Resilient Security Technology for Rapid Recovery from Cyber Attacks

Takaaki Koyama, Kunio Hato, Hideo Kitazume, and Mitsuhiro Nagafuchi

Abstract

Cyber attacks are a constant threat. In addition to taking the conventional—mainly defensive—countermeasures, it is important to do the utmost to control the effects of an attack once it has occurred in order to recover from those effects as rapidly as possible. In this article, we describe the concept of resilient security, present some use cases, and explain the technology that is used.

Keywords: network security, resilient security, security orchestration

1. Introduction

Public organizations and private enterprises have been subject to a barrage of cyber attacks in recent years. Those attacks cleverly work their way past conventional defensive measures in order to penetrate and exploit servers and network systems. Taking proactive security measures is a matter of course, but it is also important to assume there will be some damage from such attacks and to exert the utmost effort to control the damage and rapidly recover from the effects of an attack once it has been launched.

The development of computing resource virtualization has led to the study of network functions virtualisation* (NFV) and network software control. Virtual appliance products such as virtual switches and virtual firewalls are also beginning to appear in the actual market. These new technologies can be used to enable appropriate measures against attacks to be rapidly implemented on the network side by constructing flexible, reconfigurable networks.

In this article, we introduce the concept of resilient security, which is implemented with the technologies described above. We also present use cases and describe the virtual network and virtual appliance control technologies applied in those cases. Additionally, we discuss the work being done in our laboratories.

2. Objectives of resilient security

We are working to maintain service continuity in the event of unpredictable natural disasters or incidents involving security threats that evolve from year to year by autonomously implementing measures that have multiple layers and multiple aspects as virtual appliances. The objectives are to limit the scope of effects on services to the very minimum by controlling multiple devices at the appropriate points according to the type of attack and to provide clean pipe functions to isolate attacks and achieve rapid recovery.

One difficulty, though, is that the burden on operators to analyze and deal with sophisticated cyber attacks has been increasing rapidly. Reducing that burden is thus another aspect of our work, and we are developing recommendations for operators based on information we obtain about detected attacks and scenario-based autonomous control of multiple virtual appliances in order to implement measures that do not depend on the skill level of operators.

Also, even in cases where it cannot immediately be determined that an attack is in progress, it is still possible to secure the time needed for analysis by flexibly reinforcing virtual firewall resources and isolating the

* The British spelling used by the European Telecommunications Standards Institute

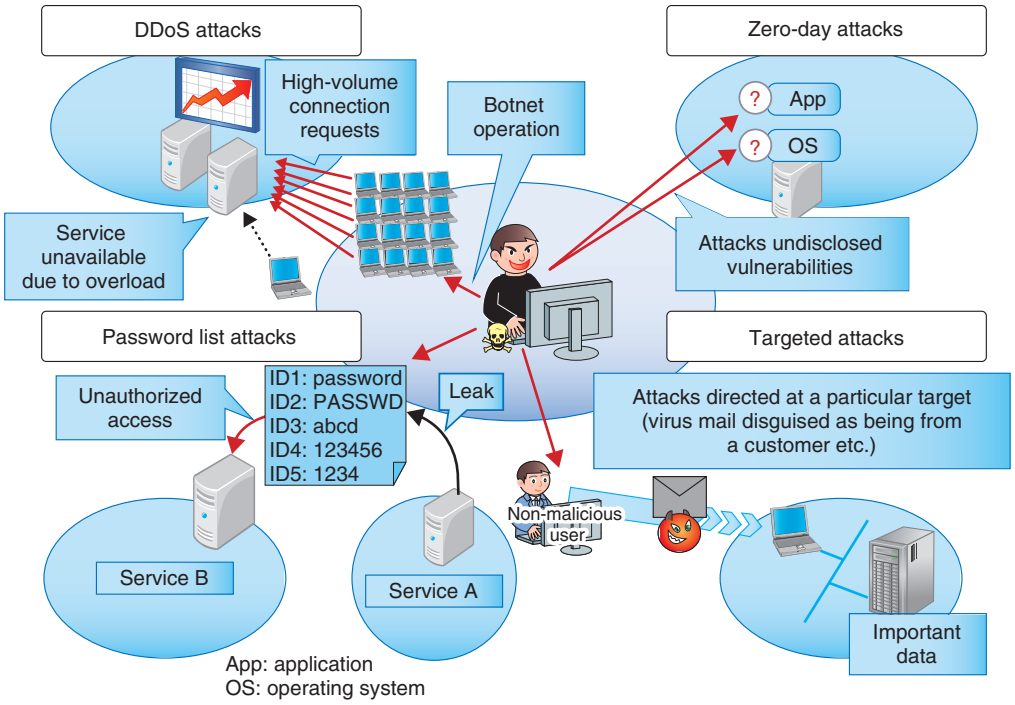

Fig. 1. Increasingly sophisticated cyber attacks.

attacked virtual machine (VM) to a quarantine network.

This application is also planned for network services, and to achieve this, the NTT Secure Platform Laboratories is also providing safe and secure platform technology to eliminate end-user concerns about the security of cloud or network services.

3. Advanced cyber attacks

This section introduces typical examples of recent cyber attacks (**Fig. 1**) and gives an overview of those that are becoming difficult to prevent by pre-incident measures only.

3.1 DDoS attacks

A distributed denial of service (DDoS) attack targets a service that is open to the public and uses a botnet composed of a very large number of terminals to flood servers with connection requests, thus overloading the servers and interfering with the provision of the targeted service. This kind of attack is difficult to distinguish from ordinary user traffic when the connections are examined one at a time, so it is very difficult to recognize and block only the malicious communication.

3.2 Zero-day attacks

A zero-day attack exploits software vulnerabilities (security holes) that are unannounced and for which countermeasures have not been established. This type of attack generally targets unknown vulnerabilities, so the attack is launched before patches to remove the vulnerabilities are applied, making defense against such attacks very difficult.

3.3 Password list attacks

In this type of attack, a list of identifications (IDs) and passwords that was somehow leaked from one source is used to attack a completely different service by attempting an unauthorized log-in to another person's account. These attacks appear as individual log-in requests that are essentially no different from normal user use, and the ID and password combinations appear to be genuine, which makes it very difficult to distinguish the behavior as an attack and eliminate it.

3.4 Targeted attacks

This type of attack is characterized by the targeting of a particular company or organization for a particular purpose, such as theft or falsification of personal information or assets. Such attacks are designed for

specific situations, so the methods are difficult to predict by looking at past attacks. They apply social engineering approaches that take advantage of human emotion and curiosity to create security vulnerabilities. It is therefore difficult to defend against this type of attack automatically with a security system.

4. Trends in virtual networks and virtual appliances

In this section, we introduce the virtual networks and virtual appliances that are used in current networks as technical elements of resilient security, which serves as an effective means of dealing with the different types of attacks described in the previous section. We also explain security orchestration functions for achieving resilient security.

4.1 Virtual networks

Virtual networks (NWs) are a virtual private network (VPN) technology for creating isolated networks for individual customers as an Internet Protocol (IP) network that is constructed within a cloud system and extends to the customer's premises. IP networks can be constructed for both on-demand and high-volume use. Three types of systems are used: tagged VLAN (virtual local area network), OpenFlow-based hop-by-hop systems, and tunneling-based overlay systems [1].

Also, working in coordination with a cloud management system makes it possible to change network settings automatically for live migration of VMs. If a VM is moved to a different hypervisor, the customer's IP network can be moved to a different physical network without terminating the session, and isolation is also possible. In 2012, the OpenStack open source software (OSS) cloud management system also began providing virtual NW construction and other such operations [2].

4.2 Virtual appliances

A virtual appliance can provide network functions that have previously been provided by dedicated hardware such as routers, firewalls (FWs), and load balancers (LBs) as software implementations in a virtual environment. These functions constitute the set of functions needed to construct an enterprise intranet, and virtual appliances were developed to meet the need to use those functions with a virtual network. Research has been done recently on appliances running in dedicated virtual environments as dedicated network equipment for which functions can be freely combined and replaced. Standardization under the general name of NFV is also in progress. Virtual appliances that provide an intrusion detection system, web application firewall, and other such security functions in addition to an FW and LB have also been developed. In 2013, Linux network namespace settings for the OpenStack OSS virtual router, virtual FW, and virtual LB became available, and the number of virtual appliance products that can be controlled with OpenStack is increasing.

4.3 Distributed virtual appliances

The standard specifications for routers and FWs specify one operating unit, with others serving as spares. This prevents the distribution of virtual appliances and makes it difficult to distribute the virtual appliance load or completely separate communication paths that pass through virtual appliance input/output interfaces in units of IP addresses and end-to-end connections. Techniques for a distributed arrangement of multiple virtual appliances and route changing in a flow unit at layer 4 are therefore required. In regard to the distributed arrangement of virtual appliances, companies such as VMware, vArmour Networks, and others are making progress in implementing configurations of their own products in which multiple appliances connected in a dedicated virtual network work cooperatively to reduce the processing load. Rerouting techniques include those that use conventional switches and those that use advanced switches. Conventional switches can be used in three ways: using a routing protocol and directly rewriting the routing table to change the routing destination; using address conversion techniques and a DNS (domain name system) server to change the destination IP address; and rewriting the media access control (MAC) address table to change the destination MAC address without changing the IP address. When advanced switching functions are used, switching can be done according to IP packet header data such as the TCP (transmission control protocol) or UDP (user datagram protocol) port number in addition to the IP address [3]. The built-in switch of the hypervisor or the OpenFlow switch can be used, and implementation using ordinary OpenFlow switches, etc., as well as VMware NSX or the OSS Linux OpenvSwitch is also possible.

4.4 Security orchestration functions

Currently, the NTT Secure Platform Laboratories is developing ways to implement resilient security using virtual NWs and virtual appliances as well as

distributed virtual appliances. Specifically, security orchestration functions have been configured that can work in cooperation with various devices to collect information and define device control scenarios. The security orchestration system functions together with multiple types of virtual appliances located on networks and systems and with server and network device logs to detect indications of cyber attacks and the damage they have caused. Even though the zero-day attacks, password list attacks, targeted attacks, and other attacks described in section 3 are themselves difficult to detect, it is not impossible to discover proof of damage that corresponds to the purposes of attacks, such as the altering of data or information leaks. Using virtual appliances as security sensors enables the placement and number of units to be changed dynamically for efficient detection. Detected cyber attacks are automatically classified as those for which countermeasures are possible and those for which countermeasures are not possible. Even for the attacks for which an automated response is not possible, automatic generation and notification of response recommendations that guide the decisions of the operator is possible. That function is implemented by arranging the appropriate virtual appliances at the right places in the system in order to control servers and network equipment. When the existing configuration is inadequate, virtual appliances are automatically added, and control is performed to move traffic to the virtual NW, thus preventing major harm, blocking the attack, and strengthening the system. Even when it is difficult to directly block an attack, such as with a DDoS attack, if the system can be strengthened and services continued by automatically adding resources such as virtual appliances in response to the attack, then the attack can be withstood, and the purpose of the attack can be defeated.

5. Resilient security engine through security orchestration

The resilient security engine being developed by the NTT Secure Platform Laboratories is intended for implementation as a security orchestration system for coping with cyber attacks. As the first step, we are currently developing a security orchestration system for protecting normal communication with VMs against DDoS attacks on a datacenter (DC) on which cloud services are running and for minimizing the harm to the DC and the VM under attack. The operation of the system is illustrated in **Fig. 2**. There are functions for recommendations to deal with three cases: 1) a DDoS attack on the DC or FW set up for each customer IP network will prompt a recommendation to the operator to use external network equipment to block the attack; 2) an attack that can be clearly determined to be on a VM will prompt a recommendation to the operator to block the attack with a virtual FW or external network equipment; and 3) discovery of communication that is suspected to be an attack on a VM will prompt a recommendation to reinforce the virtual FW resources, migrate to a different DC, or block the attack by a virtual FW or external network equipment. The first of these three cases is a matter of maintaining continuity of the network service, the second involves preventing an attack on a VM, and the third involves implementing a response when a gray zone is determined. Defense against a DDoS attack is described here, but the functions for the second and third cases described above are being designed for application to various types of attacks, with a view to applying them to targeted and other attacks.

The three internal functions are for logging, analysis and identification of an attack, and appliance setup. Functions are provided for analysis and determination according to scenarios for which conditions are set within the resilient security engine using flow data, attack detection data, and data collected by security sensors for judging suspected attacks, and for making recommendations to the security operator in the cases of automatic virtual FW setup and blocking with external network equipment. Naturally, the security operator is informed even when the setting is for the reinforcement of virtual FW resources or migration to another DC; the setting for manual blocking for the virtual FW can be performed later based on the security operator's decision. We are moving forward with development in which we describe the operation for the three cases described above as scenarios. Customization is possible according to the individual operation conditions and descriptions.

6. Future development

We are currently developing virtual FW control technology for dealing with DDoS attacks. When this development is completed, we plan to conduct trials to evaluate its effectiveness. We also plan to expand the extraction of control scenarios from actual operation sites and extend the types of virtual appliances in order to cope with complex, advanced, and sustained attacks.

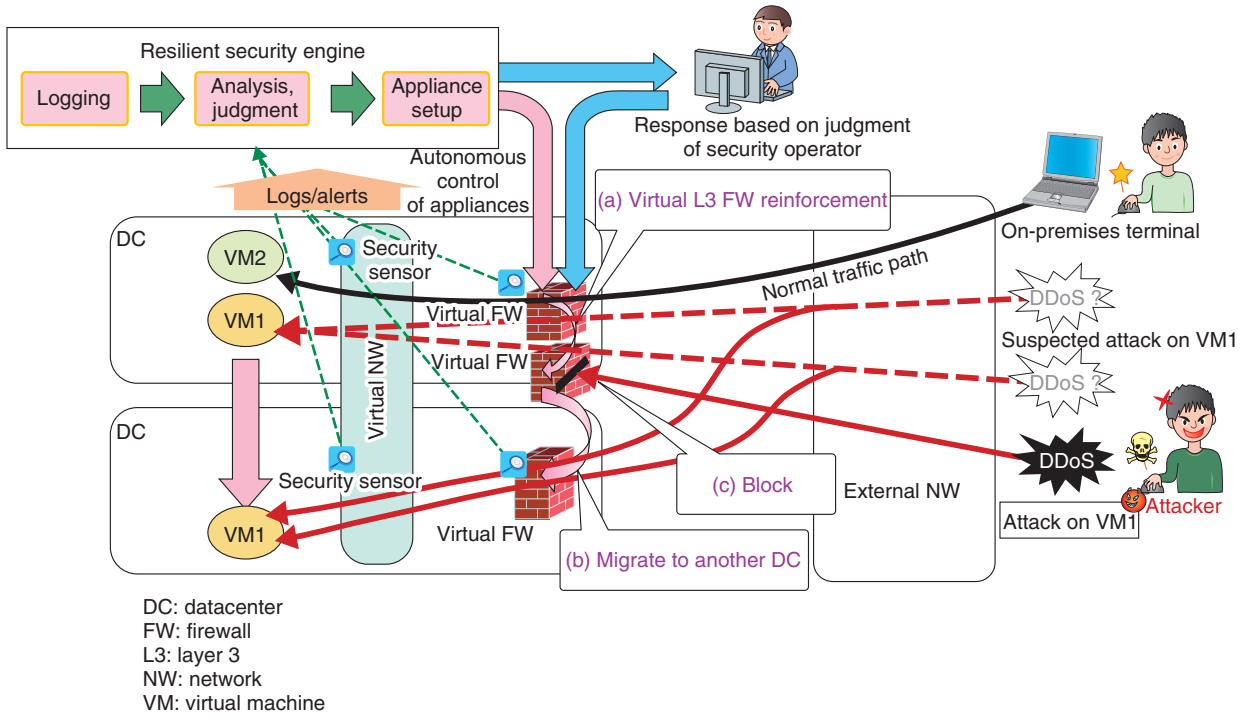

Fig. 2. Resilient security engine.

References

[1] H. Kitazume, T. Koyama, Y. Tajima, T. Kishi, and T. Inoue, "Network Virtualization Technology for Cloud Services," NTT Technical Review, Vol. 9, No. 12, 2011. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201112fa4.html

[2] S. Mizuno, H. Sakai, D. Yokozeki, K. Iida, and T. Koyama, "IaaS Platform Using OpenStack and OpenFlow Overlay Technology," NTT Technical Review, Vol. 10, No. 12, 2012. https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr201212fa1.html

[3] T. Koyama, T. Kishi, T. Inoue, Y. Nagafuchi, and H. Kitazume, "Report on the Effects of Multiple Active Virtual Routers and Virtual L3 FW," IEICE Technical Report, Vol. 113, No. 303, IN2013-89, pp. 13–18, 2013.

Takaaki Koyama
Senior Research Engineer, Network Security Project, NTT Secure Platform Laboratories.

He received the B.A. and M.M.G. in media and governance from Keio University, Tokyo, in 1994 and 1996, respectively. He joined NTT Software Laboratories in 1996 and has been studying software CALs (client access licenses). Since 1999, he has been studying a type of IP-VPN technology called GMN-CL, and developing network equipment. His recent research interests are enterprise cloud network systems and security orchestration systems. He is a member of the Information Processing Society of Japan.

Kunio Hato
Senior Manager, Network Services, NTT Communications Corporation.

He received the B.E. and M.E. in information processing from Tokyo Institute of Technology in 1997 and 1999, respectively. Since joining NTT in 1999, he has been engaged in researching and developing IP VPNs, Wide Area Ethernet, network security systems and intercloud computing systems. He is a member of the Institute of Electronics, Information and Communication Engineers (IEICE).

Hideo Kitazume
Senior Research Engineer, Supervisor, Network Security Project, NTT Secure Platform Laboratories.

He received the B.E and M.E. in computer science from Gunma University in 1987 and 1989, respectively. He joined NTT in 1989 and engaged in researching and developing ATM-LAN systems, studying ATM traffic control, and developing a global networking service platform. From 1998 to 2010, he was involved in the development, design, and operation of IP-VPN services at NTT EAST. He is currently researching and developing network security orchestration technologies based on network virtualization. He is a member of IEICE and the Operations Research Society of Japan.

Mitsuhiro Nagafuchi
Manager, Produce Section (Security), Research and Development Planning Department.

He received the B.A. in mechanical information science and technology from Kyushu Institute of Technology in 1997. He joined NTT in 1997. He was with the Corporate Sales Department of NTT WEST from 1999 to 2013.