International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 7, Issue 2, February 2022, http://ijmec.com/

DYNAMIC NETWORK SECURITY ISSUES FOR INTRUSION PREVENTION

[1]Phaniraj Kumar [2]Gopi Gandikota,[3]Dr.T.Muni Sankar
[1] Assistant Professor, Department of CSE, RISE Krishna Sai Prakasam Group of Institutions, Ongole,
[2] Assistant Professor, Department of CSE,RISE Krishna Sai Gandhi Group of Institutions, Ongole,
3 Associate Professor, Department of CSE,RISE Krishna Sai Gandhi Group of Institutions, Ongole.

Abstract— Driven by the rapid development of the Internet of Things, cloud computing and other emerging technologies, the connotation of cyberspace is constantly expanding and becoming the fifth dimension of human activities. However, security problems in cyberspace are becoming serious, and traditional defense measures (e.g., firewall, intrusion detection systems, and security audits) often fall into a passive situation of being prone to attacks and difficult to take effect when responding to new types of network attacks with a higher and higher degree of coordination and intelligence. By constructing and implementing the diverse strategy of dynamic transformation, the configuration characteristics of systems are constantly changing, and the probability of vulnerability exposure is increasing. Therefore, the difficulty and cost of attack are increasing, which provides new ideas for reversing the asymmetric situation of defense and attack in cyberspace. Nonetheless, few related works systematically introduce dynamic defense mechanisms for cyber security. The related concepts and development strategies of dynamic defense are rarely analyzed and summarized. To bridge this gap, we conduct a comprehensive and concrete survey of recent research efforts on dynamic defense in cyber security. Specifically, we firstly introduce basic concepts and define dynamic defense in cyber security. Next, we review the architectures, enabling techniques and methods for moving target defense and mimic defense. This is followed by taxonomically summarizing the implementation and evaluation of dynamic defense. Finally, we discuss some open challenges and opportunities for dynamic defense in cyber security.

Keywords— **Cyber security, Dynamic defense, Moving target defense, Mimic defense**

I. *INTRODUCTION*

With the continuous development of the Internet of Things (IoT), cloud computing and other emerging technologies, various Cyber-Physical Systems (CPS) have been established in all walks of life, in which information resources are fully shared and utilized concurrently. On the one hand, these resources have become the key strategic infrastructures of all countries and organizations, which support the effective operation of national power, transportation, finance, energy and other important and influential fields. On the other hand, these resources profoundly affect and change people's way of production and life, giving birth to a new normal of social operations [1,2]. Nonetheless, benefiting from the enriching information resources and services, security threats of global cyberspace are also taking on new dimensions. Various cyber security incidents frequently occur while diverse novel cyber-threats are spreading globally. Major security incidents (e.g., Wanna Cry ransomware virus, eBay data breach) have repeatedly shown that cyber security faces serious challenges over the years [3].

In view of defense for cyber security, researchers have conducted extensive findings. The traditional cyber defense technologies (e.g., authentication, access control, information encryption, intrusion detection system, vulnerability scanning and virus protection) have provided a certain degree of security [4,5], whereas with the development of diversification attacks, the traditional cyber defense is inadequate. The existing defense mechanisms are inadequate to prevent various types of attacks, and the dominating reasons include:

1. **The universality of vulnerability.** Limited by the technological capabilities and engineering skills, it is impossible to fully avoid, detect andeliminate vulnerabilities in static hardware/software components, systems, tools, environments and protocols.

2. **The easy installation of backdoors.** Under the globalization of the information industry, it is easy to implant backdoors through the product design chain, the tool chain, manufacturing chain, processing chain, supply chain, service chain, and other links.

3. **The oneness of genes in cyberspace architecture.** Cyberspace technologies and system architectures have homogeneity (e.g., use the same processor, operating system, office software and database). Due to their static, deterministic and similar situational mechanisms (e.g., system configuration, operation agreement, topology and transport routes), the ecological environment is very fragile. It not only causes vulnerability and makes the backdoor be attacked easily, but also enables the attack chain to be sustained and effective for a long time.

4. **The asymmetry between offense and defense.** From the perspective of attackers, all it takes is a single exploitable vulnerability in the entire security chain to disrupt or take control of the entire system. Meanwhile, it has a target space that is almost free from any constraint. Moreover, they have the initiative to launch sudden attacks at any time. From the perspective of defenders, they have to defend against known and unknown threats in all aspects of the communication network and information system.

Therefore, cyber-attacks based on unknown system vulnerabilities and backdoors are still the greatest threat in communication networks. The inevitability of vulnerabilities and the limitations of perceived defense methods force administrators to change defense strategies and innovate defense mechanisms, so as to reverse the passive situation of being prone to attacks and difficult to take effect in cyber security. Dynamic defense in cyber security based on mobile target defense and mimicry defense rises in response to the proper time and conditions.

2.Moving target defense

Moving Target Defense (MTD) is a game-changer for cyber security proposed by the United States of America (U.S.A.) in view of the current inferior position of the defender [6,7]. It is expected to confuse the attackers by continuous and dynamic changes, so as to increase the cost, complexity and failure rate of the attack [8,9]. It is important to note that MTD is not a specific defense method but a design guideline. MTD does not attempt to establish a system without loopholes, but to employ the resources, time and space environment of the target system to present the attacker with a constantly changing attack surface, which increases the difficulty of the attacker's cognition of the target system and reduces the duration of system vulnerability exposure [[10], [11], [12], [13]]. Therefore, attackers barely develop effective attack methods against the target system in a limited time to improve the resilience and active defense capability of the target system.

Mimic Defense (MD), as a neoteric active defense technology in cyberspace, aims to improve the anti- attack capability of information devices through endogenous mechanisms of its construction. The core idea of MD is to organize multiple redundant heterogeneous functionalities to jointly handle the same external request [[14], [15],

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 7, Issue 2, February 2022, http://ijmec.com/

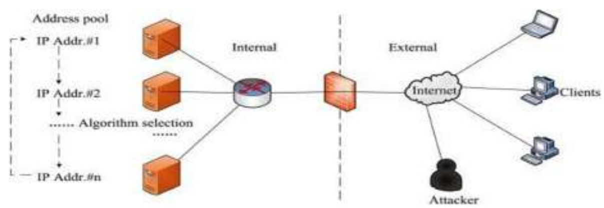
[16]]. Meanwhile, MD implements dynamic scheduling based on negative feedback among multiple redundancies to compensate for the security flaw in the current cyberspace.

In recent years, dynamic defenses of cyber security based on MTD and MD have been frequently investigated in academia and industry. Dynamic defense technologies applied to information systems have been put forward and achieved certain defense abilities. However, research on dynamic defense technologies is still in its infancy at present, and the theoretical study and engineering applications are facing several problems and challenges, such as the theoretical model of dynamic defense mechanism, the mechanism strategy of dynamic defense, the theoretical method of measuring the effectiveness of dynamic defense, and the index system of the influence of dynamic defense on system performance, etc. Therefore, in-depth theoretical study and system improvement of dynamic defense have important theoretical guidance and practical significance for promoting active defense capability.

Although numerous researches and practices on the dynamic defense in cyber security have emerged, there are only a handful of publications that systematically introduce this kind of work. The related concepts and development strategies of dynamic defense are rarely analyzed and summarized. To bridge this gap, a comprehensive and concrete survey of the recent research efforts on dynamic defense in cyber security are conducted in this paper.

The paper is organized as follows. Section 2 introduces an overview of the basic concepts and definitions of dynamic defense in cyber security. Furthermore, Section 3 surveys the architectures, enabling techniques, and methods for MTD in cyber security. Section 4 presents the architectures, enabling techniques, and methods for MD in cyber security. After that, Section 5 reviews the implementation and evaluation of dynamic defense in cyber security. Finally, Section 6 discusses future directions and open challenges of dynamic defense in cyber security.

Moving target defense provides a new way of thinking to solve the problem. At present, a large number of studies have been proposed which involve many aspects of MTD. In this section, we systematically introduce, classify and summarize the existing achievements in MTD. An example of an MTD model is given in Fig. 1.



Attack surface and attack surface conversion

As a matter of fact, there is currently no standard definition of attack surface [22], and the existing definition is usually relevant to the scenario. Manadhata et al. [23] regarded the system attack surface as a subset of resources utilized by attackers to carry out attacks in the system. Zhuang et al. [24] believed that the attack surface in the system consists of the resources revealed to the attacker (e.g., software on the host, communication ports among hosts and vulnerability points of each component) and network resources that have been compromised and be utilized to enter the system. Zhu et al. [20] regarded the attack surface as the set of vulnerabilities explicit to the system that an attacker might use for the attack. Peng et al. [25] consider the attack surface of an instance virtual machine instance in a cloud service as the total resources available.

Although the concept of attack surface has been widely used in the research of mobile target defense, the existing definition of attack surface still lacks comprehensiveness, accuracy and popularity. Therefore, to better illustrate the defense process against moving targets, it is necessary to

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 7, Issue 2, February 2022, http://ijmec.com/

further describe the characteristics of the attack surface.

Huang et al. [26] graphically described the transformation process of the attack surface but did not provide a formal definition. After that, Manadhata [19] firstly proposed the concept of attack surface shifting and defined it as follows:

- **Definition 1.** Attack surface parameters. The attack surface parameter represents the system configuration vulnerability or property of the attacker that initiates the attack, including software and hardware configuration property vulnerability of the system, such as buffer overflow vulnerability. In addition, it also includes the network properties exploited by the attacker, such as IP address, service port, and so on.
- **Definition 2.** The attack surface. At any time, the attack surface of the system is determined by the attack surface parameter set and the specific value of each parameter in the set. The system attack surface at time t is denoted $As = \{Mt, Et\}$, where $Mt = \{m1t, m2t, \ldots, mlt\}$ represents the attack surface parameter set at time t, and $m_{it}(1 < i < L)$ refers to a specific attack surface parameter at time t, whose range is u_i. In addition, $E_t = \{e1t, e2t, \ldots, elt\}$, where $elt \in ui$ represents the specific value of the parameter $m_{it}(1 < i < L)$ at time t.
- **Definition 3.** For a specific system G, the previous attack surface of G is denoted as R_o, and the new attack surface is denoted as R_n. If there is a resource r that satisfies one of the following two conditions, then the attack surface of G has been transformed from R_o to R_n:

1.r is a member of Ro but not of Rn;

2.r is a member of both Ro and Rn, but the role of r in Ro is greater than that in Rn.

This definition considers that the transformation of the attack surface can be realized either by changing system resources or by changing the role of a system resource, and it is not easy to quantify the role of resources in the attack surface.

The basic definitions of MTD are summarized in Table 1.

Table 1. Summary of the basic definitions of MTD.

Category	**Reference**	**Contribution**
		3.Net work attack model
The definition of the	[23]	Resources (e.g., meth Network attack against CP ods, channels, data, etc.) t the communication hat are utilized by behavior without permission the to launch power CPS functions and att an attack on a subset resources by utilizing vulne of system resources defect s in power informatio network [87]. Network attac
	[24]	Resources (such inatsegrity, availability and sec software, ports, etc.) t Tahte most striking feature of are exposed to aattnack methods and means va attacker, as well Tahse direct and indirect depe network resources tihnaftormation

		side and the phy have been compromi seudbtle changes in the attac and can be used to acctersisgger different CPPS respon the system
	[20]	The complex and changea An explicit set of attack steps require the ada vulnerabilities of attaack modeling methods system that can be usaedd aptability of network atta by an attacker needs to be higher.

Category	Reference	Contribution
	[25]	A virtual server pool with diversity is taken as an example to illustrate the means of the attack surface movement graphically
The definition of attack surface transformation	[26]	The concept of the attack surface transformation is defined graphically and formally, in which the contribution of resources to the attack surface is very important
	[19]	The transformation of the attack surface is defined graphically and formally, and the main contribution of this paper is the importance of resources to attack the surface

3 .Network attack model

The study improves the network attack modeling method to adapt to the characteristics of CPPS in the field of information and communication, and uses the related functional interface of the CPPS component model to reduce the complexity of process modeling [88].

The information physics hybrid modeling method focuses on the real-time interaction and coupling characteristics of the information side and physical side in CPPS, which considers the corresponding relationship between the attack process and the physical side response. The hybrid modeling method grasps the overall state change of CPPS in the whole process of attack, which reflects the interactive process of attack and defense at a multi- space-time scale and lays a foundation for attack detection and protection [89,90].

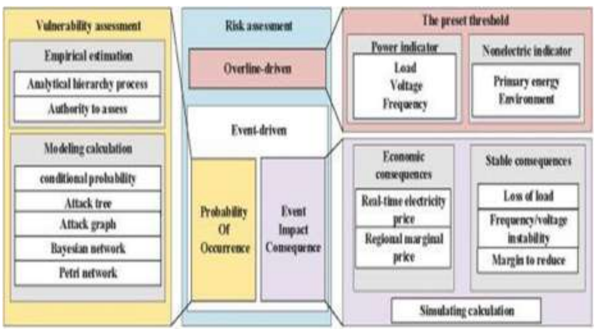
The modeling method of human intention incorporates subjective volition into the attack model. In the game, the players of attack and defense follow the principle of the highest to conduct attack and defense [91]. In the original human factor modeling, the influence model of the environment, psychology, workload and other factors is used to model the human decision-making process in the CPPS attack and defense.

Security assessment of CPPS network attacks

Considering the threat of network attack, CPPS security expands the connotation of information security and control security based on the traditional connotation of power grid security and stability. The physical side of CPPS is integrated into this information security assessment system, which mainly includes CPPS vulnerability assessment and risk assessment [92]. Vulnerability refers to the vulnerability of a powerful information system or secondary system that can be exploited or triggered by a threatening source [93]. The vulnerability assessment refers to assessing the possibility of exploitation of the vulnerability points mentioned above. CPPS security risk refers to the potential impact on CPPS

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 7, Issue 2, February 2022, http://ijmec.com/

functions caused by network attack threats. The risk assessment refers to the assessment of the expected impact degree of CPPS under threat [94]. The risk analysis is based on vulnerability analysis, which integrates vulnerability assessment and physical consequence assessment. The relationship between vulnerability assessment and risk assessment in the security assessment of CPPS is shown in Fig. 6.



4. Open challenges

According to the comprehensive discussions above on existing efforts, the key open challenges and future research directions are articulated for dynamic defense for cyber security.

1) 4.1. Vulnerability problem

Dynamic defense for cyber security resists attackers by diverting the attack surface. However, system vulnerabilities still exist. Defenses randomize the moving targets such as software, but if the software of vulnerability has not been fundamentally solved, the attacker can still dig through the leaks and buffer overflow vulnerabilities to specific targets. Only with the software after randomization, different users of the binary code are different, and therefore it cannot be used for other goals in the same way to carry out attacks [117]. Another example is instruction set randomization. Although it prevents attackers from inserting binary instructions into the target program to execute the attack successfully, the vulnerability of the target program has not been eliminated, and the well- designed worms and viruses can still break through the defense line of instruction set randomization [40].

1) 4.2. Integration with existing techniques

Existing dynamic defenses for cyber security, such as firewall, intrusion detection system, and anti- virus systems, are deployed in the network. The network topology and configuration are relatively fixed, while the defense of the moving target will change the existing network configuration. Therefore, the network availability may be reduced, and the existing network security defense technology may be interfered with. Mobile target defense technology must be implemented on the basis of not affecting the existing network operation and must adapt to the existing network infrastructure, network services and network protocols. With the deepening of the research, the dynamic defenses for cybersecurity techniques will be better integrated with the existing network security protection technology and be better embedded in the existing network [21,118].

2) 4.3. Systematic development

At present, abundant researchers propose various attack surface transfer schemes based on the moving targets defense idea. However, the schemes have not formed a system, and the overlapping use of different moving targets defense techniques may lead to conflicts. As a result, the analysis of the influence on the moving target defense technology system or network attributes and the judgment of the stack using different moving target defense techniques to form a dynamic defense for cyber security system is an important work in the future [119].

3) 4.4. Integration with emerging techniques

Dynamic defense for cyber security tends to change network configuration, which results in the loss of availability. The IP address change interferes with the attacker's scanning and intrusion, but may cause the failure of the entire network communication. In addition, the new software to define network SDN fundamentally changes the network structure, which makes the central controller have the ability of global regulation in the network. Therefore, based on the SDN technique, the change of IP makes the dynamic defense for cyber security technique minimize the impact of the entire network [25].

Conclusion

With the rapid development of various computing paradigms, information resources are widely shared and fully utilized. Consequently, cyber security problems are aggravated. To cope with this challenge, moving target defense and mimic defense are investigated to improve the defense effect. Furthermore, improving dynamic defense system construction has important theoretical guidance and practical significance for improving network active defense capability.

In this paper, a comprehensive survey of recent research on dynamic defense in cyber security is conducted. Technically, the background and motivation for the dynamic defense in cyber security are first reviewed. Then, an overview of the frameworks, architectures and emerging key techniques for cyber security is provided. Afterwards, the implementation and evaluation of dynamic defense are discussed. Finally, the open challenges and future research directions on dynamic defense in cyber security are investigated. We hope that the survey is able to elicit further discussions and research on dynamic defense in cyber security.

Acknowledgements

This research is supported by the Financial and Science Technology Plan Project of Xinjiang Production and Construction Corps, under grants No.2020DB005 and No.2017DB005. In addition, this work is also supported by the Priority Academic Program Development of Jiangsu Higher Education Institutions fund.

References

1. [1]J. Clements, Y. Yang, A. Sharma, H. Hu, Y. L ao Rallying Adversarial Techniques against Deep Learning for Network Security, arXiv Preprint arXiv (1903), p. 11688 Google Scholar
2. [2]A. Aydeger, N. Saputro, K. Akkaya A moving target defense and network forensics framework for sp networks using sdn and nfv Future Generat. Comput. Syst., 94 (2019), pp. 496-509 View PDFView articleView in ScopusGoogle Scholar
3. [3]Y. Liu, W. Peng, J. Su A study of ip prefix hijacking in cloud computing networks Secur. Commun. Network., 7 (11) (2014), pp. 2201-2210 View article CrossRefGoogle Scholar[4]D.C. MacFarland, C.A. Shue The sdn shuffle: creating a moving-target defense using host-based software-defined networking Proceedings of the Second ACM Workshop on Moving Target Defense, ACM (2015), pp. 37-41 View article CrossRefView in ScopusGoogle Scholar
4. [5]Y.-B. Luo, B.-S. Wang, X.-F. Wang, X.- F. Hu, G.-L. Cai, H. Sun Rpah: random port and address hopping for thwarting internal and external adversaries 2015IEEE Trustcom/BigDataSE/ISPA, vol. 1, IEEE (2015), pp. 263-270 View article CrossRefGoogle Scholar
5. [6]B. Van Leeuwen, W.M. Stout, V. Urias Operational cost of deploying moving target defenses defensive work factors MILCOM 2015-2015 IEEE MilitaryCommunications Conference, IEEE (2015),pp. 966-971View article CrossRefView in ScopusGoogle Scholar

International Journal of Multidisciplinary Engineering in Current Research
ISSN: 2456-4265, Volume 7, Issue 2, February 2022, http://ijmec.com/

6. [7]M. Zhang, L. Wang, S. Jajodia, A. Singhal, M. Albanese Network diversity: a security metric for evaluating the resilience of networks against zero-day attacks IEEE Trans. Inf. Forensics Secur., 11 (5) (2016),pp. 1071-1086View in ScopusGoogle Scholar

7. [8]J.B. Hong, D.S. Kim Assessing the effectiveness of moving target defenses using security models IEEE Trans. Dependable Secure Comput., 13 (2) (2015), pp. 163-177View article

-
CrossRefView in ScopusGoogle Scholar

8. [9]T.C. Eskridge, M.M. Carvalho, E. Stoner, T. T oggweiler, A. Granados Vine: a cyber emulation environment for mtd experimentation Proceedings of the Second ACM Workshop on Moving Target Defense, ACM (2015), pp. 43-47 View article
CrossRefView in ScopusGoogle Scholar

9. [10]C. Corbett, J. Uher, J. Cook, A. Dalton Countering intelligent jamming with full protocol stack agility
IEEE Secur. Priv., 12 (2) (2013), pp. 44-50

-