Secure Virtual Machine Migration in Xen Hypervisor

Thant Zin Tun
University of Computer Studies, Yangon
thantzintunster@gmail.com

Abstract

Nowadays, virtualization technologies become increasingly popular in enterprise and organizational networks: such as data center. In order to facilitate fault management, high-availability, load balancing and low-level system maintenance, live migration functionality of virtual machine (VM) is very essential. By carrying out the migration process, there are many research challenges. However, we only focus on security issue. There are different vulnerabilities, security threats and various prevention strategies. In this paper, the attacks which occur in live migration are firstly described. A secure VM migration framework using enhanced IPSec security strategy based on dynamic pre-shared key is proposed to prevent denial of service attack and man-in-the-middle attack. We design it on Citrix Xen open-source hypervisor. To evaluate how much secure in migration, state-of-the-art implementation is as part of future work.

1. Introduction

Datacenters are increasingly virtualized to reduce their total cost of ownership. Cost reductions are realized by sharing each hardware platform among multiple software workloads, with each workload running in its own set of virtual machines.

Virtualization technology is becoming increasingly common in datacenters, since it allows for collocation of multiple workloads, consisting of operating systems, middleware and applications, in different virtual machines (VMs) on shared physical hardware platforms. As virtualization technology becomes popular in many datacenter networks, operators and administrators are using live migration of virtual machines for the purpose of workload balancing and management. Live migration of virtual machines, the process of transitioning a VM from one virtual machine monitor (VMM) to another without halting the guest operating system, often between distinct physical machines, has opened new opportunities in computing. Live migration can aid in aspects such as high-availability services, transparent mobility, consolidated management, and workload balancing.

There are many ways in which a virtual machine can be moved from one VMM to another. Since virtual systems are typically stored as regular files on disk, the files associated with a halted system can be copied to another VMM using a network or using portable storage devices such as USB drives. In addition to the migration of halted virtual systems, many popular VMMs support live migration, the process of simply moving the VM running on a source node to destination node without disrupting any active network connections even after the VM is moved to the target node.

Despite the high availability of VM migration, security is still one of the major obstacles of virtual machines. In particular, there are novel concerns associated with virtual environments such as securing large numbers of virtual machines, securing a diverse range of operating mobile virtual machines that may move between different physical hosts and networks. Virtual machine monitor that incorporates a vulnerable implementation of live migration functionality may expose both the guest and host operating system to attack and result in a compromise of integrity. There are different attacks to live virtual machine migration.

Even if proper encryption and identity management is used, it still may be possible for an attacker to gain valuable information from snooping on a migration stream. The popular VMMs deployed in production networks, such as Xen and VMware, fail to implement even simple data plane protection to ensure guest OS integrity during live migration and are vulnerable to attack. This paper presents a framework to prevent the attacks which occurred in live virtual machine migration by using enhanced IPSec security strategy based on dynamic pre-shared key.

The rest of this paper is organized as follows. In the next section, the related work is discussed. In section 3, this paper classifies the virtual machine attacks. And then the architecture of IPSec is described in section 4. In section 5, proposed system architecture is introduced. It will be followed by conclusion in section 6.

2. Related Work

F. Hao, T.V. Lakshman et al. [5] proposed an architecture that takes advantages of network virtualization and centralized controller. Their architecture overcomes scalability limitations of prior solutions based on VLANs, and enables users to customize security policy settings the same way they control their on-site network. It can also enable users to combine cloud-based resources seamlessly with their existing network infrastructure through VPN.

J. Oberheide et al. showed how a malicious party using the attack strategies can exploit the latest versions of the popular Xen and VMware virtual machine monitors and present a tool to automate the manipulation of a guest operation system's memory during a live virtual machine migration [8]. They presented strategies to address the deficiencies in virtualization software and secure the live migration process.

VSITE, a scalable and secure architecture for seamless L2 enterprise extension in the cloud was proposed by Li Erran Li and Thomas Woo [3]. VISITE achieves abstraction through the use of VPN technologies, the assignment of different VLANs to different enterprises and the encoding of enterprise IDs in MAC addresses. It suppresses layer2 MAC learning related broadcast traffic. It also makes use of location IP for scalable migration support.

Fagui LIU et al. proposed a new method of building a bridge firewall based on Xen and developing independent extension of firewall for special purpose and to supervise the host and guest system to enhance the computer system security. They also presented the test for the functions and performance of firewall extension and analyze the outcomes [7].

The IBM trusted virtual Datacenter (TVDc) technology developed to address the need for strong isolation and integrity guarantees is implemented by S. Berger et al [1]. It significantly enhances security and systems management capabilities in virtualized environments.

A. S. Ibrahim, J. Hamly Harris and J. Grundy [6] discussed the existing security approaches to secure the cloud virtual infrastructure and their drawbacks. They proposed and explore some key research challenges of implementing new virtualization-aware security solutions that can provide the preemptive protection for complex and ever-dynamic cloud virtual infrastructure.

Many researchers proposed various solutions to enhance the security for virtualized datacenters. However there are security challenges for virtual machines migration. This paper pays attention the live virtual machines migration attacks and proposes the virtualized architecture to prevent these attacks.

3. Virtual Machine Migration Attacks

In this section, the attacks which occur in live migration are discussed. Although there are multiple features of virtualization that can be targeted for exploitation, the more common targets include VM migration and virtual networking functions. VM migration, if done insecurely, can expose all aspects of a given VM to both passive sniffing and active manipulation attacks.

3.1. Denial of Service Attack

A lack of proper access control may allow an attacker to arbitrarily initiate migrations. By initiating outgoing migrations, an attacker may migrate a large number of guest VMs to a legitimate victim VMM, overloading it and causing disruptions or a denial of service attacks.

3.2. False Resource Advertising Attack

In an environment where live migrations are initiated automatically to distribute load across a large number of servers, an attacker may be able to falsely advertise available resources via the control plane. By pretending to have a large number of spare CPU cycles, the attacker may be able to influence the control plane to migrate a VM to compromised VMM.

3.3. Man-in-the-Middle Attack

An attacker may be able to logically position himself in the migration transit path using a number of techniques such as ARP spoofing, DNS poisoning, and route hijacking. An inline attacker may manipulate the memory of a VM as it is migrated across the network. Such a man-in-the-middle attack may result in a complete and convert compromise of the guest OS. By monitoring the migration transit path and associated network stream, an attacker can extract information from the memory of the migration VM such as passwords, keys, application data, and other protected resources.

3.4. Migration Module Attack

The VMM component that implements live migration functionality must also be resilient to attacks. As the migration module provides a network service over which a VM is transferred, common software vulnerabilities such as stack, heap, and integer overflows can be exploited by a remote attacker to subvert the VMM. Given that VM migration may not commonly be viewed as a publicly exposed service, the code of the migration module may not be scrutinized as thoroughly as other code.

If an attacker is able to compromise a VMM through its migration module, the integrity of any guest VMs running within the VMM, and any VMs that are migrated to that VMM in the future, may also become compromised.

With the virtual machines migration, an attacker can conduct the attacks as illustrated in figure 1. The security of source and destination VMs is necessary for a secure migration.

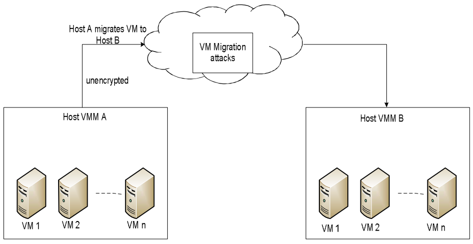

Figure 1. An attack against a live VM migration

4. IPSec Architecture

4.1. Second Order Heading

IPSec architecture is defined by a series of RFC document, the whole document consists of 8 parts, as shown in figure 2, in which the security architecture of IPSec includes the general concepts, security requirements, definitions and mechanisms, Encapsulating Security Payload (ESP) includes ESP encryption/authentication specification Authentication Header (AH) includes specifications about the AH authentication package, the encryption algorithm describes various encryption algorithms used in ESP, the authentication algorithm describes various authentication algorithms used in AH and ESP, key management describes the key management mechanism: IKE and strategy, domain of interpretation includes some parameters relative to other documents, such as recognized encryption algorithm identification and authentication algorithm is identification , and key life cycle parameters [2].

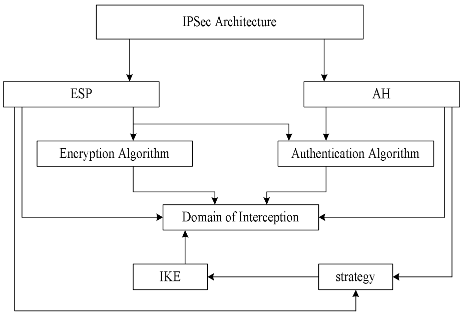

Figure 2. Structure of IPSec documents

4.2. IPSec Mechanism

Security Association (SA) is the basis for IPSec, which determines the security parameters used in communication such as IPSec security protocol, hash function, encryption algorithm and key.

IPSec uses two mechanisms: Encapsulating Security Payload (ESP) and Authenticated Header (AH), AH provides an integrity protection, anti-replay and access control, while ESP provides confidentiality and traffic control as well as those services provided by AH. According to the difference of the content of the payload, these two mechanisms have two modes: transport mode and tunnel mode. Transport mode provides protection for upper level protocol, the IPSec header (AH/ESP) is inserted between the IP header and the transportation layer header, the package structure is as shown in figure 3. In tunnel mode, the entire IP packet is encapsulated in a new IP packet, and the IPSec (AH/ESP) header is inserted in between the original IP header and the new IP header, the structure is shown in figure 4.

IP Header	IPSec Header	TCP Header	Data

Figure 3. Structure of the transport mode packet

New IP Header	IPSec Header	IP Header	TCP Header	Data

Figure 4. Structure of the tunnel mode packet

4.3. IPSec Key Management

There are two ways to generate keys used in security associations. One is the manual mode, the other one is IKE (Internet Key Exchange) automatic negotiations. In practical application, the configuration of the former is relatively complex, the information needed in creating the security association needs to be manually configured, and some advanced features of IPSec (such as periodic key update) are not supported. But its advantage is that the functions of IPSec can be realized without IKE. IKE is relatively simple, once the security policy information is configured, the IKE will create and maintain SA automatically.

In the case of the number of communications devices is small or in a static environment, the establishment of the security association manually is feasible. But for medium and large-scale dynamic network environment, SAs should be established by IKE.

IKE is used to establish security associations dynamically, and to negotiate information needed by IPSec such as encryption algorithm, keys, identity. IKE is a hybrid protocol, which is built on the framework defined by ISAKMP (Internet Security Association and Key Management Protocol), and uses the key exchange mode of Oakley and the share and re-key techniques of SKEME (Secure Key Exchange Mechanism). IKE has two phases which negotiate and create security associations for IPsec. The first phase establishes IKE SA, the second phase negotiate IPSec SA using this existing SA.

4.4. Second Order Heading

In the pre-shared key authentication, communication parties generate four kinds of keys from the pre-shared key and other materials using pseudo random function: SKEYID,

SKEYID-d, SKEYID-a, and SKEYID-e. The keys in pre-shared key authentication method are derived as follows:

SKEYID=PRF(pre-share-key, $N_i|N_r$)
SKEYID-d=PRF(SKEYID,g^{xy}|CKY-I|CKY-R|0)
SKEYID-a=PRF(SKEYID,SKEYID-d|g^{xy}|CKY-I|CKY-R|1)
SKEYID-e=PRF(SKEYID,SKEYID-a|g^{xy}|CKY-I|CKY-R|2)

N_i is the random number of the initiator, N_r is the random number of the responder, g^{xy} is the shared secret key from the Diffie-Hellman exchange, CKY-I, CKY-R are the cookies of the initiator and the responder.

To enhance the security, the pre-shared key should be dynamically generated before the SA negotiation. This way the security of the system will not be threatened even if the pre-shared key was cracked. The dynamic pre-shared key generation method with enhanced security is as follows: (suppose the initial pre-shared key by A and B is K_{ab}):

(1) A generates random number N_a, xor it with K_{ab} and sends the result $K_{ab} \wedge N_a$ and its ID I_a to B.

(2) B gets Na from $K_{ab} \wedge N_a \wedge K_{ab}$, then B generates random number N_b and sends Hash（N_a）together with $K_{ab} \wedge N_b$ and its ID I_b to A.

(3) A authenticates Hash(N_a), gets N_b from $K_{ab} \wedge N_b \wedge K_{ab}$ and sends Hash（N_b）to B.

(4) B authenticates Hash(N_b).

(5) If each party passes authentication, A and B use $N_a||N_b$ as the new pre-shared key.

The improved method is easy to compute and efficient. For passive attackers, even if they have access to $K_{ab} \wedge N_a$ and $K_{ab} \wedge N_b$, as they don't know K_{ab}, they cannot extract $N_a||N_b$. For active attackers, they may be able to disguise as the sender or recipient, the genuine sender and the recipient can be verified by authenticating Hash(N_a) or Hash(N_b), therefore avoids man-in-the-middle attack. Every time when the SA is created, new pre-shared key will be automatically generated, the drawbacks of fixed pre-shared key are thus avoided, and the security of the system is enhanced. In the negotiation process of the new pre-shared key, the attacker can get Hash (N_a), Hash(N_b), under the protection of the current Hash function, the attacker could not crack N_a and N_b within limited time, because the pre-shared key is dynamically generated, the act that the attacker spends lots of energy to crack the pre-shared key in order to enter the system is made meaningless. In addition, the pre-shared key negotiation before the SA establishment has the function of two-way authentication, if the authentication is not successful, the SA establishment will not start. So the improved method can effectively resist the DoS attack on Diffie-Hellman exchange.

5. Proposed System Architecture

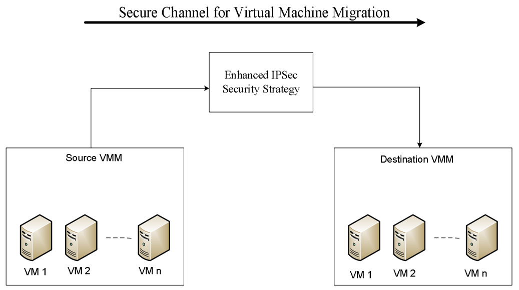
Secure Channel for Virtual Machine Migration
Enhanced IPSec Security Strategy
Source VMM
Destination VMM
VM 1
VM 2
VM n
VM 1
VM 2
VM n

Figure 5. Proposed system architecture for VM migration security

There are security challenges in the virtualization technology because of different vulnerabilities and security threats to virtual machine migration. Traditional solutions do not map well to the virtualized environments, because of the complex and ever-dynamic nature of the virtualization. The proposed system combines the enhanced IPSec strategy based on dynamic pre-shared key with the virtualization technology.

The enhanced IPSec provides data authentication, integrity and confidentially with AH authentication header, ESP-Encapsulation security payload and IKE-internet key exchange. The proposed system architecture in figure 5 uses the enhanced IPSec protocol to prevent the different virtual machine migration attacks mentioned in section 3. IPsec protocol increases data security when migrating virtual machines. It will be implemented by authenticating source and destination virtual machine when migrating.

The system architecture enhances the security of virtual machine migration by using the enhanced IPSec strategy based on dynamic pre-shared key.

6. Conclusion

With the development of virtualization technology and the increasing demand of load balancing and management of migration, the security systems based on virtual machine are getting more and more popular. This paper discussed the different attacks of live virtual machine migration and proposed the system architecture using the enhanced IPSec strategy based on dynamic pre-shared key. As an ongoing research, we will implement this architecture on Xen open-source hypervisor. Detailed implementation and evaluation of how much secure in migration are part of the future work.

References

[1] S. Berger, R. Caceres, D. Pendarakis, R. Sailer, E. Valdez, “TVDc: Managing Security in the Trusted Virtual Datacenter.”

[2] A. V. Cleeff, W. Pieters, R Wieringa, “Security Implications of Virtualization.” in *International Conference on Computational Science and Engineering, 2009.*

[3] L. Erran Li, T. Woo, “VSITE: a scalable and secure architecture for seamless L2 enterprise extension in the cloud.”

[4] W. Huang, F. Kong, “The Research of VPN on WLAN.” in *International Conference on Computational and Information Science, 2010.*

[5] F. Hao, T. V. Lakshman, S. Mukherjee, H. Song, “Secure Cloud Computing with a Virtualized Network Infrastructure.”

[6] A. S. Ibrahim, J. Hamly Harris and J. Grundy, “Emerging Security Challenges of Cloud Virtual Infrastructure.” in *Proceedings of APSEC Cloud Workshop, Sydney, Australia, 30th Nov 2010.*

[7] Fagui LIU, Xiang SU, Wenqian LIU, Ming SHI, “The Design and Application of Xen-based Host System Firewall and its Extension.” in *International Conference on Electronic Computer Technology, 2009.*

[8] J. Oberheide, E. Cooke, F. Jahanian, “ Empirical Exploitation of Live Virtual Machine Migration.”