DOI 10.15302/J-SSCAE-2016.06.013

A Review of the Basic Theory of Mimic Defense

Si Xueming[1], **Wang Wei**[1], **Zeng Junjie**[1], **Yang Benchao**[1], **Li Guangsong**[1], **Yuan Chao**[1], **Zhang Fan**[2]

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

Abstract: With the development of the Internet, the major issues of cyberspace security related to national security have arisen. This paper first introduces some of classic cyber defense technologies. It then introduces the technology of mimic defense, including mimic defense systems, scientific problems with mimic defense, and the theoretical framework. The effectiveness of a mimic defense system is also analyzed in comparison with traditional cyber defense technologies. Finally, some problems worthy of study are presented regarding the basic theory of mimic defense.

Keywords: mimic defense; cyberspace; moving target defense; mimic transformation

1 Introduction

Many powerful countries have recently begun paying more attention to the rising field of cyberspace security, and are rivaling each other in terms of its development, control, and domination. With the increasing importance of cyberspace security, vital problems need to be resolved regarding the core technologies of national interest and security [1].

Traditional cybersecurity defense is built on existing Internet network infrastructure, including the establishment of a security gateway, firewall, security router/switch, intrusion detection, virus protection, user authentication, access control, data encryption technology, security assessment and control, trusted computing, and hierarchical protection, and improve cybersecurity and its application. It is based on different traditional security technologies. However, increasing number of cybersecurity accidents have been exposed, which indicates the presence of a serious flaw in the current system. Hence, the breakthrough of the limitation of a static and passive defense technology depending on prior knowledge, the proposition of innovative ideas regarding dynamic cybersecurity defense, and the study on the basic theory and key technologies of the new cybersecurity architecture have become important research directions in the field of cybersecurity.

2 Related theoretical research results at home and abroad

2.1 Moving target defense technology

Moving target defense (MTD) is one of the revolutionary technologies in cyberspace proposed by the United States in recent years, and is "changing the rules of the game." Its construction, evaluation, and deployment mechanisms and strategies are diverse and ever-changing [2–5]. Such variability can increase the difficulty and cost of attacks, effectively limiting the vulnerability of exposure and the chances of being attacked, and improving the flexibility of the system. In a theoretical study, Zhuang et al. [6]. proposed a preliminary theory as a solution to the validity of MTD. In addition, they formally discussed the key concepts and basic properties of the MTD system and proposed an MTD entropy hypothesis. Finally, they determined that the larger the entropy of the system configuration, the more effective the system becomes

---

Received date: 21 October 2016; **revised date:** 1 November 2016

Corresponding author: Si Xueming, State Key Laboratory of Mathematical Engineering and Advanced Computing, PLA Information Engineering University, Professor. Major research fields include network cryptography and mimic defense. E-mail: sxm@fudan.edu.cn

Funding program: CAE Major Advisory Project "Research on Cyberspace Security Strategy" (2015-ZD-10); National key research program (2016YFB0800101, 2016YFB0800100); Open program of State Key Laboratory of Mathematical Engineering and Advanced Computing (2015A14); National natural science foundation of China (61521003, 61572520, 61602512).

Chinese version: Strategic Study of CAE 2016, 18 (6): 062–068

Cited item: Si Xueming et al. A Review of the Basic Theory of Mimic Defense. *Strategic Study of CAE*, http://10.15302/J-SSCAE-2016.06.013

2.2 End-hopping technology

End-hopping technology refers to that both parties of communication in an end-to-end data change the port, address, time slot, encryption algorithm, and even the protocol information pseudo-randomly according to an agreement to undermine enemy attacks and interference and achieve active protection.

An active protection model based on end hopping includes four modules, i.e., early warning analysis, cooperative control, end information management, and task switching, as well as several task clusters. The early warning analysis module is responsible for information collection and analysis of attacks suffered by the current Internet network. The cooperative control module is the core of the whole system, and it is responsible for the coordination of the module to achieve network defense. The end-information management module is used to pseudo-randomly generated end information jump patterns. A task-switching module is responsible for task switching in accordance with instructions regarding the co-control module interference, communications, honeypots, and other tasks required to achieve a collaborative defense. The results illustrate that compared to traditional Internet network-protection technologies, terminal information hopping has the advantage of a strong anti-attack capability, initiative, anti-interception ability, and performance improvements [7].

2.3 Dynamic game model based on a mimic honeypot

A mimic honeypot refers to a simulation of the evolution of pseudo-mimicry and a confrontation game through the integrated use of a protective coloration mechanism of simulated service environment and a warning coloration mechanism of the simulated honeypot characteristics based on a traditional honeypot network to effectively confuse and trick an attacker into achieving a network confrontation. Protective coloration refers to that honeypots imitate the characteristics of the surrounding server and Internet network environment in hardware, software, data, service information, and other aspects, making it difficult for attackers to identify the presence of the honeypots. Warning coloration refers to that the server imitates the honeypot characteristics regarding hardware, software, or data to allowe attackers to identify a system as a honeypot and avoid an attack [8,9].

A honeypot defense is a rational and non-cooperation decoy process in which both the defender and attacker participate. The two strategies are interdependent, and both expect to protect their own information and obtain information on the other side to maximize their profit. Thus, a non-cooperative incomplete information dynamic game is formed. From the point of view of different players in the game, the game opponents have different types: from the attacker's perspective, the game opponent is no longer only a rival with "real service" in this single type of service, but rather an increased "honeypot" or "pseudo honeypot" of the two types of deceptive services. From a defensive perspective, the game opponents have legitimate users and attackers of two different types of visitors. According to whether or not an attacker knows the existence of a pseudo honeypot, the conditions of the two strategies to reach Bayesian-Nash equilibrium can be determined.

2.4 Dissimilar redundancy computer system

A computer system of dissimilar redundancy is a computer system used in a flight control system, which uses a different, completely independent design group through different development languages and different development tools, and runs on different processors, to avoid common faults and improve the mission reliability of the critical system. The designer applies a simplified Markov model to a reliability analysis. The results show that the reliability of a dissimilar redundancy computer system（DRCS）is improved and that the mean time between failures (MTBF) is more than 9 000 h [10].

3 Formalized description of the information system and its security

To carry out reasonable mathematical modeling in cyberspace, and determine the relationship between various perplexing factors and their influence, more scientific and reasonable descriptions of the information system are needed. In addition, formalized methods are then used to describe a mimic defense system. This formalized description of a mimic defense system can provide a theoretical solution to explain how to apply the ideas regarding mimic defense to protect an information system in cyberspace and introduce the principle and method of a mimic transformation.

3.1 Formalized description of a traditional information system

Based on different perspectives and research purposes, information systems can be described using different core elements. Generally, there are many elements of an information system, such as software, hardware, operations, and strategies. For a convenient expression, a vector group (v_1, v_2, …, v_n) in a multi-dimensional space can be applied as a tool (Fig. 1).

Information systems are usually not static and often need

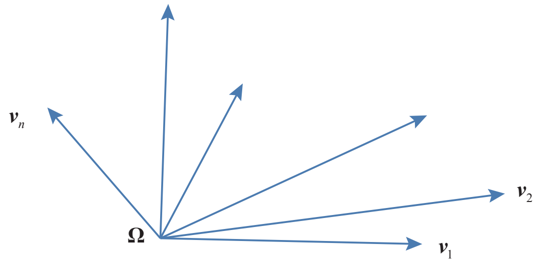

Fig. 1. Multi-dimensional vector diagram of an information system.

to change according to the external or surrounding conditions, and thus, an information system can be affected over time. If the current research focuses on m information system elements in addition to the time factor, then the information system may have a number of different states at different times. Of course, these different elements can be further subdivided into smaller indicators, that is, according to the needs of the research issues, and the appropriate size of the representation of an information system can be selected.

3.2 Example of an information system from the perspective of security

There are many factors related to the security of an information system in cyberspace, and a specific factor that has an impact on information system security is called a basic element, which is the basic unit we intend to study. These basic elements can usually be classified as the network, platform, running environment, software, data, and other categories, and form a different level of the system.

In general, the number of basic elements of each factor differs, and to describe the unified factors and basic elements, we assumed that the information system has m factors, each of which has n basic elements. Let $n = \max\{n_1, n_2, ..., n_m\}$, $i = 1, 2, ..., m$, where n_i is the number of basic elements of the ith factor. If the number of basic elements of one factor is less than n, then the number of basic elements is expanded by an empty element. Let x_i^j be the state of the jth basic element of the ith factor, then the state of the information system at time t can be represented through matrix $\Omega(t)$.

$$\boldsymbol{\Omega}(t) = \begin{pmatrix} x_1^1(t), x_1^2(t), \cdots, x_1^n(t) \\ x_2^1(t), x_2^2(t), \cdots, x_2^n(t) \\ \vdots \qquad\qquad \vdots \\ x_m^1(t), x_m^2(t), \cdots, x_m^n(t) \end{pmatrix}$$

To facilitate this study, we assumed that the current security-related factors are divided into the following five categories: the network, platform, running environment, software, and data.

(1) Network factors include the form of the network connectivity, communication standards, security protocols, topology, network address, and network port.

(2) Platform factors refer to the hardware, support software, and other components that the information system depends on, including a variety of hardware devices, operating systems, processor architecture, virtual machines, and storage systems.

(3) The running environment factors refer to the interfaces between the platform and the application of upper layer, including the instruction set and address space.

(4) Software factors refer to a variety of application software types installed in the information system, including the executive entities of different software, the program instruction sequence, the instruction format, and the internal data structure.

(5) Data factors refer to all types of data stored in the system related to the information services, such as the format, syntax, and coding. The above network, platform, running environment, software, and data contain all elements that are closely related to the security of an information system. In this sense, the information system can be regarded as being composed of network, platform, running environment, software, and data in a five-tier architecture.

4 Mimic defense system and its formalized description

The existing information systems in cyberspace are mostly static, similar, and deterministic, and their security flaws are persistent, stable, and usable at the architecture level; they can be easily attacked or controlled. Attacks against these systems, based on vulnerabilities and backdoors, are highly dependent on the static nature, similarity, and determinacy of the target system. The longer the target system is exposed, the more time an attacker has to study its operational rules, discover its weaknesses, and create and validate attack methods. If one can dynamically change the state of an information system, blocking or disrupting the static nature, similarity, and determinacy that the chain of attacks depends on, risks to system security can be controlled.

4.1 Mimic defense system

A mimic defense system generally consists of information systems, mimic transformations, heterogeneous executive entities, and voting devices, among other elements. A mimic defense system can proactively change the state of the elements of an information system, changing the state of the information system itself. Such a method is called a mimic transformation. A mimic transformation can effectively change the static and deterministic nature of the system, which cyber attacks rely upon. A mimic transformation is described in detail in the following section. The introduction of a voting device is aimed at confusing an attacker further, reducing the risk of the system being attacked, and increasing the system reliability. Moreover, uncertainty mapping is introduced between the meta-function of a target object and its equivalent multivariate implementation structure or algorithm, concealing the real relationship between the system input and output. An MTD system can be seen as a special case of a mimic defense system, which makes the system possess dynamic characteristics through certain mimic transforms; however, the system does not apply a heterogeneous redundant architecture [11,12].

4.2 Mimic transformation

A mimic transformation is implemented by changing the basic elements of the information system components. A mimic transformation can transform only one basic element of a certain constituent element, transform a plurality of basic elements of the constituent element, or transform the basic elements of a plurality of constituent elements at the same time, which can be regarded as the superposition of a plurality of basic mimic transformations. To achieve the goal of confusing an attacker, the transition of the information system between different states during its lifetime should be random. That is, the type of mimic transformation that should be used to change the state of the information system at different times, and the elements and basic components that should be transformed must have uncertainty and randomness.

A mimic transformation should satisfy the following properties:

(1) Functional equivalence: The system functions are the same before and after the mimic transformation.

(2) Security: The system security after the transformation is higher than that before the transformation.

(3) Randomness: An attacker cannot predict the state of the system after the transformation.

(4) Superposition: The effects of a number of mimic transformations acting on the system are equivalent to a more complex mimic transformation.

4.3 Design of the mimic transformation

The design of a mimic transformation is mainly based on the principles of heterogeneous redundancy, dynamism, randomization, fragmentation, and hiding and camouflage, and it needs to consider the characteristics of the constituent and basic elements at different layers. Changing the state of an element may cause other elements to change their state, which may affect changes in the system state. Therefore, this needs to be analyzed based on the specific situation. Here, we only consider the construction of different mimic transformations, changing a state to obtain a basic transformation, and do not consider the equivalence between mimic transformations changed from different element states.

(1) Heterogeneous redundancy principle

The heterogeneous redundancy principle is used to produce many heterogeneous executive entities or variants for the basic elements of the system, and switch randomly in these isomers according to a set of rules. At the platform layer, for example, the operating system is a basic element, and the heterogeneous redundancy principle is used to prepare a variety of different operating systems for an information system.

(2) Dynamism principle

The dynamism principle is used to make the state of the basic elements of an information system change dynamically. In a network layer, for example, the system IP address is a basic element, and dynamism is used to design a mechanism, dynamically changing the IP address of the system.

(3) Randomization principle

The randomization principle is used to change the basic elements of the information system into random information within a certain range. For the data-storage state element at the data layer, encryption is a well-understood mimic transformation that can change the stored information into random information.

(4) Fragmentation principle

Fragmentation is the main principle for the data layer, which indicates that a file can be divided into several fragments stored at different locations in order, or divided into more fragments stored in random locations. Assuming a file size of 1 Mb, a mimic transform can be designed as follows: The file is divided into 1 000 fragments, each 1 Kb in size. It is assumed that the number of file directories in computer system is 2 000, from which we randomly select 1 000, where we store the file fragments.

(5) Hiding and camouflage principle

The hiding and camouflage principle refers that a system proactively hides the true properties of a state to confuse an attacker. For example, we define a mimic transformation and change the suffix of the file name. Suppose that M is a PDF file, and through a transformation, its file name type is changed to a Word type ended with ".doc." Thus, if an attacker gets access to this file, the attacker cannot open it using Word, and will mistakenly believe it is a corrupt file and discard it. Thus, the transformation plays a role in protecting the file.

Based on the above principles, according to the basic elements at different layers, we can design the corresponding basic mimic transformations, and then construct more complex mimic transformations than these basic mimic transformations. In Table 1, we list the main elements for the five-layer architecture of an information system, where some transformations can be designed.

5 Scientific problems and theoretical framework of mimic defense

5.1 Scientific problems of mimic defense

The goal of theoretical research on the security of mimic defense is to solve the scientific problems regarding the mechanism of active mimic defense in theory, and to establish a basic theoretical security system of mimic defense. Based on this, the key technologies applied in the security of mimic defense and the evolution methods of an existing system to a security system of mimic defense are studied. The basic scientific problems of mimic security include the rules of cyber-attack behaviors, the mimic security mechanism, the validity of mimic security, and a quantitative assessment of the mimic security system.

The study on the rules of cyber-attack behaviors is based on the cyber-attack methods of the information system. A model of the cyber-attack chain has been established. The relationships between the establishment of the attack chain and the static nature, determinacy, similarity, and persistence of the network system have been researched. In addition, a formalized description method of the exploitation mechanism of vulnerabilities has been studied.

Table 1. Mimic transformation in a mimic defense system at different layers.

The main layers or constituent elements	The basic elements in a layer or unit	The main mimic transformations
Network layer	Address, protocol, port, etc.	Change the IP address of the target information system Change the port of the target system Change the protocol used by the target system The superimposition of the above three transformations
Platform layer	Operating systems, heterogeneous redundant devices, virtual machine instances, storage systems, etc.	Change the operating systems Heterogeneous device switching Change the virtual machine instances Change the storage systems The superimposition of the above four transformations
Running environment layer	Instruction set, address space, etc.	Instruction set randomization Address space randomization The superposition of the above two transformations
Software layer	Software heterogeneous variants, software program instruction sequence, instruction format, internal data structure layout, etc.	Software variant switching Change the executive instruction sequence and form Dynamic storage resource allocation scheme The superimposition of the above three transformations
Data layer	Data form, syntax, coding, etc.	Change the data form Change the data syntax Change the data coding The superimposition of the above three transformations

The mechanism of mimic security has been studied regarding the reconfiguration, polymorphism, randomization, and other characteristics of the system, as well as the degree of change in its static nature, similarity, determinacy, and persistence. The mechanism of the damage to the formation of the attack chain has been described, and the attack success rate has been reduced to reveal the nature of risk control of mimic security. Through the abstraction of relevant concepts, a formalized language to describe the basic idea of mimic security has been established.

The scientific proof of the validity of mimic security is based on a rule of cyber attacks, as well as a formalized description of the mimic security system based on the mimic security mechanism.

A quantitative evaluation method for a mimic security system establishes a quantitative assessment model of the security evaluation of the mimic system. In addition, new problems brought about by the changes in the mimic security system structure are analyzed and compared with traditional information-security evaluation methods.

5.2 Theoretical framework of mimic defense

Based on the scientific problems of mimic defense, theoretical studies on mimic security are mainly concentrated on the following five aspects.

5.2.1 Analysis and modeling of the cyber attack behaviors

There are many methods of modeling for cyber attacks, such as attack language, attack tree, attack network, state transition diagram, and attack graph. The mimic defense system abstracts the information system into five layers, extracts the variable elements of each layer, and formalizes the description. In the attack and defense of an information system, attackers need to use five layers and their elements to achieve the purpose of the attack. An analysis of cyber attack behaviors is conducted mainly through the analysis of the attack process extracting knowledge related to the system and establishing a knowledge map. The attacked surface and knowledge flow are unified to represent the cyber attack behaviors, and a cyber-attack chain model is established.

5.2.2 Theory of mimic transformation

According to the idea of mimic security, a mimic transformation can be defined as follows.

$$\sigma\colon \boldsymbol{\Omega}(t_i) \rightarrow \boldsymbol{\Omega}(t_{i+1})$$

The domain of definition of this transformation is a set of all states of the system, $\boldsymbol{\Omega}$. The range is also $\boldsymbol{\Omega}$. Different elements of the transformation method correspond to different transformations, which is referred to as $\sigma = \{\sigma_1, \sigma_2, \cdots, \sigma_n\}$, where σ_1 denotes the mimic transformation of the first element, and so on. If $\boldsymbol{\Omega}(t)$ is represented by a (0, 1) sequence, then σ can be regarded as a scrambling sequence, where different scrambling sequences correspond to different transformations.

The goal of a mimic security system can be formalized as follows:

Condition 1: $sr\,(\boldsymbol{\Omega}(t, \sigma)) \leqslant a$, where sr denotes the function used by $\boldsymbol{\Omega}(t)$ to calculate the resources such as storage interconnections.

Condition 2: $pf\,(\boldsymbol{\Omega}(t, \sigma)) \leqslant \mathrm{b}$, where pf represents the performance function of $\boldsymbol{\Omega}(t)$, and b is a constant.

Under Constraint 1 or 2, the appropriate mimic transformation σ is chosen to achieve $\mathrm{Max}(sp_t|\sigma)$.

The mimic transform gives the mimic security system the characteristics of randomness, dynamism, and diversity, which effectively improves the determinacy, static nature, and similarity of a traditional system, as well as the security of the entire information system.

5.2.3 Construction methods for the mimic security system

The construction methods for a mimic security system mainly include the methods of situational awareness, mimic methods, and synergistic methods. The methods deploying a soft sensor in the mimic security network and application strategy, the awareness of security threat and security situation, and risk assessment and security-situation evolution prediction have been studied, and a unified description model, parameter set, description language, description method, reasoning rule, decision-making model, and a knowledge-based system are implemented to support perception, cognition, and decision-making. This can optimize and decide the intensity, active changes, synergetic timing of a mimic security system. This paper studies the mimic methods of randomization, diversification, and dynamism of a mimic security system to provide a specific method and a combined application method to implement a dynamic randomization mechanism, input-output agent mechanism, heterogeneous redundancy mechanism, fragmentation mechanism, single-line contact mechanism, as well as camouflage, honeypot, and other “deceptive” mechanisms.

5.2.4 Validity theory of mimic security

A study on the active defense theory and the mechanism with the characteristics of reconfiguration, diversification, and randomization verifies the validity of current mainstream cyber attacks. A study on the effective combination of various mimic defense mechanisms can establish a description for attacked surface for the mimic security defense of an information system. A study on the influence of mimic security defense on the attacked surface can describe its contribution to resisting attacks.

5.2.5 Quantitative assessment theory of mimic security

The traditional quantitative evaluation models of cybersecurity include a fault tree model, an attack tree model, a Petri Net model, a privilege graph model, and an attack graph model. Although these models have certain reference values, the characteristics of a mimic defense system are different from the deterministic, static, and similar aspects of these traditional systems. Therefore, it is necessary to establish an evaluation model for mimic cybersecurity according to the definition and characteristics of the mimic network and the attributes of security at all levels of the network, refine the evaluation indexes on different dimensions in the model, and construct a hierarchical mimic cybersecurity-evaluation index system. According to the evaluation index system and the safety factor model of the mimic network, the mappings between the safety index and the security element state of the mimic network are established, which can clearly depict the security protection capability of the mimic network based on the evaluation indexes. The security space is divided through clustering and other means, and the mimic cybersecurity grade is established.

6 Analysis of the validity of the mimic defense system

Under normal circumstances, the attackers divide the attack processes into several steps to achieve their goals. The results show that different mimic mechanisms enforce stronger security against cyber attacks. The analysis of the validity of the mimic defense system based on a cyber-attack chain model is shown in Table 2.

Heterogeneous redundancy mechanism: The redundancy mechanism can effectively defend against attacks based on vulnerabilities or backdoors. In particular, if each redundant component is heterogeneous, the probability of success in accessing the systems or elevating the operating privilege through such attacks will fall sharply.

Single-line contact mechanism: Through this mechanism, because of the different permissions in the sensitive paths and key links, the information and Information interception is incomplete, which may minimize the successful probability of attack.

Fragmentation mechanism: The files and system information are divided into storage slices and multi-path transmissions, which can effectively reduce the probability of success through illegal access to them. This means can effectively counter the information collection and information interception.

In the attack chain model, each attack chain, under different mimic mechanisms, can reduce the successful probability of a few steps to attack them, thereby reducing the probability of

Table 2. The analysis of the validity of the mimic defense system.

Security mechanism	Information collection	Accessing			Obtain permission		Information interception or destruction
		Password sniffer	Brute-force attack	Penetration testing tool	Password cracking	Vulnerability exploitation	
Heterogeneous redundancy mechanism				√		√	
Single-line contact mechanism	√					√	√
Fragmentation mechanism	√					√	√
Input /output agent mechanism	√						√
Random and dynamic mechanism	√	√	√		√	√	√

attacking the whole attack chain successfully. Therefore, and the probability of attacking a mimic security system successfully is less than that of attacking a traditional information system successfully.

7 Conclusions

Research on mimic security systems is still in its primary stage. Many researchers have focused on the formalized descriptions of an information system and a mimic defense system. Some specific methods to realize different mimic mechanisms have been proposed. In the next step, the basic theoretical research of mimic security will focus on a fine-grained formalized description of information systems, a formalized description of cyber attack behaviors, a classification and description of cyber attack scenarios, the security evaluation of cybersecurity, the detailed analysis on validity of five mechanisms of mimic security, and mathematical abstraction of a mimic security architecture.

References

[1] Zhang H G, Han W B, Lai X J, et al. Survey on cyberspace security [J]. Scientia Sinica Informationis, 2016, 46 (2):125–164. Chinese.

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

[3] Evans D, Nguyen-Tuong A, Knight J. Effectiveness of moving target defenses [M]// Jajodia S, Ghosh A K, Swarup V, et al, editors. Moving Target Defense—Creating asymmetric uncertainty for cyber threats. New York: Springer Publishing Company, 2011: 29–48.

[4] Han Y J, Lu W L, Xu S H. Characterizing the power of moving target defense via cyber epidemic dynamics [C]// HotSoS’14 proceedings of the 2014 symposium and bootcamp on the science of security. New York: Association for Computing Machinery (ACM), 2014: 1–12.

[5] Zhang X Y，Li Z B. Overview on moving target defense technology [J].Communications Technology, 2013, 46 (6): 111–113. Chinese.

[6] Zhuang R, DeLoach S A, Ou X M . Towards a theory of moving target defense[C]// MTD’14 proceedings of the first ACM workshop on moving target defense. New York: ACM, 2014: 31–40.

[7] Shi L Y, Jia C F, Lv S W. Research on end hopping for active network confrontation[J]. Journal on Communications, 2008, 29 (2): 106–110. Chinese.

[8] Li Z T, Xu X D. The analysis of dynamic honeypot and its design [J]. Journal of Huazhong University of Science and Technology (Nature Science Edition). 2005, 33 (2): 86–88. Chinese.

[9] Shi L Y, Jiang L L, Liu X, et al. Game theoretic analysis for the feature of mimicry honeypot [J]. Journal of Electronics & Information Technology, 2013, 35 (5): 1063–1068. Chinese.

[10] Zang H W, Han W, Gao D Y. Dissimilar redundancy computer system and reliability analysis [J]. Journal of Harbin Institute of Technology, 2003, 33 (3): 492–494. Chinese.

[11] Wu J X. Meaning and vision of mimic computing and mimic security defense [J]. Telecommunications Science, 2014, 30 (7): 2–7. Chinese.

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