# Network Security for Virtual Machine in Cloud Computing

Hanqian Wu
[1]College of Software Engineering
Southeast University
Nanjing, China
Hanqian@seu.edu.cn

Yi Ding
[2]Department of Electrical and Computer Engineering
Purdue University Calumet
Hammond, IN, USA
dingy@calumet.purdue.edu

Chuck Winer
[3]Department of Computer Information Technology & Graphics
Purdue University Calumet
Hammond, IN, USA
Winer@calumet.purdue.edu

***Abstract*- Cloud computing is the next generation of networking computing, since it can deliver both software and hardware as on-demand resources and services over the Internet. Undoubtedly, one of the significant concerns in cloud computing is security. Virtualization is a key feature of cloud computing. In this paper, we focus on the security of virtual network in virtualized environment. First, we outline the security issues in virtual machines, and then security problems that exist in a virtual network are discussed and analyzed based on Xen platform. Finally this paper presents a novel virtual network framework aimed to control the inter-communication among virtual machines deployed in physical machines with higher security.**

## I. INTRODUCTION

In the past decades, the world of computation has experienced some dramatic changes from stand alone application to client-server architecture and from distributed to service oriented architecture. All of these transformations aimed to make the software easier to use and improve business process execution efficiency [1]. Cloud computing, an emerging IT delivery model, is the next generation of networking computing which can deliver both software and hardware as on-demand resources and services over the internet with lower IT costs and complexities[2-4][6]. Many companies such as Amazon, IBM, Google, Oracle, Microsoft, Salesforce and HP are rushing to provide cloud solutions in various ways.

Cloud computing, the hottest buzzword in the IT area, has been frequently discussed in workshops, conferences and even magazines [5]. Nevertheless, to define cloud computing is not an easy task, confusion still remains about what exactly the definition of cloud computing is. From different perspectives, there are more than a dozen definitions for cloud computing in academia [7-8]. But the following features of cloud computing defined among them are common:

- Cloud computing is a computing platform to enable resource sharing in terms of scalable infrastructures, middleware and application development platforms and applications.
- New computer technologies, such as service oriented architecture, virtualization, high power enterprise servers and high band width, support to realize cloud computing platforms.
- Typically, services provided in clouds can be grouped into 3 categories: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS).

Cloud computing enables users to store and process all their data on the web via the Internet, with no doubts security is one of main significant concerns [9] [26]. A more fundamental reason preventing companies from moving to cloud computing is that the cloud computing platform is inherently less secure than the traditional network infrastructure [10] [25]. Security must be integrated into every aspect of cloud computing platforms to make users trust that their data is secure [27].

One of biggest challenges of security issues in the design of a cloud computing platform is that of virtual machine (VM) instance interconnectivity [11]. Because users who are granted super-user access to their provisioned VMs, without care, may have possibilities that a VM can monitor another VM or access the underlying network interfaces, which we call the break of isolation. In this paper, we focus on network security for virtual machines and we select the open source project - Xen hypervisor as the research platform. In this work, we discuss and analyze the network secure problems existed in VMs, and then present a novel virtual network model which can control the inter-communication among VM instances running on the hypervisor with higher secure.

## II. NETWORK SECURITY IN VMs

### *A. Security of Virtual Machines*

The technology of virtualization has been started with the development of the system/360 by IBM in 1970 [12]. The main purpose of virtualization is to improve the performance of a server by providing users virtual machines within an operating system (hypervisor). Over the last several years, virtualization has become a fundamental technology in cloud computing and enabled cloud computing platforms to dynamically allocate virtual machines as scalable Internet services (i.e., Amazon EC2/S3 [13]). However, Virtual Machine technology is going mainstream in the IT industry, security of VMs becomes the significant concern. MacDonald [14] pointed out, "Through 2009, 60 percent of production VMs will be less secure than their physical counterparts."

Virtualization brings a more complex and risky security environment. Reiser, Garfinkel and Kirch [15] [16] [17] [18] analyze the security vulnerabilities in virtualization environment and mainly conclude the following security issues:

- The break of isolation. A VM can monitor another one or even have access to the host machine.
- Remote management vulnerabilities. Commercial hypervisors normally have management consoles as new facilities for administrators to manage VMs. Xen, for instance, uses XenCenter to manage their VMs. These consoles also open new vulnerabilities, such as Cross-site scripting, SQL injection, etc.
- Denial of service (DOS) vulnerabilities. In virtualization environment, resources such as CPU, memory, disk and network are shared by VMs and the host. So it is possible that a DOS will be imposed to VMs which correspondingly take all the possible resources from the host. As a result, the system will deny any request from the guests because of no resources available.
- Virtual machine based Rootkit. The concept of Rootkits appeared in the UNIX world. A Rootkit is a collection of tools (programs) that enables administrator-level access to a computer or computer network. If a Rootkit compromises the hypervisor, it can gain the control the whole physical machine. Two examples of typical Rootkits are BluePill and SubVirt [28].
- Revert to snapshots problem. Snapshot is a mechanism to allow the administrator to make a snapshot of the machine in a certain point and to revert to the snapshot in case of necessity. Snapshot also brings some security problems such as using old security policies, re-enabling previous disabled accounts and passwords.

### *B. Virtual Network*

One of the key issues in virtualization is isolation [19]. Isolation plays a crucial role in VMs in order to guarantee that one VM can not affect the other VMs running in the same host. Virtual network is a method of creating independent or isolate logical network within a shared physical network. We can find many current hypervisors (i.e., Xen, VMware) offering virtual network mechanism for VMs to access physical network. In this paper we take Xen hypervisor as the example to demonstrate how the virtual network works.

Xen, originated as a research project at the University of Cambridge, is the powerful open source industry standard for virtualization [20] [21]. Today, The Xen hypervisor is becoming the fastest and most secure infrastructure virtualization solution. It supports a wide range of guest operating systems including Windows, Linux, Solaris and various versions of the Free BSD. A Xen system has multiple layers, the lowest and most privileged of which is Xen itself [22]. Xen in turn may host multiple guest operating systems, each of which is executed within a secure virtual machine (in Xen terminology, a domain). The first domain, domain 0, is created automatically when the system boots and has special management privileges. Xen offers two modes for users to configure virtual network [23]:

#### *B.1 Bridge*

This mode instructs Xen to attach the VM's interface directly to a software Ethernet bridge connected to the physical network. The administrator can handle VM network DHCP requests the same way as handling common network DHCP requests. Figure 1 illustrates the structure of Network Bridge and Virtual Interface (VIF) Bridge in Xen.

By default, when Xen starts up, Network Bridge is configured as following steps:

- Create a new bridge named Bridge0;
- Real Ethernet interface eth0 is brought down and the IP and MAC addresses of eth0 are copied to virtual network interface veth0;
- The real interface eth0 is renamed peth0 and the virtual interface veth0 is renamed eth0;
- Peth0 and VIF0.0 are attached to bridge Bridge0;
- The bridge, peth0, eth0 and VIF0.0 are brought up.

When a virtual machine (dom) starts up, VIF<id#>.0 and Bridge0 are attached and VIF<id#>.0 is brought up.

#### *B.2 Route*

The second mode offered by Xen for the configuration of virtual network is route. This configuration allows the administrator to create a point-to-point link between dom0 and each VM. A set of MAC and IP addresses must be defined in advance because routes to each VM should be added to dom0's routing table before a VM is started. So, in this mode, each VM instance created by Xen is assigned a free MAC/IP tuple and released when the VM is terminated. DHCP doesn't work in route mode. Figure 2 presents the structure of route in Xen.

The steps to configure routing in Xen are as follows:

- Enable IP forwarding within dom0;
- Copy the IP address from eth0 to VIF<id#>.0;
- Bring up VIF<id#>.0;
- Add host static route for dom* IP and MAC addresses specified in dom* config file and point at interface VIF<id#>.0.

### *C. Virtual Network Vulnerabilities*

Virtual network significantly affects the VMs interconnectivity which is one of the biggest security challenges in the design of cloud computing platform. The more secure way to isolate each VM is using dedicated physical channel for each host-VM link. However, as we previously discussed the virtual network configuration modes in Xen, it is common that most hypervisors (i.e., VMware EXSi, Virtual box) offer virtual network to link VMs by using bridge and route. In these modes, the performance of inter-VM communication is near-native when VMs are running on the same host. As a result, isolation is easy to be broken.

The follows are the vulnerabilities existing in the current virtual network:

- Sniffing virtual network. In the bridge mode, bridge

plays a role as a "virtual" hub. All VMs share the "virtual" hub to communicate network, in which a VM is able to sniff the virtual network by using sniff tool such as "Wireshark" [29]. Figure 3 presents a shared virtual network example. Three virtual machines connect the "virtual" hub in Xen hypervisor. In this way, packets sent to VM1 or VM3 could be easily sniffed by VM2, therefore isolation is able to be broken.

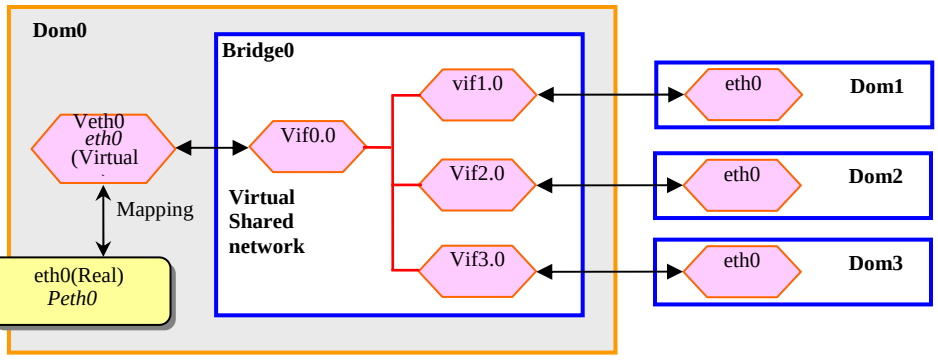


Fig.1. Structure of Network-Bridge and VIF-Bridge in Xen

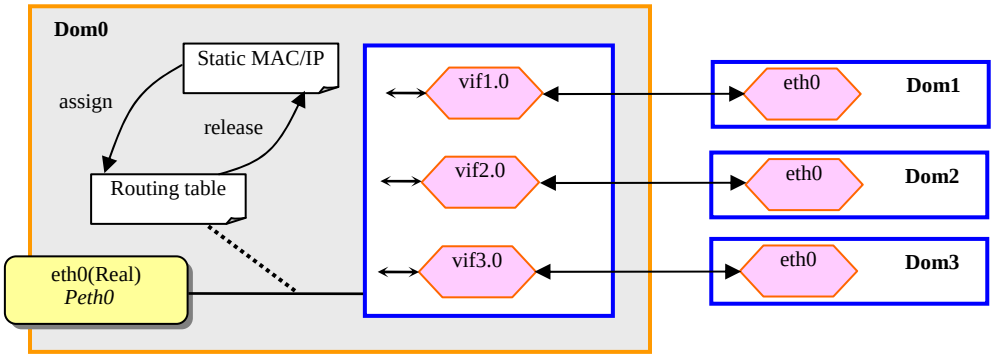


Fig.2. Structure of route in Xen

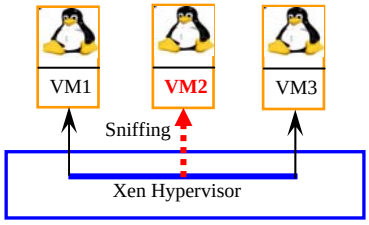


Fig.3. Sniffing in virtual network

- Spoofing virtual network. In the route mode, route plays a role as a "virtual switch". The virtual switch uses a dedicated virtual interface to connect each VM (see figure 2). In this case, a VM can do an Address Resolution Protocol (ARP) spoofing [24], redirecting packets to them and be able to sniff packets going to and coming from other VMs.

Figure 4 demonstrates the process of spoofing in virtualization environment. A virtual route starts up and initializes the routing table by sending an ARP command to each VM in boot time. The routing table records the information fed back from each VM consisting of port, IP and MAC addresses. In this example, VM3 launches an ARP spoofing attack. It forged a same IP address with VM1 and sent an ARP to the virtual route. The virtual route will update the routing table information when it receive the ARP request from VM3, as a result, any traffic meant for VM1 would be mistakenly sent to VM3 instead, then VM3 could choose to sniff or modify it before forwarding it.

## III. A NOVEL VIRTUAL NETWORK MODEL

According to the analysis of vulnerabilities existed in the virtual network above, we leverage the characteristics of "route" and "bridge" modes and combine them to propose a novel virtual network model to make the communication among VMs more secure. This model is composed of three layers: routing layer, firewall and shared network, as shown in figure 5.

- Routing layer

This layer has the same functions with the traditional route mode. It is this layer's responsibility to connect the physical network and create a logical dedicated channel for the communication between the virtual network and the physical network. In this layer, a set of unique static IDs are specified

by the administrator in advance and are stored in a configuration file, which can be assigned to a shared network as a unique tag. In this way, we can use the unique tag to monitor the source of packets sent from each shared network.

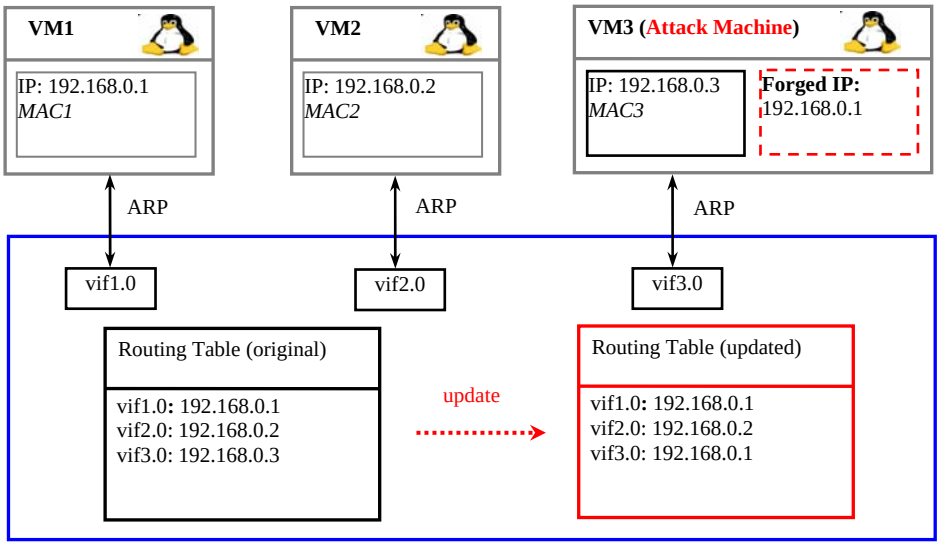


Fig.4. Spoofing in virtual network

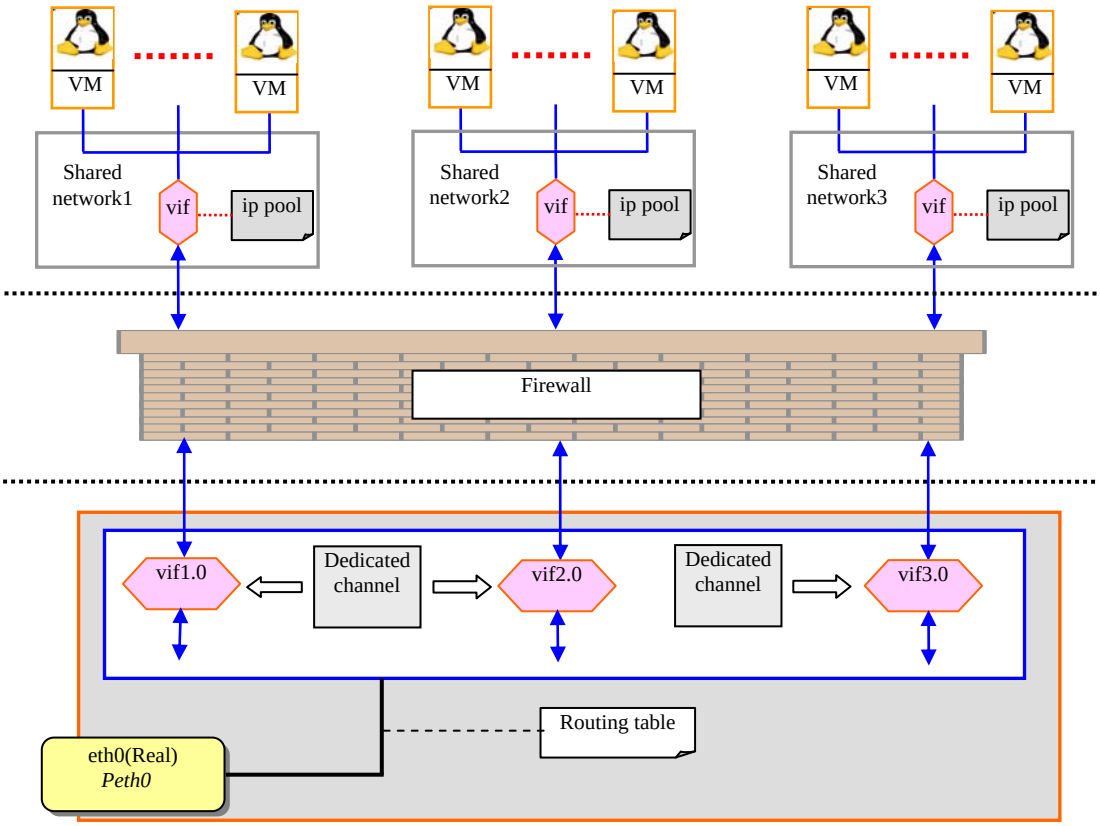


Fig.5. A virtual network model

- Firewall

The main purpose of this layer is to prevent spoofing attacks launched from virtual shared networks by identifying the network ID specified in the configuration file. In this layer, we define a set of security policies mainly including: (1) each virtual interface in the routing layer that connects with a virtual shared network can not communicate with any other

virtual shared network; (2) any packet (i.e., ARPing) that tries to modify the routing table will be dropped. The administrator may dynamically configure the security policies to meet the new requirements. These security policies can be implemented by using iptables packet filtering system in Xen.

- shared network layer

To block the communication among VMs within a shared network is not an easy task as we have previously discussed. In this layer, we assume that VMs belong to a same virtual shared network are trustful to each other. This assumption means VMs working for the same company or organizations should be allocated in the same shared network.

In order to further enhance security of this model, we specify a set of subnets (i.e., 128.128.10.0, 10.232.193.0, 10.232.194.0) in advance and each shared network will be bound with a unique subnet by the administrator when a new shared network instance is created.

## IV. CONCLUSION AND FUTURE WORK

A survey shows that security is the most significant user's concerns in cloud computing [9]. In this paper, we focus on the security of virtual network which is a key technology of cloud platforms. We propose a novel virtual network framework in order to improve security of the inter-communication among virtual machines deployed in physical machines based on the analysis of Xen. Firewall, specified subnets and routing table are the key features of this model, which can efficiently prevent VMs from attacks such as sniffing and spoofing in theory.

Our research can be extended in several directions. First, we are going to implement this model in Xen platform to validate its security, and then we can find out how to further improve security of the model. Second, further study should be conducted to evaluate the performance of the model in the virtualization environment. Third, we plan to test this model on different hypervisors.

## ACKNOWLEDGMENT

We would like to thank Mathew Borton, who is the system administrator of Computer Information Department and Graphics of Purdue University Calumet, for helping construct the research platform.

## REFERENCES

[1] Zeeshan Pervez, Sungyoung Lee, Young-Koo Lee. Multi-Tenant, Secure, Load Disseminated SaaS Architecture. *In proceedings of the 12th Advanced Communication Technology (ICACT) International Conference. Phoenix, USA*, 2010, pp. 214 – 219.

[2] M. P. Rad, A. S. Badashian, G. Meydanipour, M. A. Delcheh, M. Alipour, and H. Afzali, "A Survey of Cloud Platforms and Their Future," in *Lecture Notes in Computer Science*, 2009, pp. 788-796.

[3] Sun Microsystems, Inc. Introduction to Cloud Computing Architecture. White Paper, 1st edition, June 2009.

[4] Galen Gruman and Eric Knorr. What cloud computing really means. InfoWorld, April 2008. Electronic Magazine, available at http://www.infoworld.com/article/08/04/07/15FE-cloud-computing-reality 1.html.

[5] Cloud Computing, http://www.ibm.com/ibm/cloud/.

[6] Armbrust, M., et al. , Above the Clouds: A Berkeley View of Cloud Computing. 2009, EECS Department, University of California, Berkeley.

[7] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," *SIGCOMM Comput. Commun. Rev.*, vol. 39, pp. 50--55, 2009.

[8] Jeremy Geelan. Twenty one experts define cloud computing. Virtualization, August 2008. Electronic Magazine, article available at http://virtualization.sys-con.com/node/612375.

[9] Whyman, B.: Cloud Computing, Information Security and Privacy Advisory Board, pp.11–13 (December 5, 2008).

[10] Security-as-a-Service - The next growth area for cloud computing (Oct 26, 2009), http://www.scmagazineuk.com/security-as-a-service--the-next-growth-area-for-cloud-computing/article/156193/.

[11] D. Nurmi, R. Wolski, C. Grzegorczyk, G. Obertelli, S. Soman, L. Youseff, and D. Zagorodnov, "The Eucalyptus Open-source Cloud-computing System," in *9th IEEE/ACM International Symposium on Cluster Computing and the Grid*, 2008, pp. 124 - 131.

[12] Virtualization Concept and History (Jan 24, 2010), http://www.remoteitservices.com/content/virtualization-concept-and-history.

[13] Amazon Elastic Compute Cloud (Amazon EC2), http://aws.amazon.com/ec2/.

[14] Neil MacDonald. Security considerations and best practices for securing virtual machines. Gartner, Inc., March 2007.

[15] Hans Peter Reiser. Security Challenges with Virtualization. December 2009.

[16] Virtualization: What are the security risks? (Jan 22, 2008), http://www.zdnet.com/blog/security/virtualization-what-are-the-security-risks/821.

[17] Tal Garfinkel and Mendel Rosenblum. When virtual is harder than real: security challenges in virtual machine based computing environments. In HOTOS'05: Proceedings of the 10th conference on Hot Topics in Operating Systems, pages 20–20, Berkeley, CA, USA, 2005. USENIX Association.

[18] Joel Kirch. Virtual Machine Security Guidelines Version 1.0. The Center for Internet Security, September 2007.

[19] Discover the linux kernel virtual machine (April 2007), http://www.ibm.com/developerworks/linux/library/l-linux-kvm/.

[20] Xen, http://en.wikipedia.org/wiki/Xen#History.

[21] Xen Hypervisor - Leading Open Source Hypervisor for Servers, http://www.xen.org/products/xenhyp.html.

[22] Xen Documentation Support, http://www.xen.org/support/documentation.html.

[23] Xen Networking, http://wiki.xensource.com/xenwiki/XenNetworking.

[24] An Introduction to ARP Spoofing (Nov 2008), http://www.cse.iitm.ac.in/~jvimal/cs410/arp-spoof.html.

[25] B. R. Kandukuri, R. P. V. and A. Rakshit, "Cloud Security Issues ," in *Proceedings of the 2009 IEEE International Conference on Services Computing* , 2009, pp. 517-520.

[26] M. Jensen, J. Schwenk, N. Gruschka, and L. L. Iacono, "On Technical Security Issues in Cloud Computing," *Cloud Computing, IEEE International Conference on*, vol. 0, pp. 109-116, 2009.

[27] Cloud Security Is Not (Just) Virtualization Security (Nov 2009), http://whitepapers.zdnet.com/abstract.aspx?docid=1621585.

[28] Introducing Blue Pill (June 2006), http://theinvisiblethings.blogspot.com/2006/06/introducing-blue-pill.html.

[29] Wireshark, http://openmaniak.com/wireshark.php.