JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 8, pp. 31-37, August 2020
https://doi.org/10.9708/jksci.2020.25.08.031

Research on System Architecture and Methodology based on MITRE ATT&CK for Experiment Analysis on Cyber Warfare Simulation

Myung Kil Ahn*, Jung-Ryun Lee*

*Student, School of Electrical and Electronics Engineering, Chung-Ang University, Seoul, Korea
*Professor, School of Electrical and Electronics Engineering, Chung-Ang University, Seoul, Korea

[Abstract]

In this paper, we propose a system architecture and methodology based on cyber kill chain and MITRE ATT&CK for experiment analysis on cyber warfare simulation. Threat analysis is possible by applying various attacks that have actually occurred with continuous updates to reflect newly emerging attacks. In terms of cyber attack and defense, the current system(AS-IS) and the new system(TO-BE) are analyzed for effectiveness and quantitative results are presented. It can be used to establish proactive cyber COA(Course of Action) strategy, and also for strategic decision making. Through a case study, we presented the usability of the system architecture and methodology proposed in this paper. The proposed method will contribute to strengthening cyber warfare capabilities by increasing the level of technology for cyber warfare experiments.

▸ **Key words**: Cyber Warfare Simulation, Cyber Modeling&Simulation, Cyber Course of Action, System Risk Analysis, Cyber Attack Modeling

[요 약]

본 논문에서는 사이버 전투실험 분석이 가능한 사이버 킬체인 및 MITRE ATT&CK 기반의 시스템 구성 및 분석 방법론을 제안한다. 사이버 킬체인을 기반으로 공격 과정을 모의하고, MITRE ATT&CK를 기반으로 공격 목적 및 구체적인 공격 방법을 적용하여, 실제 발생한 다양한 공격 및 새롭게 등장할 공격에 대한 시스템 위협 분석이 가능하도록 한다. 또한, 현 시스템(AS-IS)과 새로운 대응 시스템이 적용될 경우(TO-BE)에 대한 사이버 공격 및 대응 측면의 효과도 분석을 정량적으로 제시하여, 선제적 방어방책 및 소요 반영을 위한 의사결정에도 활용이 가능하다. 제안하는 시스템 및 방법론의 활용성을 제시하기 위해, 테스트베드 환경에서 프로토타입을 구축하고 사례 연구를 수행하였다. 제안된 방안은 사이버 전투실험의 기술 수준을 높여 사이버전 역량 강화에 기여할 것으로 기대한다.

▸ **주제어**: 사이버전 시뮬레이션, 사이버 전투실험, 사이버 모델링&시뮬레이션, 시스템 위협 분석, 사이버 공격 모델링

• First Author: Myung Kil Ahn, Corresponding Author: Jung-Ryun Lee
*Myung Kil Ahn (lovedew@cau.ac.kr), School of Electrical and Electronics Engineering, Chung-Ang University
*Jung-Ryun Lee (jrlee@cau.ac.kr), School of Electrical and Electronics Engineering, Chung-Ang University
• Received: 2020. 07. 20, Revised: 2020. 08. 10, Accepted: 2020. 08. 10.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

전투실험은 전투발전분야에 운용개념이나 요구성능에 부합하는 새로운 기술이나 시스템을 적용하기 위한 대안들을 도출하는 과정으로, 다 요소 의사결정법과 M&S (Modeling and Simulation) 방법들이 활용될 수 있다[1]. 사이버전 분야도 새로운 소요 도출 및 분석을 위해 전투실험을 활용한 접근이 필요하다.

사이버전을 대비해 공격을 탐지하고 방어하기 위한 많은 노력을 기울이고 있음에도 불구하고, 사이버 공격은 계속 증가하고 있으며, 고도화된 새로운 유형이 지속적으로 출현하고 있다[2][3].

이러한 위협에 선제적으로 대응하기 위해, 사이버 공격이 시스템 및 네트워크에 미칠 수 있는 피해를 사전에 분석하고 대비할 수 있는 능력이 필요하다. 하지만, 실제 운용하고 있는 시스템 및 네트워크에서 이를 수행하는 것은 많은 제약이 따르므로, 평상 시 끊임없이 분석할 수 있는 환경이 필요하다. 이에 대한 환경 구성은 디지털 트윈[4]과 유사한 시스템 트윈의 개념으로 물리적 시스템 및 네트워크에 대한 쌍둥이 환경을 만들고, 현실에서 발생할 수 있는 동작 및 상황을 시뮬레이션하는 가상의 모델로 정의할 수 있다. 사이버 위협 분석을 위해서는 사이버 모의 요소를 기반으로 대규모 시스템 및 네트워크의 피해 분석이 가능한 M&S 환경으로 구축할 수 있다[5][6]. 하지만, 특정 공격 유형의 분석으로 제한될 수 있다.

또한, 사이버 위협에 대비하여 새로운 대응 시스템 및 방어방책도 지속적으로 개발되어 적용되고 있다. 하지만, 새로운 대응 시스템이 얼마나 효과적인지 어디에 배치해야 최적인지에 대해, 현재는 전문가 및 정성적인 방법에 의존하고 있는 실정이다.

이러한 문제를 해결하기 위해, 본 논문에서는 사이버 전투실험 분석이 가능한 시스템 구성 및 분석 방법론을 제안한다. 사이버 킬체인[7][8] 및 MITRE ATT&CK[9] 기반으로 실제 발생한 다양한 공격을 적용하여 시스템의 위협에 대한 분석이 가능하도록 하고, 현 시스템(AS-IS)과 새로운 대응 시스템이 적용될 경우(TO-BE)에 대한 사이버 공격 및 대응 측면의 효과도 분석을 정량적으로 제시하여, 선제적으로 방어방책을 수립하는데 활용할 수 있도록 한다.

본 논문의 구성은 다음과 같다. II장에서는 시스템 소요 분석 방법 현황 및 사이버 모의 공격 시뮬레이션 관련 기술을 살펴보고, III장에서는 제안하는 시스템 구성 및 방법론을 기술한다. IV장에서는 실제 테스트베드 환경에서 프로토타입을 구축하고, 사례 연구를 통해 제안하는 시스템 및 방법론의 활용성을 입증한다. V장에서는 향후 연구에 대해 기술하고 결론을 맺는다.

II. Preliminaries

1. Related Works

1.1 Analysis Methodology

사이버 위협에 대비한 새로운 대응 시스템 및 방어방책의 효과평가를 위해 다양한 방법들이 활용될 수 있으며, 델파이 기법 및 계층분석방법(AHP, Analytic Hierarchy Process)과 같은 다 요소 의사결정법과 M&S기법이 대표적이다[1].

델파이 기법[10]은 전문가의 직관을 객관화하여 미래를 예측하는 기법으로 미래의 대안 탐색에 활용될 수 있다. 수차례에 걸친 전문가들의 의견조사를 통해 합의된 내용을 얻는 정성적인 방법이다. 하지만 현재와 신규 사이버 시스템의 비교 방법으로는 제한된다.

계층분석방법[10]은 평가 기준이 다수인 상황에서 대안들의 상대적인 중요도를 체계적으로 점수화하는 다 기준 의사결정 방법이다. 전문가가 참여하고 다양한 평가 기준을 적용하여, 여러 측면에서 소요 대안 별 비교 평가가 가능한 정성적인 방법론이다. 하지만, 신규 사이버 시스템 적용에 따른 효과를 객관적으로 예측하기에는 어려움이 있다.

M&S기법은 사이버 모의 요소를 기반으로 시간의 흐름에 따른 사이버전의 효과를 객관적이고 정량적으로 분석할 수 있는 방법이다. 사이버 공격에 따른 피해분석이 가능하고, 새로운 대응 시스템 및 방어방책의 효과를 측정할 수 있는 모델 및 도구의 개발이 필요하다.

[5]에서는 사이버 공격에 대비하여 위험을 평가하고 네트워크의 탄력성을 향상시키는 사이버 방어 시뮬레이션 툴킷을 제공한다. 하지만, 시뮬레이션을 기반으로 사이버 공격들을 모의할 때, 복잡한 사이버 공격 시나리오를 단계적으로 설정하고 적용하는 것에 어려움이 있으며, 특정 CVE(Common Vulnerability Enumeration)[11] 취약점을 활용한 공격으로 국한되는 단점이 있다.

[6]에서는 사이버 전투실험에 대한 가능성을 제시하였으며, 대표적인 침해지표 규약인 IODEF (Incident Object Description and Exchange Format)[12]를 활용하여 사이버 위협을 모의하였다. 특히, Impact Type을 기반으로 공격이 시스템 및 네트워크에 미치는 피해 영향을 모델링하였으나, 공격자의 상세한 공격 목적 및 방법을 모델링하는데 제한이 될 수 있다.

[13]에서는 공격 그래프 기반의 보안 평가 프레임워크를

제안하였다. 공격 그래프 생성 및 실시간 이벤트 분석 기능을 제공하고, 공격 그래프 분석을 통해 영향 평가를 수행한다. 또한, Cauldron[14]은 공격 그래프의 구성 및 분석 내용을 제공하고, 원시 보안 데이터를 공격 그래프로 변환하여 취약점이 전체 네트워크 보안에 미치는 영향을 제시해준다. 이러한 공격 그래프 접근 방법은 사이버 공격을 모델링하기 위한 가장 전통적인 접근 방법 중 하나이다[15]. 공격 그래프 기술은 공격자가 공격할 수 있는 모든 경로를 식별하고 찾아내기 위한 기술이지만, 사이버 전투실험에서 요구되는 공격자의 다양한 공격 과정 및 목적, 방법 등으로 활용하기에는 한계가 있다.

취약점 점검 신기술의 하나인 침입 및 공격 시뮬레이션인 BAS(Breach and Attack Simulation) 기술을 활용한 솔루션들이 소개되고 있다[16][17]. 방어 측면보다는 공격자 관점에서 보안 인프라를 공격 시뮬레이션하는 것에 초점이 맞춰져 있으며, 일관성있고 반복적으로 공격을 자동화하는데 목적이 있다.

1.2 Cyber Kill Chain based ATT&CK Framework

사이버 전투실험을 수행하기 위해서는, 공격자의 관점에서 시나리오를 기반으로 다양한 사이버 공격을 실행시키는 사이버 모의 공격 시뮬레이션이 필수적이다. 공격 과정을 모델링하기 위해 사이버 킬체인 기술과 공격 목적 및 방법을 모델링하기 위해 MITRE에서 제공하는 ATT&CK 프레임워크가 활용될 수 있다.

사이버 킬체인[7]은 기존의 군사적 용어인 킬체인에서 유래한 것으로, 킬체인은 표적을 탐지하고 파괴하기까지의 연속적인 처리 과정을 의미한다. 사이버 킬체인 모델링은 수 년 동안 미 국방부의 사이버 방어 및 전투 분야에서 활용되어 왔다. 사이버 공격은 연속된 단계로 구성되어 있으며, 방어자가 중간에 한 단계만 차단해도, 공격자가 다음 단계로 진행할 수 없다는 개념이다. 사이버 킬체인은 록히드 마틴 社의 cyber kill chain 모델을 시작으로 미 국방부의 cybersecurity kill chain 모델, 가트너 社의 Attack Chain Model 등 다양한 모델이 제안되고 있다. 특히, 록히트 마틴 社 는 정찰(Reconnaissance), 공격코드 제작(Weaponization), 전달(Delivery), 취약점 공격(Exploitation), 설치(Installation), 명령 및 제어(Command &Control), 목적시스템 장악(Actions on Objectives)의 7단계로 구성된 Cyber kill chain 모델을 제안하였다[8].

미국의 비영리기관인 MITRE에서 제공하는 ATT&CK [9] 프레임워크는 Adversarial Tactics, Techniques, and Common knowledge로서, 실제 발생한 사이버 공격 사례를 기반으로 하며, 적의 공격 라이프 사이클을 반영한 사이버 공격자의 행위 모델이다. 매트릭스 형태로 제시되며, Tactics은 적의 공격 목적에 해당하고, 공격 목적을 달성하기 위한 구체적인 방법으로 Techniques을 제시한다.

ATT&CK 서비스는 종단에서 공격을 탐지하고 대응하는 제품들을 평가하는 기술에 활용될 수 있다. 각 종단 보안 제품군이 각 기법들에 대해 어떻게 대응하는지 확인을 통해, 제품들에 대한 객관적인 평가가 가능하다. 종단 위협 탐지 및 대응을 위한 EDR(Endpoint Detection and Response) 솔루션의 경우 초기에는 발생하는 이슈들을 최대한 수집하고 분류하여 탐지하는데 초점이 맞춰져 있었으나, ATT&CK를 적극적으로 활용하여 각 공격기법에 대응하는데 주력하고 있다.

ATT&CK는 지식 베이스(knowledge base)를 기반으로 하며, 새로운 공격 목적 및 방법을 반영하여 지속적으로 업데이트되고 있다.

III. The Proposed Scheme

본 연구에서는 사이버 전투실험 분석을 위한 사이버 킬체인 및 MITRE ATT&CK 기반의 시스템 구성 방안과 새로운 대응시스템 및 방어방책의 효과분석 방법론을 제시한다.

1. System Configuration

사이버 전투실험 분석을 위해, 네트워크 구성 정보를 활용하여 시스템과 네트워크 모델을 배치한다. 사이버 킬체인 및 MITRE ATT&CK 정보를 활용하여 사이버 모의 공격을 구성하고, 사이버 대응 및 방어 정책을 활용하여 대응 및 방어 시스템을 구성한다. 사이버 모의 공격 시뮬레이션이 진행되면서, 공격의 성공 여부가 판단되고, 공격의 성공 여부에 따른 효과분석이 수행된다. 사이버 전투실험이 종료되면 공격과 방어 측면의 분석지표가 제시된다. 사이버 대응 및 방어 능력 분석 결과에 따라, 현재 시스템에 대한 분석 및 신규 시스템 소요와의 비교 분석이 가능하다. 시스템의 운영 개념은 그림 1과 같으며, 신규 소요 반영 여부를 위한 결정에 활용이 가능하다.

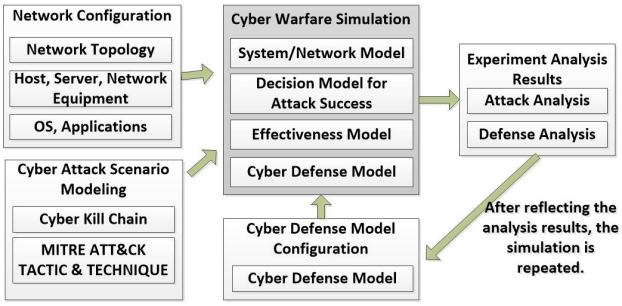

Fig. 1. Concept of operation

2. Cyber Attack Modeling

사이버 전투실험 분석을 위한 모의공격은 사이버 킬체인 기반 ATT&CK를 활용하여, 공격 단계 별 다양한 공격 목적 및 세부 공격 방법에 따라 시뮬레이션을 수행한다. 모든 공격이 사이버 킬체인 7단계를 전부 수행하지는 않지만, 부분적으로 대입해 활용할 수 있다.

예를 들어, 사이버 킬체인의 유포(Delivery) 단계에서 타겟에 악성코드를 전달하기 위해, ATT&CK의 Initial Access Tactic의 Drive-by Compromise(T1189) Technique을 활용할 수 있다. 그림 2와 같은 과정으로 수행하며, 공격자가 특정 노드(WebServer)를 공격하여 권한을 탈취하였을 때, 해당하는 노드에 접근하는 사용자(Victim)는 권한이 탈취된 노드로부터 악성정보를 받아서, 해당 위협이 실행되는 형태로 모의한다.

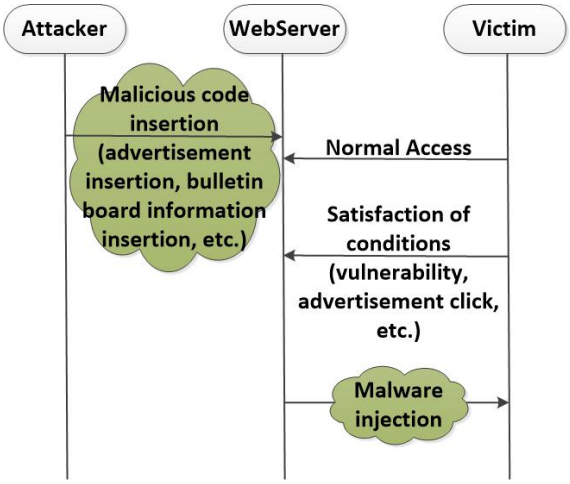

Fig. 2. Flow of Drive-by Compromise Technique

사이버 킬체인 단계 별 공격 과정을 모의하고, 각 공격 과정에서 ATT&CK을 활용하여 공격 목적 및 방법을 모의한다. 또한, 새롭게 출현하는 공격 목적과 방법도 지속적으로 업데이트가 가능하다.

3. Cyber Defense Modeling

사이버 대응 및 방어 정책을 활용하여, 다양한 대응 및 방어 시스템을 구성할 수 있다. 대표적인 네트워크와 단말 장비로 그림 3과 같이 모델링할 수 있다.

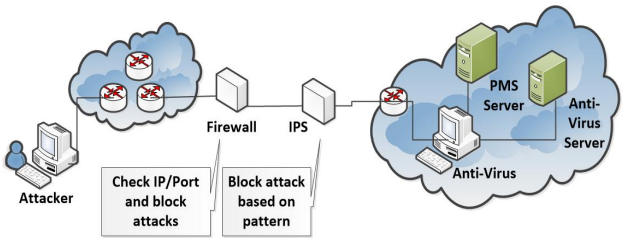

Fig. 3. Cyber Defense Models

Firewall 모델은 정책 기반의 네트워크 방어와 프로토콜 동작 기반의 네트워크 방어로 모델링된다. IPS (Intrusion Protection System) 모델은 트래픽 패턴 기반으로 네트워크를 방어하는 기능과 패킷 패턴 기반으로 네트워크 방어를 수행하는 기능으로 모델링된다. 안티바이러스 서버는 패치 관리 기능을 수행하고, 클라이언트는 공격이 유입되는 경우 방어 기능을 수행하며, 감염이 이루어진 상태의 경우 치료 기능을 수행한다. PMS(Patch Management System) 서버 모델은 패치 관리 기능을 수행하고, 클라이언트 모델은 패치 요청 및 수행 기능을 제공하도록 모델링한다.

새로운 대응 시스템 및 방어방책을 모델링하여, 효과성 입증을 통한 신규 소요 반영 및 최적 배치에 활용할 수 있다.

4. Cyber Effectiveness Analysis

사이버 공격이 전개되면서, 사이버 대응 및 방어 장비에 의해 공격이 중단되기도 하고, 정책 미비로 공격이 계속 진행되기도 한다. 또한, 단말의 취약점으로 인해 공격자가 호스트를 점유하기도 하고, 공격이 실패할 수도 있다. 이에 따른 사이버 공격과 방어, 네트워크 측면에서 다양한 효과 지표들을 산출하고 전투실험 분석이 가능하다. 대표적인 지표는 표 1과 같다.

사이버 공격 측면에서는 공격 성공률과 호스트 감염률 지표로 정의할 수 있고, 사이버 방어 측면에서는 방어 성공률 지표로 정의할 수 있다. 또한, 네트워크 측면에서는 정보의 적시성 및 전송 실패율 지표 등으로 정리할 수 있다.

Table 1. Key Cyber Effectiveness Index

Index	Formula
Attack Success Ratio	(Number of successful attacks) / (Total number of attacks) X 100
Host Infection Ratio	(Number of infected hosts) / (Number of target hosts) X 100
Defense Success Ratio	(Number of blocked attacks) / (Total number of attacks) X 100
IER Success Ratio	(Number of success count) / (Total number of information exchange requests) X 100
IER Failure Ratio	(Number of failure count) / (Total number of information exchange requests) X 100

특히, IER (Information Exchange Requirement)은 군에서 임무 및 작전 수행을 위해 필요한 정보교환요구소요이며, 제안하는 시스템을 통해 적시성 충족 여부를 분석하는 전투실험이 가능하다. 본 시스템을 통해 새로운 대응 시스템 및 방어방책의 효과를 정량적으로 분석할 수 있으며, 가장 효과적인 최적의 배치 위치를 결정하기 위한 실험에도 활용이 가능하다.

IV. Experiment

사이버 전투실험 분석을 위해 테스트베드 환경에서 프로토타입을 구축하고 사례 연구를 통해, 제안하는 시스템 및 방법론의 활용성을 제시하고자 한다.

사이버 모의 요소를 기반으로 시간의 흐름에 따른 사이버전의 효과를 객관적이고 정량적으로 분석하기 위해, M&S기반으로 시스템을 구축하였다. Riverbed Modeler 이산사건 시뮬레이션(DES, Discrete Event Simulation) 엔진을 기반으로 프로토타입을 구축하였으며, 시스템 및 네트워크 장비, 사이버 대응 및 방어 장비를 모델링하여 배치하였다.

공격자(Attacker) 단말, BotNet 생성을 위한 피해 서버인 웹서버(Webhard Sever), 최종 DDoS(Distributed Denial of Service) 공격 대상인 타겟 서버(Target Server)로 구성된다. 또한, 웹서버에 접속 후 감염되어 BotNet으로 활용되는 단말들, IER을 통해 주요 정보를 주고받는 단말, 라우터, 스위치, 방어 장비들로 구성되어 있다. 네트워크 토폴로지는 그림 4와 같다.

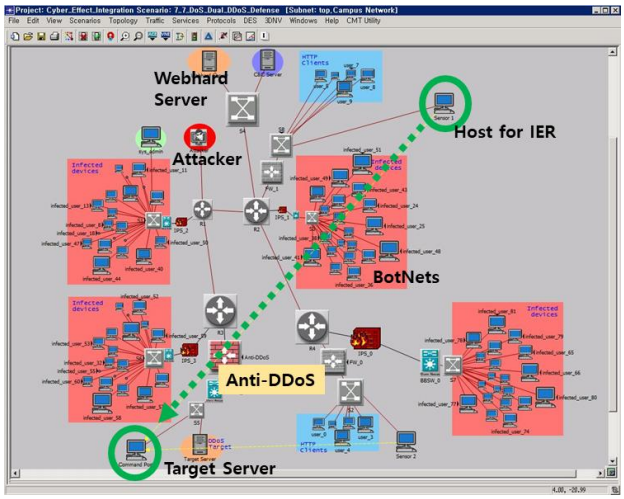

Fig. 4. Network Topology

분석 실험은 새로운 대응 시스템인 Anti-DDoS 배치의 효과성을 분석하기 위해, 현 시스템(AS-IS)과 새로운 대응 시스템이 적용될 경우(TO-BE)에 대한 사이버 공격 및 대응 측면의 전투실험을 수행한다.

상세한 사이버 공격 절차는 그림 5와 같다.

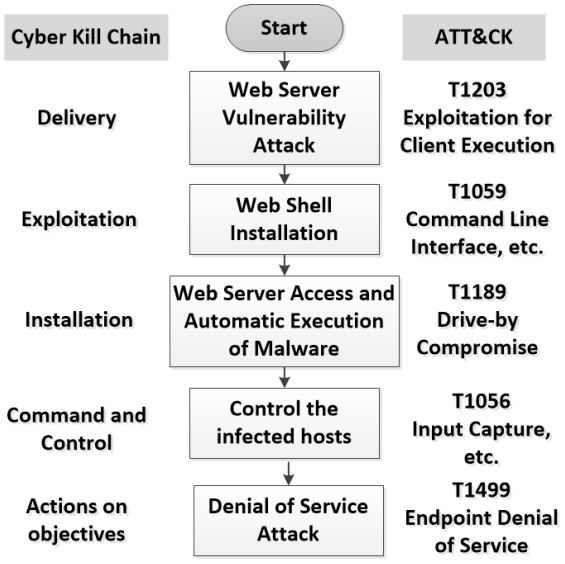

Fig. 5. Attack Scenario

공격자는 웹서버(Webhard Server)에 CVE 2012-1823 취약점 공격을 이용하여 웹서버를 탈취한다. Web Shell을 웹서버에 업로드하고 원격으로 명령을 수행할 수 있도록 한다. 다수의 사용자들이 웹서버에 접속하는 것만으로도 악성코드가 자동 실행된다. DarkComet 악성코드가 자동 실행되며, 공격자는 악성코드에 감염된 컴퓨터를 조종할 수 있게 된다. 악성코드는 감염자의 컴퓨터에 잠입하여 공격자의 명령을 기다리고, 명령에 의해 타겟서버(Target

Server)로 DoS(Denial of Service)공격을 수행하게 된다.

새로운 소요인 Anti-DDoS 시스템이 배치되지 않은 시나리오(AS-IS)와 배치되어 동작하는 시나리오(TO-BE)에 대해 전투실험을 수행하고, 그림 6과 같이 사이버 공격 성공률(Attack Success Ratio)과 IER 실패율(IER Failure Ratio)에 대한 결과를 도출하였다.

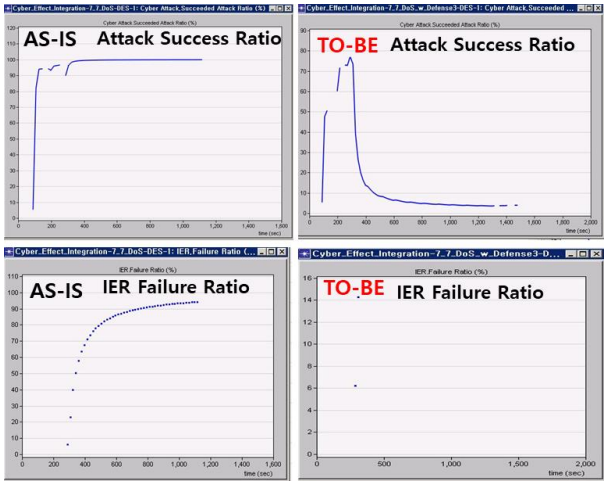

Fig. 6. Experimental analysis results

감염된 BotNet들이 타겟 서버로 DDoS 공격을 수행하는 시점에, Anti-DDoS 시스템이 배치되지 않은 시나리오(AS-IS)는 모든 DDoS 공격이 성공하게 되고, 시스템 및 네트워크의 과부하로 인해, IER의 실패율은 높아지게 된다. 반면, 새로운 소요인 Anti-DDoS 시스템이 배치된 시나리오(TO-BE)는 DDoS 공격이 새로운 대응 시스템에 의해 실패하게 되고, IER도 원활하게 송수신 된다.

본 실험을 통해 신규 소요인 Anti-DDoS 시스템에 대한 효과를 정량적으로 도출할 수 있으며, 소요 반영을 위한 의사결정에 활용할 수 있다.

V. Conclusions

본 논문에서는 사이버 전투실험 분석이 가능한 사이버 킬체인 및 MITRE ATT&CK 기반의 시스템 구성을 제안하였다. 특정 공격 및 유형으로 국한되지 않고, 실제 발생한 다양한 공격을 적용하여 위협 분석이 가능하고, 새롭게 출현하는 공격을 반영하여 업데이트가 지속될 것이다.

또한, 현 시스템(AS-IS)과 새로운 대응 시스템이 적용될 경우(TO-BE)에 대한 사이버 공격 및 대응 측면의 효과도 분석을 정량적으로 제시하여, 선제적으로 방어방책을 수립하는데 활용할 수 있도록 전투실험 분석 방법론을 제시하였다.

본 논문에서 제안한 시스템 및 방법론의 활용성을 제시하기 위해, 테스트베드 환경에서 프로토타입을 구축하고 사례 연구를 수행하였다. 새로운 시스템 및 방어방책의 효과를 정량적으로 분석할 수 있으며, 소요 반영을 위한 의사결정에도 활용이 가능하다.

현재 국방 사이버전 분야의 전투실험 활용은 미흡한 실정이며, 주로 전문가 및 정성적인 방법에 의존하고 있다. 본 논문에서 제안한 시스템 및 방법론을 활용하여, 과학적 분석 및 검증이 가능하다. 신규 사이버 대응 시스템 소요 결정 및 배치 위치, 특정 사이버 공격에 대한 피해 가능성 및 피해 정도 분석, 선제적 방어방책 수립 등의 주요 전투실험 분야에 응용될 수 있다. 이를 통해 사이버전 역량 강화에 기여할 것으로 기대한다.

향후, 사이버 공격이 주요 임무나 사이버 작전에 미치는 영향을 분석할 수 있도록, 전투실험 분석 영역을 확장하여 연구를 지속할 계획이다.

ACKNOWLEDGEMENT

This work was supported by UM17312RD3.

REFERENCES

[1] Ryu Young ki, “Systematic Analysis technique for Determining ROCs”, Kongju University Doctoral Thesis, 2011.

[2] Symantec, “2019 Internet Security Threat Report”, Volume 24, February 2019.

[3] AhnLab, “ASEC REPORT”, Vol.98, 2020.

[4] Gartner Research, “Gartner’s Top 10 Strategic Technology Trends for 2017”, October 2016.

[5] S. Hassell, P. Beraud, A. Cruz, G. Ganga, S. Martin, J. Toennies, P. Vazquez, G. Wright, D. Gomez, F. Pietryka, N. Srivastava, T. Hester, D. Hyde, and B. Mastropietro, “Evaluating network cyber resiliency methods using cyber threat, vulnerability and defense modeling and simulation,”, 2012 IEEE Military Communications Conference, pp.1-6, Orlando, FL, USA, Oct. 2012, DOI: 10.1109/MILCOM.2012.6415565.

[6] Myung Kil Ahn, and Yong Hyun Kim, “Research on System Architecture and Simulation Environment for Cyber Warrior Training”, Journal of The Korea Institute of Information Security & Cryptology, VOL.26, NO.2, pp. 533-540, Apr. 2016,

DOI:10.13089/JKIISC.2016.26.2.533.

[7] United States. Joint Chiefs of Staff, “Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace”, JP 2-01.3, 2000.

[8] E. M. Hutchins, M. J. Cloppert, and R. M. Amin, “Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains”, Leading Issues in Information Warfare & Security Research, vol. 1, p. 80, 2011.

[9] MITRE, ATT&CK, Available at *https://attack.mitre.org*.

[10] Jungyun Kwon, Soomin Han, Sangyun Choe, Hanil Jeong, “A Study on Developing Performance Evaluation System Using Delphi Technique and Analytic Hierarchy Process”, Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, Vol.6, No.9, pp. 99-110, September 2016, DOI:10.14257/AJMAHS.2016.09.40

[11] MITRE, CVE, Available at *http://cve.mitre.org/*

[12] ECSIRT, IODEF/IDMEF Solutions, Available at *http://www.ecsirt.net/service/products.html*

[13] I. Kotenko, A. Chechulin, “A Cyber Attack Modeling and Impact Assessment Framework”, Proceedings of the 5th International Conference on Cyber Conflict 2013 (CyCon 2013), pp.119–142, Tallinn, Estonia, July 2013.

[14] Jajodia, S., Noel, S., Kalapa, P., Albanese, M., Williams, J., “Cauldron: Mission-Centric Cyber Situational Awareness with Defense in Depth”, MILCOM 2011 Military Communications Conference, Baltimore, USA, Nov. 2011, DOI:10.1109/MILCOM.2011.6127490.

[15] H. Al-Mohannadi, Q. Mirza, A. Namanya, I. Awan, A. Cullen, J. Disso, "Cyber-attack modeling analysis techniques: An overview", 2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW), pp.69-76, Vienna, Austria, Aug. 2016, DOI:10.1109/W-FiCloud.2016.29

[16] AttackIQ, Available at *https://attackiq.com/*

[17] SafeBreach, Available at *https://safebreach.com/*

Authors

Myung Kil Ahn received the B.S. degree in Information and Communication Engineering from the Chungnam National University, in 1997, and M.S. degree in Computer Engineering from the Sogang University, Seoul, Korea in 2003. She is currently pursuing the Ph.D. degree in School of Electrical and Electronics Engineering, Chung-Ang University. She is currently a principal researcher at 2nd R&D institute, Agency for Defense Development, Seoul, Korea. Her research interests include computer security and cyberwarfare modeling&simulation.

Jung-Ryun Lee received the B.S. and M.S. degrees, both in mathematics from the Seoul National University, in 1995 and 1997, respectively. He received the Ph.D. degree in electrical and electronics engineering from the Korea Advanced Institute of Science and Technology (KAIST), in 2006. From 1997 to 2005, he was a chief research engineer at LG Electronics, Korea. From 2006 to 2007, he was a full time lecturer of Electronic Engineering at University of Incheon. Since 2008, he has been a professor in School of Electrical and Electronics Engineering, Chung-Ang University, South Korea. His research interests include low energy networks and algorithms, bio-inspired autonomous networks, artificial intelligence based networks. He is a member of IEEE, IEICE, KIISE and KICS.