Active defense technology and its developing trend

Qing Zhang*, Caixia Liu, Ganqiang Lu

National Digital Switching System Engineering & Technological Research Center, Zhengzhou, China

Received 1 September 2014, www.cmnt.lv

Abstract

Active defense technology has attracted more and more attention in the field of network security. This paper introduces the main threats of computer network and traditional network security defense technology. Aiming at the shortcoming of the traditional defense technology, the active defense technology is proposed. Finally, according to the current research hotpots, this paper presents the new direction of active defense: Moving Target Defense and Mimicry Security Defense.

Keywords: traditional defense, active defense, honeypot technology, moving target defense, mimicry security defense

1 Introduction

Through more than 30 years' development, computer network technology has penetrated every aspects of the information society as the infrastructure. Along with the great convenience of information access and acquisition provided by the network popularization, the network security problems are increasingly serious. According to the National Computer network Emergency Response technical Team Coordination Center of China (CNCERT or CNCERT/CC) monitoring, in 2012, 16388 websites were tempered within domestic. Among these attacked websites, there were 1802 government websites, with a growth of 6.1% and 21.4% compared with 2011, respectively. There were 52324 websites which were secretly implanted the Trojan-horse programs with 3016 ones were government websites, increasing by 213.7% and 93.1% respectively [1]. Website security, especially the security of information and data of the users in the website are facing severe threat.

Many network security issues happened in recent years. In January 28, 2013, the IP address of People.cn suffered the DOS attacks from overseas. Significant abnormal flow occurred between 18:30 and 20:20 with the peak flow rate of 100Mbps, 12 times the normal traffic. UDP traffic accounts for 95% of it and about 88 percent of that comes from outside. At 15:20 on January 28, 2013, a large number of Internet users in China were unable to access website with domain name sending with'. Com','.net' etc. The available data analysis provides a pre-judgment that network attack from USA caused this exception when internet users in the territory of our country tried to get the DNS service from international top-level domain name.

Besides, the computer virus and Trojan technology is developing rapidly. The "2010 Chinese computer virus outbreak investigation analysis report" indicates that although the anti-virus software has been installed as the necessary software in the computers of most users, the computer virus infection rate is 70.51%. Although this rate decreases compared with last year, it still maintains at a high level and the ratio of multiple injection times is 42.71%.

In conclusion, not only to the daily life of ordinary people, but also to the national security, the network security issues should be treated with enough caution. The research of the secure and reliable network defense system is of significant importance.

2 Studies and classification of main security treats

The conclusion that the current network security is threated by the hacker and computer viruses could be summed up though the mentioned issues.

A. Classfication of Hacker Attack.

Hackers common attack means can be classified into non-destructive attack and destructive attack. Generally, the non-destructive attack is to mess up the operation of system rather than steal system information by denial of service (DOS) or information bomb. The destructive attack is intended to hack into the computer system, steal the confidential information of system and destroy the data of target system.

As attacks happening quickly, attacking methods become more and more complicate, intelligent and diversified. The purposes of hackers to launch an attack transform from showing off technology to the economic interests. Figure 1 shows the comparison between the ability of the hackers' requirements and attack tools when attack happens in recent years. We can see that with the automation of attack tools continuously improving, the ability of tools and attack complexity are increasing, but the technology level that a hacker requires decreases.

* ***Corresponding author's*** e-mail: feiying910103@163.com

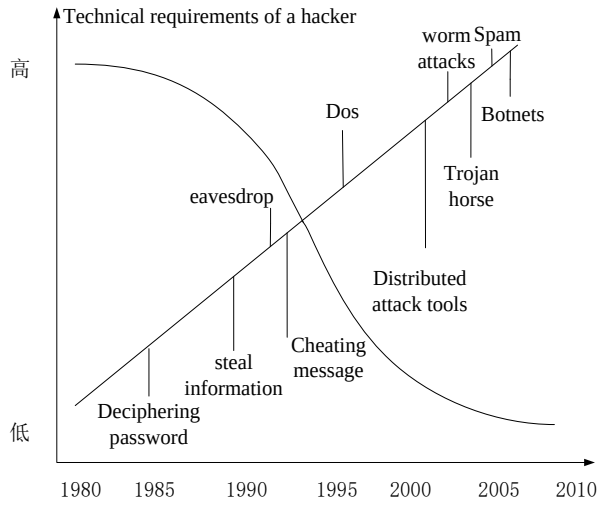

FIGURE 1 The comparison between the ability of the hackers' requirements and attack tools

Next section introduces two common means of a hack attack.

Denial of Service.

Denial of services also known as distributed DOS attack [2] which uses a large number of packets that exceed the processing capacity of the targets to consume available bandwidth resources and result in the crash of the network services. This might cause great damage to the specified target by concentrating large web server bandwidth which could consume the bandwidth resource of the target immediately resulting in the server paralysis.

Network Sniffing.

Network sniffing is an administrative tool to monitor the status of the network, data stream and information transmission on the internet. Although it could set the network interface to monitoring mode and intercept information transmitted online, it can only be used in the hosts which are connected to the same network segment as a tool to get the password of the users.

B. Classification of Viruses.

This paper manly introduces some virus usually seen in our life:

Shell viruses. The virus surrounds itself around the host program, and do not modify the original program. This virus is the most common, easy to write and easy to find too.

Operating system viruses. The viruses replace the legitimate program module of operating system by their logic part when they are running, doing damage to the operating system. This type of virus is highly destructive and can lead to paralysis of the entire system, such as: dot viruses and marijuana viruses.

Embedded viruses. Embedded viruses embed itself to an existing program, linking the main body of computer virus with the attacking target in the form of inserting. This kind of viruses usually is hard to create, and once it is difficult to eliminate once embedded in the program. It will bring great challenges to the current anti-virus technology if the polymorphic virus technology, super virus technology and conceal virus technology are used at the same time.

3 Traditional security defense technologies

In order to cope with the flood of hackers and virus threats, people put forward many methods to protect the security of network, such as: anti-virus software, firewall and intrusion detection system etc.

A. Anti-virus Software.

The core idea of traditional anti-virus technology, which is called eigenvalue scanning technology [3], is to extract eigenvalue from the virus code which is already known, then the computer anti-virus software compares the object to be examined with the eigenvalue of virus, if the contrast succeeds, it will be reported as this kind of virus. The working process of the traditional anti-virus software is shown in Figure 2.

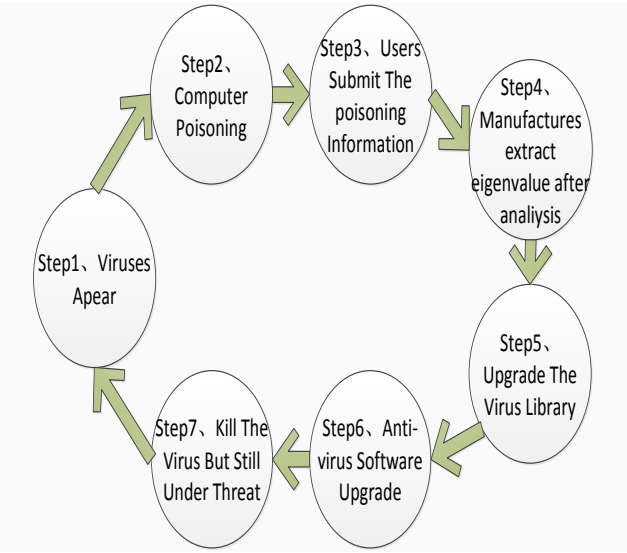

FIGURE 2 The basic flow of Anti-software

It can be seen in Figure 2: if the eigenvalue of virus is not updated to user's anti-virus software, the virus cannot be identified by anti-virus software. Recently, there appears some software such as automatic packer, automatic to avoid pitfalls to against the traditional anti-virus software [3], traditional anti-virus technology lags behind the virus technology has been an indisputable fact.

B. Firewall.

Firewall is a barrier set between the protected network and the external network, controlling the information flow accessed to network according to safety rules to avoid unpredictable invasion [4]. The firewall itself has strong anti-attack capability, which could provide information security services, implementation of network and information security. The firewall is shown in Figure 3:

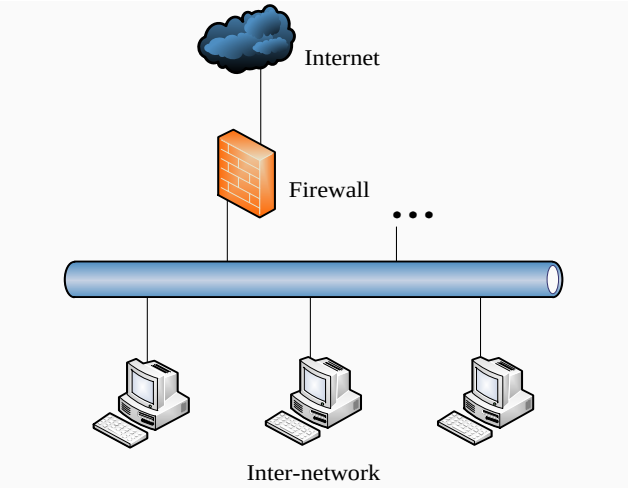

FIGURE 3 The working principle of firewall

This paper takes application proxy firewall as an example to introduce its working principle. The application proxy firewall, which works at the top layer of OSI, blocks the network traffic. It could monitor the traffic of application layer by making Make special agent on each application. Figure 4 shows the working principle of application proxy firewall.

Form the picture we can see that the data of client is no longer directly transmitted to the real server on the network, but to the proxy server of application proxy firewall in the application layer. After the protocol analysis, if the packet is normal, then passed on to the real server on the network via agent client. The procedure is same when a packet transmitted from network to server. Application proxy firewall is between the client and the server, filtering the data communicating between them two. From the perspective of client, the proxy server is equal to the real server in the network.

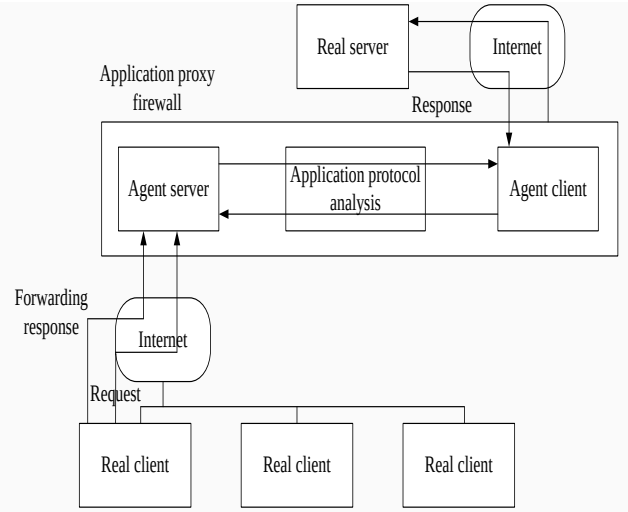

FIGURE 4 Application proxy firewall

As the first layer of traditional defense system, firewall is the core of whole defense system. But it is because the firewall is in the outermost layer of the defense system that it can only rely on the rules matching filter instead of analyzing and grasping the integrity of the data. And firewall cannot detect encrypted Web traffic, cannot stop the file transferring which is infected by virus. Therefore the firewall is incapable of action in many respects.

C. Instruction Detection System.

Intrusion Detection System (IDS) is the second layer of the traditional defense system, which is a reasonable supplement of firewall. The so-called IDS collect and analyze the information of key nodes in computer system to find whether there are signs of being attacked in the network [5].

Constitution of IDS.

According to the Common Instruction Detection Framework (CIDF) model, IDF usually consists of four parts: Event Generators, Event Analyzers, Response Units, and Event Databases. Its general structure is shown in Figure 5.

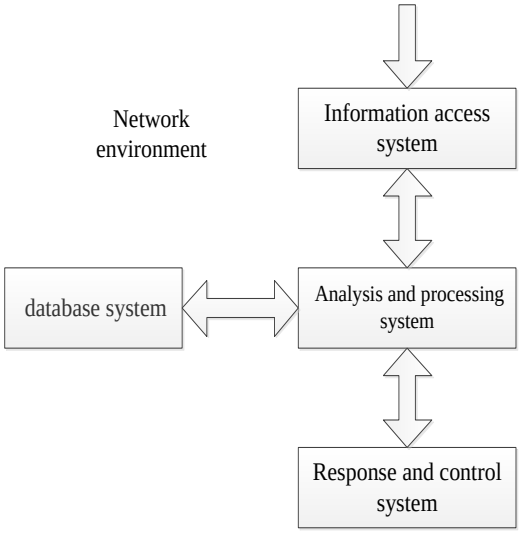

FIGURE 5 Structure of IDS

The picture shows that the event generator is used to capture issues from the environment, and to provide the issues for other parts of the system. Time analyzer analyses the received data and response for different results, such as: cutting connection, changing file attributes or a simple alarm. Event database is to store all kinds of middle and final data; it can be a complicated database or just a simple text file.

IDS Common technology.

1) Static Configuration Analysis Technology: viewing the current system configuration. It mainly refers to the static characteristics of the system, in order to check whether a system will be destroyed.

2) Anomaly Detection Technology: analyzing system and auditing data, so as to establish a system. During the concrete implementation process, if the auditing data in system is different from the normal behavior of newly established system that means intrusion has happened [6].

The traditional computer network information defense technology mainly includes anti-virus software, firewalls,

intrusion detection technology, which have some common disadvantages:

1) Static defensive ability [7]. Taking firewall as an example, it relies entirely on the network administrator to manually configure the firewall to achieve its function, which can easily be exploited by the worm on the network.

2) Passivity of defense [8]. These tools begin to defend only after the attack occurs, but not before the attacks have been identified. Such as IDS.

3) Cannot identify new network attack [9]. For example, anti-virus software can do nothing to a certain virus until its eigenvalue has been identified, which cannot solve the problem of network security fundamentally.

4 Active defense systems

Active defense [10] is an emerging technology in recent years in the field of network security. It is a real-time protection technology which is based on program independent analysis behavior, which will take all kinds of protection measures to prevent the attacker from achieving the intended purpose.

Researchers have made many researched in active defense technologies, especially on the aspect of detecting and identifying technology, many different strategies and methods are raised one after another, B. Xiao and the others proposed an identifying method based on TCP connecting state [11]. Reference [12] presented an identifying method based on exceptional traffic detecting model. The Network ICE company put forward the concept of IPS firstly, and launched the first IPS product in 2009 [13]. Reference [14] proposed a special active system which could monitor and control the whole system at the same time. Liu Huaqun and others discussed active protection for campus network based on multi-cores UTM [15]. Jianpeng Zhao proposed an active defense model for web accessing DOS attacks [16].

A. Introduction of Active Defense Technology.

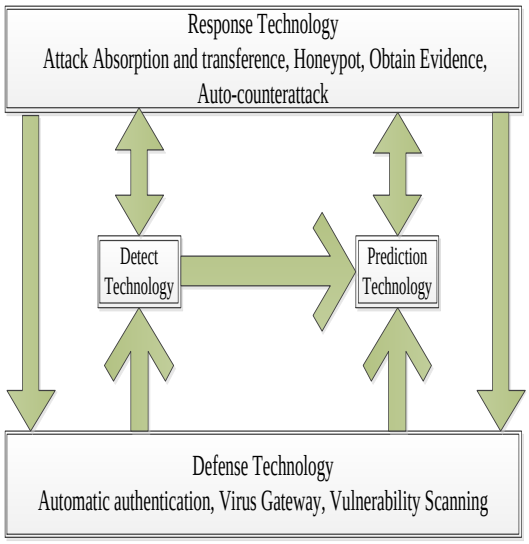

FIGURE 6 Active defense system

From Figure 6, we can see that the technology used in active defense system contains: instruction prevention technology, instruction prediction and instruction response technology [17].

Instruction prediction technology.

The intrusion prediction function is an obvious feature of active defense that is different from the traditional defense. Intrusion prediction reflects the important characteristics of active defense: predicting instruction information before the attack occurs, providing clues for the protection and response of information system, getting the initiative of system defense.

At present, there are two main types of intrusion prediction technology [18]. First, prediction methods based on security incidents. According to the history regularity of intrusion events, predict security situation for a period of time in the future. Second, prediction method based on traffic monitoring. According to the influence of the attack on the statistical characteristics of the network traffic to predict occurrence and development trend of the attack. It can predict short-term security situation and unknown attacks.

Instruction Response Technology (IRT).

Intrusion response technology is the essential difference between active defense and traditional defense. It embodies the initiative of active defense technique in network intrusion protection. IRT is used to process the detected information, and return the result to system, thus future improving the protective ability of the system. The main intrusion response technology [19] includes intrusion tracing technology, honeypot technology, forensics, automatic counterattack.

This paper takes honeypot technology as an example to introduce its working principle. Honeypot [20] is a bait that is used to deceive the attacker. In order to attract the attacker to take the bait, it will provide the attacker some resource that looks very useful (such as severs and ports). When attackers scan and try to use these resources, they will mistakenly think themselves into the core area of the system; In fact, they have fallen into the trap. Then the network administrator can observe the behaviors of attackers in the trap, investigate their attacks and tools they are using.

According to the levels of interaction, the honeypot can be divided into low interaction honeypot, middle interaction honeypot and high interaction honeypot. The higher of the interaction level, the more services and data it can provide, the greater ability that the honeypot withstand attack, the more attack information that administrator can capture from the honeypot. The paper takes honeynet technology [21], a special kind of high interaction honeypot, as an example to introduce its design model.

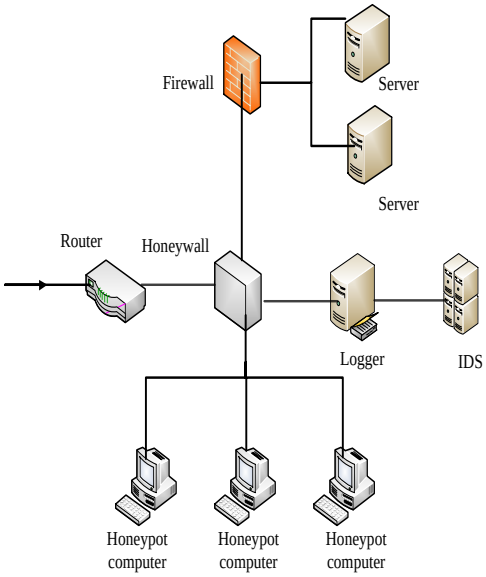

FIGURE 7 The architecture of honey-net

As shown in Figure 7, honey-wall is the central control of the entire honey-net, all the data, in or out of the honey-net, must pass through honey-wall, which separate honey-net and external network. The honey-wall has three Network interfaces: One network interface is connected to the log server, which makes it convenient for the remote management of honey-wall and real-time updating rules of intrusion detection system. If invaders had compromised honeypot, in order to prevent intruders taking honeypot system as a springboard to attack other hosts, the honey-wall follow "wide into strict out" policy, that means allowing the honey-net to accept all foreign data, but strictly control the data out of it [22].

B. The New trend of Active Defense Technology.

With the development of protection technology, Active defense technology appeared some new direction. Among them, Moving Target Defense (MTD), proposed by America research institutions, and Mimicry Security Defense (MSD), proposed by China scientists, represents the new direction of the active protection domain.

Moving Target *Defense (MTD).*

In cyber space, attackers have an asymmetric advantage in that they have time to study our networks to determine potential vulnerabilities and choose the time of attack and gain the maximum benefit. Additionally, once an attacker acquires a privilege, that privilege can be maintained for a long time without being detected [23].The static nature of current network configuration approaches has made it easy to attack and breach a system and to maintain illegal access privileges for extended periods of time. Thus, a promising new approach to network security has been suggested called the moving target defense (MTD) [24].While there are many facets of MTD, for computer networks, one can broadly interpret MTD as the fact that the network constantly changes to reduce/shift the attack surface area available for exploitation by attackers. Here, the attack surface consists of the system resources exposed to attackers (e.g. the software residing on the hosts, the ports open to communicate between hosts, and vulnerabilities in the various components) as well as compromised network resources that can be used to further penetrate the system.

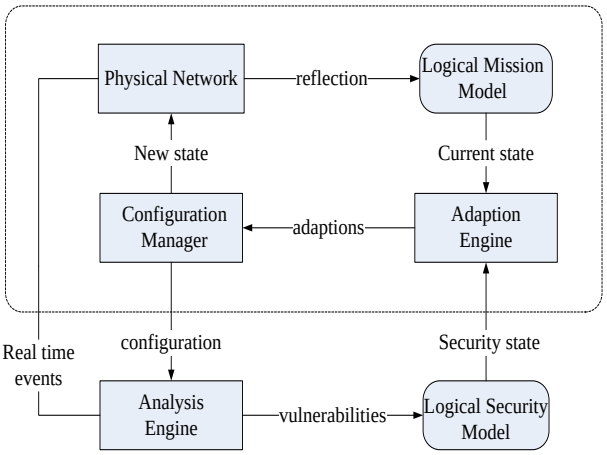

FIGURE 8 Moving target defense system design

Rui Zhuang et al. proposed a high-level architecture of MTD system that adapts in a purely randomly fashion is shown in Figure 8. This system produces random adaptations that do not inhibit correct system operation. The key to making these random adaptations is that they are based on a Logical Mission Model, which captures an abstract view of the Physical Network's current configuration along with the functional requirements of the network. The driver is the Adaption Engine, which orders random adaptations to the network configuration at random intervals. These adaptations are implemented by the Configuration Manager, which controls the configuration of the Physical Network. The basic operation of the random adaptation remains the same; however, it has added an Analysis Engine that takes real-time events from the Physical Network and the current configuration from the Configuration Manager to determine possible vulnerabilities and on-going attacks. The Adaptation Engine is extended to look at the network's current state along with its security state, as captured in the Logical Security Model. The Logical Security Model also consists of two runtime models: a goal model and a model of system vulnerabilities. The goal model captures the system's security goals while the vulnerability model is in the form of a novel Conservative Attack Graph (CAG), which captures both known and unknown system vulnerabilities and how an attacker might move through the system to gain specific privileges.

Moving target cyber-defense systems encompass a wide variety of techniques in multiple areas of cyber-security. The dynamic system reconfiguration aspect of moving target cyber-defense can be used as a basis for providing an adaptive attack surface. Making this approach difficult is the large software monoculture in common use that provides a stable, widespread attack surface that is difficult to reconfigure in proprietary off-the-shelf systems. This dynamic system reconfiguration is informed by intrusion detection systems as to the current overall attack state. Intrusion detection systems also

identify which system reconfiguration is appropriate for reduction of the attack surface against the currently appearing threats. The problem here is that intrusion detection is imperfect and can lead to costly overreactions by a moving target system that will have minimal effect on the security of the system. We need a moving-target defense system with a variety of potential reconfiguration techniques, which can use all available information about the system's security to estimate the current state, and the ability to take actions that enhance system security overall.

MTD technology includes IP address variable, random network and host identity, Random code execution, random data etc... In recent years, moving target defense technology has a lot of new progress, including deformation network, self-adaptive computer networks, self-cleaning network, moving target IPv6 defense and open stream random hosts conversion technology et.

Deformation Network.

August 2012, the U.S. Army awarded Raytheon "Enemy reconnaissance Limit Deformation Network Infrastructure (MORPHINATOR)" project, worthing 3.1 million dollar, to do research on "deformed" capacity computer network prototype. The main purpose of this project is to realize that the network administrator dynamically adjusts and configures the network, hosts and applications with certain purpose to prevent, delay or stop network attacks, in the condition of that the enemy cannot make any detection and prediction.

Adaptive Computer Network.

May 2012, the University of Kansas began researching "Adaptive Computer Network" for the United States Air Force Office of Scientific Research, focusing on investigating and quantifying the impact of moving target defenses to computer networks. They Study the computer networks by automatically change their settings and structures to combat the feasibility of online attacks, and develop effective analytical model to ensure the effectiveness of a moving target defense system.

Self-Cleaning Network.

Self-cleaning Intrusion Tolerance (SCIT) architecture blocks or limit network attacks by constantly cleaning off the server and changing the criteria of individual server. This actually is an application of a moving target defense technology, which has made a lot of successful researches.

IPv6 moving target defense.

Moving target IPv6 Defense (MT6D) presented a new idea of moving target IPv6 defense.

The Internet Protocol version 6 (IPv6) brings with it a seemingly endless supply of network addresses. It does not, however, solve many of the vulnerabilities that existed in Internet Protocol version 4 (IPv4). In fact, privacy-related crimes in IPv6 are made easier due to the way IPv6 addresses are formed. [25] developed a Moving Target IPv6 Defense (MT6D) that leverages the immense address space of IPv6. The two goals of MT6D are maintaining user privacy and protecting against targeted network attacks. These goals are achieved by repeatedly rotating the addresses of both the sender and receiver. Address rotation occurs, regardless of the state of ongoing sessions, to prevent an attacker from discovering the identities of the two communicating hosts. Rotating addresses mid-session prevents an attacker from even determining that the same two hosts are communicating. The continuously changing addresses also force an attacker to repeatedly reacquire the target node before he or she can launch a successful network attack. Results showed that, MT6D not only feasible, but also seamless binding with the new IPv6 addresses. Meanwhile MT6D is able to provide a powerful moving target solution for platform and application layer [25].

Moving Target Defense Against Internet Denial of Service Attacks (MOTAG).

Distributed Denial of Service (DDoS) attacks still pose a significant threat to critical infrastructure and Internet services alike. The MOTAG, a moving target defense mechanism that secures service access for authenticated clients against flooding DDoS attacks. MOTAG employs a group of dynamic packet indirection proxies to relay data traffic between legitimate clients and the protected servers. Its design can effectively inhibit external attackers' attempts to directly bombard the network infrastructure. As a result, attackers will have to collude with malicious insiders in locating secret proxies and then initiating attacks. However, MOTAG can isolate insider attacks from innocent clients by continuously "moving" secret proxies to new network locations while shuffling client-to-proxy assignments. Simulations have been used to investigate MOTAG's effectiveness on protecting services of different scales against intensified DDoS attacks, and the results verify the effectiveness of the method.

Stephen Groat et points that as computing becomes mobile and systems enable connectivity through mobile applications, the characteristics of the network communication of these systems change due to the instability of mobile nodes on networks. Mobile devices logically move by changing addresses throughout the course of their communication in the system. These mobiles nodes acquire characteristics of a moving target defense, in which nodes change addresses to avoid detection and attack. Yet, as mobile nodes change addresses, the critical points in the system that applications are set to communicate with, such as servers, cloud services, and peer registration servers, remain static and become easily identifiable. Mobile-enabled systems are beginning to model heterogeneous moving target networks, in which some nodes move while others remain static. Heterogeneous moving target networks expose relationships and dependencies between nodes, helping an attacker easily identify the static, critical nodes within a mobile-enabled system. Homogeneous moving target networks, in which all nodes change addresses, mask the critical points within the system, blending the mobile nodes with the critical, static nodes, and provide additional security for the static nodes. By applying a moving target defense to all nodes within a mobile-enabled system, the critical points can be masked and additional security can be provided.

The advantages of MTD technology are mainly embodied in the following aspects:1) Break through the original technology, realize a fundamental change, it is committed to building a dynamic, heterogeneous, uncertain, "live" network, not the current static,

homogeneous, certain, "dead" network;2) Breakthrough the situation of "easy to attack difficult to defend" in network attack and defense. MTD can make the attack surface of system become unpredictable for attackers, which will greatly improve the defense capability of system, so as to reverse attacker's advantages.

Of course, the MTD technology still faces many challenges, for example: security of virtual infrastructure, security and elastic technology of mobile system in virtual environment, Automatic change technology, method to demonstrate the effectiveness of MTD. Moving target defenses require significant and frequent modifications to system parameters to successfully create entropy and act as a viable defense. While system architecture in dependent languages, such as Python and Java, allow for code portability and reuse, the operations of a MTD that are required to create entropy are too resource intensive for these languages. By using languages that are tailored to specific system architectures, MTDs such as MT6D can be successfully deployed in many different types of network systems, including resource constrained environments.

Mimicry Security Defense.

There is a special kind of octopus living in deep ocean, it can twist its body, change its color, imitating at least fifteen different animals' appearances and behaviors. Disguise itself, to ensure the security of living in ocean. Scientists of china are inspired by the Mimic Octopus, put forward the design thought of mimicry computer, and successfully develop the world's first computer mimicry In September 2013.

According to the thought of structural dynamic variable of mimicry computer, Chinese researchers in related fields proposed the new concept-"mimicry security". It aims to improve the uncertainty of environment or actuator, random change the system architecture in the way of defender controlled. So attackers are difficult to observe and forecast attacking targets, which can reduce security risks caused by virus, vulnerability and the back door.

5 Conclusion and prospect

This paper introduces the development of defense technology researches and the importance of such researches for the field of network security. It makes an overview of main threats in usual life. Then we present the traditional defense methods as well as their advantages and disadvantages. According to the disadvantages, we discuss the methods of active defense. Finally, based on the current developing trend, we analyze the new ways to protect the security of network, which are Moving Target Defense and Mimicry Security Defense.

Active defense technology has played an important role in solving network security problems. Current active defense technologies have been improved. But the development is still in its infancy. Researchers keep seeking a way to constantly change its attack surface. But the difficulty can be imagined. What's more, there has been little work to study how much proactively changing a network's configuration can increase the difficulty for attackers and thus improve the resilience of the system under attack. That is to say, we have little idea about the method to demonstrate the effectiveness of MTD and MSD.

Acknowledgments

This work was supported in part by a grant from a project numbered 2013ZX03006-002.

References

[1] www.cert.org.cn/publish/main/15/index.html
[2] Sun Z X, Jiang J L, Jiao L 2007 DDoS Attack Detecting and Defending Model *Journal of Software* **18**(9) 2246-57
[3] http://baike.niguo.com/doc-view-31665.shtml
[4] Liang Y, Deng W 2008 Verify Consistency between Security Policy and Firewall Policy with Answer Set Programming *Proceedings of Computer Science and Software Engineering* 196-200
[5] Zhang R, Qian D, Chen H 2003 Collaborative Intrusion Detection Based on Coordination Agent *Proceedings of the 4th International Conference on Parallel and Distributed Computing, Applications and Technologies(PDCAT'03) Chengdu China* 175-9
[6] Valeur F, Vigna G, Kruegel C, et al 2004 A Comprehensive Approach to Intrusion Detection Alert Correlation *IEEE Transactions on Dependable and Secure Computing* **1**(3) 146-69
[7] Wu N, Qian Y, Chen G 2006 A Novel Approach to Trojan Horse Detection by Process Tracing Networking, Sensing and Control *Proceedings of the 2006 IEEE International Conference* 721-6
[8] Tevis J-E J, Hamilton J A 2004 Methods for the Prevention, Detection and Removal of Software Security Vulnerabilities *Proceedings of the 42nd annual Southeast regional conference ACM*
[9] He, Zhang 2005 An Efficient and Secure Dynamic Group Signature Scheme *Journal of Software* **16**(4) 609-15
[10] Kim H J, Lim J I 2010 Efficient and Secure Member Deletion in Group Signature Schemes *Information Security and Cryptology-ICISC 2000 Berlin Springer-Verlag* 150-61
[11] Xiao B, Chen W, He Y H 2005 An active detecting method against SYN flooding attack *Proceedings of the 11th IEEE International Conference on Parallel and Distributed Systems* 1 709-15
[12] Kim Y W, Lau W C, Chuan M C 2004 Packet score: Statistical-Based overload control against distributed denial-of-service attacks *Proceedings of the 23rd Annual Joint Conference of the IEEE Computer and Communications Societies* 4 2594-604
[13] http://news.163.com/08/0813/10/4J7I603C00011MTO.html
[14] Thimbleby H, Anderson S, Cairns P 2000 A Framework for Modeling Trojans and Computer Virus Infection *The Computer Journal* 41 444-58
[15] Liu H, Zheng L 2010 Application and research on active protection for campus network based on the multicores UTM *International Conference on Multimedia Information Networking and Security* 589-92
[16] Zhao J, Guo S, Zheng K, Niu X, Jiang Y 2010 A Active Defense Model for Web Accessing Dos Attack *Journal of Computer Research and Development* **29**(8) 314-8
[17] Fuchsberger A 2005 Intrusion Detection Systems and Intrusion Prevention Systems *Information Security Technical Report* **10**(3) 134-9
[18] Chan A C-F 2011 Efficient Defence Against Misbehaving TCP Receiver DoS Attacks *Computer Networks* **55**(17) 3904-14
[19] Sun Q D, Zhang D Y, Gao P 2005 Detecting Distributed Denial of Service Attacks Based on Time Series Analysis *Chinese Journal of Computers* **28**(5) 767-73
[20] Sadasivam K, Samudrala B, Yang T A 2005 Design of network security projects using honeypots *University of Huston-Clear Lake* 282-93
[21] Chinese Honey net Project, http://www.honeynet.org.cn/

[22] Balas E, Viecco C 2005 Towards the Third Generation Data is Capture Architecture for Honey nets *Computer and Information Technology* 90-2
[23] Barrett D 2011 Hackers penetrate nasdaq computers http://online.wsj.com/article/
[24] National Cyber Leap Year Summit 2009 co-chairs' report, networking and information technology research and development *Technical report* 2009
[25] Matthew D, Stephen G, William U, et.al 2011 MT6D: A Moving Target IPv6 Defense *IEEE Communication Committee* 1321-6

Authors

Qing Zhang, January, 1991, Dongying, Shandong, China.

Current position, grades: master degree, graduate student at Zhengzhou University since 2009.
University studies: BS degree in communication engineering from Nanjing University in 2009.
Scientific interest: mobile communication security.

Caixia Liu, October, 1974, Weihai, Shandong, China.

Current position, grades: Associate professor in the School of Zhengzhou University.
University studies: PhD degree from the Zhengzhou University.
Scientific interest: mobile communication, social network.
Publications: 30 papers.

Ganqing Lu, December, 1991, Jining, Shandong, China.

Current position, grades: Master degree, graduate student at Zhengzhou University since 2009.
University studies: BS degree in communication engineering from Poly-technic University of Shenyang in 2009.
Scientific interest: mobile communication security