Multimed Tools Appl (2015) 74:6381–6390
DOI 10.1007/s11042-014-2109-9

A study on stable web server system using virtualization technology against attacks

Hwan-Seok Yang · Dong-Hwi Lee · Seung-Jae Yoo

Received: 10 April 2014 / Accepted: 12 May 2014 / Published online: 23 May 2014

Abstract Computing environment has greatly changed by development of computing technology and distribution of extensive network. But the damage is taken seriously while attack techniques are diverse and attack target also is increasing. Thus, the normal network service should be done coping with these attacks actively. In this study, we propose new technique that can provide collection of attack information using virtualization technology and stable web service. The collection of attack information is done dynamically in honey system and managed by HSC. The continuous service of web server is performed by LBC. The superior performance of proposed method is confirmed through experiment.

Keywords Virtualization · Computer security · DoS attack · Honeypot

1 Introduction

Computing environment has been changed greatly and internet user has been increased rapidly due to development of network technology [10]. On the other hand, security incidents in many areas are increasing. These damages cause more damages that critical information assets or customer information of corporate and individual are easily leaked outside. The recent attack techniques are more intelligent and various. So, it is not easy to prepare for this. Information protection method about attack of illegal intruders via the internet is firewall, Intrusion Detection System (IDS), and Intrusion Prevention System (IPS). DoS/DDoS attack among them is that detecting attack is not easy because the kind is various and the damage is very large than the other type of attack. Web server is one of the main targets of DoS/DDoS attack and stop service of web server can result in serious damage socially [1, 8, 9]. That the web

H.-S. Yang · S.-J. Yoo (✉)
Department of Information Security Engineering, Joongbu University,
101, Majeon-ri, Chubu-myeon, Geumsan-gun, Chungnam, South Korea
e-mail: sjyoo@joongbu.ac.kr

H.-S. Yang
e-mail: yanghs@joongbu.ac.kr

D.-H. Lee
Department of Industrial Security, Kyonggi University,
San 94-6, Iui-Dong, Yeongtong-Gu, Suwon, South Korea

server provides a continuous service is important even though DoS/ DDoS attack happens. Information collection about new types of attack is a very important factor influencing the performance of the security system because most of the security systems prepare to attack against known vulnerabilities. The honeypot is resources being attacked deliberately to find out attack methods and means of attacker. Building honeypot similar to the real system is too expensive and difficult to set location [5].

In this paper, we propose new technique that provides a stable web service even external attack. It is possible to prepare to this actively by consisting honey system using virtualization technology and collecting attack information of attacker. We propose a technique that the honeyVM consisting honey system can be created and deleted dynamically considering the amount of resource usage of host system. And we propose virtual server system that the service by backup server can be continued if overload by DoS/DDoS attack occurs while several web servers are consisted in virtual environment and usually two web servers provide service. The technique that continuous service can be done even though any attack or impediment occurs is proposed.

The organization of this paper is as follows. In section 2 described virtualization technique and honeypot and web service technology using virtualization technique is described in section 3. In section 4, the performance of the proposed method is evaluated and finally, section 5 concludes the paper.

2 Related work

2.1 Network security threats

Network security threats are diverse depending on the target and type. In particular, the most typical attack type among them is divided into three [3, 4]. It is network sniffing, spoofing, and denial of service. Sniffing attack as attack which destroys confidentiality intercepts all packets, acquires ID or password of a specific system, and attacks another system. Spoofing attack forges IP as it is sent from a trusted host and the unauthorized user get certification on the system. Even today, several attack techniques using TCP/IP weak point are constantly appeared. DoS/DDoS attacks structural vulnerability of a system or network and is depleted resources not to be able the normal service. This attack can be divided into flooding attack causing mass traffics, connection attack requesting excessive session, and attack utilizing other application characteristics. Flooding attack depletes the resources of the Target system and network by sending randomly normal packet and disturbs normal service provision. Connection attack is divided into HTTP attack and TCP attack, and disturbs normal connection to server by exceeding linkable value. Application-based attack uses vulnerability of many protocols using various applications and is divided into DNS attack and RPC attack. Table 1 shows characteristics of network attack type.

2.2 Virtualization technology

Virtualization Technology is used in the overall IT field of network, server, storage, etc. by entering cloud computing environment providing user-centered service [7, 11]. In particular, it has many advantages of the application increase, cost reduction, a variety of scalability, and enhanced provisioning due to re-utilization of resources in terms of infrastructure. And, it can divide one physical system into several logical systems or combine multiple physical systems into one logical system. Like this, virtualization technology is being applied in a variety of

Table 1 Types and characteristics of network attacks

	Attack Technique	Characteristic
Sniffing	• ARP Redirect • ICMP Redirect • Switch Jamming	• Data theft of system accounting information
Spoofing	• ARP spoofing • IP spoofing • DNS spoofing	• Data theft and falsification by service characteristic
DoS/DDoS	• SYN flooding • Land • Smurf • Ping of Death	• Reliability depression by paralyzed of server or network service

areas [12]. Server virtualization among this allocates physical hardware resources to the multiple virtual machines and provides services using each required resources. It constitutes hypervisor on the one server like Fig. 1 and installs multiple operating systems independently. Here, the hypervisor is management software that resources such as physical processor or memory server are made available to virtual.

A representative function of server virtualization is share, aggregation, emulation, and insulate. The share function means that one same physical resource connects with multiple virtual resources and is a virtual disk, virtual LAN, virtual machine, etc. An aggregation as opposed concept of share is that virtual resource can be made using multiple physical resources and managed easily. The following Table 2 shows type, advantages and disadvantages of these server virtualization technologies.

2.3 Honeypot

Honeypot is system having the characteristics that should look to be vulnerable and easily exposed to collect information about attack tool or means of attacker [2]. Log server and IDS is essential factor to configure honeypot. In case that honeypot locates in front of firewall, the risk of internal network by honeypot attack is low. But efficiency is poor because occurred invalid data is increased. If honeypot locates behind firewall, efficiency is high and the risk of internal network is increased. In addition security level of the internal network is debased because filtering rules of firewall is affected. These honeypot can be classified production honeypot to strengthen security of organization or specific environment and reduce the risk and research honeypot to get information about hacker community and research. Honeypot can

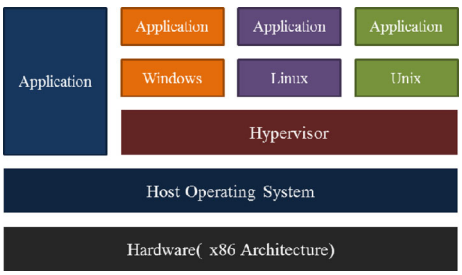

Fig. 1 Server virtualization architecture

Table 2 Compare features of server virtualization

Type	Advantage	Disadvantage
Full Virtualization	• Any operating system can be installed. • No need to modify the kernel	• Overhead process
Para Virtualization	• Faster execution speed	• Requires modification of the kernel • Not available of OS that kernel modification is not possible
OS-Level Virtualization	• Available Distribution of hardware resource • Independent operation between the servers is available	• All virtual servers use the same operating system

be classified into following three stages by the degree of interaction performing with attacker [6]. Low level allows access for only specific ports and doesn't provide service. And the attacker can login attempts and do only very limited interaction. Medium level provides limited service environment and provides in the form of virtual service acting like actual service. High level provides practical OS and all services. So, a lot of information can be gotten but the risk that gives damage to other system has had.

3 Proposed method

In this section, we explain technique that actively copes with an external attack through collection of attack information such as DoS/DDoS using honeynet and web service provides normally even if a particular attack using virtualization technology.

3.1 System architecture

In this study, we propose honeynet system to provide service while web server is protected from a variety of attacks securely. Honeynet system proposed in this paper is largely composed of honey system and virtual server system. Honey system configures the honeypot dynamically in order to provide many resources to attacks using virtualization technology. It consists of honeyfarm being made up of honeyVM for collection of attack information, Honey System Controller (HSC) that performs practical management of creation and deletion of honeyVM, and Load Balancing Controller (LBC) to evenly distribute load of web server. There are three web server and a database server in the virtual host system. Web server is performed by connecting database server and each web server to NFS using RPC. Figure 2 shows the structure of the proposed honeynet system.

3.2 Honey system management

The attack information collection of attacker is performed in honeyVM consisting of honeyfarm. The honeyVM must be created a lot in order to obtain more information about attack technique because the more this honeyVM is many, the more resources are provided. But, the performance of the system is deteriorated if honeyVM is many. Therefore, Mamdani fuzzy inference is used to determine dynamically the number of honeyVM considering the resource usage. The input variables of host system to determine the number of honeyVM generation is CPU and the amount of used memory. And indicator of variables is set largely low(20 %), medium(50 %), and high(80 %). CPU and the amount of used memory are applied

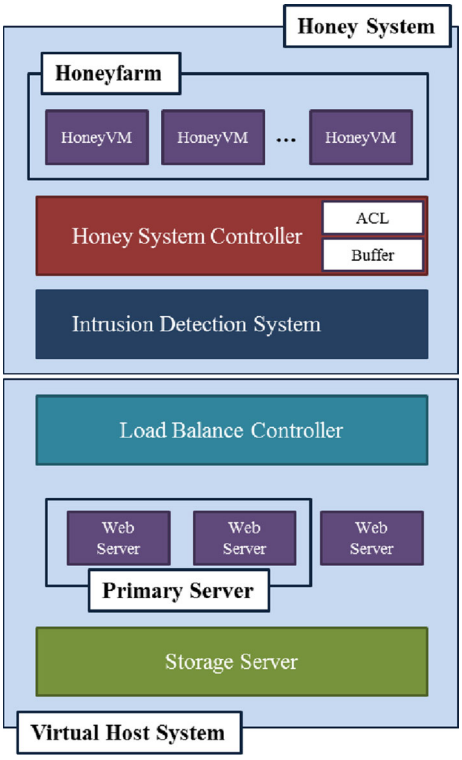

Fig. 2 The structure of proposed honeynet system

to membership function after it accepted from fuzzy input evaluates rule. Then COG(Center Of Gravity) method, equation s1, is used to determine the number of honeyVM generation.

$$COG = \frac{\int_a^b x\mu_A(x)dx}{\int_a^b \mu_A(x)dx} \tag{1}$$

The generated honeyVM like this is generated and operated within the range which is not given load to the host system. The collected attack information by honeyVM is analyzed by IDS. By doing so, coping with new attack actively is possible and attack of internal packet between honeyVMs is detected.

The creation and deletion of honeyVM consisting honey system is managed in HSC and monitoring function of internal traffic between each honeyVM is performed. Stream buffer is so had that internal IDS can access to larger amount of data flow without direct access to memory of host system. And access control list is had to help detection of misbehavior by controlling user access approaching to honeyVM.

LBC is performed pathway role connecting honey system and virtual server system. It is implemented using a virtual server system. It is performed function that normal traffic passed through IDS distributes evenly traffic not to impose large load to web servers. LBC controls not to concentrate traffic to one side of the main web server if traffic comes from external network. However, if normal service of web server is generated in a difficult situation due to

Table 3 Simulation parameters

Parameter	Value
CPU	I7-4770 K(3.5GHz)
Memory	32GB
Start number of honeyVM	5
Max number of honeyVM	20

attack like DoS or DDoS, then backup server is operated and the normal web service is performed. To do this, each web server and a storage server were connected to NFS.

4 Performance evaluation

4.1 Simulation environment

The experiment is performed in environment like Table 3 to evaluate the performance of robust web server system proposed in this study. HSC performs load measurements of host system every 3 min for honeyVM creation of honey system. Service in two web server is done in virtual host system and one backup server and storage server is composed.

4.2 Simulation result

There is evaluated the performance of the proposed method for collection of attack information and continuous web service in this chapter. Standard of the performance evaluation is attack detection rate through collection of attack information by honeyVM, the number of honeyVM by system load, detection rate and conversion ratio of backup server. Figure 3 shows the result of collected TCP-SYN flooding attack and ARP spoofing attack detection rate. As shown in Figure, attack detection rate is excellent because attack information collection is easy the more the number of honeyVM is many the more attack target is many. But almost the same performance regardless of the number is shown if the number of honeyVM is more than some degree. This is because attack detection is possible even though small number of honeyVM is

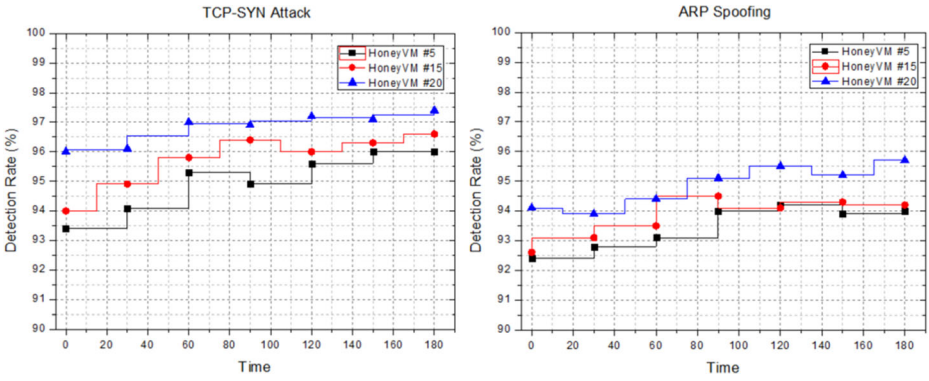

Fig. 3 Attack detection rate by HoneyVM

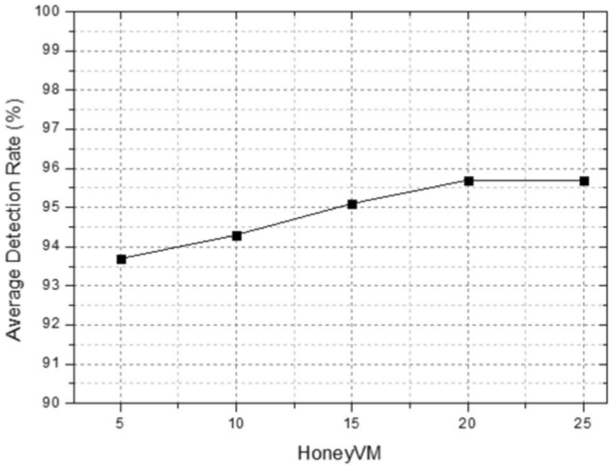

Fig. 4 The average detection rate by system load

used about well-known attacks. That is, the many number of honeyVM appropriately are configured to collect attack information about the unknown attacks.

Figure 4 shows the relationship of the number of generated honeyVM dynamically after HSC measures load of virtual host system and attack detection rate. As shown in the result, creation of honeyVM by HSC manages dynamically to prevent a large load on system and attack detection rate by the number of honeyVM is also proportional.

Figure 5 shows conversion ratio of web server by attack representing the performance. As shown in the figure, conversion ratio of backup server is shown very good results and this means that can provide stable web service under any circumstances. High resource utilization of proposed method and continuity of service is confirmed through experimental results.

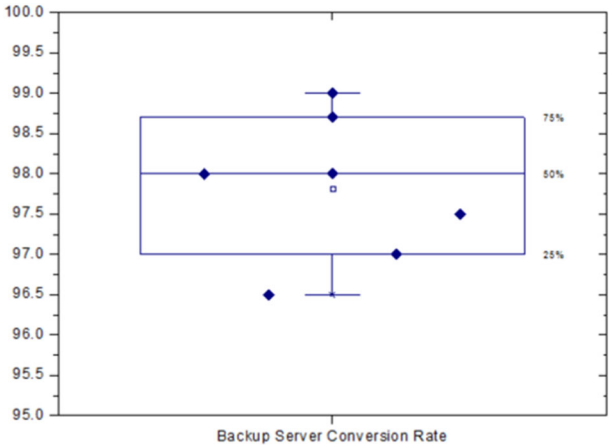

Fig. 5 Backup server conversion rate

5 Conclusion

In this study, active collection of attack information and this-based continuous web service provision technique using virtualization technology is proposed. After honey system constituting for attack information collection measures load of virtual host system, it determines the number of honeyVM creation. Attack using collected information in the created honeyVM like this is detected and the technique that continuous service can be performed by operation of backup server in the situation that web service by attack traffic doesn't do. Proposed method in this study can prevent service disruptions by attack, be economical because configuration of physical server isn't required using virtualization technology, and maximize efficiency. Stable performance of proposed method through experiment is confirmed.

References

1. Chen CL (2008) A new detection method for distributed denial-of-service attack track based on statistical test. J Univ Comput Sci 15:488–504
2. Dobrilovic D, Odadzic B (2006) "Virtualization technology as a tool for teaching computer networks," Int J Soc Sci Spring
3. Francois J, Aib I, Boutaba R (2012) FireCol: a collaborative protection network for the detection of flooding DDoS attacks. IEEE/ACM Trans Netw 20:1828–1841
4. Fuertes W, López de Vergara JE (2007) "A quantitative comparison of virtual network environments based on performance measurements," In Proc. 14th HP Software University Association Workshop, Munich, Germany, pp 8–11
5. Gupta BB, Joshi RC, Misra M (2012) ANN based scheme to predict number of zombies in DDoS attack. Int J Netw Secur 14:36–45
6. Ikinci A, Holz T, Freiling FC (2008) "Monkey-spider: detecting malicious websites with low-interaction Honeyclients," In Sicherheit'08, pp 407–421
7. Keller J, Naues R (2006) "A collaborative virtual computer security Lab," e-science, In Proc. Second IEEE International Conference on e-Science and Grid Computing (e-Science'06), Los Alamitos, CA, USA, pp 126
8. Kumar PAR, Selvakumar S (2011) Distributed denial of service attack detection using an ensemble of neural classifier. Comput Commun 34:1328–1341
9. Li M, Li M (2009) "A new approach for detecting DDoS attacks based on wavelet analysis," IEEE Proceedings of the 2nd International Congress on Image and Signal Processing, Tianjin, China, 17–19 October, pp 1–5
10. Paul O (2006) "Improving web servers focused DoS attacks detection," in Proc. of IEEE/IST Workshop on Monitoring, Attack Detection and Mitigation (MonAM 2006), Tuebingen, Germany
11. Pizzonia M, Rimondini M (2008) "NetKit: easy emulation of complex networks on inexpernsive hardware," In Proc. TridentCom 2008, Innsbruck (Austria)
12. Provos N (2004) "A Virtual Honeypot Framework," In proceedings of the 13th USENIX Security Symposium, pp 1–14

Hwan-Seok Yang is holding Assistant Professor position in Information Security at Joongbu University. In 2007–2010, he worked as a Research Professor in Dept. of Cyber Investigation Police at Howon University. He received the Ph. D. degree in Computer Science and Statistics from the University of Chosun in 2005. He conducts research in the general areas of security analysis of computer system and mobile networks.

Dong-Hwi Lee received the B.S. degree in Computer Science from Kyonggi University, Korea, in 1994 and 2001. He received M.S. and Ph.D degree in Information Security from Kyonggi University, Korea, in 2001 and 2007. and Research Scholar of University of Colorado Denver, USA, in 2011 and 2012. He is currently a Treatment Professor in Industrial Security, Kyonggi University, Korea. His research areas include Information Security and Cyber Early warning System.

Sueng-Jae Yoo received the B.S. degree in Mathematics from Dongguk University, Seou,l Korea, in 1988. He received M.S. and Ph.D degree in Mathematics from Dongguk University, Seoul, Korea, in 1991 and 1997. Now he is a full professor in Dept. of Information Security Engineering, Joongbu University, Korea. His research areas include Information Security.