DOI 10.15302/J-SSCAE-2016.06.014

Mimic Defense Technology

Luo Xingguo[1], Tong Qing[2], Zhang Zheng[2], Wu Jiangxing[1]

1. National Digital Switching System Engineering & Technological R&D Center, PLA Information Engineering University, Zhengzhou 450002, China
2. State Key Laboratory of Mathematical Engineering and Advanced Computing, PLA Information Engineering University, Zhengzhou 450001, China

Abstract: Cyberspace security is in an unbalanced state, in which it is easy to attack and difficult to defend. Active defense technology is a new direction in cyberspace security research, which is attracting increasing attention. This paper summarizes the development of active defense via the introduction of intrusion-tolerant technology and moving target defense technology. Furthermore, the theory, implementation, and testing of mimic defense are introduced. Based on a comparison of mimic defense with intrusion tolerance and moving target defense, the research direction and the key points of cybersecurity rebalancing strategy are proposed to provide a reference for the development of national cybersecurity.
Keywords: mimic defense; active defense technology; cybersecurity rebalance

1 Current state of cyberspace security

With the advancement of social informatization and global networking, the dependence of national security, politics, economy, and social development on cyberspace is increasing. Thus, cyberspace is an important support for social functioning and activities. Cybercrime, cyber-terrorism, hacking, and cyber-warfare are threatening national security; this forces countries to elevate cyberspace security to a strategic level of national security, to emphasize the importance and significance of cyberspace for national interests and national security, and to begin to envision cyberspace as the fifth domain after land, sea, air, and space.

At present, the attack and defense state of cyberspace is that it is easy to attack and difficult to defend. Moreover, this state has caused an asymmetry between attack and defense in many aspects. In design, production, supply, and service chains, cyberspace information systems have lost control of credibility and security risks. This means that no country or organization can fundamentally eliminate security vulnerabilities in information systems or network infrastructures. On the other hand, if an attacker discovers and exploits one of these vulnerabilities successfully, it can lead to unpredictable security risks to the information system.

Most defense technologies and products, such as firewalls, anti-virus software, and signature-based intrusion detection technologies, are widely used. However, these technologies are based predominantly on blocking and detection, and are, to a certain degree, passive and lagging [1]; thus, they are a passive defense. These passive defense technologies can barely deal with unknown vulnerabilities and backdoor threats, and have certain defensive deficiencies.

As passive defense technologies face a dilemma in that they are unable to deal with unknown vulnerabilities and backdoor threats, active defense technologies have developed gradually and become the focus of study and research. Active defense refers to a type of defense technology with the ability to achieve defensive deployment and defend effectively against threats prior to detection of the specific attack methods or steps. Compared with passive defense technologies, active defense can reduce the attack destruction on the system, and provide better protection against the occurrence or performance of attacks, especially unknown attacks. Active defense achieves a more proactive and active defense; examples are intrusion tolerance, moving target defense, and mimic defense. Mimic defense is a burgeoning active defense technology, and its advantages have been tested in practice and in mimic defense technology applications. The practical

Received date: 10 October 2016; **revised date:** 25 October 2016
Corresponding author: Luo Xingguo, National Digital Switching System Engineering & Technological R&D Center, PLA Information Engineering University, Professor. Major research fields include communication network and cyberspace security. E-mail: lxg@ndsc.com.cn
Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10)
Chinese version: Strategic Study of CAE 2016, 18 (6): 069–073
Cited item: Luo Xingguo et al. Mimic Defense Technology. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.014

tests have proved that it has considerable development prospects in the cyberspace defense. Mimic defense is expected to become a strong starting point for cybersecurity rebalancing strategies.

2 Development of active defense

Relative to traditional defense technologies, active defense technology takes the initiative to locate and deal with possible attacks at any time prior to system attack. Traditional defense methods, such as intrusion detection, virus detection, and firewalls, usually lag the attacks. Moreover, these methods require analysis of the behavioral characteristics; the virus code to propose pertinent defensive measures; supplementation sandbox, honeypot, and other means to capture attacks; and a reduction in hardware and software vulnerabilities via patching and upgrading [2]. However, it is difficult to eliminate fundamental vulnerabilities in these methods; in addition, they cannot deal well with unknown vulnerabilities and backdoor threats. The goal of active defense technology is usually to construct a secure system architecture, or operation mode, to increase the difficulty and reduce the probability of attack. Thus, active defense technology has a strong resistance to new and unknown attacks, and is a hot topic in cybersecurity research.

The early form of active defense technology is intrusion-tolerant technology, which is developed from fault-tolerant technology. Fault-tolerant technology was originally proposed for computer systems, especially distributed systems, to solve the consistency problem. In the 1980s, fault-tolerant technology was applied for the defense of malicious vulnerabilities. This "fault tolerance" developed into "intrusion tolerance," which resulted in the concept of intrusion-tolerant technology [3]. Intrusion tolerance uses fault-tolerant technology to achieve tolerance and maintain the system survivability and flexibility, which was the focus of information system security technology at that time. A system based on intrusion-tolerant technology is called an intrusion-tolerant system (ITS). ITSs do not have a well-defined and widely adopted definition. As a generalization, an ITS is a system that can continue to work correctly and provide the expected service to users, despite successful attack on some components [4–7].

ITSs are divided into three types: detection-triggered, algorithm-driven, and hybrid. The detection-triggered type mainly detects the intrusion behavior through intrusion detection, and then triggers the system recovery operation to clear the intrusion, thereby fulfilling the purpose of intrusion tolerance. The algorithm-driven type usually masks partial failure by voting, and includes the majority and Byzantine voting algorithms. The hybrid type, such as SITAR, combines the two types discussed, and performs the voting and also detects internal system errors.

The common goal of intrusion tolerance is to ensure availability and flexibility of the system. This involves maintaining the normal service or switching the server in the shortest time to minimize the mean time to failure as the system is destroyed. Intrusion-tolerant technology is developed prior to the concept of active defense, but incorporated characteristics of active defense. Owing to limitations in the features of cybersecurity threats at the time, there are several limitations in the design of ITSs. Despite this, the proposal and rich design schemes have provided a starting point and foundation for the development of active defense technology.

Owing to the high cost of redundancy, research on intrusion-tolerant technology gradually declined after a period of approximately 20 years. To solve the dilemma of cyber defense, some countries, led by the USA, shifted the ideas of defense, and assigned active prevention of unknown vulnerabilities or threats as the goal, and a substantial increase in cyber attack risk and cost as the means. The focus was the enhancement of the flexibility and dynamics of cyber defense. They vigorously explored new technologies for proactive defense, and developed theories and technologies of revolutionary innovation to ensure the overwhelming superiority of the USA in cyberspace. Thus, a series of strategies, plans, and programmatic documents were developed to carry out the top-level design. In 2011, the US National Science and Technology Council (NSTC) released a plan entitled "Trustworthy Cyberspace: Strategic Plan for the Federal Cybersecurity Research and Development Program." Moving target defense (MTD) is defined as a revolutionary defense technology that changed the rules of the game [8]. Moreover, a framework was devised; it requires federal government, industries, and academic institutions to participate in the cybersecurity R&D framework to ensure the implementation of R&D program.

Encouraged by the USA, other countries including Russia, Britain, France, India, Japan, Germany, and Korea have followed suit in upgrading cyberspace security to a national strategic level. They comprehensively promoted the relevant system, power creation, and technological innovation in an attempt to position themselves favorably in the development of a new global cyberspace pattern. Active defense technology, which is characterized by a proactive change to the system and an increase in the attack difficulty, has become the frontier of cyberspace defense.

The goal of moving target defense is to design flexible systems that can reliably operate in non-secure environments. The technology vision is to develop, analyze, and deploy defender-controlled, time-varying migration and changing mechanisms and strategies across multiple system dimensions, to limit exposure of vulnerabilities, reduce attack opportunities, and increase the cost of attack significantly [9]. Moving target defense technology has been applied in the network layer, platform layer, running environment, software layer, and data layer. The common characteristic is that the assurance of the system's dynamics, randomness, and unpredictability is made by changing the configuration, composition, or state of the system dynamically. Thus, the attacker finds it difficult to locate the target and conduct effective attacks.

Moving target defense changes the static design of the past and proposes an increase in dynamics to improve security. It is one of the typical concepts of active defense. The proposal of moving target defense, to a large extent, increases the popularity of active defense research.

3 Theory and practice of mimic defense

In recent years, with the exposure of several shocking worldwide cybersecurity events, the focus on cyberspace security has increased globally. Under the guidance of the national cyberspace security strategy, mimic defense aims at solving the problems of unknown vulnerabilities and backdoors in cyberspace, and proposes the method of constructing a risk-controlled and secure system in which the modules are prone to failure [2].

A mimic defense technology is based on mimic computing of a varying structure in the function-equivalent condition. It has the highly reliable non-similar redundancy fault-tolerance mode as the basic framework, and the multi-mode decision under the non-cooperation condition as the core mechanism. It injects uncertainty into the function and external structure. Mimic defense introduces a hybrid scheduling strategy using dynamic heterogeneous redundancy construction, and uses the re-constructional, reconfigurable, re-definable, and virtualized construction methods of dynamic heterogeneous redundancy to enhance the uncertainty so that the difficulty in detection increases nonlinearly, and the attack is transformed into a minimal probability event.

At present, the mimic defense technology has been practiced in a router and web server based on the principle of validation, and productization and other verification studies are in progress.

From January to June 2016, commissioned by the Ministry of Science and Technology of the People's Republic of China, the Science and Technology Commission of Shanghai Municipality organized nine authoritative testing facilities, including the National Research Center for Information Technology Security, to form a joint test team to conduct a testing and verification on the mimic defense principle verification system.

The tested objects are mimic defense principle verification systems in two application fields. One is a mimic router or switch principle verification system in the category of information and communication network infrastructure, and the other is the principle verification system of a mimic web server in the domain of network information service. To test the endogenous defense mechanism of the mimic defense system, the testing procedure stipulates that a tested object must not install any protection tools. In the testing process, it cannot carry out any incremental development such as vulnerability repair or backdoor blocking, and cannot use protections such as firewalls, encryption authentication, and other security measures.

The testing uses a variety of methods and means, including black-box, white-box, penetration, and comparative testing, as well as pre-building backdoor and the injection of Trojan virus. The following five questions are tested and verified:

(1) Whether the mimic defense system can conceal the unknown vulnerabilities and backdoors in the mimic system.

(2) Whether the attacker can exploit the unknown vulnerability in the mimic system to inject the unknown Trojan virus.

(3) Whether the defender can effectively suppress the cooperative attack based on unknown factors in the mimic system.

(4) Whether the use of incredible and uncontrollable hardware and software components is allowed in the mimic system.

(5) Whether the running environment allow the "toxic carrier" in the mimic system.

In the test, 13 classes, 113 items, and 204 testing cases were completed. All testing and verifications were conducted under the premise of guaranteeing the service function and performance of the target objects. The results of testing and verifications are in good agreement with the theoretical expectation. The results of the testing and analysis show that the system tested is a successful representation of the application of the theory and methods of mimic defense. Simultaneously, these results prove the correctness and feasibility of the mimic defense theory. Furthermore, they show that the engineering application yields a theoretical and practical solution to the problems in cyberspace security defense.

Mimic defense is an endogenous security architectural technology, with natural immunity against the unknown vulnerabilities, the traps or backdoors, as well as some unknown viruses and Trojans within the architecture. It can integrate with the passive defense means to form a confrontation against the known or unknown attacks in cyberspace. However, mimic defense does not attempt to solve all cyberspace security problems simultaneously and does not expect to build security systems independently. It does not exclude the integration of any defensive system and technical means that have proved the security effect, and does not hinder future acceptance of new security technologies and means in future. In short, mimic defense is a complementary means to existing cyberspace security defense system and is technically integrated into the products with autonomy and controllability.

4 Advantages and challenges of active defense

Mimic defense, intrusion tolerance, and moving targets are all categorized as an active defense technology. However, they vary in terms of proposing background, implementing methods, technology vision, and so on. The main purpose of intrusion tolerance is to maintain system availability, which gives the system good survivability and recovery ability. This reduces the average fault time, improves the survivability of the system, and ensures the reliability of services and data. However, there is limited research regarding intrusion tolerance, and discussion on cost and performance are rare. Intuitively, redundancy and voting may lead to high resource costs and time delays, which may be the

main reason for the decline in intrusion-tolerant technology.

Moving target defense can improve the threshold of attack, and play a certain role in hiding the target. This is because the attack behavior generally has a strong pertinence. Therefore, dynamic changes in the system to reduce the static decrease can make it difficult for attackers to locate the target, and can also increase the difficulty of launching attacks. However, to maintain a dynamic and effective defense, it is necessary to gain a high changing frequency, which may cause some loss in the system performance. The compromise between the performance and the change frequency is one of the focuses in the research on moving target defense. On the other hand, the system that presents diversity is a single-state system at a specific time, which may provide a wide attack surface and more attack targets to the attacker, thereby counteracting the defense of the system.

Mimic defense can disturb the information chain between attackers and attack targets and disrupt the judgment of the attacker, thus causing difficulty in launching, maintaining, and reproducing the attack. Mimic defense can not only maintain availability, but can also play a role in hiding the attack target. In contrast to the concealment principle of moving targets, mimic defense neutralizes or obscures the output of the attack targets by voting, thus rendering the attacker to believe that the attack was ineffective, which disrupts the attacker's judgment. Compared to intrusion-tolerant technology, mimic defense tends to be more protective in overall security, rather than only the availability. The technical combination of mimic defense has the potential of tuning and can achieve relatively high defense with relatively low resource cost, and it has good development prospects.

The research and development of intrusion tolerance and moving target technology is focused on developed countries (mainly the USA). Although China's academic fields have attempted to follow up, researches are lagging. Mimic defense is the first domestic proposal of cyberspace defense technology. As the importance of cyberspace security continues to be elevated, China must take the initiative to accelerate the construction of China's independently controllable defense strategy system, build active defensive fortresses, break the imbalance in the attack-defense game, and support the reconstruction of China's cyberspace security status.

5 Cyberspace security rebalancing strategy

Mimic defense technology, as an emerging active defense technology in China, facing an untrustworthy soft and hard component supply chain, assists in achieving cybersecurity and informatization goals in the era of globalization. Mimic defense contributes to the elimination of the tangible or intangible barriers caused by the integration of cybersecurity and informatization to the global free trade. In addition, it deters and decreases the threat of attacks based on unknown vulnerabilities, backdoors, viruses, and Trojans; significantly increases attack costs; and creates a diversified market prosperity rather than exclusive competition. Mimic defense provides a new idea for the development of national independently controllable information systems. It is necessary to make full use of national resources to accelerate the promotion of mimic defense applications, so as to provide a strong grasp for cybersecurity rebalancing strategy.

5.1 Application and promotion

Based on the research and testing of the pre-principle verification system of mimic defense system, the technological achievements of hardware and software that can be converted into products, such as the mimic router or switch, mimic web server, mimic file system or storage system, and mimic firewall or gateway, should be further developed.

As a strategic task, there is a need to mobilize society to develop and improve the research into the theory and method of mimic defense, further refine and optimize key technologies, and promote innovation and integration of technologies to provide complete theoretical and technical systems for productization and customization development of mimic defense.

Mimic defense should be introduced to industries by combining it with the characteristics of the field, studying customized technologies and carrying out demonstrations of applications, to promote the application of mimic defense products in various industries and the industrialization of mimic defense technology.

5.2 Standardization

The mimic defense research team has a responsibility and obligation to develop mimic defense technology standards, and these standards should include index systems and test specifications related to mimic defense technology and active defense technology. In addition, this team should prepare a grading index system that meets mimic defense equipment or assessment requirements of system certification, forming national and industrial standards, and improve the development of mimic and active defense technology.

5.3 Policy strategies

In policy and strategy research, China should exert itself to take advantage of the leading technology position, seize industry and market, form the new defense capacity of cyberspace as soon as possible, and release innovation vitality and motivation for the cybersecurity rebalancing strategy.

References

[1] Kenkre P S, Pai A, Colaco L. Real time intrusion detection and prevention system [C]// Satapathy S C, Biswal B N, Udgata S K, et al, editors. Proceedings of the 3rd international conference on

frontiers of intelligent computing: theory and applications (FICTA) 2014. Switzerland: Springer International Publishing, 2015 (1): 405–411.

[2] Wu J X. Mimic security defense in cyber space [J]. Secrecy Science and Technology, 2014, 10 (1): 4–9.

[3] Powell D, Stroud R. Project IST-1999-11583 malicious- and accidental-fault tolerance for internet applications: conceptual model and architecture of MAFTIA [R]. Newcastle: University of Newcastle upon Tyne, 2003.

[4] Jajodia S, Ghosh A K, Swarup V, et al, editors. Moving target defense: Creating asymmetric uncertainty for cyber threats [M]. New York: Springer, 2011.

[5] Gupta V, Lam V, Ramasamy HG V, et al. Dependability and performance evaluation of intrusion-tolerant server architectures [M]. Berlin: Springer, 2003.

[6] Wang F, Jou F, Gong F, et al. SITAR: A scalable intrusion-tolerant architecture for distributed services[C]// Proceedings of the 2001 IEEE— workshop on information assurance and security. New York: United States Military Academy, 2003.

[7] Malkhi D, Reiter M. Byzantine quorum systems [J]. Distributed Computing, 1998, 11 (4): 203–213.

[8] Kewley D L, Bouchard J F. DARPA information assurance program dynamic defense experiment summary [J]. IEEE Transactions on Systems, Man, and Cybernetics. Part A, Systems and Humans, 2001, 31 (4): 331–336.

[9] Okhravi H, Hobson T, Bigelow D, et al. Finding focus in the blur of moving-target techniques [J]. IEEE Security & Privacy, 2014, 12 (2): 16–26.