Data Visualization Engine for systematic MTD Strategy Configuration linked to Cyber Attack Information

Se-Han Lee
SysCore Lab.
(Convergence Engineering for Intelligent Drone)
Sejong University
Seoul, Republic of Korea
sehanlee141@gmail.com

Mohsen Ali Alawami
SysCore Lab.
Sejong University
Seoul, Republic of Korea
mohsencomm@sejong.ac.kr

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

***Abstract*— In the modern society, with the development of Information & Communications Technology (ICT), the cyber threat is also increasing, and to prepare for this, Moving Target Defense (MTD) strategy is widely used to actively protect the Mission-Critical Systems. Although the MTD strategy has shifted the paradigm from passive system defense to active system defense, the indiscriminate use of the MTD strategy has the disadvantage of acting as a large overhead on the system to be protected. To solve this problem, in this paper, we derive the attack surface of the system to be protected using cyber attack information (OpenIOC). Then, based on the derived data, we propose a data visualization engine that can help configure a systematic MTD strategy by linking it with MTD strategy components. Through the proposed data visualization engine, existing and new MTD strategy researchers can configure a more systematic MTD strategy.**

Keywords*— *Moving Target Defense, OpenIOC, Cyber Attack Surface, Data Visualization

I. INTRODUCTION

Today's modern information society is transforming into a Hyper-Connected Society with the development of ICT [1]. In this society, for instance, Internet of Things (IoT) technology is an essential technology and is currently being used in various industrial fields (e.g. Smart Medical Devices, Autonomous Vehicles, Smart Cities, etc.) [2, 3]. In particular, in the case of Smart Medical Devices, medical devices that could only be used in special facilities such as hospitals have been miniaturized and developed into a form that can be used and utilized at anytime in general areas of life [4].

However, with the development of ICT, various cyber attacks are occuring [5]. As a representative example, there is a case of an IoT attack using the Mirai Botnet [6], which is a case of a large-scale DDoS attack by targeting vulnerabilities in IoT devices and inserting malware and distributing it through a shared network.

At a time when ICT being used across industries, MTD strategy that can actively protect Mission-Critical Systems have emerged and are being utilized [7]. The MTD strategy can help protect the system safely from cyber threats by providing a way to take active action targeting the system to be protected, and many research results related to this are currently emerging [8]. However, the indiscriminate use of the MTD strategy has the disadvantage of applying a large overhead to the system to be protected.

To solve this, there is a need for indicators in the form of visualization data that can help configure an systematic MTD strategy by identifying various components of the three core perspectives of the MTD strategy (When to move, What to move, How to move) and the attack surface of various cyber threats.

Accordingly, in this paper, we analyzed the results of existing MTD strategy research to derive each component of three key perspectives of MTD strategy, and derived components (Attack Surface) for cyber attack information using the Open Indicators of Compromise (OpenIOC) standard. Afterwards, we designed and implemented a Data Visualization Engine to provide a single piece of visual information that can show the connection points between each derived component. Through this, we aim to help provide component combination indicators in configuring a more systematic MTD strategy.

This paper is structured as follows. In Section II, we explain the MTD strategy and OpenIOC standard necessary to carry out this research. In Section III, we describe the composition of component datasets for use in the Data Visualization Engine. In Section IV, we show the structure and implementation of the Data Visualization Engine. Additionally, we explain how to use this engine for existing and new MTD strategy researchers. Finally, we explain the conclusion and future research plans in Section V.

II. BACKGROUND

A. Moving Target Defense(MTD) Strategy

The Moving Target Defense(MTD) strategy forces attackers to put more effort into analyzing vulnerabilities by actively and continuously changing the system configuration itself, which can be the target of an attack [8]. Additionally, even if a discovered vulnerability exists, it has the advantage of being able to nullify the vulnerability over time [7, 8, 11]. An overview of MTD strategy is shown in "Fig. 1".

In order to implement this MTD strategy, a combination of components from three core perspectives is required, which is include: ("What to move", "When to move", and "How to move") [7, 8]. The description of each perspective is as follows.

- ***Perspective of What to move***: This perspective analyzes the attack surface within the system and considers what needs to be changed in order to implement an MTD strategy to be applied to a mission-critical system.
- ***Perspective of When to move***: This perspective considers the optimal time to change from the current state to a new state when the MTD strategy is applied

* Corresponding author

to a mission-critical system. Through this perspective, vulnerability information obtained by an attacker can be invalidated.

- ***Perspective of How to move***: This perspective is about how to confuse attackers by changing their targeted attack surface within mission-critical system.

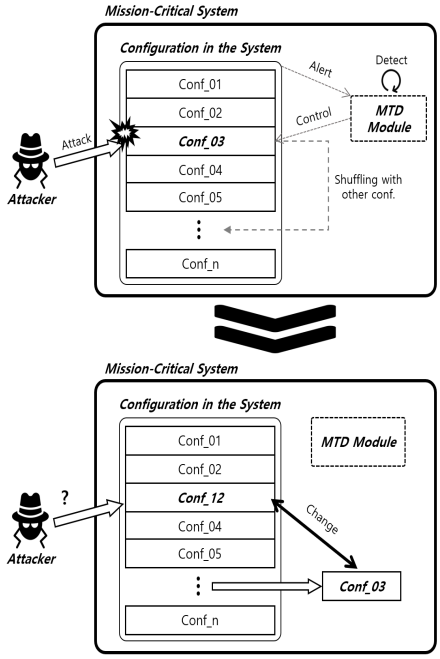

Fig. 1. An overview of Moving Target Defense (MTD) Strategy.

B. *Open Indicators of Compromise(IOC) Standard*

The Open Indicators of Compromise(IOC) standard [9, 11] is an open incident indicators for cyber threat, an open source-based framework developed by Mandiant. It provides various indexes that can identify data from various attack surfaces contained in one cyber threat information. A simple example of OpenIOC is shown in “Fig. 2”.

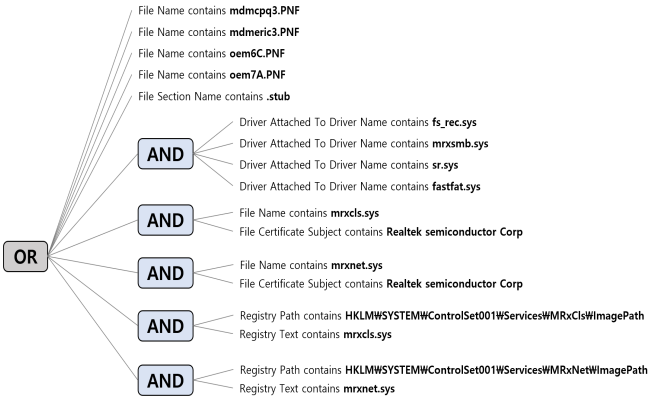

Fig. 2. An example of *Stuxnet* expression using OpenIOC [10].

This incident indicators is widely used when analyzing cyber threat within governments or companies. It is provided in the form of an XML document that helps capture various artifacts about specific cyber attack information. In addition, it provides indexes that can identify various artifact information from a digital forensics perspective, and collects various data corresponding to each index. This helps to determine which attack surface is being used for a specific attack information to perform the cyber attack.

III. Configure Dataset for Data Visualization Engine

We classified system sections to show the overall system structure through the data visualization engine proposed in this paper. To classify system sections, various artifact indexes were analyzed with reference to the OpenIOC standard and classified into a total of 5 system sections—*Network Section*, *OS Configuration Section*, *Storage Section*, *Application Section* and *Log Section*.

In addition, a dataset was configured by classifying attack surface components corresponding to each section. When configuring the dataset to express each system section, *Network Section* was expressed as *N*, *OS Configuration Section* as *O*, *Storage Section* as *S*, *Application Section* as *A*, and *Log Section* as *L*.

A. *Configure Dataset of MTD Strategy Components*

In order to derive MTD strategy components to be used in the data visualization engine, existing MTD strategy research results were analyzed [12]. And based on the analysis results, components were derived from three key perspectives of MTD Strategy— What to move, When to move, and How to move. Afterwards, the components of each perspective derived were utilized to configure a dataset that could be used in a data visualization engine. In addition, the Section Code attribute was added to help distinguish which MTD strategy is targeting out of a total of five system sections.

The method of configuring the MTD strategy dataset to be used in the data visualization engine is shown in "Fig. 3".

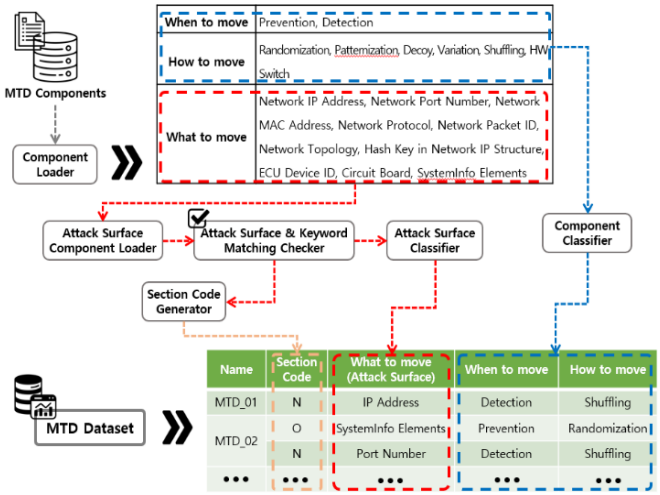

Fig. 3. A method for configuring MTD Strategy Components Dataset.

The explain of the MTD strategy components dataset configuration process is as follows.

The dataset configuring process begins by importing the analyzed MTD strategy components through “Component Loader”. The components of the *When to move* perspective and the *How to move* perspective are combined into components of one MTD strategy by the “Component Classifier” and stored in the dataset. Components from the *What to move* perspective can be classified as attack surfaces, so component data is first imported by the “Attack Surface Component Loader”. Afterwards, through the “Attack Surface & Keyword Matching Checker”, it is classified into which section of the system the attack surface exists. And through the “Attack Surface Classifier”, data is generated according to each section of the system and stored in the dataset.

This process is repeated to configure the MTD strategy components dataset, and an example of which is shown in "TABLE I".

TABLE I. AN EXAMPLE OF MTD STRATEGY COMPONENTS DATASET

Name	Section Code	What to move	When to move	How to move
MTD-01	N	IP address	Prevention	Shuffling
MTD-02	N	Port Protocol	Detection	Patternization
MTD-03	S	File Name	Detection	Randomization
MTD-03	S	File Path	Detection	Randomizaiton
MTD-04	O	Registry Path	Detection	Decoy
MTD-04	A	Process PID	Prevention	Decoy
MTD-01	N	MAC Address	Prevention	Shuffling
MTD-01	S	File Name	Prevention	Randomization

B. *Configure Dataset of Cyber Attack Information*

In order to show in what section cyber attack occur through the data visualization engine, components were derived using the OpenIOC standard [12]. Afterwards, each derived component was used to classify the attack surfaces of each cyber attack, and a dataset was configured to indicate which section (one of a total of 5 system sections) the attack surface belongs to.

The method of configuring the cyber attack information dataset to be used in the data visualization engine is shown in "Fig. 4".

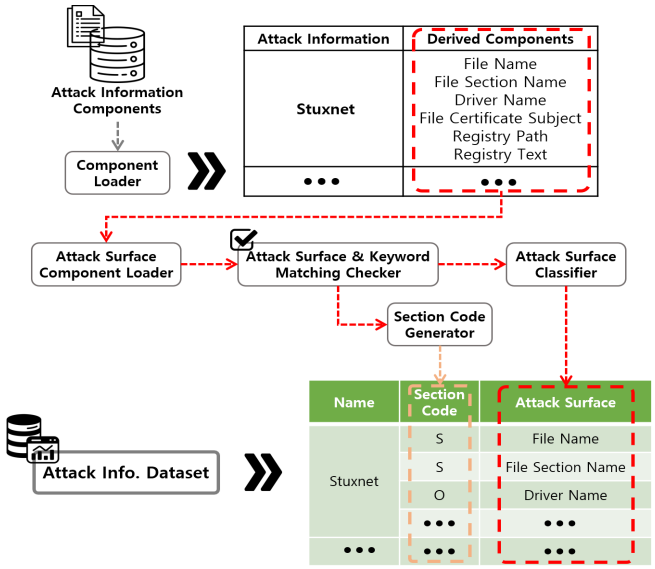

Fig. 4. A method for configuring Cyber Attack Information Dataset.

The explain of the cyber attack information dataset configuration process is as follows.

The dataset configuring process begins by importing the analyzed cyber attack information components through "Component Loader". Since the components of the analyzed cyber attack information have been identified as the attack surface, the components are imported directly through "Attack Surface Component Loader". Afterwards, it is classified into components for each section of the mission-critical system through the "Attack Surface & Keywords Matching Checker". And then, data is generated according to each system section using the "Section Code Generator" and "Attack Surface Classifier" and stored in the dataset. By repeating this process, a cyber attack information component dataset that can be used in a data visualization engine is configured in the same way that the MTD strategy component dataset was configured.

An example of the configured cyber attack information dataset is shown in "TABLE II". It is configured from the name of the cyber attack information, the system section code to which the attack surface of the attack information belongs, and the attack surface data contained in the attack information.

TABLE II. AN EXAMPLE OF CYBER ATTACK INFORMATION DATASET

Name	Section Code	Attack Surface
Attack-01	N	IP Address
Attack-02	O	Registry Path
Attack-02	O	Registry SecurityID
Attack-03	N	MAC Address
Attack-03	A	Process PID
Attack-04	N	IP Address
Attack-04	S	File Path
Attack-04	A	Process PID
Attack-04	L	EventLog User

IV. DATA VISUALIZATION ENGINE FOR SYSTEMATIC MTD STRATEGY CONFIGURATION

In this section, we describe the design and implementation of data visualization engine for configuring systematic MTD strategy. And also explains how to use the data visualization engine.

A. *System Structure Design for Data Visualization Engine*

In this research, we derived and classified the components of various existing MTD strategy research information and cyber attack information. In addition, a component data visualization engine is designed to provide visual information to identify the connectivity between the two datasets conveniently, and to identify what attack surfaces the MTD strategy information can respond to in actual cyber-attacks.

The data visualization engine configuration diagram designed in this research is shown in "Fig. 5".

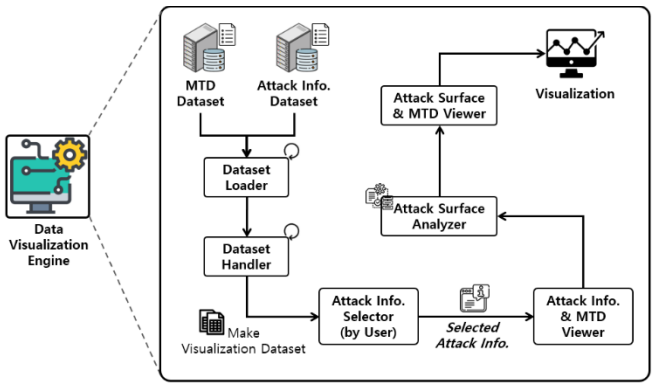

Fig. 5. A system structure diagram designed for Data Visualization Engine.

The explain of the system structured diagram designed to implement a data visualization engine is as follows.

"Dataset Loader" imports the two datasets that configured earlier. "Dataset Handler" creates a new dataset to be used inside the data visualization engine, and "Attack Information Selector" identifies specific cyber attack information selected by the user using the data visualization engine. Afterwards, "Attack Information & MTD Viewer" operates to visualize the selected specific attack information and MTD strategy information related to it. In addition, "Attack Surface Analyzer" analyzes the attack surface of selected cyber attack

information, and “Attack Surface & MTD Viewer” operates to visualize MTD strategy information that can respond to each attack surface.

B. *Implementation of Data Visualization Engine*

In this research, a data visualization engine was implemented using the previously configured dataset and visualization engine configuration diagram, and the result of implementation is shown in “Fig. 6”.

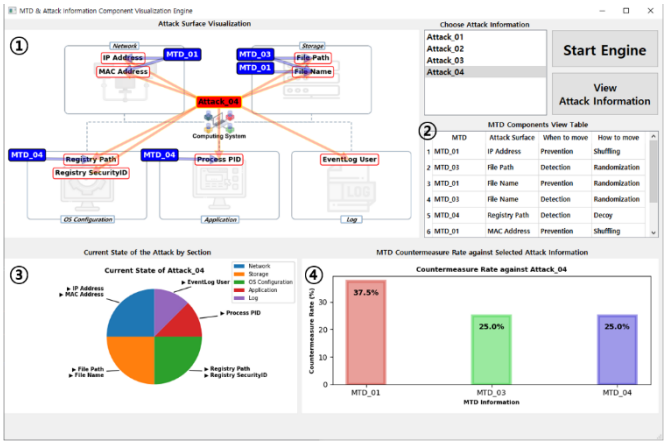

Fig. 6. An implemented Data Visualization Engine.

The explain of implemented data visualization engine is as follows.

① It visualizes the attack surface of the attack information selected by the engine user within a total of five system sections, and the MTD strategy that can respond to the attack surface.

② It displays the MTD strategy component dataset information imported when the data visualization engine starts.

③ It provides visual information as a pie chart so that the engine user can check the ratio of attack information selected by the user to which section in the system most attacks are performed out.

④ It provides visual information as a bar graph so that the engine user can check the ratio of MTD strategy information that can be responded based on the attack information selected.

C. *Utilization of Data Visualization Engine*

The data visualization engine implemented in this research can help not only existing MTD strategy researchers but also new MTD strategy researchers. Existing MTD strategy researchers can use it as an indicator to check whether their MTD strategy research is configured of optimal components. And new MTD strategy researchers can combine optimal strategy components when establishing their desired cyber attack response strategy, which can be used as an indicator to determine a research direction.

V. Conclusion

The MTD strategy, one of the strategies to actively respond to various cyber threats, has made it possible to configure a proactive defense strategy for the mission-critical system. However, indiscriminate use of the MTD strategy can actually result in a large overhead for the system. Therefore, there is a need for a method to apply the optimal protection mechanism through systematic MTD strategy configuration.

In this paper, we designed and implemented a data visualization engine that configures a dataset of MTD strategy information and cyber attack information and visually shows the connectivity of the two datasets. Through this, it can be used as an indicator of how to configure the systematic MTD strategy for specific cyber attack information.

In the future, we plan to implement the actual operation method of the MTD strategy in a simulation to configure a visual information method that can show detailed information on how the existing MTD strategy research results respond to the attack surface within the mission-critical system. Furthermore, we would like to implement a visualization engine capable of simulating its own mission-critical system attack and defense.

Acknowledgment

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) (Project No. RS-2022-00165794, 30%; Project No. 2022-0-00701, 10%; Project No. RS-2023-00228996, 10%), the ICT R&D Program of MSIT/IITP (Project No. 2021-0-01816, 10%), and a National Research Foundation of Korea (NRF) grant funded by the Korean government (Project No. RS-2023-00208460, 40%).

References

[1] J. H. Nord, A. Koohang and J. Paliszkiewicz, "The Internet of Things: Review and theoretical framework," Expert Systems with Applications, Vol.133, No.1, pp.97-108, Nov., 2019.

[2] N. 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, Apr., 2019.

[3] M. B. M. Noor and W. H. Hassan, "Current research on Internet of Things (IoT) security: A survey," Computer Networks, Vol.148, No.15, pp.283-294, Jan., 2019.

[4] D. Koutras et al., "Security in IoMT Communications: A Survey," Sensors, Vol.20, No.17, 4828, Aug., 2020.

[5] Vikas Hassija et al., "A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures," IEEE Acccess, Vol.7, pp.82721-82743, Jun., 2019.

[6] M. Antonakakis et al., "Understanding the Mirai Botnet," Proceedings of the 26th USENIX Security Symposium, pp.1093-1110, Aug., 2017.

[7] 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, Jan., 2020.

[8] Se-Han Lee and Ki-Woong Park, "Derivation of Blueprint for an IoT Device Protection Design through Analysis of MTD Research," Proceedings of the 8th International Conference on Next Generation Computing 2022 (ICNGC 2022), pp.310-313, Oct., 2022.

[9] Keoungchan Yoon et al., "Design of CTI framework that combines Open IDS and CVE based OpenIOC," Proceedings of the Korea Information Processing Society (KIPS) Spring On-line Conference 2020, Vol.27, No.1, pp.286-289, May, 2020.

[10] Jin-Kook Kim, “Utilization of IOC, IOAF and SigBase,” Forensic Insight, 2013.

[11] FireEye, "OpenIOC v1.1", https://github.com/fireeye/OpenIOC_1.1

[12] Se-Han Lee, "Data Visualization Engine Design and Implementation for configuring Moving Target Defense Strategy linked to Cyber Attack Information," Sejong University, Master dissertation, Feb., 2023