Scientific Research Publishing

Journal of Computer and Communications, 2021, 9, 1-7
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Research on Cyberspace Mimic Defense Based on Dynamic Heterogeneous Redundancy Mechanism

Junjie Xu

Jiangsu University of Technology, Changzhou, China
Email: sherlockjjobs@163.com

How to cite this paper: Xu, J.J. (2021) Research on Cyberspace Mimic Defense Based on Dynamic Heterogeneous Redundancy Mechanism. *Journal of Computer and Communications*, **9**, 1-7.
https://doi.org/10.4236/jcc.2021.97001

Received: June 4, 2021
Accepted: July 2, 2021
Published: July 5, 2021

Abstract

With the rapid growth of network technology, the methods and types of cyber-attacks are increasing rapidly. Traditional static passive defense technologies focus on external security and known threats to the target system and cannot resist advanced persistent threats. To solve the situation that cyberspace security is easy to attack and difficult to defend, Chinese experts on cyberspace security proposed an innovative theory called mimic defense, it is an active defense technology that employs "Dynamic, Heterogeneous, Redundant" architecture to defense attacks. This article first briefly describes the classic network defense technology and Moving Target Defense (MTD). Next, it mainly explains in detail the principles of the mimic defense based on the DHR architecture and analyzes the attack surface of DHR architecture. This article also includes applications of mimic defense technology, such as mimic routers, and mimic web defense systems. Finally, it briefly summarizes the existing research on mimic defense, expounds the problems that need to be solved in mimic defense, and looks forward to the future development of mimic defense.

Keywords

Cyberspace Mimic Defense, Dynamic Heterogeneous Redundancy Structure, Defense Technology, Network Security

1. Introduction

From a technical point of view, classic defense methods can be divided into three categories. The first category focuses on protecting data and information such as firewalls and building barriers between internal and external networks. The second category focuses on real-time network defense based on known features

of an attack, such as intrusion detection technology [1]. The third category is network spoofing, such as honeypots [2]. The above three defense methods are static defense, mainly based on prior knowledge of precise protection technology ideas. Although static defense can have a good defensive effect in defending against known features and fixed pattern attacks, it is difficult to defend against attacks based on unknown vulnerabilities and backdoors, as well as complex and changeable advanced attack techniques.

The drawback of static defense is mainly due to three aspects: first, every network system has inevitably vulnerabilities; second, the existing network systems are static, predictable, and monoculture; third, the existing defense technology is difficult to be effective against attacks based on unknown vulnerabilities. In response to the shortcomings of static defense, the American academic community has proposed a representative proactive defense mechanism, Moving Target Defense (MTD) [3]. MTD is a defense method that uses dynamic, randomized, and diversified attributes to increase the cost of attacks and the flexibility of the system. It attempts to continuously and randomly changes network elements and attack surfaces to reduce the static, isomorphic and determinate characteristics of the target system, thereby increasing the unpredictability of the system. Both Address Space Layout Randomization (ASLR) and Instruction Set Randomization (ISR) [4] are very successful MTD technologies. Although MTD can solve the passive situation of static defense to a certain extent, it is difficult to generate an effective strategy to achieve coverage, timeliness, and unpredictability at the same time [5].

To solve these problems fundamentally, inspired by the protective effect of mimic phenomena in the natural world, Wu and others proposed the idea of mimic defense [6] that employs dynamic, heterogeneity, and redundancy (DHR) structure. This article aims to explain the basic principles of mimic defense, including DHR architecture and attack surfaces, and introduce related applications, such as mimic web defense system and mimic router. As shown in **Figure 1**, the next section is to explain the principles of mimic defense.

2. Basic Principles of Mimic Defense

2.1. DHR (Dynamic Heterogeneous Redundancy) Architecture

Dynamic heterogeneous redundant structure is the basic principle of mimic defense, it is shown in **Figure 2**. In general, DHR architecture is a structure based on multi-mode decision-based policy distribution and multi-dimensional dynamic reconstruction of negative feedback control, it is mainly composed of functionally equivalent heterogeneous executors, input and output agents, policy-based arbitration, negative feedback control, and schedulers using an iterative mechanism. Standardized software and hardware modules can combine M sets of isomers, and dynamically select n components from set E as an executor set according to a specific strategy scheduling algorithm, and the system input agent forwards the input to each executor in the current service set. The output vectors

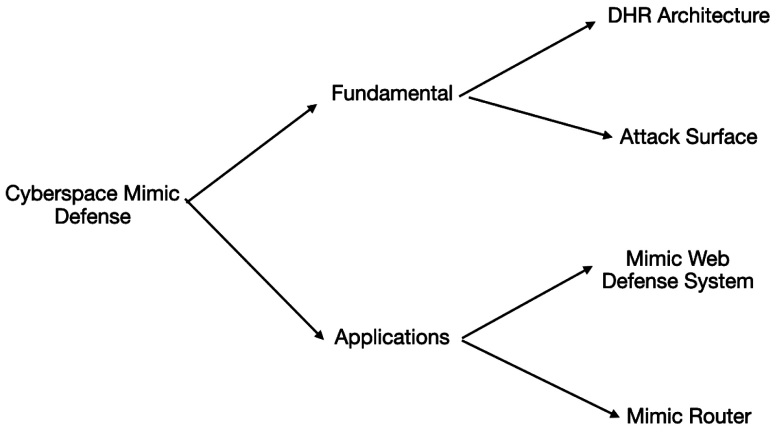

Figure 1. Main outline.

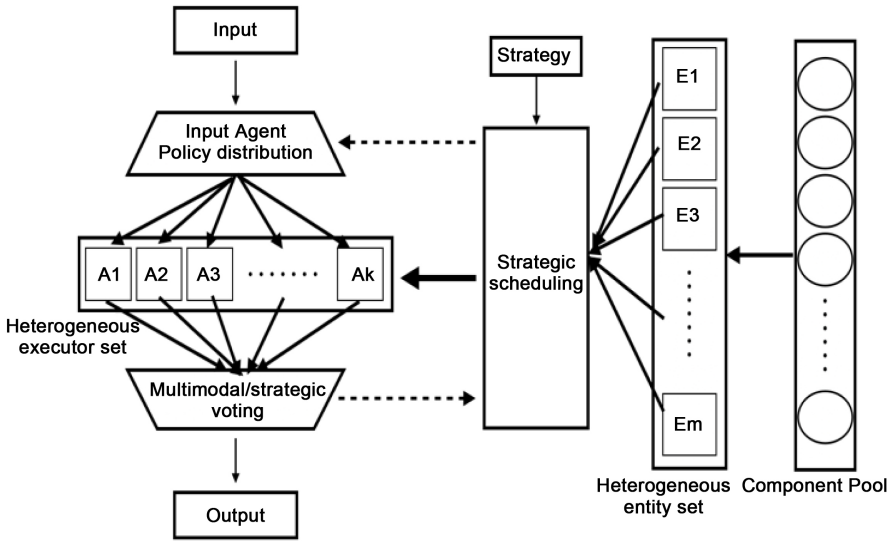

Figure 2. DHR Architecture [7].

of these executors are submitted to the voter for voting, and the system output is obtained.

In the entire process, strategic scheduling plays a central control role. On the one hand, policy-based scheduling issues instructions to policy distribution to activate the executor, complete the clean and repair of the executors, or perform other given tasks. On the other hand, strategic scheduling is also the feedback controller in the DHR architecture. When the feedback controller receives the abnormal state of the voters, it executes the corresponding action according to the present strategy.

Policy distribution corresponds to the input agent, and its main function is to allocate external input to the specified heterogeneous executors in the current service set according to the instructions of the strategic scheduling. The strategic voting segment corresponds to the output agent segment. The main function is to adopt a multi-mode output ruling strategy for the output vectors of multiple executors and report the abnormal state that occurs to the strategy scheduling

segment. The heterogeneous entity set is a collection of all the heterogeneous executors that can meet the needs. Strategic scheduling extracts elements from the heterogeneous resource pool to generate functionally equivalent new executors according to a pre-made reconstruction and reorganization plan or replaces some components in the existing executors to generate or update heterogeneous executive sets.

2.2. The Attack Surface of the DHR Architecture

The attack surface [8] of a system is the subset of system resources that an attacker can use to launch an attack. The DHR architecture essentially constructs multiple attack surfaces. Due to the diversity of the current service set and execution environment, the system resources available to the attacker are uncertain and unpredictable. Macroscopically, it appears as an irregularly moving attack surface. As shown in **Figure 3**, the attack surface at different time point t1 and t2, as the change of the set of heterogeneous executors, the attack surface presented to the outside by the target system is also different.

Especially for complex attack tasks that require multiple steps to upload data packets or send back data packets to achieve their attacks, the feasibility premise is almost impossible to guarantee. Not only that, due to the existence of a negative feedback mechanism based on multi-mode rulings, even if individual executors are destroyed, they will be eliminated or reconstructed. Therefore, if the attacker cannot control most or all the executors in the same space-time dimension, no attack can compromise the target system.

2.3. Cyberspace Mimic Defense

Cyberspace mimic defense is based on relatively true axiom, with structure determining security as the core idea. Through dynamic heterogeneous redundant architecture, systems using mimic defense technology can respond to unknown security threats, with endogenous high security and high reliability. Mimic defense ensures the dynamics and variability of the mimic defense system through dynamic scheduling mechanism and negative feedback control mechanism and ensures the robustness of the system and active cognition of aggressive behavior

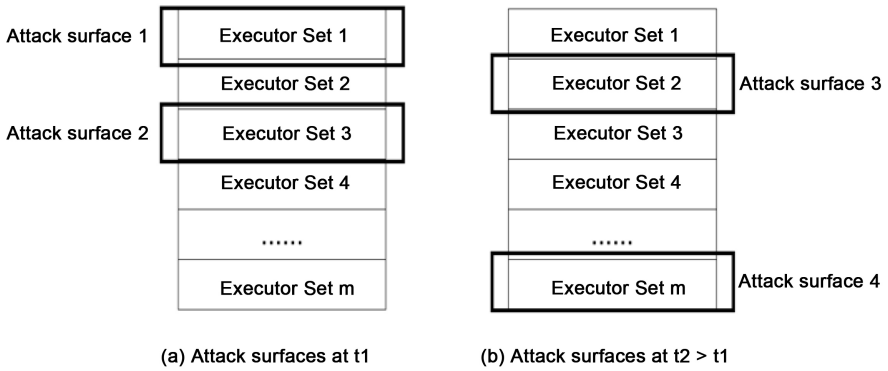

Figure 3. Attack surfaces at different times [7].

through the multi-modal adjudication mechanism.

The main idea of mimic defense is to separate the coupling relationship between meta-functions and specific implementation structures, build a multi-executor's environment with multiple functions equivalent and heterogeneous redundancy, and establish the actual mapping relationship between meta-functions and executors through a dynamic scheduling mechanism. Under the condition of ensuring that the system functions remain unchanged, making full use of dynamics, diversity, and randomness to hide various vulnerabilities within the executors, makes it hard for attackers to establish a continuous and reliable attack chain. Further introduce a multi-mode arbitration mechanism and perform multi-mode arbitration output on the output results of multi-executors to ensure the correctness of the output results.

3. Applications of Mimic Defense Based on DHR Architecture

3.1. Mimic Web Defense System

The mimic web defense system adopts a hierarchical structure design [9], as shown in Figure 4. With the support of software or hardware, the mimic Web defense system is heterogeneous in multiple levels, such as physical and virtual machine OS, server software, and SQL scripts. In the actual process, the request is replicated and distributed to multiple carriers at different levels. After layer-by-layer processing, the processing is sent to the arbiter for a unique output vote.

3.2. Mimic Router

Routing is the brain of network information interaction that determines the end-to-end path of network data from source to destination. Its related technologies have always been at the core. The development process and direction are the epitome of the development of the Internet, and they are also the key and commanding heights of offensive and defensive confrontation in cyberspace. As

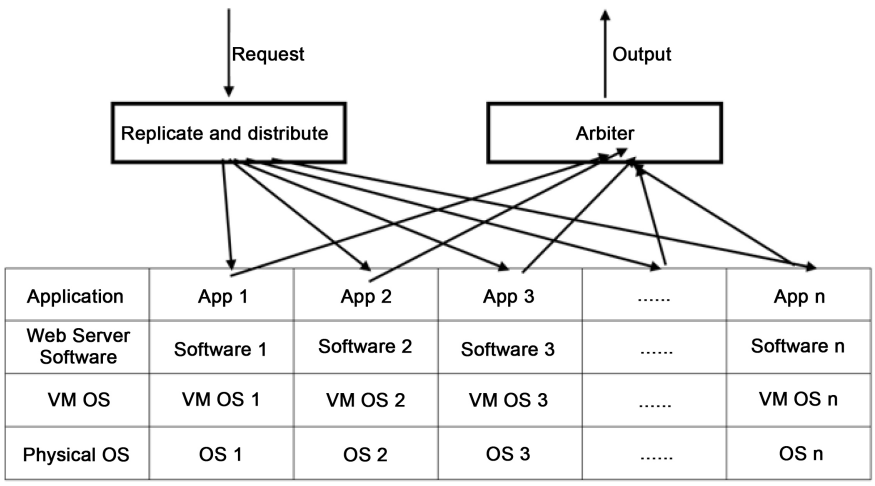

Figure 4. Mimic web defense system structure [10].

a kind of network special equipment, routers generally do not have firewalls, anti-virus and other related security protection methods, and most routers are basically undefended or unable to defend against malicious attacks. And because of the huge amount of code in the design and implementation process, there are many potential vulnerabilities. Once the attacker controls the router, he can launch a large-scale man-in-the-middle attack to steal or tamper with sensitive data. In addition, through attacks on routers, large-scale paralysis of the network can be achieved.

The mimic router introduces multiple heterogeneous redundant routing executors into its architecture and generates the routing table of the mimic router through consensus arbitration on the routing table entries maintained by each executor. Through the strategic scheduling of the executors, the uncertain changes in the external appearance of the mimic router can be realized. Under the premise of satisfying a certain differentiated design, even if an attacker controls a part of the executive body, his malicious behavior is easily blocked by the mimic ruling mechanism, thus greatly improving the router's ability to respond to network attacks.

4. Conclusions

The rapid development of the Internet has brought convenience and fun to life, but with it, many threats and risks have appeared in the network environment, and cyberspace security problems exist in every corner of people's lives. Traditional defense technology is a precise defense based on the perception of threat characteristics. For example, common defense technologies such as firewalls, intrusion detection, situational awareness can only be effectively implemented based on the prior knowledge of known attack models, attack mechanisms, and attack characteristics. For advanced attack methods based on vulnerabilities and backdoors, static defense structures are often ineffective. Although the MTD architecture reduces the attack surface by introducing randomization, dynamics, and diversification, it does not have a defensive effect against external attacks based on unknown vulnerabilities. Unlike MTD, mimic defense is unpredictable by using dynamic heterogeneous redundant architecture to make the attack surface move irregularly. Not only that, but mimic defense also requires the target object to have functionally equivalent diversified redundant software and hardware components as implementation support, that is, to improve security by increasing software and hardware resources without affecting the performance of the service function.

Mimic defense is an original integrated defense technology in cyberspace, for the open industrial chain and supply chain environment in the post-globalization era, the application of open-source software and hardware or middleware and other components with uncontrollable credibility to form a secure and credible system can reduce the life cycle cost of products. For example, the mimic web defense system verifies the feasibility of the mimic defense model and shows that

mimic defense has a good development prospect. By using different heterogeneous technologies, dynamic selection mechanisms, and other technologies, a cost-effective mimic defense web server can be constructed. Not only that, but mimic defense also has flexible deployment methods, can adapt to different application scenarios, and has a large space for development in the fields of cloud security, data security, and system security [11].

Mimic defense technologies have very important engineering significance. Although the principle of mimic defense has universal applicability, it still needs to adapt to local conditions for different fields. As more and more technologies are open source, mimic defense can use more technologies. In the future, it is more likely to change the asymmetry of offense and defense in cyberspace.

Conflicts of Interest

The author declares no conflicts of interest regarding the publication of this paper.

References

[1] Top Layer Networks (2002) Beyond IDS: Essentials of Network Intrusion Prevention. http://www.forum-intrusion.com/archive/BEYONG%20IDS.pdf

[2] Spitzner, L. (2003) Honeypots: Tracking Hackers. Reading: Addison-Wesley, Reading.

[3] Jajodia, S., *et al.* (2011) Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats. Springer, New York, USA. https://doi.org/10.1007/978-1-4614-0977-9

[4] Lu, K., Song, C., Lee, B., *et al.* (2015) ASLR-Guard: Stopping Address Space Leakage for Code Reuse Attacks. *Proceedings of the* 22*nd ACM SIGSAC Conference on Computer and Communications Security*, Denver Colorado, USA, 12-16 October 2015, 280-291. https://doi.org/10.1145/2810103.2813694

[5] Hobson, T., Okhravi, H., Bigelow, D., Rudd, R. and Streilein, W. (2014) On the Challenges of Effective Movement. *Proceeding* 1*st ACM Workshop Moving Target Defense* (*MTD*), Scottsdale Arizona, USA, 7 November 2014, 40-50. https://doi.org/10.1145/2663474.2663480

[6] Hu, H., Wu, J. and Wang, Z. (2018) Mimic Defense: A Designed-In Cybersecurity Defense Framework. *IET Information Security*, **12**, 226-237. https://doi.org/10.1049/iet-ifs.2017.0086

[7] Wu, J. (2020) Cyberspace Mimic Defense Generalized Robust Control and Endogenous Security (Wireless Networks). Springer, Cham. https://doi.org/10.1007/978-3-030-29844-9

[8] Manadhata, P.K. (2008) An Attack Surface Metric. Carnegie Mellon University, Pittsburgh.

[9] Li, W.C. and Feng, J.L. (2018) Research on Dynamic Heterogeneity Redundant Web Threat Awareness Technology. *Intelligent Computer and Applications*, **8**, 42-46+52.

[10] Chen, L.Y., Sun, X., Cheng, T.S. and Wu, C.M. and Chen, S.X. (2020) Defense of Hidden Backdoor Technology for Web. *Telecommunications Science*, **36**, 39-46.

[11] Tong, Q., Zhang, Z., Zhang, W.H. and Wu, J.X. (2017) Design and Implementation of Mimic Defense Web Server. *Journal of Software*, **28**, 883-897.