International Journal on Data Science and Technology
2018; 4(3): 84-92
http://www.sciencepublishinggroup.com/j/ijdst
doi: 10.11648/j.ijdst.20180403.12
ISSN: 2472-2200 (Print); ISSN: 2472-2235 (Online)

The New Progress of Motive Target Defense Technology

Tan Tiantian[1], Wang Baosheng[1], Wang XiaoFeng[1], Cai Guilin[2], Luo Yuebin[1], Xiang Zheng[3]

[1]Department of Computer, National University of Defense Technology, Changsha, China

[2]Faculty of Crap, Crap 95942, Wuhan, China

[3]Department of Network, Hunan Institute of Information Technology, Changsha, China

Email address:

happinesschild@126.com (Tan Tiantian), wbs@nudt.edu.cn (Wang Baosheng), xf_wang@nudt.edu.cn (Wang Xiaofeng), caiguilin@nudt.edu.cn (Cai Guilin), luoyuebin@nudt.edu.cn (Luo Yuebin), happinesschild@126.com (Xiang Zheng)

To cite this article:

Tan Tiantian, Wang Baosheng, Wang XiaoFeng, Cai Guilin, Luo Yuebin, Xiang Zheng. The New Progress of Motive Target Defense Technology. *International Journal on Data Science and Technology*. Vol. 4, No. 3, 2018, pp. 84-92.
doi: 10.11648/j.ijdst.20180403.12

Received: May 19, 2018; **Accepted**: July 1, 2018; **Published**: August 16, 2018

Abstract: The concept of moving target defense (MTD) is an excellent solution proposed in USA to make the defender become dominant player while the defender is the disadvantage one in the game of defender and attacker. Focus on summarized the attack surface characteristic and functional connotation of moving target defense, according to the hierarchy in the execution stack, this paper classified and analyzed current moving target defense technologies into four categories, such as dynamic communication network, dynamic communication run-time environment, dynamic communication data and dynamic communication application, described the theory of every mechanism in each category, summarized the advantages and disadvantages of each mechanism. On the basis of the study of current mechanisms of moving target defense technologies, this paper designed a moving target defense system based on terminal information hopping and analyzed its anti-attack performance. The experiment result proven that system can effectively increase the time consumption and complexity of successful attack, and decrease successful attack rate by continually shifting the attack surface, our design greatly improved the strength of inactive defense. This study can provide the theoretical guidance for the design and implementation of muti-mechanisms moving target defense systems.

Keywords: Moving Target Defense (MTD), Active Defense, Communication Network Security, Shifting Mechanism, Survey

1. Introduction

Static characteristics of the current communication network, communication protocols and communication applications provide the attacker with plenty of time and convenience. Major existing defense mechanisms include eliminating bugs, attack code identification, public patches or starting with the behaviors of malicious code. However, each of these has its limitations on the effects. In order to change the disadvantage role of communications defender in the game of attack and defense [1], and improve the ability of anti-attack and flexibility of communication equipment and applications, researchers in USA proposed the concept of moving target defense (MTD) technology. The article which introduced MTD systematically in the domestic academia is few. Starting from the related concepts and development strategies, focus on current MTD technology research, analysis, this article classified the current MTD technologies into dynamic communication network, dynamic communication run-time environment, dynamic communication data and dynamic communication application, this paper then introduced the principle of each categories and the new progress. It can provide a guidance for the design and implementation of the future MTD technologies based on multiple mechanisms.

2. Relevant Concept

The major concepts of MTD include attack surface, attack surface shifting, moving target defense and moving target.

2.1. Attack Surface

The concept of a system attack surface was formally

defined by Manadhata [2] as a set of methods which allow attackers enter into system and make potential threats. Zhu [3] et al. defined the attack face as a set of system vulnerabilities which could be exploited by the attacker. Wei et al. defined the attack surface of an active virtual machine in the cloud service as the whole available resources [4]; Zhuang et al. believed that the system attack surface was composed of the system resources exposed to the attacker and the network resources that could be used to violate the system. [5]

2.2. Moving Target and Moving Target Defense

The White House National Security Council reported [6] that the moving target was a system that could be moved in multiple dimensions to reduce an attacker's advantage and had higher flexibility. The network security research and development of the rules of the game released in 2010[7] described the characteristics of moving target defenses as continuous shifting one or more of the system properties under management, made an attack surface unpredictable to attacker for a lower probability of successful attack.

As shown in table 1, current study argues that the connotation of motive targets defense technology should include the transformation of the target, the manageability, sustainability, diversity, and the rapidity of transformation. The technology to transform target is the key technology of moving target defense technology, all technologies which use attack surface transformation to make communication system unpredictable can be classified as moving target defense technology. [8, 9]

Table 1. *The functional connotation of MTD.*

Functional characteristic	Connotation
The transformation of the target	Shift the configurations and characteristics of current communication network, let target moving to result in defense easier than attack.
The manageability of transformation	Attack surface transformation must has an efficient manageability to ensure the sustainability of tasks and the function and performance of system.
Sustainability of transformation	Decrease static depended on attack and increase the complexity of attack.
Diversity of transformation	The method of transformation is diversity, the parameters range of attack surface is diversity, improve the security and flexibility of system in muti-dimensions
The rapidity of transformation	Lead the game and let information collected by attackers' failure rapidly.

3. Analysis of the Moving Target Defense Mechanism

According to the hierarchy in the execution stack, this paper classified the current moving target technologies into four categories: dynamic communication network, dynamic communication run-time environment, dynamic communication application and dynamic data, the four categories are shown as figure 1.

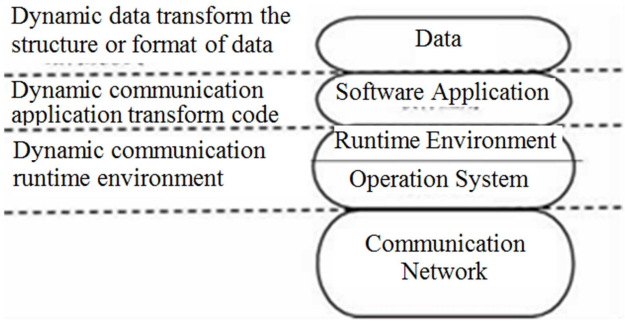

Figure 1. *The categories of motive target defense.*

3.1. Dynamic Communication Network

Using various encryption algorithms to shift the communication protocol, and even the information of both or one of communication terminal, such as the port, address, time slot, dynamic communication network mechanism dynamically transform network information to against the attack and interference through the attacker cannot collect information by traditional methods efficiently, or the effective information collected can be disable quickly, increase the time consumption and complexity of a successful attack, effectively restrain the loss of attack.

3.1.1. Translation Mechanism Based on Port Information Calculation

Port information calculation is that both communication terminal calculate the next connection information using the known information (such as address, port, key, time, etc.).

1) Dynamic network address translation.

Dynamic network address translation (DYNAT) [10] is used to prevent network sniffing attacks by transforming the host identity information in the message header. Before routing, it transform port and address information of sender in the message header, transform algorithm is predefined with time parameters, DYNAT gateway parse the packet headers to obtain initial identity information and send to the receiver. This mechanism was designed to protect static nodes which deploy inner the gateway of centralized network, it is not transparent to users, and the synchronization failure of nodes may occur when DYNAT gateway has large payload or dynamic network configuration is fast.

2) Motive target IPv6 defense

Motive target IPv6 defense (MT6D) [11] is moving target defense method in network layer for IPv6. Both terminals of communication use their interface identifier of current address, a shared symmetric key, and the system time, to compute the interface identifier and notice used in next step, and then use it.

The continuous diverse transformation of IPv6 addresses

on both terminals can increase the costs and difficulties to attacker. At the same time, the storage of multiple addresses and information of both terminals of each connection, in router makes storage consumption higher.

3.1.2. Mechanism Based on Random Translation

Mechanism based on random transformation implements the dynamic transformation of network by assigning IP addresses generated randomly to the host.

1) IP address translation.

OpenFlow Random Host Mutation (OF-RHM) and Random Host Mutation (RHM) [12, 13] are the virtual address random transformation technology proposed by alshaer et al. OF-RHM is applied to SDN network, and provides the random virtual IP allocated by OpenFlow, and the translation of real IP and virtual IP is performed by the OF-RHM. The network structure of OF-RHM is shown as figure 2.

RHM, which applied in the traditional communication network, uses low frequency mutation (LFM) and high frequency mutation (HFM) to realize the distribution of virtual IP, the low frequency transform interval has multiple high frequency conversion intervals. In each low frequency transform interval, the system choose a range of random address satisfied conditions for each host, in each high frequency transformation interval, it randomly assign a virtual IP from the address range to the host. The disadvantage is that it is more complex to implement.

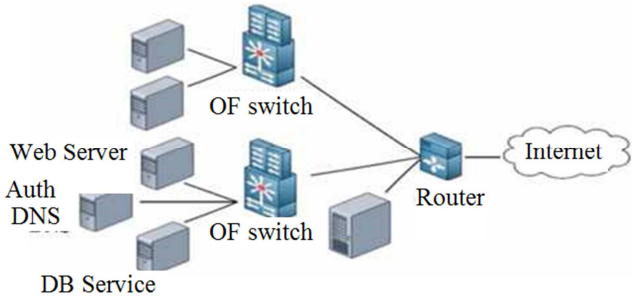

Figure 2. *OF-RHM network structure.*

2) Network address space randomization

Network address space randomization (NASR) [14] adjusts the transform frequency of LAN node IP address in the dynamic allocation of communication network address to prevent worm attacks. This mechanism needs to configure the dynamic host configuration protocol (DHCP), which terminates the DHCP lease (lease) at different intervals to randomize the real address. The disadvantage is that it is necessary to modify the operating system of the terminal host and the interrupt the activity connection between the terminals, so the cost is higher.

3.1.3. Mechanism Based on Hopping

The mechanism based on hopping is mainly realized by the hopping function.

Server connection information shifts dynamically and continuously, make the attacker has no method to know the current server connection information effectively, thus it can increase cost and complexity of a successful attack, control the range of loss of attack.

1) Communication port hopping

Lee et al. proposed a jump function with system time, server and user shared private key as parameters to perform UDP/TCP port hopping [15]. The technology is compatible with the existing protocols, it does not need to change current Internet infrastructure, is easy to implement, and simplifies the malicious message detection and filtering, but in low latency and congestion environment, strict time synchronization mechanism may lead to lower adaptability.

Badishi et al. proposed a mechanism based on channel-port matching [16]. Different channels have different ports, and the ports used by each channel are different at different times. Port is selected by pseudo-random PRF* hopping function in the range of port collection used recently.

This mechanism will transmit the newly selected port information with ACK message to realize the synchronization of information, it exists a potential weakness of port information leakage.

2) Network address hopping

Network address hopping uses a data stream that communicates a communication session through a data connection of multiple channels [17]. The mechanism changes the two communication modes of communication between the communication objects, shifts sequence information plain-text transmit by the initial response message (such as TCP SYN-ACK) from server to user, there is a potential weakness of the leakage of message transmission way by intercepted.

3) Network address and port hopping

Application that participates in their own defense [18] project provide general network centered defense project by port and address hopping at the same time in order to improve the flexibility of application, but it needs install specific client component to complete address and port transformation, deploy NAT gateway to realize the reverse mapping. The change of actual address and port can defend internal attacks.

Raytheon MORPHINATOR (Morphing Network Assets to Restrict Adversarial Reconnaissance) project [19] is focused on the port and address hopping technique to research a deformation computer network, it can deform with time to confuse offender and prevent network attack. MORPHINATOR used the motive network to dynamically change the attack network and configuration to make the host and application unpredictable, it can prevent or delay the network attack under a good management.

Port address hopping (PAH) communication applied in wireless communications provide hops for each session lasting only a few seconds/minutes. To solve the problem that hops can be easily influenced by network events such as traffic jams, transmission delays, packet dropouts, re-transmission, and reordering, Luoyuebin et al. improved the synchronization mechanism by generating message authentication code (MAC) based on the hash based MAC

(HMAC) as the synchronization information for port address encoding and decoding, communicating with one-packet-one-hopping to change identities constantly without authentication message transmission. [20, 21, 22]

4) Mechanism based on communication protocol

Even if the host system with a high degree of diversity, the attacker can still implement a successful attack by exploring the vulnerabilities of specific communication protocol, the transformation mechanism based on communication protocol has higher security level and better flexibility than any specific communication protocol in term of against to some specific vulnerabilities of network attack.

Protocol hopping cover channels, PHCC [23], covers channel by changing the channel established by protocol, it needs to select a set of spare protocols (select principle has nothing to do with whether the protocol is being used), and randomly shifts channels in the process of communication between two nodes, or different parts within a certain device, according to a predefined order.

3.1.4. Other Mechanisms

1) The mechanism based on self-shielding

Dynamic network architecture (SDNA) combines muti-techniques [24], such as the existing communication network technology, hyper-visor winding technology, authentication technology based on CAC, IPv6 technology etc., changes the network structure in order to improve the overall security degree, limit the attacker information collection and network transmission capacity. But the structure requests at least one message forwarding by an intermediate nodes before arrival and the source nodes to gradually establish a secure channel for transmission of data authentication, overhead will affect the user's network operation.

2) The mechanism based on lure

Clark proposed a moving target defense mechanism [25] based on lure, it randomly generates real nodes and alluring nodes IP address by introducing a large number of alluring nodes with legal addresses and simplified general communication protocol into communication network to reduce the identification probability to a real node. The disadvantage is that frequent address switching affects communication capabilities, and the deployment of a large number of virtual nodes can increase resource overhead.

3.2. Dynamic Communication Run-Time Environment

Dynamic communication run-time environment mechanism is a combination of dynamic communication platform and the execution environment, it implements the attack surface conversion, attack range and influence control by the transformation of communication application execution environment (including software and hardware, operating system, configuration files, etc.).

3.2.1. Dynamic Communication Platform

The transformation communication platform can resist the attack on the characteristics of communication platform, including shifting operating system, processor structure, virtual machine instance, storage system, communication channel and other low-level environment. Dynamic communication platform technology can transfer communication applications between platforms or perform the same communication application on the related platform.

1) Trusted dynamic logical heterogeneity

Trusted dynamic logical heterogeneity (TDLH) system improved survivability framework [26] by platform diversity. In random time interval, it allows running communication applications migrate to other heterogeneous platform with state (including execution status, open files, and network connections). In order to ensure the security of the target platform, trusted platform module (TPM) is used to carry out credible verification before migration.

2) Self-cleansing intrusion tolerance, SCIT

Self-cleansing intrusion tolerance (SCIT) [27] can use vitalization technology to create multiple virtual server with the same initial condition to provide same service in turn, it can select online virtual server randomly, and reset offline virtual server according to predetermined configuration. The disadvantage is that using the vulnerabilities of the virtual machine's initial configuration, the attacker can still successfully launch the corresponding attack. The moving attack surfaces (MAS) [28] configures an unique set of software for each virtual server that provides web services, and the diversification of the attack surface is successfully make up for the weakness of SCIT. However, multiple virtual machines are configured to provide the same service at the same time, control module should shift them in a very short time, and SCIT may lead to high resource redundancy and high management overhead.

3.2.2. Dynamic Execution Environment

Dynamic execution environment mechanism confuses attackers by unpredictable of communication platform configuration, target address, instruction set, it increases the attack consumption, and attack methods cannot be transplanted easily, so it can inhibit the range of attack.

1) Address space randomization

Address space randomization (ASR) can disable the attacks depend on the target address information [2] by randomly allocating address of the target in memory. The instruction-set randomization (ISR) technology [29] protects the system from code injection by using a key with a smaller random range to encrypt the system instruction set, it is possible to be successfully cracked.

2) Shift machine configurations

John et al. proposed a machine configurations shifting method to obtain a more secure configuration [30, 31]. This method firstly codes system configures into chromosomes by found component, executes genetic algorithm, produces offspring with a higher degree of security configuration, and sends the offspring population to achieve component, implementation component in a set of virtual machine to implement the offspring population, reserve grading rules and scan tool is used by assess components (such as Nessus) to evaluate on the safety of new groups. According to the

evaluation results, it selects chromosomes found components for a new round of evolution, and selects a suitable configuration of the chromosomes to deploy on the host.

3.3. Dynamic Communication Application

The dynamic communication application mechanism mainly uses a software as a change object, and implements various transformation techniques to increase the corresponding attack difficulties, and improve the anti-attack ability by unpredictable target.

3.3.1. Diversity Transformation Mechanism

Using different methods, the various transformation of communication application mainly produces multiple variants with equivalent functions and different behaviors characteristic, these variants run alternately and make system attack surface change in a rich range, and make attacks are difficult to transplant, Jackson et al. proposed a mechanism that can translate machine into various formats during the process of compiling code, it automatically generates unique variant with equivalent function for programs with general security requirements [32]. Large-scale software diversity increases the difficulties of the successful attack to an exponential level; it uses muti-variants execution environment (MVEE) programs with higher safety requirements, simultaneously operates multiple variants which is detected by monitoring agents, a variant will be switched off immediately when the attack is detected, thus the attack effect is effectively controlled. Christodorescu et al. proposed a universal P2P software diversification method [33], it transforms different programs by different strategy repeatedly. The disadvantage is that changing current process of development, deployment and operation makes the actual deployment consumption higher.

3.3.2. Mechanism Based on Minimization of Function

Rinard believes that the functionality of existing software systems often exceeds what is needed, and that unnecessary functionality always makes more security vulnerabilities. In order to meet the demand of requirement, the communication application should remove unnecessary function by current mature technologies, such as input rectification, functionality excision, functionality replacement, loop perforation, cyclic memory allocation, etc., to reduce the system attack surface. However, during the process of being attacked, mechanism based on minimization of function cannot effectively control the scope and effect of attack.

3.3.3. Other Transformation Mechanisms

Through time and space diversity engine, helix metamorphic shields, HMS [34] can reset random key pair with high-speed for dynamic instruction set randomization of communication applications in order to realize the attack surface change transformation, generate an event of a detected attack to indicate the vulnerabilities, trigger repair engine produce variants by evolutionary algorithms, deploy variant after diversified transformation. HMS has been used to repair the attack surface while moving the attack surface, this makes the communication application automatically evolve into a variant with less vulnerability, but it can cause a higher consumption of calculation, detection and repair.

3.4. Dynamic Data

The dynamic data mechanism executes semantic equivalence transformation of the communication application data to resist the illegal use or access.

3.4.1. Data Diversity

Data diversity [35] runs semantic equivalent data through each variant of the communication application, the different semantics caused by malicious input can be detected by the mutation monitor. Separating variable address and running space can help reduce the injection attack which depends on the specific memory address. The disadvantage is that an attacker can still locate the data part of the application, or use the advanced control injection attack that affects all variants at the same time.

3.4.2. Data Randomization

The existing data randomization (DR) [36] machine can mainly randomize different data objects through XOR operation. Cowan et al. proposed that XOR the pointer and the randomized key, then save result to memory [37], restore pointer after it is put into the register to against pointer failure attack; Cadar et al. proposed the method to classify equivalent instruction operands by static analysis, and XOR the random operands assigned for each equivalence class and corresponding data [38]. An attacker will lead to errors when makes a different visit with the analysis result, thus against the detection attack which depends on the memory error. Bhatkar et al. proposed a method that analyze all the data types contained in a program at the time of initialization, and then select the unique random number for each data object to implement the XOR encryption, and only do a decryption when the data is referenced, it can against relative address attack [39].

Table 2. *The role of the four mechanisms in the attack chain.*

MTD	Attack Chain				
	Explore	**Visit**	**Develop**	**Exploit**	**Persistent**
Dynamic Communication Network	+			+	
Dynamic Communication Run-time Environment		+	+		+
Dynamic Communication Application			+	+	
Dynamic Communication Data			+	+	

Using the attack chains published in MIT Lincoln laboratory to evaluate motive targets defense, this paper analyzed four motive targets defense technology, such as the dynamic communication network, the dynamic

communication operational environment, dynamic communication applications, dynamic data, and the role of each mechanism in attack chain is shown as table 2.

4. Design and Performance Analysis of Active Defense System

Based on jump mechanism, the design of the communication network active defense system framework (figure 3) is shown as figure 3, Using the pseudo random algorithm to make port hopping, information of address, protocol, service time slot etc., it can make denial of service.

attacks difficult to achieve, and trick attackers into honeypot host at a certain possibility, the adaption of encryption hopping algorithm makes message difficult to sort and decryption, When the message collection is complete, it will fail to obtain effect information, greatly increase the time consumption of a successful attack, improve the availability and confidentiality of system. It is shown as figure 3, control module is central to the system framework, warn module can collect information during the process of being attacking, manage module can generate communication information hopping figure of nodes, according to instructions provided by control module, management module can change current task from communication task, interaction task, honeypot task by changing communication host, interaction host and honeypot host.

Table 3. *Configuration of anti-Dos experimental.*

	Contro	Sync	Server	Clie	DoS	Inter
Bandwit	100	100	100	100	100	100
Operatio	Win-	Win-	Linux, Win-		Linux	Win-
Mechani	Agent	UDP	Terminal		SYN-	Snifin

Assuming that the attacker has known the terminal information hopping strategy to launch an attack, as the hopping figure at every time is unique, the time consumption of an successful attack can be inferred by formula 1.

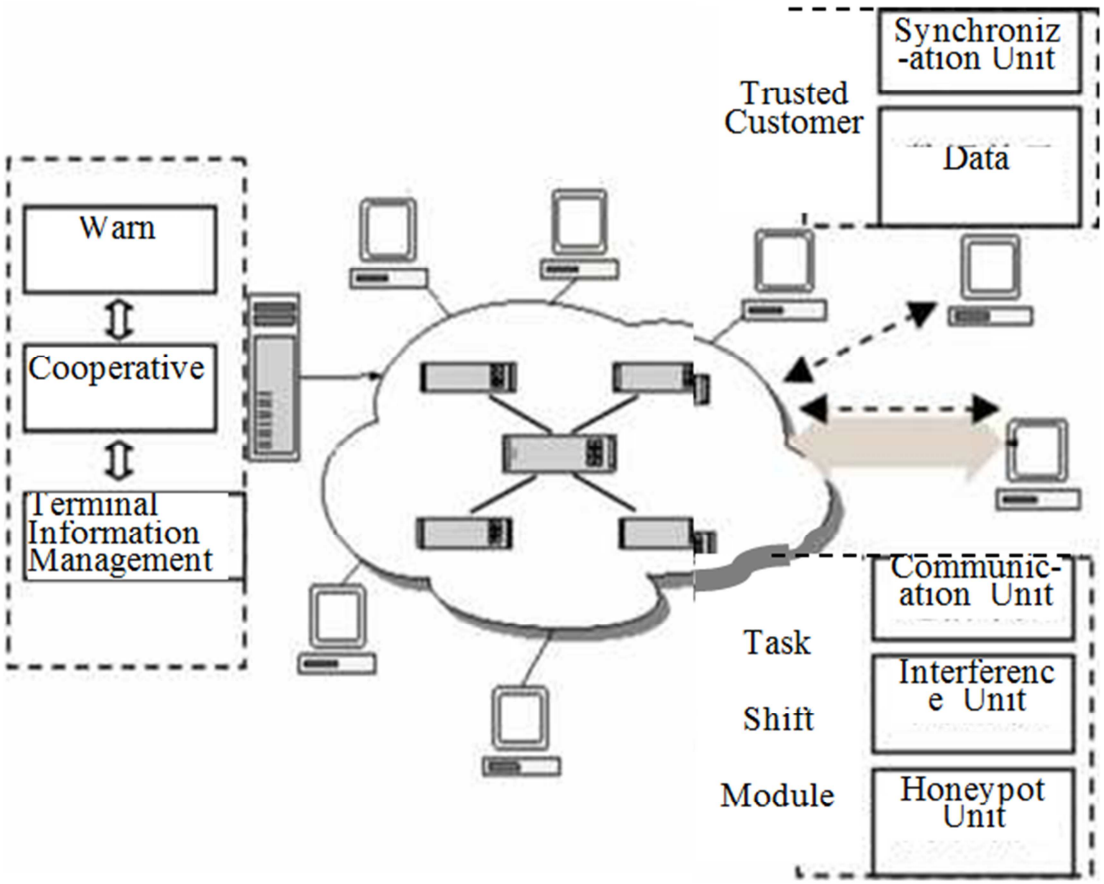

Figure 3. *The inactive defense mechanism based on hopping.*

$$T' = T(1 + \sum_{i=1}^{nmk-1} \left(i \frac{C_{nmk-1}^{i}}{C_{nmk}^{i} C_{nmk-i}^{1}} \right) \quad (1)$$

Among them, n is the number of hopping address, m is the number of ports, k is the protocol number, and the number of hopping figures can be calculated to nmk. It proved that terminal information hopping can greatly increase the time consumption of attackers.

Assuming the continuous time T is the threshold of system, T>>t, average strength of attack X is greater than X_r, thus, X can be calculated as formula 2:

$$X = \frac{r/s}{nmk} \quad (2)$$

Invalid probability of time slot P_i and valid probability of system steady-condition P_{Avail} is:

$$P_t = p(X > X_t) = p(\frac{\frac{r}{s}}{nmk} > X_T) \quad (3)$$

$$P_{Avail} = 1 - \sum_{i=T/t}^{\infty} P_T^i \left(1 - \frac{P_t^{T/t}}{1-P_t}\right) \quad (4)$$

Among them, r is the attack speed rate of Dos, s is the size of attack message, t is the average hopping time slot. It can be inferred easily that the more hopping figures (nmk) are, the less the average strength of attack in one unit, the less the average strength of attack in one unit or the faster the terminal information hopping, the better performance the system will have.

For intercept attack, the system spread the data messages in background data noise by the hopping of port, address, protocol, time slot, the successful probability of intercepting, regrouping, decoding complete message is:

$$P_s = (\frac{1}{P_{\lceil N_0/S \rceil + l}^1})^k = \frac{1}{((\lceil \frac{N_0}{S} \rceil + 1)l)^k} \quad (5)$$

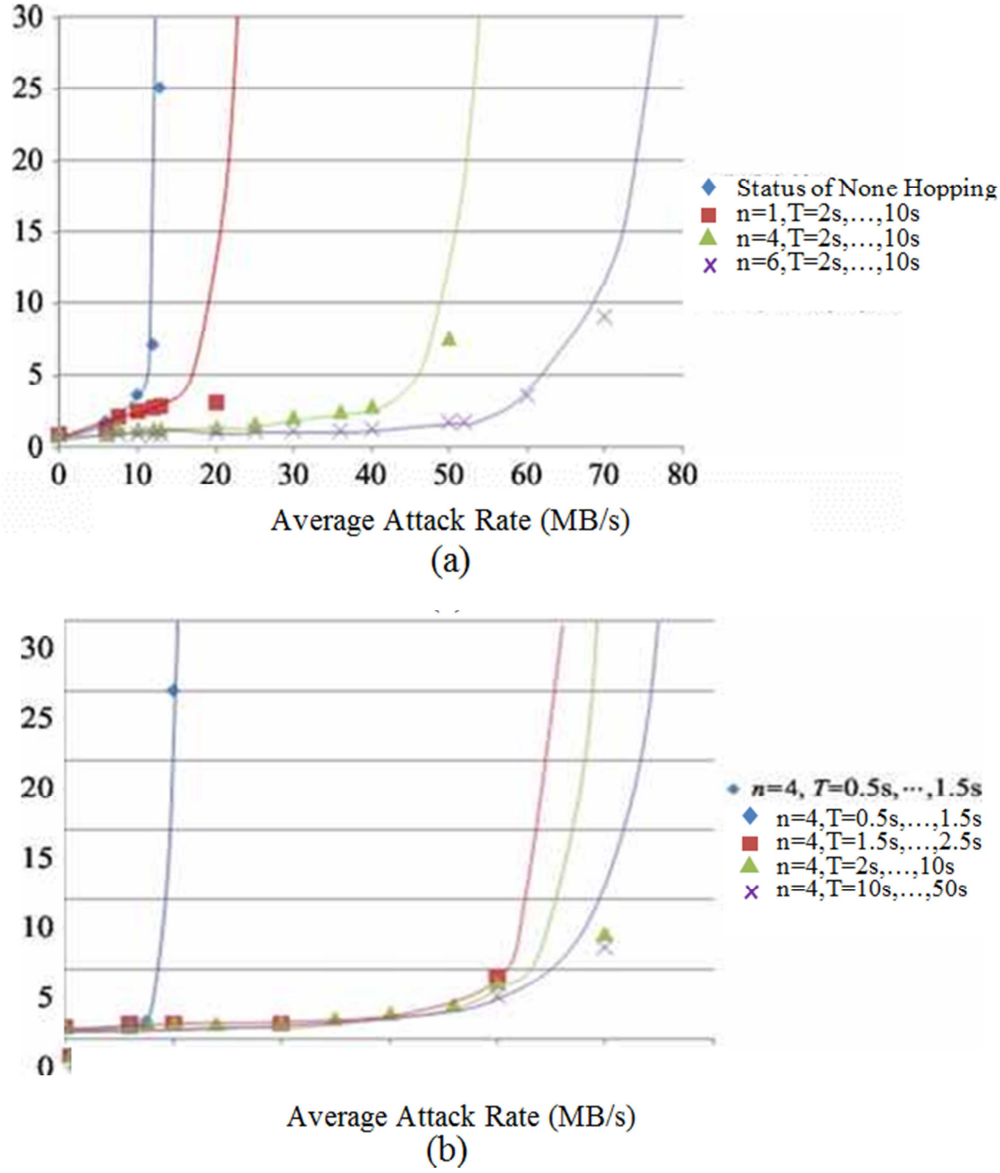

Figure 4. *The experimental data of anti-DoS attack performance.*

Among them, l is the number of available encryption algorithms, N_0 is the data volume with the ideal balance background noise, s is the number of valid message data, and k is the segment number of a complete data-gram.

Therefore, the terminal information hopping mechanism reduces the probability of the attacker's success, increases the time cost, and improves the confidentiality of the system.

The SYN-Flood attack and interception attack experiment were performed on the defense system, the experimental environment configuration is shown in table 3, and the experimental results are shown in figure 4.

It can be seen from figure 4(a), the performance of

terminal information hopping is far better than that of typical service and simple port hopping service, and the more hopping address, the better performance, figure 4(b) shown that, shift service frequently will lead to performance decreasing. Active defense system based on terminal information hopping can greatly improve the performance against Dos, but the hopping rate should be based on the network rules, congestion degree and other settings.

The intercept attack experiment selected the setting that is most favorable to the attacker. The interceptor is located in the shared Hub LAN with no interference from other hosts, 5 servers and 6 clients.

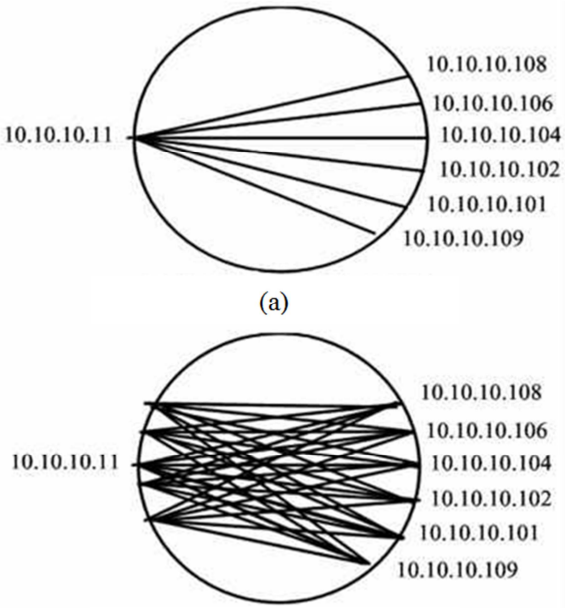

Figure 5. *The intercept attack data of anti-terminal information hopping.*

The experimental results are shown as figure 5. Compared with the non-hopping and port hopping, the terminal information hopping mechanism effectively decentralized network traffic, and the pseudo-random hopping encryption algorithm greatly increased the complexity of crypt analysis.

5. Conclusion

As a revolutionary communication defense technology, motive target defense is highly concerned by researchers. High quality targets defense system urgently needs a comprehensive theory as the guidance, from the attack surface features and the function intensive of motive target defense, this article classified and analyzed current motive targets defense technique, systematically studied the motive target defense mechanism and the new progress, designed a active defense system based on the terminal information hopping mechanism, analyzed from the attack resistance, and laid a theoretical foundation for the design and implement of muti-mechanisms of moving targets. In addition, the transformation mechanism, control mechanism, practical application, performance evaluation of moving targets defense, as well as how to combine motive target defense theory to improve the effect of traditional static defense will become the focus in the future communication defense.

Acknowledgements

This paper would like to thank National Natural Science Foundation of No.61472437 for economic support, and researchers in National University of Defense and Technology for technology guidance, Xuejun Yang, Jianping Yin, Yan Jia, Xinjun Mao for help and the authors of reference for new progress in binary vulnerability analysis.

References

[1] Gui-lin CAI, Bao-sheng WANG, et al. "Moving target defense: state of the art and characteristics," Frontiers of Information Technology & Electronic, vol. 17. 11, pp. 1122-1153, 2016.

[2] Manadhata, Pratyusa K., and J. M. Wing. "An Attack Surface Metric,"*IEEE* Transactions on Software Engineering, vol. 37 (3), pp. 371-386, 2011.

[3] Zhu Q, Ba§ar T. “Game-theoretic approach to feedback-driven multi-stage moving target defense,” Proceedings of the 4th International Conference on Decision and Game Theory for Security, Fort Worth, USA, pp. 246-263, 2013.

[4] Wei P, Feng L, Chin-Tser H, et al. “A moving-target defense strategy for Cloud-based services with heterogeneous and dynamic attack surfaces,” Proceedings of IEEE International Conference on Communications, Sydney. Australia, 2014, pp. 804-809.

[5] Zhuang R, Zhang S, Deloach S A, et al. “Simulation- based approaches to studying effectiveness of moving-target network defense,” National Symposiumon Moving Target Research, vol. 53. 39, pp. 15111-15126, 2013.

[6] July. “Cybersecurity Progress after President Obama’ s Ad-dress,” The White House National Security Council, 2012.

[7] NITRD CSIAIWG. “Cybersecurity Game-Change Research & Development Recommendations,” NITRD, 2010.

[8] Cai G L, Wang B S, Luo Y B, et al. “Research and Development of moving target defense technology,” Journal of Computer Research and Development, vol. 53. 5, pp. 968¬987, 2016.

[9] Manadhata P. “Game Theoretic Approaches to Attack Surface Shifting,” New York: Springer,, 2013, pp. 1-13.

[10] Kewley D, Fink R, Lowry J, et al. “Dynamic approaches to thwart adversary intelligence gathering,” Proceedings of the DARPA Information Survivability Conference & Exposition II, Anaheim, USA, pp. 176-185, 2001.

[11] Basam D, Ransbottom JS, Marchany RC, et al. “Strengthening MT6D defenses with LXC-based honeypot capabilities,” Electricaland Computer Enginering, vol. 2, pp. 12, 2016,

[12] Jafarian J H, Al-Shaer E, Duan Q. “Adversary-aware IP address randomization for proactive agility against sophis-ticated attackers,” Proceedings of 2015 IEEE Conference on Computer Communications (INFOCOM), Hong Kong, China, pp. 738-746, 2015.

[13] Jafar Haadi Jafarian, Al-Shaer E, Duan Q. “An effective address mutation approach for disrupting reconnaissance attacks,” IEEE Transactions of Information Forensics and Security, vol. 10(2), pp. 2562-2577, 2015.

[14] Antonatos S, Akritidis P, Markatos E P, et al. “Defending against hitlist worms using network address space randomization,” Proceedings of the 2005 ACM Workshop on Rapid Malcode, Fairfax, USA, pp. 30-40, 2005.

[15] Lee H C, Thing V LL.” Port hopping for resilient networks,” Proceedings of 2004 IEEE 60th Vehicular Technology Conference, Los Angeles, USA, pp. 3291 – 3295, 2004.

[16] Badishi G, Herzberg A, Keidar I. “Keeping denial of service attackers in the dark,” IEEE Transactions on Dependable & Secure Computing, vol. 4(3), pp. 191-204, 2007.

[17] Sifalakis M, Schmid S, Hutchison D. “Network address hopping: a mechanism to enhance data protection for packet communications,” Proceedings of IEEE International Conference on Communication, Beijing, China, pp. 1518-1523, 2005.

[18] Atighetchi M, Pal P, Webber F, et al. “Adaptive use of network-centric mechanisms in cyber-defense,” Proceedings of IEEE International Symposium on Object-Oriented Real-Time Distributed Computing, Hokkaido, Japan, pp. 183-192, 2003.

[19] Raytheon Company. “MORPHINATOR,” http://www.raytheon.com+: Raytheon company, 2012.

[20] Wendzel S. “Protocol hopping covert channels,” http:// www. wendzel. de/dr. org/files/Papers/protocolhopping _ MP_DE.pdf: Wendzel, 2008

[21] Guang-jia SONG, and Zhen-zhou JI. "Anonymous-address-resolution model," Frontiers of Information Technology& Electronic Engineering, Vol. 17(10), pp. 1044-1055, 2016.

[22] Mian CHENG, Jin-shu SU, and Jing XU. "Real-time pre-processing system with hardware accelerator for mobile core networks," Frontiers of Information Technology & Electronic Engineering, Vol. 18(11), pp. 1720-1731, 2017.

[23] Peng JIANG, Qiaoyan WEN, et al. “An anonymous and efficient remote biometrics user authentication scheme in a multi-server environment,” Frontiers of Computer Science, vol. 9(1), pp. 142-156, 2015.

[24] Yackoski J, Xie P, Bullen H, et al. “A self-sliielding dynamic network architecture,” Proceedings of the Military Communications Conference, New York, USA, 2011, pp. 1381-1386.

[25] Clark A, Sun K, Poovendran R. “Effectiveness of IP address randomization in decoy-based moving target defense,” Proceedings of the Decision and Control, Florence, Italy, pp. 678-685, 2013.

[26] Okhravi H, Comella A, Robinson E, et al. “Creating a cyber moving target for critical infrastructure applications using platform diversity,” International Journal of Critical Infrastructure Protection, vol. 5(1), pp. 30-39, 2012.

[27] Bangalore A K, Sood A K. “Securing web servers using self cleansing intrusion tolerance,” Proceedings of the International Conference on Dependability, Brunow, Poland, pp. 60-65, 2009.

[28] Huang Y, Ghosh A. “Introducing Diversity and Uncertainty to Create Moving Attack Surfaces for Web Services,” New York: Springer, vol. 54, pp. 131-151, 2011.

[29] Kc G S, Keromytis A D, Prevelakis V. “Countering code injection attacks with instruction-set randomization,” Proceedings of ACM Conference on Computer and Communications Security, Washington, USA, pp. 272-280, 2003.

[30] Lucas B, Fulp E W, John D J, et al. “An initial framework for evolving computer configurations as a moving target defense,” Proceedings of the Cyber and Information Security Research Conference, New York, USA, pp. 69-72, 2014.

[31] John D J, Smith R W, Turkett W H, et al. “Evolutionary based moving target cyber defense,” Proceedings of the Companion Publication of the 2014 Annual Conference on Genetic and Evolutionary Computation, Vancouver, Canada, pp. 1261-1268, 2014.

[32] Jackson T, Salamat B, Homescu A, et al. “Compiler-generated software diversity,” Advances in Information Security, vol. 54, pp. 77-98, 2011.

[33] Christodorescu M, Fredrikson M, Jha S, et al. “End-to-End Software Diversification of Internet Services,” New York:Springer, 2011, vol. 54, pp. 117-130.

[34] Goues C, Nguyen-Tuong A, Chen H, et al. “Moving Target Defenses in the Helix Self-Regenerative Architecture,” NewYork:Springer, 2013, vol. 100, pp. 117-149.

[35] Ma J, Dunagan J, Wang H J, et al. “Finding diversity in remote code injection exploits,” Proceedings of the 6th ACM SIGCOMM Conference on Internet measurement, Riode Janeriro, Brazil, pp. 53-64, 2006.

[36] Bhatkar S, Sekar R. “Data space randomization,” Proceedings of the 5th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment, Paris, France, pp. 1-22, 2008.

[37] Cowan C, Beattie S, Johansen J, et al. “PointGuard™: protecting pointers from buffer overflow vulnerabilities,” Proceedings of the 12th Conference on USENIX Security Symposium, Washington, USA, pp. 7-12, 2003.

[38] Rinard M C, Cadar C, Dumitran D, et al. “A dynamic technique for eliminating buffer overflow vulnerabilities,” Proceedings of the 20th Annual Computer Security Applications Conference, Tucson, USA, pp. 82-90, 2004.

[39] Bhatkar S, DuVarney D C, Sekar R. “Address obfuscation:an efficient approach to combat a broad range of memory error exploits,” Proceedings of the Conference on USENIX Security Symposium, Berkeley, USA, pp. 105-120, 2003.