THE SECURITY CHALLENGES AND COUNTERMEASURES OF VIRTUAL CLOUD

Bhupesh Mansukhani¹ and Tanveer A Zia²
¹,² School of Computing and Mathematics, Charles Sturt University
New South Wales, Australia
¹bhupeshmansukhani@yahoo.com, ²tzia@csu.edu.au

Abstract
The adaption of cloud computing is on a rise these days, due to the various effects that it has on enterprise. As it allows the users to have scalable infrastructure and economical benefits which indeed a way to boost any enterprise mind in opting for such service. Cloud Computing offers a whole new paradigm to allow the users to have high-end and scalable infrastructure at an affordable cost and without even the need of managing the inventory. The interesting part of cloud computing is it offers three platforms to choose from IaaS, PaaS, and SaaS, these three platforms together, form cloud computing. Out of these three platforms, the interesting one is IaaS (infrastructure as a service) that allows the users to have ‘on the fly’ infrastructure. Although IaaS offers great benefits to the users, the complexity in its structure, open doors to unseen and forcible threats to the security of the data and to cloud computing. In this paper, the authors have proposed countermeasures to secure cloud computing IaaS virtual platform by High Trust Zone. The solution proposed would minimize the threats to the virtualized infrastructure of the cloud by binding the VMs (Virtual Machines) in one trusted zone, irrespective of the Users applications and security policy, this zone will provide utmost protection to the other running VMs and devices of the physical host such as memory, hardware etc. The authors believe that by using the proposed solution, (High Trust Zone), it can offer pre-emptive protection words complex and dynamic cloud virtual infrastructure.

Keywords
Cloud security, cloud computing, private cloud computing security, VM security, high trust zone, cloud risks, SecVM, VM.

INTRODUCTION
Cloud computing is a model for delivering information services that provides flexible use of servers, scalability and management services. In terms of its essential features Cloud computing is a unique combination of capabilities which include:

- Scalable and dynamic infrastructure
- Global/Remote access
- Précised usage controls and pricing
- Standard Platform
- Support Services – IT and Management

The aforesaid capabilities enable a number of variations in cloud computing services. For instance, one will provide database infrastructure services, and the other one will provide a fully functional CRM model (Appistry, 2010). Cloud computing refers to the use of networked infrastructure software and capacity to provide resources to users in an on-demand environment. With cloud computing, information is stored in centralized servers and cached temporarily on clients that can include desktop computers, notebooks, handhelds and other devices. Cloud infrastructure can reside within the company’s datacenters (as internal clouds or on-premise solutions) or on external cloud computing resources (off-premise solutions available through service providers). It encompasses any subscription-based or pay-per-use service that extends existing IT capabilities. Typically, Clouds utilize a set of virtualized computers that enable users to start and stop servers or use compute cycles only when needed (also referred to as utility computing). By design, cloud computing is scalable, flexible and elastic – offering IT staff a way to easily increase capacity or add additional capabilities on demand without investing in new and expensive infrastructure, training new personnel or licensing more software.

Cloud Computing – Platforms
Cloud computing is like an ocean, it’s vast, gigantic and complex due to its virtualized architecture. That being said, cloud computing does not mean we can go to a service provider and ask them to provide a cloud computing solution; the users have to be specific on exactly what they demand? Do we want Infrastructure? Or we want
applications? Or we need OS or platform? So to answer these questions, here is the key - there are three major elements or platforms of Cloud Computing, and they are described as:

- **IaaS** – referred as Infrastructure-as-a-Service, this type of cloud enables IT infrastructure to be deployed and used via remote access and made available on an elastic basis.
- **SaaS** – referred to as Software-as-a-Service, this type of cloud is referring to a business-level service. Typically available over the public Internet, these clouds are information-based.
- **PaaS** - referred as Platform-as-a-Service, cloud development platforms enable application authoring and provide runtime environments without hardware investment.

**Virtualisation and IaaS**

IaaS is the most popular service when it comes to cloud computing services; IaaS allows users to scale their infrastructure and storage resources on the fly without affecting the runtime resources and without affecting the inventory management records of the enterprises and/or large scale investment. The IaaS concept resource is virtualisation that means the core of IaaS is virtualised hardware. Virtualisation enables the execution of multiple operating systems or also known as Virtual Machines (VMs) – on the same server or physical machine also known as the Host Machine. Each virtual machine functions with dedicated operating system and hosted applications. The important aspect of virtualisation is achieving higher hardware utilisation rates without the need of more servers by aggregating a collection of physical servers into one server. However the structure of a basic cloud physical server with virtualised infrastructure is composed of three components shown in the figure below:

![Figure 1: Server Virtualization on Cloud Computing IaaS Platform - adapted from Ibrahim et al. (2010)](image)

1. **Hypervisor Layer** – Hypervisor is the abstraction layer that provides the necessary resource to share hardware resources between the virtual machines. Hypervisor layers have two main models: Para-virtualization, such as Xen and Hyper – V and the other model is full virtualization such as VMWare. Often these two models trade-off a level of isolation to increase the sharing of resources among VMs.
2. **vSwitch or Virtual Network Layer** – this layer is responsible for multiplexing traffic between virtual NIC (network interface card) and physical NIC (network interface card). The vSwitch also controls the VM traffic of a single host that does not touch the physical NIC of the host, and vSwitch manages the customer trust zone. The virtual network also acts like a physical switch in non-virtualised environments.
3. **Virtual Machines** – VM’s is a software layer that emulates the real physical machine, these VMs run under the control of hypervisor layer that further virtualizes and emulates the hardware resources and returns the same to the virtual machines.

**Virtual Cloud Infrastructure Security**

Cloud computing provides organizations with effective, efficient and scalable resources to the users. It is an innovative alternative to traditional computing resources however over the cloud, or as commonly referred to as the Internet. Various security practitioners, researchers and hackers around the world have shown the capabilities through which virtualization can be exploited in variety of ways, furthermore they have also shown different ways through which they can prepare various malware that are hard to detect and can breach the virtualised component of cloud computing hence effecting the IaaS platform (Skapinetz, 2007).
SECURITY CHALLENGES

Threat Model
The virtualised architecture of cloud computing offers various benefits to the cloud user however security of the cloud is the responsibility that is shared between the cloud user and cloud provider. The users of cloud computing are not aware of the security policies through which their VMs are protected. On the other side, cloud providers running VMs are not aware of the contents of the VMs. Thus, there is no complete trust between cloud customers and providers. From a cloud provider perspective, the VMs of the user cannot be trusted (due to the unknown applications and various security policies which may or not may be disclosed to the cloud provider). In the threat model that we will describe, a hacker can be either a cloud user that may be already hosting a service or is non-cloud user. In either of these models the victim is the cloud provider who runs the service to host the VM’s of the users. Incase of a security breach, the responsibility and the infrastructure that is compromised belongs to the provider. In the former threat model, hackers have more chances of success due to the fact that they have more access to the cloud computing virtual infrastructure and have the ability to run various malware to gain access on the system.

Security Threats
It is evident that breaching any component of the virtualized cloud infrastructure greatly impacts on the security of the other components and affects the overall security of the cloud computing virtualized infrastructure. Grobauer, Walloschek, & Stöcker, (2010), investigated several vulnerabilities and threats to the security of the cloud computing especially focusing on the virtualized cloud computing security. These threats can be broadly categorized in three categories:

I. Hypervisor Vulnerabilities - The hypervisor attack is hackers potential target because of only one reason, gaining access to the hypervisor layer will provide access to the underlying layers of the hypervisor and hence will provide access to the hacker on virtual machines installed on the host physical server. If the hypervisor layer is compromised all the virtual machines and their running operating systems and application will come under the attack of the hacker and hence will breach the security of the entire virtualized environment. Many such attacks have been popular on the hypervisor layer, Carbone, Zamboni, & Lee, (2008) describe HyperJacking, BluePill and Vitriol and King, Chen, & Wang, (2006) describe SubVir and DKSM as few attacks that can target the virtual layer at the runtime. Basically all these attacks are capable of injecting a malicious hypervisor during the runtime or modifying the existing hypervisor to enable the hacker to gain control over the physical host. However the afore said was a case of traditional hypervisor attack, in some cases the Xen hypervisor, the hypervisor is not only responsible for administering the Virtual Machines but also controls the other VM’s that are running on the same physical host. Imagine a hacker gaining access to the Xen hypervisor, they will not only control single hosted VMs but multiple VMs running on the same physical host.

II. Virtual Network Layer Vulnerabilities – The virtual network layer or vSwitch layer is also vulnerable to variety of attacks. These attacks can be vSwitch configurations, VLAN’s, Trust Zones and ARP tables’ corruption. Cabuk, Dalton, & Edwards (2008) state that vSwitch attacks are not common as they have mostly occurred in the past using a physical network, for instance corrupting the ARP tables of the physical host and then attacking the VMs with a spoofed IP. Hence to attack the vSwitch layer many hackers have to attempt hacking the physical host network layer and if the network layer is vulnerable then the possibility of attacking the vSwitch layer increases.

III. Virtual Machine Vulnerabilities – As it is evident a virtualised cloud infrastructure can contain various VM images and not all of them can be active at once, some of them will be offline and some of them will be online. In either stage whether offline or online they are all prone to serious vulnerabilities. Any attack on the active VM can make the hacker gain access over the physical system however once the VM is compromised, it can be a possibility that the other VMs on the same physical server be compromised too at the same time. According to Ormandy (2007) sharing the same resources increases the risk of attack on other VMs installed on the physical server as all of the VMs installed share the same physical server resources such as memory, hard drives, optical media and hypervisor layer. Having multiple VMs on a single server increases the severity of the damage caused and the risk of VM-to-VM attacks. However if the physical server is in off state, it is safe from any hacker attacks but on the other hand if the VM is offline it is still prone to various attacks as it is available as a virtual
image file that can be easily tampered by an internal or external attack provided the physical server state is on.

These security threats are due to the complex virtualized infrastructure and dynamic nature of the cloud and they can be further details here under:

i. Multiple Users – A virtualised cloud layer such as IaaS can hold up various virtual machines and can provide multiple access to different users from around the globe, this kind of sharing is responsible for information leakage and hence increases the risk of VM-to-VM attacks.

ii. Minimal Control – Users of the cloud are not aware of the location of the physical server, as all these physical servers belong to the data centers of the providers hence the users are not aware of the location of their VMs (which server or location they are getting installed) and the provider is not aware of the contents of the VM or its applications hence giving a way to the security threats.

iii. Single Point of control - All the virtualized servers are connected to one or limited number of network interface cards (NIC). This in turn causes more vulnerabilities in the virtual environment, any compromise to the security of the VMs or the physical server will lead to the compromise of either the VM or the physical server and will enable the hacker to gain access to either physical server vSwitch or VMs vSwitch or to both.

TRADITIONAL METHODS OF SECURING VIRTUAL CLOUD

This section discusses about the current technologies that can be used to secure virtual cloud computing such as IDS (intrusion detection system), firewalls, hardware firewalls and network intelligence. Liu, Su, & Liu (2009) use a firewall to protect the Xen hypervisor virtual network or vSwitch. They use a firewall hook framework called “Netfilter”. Roschke, Cheng, & Meine (2009) introduced the concept of cloud computing based IDS deployment model. This model deploys IDS sensors with each layer with a centralised IDS management module. However all these approaches have certain limitations when comes to deployment on the VM cloud infrastructure because of their traditional approach. Most of these solutions generally impact the performance of the system as they trap every I/O (input/output) request, system call and access systems memory before forwarding the user requests to the hypervisor. Furthermore, these approaches are used regardless of the cloud complexity that can result changes in cloud topology, network traffic, system usage, and communications between the VMs. Even if the aforesaid challenges are overlooked there will be always a lack of security in the vSwitch software and VLAN (virtual local area network) configurations thus keeping an open end for the hackers.

Securing VM

Another approach to secure the virtual machines is to deploy the security software in a dedicated and privileged VM (or SecVM). The privileged VM will have access to the hypervisor to secure the other VMs (mostly the untrusted VMs) which are installed in the same physical server (refer to figure 2).

As shown in figure 2, the SecVM utilises VM introspection techniques (Jiang, Wang, & Xu, 2007) that enables monitoring and observing VM from outside a VM and then get a view of the VM at the hypervisor level. This approach isolates the security solution from the other server workload by using the isolation feature of virtualization. It is installed in lower layer than the one being protected. The virtual introspection techniques monitor untrusted VMs from outside the VM without installing any hooks or drivers inside the untrusted VM making it hard for a hacker to detect the installed security software and thus protecting SecVM layer from any attack tampering the security software.

By utilising the virtualisation aware security solutions, organizations can enable different security technologies throughout VMs on a protected physical layer. However certain security functions/tasks such as managing encrypted data/traffic, accessing real-time information, cleaning or detecting malwares from VMs will continue to require VM based agents. Though introspection has many applications, it has limitations due to the fact it can only perform on passive monitoring (Payne, Carbone, Sharif, & Lee, 2008). Besides passive monitoring limitations, this approach does not consider the mobility and complexity of the VMs and its components and can only provide security to a limited number of hosts.
Hypervisor Protection

This section discusses more about the protection of the hypervisor layer itself against root-kits and page-level memory attacks. These attacks can arise from shared memory pages and software level memory page. Riley, Xuxian, & Xu (2008) introduced memory management techniques and secure software-based page-level protection to secure the hypervisor layer. New generations of Intel and AMD processors have been provided with two layers of page tables at the hardware level. These processors have powerful features that enhance the trust level and the protecting operating platform. Some of these features are multi-queue networking, efficient I/O memory management and isolation enforcements. These features help the hypervisor to be more effective and restrict the range of physical memory locations that I/O devices are able to access (Uhlig & Munoz, 2009). This solution seems to be working for most organizations but when it comes to attacks on VMs this solution hardly fits.

PROPOSED COUNTERMEASURES – SECURING THE VIRTUAL MACHINES ON PRIVATE CLOUD

Keeping in mind that chip manufacturers such as Intel and AMD have introduced new generation of processors that can safeguard the hypervisor layer but not the VM layer, if the security in the VM layer is enhanced and is regulated by series of steps then it can be possible that both of these layers such as the hypervisor and the VMs can be secured by many attacks in the future. This section will describe an approach that can be adapted to secure most crucial and critical applications running on the most new generation of processors and hardware. These applications can be categorized as:

1. highly sensitive data
2. security functions and administrative applications
3. mission critical applications
4. and applications that are under regulatory controls

Before discussing this solution, the authors would like to discuss about the parameters on which the upcoming solution is based:

- Trust calculation – granting access to the user dynamically and what kind of access need to be provided based on the user’s role in the organisation. This is based on many parameters such as user’s device, location, resources requested and what existing controls are available with the user.
• Balanced controls – installing detective and corrective controls such as IDS (intrusion detection systems) and firewalls increase the flexibility and recovery ability.

• Security zones – Dividing the environment or the infrastructure in zones according to the sensitivity of the data and role based access, enable control and monitoring over each zone and prevent spread of compromise on other connected zones.

High Trust Zone

For the proposed solution to safeguard virtual cloud computing on IaaS platform, the authors propose HTZ (High Trust Zone) virtual environment, creating a high trust zone or HTZ will create higher degree of trust between the data, users, providers and the systems.

Figure 3 Proposed Approach for building a High Trust Zone

Figure 3 illustrates how our proposed approach can be used by cloud providers to secure the VMs and the cloud infrastructure on an IaaS platform by following the security in proposed phases.

Phase -1 - Configuring the Virtualized Infrastructure

Step -1 - Securing the Virtual Cloud

The first step to protect the virtual cloud is to protect the virtualization infrastructure by isolating the infrastructure (virtualised) from the servers that are going to be virtualized, also by protecting accounts that will be used to control virtualisation, securing applications by moving them to the High trust zone and by hardening the OS. By hardening the OS, the unnecessary applications or features of the OS will be removed and only the required ones will be kept. The most important factor of this process is to isolate the virtualisation infrastructure, this means that the customer VMs will not impact any of the system or data center VMs of the cloud provider. As shown in figure 3 the data centre zone is the one where all the necessary VMs of the data centre resides whereas the HTX landing zone where all the VMs belonging to the clients will be hosted, this ensure that all the VMs share their space accordingly and in case of any breach in HTZ layer the data centre layer will be least impacted since it is already isolated and has separate storage.

Step -2 - Securing applications and moving them to High Trust Zone

Before moving applications to High Trust Zone it is necessary to build a preproduction virtualised environment. This will be used to test the application (to be moved) for testing, compatibility, application review and some testing on the security perspective of the application. The goal for application testing from a security perspective is to ensure that existing policies of the application or the VM is carried over from the physical world to the virtual world. For instance whether to allow the GPO (group policy objects) in the application such as remote deployment of application updates and so on. Hence the user of the cloud should ensure that they carry the same security policy of their physical hosts on the hosted VMs. This is to ensure the safety of their VMs and being in-line with their existing enterprise security policies. If the security policies are not implemented on the VMs then this solution might not work.
Step – 3 - Risk Assessments of Applications

Risk assessment of applications is mandatory to find out the risks associated with the applications before moving them to the High Trust Zone. This assessment is required to ensure that applications or the system being added to the high trust zones do not have any additional risks associated with them or add to the security risks of the High Trust Zone security environment. This assessment can also provide additional benefit of identifying the opportunity of understanding and re-examining the security risks associated with legacy applications. The following should be considered before conducting the risk assessment:

- Eliminate overlap access from outside High Trust Zone
- Evaluate the network architecture to properly define firewall rules and identify required configurations for proxies and bastion hosts. A bastion host is a computer on a network specially designed to withstand attacks (Dillard, n.d.).
- Understanding the security requirements of the application, such as logging capabilities of the application, the data being stored by the application, the directory permissions that the application need, authentication and security lifecycle of the application.
- Evaluating the security of the system including authentication, access control, restrictions and group policies (if any).

Phase - 2 Network Monitoring

To secure the High trust zone and to provide the High Trust Zones with the capability of prevention and protection environment, there is a strong need of implementing a mix of network attack and intrusion detection capabilities. At first, the network intrusion monitoring has to be implemented that will analyze and monitor all traffic coming into and going out of the high trust zone. Additionally, there is a strong need of implementing network traffic analysis behaviour. This process would ensure the normal traffic patterns and shall enable abnormal traffic activity, with a facility for sending appropriate alerts.

Besides the aforesaid the authors also suggest implementing both a Host Based Intrusion Prevention System (Newman, 2009) and a Host Based Intrusion Detection System specifically on the VMs deployed on the High Trust zones, this would help to have a broader and wide coverage of the attacks specifically to the VMs.

CONCLUSION

Like every other technology Cloud computing has security challenges and obtaining 100% secured cloud is difficult until unless a reverse approach is achieved to secure each elements of cloud computing. In this paper we have presented various security challenges that are hovering around the current IaaS and virtualised cloud architecture and the existing security solutions that are being used to safeguard the cloud, however each of these traditional methods have their own shortcomings. On the other hand a layered, definite and systematic approach is proposed to secure the virtualized cloud and VMs in a better way by isolating the VMs to run in a high trust zone. The proposed approach increases the monitoring of the network of incoming and outgoing traffic also by providing extra host level security protection to the individual VMs by implementing Host Intrusion Detection system and Host Intrusion Prevention system at the each of the VMs deployed on the High Trust Zone.

Besides the proposed approach there is still a need for intelligent self-defence and the provision of real-time detection to safeguard cloud computing IaaS platform from known and unknown threats. As part of our future work we will keep focusing on such new intelligent solutions in the future to completely safeguard at least one aspect of cloud computing, IaaS and Virtualised Cloud architecture.

REFERENCES


