DOI: http://dx.doi.org/10.23089/jdca.2022.5.2.008

MTD 전략 연구 결과 분석을 통한 IoT 장치 보호 소프트웨어 정의 MTD 연구 방향성 도출 방안

A Method for Derivation of Software-Defined MTD Research Direction for secure IoT Device through Analysis of MTD Strategy Research Result

이세한(Se-Han Lee) | 세종대학교 일반대학원 정보보호학과 석사과정 | sehanlee141@gmail.com
박기웅(Ki-Woong Park)† | 세종대학교 정보보호학과 교수 | woongbak@sejong.ac.kr

목 차

초 록

다양한 사물에 인터넷이 연결되어 초연결 사회를 이룰 수 있는 사물인터넷 환경에서 능동적인 보호 전략을 구사하기 위해 MTD (Moving Target Defense)가 활용되고 있다. 그러나 최적의 전략이 바탕이 되지 않은 MTD 전략 구사는 보호 대상 시스템에 하나의 큰 오버헤드로 작용할 수 있는 단점이 존재한다. 이를 해결하기 위해 본 논문에서는 최근 MTD 전략 연구에 대해 조사하고 각각의 연구 결과들을 분석한다. 이후 분석한 연구 결과들로부터 MTD 전략의 세 가지 관점(When to move, What to move, How to move)의 다양한 속성들을 도출하여 향후 IoT 장치 보호를 위한 새로운 소프트웨어 정의 MTD 연구를 수행할 때 필요한 연구 방향성을 도출할 수 있는 방안을 제안한다.

* 키워드: Moving Target Defense(MTD), 소프트웨어 정의형 시스템, 능동 보호, 시스템 보안, 시스템 속성

ABSTRACT

Moving Target Defense (MTD) is being used to implement an active protection strategy in the Internet of Things (IoT) environment where various things are connected to the Internet to form a hyper-connected society. However, there is a disadvantage that the use of an MTD strategy that is not based on an optimal strategy can act as a large overhead for the system to be protected. In this paper, we survey and analyze recent MTD strategy research to solve this problem. And we derive various properties of the 3 perspectives in MTD strategy from analyzed MTD strategy research. With derived various properties, we propose a method to derive the research direction of the new software-defined MTD research for secure IoT device in the future.

* KeyWords : MTD, Active Protection, System Security, Research Direction, Property

† 교신저자

• 본 논문은 과학기술정보통신부의 재원으로 정보통신기획평가원의 대학ICT연구센터육성지원사업(No. 2021-0-01816, 20%), 정보보호핵심원천기술개발사업(No. 2019-0-00426, 20%), 정보보호국제공동연구(No. RS-2022-00165794, 20%), 국방ICT융합사업(No. 2022-0-00701, 20%) 및 한국연구재단 중견연계연구지원사업(No. NRF-2020R1A2C4002737, 20%)의 지원을 받아 수행된 연구임.
• 논문접수 : 2022년 9월 8일 •최초심사일: 2022년 10월 1일 •심사완료일: 2022년 10월 1일

1. 서론

현대의 정보화 시대에는 다양한 사물이 서로 인터넷으로 연결되어 초연결사회를 이루는 사물인터넷(IoT, Internet of Things) 사회가 등장하여 발전하고 있다. 이러한 사물인터넷 기술의 발전으로 IT 기술이 다양한 산업 분야 (예를 들어 자율주행 자동차, 스마트 의료기기, 스마트그리드 등)에서 활용되고 있다(Mardiana Binti Mohamad Noor & Wan Haslina Hassan, 2019). 하지만 IoT 기술의 발전과 더불어 다양한 사이버 위협이 나타나고 있는 상황이다. 대표적으로 미라이 봇넷을 이용한 사이버 공격 사례가 존재하며, 이는 취약한 IoT 기기가 악성코드에 감염이 되고 호스트 PC가 좀비 PC로 악용되어 대규모 DDoS 공격에 사용되었으며 결국 IoT 서비스 마비가 유발되었던 사례이다(M. Antonakakis et al., 2017).

IoT 기술이 산업 전반에서 사용되고 있는 현 상황에 있어 중요한 시스템을 능동적으로 보호할 수 있는 대표적인 사이버 보호 전략으로 MTD(Moving Target Defense)(Jin-Hee Cho et al., 2020)가 활용되고 있다. MTD 전략은 기존의 정적인 특성을 지니고 있는 시스템에 능동적인 행동을 제공하여 새로운 보호 알고리즘을 구성할 수 있도록 도움을 주며, 현재 많은 연구 결과가 나타나고 있는 상황이다. 그러나 MTD 전략을 활용함에 있어 최적의 전략 구성이 바탕이 되지 않으면 오히려 기존 시스템에 하나의 큰 오버헤드로 작용하여 비용 대비 효율적인 보호 시스템 구축이 어려운 단점이 존재한다. 이를 해결하기 위한 하나의 방안으로서 MTD 전략을 세 가지 핵심적인 관점 (When to move, What to move, How to move)의 다양한 속성 조합으로 표현하여 최적의 전략을 구사하기 위한 방향성 도출 방안이 필요한 상황이다.

이에 본 논문에서는 세 가지 핵심적인 관점에서의 다양한 속성들을 도출하기 위해 현재까지 어떤 MTD 전략 연구가 진행되었는지를 조사하고 어떠한 연구 결과가 나타났는지를 분석한다. 이를 토대로 MTD 전략의 세 가지 관점에 대한 다양한 속성들을 도출하고, 속성의 조합으로 어떠한 연구 결과가 나타나는지를 표현한다. 이와 같이 분석된 세 가지 관점에서의 다양한 속성 조합으로 IoT 장치를 보호함에 있어 최적의 전략 구성이 가능한 새로운 소프트웨어 정의 MTD 연구 방향성을 도출할 수 있는 방안을 제안하고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 현재 IoT 환경에서의 사이버 보안 위협 사례에 대해 설명하고, MTD 전략과 세 가지 핵심적인 관점에 대해 설명한다. 3장에서는 MTD 전략의 세 가지 관점 내 다양한 속성들을 도출하기 위한 사전 작업으로 MTD 전략 연구들을 조사하고 조사한 내용을 바탕으로 어떤 연구 결과가 나타났는지를 분석한다. 4장에서는 3장에서 분석된 내용을 기반으로 세 가지 관점의 다양한 속성들을 도출하여 이를 바탕으로 각각의 MTD 전략 연구 결과가 어떠한 속성을 지니고 있는지를 시각적으로 표현하고, 다양한 속성들의 조합으로 소프트웨어 정의 MTD 연구 수행에 있어 새로운 연구 방향성을 도출할 수 있는 하나의 방안을 제안한다. 마지막으로 5장에서는 결론과 향후 연

구 계획에 대해 설명한다.

2. 관련 연구

본 장에서는 현재 IoT 장치를 대상으로 하는 사이버 보안 위협이 무엇이 있는지를 조사하고 설명한다. 또한 MTD(Moving Target Defense) 전략이 무엇인지에 대해 설명하고, MTD 전략의 장점과 MTD 전략을 활용하기 위한 세 가지 핵심적인 관점(When to move, What to move, How to move)에 대하여 설명한다.

2.1 IoT 장치 대상 사이버 보안 위협 사례

IoT 기술의 궁극적인 목표는 다양한 첨단 기술을 활용하여 사물 및 기계, 인간 사이의 초연결 네트워크를 구성하여 실시간 상호 작용을 구현하는 것이다. 오늘날 IoT 기술은 스마트 헬스케어, 자율주행 자동차, 스마트 시티 등 다양한 분야에서 활용되고 있으며 다양한 IoT 장치가 등장하고 있다(Mardiana Binti Mohamad Noor & Wan Haslina Hassan, 2019). 최근에는 점점 소형화된 IoT 장치가 등장하여 IoT 기술 활용에 있어 편리성을 증대시키고 있지만, 이러한 IoT 장치를 대상으로 하는 사이버 보안 위협이 지속적으로 발생하고 있는 상황이다(V. Hassija et al., 2019). IoT 장치 보안 위협으로는 기기 자체를 정지시키거나 오작동을 유발하여 인프라를 마비시키고 인명피해(예를 들어 인슐린 펌프 장치의 통제권 획득)를 일으킬 수 있는 위협이 존재하며, 기기의 분실, 도난, 위변조 등에 의해 개인정보가 유출되거나 변조되는 위협이 존재한다(김정녀, 진승헌, 2017). 또한 IoT 장치 간 네트워크 환경에서의 악성코드 유포 등으로 인해 취약점 공격이 발생할 수 있는 위협이 존재한다(금융보안원, 2016).

<표 1> IoT 장치 유형 분류 및 사이버 보안 위협 사례

유형	장치	보안 위협
센서	온도 및 습도 센서 등	· 장치 분실 및 도난으로 인한 데이터 유출 · 장치 내 USB 포트를 이용한 악성 코드 유포 · 전기 소모량 및 신호 등 부채널 분석을 통한 공격 · 차량 내 OBD-II 포트에 연결하여 스마트 키 복제 · 차량 인포테인먼트 시스템에 접근(USB 포트, 또는 차량 네트워크 원격 접속 등)하여 무인주행기능 오동작 유도 · 센서 데이터 변조 등으로 기기 멈춤 및 이상 행위 동작을 유발하는 스푸핑 공격
생활가전	로봇청소기, AI 기반 냉장고 등	
자율주행 자동차	인포테인먼트, OBD-II 포트 연결 장치 등	
스마트 헬스케어	인슐린 펌프, 심장박동기 등	

2.2 MTD 전략의 개요

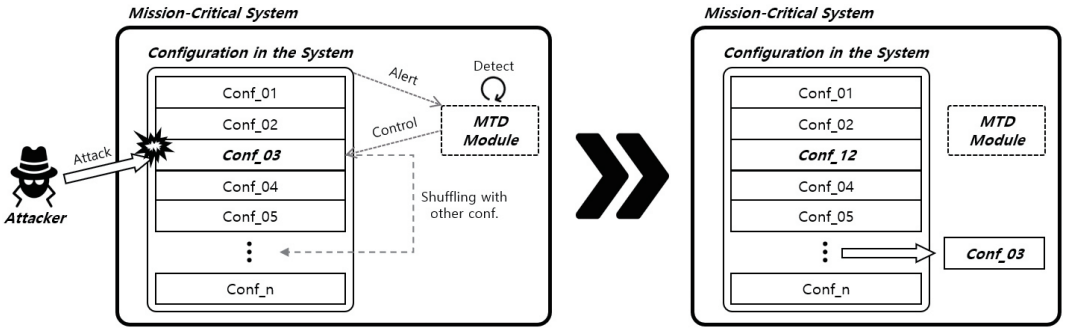
MTD(Moving Target Defense) 전략은 공격의 대상이 되는 중요 시스템 자체의 공격 대상 표면을 능동적으로 그리고 지속적으로 변화시켜 공격자가 공격 목표 시스템의 취약점 자체를 찾기 어렵게 하기 위한 하나의 시스템 능동 보호 전략이다(Jin-Hee Cho et al., 2020). MTD 전략을 활용하게 되면 IoT 환경에서의 사이버 위협에 대하여 능동적으로 대응할 수 있는 장점이 있으며, 공격자가 이전에 미리 파악한 취약점이 존재하더라도 시간이 지나면서 이를 무효화할 수 있는 장점이 존재한다. MTD 전략의 등장으로 인해 사이버 위협에 대한 기존의 소극적인 방어 기법에서 적극적인 방어 기법으로 사이버 보안 패러다임이 변화하게 되었다(Renzo E. Navas et al., 2021).

MTD 전략은 총 세 가지의 핵심적인 관점(When to move, What to move, How to move)(Jin-Hee Cho et al., 2020)으로 나누어질 수 있으며, 각각의 관점을 토대로 MTD 전략 기술 개발의 방향성이 결정된다. 각각의 관점에 대한 설명은 다음과 같다.

① When to move(언제 이동할 것인가): MTD 전략이 적용된 시스템이 현재 상태에서 새로운 상태로 변화하기 위한 최적의 시간을 고려하고, 현재 상태에서 시스템 공격자가 얻은 취약점 정보를 무효화하는 것에 대한 관점이다.

② What to move(무엇을 이동할 것인가): MTD 전략을 수행하기 위해 중요 시스템 내 공격 표면(또는 시스템 구성 요소)을 분석하고 무엇에 변화를 줄 것인지에 대해 고려하는 관점이다.

③ How to move(어떻게 이동할 것인가): 중요 시스템을 보호하기 위해 분석된 공격 표면을 어떻게 능동적으로 변화하여 공격자를 교란시킬 수 있는지(또는 시스템을 어떻게 난독화할 수 있는지)에 대해 고려하는 관점이다.



<그림 1> Moving Target Defense 전략의 개념도

3. 국내외 MTD 전략 연구 조사 및 분석

본 장에서는 최근에 MTD 전략을 활용한 보호 시스템 또는 보호 메커니즘 연구가 무엇이 있는지에 대해 조사하고, 각각의 연구 결과를 분석하여 MTD 전략을 활용한 연구 결과에 있어 전체적인 IoT 환경에서 무엇을 대상으로 연구가 진행되었는지를 파악하고 설명한다. MTD 전략에 관한 연구는 국내외적으로 활발히 진행되고 있는 상황이다. 국내에서 발표된 MTD 전략 연구 결과로는 총 3개의 연구 결과를 조사하였으며, 국외에서 발표된 MTD 전략 연구 결과로는 총 7개의 연구 결과를 조사하였다.

<표 2> 국내외 MTD 전략 활용 연구 조사 및 분석

분류	참고문헌	연구 내용	적용 대상
국내	(문서연, 2018)	APT 공격으로부터 공격받을 수 있는 시스템 환경 요소를 도출하여 APT(Advanced Persistent Threat) 공격의 연속성을 차단함.	SW 시스템 환경 요소
	(임성민, 이민우, 임재성, 2019)	드론 식별을 위한 해시값 노출 위험을 감소하기 위해 PHT(Preposition Hash Table)을 사용한 MTD 메커니즘을 제안함.	네트워크 패킷 내 Hash Key
	(박태근, 박경민, 문대성, 2019)	HTN(Hidden Tunnel Networking)이라는 네트워크 기반 MTD 전략에 따라 IP 주소와 포트 번호를 변경하는 메커니즘 제안함.	네트워크 IP 주소 및 포트 번호
국외	(Jin B. Hong et al., 2017)	셔플링 기반의 온라인 MTD를 이용한 SDN 네트워크 토폴로지 분석을 통해 최적의 네트워크 구성 방안을 제안함.	네트워크 토폴로지
	(J. Narantuya et al., 2019)	SDN(Software-Defined Network) 기반 네트워크 환경에서 다수의 SDN 컨트롤러를 사용하여 IP 주소를 셔플링함.	네트워크 IP 주소
	(Samuel Woo et al., 2019)	NAS(Network Address Shuffling)를 사용하여 차량 내 네트워크를 보호하기 위해 CAN ID를 셔플링함.	CAN 네트워크 ID
	(R. Brown et al., 2020)	난수화 시드를 사용하여 ECU ID를 무작위로 생성하는 새로운 CAN 버스 프로토콜을 제안함.	ECU ID
	(Jun-Gyu Park et al., 2020)	네트워크 프로토콜 변형 패턴을 사용하여 패턴을 알고 있는 사용자만 서버에 액세스할 수 있는 메커니즘을 제안함.	네트워크 프로토콜
	(Seunghyun Yoon et al., 2020)	보호 대상 호스트 시스템의 공격 그래프를 기반으로 네트워크 구성 요소(예를 들어 MAC 주소, IP 주소, 포트 번호)을 셔플링하는 메커니즘을 제안함.	네트워크 구성 요소
	(B. Groza et al., 2021)	자율주행 차량 내부의 CAN 버스 회로에 스위치를 구성하여 인증된 CAN 네트워크 패킷만 전송될 수 있도록 하는 메커니즘을 제안함.	HW 회로 기판

현재 MTD 전략 연구는 SW를 기반으로 보호 기술을 구현하고 있으며, 주로 네트워크 계층에 존재하는 시스템을 보호하기 위한 연구가 많이 진행되고 있다. 대표적인 공격 표면으로는 IP 주소, Port 번호, MAC 주소가 도출되어 있는 것을 확인할 수 있다. 또한 네트워크 토폴로지, 패킷 ID, 네트워크 프로토콜에 변화를 주는 연구 결과도 확인할 수 있다.

SW 기반 기술 외에 HW 기반 기술 또한 연구가 진행되고 있는 것을 확인하였다. 대표적으로는 자율주행 차량 내부에 위치한 CAN 통신 버스 회로를 스위치로 재구성하여 악의적인 CAN 네트워크 트래픽을 우회시켜 시스템에 피해를 줄 수 없도록 하는 연구 결과이다.

4. IoT 장치 보호를 위한 소프트웨어 정의 MTD 연구 방향성 도출 방안

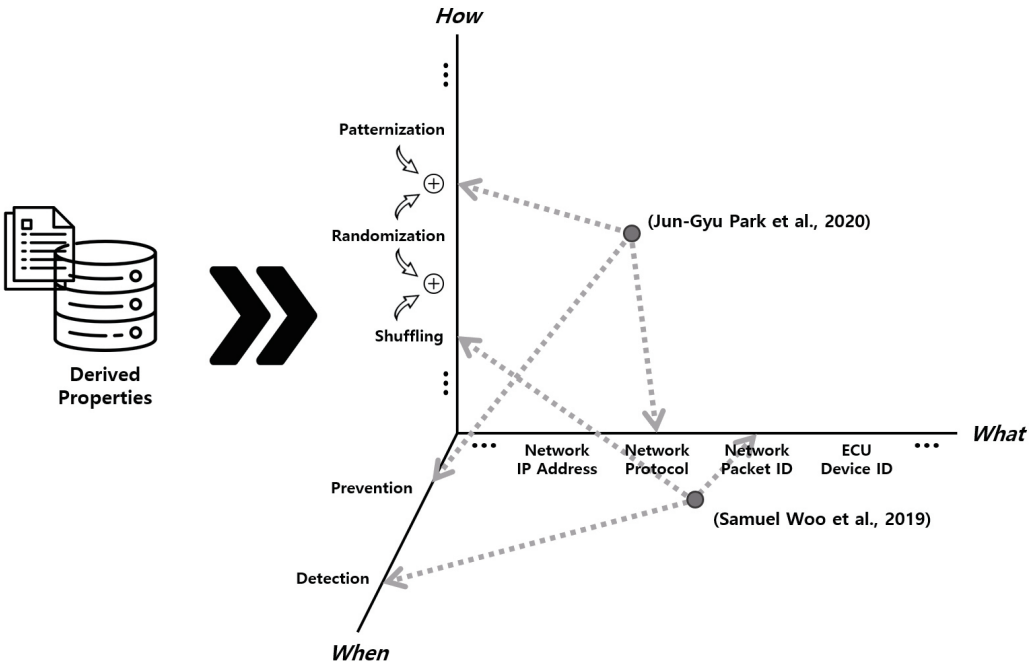
본 장에서는 3장에서 분석한 최근의 MTD 전략 연구 조사 결과 내용을 바탕으로 MTD 전략의 세 가지 핵심적인 관점(When to move, What to move, How to move)의 다양한 속성들을 도출하고, 조사한 연구 결과가 어떠한 속성들을 지니고 있는지를 편리하게 확인할 수 있도록 시각화하여 표현한다. 또한 도출된 속성의 다양한 조합을 바탕으로 새로운 소프트웨어 정의 MTD 전략 연구를 수행함에 있어 하나의 지표로 활용할 수 있는 연구 방향성을 도출하는 방안에 대해 제안한다.

연구 방향성 도출 방안을 제안하기 위해 사전에 도출된 다양한 속성들은 <표 3>과 같다. 첫 번째로 "When to move" 관점에서는 총 2개의 속성을 도출하였으며, 사전 예방(Prevention)의 경우와 공격 감지(Detection)의 경우로 분류되었다. 두 번째로 "What to move" 관점에서는 총 10개의 속성을 도출하였으며, 네트워크 IP 주소(Network IP Address), 네트워크 포트 번호(Network Port Number), 네트워크 MAC 주소(Network MAC Address), 네트워크 프로토콜(Network Protocol), 네트워크 패킷 ID(Network Packet ID), 네트워크 토폴로지(Network Topology), 네트워크 패킷 내 Hash Key(Hash Key in Network Packet), ECU 장치 ID(ECU Device ID), 회로 보드(Circuit Board), 시스템 환경 요소(System Environment Elements)로 분류되었다. 마지막으로 "How to move" 관점에서는 총 6개의 속성을 도출하였으며, 미끼(Decoy), 변이(Variation), 셔플링(Shuffling), 난수화(Randomization), 패턴화(Patternization), HW 스위치로 분류되었다.

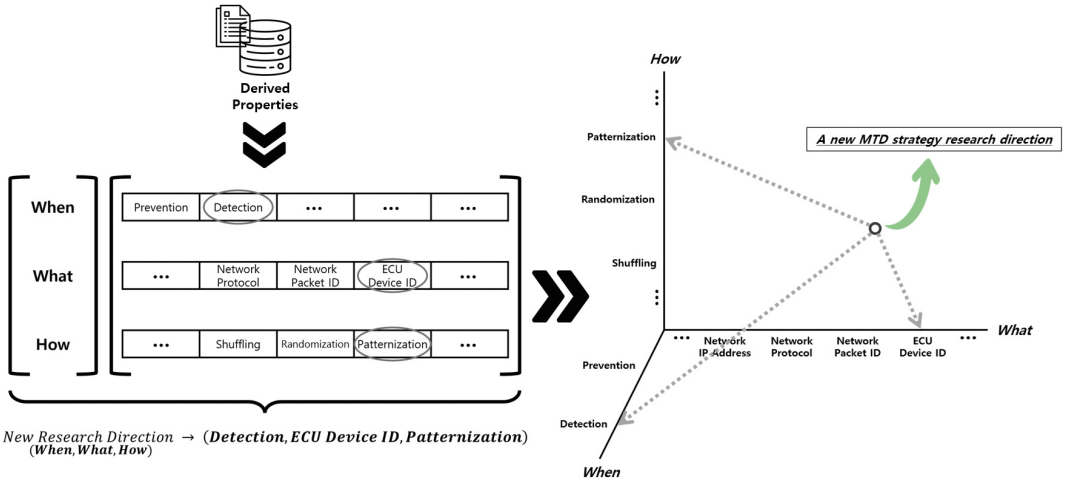
<표 3> MTD 전략의 세 가지 핵심적인 관점에서의 도출된 속성들

분류	도출된 속성들
When to move	Prevention, Detection
What to move	Network IP Address, Network Port Number, Network MAC Address, Network Protocol, Network Packet ID, Network Topology, Hash Key in Network Packet, ECU Device ID, Circuit Board, System Environment Elements
How to move	Decoy, Variation, Shuffling, Randomization, Patternization, HW Switch

도출된 속성들을 토대로 3장에서 조사한 연구 결과의 일부가 어떠한 속성들을 지니고 있는지를 시각적으로 표현한 것은 <그림 2>와 같다. 본 시각화 예시에서는 MTD 전략 연구 조사 결과 중 두 개의 연구 결과가 어떠한 속성들의 조합으로 표현이 될 수 있는지를 보여주며, MTD 전략에서 세 가지 관점의 속성 조합으로 하나의 연구 결과가 나타나는 것을 확인할 수 있다.



<그림 2> 최근 MTD 전략 연구 결과의 시각화



<그림 3> 새로운 소프트웨어 정의 MTD 연구 방향성 도출 방안

도출된 다양한 속성들의 조합으로 새로운 소프트웨어 정의 MTD 연구에 있어 하나의 지표로 활용할 수 있는 연구 방향성을 도출하는 방안은 <그림 3>과 같다. ($When$, $What$, How)와 같이 MTD 전략의 세 가지 관점의 속성 키 쌍으로 표현할 수 있음을 보여주며, 새롭게 나타난 연구 방향성이 어떠한 속성들을 가리키고 있는지를 시각화 표현으로 확인할 수 있다. 본 예시에서는 “When to move” 관점의 공격 감지(Detection), “What to move” 관점의 ECU 장치 ID(ECU Device ID), “How to move” 관점의 패턴화(Patternization) 속성 키 조합으로 하나의 새로운 연구 방향성을 도출할 수 있는 방안을 보여준다.

5. 결론

MTD 전략은 사이버 위협이 될 수 있는 중요 시스템의 구성 요소(또는 공격 목표 대상이 될 수 있는 공격 표면)를 능동적으로 그리고 지속적으로 변화시키고 기존의 시스템 동작 변경을 최소화하여 안전하게 보호할 수 있는 전략 중 하나이다. 이 전략은 공격자를 교란시키기 위해 중요 시스템의 정확한 구성을 파악할 수 없도록 난독화시키는 장점이 존재한다. 하지만 최적의 전략 구사가 없는 MTD 전략의 활용은 오히려 보호 대상 시스템의 전체적인 구성에 있어 하나의 큰 오버헤드로 적용될 수 있는 단점

이 존재한다. 이를 해결하기 위해서는 최적의 전략을 바탕으로 비용 대비 효율적인 시스템 보호 알고리즘을 구성하는 방안이 필요한 상황이다.

본 논문에서는 최근 MTD 전략 연구 결과들에 대해 조사하고 분석하여 MTD 전략의 세 가지 핵심적인 관점에 있어 어떠한 속성들이 존재하는지를 도출하였다. 이후 도출된 각 속성들의 조합으로 각각의 연구 결과가 어떠한 보호 알고리즘 전략으로 구성되었는지를 쉽게 파악할 수 있도록 하나의 그래프 및 3가지 속성 배열로 표현하고, 도출된 다양한 속성들의 조합으로 새로운 소프트웨어 정의 MTD를 연구함에 있어 하나의 연구 방향성을 도출할 수 있는 방안을 제안한다. 제안된 방안은 MTD 전략을 활용하고자 하는 다양한 연구 분야에 있어 최적의 전략 보호 알고리즘을 구사할 수 있는 하나의 지표로서 활용이 가능하다. 향후 본 논문에서 제안한 방안을 토대로 새로운 소프트웨어 정의 MTD 보호 기술을 연구함에 있어 베스트 프렉티스로 활용할 수 있는 전략 구성 프레임워크를 개발하고자 한다.

참고문헌

김정녀, 진승헌 (2017). 초연결 환경에서 보안위협 대응을 위한 사물인터넷(IoT) 보안 기술 연구. 한국통신학회지(정보와통신), 34(3), 57-64.

금융보안원 (2016). 사물인터넷(Internet of Things) 보안위협 및 사고사례. 서울: 금융보안원.

임성민, 이민우, 임재성 (2019). 드론 네트워크 보안을 위한 해시표 대체 방식의 능동 방어 기법. 한국정보통신학회논문지, 23(4), 477-485.

박태근, 박경민, 문대성 (2019). Attack Surface Expansion through Decoy Trap for Protected Servers in Moving Target Defense. 한국컴퓨터정보학회논문지, 24(10), 25-32.

문서연 (2018). 지능형 지속 위협 보안을 위한 공격목표 교란기술 모델에 관한 연구. 한국통신학회 학술대회논문집, 598-599.

Mardiana Binti Mohamad Noor & Wan Haslina Hassan (2019). Current research on Internet of Things (IoT) security: A Survey. Computer Networks, 148, 283-294.

M. Antonakakis, T. April, M. Bailey, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, J. A. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Zane Ma, J. Mason, D. Menscher, C. Seaman, N. Sullivan, K. Thomas & Yi Zhou (2017). Understanding the Mirai Botnet. Proceedings of the 26th USENIX Security Symposium, USENIX.

Jin-Hee Cho, Dilli P. Sharma, Hooman Alavizadeh, Seunghyun Yoon, Noam Ben-Asher, Terrence J. Moore, Dong Seong Kim, Hyuk Lim & Frederica F. Nelson (2020). Toward Proactive, Adaptive Defense: A Survey on Moving Target Defense. IEEE Communications Surveys & Tutorials, 22(1), 709-745.

Renzo E. Navas, F. Cuppens, N. B. Cuppens, L. Toutain & Georgios Z. Papadopoulos (2021). MTD, Where Art Thou? A Systematic Review of Moving Target Defense Techniques for IoT. IEEE Internet of Things Journal, 8(10), 7818-7832.

V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal & B. Sikdar (2019). A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures. IEEE Access, 7, 82721-82743.

Jun-Gyu Park, Yangjae Lee, Ki-Wan Kang, Sang-Hoon Lee & Ki-Woong Park (2020). Ghost-MTD: Moving Target Defense via Protocol Mutation for Mission-Critical Cloud Systems. Energies, 13(8).

Seunghyun Yoon, Jin-Hee Cho, Dong Seong Kim, Terrence J. Moore, Frederica Free-Nelson & Hyuk Lim (2020). Attack Graph-Based Moving Target Defense in Software-Defined Networks. IEEE Transactions on Network and Service Management, 17(3), 1653-1668.

Samuel Woo, Daesung Moon, Taek-Young Youn, Yousik Lee & Yongeun Kim (2019). CAN ID Shuffling Technique (CIST): Moving Target Defense Strategy for Protecting In-Vehicle CAN. IEEE Access, 7, 15521-15536.

B. Groza, L. Popa, Pal-Stefan Murvay, Y. Elovici & A. Shabtai (2021). CANARY - a reactive defense mechanism for Controller Area Networks based on Active RelaYs. Proceedings of the 30th USENIX Security Symposium, USENIX.

J. Narantuya, Seunghyun Yoon, Hyuk Lim, Jin-Hee Cho, Dong Seong Kim, T. J. Moore & F. F. Nelson (2019). SDN-based IP Shuffling Moving Target Defense with Multiple SDN Controllers. 2019 IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S), 15-16.

Jin B. Hong, Seunghyun Yoon, Hyuk Lim & Dong Seong Kim (2017). Optimal Network Reconfiguration for Software Defined Networks Using Shuffle-Based Online MTD. 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), 234-243.

R. Brown, A. Marti, C. Jenkins & S. Shannigrahi (2020). Dynamic Address Validation Array (DAVA): A Moving Target Defense Protocol for CAN bus. Proceedings of the 7th ACM Workshop on Moving Target Defense, 11-19.

국한문 참고문헌의 영문 표기

(English translation / Romanization of reference originally written in Korean)

Jeong-Nyeo Kim, Seung-Hun Jin (2017). A Study on Internet of Things Security Technique to respond the Security Threats in Hyper-Connected Environment. The Journal of The Korean Institute of Communication Sciences, 34(3), 57-64.

FSI (Financial Security Institute) (2016). Internet of Things Security Threats and Incidents. Seoul: FSI (Financial Security Institute).

Sungmin Leem, Minwoo Lee & Jaesung Lim (2019). MTD (Moving Target Defense) with Preposition Hash Table for Security of Drone Network. Journal of the Korea Institute of Information and Communication Engineering, 23(4), 477-485.

Tae-Keun Park, Kyung-Min Park & Dae-Sung Moon (2019). Attack Surface Expansion through Decoy Trap for Protected Servers in Moving Target Defense. Journal of The Korea Society of Computer and Information, 24(10), 25-32.

Moon Seo Yeon (2018). A Study on the Moving Target Defense Model for Advanced Persistent Threat Security. Proceedings of Symposium of the Korean Institute of Communications and Information Sciences, 598-599.