Confidentiality, Integrity, Availability
CVE-2010-4530	Reflected Injection	Hardware failure that assigns root level access other clients	8.1	Integrity, Availability
CVE-2005-0109	Parallel execution threat	Unauthorized access of resource while blocking resource for specified client	9.8	Confidentiality, Integrity

3. Software Based Security Attacks

3.1 Allow User to Access Root Level

SVGAlib zgv 3.0 allows user gain root level access via a privileged leak of the iopl privileges to child process [CVE-1999-1482]. This allows cloud client to access root level resources without any barriers from security group. This attack leads to failure of complete confidentiality, integrity and availability. This attack doesn't require any authentication and access complexity is very low[11].

3.2 Denial of Service Attack

In Linux kernel 3.2.10 and earlier, the regset method doesn't manage .set and .get methods in case absence while communication with local system. This allows cloud user to launch a denial of service attacks. These two more methods pose unintended threats to linux machine: PTRACE_SETREGSET and PTRACE_GETREGSET. This attack impacts on confidentiality, integrity, access complexity and availability of data storage system and authentication is never required to exploit a vulnerabilities of system[12].

3.3. Xen Hypervisor Vulnerability

Xen hypervisor 4.1 has much vulnerability as specified in[10] and it has a lot of security aspects of a guest user (Domain U). When Domain U using PCI based pass-through on VT-d chipset that doesn't remains interrupts remapping technique, it leads guest OS users to gain privileges by raising Message Signalled Interrupts (MSIs) that leads to write interrupt injection registers. Once domain U obtains a privilege that provides an evidence of losing confidentiality, authentication and availability of other domain user data in cloud environment[13].

3.4. Sparc Hypervisor Vulnerability

A sun micro system's Sparc hypervisor firmware 6.6.3 to 7.1.3 on ultra-sparc processors T1 to T2+ system processors allows guest users to access the memory via unknown vectors with any need of authentication bypass on root level system. This attack leads to severe problem to cloud computing when it is configured with sparc hypervisor system. This attack makes the loss of data availability and confidentiality[14].

3.5. VMM Vulnerability

In Microsoft virtual machine server 2005 Release 2 SP1 doesn't maintain root level privileges for all host level machine instruction execution. This allows guest VM to execute malware code in kernel level and obtain other VM privileges within the virtual environment via special software like aka. This poses great issue to the entire virtual environment such data breaches, data loss, data confidentiality and privacy[15].Software vulnerabilities with different parameters are mentioned in Table 2.

Table 2. Software vulnerabilities

Code	Attack	Reasons	Impact(10)	Loses
CVE-1999-1482	SVGAlib	Allows cloud client to access root level resources without any barriers	7.4	Confidentiality, Integrity
CVE-2012-1097	Denial of service attack	Allows cloud user to launch a denial of service attacks	6.8	Integrity, Availability
CVE-2011-1898	Xen injection attack	MSI interrupts that leads to write interrupt injection registers	8.3	Confidentiality, Integrity, Availability
CVE-2008-4992	Sparc vulnerability	Authentication bypass on root level system	7.8	Integrity, Availability
CVE-2009-1542	VMM host access	obtain other VM privileges within the virtual environment	7.6	Confidentiality, Integrity

4. Possible Attacks on VM Migration

4.1Software vulnerabilities

An intruder can use several software vulnerabilities in VM migration like integer overflow, stack overflow and heap overflow to launch several attacks in migration code module. Possible platforms to implement an attack are Xen hypervisor and Oracle virtual box[16].

4.2. Replay Attack

While authenticating the cloud user, an authentication message contains authentication tokens those used for earlier communication and it sniffed by the intruder or attacker to launch a replay attack. These attacks can be mitigated through the nonce values in authentication messages and continues changing of message content. It takes an intruder to analyze message content from the original data format but random generation of nonce values provide more secure for replay attack. In cloud environment, cloud user and cloud service provider has authenticated the user before start the session and the session will be established by synchronizing with each other. It is highly difficult to implement timestamp concept in distributed cloud computing environment and it poses huge risk in terms of replay attacks. In live VM migration, control messages are sent in unprotected mode and attacker can access the credentials and reply to live migration process by sending its VM to actual or host OS. Possible platforms to implement an attack are Xen hypervisor and Micro soft Hyper-v[17].

4.3.Masquerading

A masquerader attack refers to a way to obtain legitimate credentials from actual user with fake identity. Detection of these attacks made by analyzing the masquerader activities on victim resource in cloud paradigm. After obtaining the credential of host OS, an attacker simply launch an attack on VM migration module to stop or suspend current migrating VM process and attacker VM acts like an original source of a system[18]. Possible platforms to implement an attack are Xen hypervisor and Oracle Virtual box[17].

5. Conclusion

Cloud computing provides an effective way of delivering services over an internet with various service models and different infrastructure resources those are configured and pooled. In this paper, we investigated and studied various practical attacks on cloud infrastructure with possible attack vectors. We identified hardware level and software level threats and possibility of attack nature in cloud infrastructure.

6. References

1. Abbas A, Khan SU A review on the state-of-the-art priva-

cy preserving approaches in e-health clouds IEEE Journal Biomedical Health Information. 2014 July; 18(4):1431–41.

2. Abbas A, Bilal K, Zhang L, Khan SU. A cloud based health insurance plan recommendation system: A user centered approach. Future Generation Computer Systems. 2015 Feb;43(44):99–109..
3. Agrawal R. Legal issues in cloud computing. IndicThreads, Conference on Cloud Computing, 2011.
4. Alhamazani K, Ranjan R, Mitra K, Rabhi F, Khan SU, Guabtni A, Bhatnagar V. An Overview of the Commercial Cloud Monitoring Tools: Research Dimensions, Design Issues, and State-of-the-Art. Computing. 2015 April; 97(4):357–77.
5. Ali M, Dhamotharan R, Khan E, Khan SU, Vasilakos AV, Li K, Zomaya AY. SeDaSC: secure data sharing in clouds. IEEE Systems Journal. 2015 Jan; PP(99):1–10.
6. Alowolodu OD, Alese BK, Adetunmbi AO, Adewale OS, Ogundele OS. Elliptic curve cryptography for securing cloud computing applications. International Journal Of Computer Applications. 2013 March; 66(23).
7. Anala MR, Shetty J, Shobha G. A framework for secure live migration of virtual machines. International Conference on Advances in Computing, Communications and Informations.IEEE;2013.
8. Andrieux A, Czajkowski K, Dan A, Keahey K, Ludwig H, Nakata T, Pruyne J, Rofrano J, Tuecke S, Xu M. Web services agreement specification (WSagreement). International Conference on Advances in Computing, Communications and Informatics. 2013, 243–8.
9. Aslam M, Gehrmann C, Bjorkman M. Security and trust preserving VM migrations in public clouds.11th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). IEEE; 2012. 869–76.
10. Balduzzi M, Zaddach J, Balzarotti D, Kirda E, Loureiro S. A security analysis of amazon's elastic compute cloud service. Proceedings of the 27th Annual ACM Symposium on Applied Computing. 2012 March; 1427–34.
11. CERT civis :http://cert.civis.net/index.php?action=alert&param=CVE-1999-1482
12. Gunasekhar T, Thirupathi Rao K, Trinath Basu M. Understanding insider attack problem and scope in cloudCircuit, Power and Computing Technologies. International Conference on Circuits, Power and Computing Technologies (ICCPCT).IEEE; 2015.
13. Gunasekhar T, Rao KT, Saikiran P, Lakshmi PS.A Survey on Denial of Service Attacks.
14. Gunasekhar T, Rao KT, Reddy VK, Kiran PS, Rao BT. Mitigation of Insider Attacks through Multi-Cloud. International Journal of Electrical and Computer Engineering. 2015 Feb; 5(1):136–41.
15. Durairaj M,Manimaran A. A Study on security issues in cloud based E-learning. Indian Journal of Science and Technology. 2015 April; 8(8): 757–65.
16. Sugumar R, Sheik Imam SB. Symmetric Encryption Algorithm to Secure Outsourced Data in Public Cloud Storage. Indian Journal of Science and Technology. 2015 Sep; 8(23).
17. Karthik K. et al. A Study on IP Network Recovery through Routing Protocols. Indonesian Journal of Electrical Engineering and Informatics (IJEEI). 2016; 4(3):176–80.
18. Sastry K, Narasimha B. Thirumala Rao, Gunasekhar T. Novel Approach for Control Data Theft Attack in Cloud Computing. International Journal of Electrical and Computer Engineering. 2015 Dec;5(6):1545–52.