ISSN 2672-1562
VOL. 8

The 8th International Conference on Next Generation Computing 2022

ICNGC 2022

Dates October 6(THU) ~ 8(SAT), 2022

Venue ICCJEJU 201~202, Jeju, Korea

Organized by | 사단법인 한국차세대컴퓨팅학회 Korean Institute of Next Generation Computing · Jeju 제주특별자치도 · ICC JEJU · JEDIA JEJU DRONE INDUSTRY ASSOCIATION

Sponsored by | IITP Institute of Information & Communications Technology Planning & Evaluation · LG히다찌 · ESTsecurity · TRACOM · SK broadband · 쌍용정보통신주식회사 SangYong Information & Communications Corp. member of ITGroup · FIT forum Future IT forum

Derivation of Blueprint for an IoT Device Protection Design through Analysis of MTD Research

Se-Han Lee
SysCore Lab.
(Convergence Engineering for Intelligent Drone)
Sejong University
Seoul, Republic of Korea
sehands@sju.ac.kr

Ki-Woong Park*
Dept. of Computer and Information Security
Sejong University
Seoul, Republic of Korea
woongbak@sejong.ac.kr

***Abstract*— To increase the convenience in daily life activities, the Internet of Things (IoT) technology has been developed and used; it can achieve a hyper-connected society by connecting various devices and systems through the Internet. In building an IoT environment, the moving target defense (MTD) strategy is used as a method to construct an active defense strategy for a mission-critical system. However, there is a lack of indicators that can easily identify the various properties of the MTD strategy and enable in constructing and establishing a new MTD strategy-based protection plan. To solve this problem, in this paper, we survey various MTD strategy research results and analyze the research that has been conducted to derive the various properties of the three perspectives in the MTD strategy (When to move, What to move, How to move). In addition, based on the various derived properties, we propose a graph that can easily identify the various research results that appear. Additionally, it shows that the combination of various properties can be used as an indicator to understand the research direction of a new protection strategy research based on the software-defined MTD strategy for IoT device protection.**

Keywords—Moving Target Defense, Software-Defined MTD, System Security, IoT Security

I. INTRODUCTION

In modern society, the development of Internet of Things (IoT) technology has led to the application of IoT in various industrial fields (e.g., autonomous vehicles, smart health care systems, smart city, and smart grid) [1]. However, with the development of IoT technology, various cyber threats are also emerging [2]. A typical case is the Mirai Botnet, which infected vulnerable IoT devices with malicious code; the host system was used as a zombie computer for a large-scale DDoS attack, and eventually the IoT services were paralyzed [2].

In the industrial applications, moving target defense (MTD) [3] is a representative cyber protection strategy that can actively protect mission-critical systems from cyber threats. The MTD strategy, which helps construct a new protection algorithm by providing an active behavior to the system with existing static characteristics, is rapidly developing, and many research results have been reported. However, the protection technology based on the MTD strategy, which is not based on the optimal strategy, has a disadvantage that it can be applied as a large overhead to the protected system. Representing the MTD strategy as a combination of various properties of three perspectives (When to move, What to move, How to move) is one way to solve this problem. Additionally, an indicator is needed that can be used as a reference when building an optimal strategy.

Therefore, in this paper, we survey and analyze the various MTD strategy research that have been conducted and derive various properties of the three perspectives in the MTD strategy. Additionally, we analyzed the research results and show a graph of the type of research results that appear with the combination of properties. When conducting research on a new software-defined MTD strategy, the combination of the derived various properties can be used as an indicator that can conveniently identify the research direction.

This paper is structured as follows. In Section Ⅱ, we explain what an MTD strategy is and the three perspectives of an MTD strategy—When to move, What to move, How to move. In Section Ⅲ, we survey various MTD strategy research results and analyze what results have been obtained based on the contents of the survey. In Section Ⅳ, we derive various properties of the three perspectives based on the contents analyzed in Section Ⅲ and propose a graph that can identify the research results. Additionally, we show the combination of various properties and identify one direction that can be referenced on the new software-defined MTD strategy research. Finally, we explain the conclusion and future research plans in Section Ⅴ.

II. BACKGROUND OF MTD STRATEGY

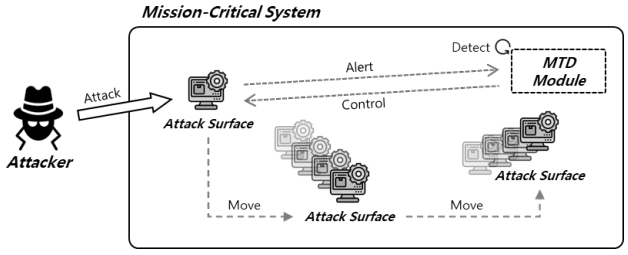

Fig. 1. Overview of Moving Target Defense Strategy Concept.

The MTD strategy is a system protection strategy to make it difficult for an attacker to find the vulnerability of the target system by actively and continuously changing the main properties of the attack target system [3].

*Corresponding Author

Using the MTD strategy has the advantage that it can actively respond to cyber threats, and any previously existing vulnerabilities that have been identified by an attacker can be nullified over time. With the advent of the MTD strategy, the paradigm has changed from passive defense against cyber attacks to active defense [4].

MTD strategy can be divided into three core perspectives—When to move, What to move, How to move; and the direction of MTD technology development is determined based on each perspective [3]. The description of each perspective is as follows.

- ***When to move***: It is the perspective of considering the optimal time for the system to which the MTD strategy is applied to change from the current state to the new state, and invalidating the vulnerability information obtained by the system attacker in the current state.
- ***What to move***: It is the perspective that analyzes the attack surface in critical systems and considers what to change in order to implement the MTD strategy.
- ***How to move***: It is the perspective that considers how to confuse an attacker by actively changing the analyzed attack surface to protect critical systems.

III. Research Trend analysis of MTD Strategy

TABLE I. SURVEY OF RESEARCH AND CONTENT ANALYSIS ABOUT MTD STRATEGY

Ref.	Detail	Target
[5]	Mutate IP address and port number according to the network-based MTD strategy called Hidden Tunnel Networking.	Network IP Address and Port Number
[6]	Block the continuity of advanced persistent threat (APT) attacks by deriving system environment elements that can be attacked from APT attacks.	System Environment Elements
[7]	Use the network protocol variation patterns to ensure that only users who know the patterns can access the server.	Network Protocol
[8]	Shuffling the network configuration properties (e.g., MAC Address, IP Address, Port Number) based on an attack graph of the host system that needs to be protected.	Network Configuration Properties
[9]	Shuffling the controller area network (CAN) ID to protect the in-vehicle network using network address shuffling (NAS).	CAN Network ID
[10]	A strategy to secure CAN network communications by configuring switches in the CAN bus circuit inside the vehicle.	CAN Bus Circuit Board
[11]	Shuffling IP address using multiple software-defined network (SDN) controllers in SDN-based network environment.	Network IP Address
[12]	Provides optimal network configuration through SDN network topology analysis using shuffle-based online MTD.	Network Topology
[13]	Provide a new CAN bus protocol that uses randomization seeds to randomly generate ECU IDs.	ECU ID on the CAN Bus

Research on protection technology using the MTD strategy is currently being actively conducted. The contents of the latest MTD strategy research trend survey and analysis are shown in “TABLE I.”

Currently, MTD strategy research implements a protection technology based on a SW, and many researches are conducted to protect a system that exists primarily in the network layer. As a representative attack surfaces, it can be seen that the IP address, port number, and MAC address are derived. Additionally, we can also check the other attack surfaces of the network topology, packet ID, and network protocols.

In addition to SW-based technology, it was confirmed that HW-based technology is also being researched. A typical example is to reconfigure the CAN communication bus circuit located inside the autonomous vehicle with a switch to bypass malicious CAN network traffic and prevent damage to the system.

IV. Derivation of Properties of Three Perspectives in MTD Strategy

In this paper, as a way to develop a cost-efficient protection technology using MTD strategy, we intend to represent the MTD strategy as a combination of various properties of the three perspectives (When to move, What to move, How to move). To do this, based on the contents analyzed in "TABLE I," we analyzed the individual properties of each perspective.

TABLE II. PROPERTIES OF THREE PERSPECTIVES OF MTD STRATEGY THROUGH ANALYSIS OF MTD RESEARCH RESULTS

Ref.	When to move	What to move	How to move
[5]	Prevention	Network IP Address, Network Port Number	Decoy, Variation
[6]	Prevention	System Environment Elements	Variation
[7]	Prevention	Network Protocol	Randomization, Patternization
[8]	Prevention	Network IP Address, Network Port Number, Network MAC Address	Shuffling
[9]	Detection	Network Packet ID	Shuffling
[10]	Detection	Electric Signal in to the Circuit Board	HW Switch
[11]	Detection	Network IP Address	Shuffling
[12]	Detection	Network Topology	Shuffling
[13]	Prevention	ECU Device ID	Shuffling, Randomization

The properties derived from the three perspectives of the MTD strategy are presented in "TABLE II."

First, in the perspective of "When to move," a total of two properties were derived and classified into a case of prevention and detection of a cyber threat. Second, in the perspective of "What to move," a total of nine properties, including network IP address, network port number, network MAC address, ntwork protocol, network packet ID, network topology, ECU device ID, circuit board, and system environment elements, were derived and classified. Finally, in the perspective of "How to move," a total of six properties, including decoy, variation, shuffling, randomization, patternization, and HW switch, were derived and classified.

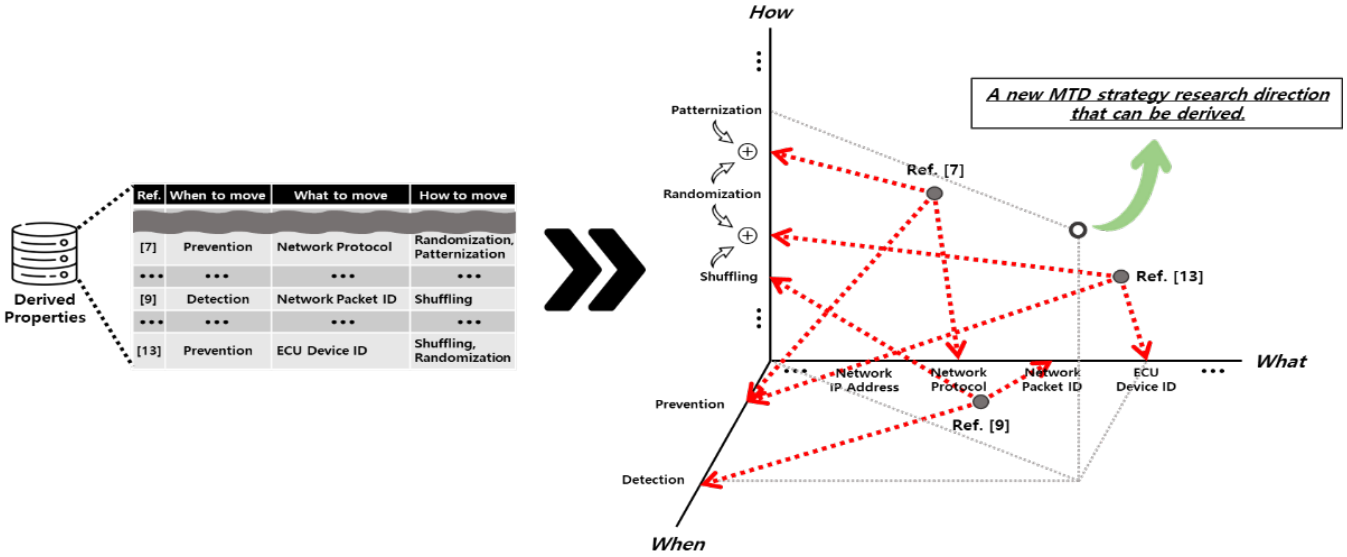

Fig. 2. Graph that can be represented as a combination of properties in three perspectives.

As shown in Fig. 2, we represented the type of research results that appear with the combination of derived properties as a graph. The graph proposed in this paper identifies the strategic structure of the recent MTD strategy research results based on the research direction.

In addition, the proposed graph shows that another combination of derived properties is possible. Moreover, it can be used as an indicator that can be referred to as a research direction in building a new software-defined MTD protection algorithm. In Fig. 2, we represent the properties that indicate the results of three researches as an example. Additionally, it shows an example that can be referenced as a new MTD strategy research direction.

V. Conclusion

The MTD strategy is a constructive defense strategy that protects against cyber attacks by actively changing the main properties of a system that can become a cyber threat and minimizes changes in the existing system behavior. This strategy has the advantage of obfuscating the exact configuration of the system to confuse the attacker. However, if the MTD strategy is used without an optimal algorithm configuration, it will increase the overhead of the entire system. To solve this problem, it is necessary to construct a cost-effective protection algorithm with an optimal strategy.

In this paper, we survey and analyze the recent MTD strategy research results to derive the properties that exist in the three perspectives of the MTD strategy. Then, we propose a graph that can easily identify the protection algorithm strategy of each research result by combining the derived properties. Based on the proposed graph, it is possible to confirm how the direction of MTD strategy research is constructed, and it can be used as an indicator to conveniently grasp the direction in conducting a new software-defined MTD strategy research with a combination of other properties.

In the future, based on the method to identify the research direction of a new protection strategy derived from this paper, we intend to develop a framework for constructing a software-defined MTD strategy that can be used as a best practice in researching new software-defined MTD protection technology. Moreover, this new framework could be applied to the research of a new security system using the MTD strategy.

Acknowledgment

This work was partly supported by the ICT R&D Program of MSIT/IITP (Project No. 2021-0-01816, A Research on Core Technology of Autonomous Twins for Metaverse, 10%), the Institute of Information & Communications Technology Planning & Evaluation (IITP) (Project No. 2019-0-00426, 20%; Project No. RS-2022-00165794, Development of a Multi-Faceted Collection-Analysis-Response Platform for Proactive Response to Ransomware Incidents, 30%; Project No. 2022-0-00701, Development of Security Technology for Interworking between M-BcN and 5G Commercial Network, 10%), a National Research Foundation of Korea (NRF) (Project No. NRF-2020R1A2C4002737, 30%) grant funded by the Korean Government.

References

[1] Mardiana Binti Mohamad Noor and Wan Haslina Hassan, “Current research on Internet of Things (IoT) security: A Survey,” Computer Networks, vol. 148, pp. 283-294, January 2019.

[2] Nataliia Neshenko et al., “Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations,” IEEE Communications Surveys & Tutorials, vol. 21, No. 3, pp. 2702-2733, April 2019.

[3] Jin-Hee Cho et al., “Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense,” IEEE Communications Surveys & Tutorials, vol. 22, No. 1, pp. 709-745, January 2020.

[4] Gui-lin Cai et al., “Moving target defense: state of the art and characteristics,” Frontiers of Information Technology & Electronic Engineering, vol. 17, pp. 1122-1153, November 2016.

[5] Tae-Keun Park et al., “Attack Surface Expansion through Decoy Trap for Protected Servers in Moving Target Defense,” Journal of the Korea Society of Computer and Information, vol. 24, no. 10, pp.25-32, October 2019.

[6] Moon Seo Yeon, “A Study on the Moving Target Defense Model for Advanced Persistent Threat Security,” Proceedings of the Korean Institute of Communications and Information Sciences Summer Conference 2018, June 2018.

[7] Jun-Gyu Park et al., "Ghost-MTD: Moving Target Defense via Protocol Mutation for Mission-Critical Cloud Systems," Energies, vol. 13, no. 8, April 2020.

[8] Seunghyun Yoon et al., "Attack Graph-Based Moving Target Defense in Software-Defined Networks," IEEE Transactions on Network and Service Management, vol. 17, no. 3, pp.1653-1668, September 2020.

[9] Samuel Woo et al., "CAN ID Shuffling Technique (CIST): Moving Target Defense Strategy for Protecting In-Vehicle CAN," IEEE Access, vol. 7, pp. 15521-15536, February 2019.

[10] Bogdan Groza et al., "CANARY – a reactive defense mechanism for controller Area Networks based on Active RelaYs," Proceedings of the 30th USENIX Security Symposium, August 2021.

[11] Jargalsaikhan Narantuya et al., "SDN-Based IP Shuffling Moving Target Defense with Multiple SDN Controllers," 49th Annual IEEE/IFIP International Conference on Dependable Systems and Networks – Supplemental Volume (DSN-S), pp. 15-16, August 2019.

[12] Jin Bum Hong et al., "Optimal Network Reconfiguration for Software Defined Networks Using Shuffle-Based Online MTD," 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), pp. 234-243, September 2017.

[13] Richard Brown et al., "Dynamic Address Validation Array (DAVA): A Moving Target Defense Protocol for CAN bus," Proceedings of the 7th ACM Workshop on Moving Target Defense, pp. 11-19, November 2020.