THREAT MODELLING FOR THE VIRTUAL MACHINE IMAGE IN CLOUD COMPUTING

Raid Khalid Hussein and Vladimiro Sassone

Department of Electronics and Computer Science,
University of Southampton, Southampton, The UK

ABSTRACT

Cloud computing is one of the most smart technology in the era of computing as its capability to decrease the cost of data processing while increasing flexibility and scalability for computer processes. Security is one of the core concerns related to the cloud computing as it hinders the organizations to adopt this technology. Infrastructure as a service (IaaS) is one of the main services of cloud computing which uses virtualization to supply virtualized computing resources to its users through the internet. Virtual Machine Image is the key component in the cloud as it is used to run an instance. There are security issues related to the virtual machine image that need to be analysed as being an essential component related to the cloud computing. Some studies were conducted to provide countermeasure for the identify security threats. However, there is no study has attempted to synthesize security threats and corresponding vulnerabilities. In addition, these studies did not model and classified security threats to find their effect on the Virtual Machine Image. Therefore, this paper provides a threat modelling approach to identify threats that affect the virtual machine image. Furthermore, threat classification is carried out to each individual threat to find out their effects on the cloud computing. Potential attack was drawn to show how an adversary might exploit the weakness in the system to attack the Virtual Machine Image.

KEYWORDS

Cloud Security, Virtualization, Virtual Machine Image, Security Threats.

1. INTRODUCTION

Cloud computing is a paradigm that enable its users to access infrastructure, platform and software resources as services without owning, managing or maintaining the resources. Infrastructure as a service (IaaS) delivers hardware services to users' applications such as OpenStack, Amazon web services and google cloud platform using virtualization. IaaS provides and maintain a catalog that list the available virtual machines images (VMI). The VMI may include operating system like windows, Linux or Fedora and might contains other resources like applications that are created by organization such as database management system or application server[1]. There are some security issues associated with VMI in cloud computing that has harmful impact on the security of the cloud and might affect confidentiality, integrity or availability[2]. Threat modelling is conducted to identify security threats and draw possible routes threats might follow to attack the VMI. Furthermore, threat modelling distinguishes the area where the VMI is stored, classify threats based on their unwanted effect and detect the agent of the threats which is the objective of this paper.

Natarajan Meghanathan et al. (Eds) : CCSEA, CLOUD, SIPRO, AIFU, SEA, DKMP, NCOM - 2019
pp. 119-132, 2019. © CS & IT-CSCP 2019 DOI: 10.5121/csit.2019.90911

Threat modelling process involves three high-level steps: Firstly, characterizing the system which represents cloud computing platform that was used to achieve the threat modelling. Secondly identifying threats, which represent threats that identified in the academic literature related to VMI. Finally, identifying assets and access point that represent the area threat modelling was achieved in the cloud platform. The identified threats were classified based on their effect on security. STRIDE model is used to classify the identified threats developed by Microsoft for threat modelling [3]. Beside threat modelling, it is essential to take into consideration who is conducting the attack and what type of skills is needed to achieve the attack on the identified assets. Therefore, threat agent was identified for the context of VMI. Potential attacks was drawn to show the possible attacks that an adversary might follow to attack the VMI by exploiting the system vulnerabilities.

2. RELATED WORK

There are a number of studies were conducted to detect security threats and draw countermeasures to secure the VMI. An image management system (IMS) was designed to control the access to the VMI , track its provenance, provides image filters and scanners for both users and administrators to detect threats and repair security issues. The drawback of this system is that image filters for detecting and fixing security violation was not accurate 100% to remove private information like password or illegal software like pirated software from the image before publishing it. In addition, the virus scanner does not assure to detect all the malicious software in the image. This study identified unauthorized access, leak of sensitive information, malware and non-compliance as security threats that need to be considered[4].

Kazim, Masood and Shibli (2013) suggested Encrypted Virtual Disk Images in Cloud (EVDIC) to secure the VMI. Their idea was to encrypt the VMI whenever it is terminated to avoid security threats that might attack the VMI when it is dormant. EVDIC could provide security from malicious software or malwares. The proposed system EVDIC could identify compromised disk image, unauthorized access and data leakage as security threat.

Schwarzkopf et al. (2012) demonstrated a technique to detect outdated software in VMIs and to scan for security vulnerabilities. It includes two components: the Updates checker and online penetration suite. The Update checker is used to find out Linux based virtual machine who in need of update their software. The update checker copy the information about installed packages and save them in the database. The checks for software updates is achieve faster compare to other techniques as installed package is saved in databased whereas, in other systems need to boot the VMI and shut it down after checking for software updates which is time consuming. On the other hand, online penetration suite is used to perform periodic or pre-rollout online scanning of virtual machine for software vulnerabilities. The periodic scan can be achieved in idle times

whereas the pre-rollout online scanning is accomplished before the machine goes live. The scans for software vulnerabilities is accomplished using well know security products. The drawback in this system is the update checker works with Linux only. This study could identify non-compliance as security threats [6].

An Offline Patching Scheme (OPS) could figure out a method to identify VMI with outdated software and patch VMI with latest software update efficiently therefore, it could solve the non-compliance issue. OPS based on two modules, the Collector and Patcher. Collector is used to find

out outdated software in the VMI. Patcher is used to patch the outdated software in the VMI with the latest updates and patches. However, the study has limitation to patch outdated VMI with Window OS. In addition, the system is unwilling to updates snapshots. OPS could identify data leakage and malware as security threats [7].

Another study by Jeswani et al. (2013) which could present ImageElves to detect out-dated software within VMI and patch, install software and check for compliance. This system works in two phases. The first phase is to investigate the target VMI and creates manifest and signature updates. In the second phase, VMIs are taken offline and apply the manifest. This system has advances over other related work as reduce the downtimes due to simultaneously apply the updates to all dormant images. The drawback in this system there might be failed for the higher level applications to function correctly after applying the updates. Furthermore, applying upgrade to VMI files work properly for binary files except there are possibilities to create more equivalent classes than it is necessary. Finally, there is no failure recovery capabilities for the current implementation of Image Elves in case of the system running. This study could figure out non-compliance as security threat[8].

3. THREAT MODELLING

Threat modelling is a procedure used to identify and address security threats associated with different assets in the system. Threat modelling is used to locate security threats and identify mechanisms to protect the cloud services. Threat modelling is used to study the cloud service and classified the potential threats based on their effect on the cloud. To identify security requirements for the cloud services, threats need to be analysed based on criticality and likelihood. Decisions need to be taken regarding the potential threats related to the cloud services, specifically whether to mitigate the threats or accept the risk associated with the threats. Security of the cloud services was built based on threat modelling and security requirements. Identifying the threats associated with assets in the system helps to develop proper security requirements.

This is essential in case the security requirements are damaged; indeed, this could lead to faults in the security system related to the cloud service. Properly addressing the threats and suitable countermeasures to said threats reduces the ability of the attacker to misuse the cloud service. Threat modelling looks at the cloud services from the attacker

perspective to help the designers to predict the attacker goals or which assets are targeted [9] The threat modelling process consists of the following high-level steps, as shown in Figure 1.

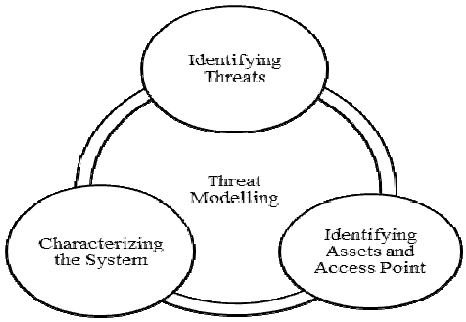

Figure 1 Threat Modelling

3.1 Characterizing the System

With regard to the scenario of OpenStack, which is one of the most popular open source cloud services, it includes the following components: Nova for computing, Glance for image services, Cinder for block storage, Neutron for networking, Keystone for identity services, Swift for object storage and Dashboard to access the cloud services. As shown in Figure 2, the physical network provides access to cloud administrators and cloud users. Firewalls are used to connect cloud administrators to the data centre, as shown in node 17 and node 19. In addition, the cloud administrators are connected to the data centre through an authentication server (host 18) and Nexus 7000 (node 20). The cloud users are connected to the data centre through the multi-layer concept used by Cisco. There are three layers where the cloud users are connected to the data centre. These layers are as follows [10]:

- In Layer 1, node 1 is used to establish connection between the cloud and the internet. Node 2 is used to link the user to the firewall. At the same time, the user, after being connected to the firewall, is connected to two different types of servers: the authentication server (host 3) as well as the DSN and Neutron server (node 4). These servers provide services to end-users and tenants. Following this, node 5, which is Cisco Nexen 7000, is used to route the request to the destination machines.

- In Layer 2, node 6 is a firewall which is used to connect the first layer to the second layer through Nexus 5000 node 7. Nexus 5000 is used to connect the rack server through Nexus 2000. Nexus 5000 is employed to connect servers inside the rack at compute level (hosts 8, 9, 10, 11 and 12).

- In Layer 3, another Nexen 7000 node 13 is used to connect layer 2 to the storage. Node 14 is a firewall which is used to connect Nexus 7000 and MDS 9000.

OpenStack components run on the authentication server in host 3 and host 18. Host 3 is designed for tenants and host 18 is designed for the administrators. In the first run the following components are working: Dashboard, Nova, Neutron, Keystone, Cinder, Swift, Glance and My SQL. In the second run, the same components along with additional components like billing system, which is known as Ceilometer. Node 4 represents the DNS server, which runs the Neutron components; this server provides the address for the machine running a requested service. The Nova is represented by nodes 8, 9, 10, 11 and 12. All physical components run four components: Hypervisor, Nova, Glance and Ceilometer. Finally, all physical machines run ssh for maintenance [11].

3.2 Identifying Threats

In the cloud data centre, as shown in Figure 2, attacks surface represent points when exploited by an attacker could leak information. Attacks surface can be classified into three types; the first attacks surface comes from physical network, which includes the hardware and software components such as servers or OS. The second type of attacks surface which are related to virtualization, such as an attack on hypervisor or virtual switches. The last type of attack surface is related to cloud computing, such as OpenStack components having security issues, e.g. Glance, Neutron, Nova, Ceilometer and keystone. It is obvious that the first attack surface is similar to

those related to the traditional network. On the other hand, attacks surface on the cloud OS and virtualization may also pose new security challenges, as they are unique to the cloud [12].

Attacks surface may come from two sides: attacks from the user side and attacks from the provider side. Let us consider an attack conducted by a user. There are two types of users: first is the normal user who is using the cloud service with the intention of attacking the service of the cloud tenant and its users or cloud providers. Second is a cloud tenant, who aims to attack another cloud tenant and his/her users or cloud provider.

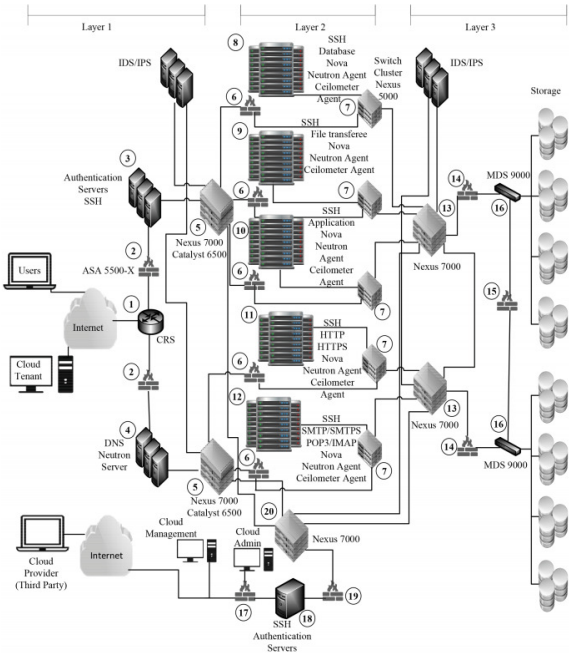

Figure 2 Cloud Data Center Infrastructure [11]

On the other hand, the Cloud provider could conduct another attack on the cloud. Cloud provider refers to the operator, who has privileged access to certain cloud components for maintenance or management, such as routers, switches or firewalls. The Cloud provider could exploit any of the aforementioned types of attacks to leak out information [11].

There are five threats related to the VMI which have been identified in the academic literature related to VMI: malware, data leakage, unauthorized access, compromised disk image and risk of non-compliance [7–11].

- Data leakage represents the intentional or unintentional leaking of sensitive information. This occurs when a user publishes his/her image without removing personal information. Sensitive information could include, for instance, cookies from the internet that can make it possible to extract sensitive information related to the image user.

- Malware are malicious software or virus that is situated inside the memory of VMI. Malware could affect the security of the VMI and might cause serious security issues for

the cloud. The malicious VMI, which includes malware, helps the attacker to bypass the security countermeasures, such as the firewall or the intrusion detection system.

- Unauthorized access is an illegal access to a service without permission. These users could bypass the security mechanisms or use illegitimate accounts to access the VMI and threaten the confidentiality, availability and integrity of the VMI.

- Compromised disk image could be disclosed during the storage stage due to someone installing malicious software on the VMI or someone gaining unauthorized access to the VMI. The disk image is vulnerable to outside attackers, and could also be susceptible to inside attacks such as malicious users or administrators.

- Non-compliance represents storing in a repository, retrieving from a repository or running VMI with expired software or unlicensed Software. This could happen when a dormant image is not patched with the latest software updates or is not scanned for worms or malicious software. Expired software represents software with an expired license and will be detected when the image is active.

3.3 Identifying Assets and Access Point

The identified asset for this research is the VMI. As this research is accomplished on OpenStack, the Glance project is used to save and maintain the VMI in the cloud service. In addition, access points in the scenario of the VMI are achieved through the Glance project, the Nova project and Cinder in OpenStack. The VMI is copied from the Glance project to the local disk inside the compute/Nova project for the purpose of lunching an instance from the VMI. In addition, a flavour needs to be selected as well as additional attributes for the launching of the VM. Flavour represents a set of virtual resources. Flavour identifies the CPU number, RAM amount available and disk size. There are predefined flavours, thus allowing the user to choose the suitable option for their requested instance. The selected flavour provides root volume, which is labelled vda in Figure 3, as well as an additional storage, labelled vdb. Vdb will be deleted once the instance is deleted, as it is an ephemeral disk. Vdc is the virtual disk, which is connected to cinder volume.

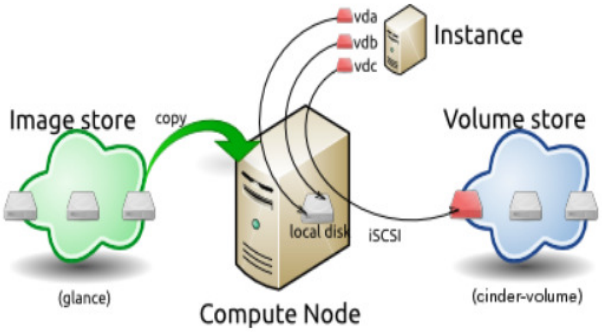

Figure 3 Instance Creation from an Image [13]

Cinder volume is a persistent block storage service provided by OpenStack and can replace the ephemeral storage provided by the instance flavour vdb. The compute project is connected to the

cinder volume through iSCSI. Once the compute node starts to provision the vCPU and memory resources, the instance boots up from the vda (OpenStack, 2018; CVE Details, 2016).

4. THREATS CLASSIFICATION

The identified threats are classified into six types based on their effects. This is achieved using the STRIDE classification model as shown in Figure 4. STRIDE classification can be broken down as follows [18]:

- Spoofing: happens when unauthorised users use the credentials of an authorised user or legitimate user with malicious behaviour trying to gain access to inaccessible assets.

- Tampering: refers to changing the data or operation to perform an attack. Users can change the data or operation which is delivered to them and return said data, therefore manipulating client-side validation.

- Repudiation: pertains to a situation whereby the user could deny his/her activity when there is no sufficient monitoring or recording of his/her activity while he/she is working on the system.

- Information disclosure: occurs when information is exposed to unauthorised users who do not have right to access it.

- Denial of service: a legitimate user is not willing to access a certain service because of malicious software, a lack of internet, or power failure.

- Elevation of privilege: unauthorized users or attacker can elevate their role to a higher privileged role in the information system.

Based on the definition of the identified threats in previous section and the above threats classification, threats are mapped to its equivalent in STRIDE classification model. Data leakage, data breaches or data lost is mapped to information disclosure and tampering as it affects data integrity and confidentiality[19].

Malware is one of security threat that is used by an adversary to attack the VMI through spoofing as the adversary can hide his identity and send malware to victim therefore, malware is linked to spoofing category in STRIDE classification model [20]. In addition, tampering threatens the data integrity or operation flow. The adversary exploits being an authorized user to attachment malware in the system therefore, malware is classified as tampering in STRIDE classification model [21]. Furthermore, Malware might cause denial of service as the service is flooded by requests to initialize instances [22]. Information disclosure is another cause of malware as it is an effect of illegitimate user who exposes data [23].

Unauthorized access is another security threats to the VMI. Spoofing is a method which can be exploited by attacker to perform unauthorized access to the VMI as spoofing permits attackers to hide their identity from the security mechanism and gain unlawful access to the VMI [24]. In addition, information disclosure might be caused by unauthorized access to the VMI from an adversary which exposes data to unauthorized access and affects data confidentiality [25].

Moreover, unauthorized access is mapped to elevation of privilege as an attacker changes the users membership or their privileges [26].

Compromised disk image is a security problem that affects the VMI which is caused by tampering with data [27] or information disclosure[28].

Non-compliance is a security issue for the VMI and needs to be considered. Non-compliance is mapped to Elevation of privilege in the STRIDE threats classification as if the VMI is not updated with latest policies or software updates which might lead to bypass authorization of the system [26].

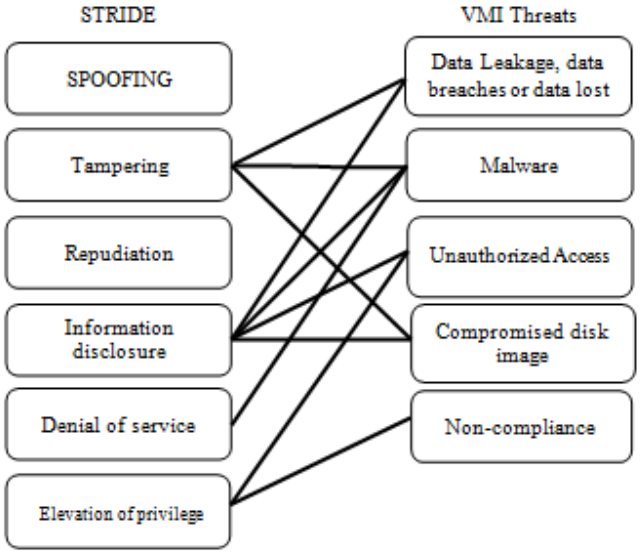

Figure 4 STRIDE Classification for the VMI threats

5. POTENTIAL ATTACK SCENARIOS FOR VMI

There are a number of vulnerabilities in the Glance project, Cinder project and Nova project in OpenStack which could be exploited by an adversary to attack VMIs. Attacks might come from:

- An adversary who has access to the Glance project, which is located in node 3 and node 18. The Glance project represents an entry point. Nova initializes an instance after copying a VMI to the Nova local disk. A malicious user can exploit one of the vulnerabilities, namely CVE-2016-7498 (OpenStack: List of all products and related security vulnerabilities) in Nova; these vulnerabilities are located in nodes 8, 9,10, 11 and 12 and perform an attack. Nova project represents here exit point to leak of information.
- An adversary could exploit one of vulnerabilities, namelyCVE-2015-5162, CVE-2014-7231, CVE-2014-7230, CVE-2014-3641 or CVE-2013-4183 (OpenStack : List of all products and related security vulnerabilities) in the Cinder project; these vulnerabilities are located in node 3 and 18. Exploiting said vulnerabilities would make it possible to perform an attack, as the Cinder volume is used by the Nova project to run an instance. In this case, the Nova or Cinder projects represent an exit point for information disclosure.

- Another possible attack could happen when the cloud tenant uploads the VMI, alongside malicious software, to the Glance project, which is located in node 3 or 18, in order to implement an attack. An infected VMI might have security implications for the security of the cloud and represents an entry point. The malicious cloud tenant could exploit one of the vulnerabilities, namely CVE-2017-7200, CVE-2015-8234, CVE-2015-5163, CVE-2015-3289 or CVE-2013-1840 (OpenStack : List of all products and related security vulnerabilities) in the Glance project to achieve an attack and threaten the security of the cloud; the Glance project therefore represents an exit point.
- The cloud provider can achieve all types of attacks on the VMI as he/she has privileged access to resources in the area between the Glance, Nova and Cinder projects, and can harm the cloud security.

TABLE 1 shows the severity of the vulnerabilities related to Nova, Cinder and Glance projects based on Common Vulnerability Scoring System (CVSS) [30]. In CVSS, the higher score shows the greater probability that the vulnerability could be exploited by an adversary. The 0 score represent the weak or no chance to conduct an attack whereas, 9.0 or 10.0 is very critical risk and can be exploited by an adversary to perform an attack.

Table 1 Nova, Cinder and Glance projects vulnerabilities with CVSS score

CVE number	**NONE**	**LOW**	**MEDIUM**	**HIGH**	**CRITICAL**
	0.0	0.1 - 3.9	4.0 - 6.9	7.0 - 8.9	9.0 - 10.0
Nova project vulnerability cvss score					
CVE-2016-7498	-	-	√	-	-
Cinder project vulnerability cvss score					
CVE-2015-5162	-	-	√	-	-
CVE-2014-7231	-	√	-	-	-
CVE-2014-7230	-	√	-	-	-
CVE-2014-3641	-	-	√	-	-
CVE-2013-4183	-	√	-	-	-
Glance project vulnerability cvss score					
CVE-2017-7200	-	-	√	-	-
CVE-2015-8234	-	-	√	-	-
CVE-2015-5163	-	√	-	-	-
CVE-2015-3289	-	-	√	-	-
CVE-2013-1840	-	√	-	-	-

6. THREAT AGENT

Threat agent is the player who force a threat on the system. It is trying to expose the integrity and confidentiality of the information saved in the system. Threat gent is an act that is made intentionally or unintentionally to destroy the system. Threats agents could be result of the following [31]:

- Natural disaster which comprises fire, flood, lighting or earthquake.
- Terrorists are kinds of threat agents which includes political terrorists, religious terrorists or anarchists.

- Competitors and organized crime that arise from commercial competitors who compete for resources such as a challenger trying to acquire a device firmware to harm its competitor's reputation.
- Thieves are threat agents who are associated with stealing mostly financial or personal data.
- Hackers cloud be group of malicious individual, employees of an organization who may be disgruntled or script kiddies. Hackers tend to use applications and tools that are developed by others such as viruses, worms or phishing.

There are two essential skills which help attackers to achieve an attack: reconnaissance skills and arsenal size. The reconnaissance skills represents the ability of an attacker to synthase accurate information regarding the target system. High reconnaissance skills expend the likelihood that will acquire enough information regards the target system while low reconnaissance skills illustrate that the attacker has no sufficient information to perform successful attack. Arsenal size represents the number of usable exploits at attacker's disposal. The strength of an attacker is evaluated by their ability to acquire or develop a large arsenal of obtainable exploits and reconnaissance skills which help to make a successful attack [32].

In the scenario of VMI, the attacker has sufficient information about OpenStack system. The attacker has a clear idea about where VMI is saved, where an instance is initialized which represent reconnaissance skills. Whereas, vulnerabilities that could be exploited to perform an attack in the projects of Cinder, Nova and Glance projects represents arsenal size. An attacker needs to have certain skills to exploit one of the vulnerabilities in Cinder, Nova or Glance project to perform the attack on the VMI.

To exploit the vulnerability in Nova project:

- The vulnerability namely CVE-2016-7498 (OpenStack: List of all products and related security vulnerabilities) required from the attacker to be logging on the OpenStack project as a legitimate user through command line or via desktop session or web interface. This vulnerability has very low access complexity to be exploited. In this vulnerability, the attacker exploit it to delete the instance while it is in resize state and cause denial of service.

To exploit the vulnerabilities in Cinder project:

- The vulnerability namely CVE-2015-5162, it is required from the attacker to create and upload a crafted disk image with malicious software to cause denial of service. This vulnerability occurs because image parser does not limit the qemu image calls.
- Another vulnerability in Cinder CVE-2014-7231 causes information disclosure when exploited. It is important that the attacker needs to be local user in order to read the log file to obtain the password related to in strutils.mask_password function and can leak information.
- For vulnerability CVE-2014-7230 required the same skills needed in the vulnerability CVE-2014-7231 but, to obtain the password to read the log is acquired from processutils.execute function. This vulnerability causes information disclosure.
- The vulnerability CVE-2014-3641 required form the attacker to be logged to the system through desktop session, command line or web interface. This vulnerability does not require sophisticated knowledge to be exploited. The attacker needs to be remotely

authenticated to obtain data from cinder volume by cloning and attaching the volume to the header of crafted qcow2 header.

- In CVE-2013-4183, the attacker requires to be a local user to obtain sensitive information from snapshot of the VMI. This vulnerability leaks information from clear_volume function in LVM Volume Driver in OpenStack Cinder as it does not clear data properly when deleting the snapshots.

To exploit the vulnerabilities in Glance project:

- The vulnerability CVE-2017-7200, masked network port scan is performed by an attacker using the image Service API v1. It is possible for an attacker to create an image with URL using the v1. The internal network could be monitored by an attacker while appearing masked.
- The vulnerability CVE-2015-8234, it is required from remote authenticated attacker to create a crafted image to bypass the signature verification process in order to attack MD5.
- To exploit the vulnerability CVE-2015-5163, it is required from an attacker to be authenticated as local user to read an arbitrary files through crafted backing file for the qcow2 image to leak information.
- Another vulnerability in Glance project CVE-2015-3289 permits an adversary to cause denial of service through continuously using import task flow API to create images and delete them.
- The vulnerability CVE-2013-1840 in Glance project allows a remote authentication attacker to obtain the operator's backend credentials via request for a cache image.

Table 2 shows the required skills to exploit a certain vulnerability.

Table 2 Skills required by an attacker to exploit a vulnerability and Vulnerability Type

CVE number	**OpenStack Project**	**Skills to attack the vulnerability**	**Vulnerability Type**
CVE-2016-7498	Nova	login as authenticated user	denial of service
CVE-2015-5162	Cinder	create and upload crafted disk image	denial of service
CVE-2014-7231	Cinder	login as authenticated user to read log files	information disclosure
CVE-2014-7230	Cinder	login as authenticated user to obtain password	information disclosure
CVE-2014-3641	Cinder	access through desktop session, command line and web interface	information disclosure
CVE-2013-4183	Cinder	remotely authenticated	information disclosure
CVE-2017-7200	Glance	perfume mask network scan	information disclosure
CVE-2015-8234	Glance	created crafted image	bypass restriction
CVE-2015-5163	Glance	login as authenticated user	information disclosure
CVE-2015-3289	Glance	login as authenticated user	denial of service
CVE-2013-1840	Glance	remotely authenticated	information disclosure

7. DISCUSSION

In the literature review, five security threats have been identified and they are: malware, data leakage, unauthorized access, compromised disk image and risk of non-compliance that threatens the security of VMI. The identified threats was classified using STRIDE classification model as shown in Figure 4. The results of threats classification show that information disclosure is the most possible type that might occur as many security threats related to VMI lead to it. In addition, the identified vulnerabilities related to Nova, Glance and Cinder projects in OpenStack as shown in TABLE 2, it is obvious most of vulnerabilities when exploited by an adversary lead to information disclosure therefore, the threats that lead to information disclosure and the corresponding vulnerabilities need special attention to provide security for the VMI.

8. CONCLUSION

Threats modelling is the key element to identify security threats related to assets in the system. Threat modelling is used to identify security threats related to the VMI in cloud computing. The identified threats was classified to its threat type to study the effect of each individual threat that might cause when an attack happen on the VMI. Potential attack scenarios were drawn based on the vulnerabilities found in projects where the VMI store and launch with the skills required from the attacker to perform an attack. In light of the threat classification, the attack scenario and the vulnerabilities related to Glance, Nova and Cinder, it can be seen that most of the vulnerabilities when exploited by an attacker cloud result in information disclosure which needs to be considered.

REFERENCES

[1] R. K. Hussein, A. Alenezi, H. F. Atlam, M. Q. Mohammed, R. J. Walters, and G. B. Wills, “Toward Confirming a Framework for Securing the Virtual Machine Image in Cloud Computing,” Adv. Sci. Technol. Eng. Syst. J., vol. 2, no. 4, pp. 44–50, 2017.

[2] R. K. Hussein, A. Alenezi, G. B. Wills, and R. J. Walters, “A Framework to Secure the Virtual Machine Image in Cloud Computing,” Proc. - 2016 IEEE Int. Conf. Smart Cloud, SmartCloud 2016, no. November, pp. 35–40, 2016.

[3] D. R. Thompson and C. W. Thompson, “Rfid security threat model,” no. May, 2014.

[4] J. Wei, X. Zhang, G. Ammons, V. Bala, and P. Ning, “Managing security of virtual machine images in a cloud environment,” Proc. 2009 ACM Work. Cloud Comput. Secur. - CCSW ’09, no. Vm, p. 91, 2009.

[5] M. Kazim, R. Masood, and M. A. Shibli, “Securing the virtual machine images in Cloud computing,” SIN 2013 - Proc. 6th Int. Conf. Secur. Inf. Networks, pp. 425–428, 2013.

[6] R. Schwarzkopf, M. Schmidt, C. Strack, S. Martin, and B. Freisleben, “Increasing virtual machine security in cloud environments,” J. Cloud Comput. Adv. Syst. Appl., vol. 1, no. 1, p. 12, 2012.

[7] K. Fan, D. Mao, Z. Lu, and J. Wu, “OPS: Offline patching scheme for the images management in a secure cloud environment,” Proc. - IEEE 10th Int. Conf. Serv. Comput. SCC 2013, pp. 587–594, 2013.

[8] D. Jeswani, A. Verma, P. Jayachandran, and K. Bhattacharya, "ImageElves: Rapid and reliable system updates in the cloud," Proc. - Int. Conf. Distrib. Comput. Syst., no. i, pp. 390–399, 2013.

[9] M. Kazim and D. Evans, "Threat modeling for services in cloud," Proc. - 2016 IEEE Symp. Serv. Syst. Eng. SOSE 2016, pp. 84–90, 2016.

[10] K. Bakshi, "Cisco Cloud Computing - Data Center Strategy , Architecture , and Solutions Point of View White Paper," Solutions, pp. 1–16, 2009.

[11] N. Alhebaishi, L. Wang, S. Jajodia, and A. Singhal, "Threat Modeling for Cloud Data Center Infrastructures," Springer, Cham, 2017, pp. 302–319.

[12] A. Alhebaishi, N., Wang, L., Jajodia, S. and Singhal, Threat Modeling for Cloud Data Center Infrastructures. 2017.

[13] R. Schwarzkopf, M. Schmidt, C. Strack, S. Martin, and B. Freisleben, "Increasing virtual machine security in cloud environments," pp. 1–12, 2012.

[14] K. Fan, D. Mao, Z. H. Lu, and J. Wu, "OPS: Offline patching scheme for the images management in a secure cloud environment," Proc. - IEEE 10th Int. Conf. Serv. Comput. SCC 2013, pp. 587–594, 2013.

[15] M. Kazim, R. Masood, and M. A. Shibli, "Securing the virtual machine images in cloud computing," Proc. 6th Int. Conf. Secur. Inf. Networks - SIN '13, no. April 2015, pp. 425–428, 2013.

[16] Openstack, "Images and instances," 2018. [Online]. Available: https://docs.openstack.org/glance/pike/admin/troubleshooting.html. [Accessed: 04-May-2018].

[17] CVE Details, "CVE-2016-7498," 2016. [Online]. Available: https://www.cvedetails.com/cve/CVE-2016-7498/. [Accessed: 18-Jun-2018].

[18] D. Thompson, "RFID security threat model," Conf. Appl. …, no. October, 2006.

[19] Cloud Security Alliance, "The Notorious Nine. Cloud Computing Top Threats in 2013," Security, no. February, pp. 1–14, 2013.

[20] A. Herzberg, "Protecting web users from phishing, spoofing and malware," 2006.

[21] A. Dehghantanha, A. Shaame, and K. Shanmugam, "An Educational Framework for Free and Open Source Software," Ijimt.Org, vol. 4, no. 1, 2013.

[22] F. C. Freiling, T. Holz, and G. Wicherski, "Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 3679 LNCS, pp. 319–335, 2005.

[23] M. Johnson and S. Dynes, "Inadvertent Disclosure-Information Leaks in the Extended Enterprise.," Weis, no. 2003, pp. 1–23, 2007.

[24] S. A. C. Schuckers and D. Ph, "Spoofing and Anti-Spoofing Measures," vol. 7, no. 4, pp. 56–62, 2002.

[25] Y. S. Shiu, S. Y. Chang, H. C. Wu, S. C. H. Huang, and H. H. Chen, "Physical layer security in wireless networks: A tutorial," IEEE Wirel. Commun., vol. 18, no. 2, pp. 66–74, 2011.

[26] G. Peterson, “From auditor-centric to architecture-centric: SDLC for PCI DSS,” Inf. Secur. Tech. Rep., vol. 15, no. 4, pp. 150–153, 2010.

[27] S. M. Specht and R. B. Lee, “Distributed Denial of Service: Taxonomies of Attacks, Tools and Countermeasures,” Proc. 17th Int. Conf. Parallel Distrib. Comput. Syst. 2004 Int. Work. Secur. Parallel Distrib. Syst., no. September, pp. 543–550, 2004.

[28] K. Woods, C. A. Lee, and S. Garfinkel, “Extending digital repository architectures to support disk image preservation and access,” Proceeding 11th Annu. Int. ACM/IEEE Jt. Conf. Digit. Libr. - JCDL ’11, p. 57, 2011.

[29] Virginia Braun & Victoria Clarke, “Openstack : List of all products and related security vulnerabilities.” [Online]. Available: https://www.cvedetails.com/product-list/vendor_id-11727/Openstack.html. [Accessed: 21-Jun-2018].

[30] First improving security together, “Common Vulnerability Scoring System v3 . 0 Examples,” no. July, pp. 1–38, 2016.

[31] S. Vidalis and A. Jones, “Analyzing Threat Agents and Their Attributes.,” Eciw, no. June 2014, pp. 1–15, 2005.

[32] N. Ben-Asher, J. Morris-King, B. Thompson, and W. J. Glodek, “Attacker skill defender strategies and the effectiveness of migration-based moving target defense in cyber systems,” 11th Int. Conf. Cyber Warf. Secur. ICCWS2016, no. March, p. 21, 2016.

AUTHORS

Raid Khalid Hussein, PhD candidate University of Southampton His research interest cyber security, cloud computing, Cloud forensic, access control and internet of things.

Prof Vladimiro Sassone, Cyber Security, Head of group, Professorial Strategy Committee and Strategy Committee. University of Southampton. His research interest are in cyber security spanning over trust, anonymity, cyber control, privacy and security of Cloud industrial control systems and internet of things.