http://ansinet.com/itj

ITJ

ISSN 1812-5638

INFORMATION TECHNOLOGY JOURNAL

ANSInet
Asian Network for Scientific Information
308 Lasani Town, Sargodha Road, Faisalabad - Pakistan

Information Technology Journal 12 (23): 7774-7777, 2013
ISSN 1812-5638 / DOI: 10.3923/itj.2013.7774.7777

Research on the Security of Virtual Network with Xen Platform

[1]Hanqian Wu, [2]Wei Li, [3]Chuck Winer and [4]Li Yao
[1,2,4]School of Computer Science and Engineering, Southeast University, Nanjing, JiangSu, 210096, China
[3]Department of Computer Information Technology and Graphics, Purdue University Calumet, Hammond, IN, USA

Abstract: As the next generation of networking computing, cloud computing can offer both software and hardware as on-demand resources and services over the Internet and therefore reduce the capital expenditure and operational expenditure for IT consumers. In order to realize these purposes, however, there are still some challenges to be solved. With no doubts, security is the most concerned issue. This is why security must be integrated into every aspect of cloud computing. Virtualization is the key technology to build a cloud computing platform, as a result, virtualization security is one of the significant concerns in cloud computing. In this paper, we focus on the security of virtual network in virtualized environment. First, we research Xen platform which is the most popular hypervisor used in the industry and then the security problems that exist in a virtual network are discussed and analysed based on Xen platform. Finally this paper presents a multi-layer virtual network framework aimed to control the inter-communication among virtual machines deployed in physical machines with higher security.

Key words: Cloud computing, virtualization, xen, security.

INTRODUCTION

A key issue in virtualization is isolation. Isolation plays a crucial role in Virtual Machines (VMs) in order to guarantee that one VM cannot affect the other VMs running in the same host(Vaquero *et al*., 2009). Virtual network is a method of creating independent or isolating logical networks within a shared physical network. However, it is common that most hypervisors (i.e., VMWare EXSi, Virtual Box) offer virtual network to link VMs by using bride and route. This method of VM isolation can be easy to be broken. To address this risk, this paper selects open source project-Xen hypervisor as the research platform, then we propose a multi-layer virtual network framework aimed to control the inter-communication among virtual machines deployed in physical machines with higher security based on the combination of bridge and route mode.

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 (Armbrust *et al*., 2009). Virtualization, as the key technology of cloud computing, is to abstract the physical resources of a computer into many separate logical resources or computing environments(Jensen *et al*., 2009). The main purpose of virtualization is to improve the performance of a server by providing users Virtual Machines (VM) 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). The commercial world also proposes multiple products and technologies to support virtualization, such as Intel VT, AMD-V.

XEN HYPERVISOR

The software layer providing virtualization is called a virtual machine monitor or hypervisor. Hypervisors can be categorized into two types:

- **Native:** The native hypervisors run directly on the physical machine, such as Xen and VMware ESX/ESXi
- **Hosted:** The hosted hypervisors run within an OS environment. Examples of this type are VMware Server and Linux KVM

Xen is an X86 hypervisor developed by the university of Cambridge Computer Laboratory and released under the GUN General Public License. Today, Xen is becoming the fastest and most secure infrastructure virtualization solution and has become one of the most popular virtualization platforms.

Corresponding Author: Wei Li, School of Computer Science and Engineering, Southeast University, Nanjing, JiangSu210096, China

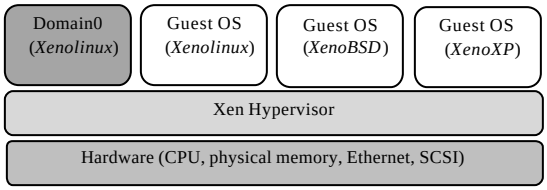

Fig. 1: Xen architecture

The Xen hypervisor abstracts the hardware for the virtual machines and fully controls the execution of the upper VMs with a set of control interfaces. 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 . Xen in turn may host multiple guest operating systems, each of which is executed within a secure virtual machine (in Xen terminology, a domain).

Figure 1 illustrates the s ystem structure of Xen (Barham *et al*.,2003). The first domain (domain0) is created automatically at boot time. Comparing with other domains, domain0 is a Xen build-in VM with special privileges. Domian0 is responsible for hosting the application-level management software and it can also use the control interfaces provided by Xen to create and terminate other virtual machines and to control their associated scheduling parameters, physical memory allocations and the access they are given to the hardware, such as: physical disks and network devices. Meanwhile, domain0 can create and delete the Virtual Network Interfaces (Vif)for VMs by using the control interfaces, these virtual I/O devices are always associated with access-control information to restrict other domain to access them.

VIRTUAL NETWORK IN XEN

Xen mainly provides 2 types of virtual networks to transfer packets between VMs and outside physical network: Bridging, Routing, both of them use Network Address Translation (NAT) mechanism.

Figure 2 shows the structure of Network Bridge and Virtual Network Interface (VIF)in Xen.

In this mode, Xen attaches the VM's interface directly to software Ethernet Bridge connected to the physical network. The channel interfaces found in dom0 are called back-end interfaces and as showing in Fig. 2 are labelled with "VifX.Y", where X identifies domU while Y is unique for the given domU's back-end interfaces. On the other side of the channel interfaces, found in the domUs, are called front-end interfaces, for example, ethY,

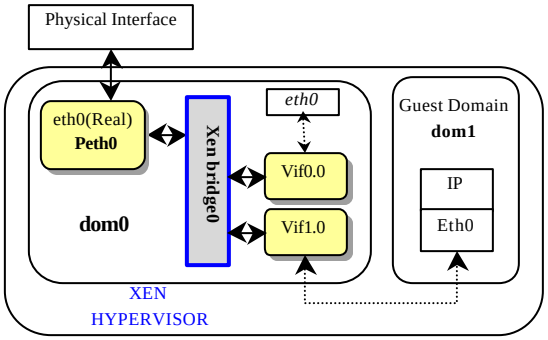

Fig. 2: Structure of Network-Bridge and VIF-Bridge in Xen

where Y identifies the front-end interfaces of domU and it represents the real network interfaces of the guest operating system running in domU.

The administrator can handle VM network DHCP requests the same way as handling common network DHCP requests. By default, when Xen starts up, Network Bridge in Xen 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 (domL) starts up, VIF1.0 and Bridge0 are attached and VIF1.0 is brought up, where "1" identifies dom1 while "0" is the identifier for the network interface of dom1.

The second mode offered by Xen for the configuration of virtual network is route, as showing in Fig 3. In routing configuration, the ethY interfaces of dom0 not only represent but are the real interfaces of physical NIC. 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. The steps to configure routing in Xen are as follows (Fig3):

- Enable IP forwarding within dom0
- Copy the IP address from eth0 to Vif1.0
- Bring up Vif1.0

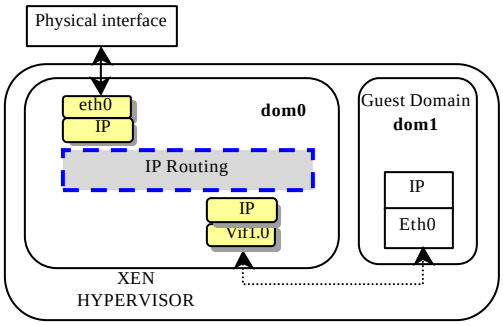

Fig. 3: Routed network in Xen

- Add host static route for dom1 IP and MAC addresses specified in dom1 config file and point at interface Vif1.0

VULNERABILITIES IN VIRTUAL NETWORK

The biggest security challenge in virtualization technology is to isolate the virtual machines hosted in the same physical server (Kirch, 2007; Garfinkel and Rosenblum, 2005). In the virtualized environment, virtual network plays the crucial role to isolate VMs. Actually, the ideal way of isolating each VM is to use dedicated physical channels 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 (Garfinkel and Rosenblum, 2005). 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 main vulnerabilities existing in the current virtual network (Dignan, 2008):

- 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 malicious VM is easy to sniff the virtual network by using sniff tool such as "Wireshark"
- 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 (Fig. 3). In this case, a VM can do an Address Resolution Protocol (ARP) spoofing, redirecting packets to them and be able to sniff packets going to and coming from other VMs

MULTI-LAYER VIRTUAL NETWORK MODEL

According to the analysis of vulnerabilities existed in the virtual network above, we leverage the characteristics

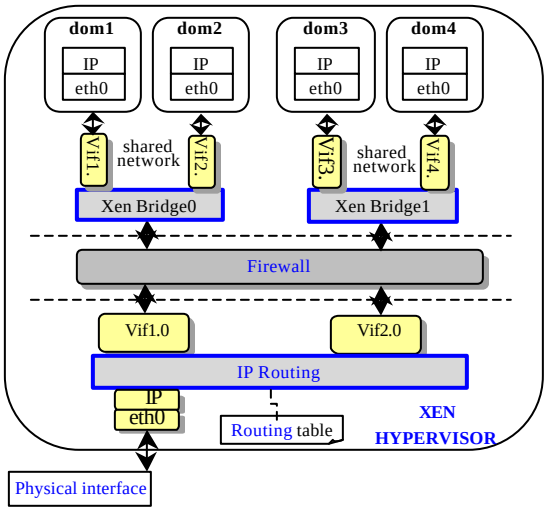

Fig. 4: Multi-layer virtual network model

Table 1: Structure of subnet table

Subnet	Network ID	Status	VM No.	Create time
10.10.1.0	0001	created	2	2011:12:20 12:30:36

of "route" and "bridge" modes and combine them to propose a multi-layer virtual network model to make the communication among VMs more secure. This model is divided into three layers: Routing layer, firewall and shared network, as shown in Fig. 4.

Shared network layer: Virtual bridge in Xen plays the same functions as shared network, 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 with unique network tag which can be identified by the next layer. So, we specify a set of subnets in advance and each shared network will be bound with a unique subnet by the administrator when a new shared network instance is created.

All the subnets are saved in a subnet table. The subnet table is responsible to record the status information of the subnet and the corresponding network ID as well. Table 1 shows the structure of the subnet Table.

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 cannot 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.

For example, "192.168.1.0" and "172.21.12.0" are two different subnets. The following script can stop the communication between the two virtual shared networks: access-list 101 deny ip 192.168.1.0 0.0.0.255 172.21.12.0 0.0.0.255.

access-list 101 deny ip 172.21.12.0 0.0.0.255 192.168.1.0 0.0.0.255.

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.

CONCLUSION

As we know, security is the user's most significant concern in cloud computing consumption (Whyman, 2008). In this study, we propose a multi-layer virtual network model 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.

ACKNOWLEDGMENTS

We would like to thank Porf.Chao, who is our vice dean, for giving me some constructive suggestions. We also thank the research group members of cloud computing in College of Software Engineering of Southeast University for helping construct the platform of Xen.

This work is supported by the National Natural Science Foundation of China under grant No.60803057.

REFERENCES

Armbrust, M., A. Fox, R. Griffith, A.D. Joseph and R.H. Katz *et al*., 2009. Above the clouds: A Berkeley view of cloud computing. Technical Report No. UCB/EECS-2009-28, February 10, 2009. http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

Barham, P., B. Dragovic, K. Fraser, S. Hand and T. Harris *et al*., 2003. Xen and the art of virtualization. Proceedings of the 19th ACM Symposium on Operating Systems Principle, October 19-22, 2003, Bolton Landing, USA., pp: 164-177.

Dignan, L., 2008. Virtualization: What are the security risks? http://www.zdnet.com/blog/security/virtualization-what-are-the-security-risks/821.

Garfinkel, T. and M. Rosenblum, 2005. When virtual is harder than real: Security challenges in virtual machine based computing environments. Proceedings of the 10th Workshop on Hot Topics in Operating Systems, June 12-15, 2005, Santa Fe, New Mexico, USA., pp: 20.

Jensen, M., J. Schwenk, N. Gruschka and L.L. Iacono, 2009. On technical security issues in cloud computing. Proceedings of the IEEE International Conference on Cloud Computing, September 21-25, 2009, Bangalore, India, pp: 109-116.

Kirch, J., 2007. Virtual machine security guidelines version 1.0. The Center for Internet Security, September 2007. http://benchmarks.cisecurity.org/tools2/vm/CIS_VM_Benchmark_v1.0.pdf

Vaquero, L.M., L. Rodero-Merino, J. Caceres and M. Lindner, 2009. A break in the clouds: Towards a cloud definition. ACM SIGCOMM Comput. Commun. Rev., 39: 50-55.

Whyman, B., 2008. Cloud computing. Information Security and Privacy Advisory Board, pp: 11-13. http:/ / csrc. nist. gov/groups/SMA/ ispab/documents/ minutes / 2008-12/cloud-computing-industry-trends-FISMA_ISPAB-Dec2008_B-Whyman.pdf