Study of Cloud Computing Security System Based on Rotational Stations

Qin Jiancheng
School of Electronic and Information Engineering
South China University of Technology
Guangzhou, China
e-mail: dragon_2k@21cn.com

Zhong Yu
School of Software
South China University of Technology
Guangzhou, China

Hu Jinlong, Lu Yiqin
Information Network Engineering and Research Center
South China University of Technology
Guangzhou, China

***Abstract*—With the rapid development of the cloud computing, the information security on the cloud platform becomes more and more important. To improve the defense abilities of the VM (Virtual Machine) platform, this paper presents a new cloud computing security system named "Alcyoneus system" based on rotational stations. Alcyoneus system uses dual layer network architecture. The VMs in its business layer like guards in the rotational station. The rotated background VMs can automatically recover and switch back to the foreground. This is implemented by the real equipments in the support layer. The experiment results reveal that Alcyoneus system can rapidly clean the attack effects in the VMs, so it can protect the cloud platform efficiently.**

Keywords-cloud computing security; virtual machine cluster; rotational station

I. INTRODUCTION

With the rapid development of the cloud computing, the information security on the cloud platform becomes more and more important. The VM (Virtual Machine) environment makes the network security complex. A cloud platform may contain hundreds of VMs which are under various threats such as viruses, warms and network attacks. How to protect so many VMs is a real problem.

At the same time, the world of the VMs may open a new space for the security defense. The VMs can be created, destroyed, copied and moved dynamically. These functions are helpful for the security protection.

This paper presents a new cloud computing security system named "Alcyoneus system" based on rotational stations. Alcyoneus system uses dual layer network architecture. The business layer is made up of VMs, and the support layer is made up of real equipments which can implement the business layer and provide computing resources to the VMs. In the business layer, the virtual routers can regularly switch some VMs between the foreground and the background like guards in the rotational station. The background VMs can automatically recover from the system snapshot and reboot, so they can clean the attack effects in themselves including unknown viruses, worms, Trojan horses and even the 0-day attacks.

The remainder of this paper is structured as follows: Section 2 discusses the security problems of the cloud platform and the related works. Section 3 introduces the design of dual layer network architecture in the cloud platform. Section 4 describes the design of Alcyoneus system. Section 5 provides a solution to keep users' data in VMs. Section 6 gives the experiment results. Conclusions are given in section 7.

II. CLOUD SECURITY PROBLEMS AND RELATED WORKS

The problem of the network defense is always the focus of the information security research. With the development of cloud computing, this problem has new conditions which can't be easily solved by traditional defending ways.

1) VMs are widely used. A cloud platform may contain hundreds of VMs and they are dynamic. That makes the situation of network security more complex.

2) Different ways of network attacks are appearing endlessly. 0-day attacks aim the new leaks of the systems which are unknown by most of the technicians. APTs (Advanced Persistent Threats) hide deeply inside the systems and harm the targets imperceptibly. The system patches for VMs can't keep up with the attacks.

3) Various viruses, worms and Trojan horses are emerging in an endless stream, and they renew rapidly. Common anti-virus softwares have not enough abilities to promptly protect the VMs in the cloud.

4) Automatic attacking tools are generated continuously. Attackers don't need high techniques to use them. Common firewalls have not enough interceptor abilities to protect so many VMs in the cloud.

To treat the problem of the cloud platform defense, related works are studying how to use the new techniques of the cloud computing to improve the security defense abilities of VMs.

Virtual computing can conceal the different details of the basic equipments and structures. If the VM computing is cleverly used, it can simplify the cloud management and improve the security. Paper [1] uses the cloud to provide security services and analyzes the effects. Paper [2] uses the cloud to find the malicious attacks. Paper [3] presents a next generation Internet architecture based on virtual networks. Paper [4] introduces the VM cluster.

Generally, current practical ways to protect the cloud security are still useful, but in the new conditions, they have some shortages.

1) Anti-virus softwares are not powerful enough to deal with the new polymorphic viruses armed with the code obfuscation and shell encryption techniques. The updates of the softwares can't keep up with the changes of viruses.

2) Firewalls can't detect and block all of the attacks in the condition of lots of VMs and various automatic attacking tools. The burden of firewalls in a cloud is heavy and hard.

3) The system patches can't prevent 0-day attacks and APTs in time. The 0-day attacks always come before the system patch updates. APTs are designed elaborately to avoid the security defense. Thus the attacks usually succeed.

4) System reinstallation may clear the previous attack effects such as rootkits, Trojan horses and viruses. But even the system clone is not quick enough to keep the VMs clean. It isn't feasible to reinstall the VM system every 5 minutes.

The above techniques are not enough to defend the cloud. Attackers still have enough time and chances to intrude the VMs. This paper presents the design of dual layer network and Alcyoneus system which can cover the defense shortages.

III. Design of Dual Layer Network Architecture

The main idea of Alcyoneus system is: Each server node in the cloud is regarded as a rotational station for more than 2 VMs. These VMs work in the same station by turns like guards on duty. For instance, a node in the external network may see a web server in the cloud, but actually there are 3 VMs acting as this server by turns.

For each station there is always one and only one VM working in the foreground to provide the service for the cloud. The other VMs are in the background and execute the batch operations of system shutdown, restore and reboot. Thus even if the foreground VM is attacked, once it is time to rotate the VMs, a brand-new VM from the background will replace the foreground VM. All the attackers' previous efforts such as password cracking and rootkit planting will be in vain.

In the virtual computing environment such as VMware, the design of dual layer virtual network is helpful to make full use of the VM advantages. Fig. 1 shows the dual layer network architecture in Alcyoneus system.

In this dual layer network, the support layer in the bottom side is made up of real hardware equipments which form the VM container clusters. The business layer in the top side is made up of VM clusters. The business layer bears all the work of connecting to the external network and providing services. The support layer only provides computing resources to the business layer and keeps it running. The external network can't access the support layer directly.

VMs like computer viruses which can clone, recover and move in the network. VMs are more complicated than viruses. They have operating system cores and they can run applications. This paper regards VMs as computer cells. Because the business layer is made up of cells, it has the ability of software self-recover.

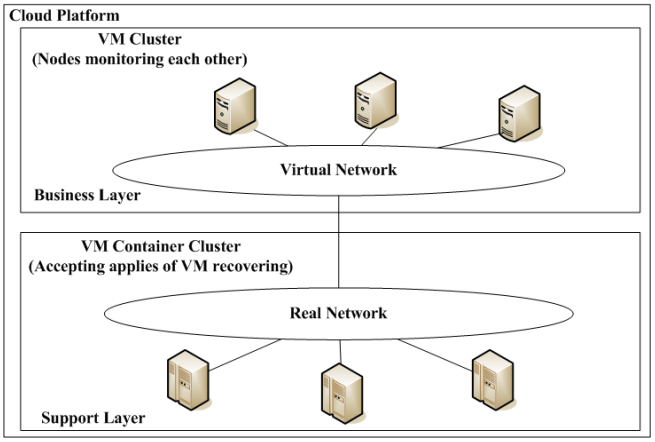

Figure 1. Dual layer network architecture.

We implement the VM self-recover function by C/C++ programs. It's not necessary to use a VM monitor, because the VM software such as VirtualBox provides the APIs (Application Programming Interfaces) or command line operations to start and stop VMs, and the immutable VDIs (virtual disk images) make it faster to recover a VM: just reboot the VM system.

We also implement the function of switching VMs in the network by C/C++ programs. It's not necessary to use the SDN (Software Defined Network[5]), because the VM software also provides the APIs or command line operations to change the network connections of the VMs.

IV. Design of Alcyoneus System

Fig. 2 shows the system of rotational stations named "Alcyoneus system" which is made up of at least 2 VMs, a virtual router and a real equipment.

Nodes from the external network can only see various nodes in the cloud, such as web servers, database servers, etc. In fact, each node in the cloud is a station. VMs work in this station by turns.

Alcyoneus system uses the dual layer network architecture. So the network is divided into 2 layers: the business layer is a virtual network, and the support layer is a real network.

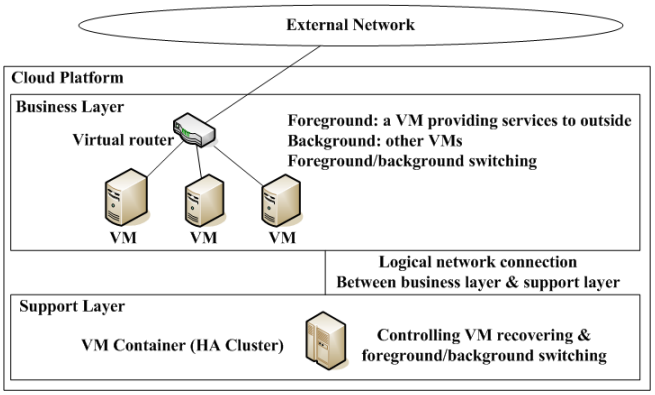

Figure 2. System of rotational stations.

In the business layer, 2 or more VMs working for a same station have same functions, e.g. the VMs are all web servers. Each VM may have different operating system or system configuration such as account, password, directory, etc. There is only one VM in the foreground, and other VMs are in the background. The virtual router switches the VMs to the foreground or background automatically. The foreground VM has routes to the external network, and the background VMs don't connect to the outside.

The background VM batches of system shutdown, restore and reboot won't affect the work of the foreground VM. A foreground VM falls back to the background, takes the above recovering batches and becomes a brand-new VM. Then this VM will rotate to the foreground by turns.

Fig. 3 shows the VM rotation process of Alcyoneus system.

In the support layer, VM containers proceed the following work:

1) Controlling the VMs and the virtual router.

2) Executing the batches of VM rotation, shutdown, restore, reboot and foreground/background switch.

3) Detecting the VM status and controlling the change of routes.

Each VM has 3 statuses: running, ready and recovering. The running status requires the VM is in the foreground, and the recovering and ready statuses require the VM is in the background. Each VM changes the 3 cyclic statuses endlessly.

1) A foreground VM is in the running status and provides services to the external network.

2) When a VM in the foreground returns to the background, its status changes from running to recovering. This needs the operations of system shutdown, restore and reboot.

3) After a successful reboot, a VM regains a brand-new system. The support layer checks whether it can provide services normally. Then it will be in the ready status and wait for the rotation to the foreground.

4) When the time of automatic rotation comes, the VM container uses the virtual router to switch this ready VM to the foreground, and this VM provides services to the external network again.

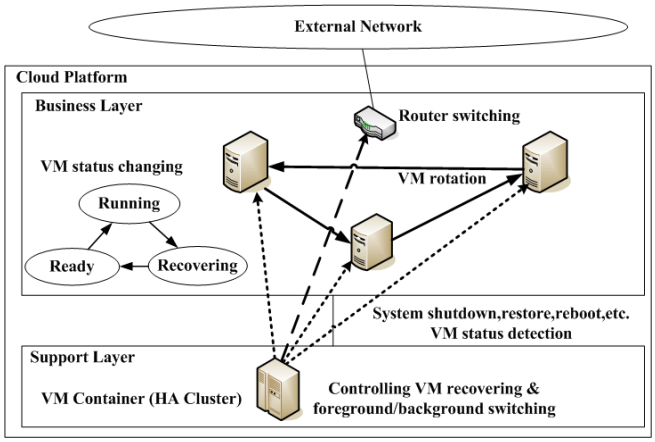

Figure 3. Process of VM rotation.

Fig. 4 shows the control flow of the VM container in the support layer.

In each cycle (typically 5 minutes), the VM container chooses a VM in ready status, switches it to the foreground and the former foreground VM to the background by controlling the virtual router, and then controls the former foreground VM to execute the batches of system recovering in the background.

After system recovering and rebooting, the brand-new background VM mentioned above is checked by the VM container. If it can provide services normally, it comes to the ready status in the background.

For each work station, there is only one foreground VM in a time. The amount of other VMs in recovering or ready status is not limited.

V. SOLUTION OF DATA KEEPING

The system recovering operations can clear the attacking effects to the VMs, but some VMs need to store users' data. We use multiple ways to treat different situations:

1) To face the external network directly, we use unchangeable VMs, e.g. firewalls, proxy servers, static webpage servers, etc. The network connections may be cut by the VM switching occasionally, but they can quickly recover.

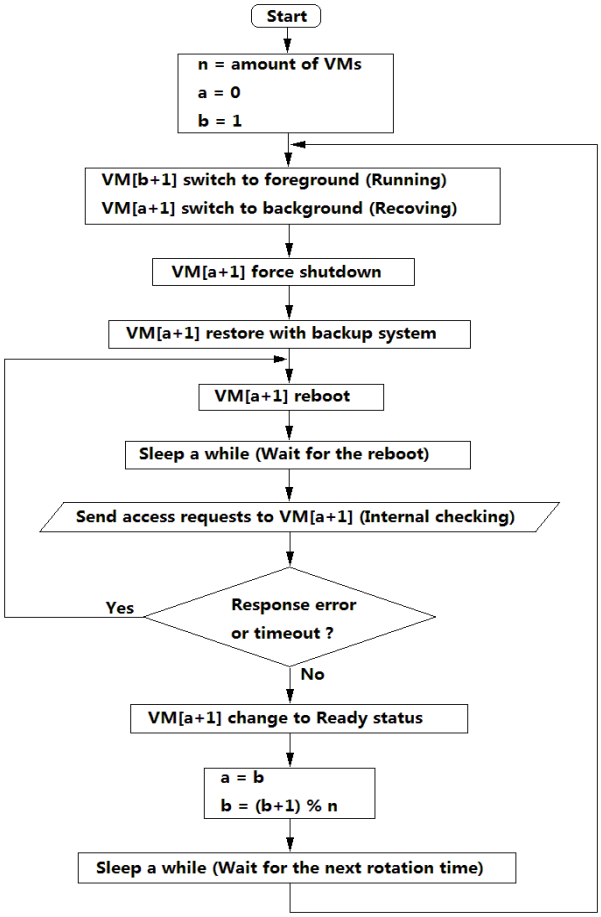

Figure 4. Control flow of VM container.

2) REST (Representational State Transfer) programming for web servers is another way to avoid storing data in the VMs. The information may be kept the browsers and URIs (Uniform Resource Identifiers).

3) Some VMs have to keep users' data, e.g. database servers. We use writable data VDIs which are different to the immutable system VDIs. And during the VM switching, the VM clusters may help to avoid the loss of the data.

4) To prevent the attackers from storing malicious data in the VMs, we develop a formalized pattern named IASI (International Airport Secure Inspection) to check the input data. IASI uses multiple barriers to filter illegal inputs like the international airports preventing terrorists among the passengers. E.g. one of the barriers is using FSMs (Finite State Machines) to validate the input data. Another is the identity authentication. IASI is an effective secure pattern, but in this paper we don't focus on it.

VI. Experiment Results

To test the defense performance of Alcyoneus system, we do a simulated attacking experiment. In the internal laboratory environment, our tester uses the SQL injection to attack a web server in our cloud which is deployed Alcyoneus system. The experiment platform includes the following real and virtual equipments: In the support layer, a blade server (Intel 4-core CPU, 32GB RAM, 500GB RAID5 HDD) is the VM container. In the business layer, 3 VMs (Linux, Apache, MySQL, PHP) take the duty of a web server rotational work station, and a Linux VM acts as a virtual router. These 3 web server VMs relieve guard by turns once per 5 minutes. And from the sight of the external network, only a common web server in the cloud is seen.

We leave a security leak of SQL injection in these 3 web server VMs, and constantly take a SQL injection attack from the external network to this "common" web server, distorting its homepage. At the same time, in order to observe the attack effects, we put a web browser in the external network, accessing the homepage of the web server once per 3 seconds.

The experiment results reveal that Alcyoneus system can continuously maintain the services in the cloud, and efficiently clear the malicious attacking effect.

1) All of the browser accesses can open the homepage in 3 seconds. That indicates the rotational routine don't affect the normal web service to the external network.

2) After each SQL injection attack, the browser accesses the homepage and sees it is distorted. That indicates the attack to the web server gets temporary success.

3) Not more than 5 minutes (average 2.5 minutes) later than the SQL injection attack, the browser accesses the homepage and sees it is recovered automatically. That indicates the effect of the attack is cleaned.

Compared to the traditional webpage protecting systems, Alcyoneus system can recover the whole VM system. It is not against the specific security attacks. That means it can clear the effects of unknown attacks, e.g. 0-day attacks, polymorphic viruses, encrypted Trojan horses, etc.

VII. Conclusions

This paper presents Alcyoneus system, a cloud defense system based on rotational stations. This system uses dual layer virtual network architecture. The support layer in the bottom side has real equipments which bear the tasks of running VMs, and the business layer in the top side has VMs which provide services to the external network.

In the business layer of Alcyoneus system, multiple VMs switch to the foreground by turns like guards on duty, which force the attackers always facing a new installed VM. The VMs switched to the background can recover automatically and clear all the effects of attacks. This is implemented by the real equipments in the support layer.

The experiment results reveal Alcyoneus system can cut off the malicious attacking effects within 5 minutes. Then the effects will disappear as soon as the VM is switched to the background, and with the VM system fast recovery, the effects will be cleaned.

This experiment isn't against the specific security attack. Thus if we cancel the SQL injection attack and use another attacks, e.g. polymorphic viruses, encrypted Trojan horses, 0-day attacks, APTs, etc., the effects will also be cleaned in time. That indicates Alcyoneus system in the cloud has certain abilities to defend unknown attacks.

References

[1] Salah K, Alcaraz C, Zeadally S, Al-Mulla S, Alzaabi M. "Using Cloud Computing to Implement a Security Overlay Network", Journal of IEEE Security & Privacy, 2013, 11(1), pp. 44-53.

[2] Chen Z, Han FY, Cao JW, Jiang X, Chen S. "Cloud computing-based forensic analysis for collaborative network security management system", Journal of Tsinghua Science and Technology, 2013, 18(1), pp. 40-50.

[3] Jin DP, Li Y, Zhou Y, Su L, Zeng LG. "A virtualization-based network architecture for next generation internet", 3rd International Conference on Anti-counterfeiting, Security and Identification in Communication, 2009, pp. 58-62.

[4] Grit L, Irwin D, Yumerefendi A, Chase J. "Virtual machine hosting for networked clusters: building the foundations for 'Autonomic' orchestration", 1st International Workshop on Virtualization Technology in Distributed Computing, 2006, pp. 7-7.

[5] McKeown N, Anderson T, Balakrishnan H, Parulkar G, Peterson L, et al. "OpenFlow: Enabling Innovation in Campus Networks", Journal of ACM SIGCOMM Computer Communication Review, 2008, 38(2), pp. 69-74.