Secure Virtualization for Cloud Environment Using Hypervisor-based Technology

Farzad Sabahi, *Member, IEEE*

***Abstract*—Cloud computing is one of today's most exciting technologies, because it can reduce the cost and complexity of applications, and it is flexible and scalable. These benefits changed cloud computing from a dreamy idea into one of the fastest growing technologies today. Actually, virtualization technology is built on virtualization technology which is an old technology and has had security issues that must be addressed before cloud technology is affected by them. In addition, the virtualization technology has limit security capabilities in order to secure wide area environment such as the cloud. Therefore, the development of a robust security system requires changes in traditional virtualization architecture. This paper proposes new security architecture in a hypervisor-based virtualization technology in order to secure the cloud environment.**

***Index Terms*—Virtualization, cloud computing, architecture, security, hypervisor.**

I. Introduction

Cloud computing is a network-based environment that focuses on sharing computations and resources. Actually, cloud computing is defined as a pool of virtualized computer resources. Generally, Cloud providers use virtualization technologies combined with self-service abilities for computing resources via network infrastructures, especially the Internet and multiple virtual machines are hosted on the same physical server. Based on virtualization, the cloud computing paradigm allows workloads to be deployed and scaled-out quickly through the rapid provisioning of Virtual Machines or physical machines. A cloud computing platform supports redundant, self-recovering, highly scalable programming models that allow workloads to recover from many inevitable hardware/software failures. Therefore, in clouds, costumers only pay for what they use and do not pay for local resources, such as storage or infrastructure. A virtual appliance relieves some of the notable management issues because most of the maintenance, software updates, configuration and other management tasks are automated and centralized at the data center by the cloud provider responsible for them. Because virtualization is not a new technology and it has not enough security capabilities for wide network such as cloud.

This paper is organized as following. Section 2 describes the cloud computing and virtualization technology. Section 3 introduces virtualization approaches. Section 4 describes relation between security and reliability in virtual environments. Sections 5 to 8 introduce issues and attacks in security and reliability of virtualization. Section 9 presents a novel approach in order to secure virtualization technology for cloud computing. Finally, Section 10 presents the conclusions.

Manuscript received November 24, 2011, revised January 8, 2012.

F. Sabahi is with the Azad University, Zanjan, Iran (email: f.sabahi@ieee.org).

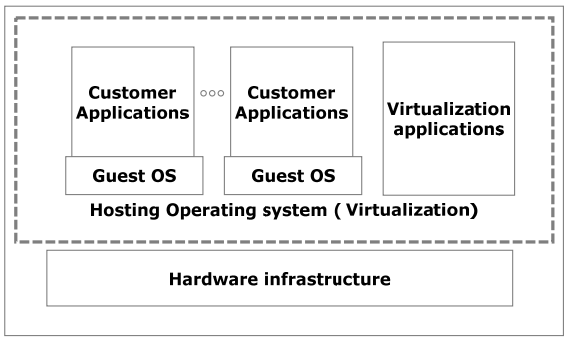
II. Virtualization Components

Virtualization is one of most important elements that makes cloud computing. Virtualization is a technology to helping IT organizations optimize their application performance in a cost-effective manner, but it can also present its share of application delivery challenges that cause some security difficulties. Most of the current interest in virtualization revolves around virtual servers in part because virtualizing servers can result in significant cost savings. The phrase virtual machine refers to a software computer that, like a physical computer, runs an operating system and applications. An operating system on a virtual machine is called a guest operating system. In addition, there is a management layer called a virtual machine monitor or manager (VMM) that creates and controls the all virtual machines' in virtual environment.

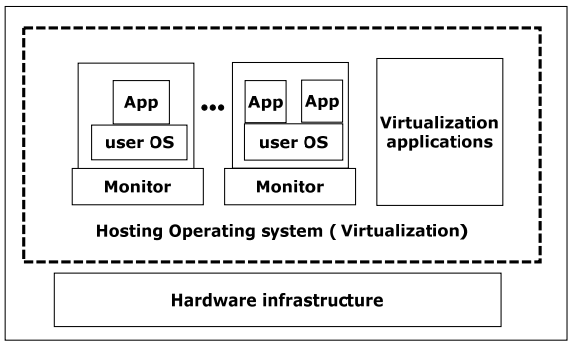
A hypervisor is one of many virtualization techniques which allow multiple operating systems, termed guests, to run concurrently on a host computer, a feature called hardware virtualization. It is so named because it is conceptually one level higher than a supervisor. The hypervisor presents to the guest operating systems a virtual operating platform and monitors the execution of the guest OS (guest operating systems). Multiple instances of a variety of operating systems may share the virtualized hardware resources. Hypervisor is installed on server hardware whose only task is to run guest operating systems.

III. Virtualization Approaches

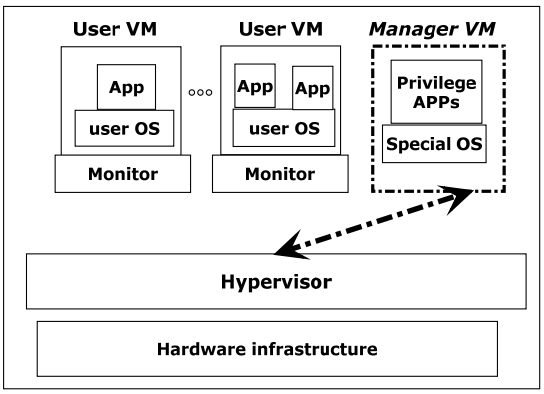
In a traditional environment consisting of physical servers connected by a physical switch, IT organizations can get detailed management information about the traffic that goes between the servers from that switch. Unfortunately, that level of information management is not typically provided from a virtual switch. Basically, the virtual switch has links from the physical switch via the physical NIC that attaches to Virtual Machines. The resulting lack of oversight of the traffic flows between and among the Virtual Machines on the same physical level affects security and performance surveying. There are several common approaches to virtualization with differences between how each controls the virtual machines. The architecture of these approaches is illustrated in Figure 1.



(a) Operating system-based Virtualization



(b) Application-based Virtualization



(c) Hypervisor-based Virtualization

Fig. 1. Virtualization approaches

A. Operating System-Based Virtualization

In this approach (Figure 1.a), virtualization is enabled by a host operating system that supports multiple isolated and virtualized guest OS's on a single physical server with the characteristic that all are on the same operating system kernel with exclusive control over the hardware infrastructure. The host operating system can view and has control over the Virtual Machines. This approach is simple, but it has vulnerabilities, such as when an attacker injects controlling scripts into the host operating system that causes all guest OS's to gain control over the host OS on this kernel. The result is that the attacker will have control over all VMs that exist or will be established in the future.

B. Application-Based Virtualization

An application-based virtualization is hosted on top of the hosting operating system (Figure1.b). This virtualization application then emulates each VM containing its own guest operating system and related applications. This virtualization architecture is not commonly used in commercial environments. Security issues of this approach are similar to Operating system-based.

C. Hypervisor-Based Virtualization

The hypervisor is available at the boot time of machine in order to control the sharing of system resources across multiple VMs. Some of these VMs are privileged partitions which manage the virtualization platform and hosted Virtual Machines. In this architecture, the privileged partitions view and control the Virtual Machines.

This approach establishes the most controllable environment and can utilize additional security tools such as intrusion detection systems [1]. However, it is vulnerable because the hypervisor has a single point of failure. If the hypervisor crashes or the attacker gains control over it, then all VMs are under the attacker's control. However, taking control over the hypervisor from the virtual machine level is difficult, though not impossible. According to this characteristic, this layer chose for implementing proposed security architecture.

IV. Relation between Reliability and Security in Virtualization

Apart from security, there are reliability-related issues in virtualization that can affect performance of cloud. For example, the provider may combine too many Virtual Machines onto a physical server. This can result in performance problems caused by impact factors such as limited CPU cycles or I/O bottlenecks. These problems can occur in a traditional physical server, but they are more likely to occur in a virtualized server because of the connection of a single physical server to multiple Virtual Machines such that they all compete for critical resources. Thereby, management tasks such as performance management and capacity planning management are more critical in a virtualized environment than in a similar physical environment. This means that IT organizations must be able to continuously monitor the utilization of both physical servers and Virtual Machines in real time. This capability allows IT organizations to avoid both over- and underutilization of server resources such as CPU and memory and to allocate and reallocate resources based on changing business requirements. This capability also enables IT organizations to implement policy-based remediation that helps the organization to ensure that service levels are being met [2].

Another challenge in Virtualization is that cloud organizations must now manage Virtual Machine sprawl. With Virtual Machine sprawl, the number of Virtual Machines running in a virtualized environment increases because of the creation of new Virtual Machines that are not necessary for business. Worries about Virtual Machine sprawl include the overuse of infrastructure. To prevent Virtual Machine sprawl, Virtual Machine managers should analyze the need for all new Virtual Machines carefully and ensure that unnecessary Virtual Machines migrate to other physical servers. In addition, an unnecessary virtual machine will able to move from one physical server to another with high availability and energy efficiency. However, consider that it can be challenging to ensure that the migrated Virtual Machine keeps the same security, QoS configurations, and needed privacy policies. It must be ensured that the

destination maintains all the required configurations of migrated Virtual Machines.

V. Virtual Machines Security

As mentioned before, there are at least two levels of virtualization, Virtual Machines and the hypervisor. Virtualization is not as new a technology as cloud, but it contains several security issues that have now migrated to cloud technology. Also, there are other vulnerabilities and security issues which are unique to cloud environment or may have a more critical role in cloud.

A. Hypervisor Security

In a virtualization environment, there are several Virtual Machines that may have independent security zones which are not accessible from other virtual machines that have their own zones. A hypervisor has its own security zone, and it is the controlling agent for everything within the virtualization host. Hypervisor can touch and affect all acts of the virtual machines running within the virtualization host [3].There are multiple security zones, but these security zones exist within the same physical infrastructure that, in a more traditional sense, only exists within a single security zone. This can cause a security issue when an attacker takes control over the hypervisor. Then the attacker has full control over all data within the hypervisor's territory. Another major virtualization security concern is "escaping the Virtual Machine" or the ability to reach the hypervisor from within the Virtual Machine level. This will be even more of a concern as more APIs are created for virtualization platforms [4]. As more APIs are created, so are controls to disable the functionality within a Virtual Machine that can reduce performance and availability.

1) Benefits and weakness of hypervisor-based systems

The hypervisor, apart from its ability to manage resources, has the potential to secure the infrastructure of cloud. Hypervisor-based virtualization technology is the best choice of implementing methods to achieve a secure cloud environment. The reasons for choosing this technology:

1. Hypervisor controls the hardware, and it is only way to access it. This capability allows hypervisor-based virtualization to have a secure infrastructure. Hypervisor can act as a firewall and will be able to prevent malicious users to from compromising the hardware infrastructure.
2. Hypervisor is implemented below the guest OS in the cloud computing hierarchy, which means that if an attack passes the security systems in the guest OS, the hypervisor can detect it.
3. The hypervisor is used as a layer of abstraction to isolate the virtual environment from the hardware underneath.
4. The hypervisor-level of virtualization controls all the access between the guests' OSs and the shared hardware underside. Therefore, hypervisor is able to simplify the transaction-monitoring process in the cloud environment.

Aside part of the benefits of hypervisor, there are some weaknesses that are able to affect performance of implemented security methods:

1. In a hypervisor-based virtualization, there is just one hypervisor, and the system becomes a single point-of-failure. If hypervisor crashes due to an overload or successful attack, all the systems and VMs will be affected.
2. Similar to other technologies, the hypervisor has vulnerabilities to some attacks, such as buffer overflow.

2) Security management in hypervisor-based virtualization

As mentioned before, hypervisor is management tools and the main goal of creating this zone is building a trust zone around hardware and the VMs. Other available Virtual Machines are under the probation of the hypervisor, and they can rely on it, as users are trusting that administrators will do what they can to do provide security. There are three major levels in security management of hypervisor as mentioned below:

- **Authentication:** users must authenticate their account properly, using the appropriate, standard, and available mechanisms.
- **Authorization:** users must secure authorization and must have permission to do everything they try to do.
- **Networking:** the network must be designed using mechanisms that ensure secure connections with the management application, which is most likely located in a different security zone than the typical user.

Authentication and Authorization are some of the most interesting auditing aspects of management because there are so many methods available to manage a virtual host auditing purpose [5]. The general belief is that networking is the most important issue in the transaction between users and the hypervisor, but there is much more to virtualization security than just networking. But it is just as important to understand the APIs and basic concepts of available hypervisor and virtual machines and how those management tools work. If security manager can address Authentication, Authorization, and Virtual Hardware and hypervisor security as well as networking security, cloud clients well on the way to a comprehensive security policy [6]. If a cloud provider at the virtualization level depends only on network security to perform these tasks, then the implemented virtual environment will be at risk. It is a waste of money if a cloud provider spends too much on creating a robust, secure network and neglects communication among virtual machines and the hypervisor.

B. Traditional Intrusion Detection Techniques in VMs

The IDSs can use in hypervisor level, because all the communication between the VMs and the hardware is under the control of hypervisor. If there is an IDS in the hypervisor, it can detect attacks better than the same IDS, running on the guest OS. The guest OS cannot monitor events in cloud, only events within its VM. However, it is possible for the guest OS to monitor VM events if the cloud provider performs this feature or if the cloud is IaaS [7].

Using IDSs, the HIDS has more performance than the NIDS. However, there are direct attacks against the IDS, and if the attack succeeds, the whole cloud is at risk, because the attacker can access all the information that NIDS has gathered, which can include a lot of important and useful data about the cloud users. In addition, in the cloud environment, all the cloud users may prefer to use encryption methods to prevent access to their data. This causes NIDSs to become less effectiveness, because it can't probe information within

cloud, due to the encryption. In addition, NIDS generally runs outside of the hypervisor in the individual VM, and the NIDS won't be able to access privileged data that is accessible only by the hypervisor in cloud technology. In traditional networks, this is achievable by NIDS, however. In addition, if the attacker is in the same cloud as his victim is, the NIDS is unable to detect him.

It seems NIDS may be best solution for cloud environment but using NIDS has serious problems that one of the main problems when using NIDS for monitoring is the encrypted data.

VI. Threats and Attacks in Virtualization

A. Threats

In the hypervisor, all users see their systems as self-contained computers isolated from other users, even though every user is served by the same machine. In this context, a Virtual Machine is an operating system that is managed by an underlying control program.

- **Virtual machine level attacks:** Potential vulnerabilities are the hypervisor or Virtual machine technology used by cloud vendors are a potential problem in multi-tenant architecture [8]. These technologies involve "virtual Machines" remote versions of traditional on-site computer systems, including the hardware and operating system. The number of these virtual Machines can be expanded or contracted on the fly to meet demand, creating tremendous efficiencies.
- **Cloud provider vulnerabilities:** These could be platform-level, such as an SQL-injection or cross-site scripting vulnerability that exist in cloud service layer which cause insecure environment.
- **Expanded network attack surface:** The cloud user must protect the infrastructure used to connect and interact with the cloud, a task complicated by the cloud being outside the firewall in many cases [8].
- **Authentication and Authorization:** The enterprise authentication and authorization framework does not naturally extend into the cloud. Enterprises have to merge cloud security policies with their own security metrics and policies.
- **Lock-in:** It seems to be a lot of angst about lock-in in cloud computing. The cloud provider can encrypt user data in particular format and if user decides to migrate to another vendor or something like [9].
- **Data control in cloud:** For midsize businesses used to having complete visibility and control over their entire IT portfolio, moving even some components into the Cloud can create operational "blind spots", with little advance warning of degraded or interrupted service [10].
- **Communication in virtualization level:** Virtual machines have to communicate and also share data with each other. If these communications didn't meet significant security parameters then they have potential of becoming attacks target.

B. Attacks

Nowadays, there are several attacks in the IT world. Basically, as the cloud can give service to legal users it can also service to users that have malicious purposes. A hacker can use a cloud to host a malicious application for achieve his object which may be a DDoS attacks against cloud itself or arranging another user in the cloud. For example an attacker knew that his victim is using cloud vendor with name X, now attacker by using similar cloud provider can sketch an attack against his victim(s). This situation is similar to this scenario that both attacker and victim are in same network but with this difference that they use virtual machines instead of physical network (Figure 2) [9].

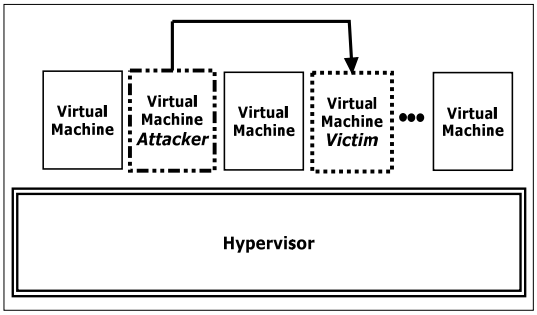


Fig. 2. Attack scenario within cloud

1) DDoS attacks

Distributed Denial of Service (DDoS) attacks typically focus high quantity of IP packets at specific network entry elements; usually any form of hardware that operates on a Blacklist pattern is quickly overrun. In cloud computing where infrastructure is shared by large number of VM clients, DDoS attacks make have the potential of having much greater impact than against single tenanted architectures. If cloud has not sufficient resource to provide services to its VMs then maybe cause undesirable DDoS attacks. Solution for this event is a traditional solution that is increase number of such critical resources. But serious problem is when a malicious user deliberately done a DDoS attacks using bot-nets.

It may be more accurate to say that DDoS protection is part of the Network Virtualization layer rather than Server Virtualization. For example, cloud systems use virtual machines can be overcome by ARP spoofing at the network layer and it is really about how to layer security across multivendor networks, firewalls and load balances.

2) Client to client attacks

One malicious virtual machine could infect all Virtual Machines that exist in physical server. An attack on one client VM can escape to other VM's that hosted in the same physical, this is the biggest security risk in a virtualized environment. When malicious user puts the focus on virtual machines become easy to access, the attacker has to spend time attacking one virtual machine, which can lead to infecting other VMs, and thereby escaping the hypervisor and accessing the environment level that officially it can't accessible from VM level. Hence, the major security risk in virtualization environments is "client to client attacks". In this attack an attacker gets the administrator privileges on the infrastructure level of virtualization environment and then can access to all VMs. If the hacker could also get control of the hypervisor and he owns all data transmitting between the hypervisor and VMs and he can perform attacks such as a spoofing attack.

VII. Other Security and Privacy Issues in Virtualization

A. Data Leakage

When moving to a cloud, there are two changes for customers' data. First, the data will be stored away from the customer's locale machine. Second, the data will be moved from a single-tenant to a multi-tenant environment. These changes can raise an important concern called data leakage. Because of them has become one of the greatest organizational risks from security standpoint [11]. Virtually every government worldwide has regulations that mandate protections for certain data types [11]. The cloud provider should have the ability to map its policy to the security mandate user must comply with and discuss the issues.

1) DLP

Currently, there is interested in the use of data leakage prevention (DLP) applications to protect sensitive data. These products aim to help with data confidentiality and detect the unauthorized retrieval of data, but they are not intended for use in insuring the integrity or availability of data [12]. As a result, there is no expectation of DLP products to address integrity or availability of data in any cloud model. Thus, DLP efficacy in cloud computing is fly-around confidentiality only.

All encryption methods rely on secure and impressive key management architectures. One of the problems that can occur in an encrypted environment is encryption key management in cloud. In cloud environments, there are several users who may use their own encryption methods, and the management of these keys is another issue to address in the context of encrypted data.

B. Data Remanence Issue in Virtualization

Data remanence is the residual physical representation of data that has been in some way erased. After storage media is erased there may be some physical characteristics that allow data to be reconstructed [13]. After storage media is erased there may be some physical characteristics that allow data to be reconstructed. As a result, any critical data must not only be protected against unauthorized access, but also it is very important that securely erase at the end of data life cycle. Basically, IT organizations which have their own servers and certainty have full control on their servers and for privacy purpose they use various available tools which give ability to them to destroy unwanted and important data safety. But when they are migrate to cloud environment they have virtual servers that controlled by third-party.

As a solution, IT governments must choice cloud which it can guarantee that all erased data by costumer are securely erased immediately. A traditional solution for securely deleting data is overwriting but this technique does not work without collaborate the cloud provider. In cloud environment customers can't access to the physical device and have access to data level. Thus, there is only one solution that is customers can encrypt their data with confidential key that prevent reconstruction data from residual data after erasing.

VIII. Virtualization Privacy

Cloud clients' data is stored in data centers that cloud providers diffuse all over the globe within hundreds of servers that communicate through the Internet. This has several well-known risks. Because of cloud services are using the Internet as communication infrastructure, cloud computing involve with several kinds of security risks [11]. Cloud providers, especially IaaS providers, offer their customers the illusion of unlimited compute, network, and storage capacity, often coupled with a frictionless registration process that allows anyone begin using cloud service [14]. The relative anonymity of these usage models encourages spammers, malicious code authors, and other hackers, who have been able to conduct their activities with relative impunity [15]. PaaS providers have traditionally suffered most from such attacks; however, recent evidence shows the hackers begun to target IaaS vendors as well [14].

In cloud-based services, user's data stores on the third-party's storage location [6]. A service provider must implement security measures sufficiently to ensure data privacy. Data encryption is a solution to ensure the privacy of the data in the databases against malicious attacks. Therefore, encryption methods have significant performance implications regarding query processing in clouds. Integration of data encryption with data is useful in protecting the user's data against outside malicious attacks and limiting the liability of the service provider.

It seems protection from malicious users who might access the service provider's system is the final goal, but this is not enough when clients also demand privacy protection from the provider himself. Any data privacy solution must use a particular encryption, but this causes another availability issue, which is data recovery. Imagine a user's data is encrypted with a user-known key and user loses his key. How can the provider recover his data if he doesn't know the key? If the user allows the provider in authority to know the key, then this makes the user-known encryption key useless. The simple way to solve this problem is to find a cloud provider whom the user can trust. This is acceptable when the data stored in cloud is not very important, and small companies may be decide to find trustable providers rather than a solution for data recovery problems. For medium-sized to large-sized companies, it is more critical to ensure privacy from cloud providers. If the service providers themselves are not trusted, the protection of the privacy of users' data is a much more challenging issue. However, for those companies it seems using private cloud is a wise solution.

If data encryption is used as a solution to data privacy problems, there are other issues in this context. One of the most important issues is ensuring the integrity of the data. Both malicious and non-malicious users can compromise the integrity of the users' data. When this happens, the client does not have any mechanism to analysis the integrity of the original data. Hence, new techniques must be applied in order to check the integrity of users' data hosted on the service provider's side.

IX. Proposed Architecture

In this paper, I added some features to virtualization architecture in order to improve security for cloud environment. In addition two main units of proposed architecture are based on this truth:

"When the workload of the VM increases abnormally, the VM may be a victim or an attacker"

Therefore, in the architecture, I included additional units for monitoring the events and activities in VMs, while trying to prevent attacks without knowing what type of data is being transmitted between VMs or VMs and hypervisor.

A. Description of Proposed Architecture

Generally, encryption is used by most of users and it is not possible to ask users not to encrypt their data. In my proposed architecture, there are not any requirements to reveal user data or encryption key to cloud providers. I have also added some new features to increase security performance in virtualization technology such as security and reliability monitoring units (VSEM and VREM).

HSEM and HREM are the main components of the security system, and all the other parts of the security system communicate with them, but HSEM decides if the VM is an attacker or a victim. Actually, HSEM receives behavioral information from VSEM and HREM and never collects any information itself. In addition, HSEM notifies the hypervisor about which VM is under Level-2 monitoring in order to set service limits until the status is determined.

Figure 3 illustrates the new secure architecture and the new units in VMs level, VSEM and VREM, which is available for all VMs (and also in Management VM) In addition, There are two other new units, HSEM and HREM, which is available in the hypervisor level. VSEM and VREM consume low resources of the VM, but they help to secure VMs against attacks.

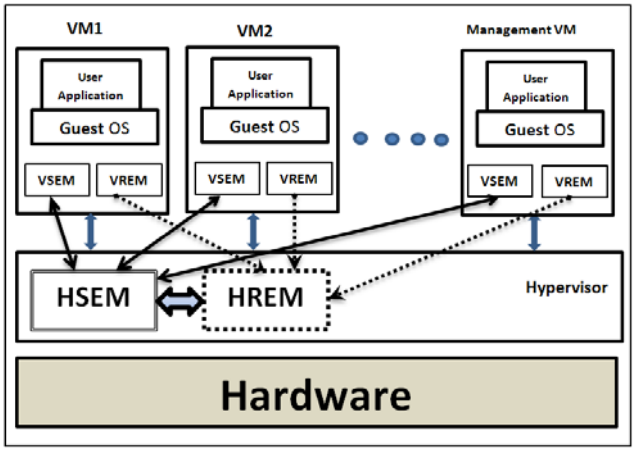


Fig. 3. Architecture of secured virtualization

B. VM Security Monitor (VSEM)

There is a VSEM within every VM that is running in a virtual environment. These monitors acts as sensors, but are different from sensors. In fact, VSEM is a two-level controller and behavior recorder in the cloud system that helps HSEM identify attacks and malicious behavior with less processing. VSEM monitors the security-related behaviors of VMs and reports them to HSEM. Because there are a large number of transmissions in cloud, and sending all of them to HSEM consumes a lot of bandwidth and processing resources, which can affect general hypervisor activity, some tasks were done by VSEMs in VMs such as collecting information that is asked by HSEM. In addition, because users don't want to consume their resources, which they paid for it, VSEMs have two levels of monitoring that consume more resource only when it is necessary. Actually, each level of VSEM is monitored almost the same events but at different detail levels.

1) Level 1

In this level, the VSEMs monitor their own VMs. In this level VSEM collects of the source and destination addresses which are in head of data, number of unsuccessful and successful tries in sending data, and number of requests that were sent to the hypervisor. At this level, VSEM, according to the brief history of the VM which provided by HSEM, looks for anomaly behavior (HSEM has had history of VMs in more details). For instance, the system identifies the VM as a potential attacker or victim if the number of service requests from the hypervisor is higher than average based on the history of requests of the VM. If abnormal behavior is detected, or the type of sending data and unsuccessful tries increase above that threshold (according to history of the VM), then VSEM switches to Level 2 and also notify HSEM about this switching in order to HSEM investigates the VM for finding malicious activities.

2) Level 2

In this level, the VSEM monitors and captures the activity of the VM in more detail, such as VM's special request from the hypervisor, details of requested resources (e.g. the number of requests), and the destination transmitted packets (to recognize if it is in the same provider's environment or outside). In this mode VSEM notifies HSEM about the level of monitoring in the VM. According to this notification, the hypervisor set activity limits in types of activities until HSEM learns that the VM is not an attacker or victim. At this level, HSEM makes a request from VREM about the reliability status of the VM, including the workload status and how many times the VM workload was close to the maximum capacity of the VM.

C. VM Reliability Monitor (VREM)

VREM monitors reliability-related parameters, such as workload, and notifies the load-balancer (within the hypervisor) about the parameter results. VREM is also used for security purposes. The VREM will send useful information such as workload status to HREM and requests the status of the VM from HSEM, and then it decides whether to give the VM more resources. Actually, if the VM requests as many resources as it can (that is different behavior according to its usage history), it may signify an overflow attack victim. Therefore, proposed HREM can detect overflow attacks and notify the HSEM about it.

X. Conclusion

In this paper, I propose virtualization architecture to secure cloud. In the proposed architecture, I try to reduce the workload, decentralize security-related tasks between hypervisor and VMs, and convert the centralized security system to a distributed one. The distributed security system is a very good way to reduce the workload from hypervisor-based virtualization, but this distribution may inject vulnerabilities to cloud. In addition, distributed security systems have more complexity than centralized ones. Because of several benefits, such as the fault-tolerant

capability, of distributed security management, it is not possible to ignore it and persist on centralized managing, but it is important to use a distributed management unit with care warily. Actually, in cloud there are lot users and their application that are running but security is important for all of them. The cloud must work properly and creates an immune environment against attacks, no matter what application is running on the cloud. In the computer world, anything makeable is breakable, however. In addition, cloud is an Internet-based technology, and but building root-of-trust cloud systems seemed impossible. Therefore, it seems main area of concern in cloud is security and cloud providers will face innumerable vicissitudes when their cloud become bigger than now.

However, this way to decentralize applications and allow universal access to data creates its own set of challenges and security problems that must considered before transferring data to a cloud. Moving toward cloud computing requires the consideration of several essential factors, and the most important of them is security.

REFERENCES

[1] L. Litty, "Hypervisor-based Intrusion Detection," M.S. thesis, Dept. Computer Science, University of Toronto, 2005.

[2] G. Rowel, "Virtualization: The next generation of application delivery challenges," 2009.

[3] G. Texiwill, Is Network Security the Major Component of Virtualization Security?, 2009.

[4] D. E. Y. Sarna, Implementing and Developing Cloud Computing Applications: Taylor and Francis Group, LLC, 2011.

[5] T. Ristenpart and e. al, "Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds," presented at the 16th ACM conference on Computer and communications security, Chicago, IL, November 9-13, 2009.

[6] "Securing Virtualization in Real-World Environments," White paper, 2009.

[7] F. Sabahi, "Intrusion Detection Techniques performance in Cloud Environments " in Proc. Conf. on Computer Design and Engineering, Kuala Lumpur, Malaysia, 2011, pp. 398-402.

[8] R. Chow, P. Golle, M. Jakobsson, E. Shi, J. Staddon, R. Masouka, and J. Molina, "Controlling Data in the Cloud: Outsourcing Computation without Outsourcing Control," presented at the ACM Cloud Computing Security Workshop, Chicago, Illinois, USA., 2009.

[9] P. Sefton, "Privacy and data control in the era of cloud computing."

[10] D. Rowe, "The Impact of Cloud on Mid-size Businesses," 2011.

[11] C. Almond, "A Practical Guide to Cloud Computing Security," 2009.

[12] F. Sabahi, "Security of Virtualization Level in Cloud Computing," in Proc. 4th Intl. Conf. on Computer Science and Information Technology, Chengdu, China, 2011, pp. 197-201.

[13] P. R. Gallagher, A Guide to Understanding Data Remanence in Automated Information Systems: The Rainbow Books, ch.3 & ch.4, 1991.

[14] Software Engineering Institute reports, N. Mead, E. Hough, and T. Sehny, "Security quality requirements engineering (SQUARE) methodolgy," Carnegie Mellon Software Engineering Institute, 2005.

[15] K. K. Fletcher, "Cloud Security requirements analysis and security policy development using a high-order object-oriented modeling," M.S. thesis, Dept. Computer Science, Missouri Univ. of Science and Technology, Rolla, MS, 2010.

Farzad Sabahi received Bachelor of Science and Master of Science degrees in Computer Engineering from Azad University in 2003 and 2007 respectively, specializing in the computer architecture. His research interests include computer architecture, distributed systems, cloud computing, hypervisor-based security and wireless network security.

He is a lecturer in the Department of Electrical and Computer Engineering at the Azad University, Zanjan, Iran. He has published several papers in distributed systems, cloud computing, and wireless network security. He has been an invited reviewer for different international conferences.

He has been member of The Institute of Electrical and Electronics Engineers (IEEE) since 2006.