Journal of the KIMST, Vol. 22, No. 6, pp. 797-805, 2019
ISSN 1598-9127(print), 2636-0640(online)
DOI https://doi.org/10.9766/KIMST.2019.22.6.797

Research Paper 정보 · 통신 부문

사이버전 훈련을 위한 ATT&CK 기반 모의 위협 발생기 설계 및 구현

홍수연*,1) · 김광수1) · 김태규1)

1) LIG넥스원㈜ C4I연구소 9팀

The Design and Implementation of Simulated Threat Generator based on MITRE ATT&CK for Cyber Warfare Training

Suyoun Hong*,1) · Kwangsoo Kim1) · Taekyu Kim1)

1) *C4I Research Center Team 9, LIGNex1, Korea*

(Received 2 September 2019 / Revised 18 November 2019 / Accepted 25 November 2019)

ABSTRACT

Threats targeting cyberspace are becoming more intelligent and increasing day by day. To cope with such cyber threats, it is essential to improve the coping ability of system security officers. In this paper, we propose a simulated threat generator that automatically generates cyber threats for cyber defense training. The proposed Simulated Threat Generator is designed with MITRE ATT & CK(Adversarial Tactics, Techniques and Common Knowledge) framework to easily add an evolving cyber threat and select the next threat based on the threat execution result.

Key Words : Cyber Threat(사이버 위협), Penetration Testing(모의 침투 테스트), Simulation(시뮬레이션), Cyber Training (사이버 훈련), MITRE ATT&CK Framework(마이터 어택 프레임워크)

1. 서 론

사이버 공간은 현대 사회의 거의 모든 정보가 집약되고 유통되는 공간으로서 정치적, 영리적 목적을 위해 대상 정보와 흐름을 탈취하고자 하는 사이버 위협은 날로 지능화되어 증가하고 있다. 실시간으로 진화하는 사이버 위협에 모두 대응할 수 있는 시스템 보안 솔루션을 구축하기란 불가능에 가까우므로 시스템 보안 담당자가 사이버 위협 발생 시 시스템 자산을 신속하게 보호할 수 있도록 대처 능력을 강화해야할 필요가 있다. 사이버 위협에 대한 시스템 보안 담당자의 대처 능력을 향상시키기 위해서는 다양한 사이버 위협 시도를 적용한 실전적 훈련 방식이 필요하나 실제 운영되고 있는 시스템을 대상으로 이를 수행하는 것은 많은 위험이 따른다. 따라서 이러한 훈련을 수행하기 위한 방안으로서 민·군에서는 실제 구축 시스템과 유사한 형태의 테스트베드를 구축하여 사이버 훈

* Corresponding author, E-mail: suyoun.hong@lignex1.com

련 수행 및 시스템의 공격 대응 능력을 검증하는 형태를 취한다[1]. 미국 DARPA(Defense Advanced Research Project Agency)가 개발한 국가 사이버전 시험장(NCR, National Cyber Range)[2]과 이스라엘에서 제공하는 사이버 보안 에뮬레이션 훈련을 위한 사이버짐[3]이 대표적 예이다.

그러나 이러한 훈련 체계들은 기본적으로 특정 위협이 적용된 상태의 테스트베드를 제공하여 훈련 대상으로 하여금 이를 분석하고 조치를 취하게 하거나 훈련 내용에 의해 미리 정해진 위협을 훈련 관리자가 수동으로 발생시켜 이에 대한 훈련자의 대응 능력을 평가하고 있다. 따라서 훈련 체계의 사이버 위협은 훈련 내용에 의해 미리 정해지며 하나의 훈련 상황에서 정해지지 않은 사이버 위협을 새로 발생시켜 적용하기가 쉽지 않은 상황이다. 본 논문에서는 이로 인해 발생하는 사이버 훈련의 경직성을 해소하기 위해 구축 시스템에 대한 보안 검증을 수행하는 기법인 모의 침투 테스트(Penetration testing)를 자동화하여 적용하는 방안을 제안한다.

모의 침투 테스트는 구축 시스템의 정보 보안 수준을 능동적으로 평가하기 위한 절차이며 실제 위협 행위(hacking)의 시뮬레이션을 수행한다[4]. 시뮬레이션은 실제 위협 발생원이 사용하는 것과 동일한 방식으로 이루어진 테스트 케이스를 적용하여 위협 실행 결과를 도출하는 것이며 그 결과를 기반으로 시스템의 공격 대응 능력을 평가하고 보완하여 효과적인 방어 프로세스를 구축할 수 있게 한다. 일반적으로 모의 침투 테스트를 담당하는 해킹 담당자는 화이트 해커(White hacker)들로 구성되나 인적 자원에 의해 직접 위협을 발생시키는 과정은 매우 고비용이 소요되어 최근에는 이를 자동화하기 위한 도구들이 연구 혹은 상업적 목적으로 개발되고 있다.

본 논문에서는 이러한 사이버 위협 자동 발생 프레임워크를 사이버 훈련체계에 적용하기 위한 모의 위협 발생기의 설계와 구현 예제를 제시하고자 한다.

본 논문의 2장은 기존 사이버 훈련체계에 대한 분석과 모의 침투 테스트를 자동화하기 위한 방안에 대한 기존 연구에 대해 설명한다. 그리고 사이버 위협을 모의하여 적용하기 위한 방안으로서 채택한 MITRE ATT&CK의 사이버 위협 분류 체계를 설명한다. 3장에서는 모의 위협 발생기의 설계 개념과 소프트웨어 구조를 설명하고 4장에서는 모의 위협 발생기의 구성 및 구현 예제에 대해 설명한다. 5장에서는 결론과 이후의 연구 진행 방향에 대해 고찰한다.

2. 기존 연구 분석

본 장에서는 서론에서 간략히 설명한 기존 사이버 훈련 시스템 분석 및 모의 침투 테스트 자동화 사례, 제안하는 모의 위협 발생기에 적용된 MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) Framework의 연구 내용을 정리한다.

2.1 기존 사이버 훈련 시스템

발생 가능한 사이버 위협에 대한 대처 능력을 강화하는 실전적 훈련을 위한 사이버 훈련 시스템은 크게 구성 모의(constructive simulation)와 실가상 환경 모의(Live-Virtual simulation) 방식으로 나눌 수 있다. 구성 모의의 경우, 실제 구축된 복잡한 시스템을 추상화 모델링(abstract modeling)을 통해 표현한 후, 수립한 방책의 효과도(measure of effectiveness)를 검증하거나 방책의 실행 순서를 훈련하는데 사용할 수 있으며 일반적으로 작전급 훈련에 사용될 용도로 개발된다. 구성 모의 훈련 시스템의 경우, 추상화된 사이버 위협의 효과를 수치상으로 모의하기 때문에 훈련 대상에게 실제와 동일한 경험을 주기 어렵다. 보다 효과적인 훈련을 위해 실제 물리 장비를 연결하여 사이버 위협의 영향이 어떤 식으로 영향을 미치는지 훈련생에게 전달하는 LC(Live-Constructive) 방식을 혼용하기도 하나 사이버 위협의 부가 효과(side effect)를 재현할 수는 없다. 이 방식의 시스템 구축 예로는 DARPA에서 개발한 LARIAT[5], 미 Scalable Network Technologies가 개발한 사이버 방어 훈련 시스템인 NDTrainer[9]가 있다.

두 번째 방식인 실가상 환경 모의 시스템은 현실적인 사이버 훈련을 위해 실제의 사이버 환경을 가상화 기술을 이용하여 동적으로 생성한 유사한 테스트베드 환경에서 실제 시스템 보안 담당자가 사이버 위협에 대해 수립된 방책의 기법 및 절차를 훈련할 수 있도록 지원한다. 이러한 방식의 사이버 위협에 대한 방어 훈련은 일반적으로 공격을 담당하는 레드팀, 방어를 담당하는 블루팀(훈련 대상), 훈련에 대한 모니터링을 수행하는 화이트팀으로 구성되어 운용되며 특정 위협이 적용된 상태의 테스트베드를 제공하여 블루팀으로 하여금 이를 분석하고 조치를 취하게 하거나 훈련 내용에 의해 미리 정해진 위협을 레드팀이 수동으로 발

생시켜 이에 대한 훈련자의 대응 능력을 화이트팀이 평가하하는 형태로 이루어진다. 이를 위해 적절한 사이버 위협 발생과 훈련 대상에의 훈련 효과 분석을 위해 레드팀과 화이트팀은 사이버전의 전문가로 구성될 필요가 있다. 시스템 구축 예로는 해외로는 이스라엘에서 2013년에 설립된 사이버 보안 에뮬레이션 훈련 센터인 사이버짐(CyberGym)[3]과 미국 DARPA(Defense Advanced Research Project Agency)가 개발한 국가 사이버전 시험장(NCR, National Cyber Range)[2] 등이, 국내 예로는 KISA의 시큐리티짐(Security-Gym)이 2017년 11월부터 공식 운영을 시작한 바 있다.

2.2 모의 침투 테스트 자동화 도구

2.1절에서 분석한 기존 실가상 환경 모의 방식의 사이버 훈련 시스템을 운용하여 블루(방어)팀의 훈련을 수행하기 위해서는 사이버전의 전문가로 구성된 레드팀 구성이 필수적이다. 그러나 전문적인 인적 자원-화이트 해커(White hacker)에 의해 직접 위협을 발생시키는 과정은 매우 고비용이 소요되고 레드팀의 수준에 의해서 훈련의 난이도가 좌우되는 문제점을 가진다.

이 문제는 보안이 중시되는 분야의 정보 시스템 구축 및 검증 시에도 동일한 형태로 발생한다. 구축 시스템에 대한 보안 검증을 수행하기 위해서 일반적으로 적용하는 모의 침투 테스트는 실제 위협 행위(hacking)의 시뮬레이션을 수행하여[4] 시스템의 공격 대응 능력을 평가하고 보완하여 효과적인 방어 프로세스를 구축할 수 있게 한다. 하지만 이러한 테스트를 수행하는 해킹 담당자는 화이트 해커(White hacker)들로 구성되기 때문에 앞 절에서 설명한 문제가 그대로 도출되는 것이다. 이를 극복하기 위한 방안으로 최근에는 침투 테스트를 자동화하기 위한 도구들이 연구 혹은 상업적 목적으로 개발되고 있다. Caldera라는 자동 공격 수행 오픈소스 플랫폼은 미국의 비영리 단체인 MITRE에서 연구하고 개발하였으며 설정된 공격 목표와 기법 등을 고려하여 Windows enterprise network에 대한 자동화된 공격을 수행한다[6].

침입 및 공격 시뮬레이션(BAS: Breach and Attack Simulation)이라는 비교적 새로운 IT 기술은 침투 테스트 자동화를 활용하여 구축 시스템의 취약점을 자동적으로 분석해주는, 최근 주목받고 있는 분야이며 전문가가 아니더라도 조직 내에 구성된 시스템의 보안 수준을 평가할 수 있도록 한다. 현재 BAS 시장의 벤더는 벤처 기업이 되는 경향이 있으며, AttackIQ, Cronus Cyber Technologies, Guardicore, XM Cyber등의 벤더가 시장에 솔루션을 공급하고 있다. 그러나 자동화된 테스트의 한계점으로 사이버 위협 간의 결과 연계를 중심으로 하는 APT 공격 절차를 제공하지는 못하며 공개된 위협을 단발적으로 시스템에 대입하는 형태에 그치고 있다.

2.3 마이터 어택 프레임워크

마이터 어택 프레임워크(MITRE ATT&CK: Adversarial Tactics, Techniques and Common Knowledge Framework)는 미국 연방정부에 기술지원 및 시스템 운영업무를 수행하는 비영리 법인이자 국제표준 보안취약점 식별체계 CVE(Common Vulnerabilities and Exposures: 공개적으로 알려진 정보 보안 결함 목록) 번호 부여 권한(CNA: CVE Numbering Authorities)을 관리하고 있는 마이터(MITRE)에서 만든 사이버 위협 단계별 전술(Tactics)과 그에 속하는 기술(Technique)을 정의한 프레임워크이다[7]. 분류된 전술과 그에 대한 설명을 Table 1에 요약하였다.

Table 1. MITRE ATT&CK matrix - october 2019

전술	설명	기술 개수
Initial Access	네트워크 내 초기 발판 구축	11
Execution	로컬/원격 시스템에서의 코드 실행	34
Persistence	시스템 상주	63
Privilege Escalation	권한 상승	32
Defense Evasion	시스템 방어 우회	73
Credential Access	자격 증명	23
Discovery	시스템 및 내부 네트워크 정보 획득	25
Lateral Movement	원격 접속 및 제어	20
Collection	민감 정보 수집	14
Command and Control	공격자에 의한 명령 및 제어	22
Exfiltration	정보 유출	10
Impact	시스템/서비스/네트워크의 가용성, 무결성 감소	16

마이터 어택 프레임워크는 기업, 정부 등 사이버 보안 제품 및 서비스 커뮤니티에서 특정 위협을 모델링하고 이를 실행하는 방법을 개발하기 위한 기반으로 적용할 수 있으며 알려진 보안 위험을 이해하고 방어 필요 작업을 식별하는데 유용하다.

3. 모의 위협 발생기 설계

본 논문에서 제안하는 모의 위협 발생기는 사이버 전 훈련 시스템에 적용할 목적을 가지며 훈련 대상에게 다양한 사이버 위협에 대한 대응 방식을 숙련시키기 위한 도구로 개발된다. 따라서 모의 위협 발생기는 사이버 위협을 체계적으로 분석하여 분류한 MITRE의 ATT&CK Framework를 기반으로 적용할 세부 위협 중 자동화가 가능한 기술을 선택하고 실행할 수 있어야 한다. 이러한 운용 개념을 Fig. 1로 나타내었다.

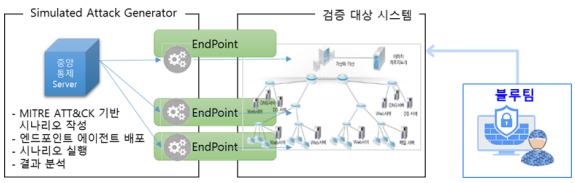

Fig. 1. Operation concept

3.1 모의 위협 발생기 소프트웨어 설계

모의 위협 발생기는 실환경과 유사하게 구축된 테스트베드에 사이버 위협을 발생시켜야 한다는 기능적 요구사항을 가진다. 그리고 발생시키는 사이버 위협 역시, 실제 위협과 유사한 형태로 진행되어야 하므로 실행한 사이버 위협의 성공/실패 여부에 따라 다음 가능한 사이버 위협을 선택할 수 있도록 개발하여야 한다. 완전한 자동화를 위해서는 다음 가능한 사이버 위협을 ATT&CK 기반의 기술들에서 모의 위협 발생기가 선택하여 실행할 수 있도록 개발하는 것이 이상적이나 현재 전체 훈련 의도에 부합하는 목적에 도달하기 위한 적절한 위협 시퀀스를 자동으로 생성하는 것은 기술적으로 불가능하다. 따라서 실행된 위협의 성공/실패 조건에 따라 다음 진행 가능한 위협 기술을 설정하도록 시나리오를 저작한다.

소프트웨어를 설계하고 구현하기 위하여 기능적 요구사항과 함께 고려되어야 할 비기능적 요구사항, 즉 품질 속성[8]을 분석하여 Table 2로 정리하였다.

Table 2. Quality attribute scenario

품질 속성	설명
1. 확장성	모의 위협 발생기는 증가하는 사이버 위협의 종류를 추가하는데 용이한 구조를 가져야 한다.
2. 성능	2-1 모의 위협 발생기는 훈련 시나리오에 따라 결정된 사이버 위협을 네트워크 단말에서 근실시간(3초 이내)로 동작시켜야 한다.
	2-2 훈련 시나리오에 의해 구축되는 테스트베드의 네트워크 망은 최대 300개의 단말을 가진다.
3. 보안	모의 위협 제어를 위한 메시지는 훈련 대상자가 훈련을 위해 사용하는 네트워크 망에 노출되지 않아야 한다.

모의 위협 발생기는 정의된 기능적 요구사항과 품질 속성 2, 3번을 고려하여 목록의 컴포넌트들이 서로 연동하여 사이버 위협을 발생시키는 구조로 설계한다.

- 시나리오 저작도구: 위협의 발생 순서를 지정
- Master Agent: 시나리오와 위협 수행 결과에 따라 필요한 사이버 위협을 발생시키기 위한 제어 수행
- Slave Agent: ATT&CK에서 정의한 기술 단위의 위협을 훈련 시스템에 적용
- 결과 분석 도구: 위협 수행 결과를 수집

이를 그림으로 나타내면 Fig. 2와 같다.

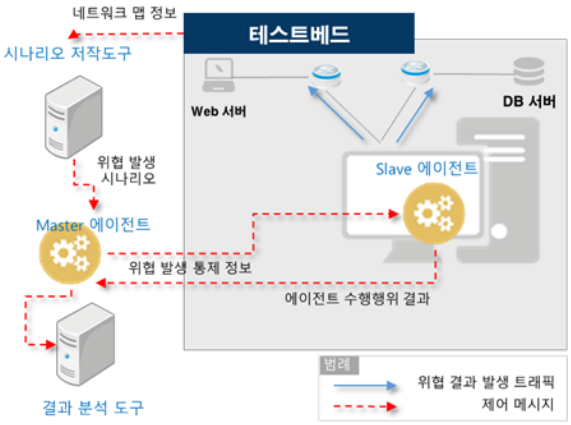

Fig. 2. Simulated attack generator architecture

Fig. 2에서 볼 수 있듯이 모의 위협 발생기는 목록과 같은 인터페이스를 가진다. 목록의 EIC는 외부 인터페이스를, IIC는 내부 인터페이스를 의미한다.

- EIC 1: 훈련 시스템의 네트워크 맵 정보를 불러옴
- IIC 1: 저작된 위협 발생 시나리오를 전달함
- IIC 2: 위협 발생을 위한 제어 메시지를 전달함
- IIC 3: 단말 노드에서 실행된 사이버 위협의 결과를 로그로 전달
- IIC 4: 결과 분석 도구에 실행된 사이버 위협 정보와 성공/실패 결과 로그를 전달

이 중 IIC 2, 3은 품질 속성 2, 3번에 영향을 끼치는 요소로 분석할 수 있다.

Slave Agent가 설치되는 테스트베드의 단말 노드는 최대 300개까지 존재할 수 있으며 노드에 부여되는 IP 주소는 훈련 시나리오에 의해 변할 수 있는 가변적인 요소이다. 이에 대해 Master agent가 각각의 모든 slave agent에 session을 유지하며 제어 명령을 전달하는 것은 불필요한 성능적 부하로 작용할 수 있으므로 제어 메시지는 publish/subscribe 구조로 Master와 Slave 간의 직접적인 연결 없이 전달될 수 있는 형태로 설계하였다[8]. 또한 품질 속성 4. 보안 요구사항에 의해 publish/subscribe 형식으로 전달되는 제어 메시지는 훈련생이 사용하는 테스트베드 내부의 네트워크 망에 영향을 주지 않아야 하므로 테스트베드 구축 시, 제어 메시지 통신을 위한 별도의 네트워크 어댑터를 추가하여 해당 어댑터에서만 제어 메시지를 처리하도록 한다. 위의 설명한 개념을 Fig. 3로 나타내었다.

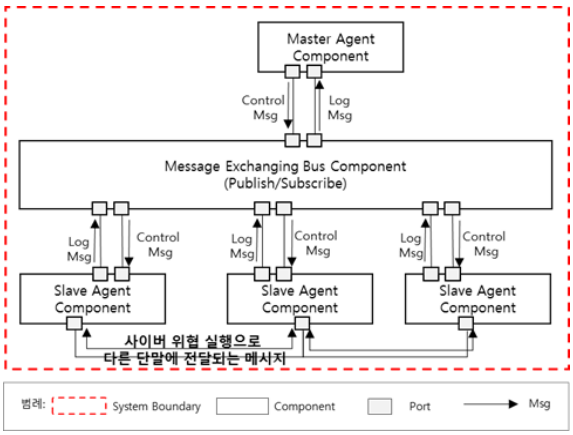

Fig. 3. Master-slave agent communication

마지막으로 고려해야하는 품질 속성은 확장성이다. 사이버 위협은 실시간으로 진화하며 위협을 수행하는 기술 역시 그에 맞춰 증가하게 된다. 따라서 지속적으로 훈련에 사용할 수 있는 모의 위협 발생기를 개발하기 위해서는 유지보수 시 새로 발견된 사이버 위협을 쉽게 추가할 수 있고 이미 배포된 상태의 모의 위협 발생기를 쉽게 업데이트할 수 있는 구조로 설계되어야 한다.

이를 위하여 테스트베드 전체 단말에 배포되어야 하는 Slave Agent의 최초 설치 상태는 Master Agent와의 통신을 위한 최소 구조로 설계하고 실제로 사이버 위협을 실행할 때마다 실행을 위한 세부 위협 모듈을 Master Agent로부터 전달받아 동작시키는 플러그인 패턴을 적용한다.

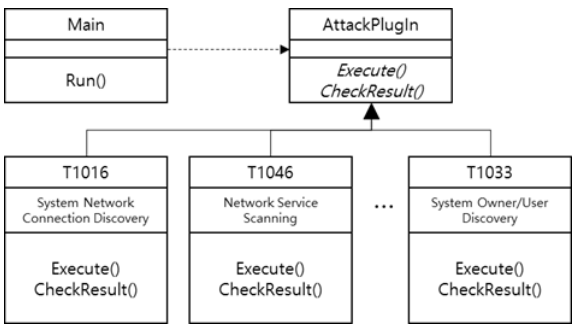

Fig. 4. Simulated attack plug-in

Main 클래스는 Slave Agent의 제어 모듈로 동작하며 Master Agent로부터 AttackPlugin을 상속받은 클래스를 plugin 실행이 가능한 형태로 전달받아 AttackPlugin 인터페이스의 Execute 함수를 이용하여 실제 사이버 위협인 T1016 등의 구현 플러그인을 동작시킨다. 그리고 이 위협의 성공/실패 여부를 판단하기 위한 결과를 확인하는 인터페이스인 CheckResult 함수를 추가적으로 realization 대상으로 둔다.

Slave Agent가 실행할 위협 플러그인 모듈은 Master Agent로부터 전달받아야 하는 구조로 설계하였으므로 Master agent는 저작된 위협 시나리오에 따라 적절한 위협 플러그인 모듈을 선택할 수 있는 인터페이스를 에이전트 외부로부터 제공받아야 하며 해당 인터페이스를 제공하는 모듈은 개발자나 유지보수자에 의해 개발된 위협 플러그인 모듈을 등록하고 외부에서 참조할 수 있는 형태로 관리할 책임을 가지게 된다. 위협 플러그인 모듈은 ATT&CK Framework의 기술 단위

를 기준으로 구현되고 위협 시나리오 저작의 경우에도 ATT&CK의 기술 중 사용할 것을 선택하는 방식으로 이루어지므로 모듈 기능 간의 응집도를 높이기 위해서 위협 시나리오 저작 모듈에 위협 플러그인 모듈을 등록하고 관리하는 책임을 할당한다.

3.2 모의 위협 발생기의 구성과 기능

3.1절에서 기술한 모의 위협 발생기의 소프트웨어 구조를 바탕으로 각 컴포넌트들을 정리해보면 Table 3과 같다.

Table 3. Simulated attack generator components

컴포넌트	역할
시나리오 저작	사이버전 훈련에 사용될 ATT& CK 기반 위협 시나리오 저작 위협 플러그인 모듈 DB 관리
메시지 교환	Master/Slave agent간 통신을 위한 publish/subscribe 구조 지원
Master Agent	위협 시나리오를 해석하여 다음 위협을 수행할 slave agent에 위협 모듈과 제어 메시지 전달
Slave Agent	테스트베드의 단말에서 사이버 위협을 실행하고 결과를 파악하여 Master agent로 전달
결과 분석	위협 시나리오 수행 결과 저장

이 컴포넌트들 간의 기능 흐름은 다음과 같다. 훈련 관리자가 시나리오 저작 컴포넌트를 사용하여 가능한 위협 경로 및 기술을 선택하여 위협 시나리오를 저작하면 Master 에이전트는 이를 해석하여 테스트베드 환경 내부의 단말에 설치된 Slave 에이전트로 통제 명령과 위협 모듈을 보낸다. 테스트베드의 규모에 따라 Slave 에이전트는 최대 300개가 될 수 있기 때문에 메시지 교환은 publish/subscribe 구조를 채택했으며 이를 위해 대용량 데이터 처리에 적합한 Kafka 서버를 사용하여 연결한다. Apache Kafka는 publish/subscribe 구조을 채용한 분산 메시징 시스템으로 LinkedIn에서 개발하여 2011년에 오픈소스로 공개된 상태이다. Slave 에이전트는 전달받은 명령을 통해 위협 플러그인을 로드하여 실행하고 실행에 따른 성공/실패 결과를 Master 에이전트에 송신한다. Master 에이전트는 작성된 시나리오에 의해 현재 실행된 노드의 천이 조건에 따라 다음 실행 위협을 결정하고 수행 결과를 결과 분석 컴포넌트로 전송한다. 결과 분석 도구는 훈련 후, 훈련 진행을 분석하기 위해 사용될 실행 로그들을 DB에 저장하게 된다.

4. 모의 위협 발생기 구현

4장에서는 3장의 설계 내역을 반영한 각각의 컴포넌트의 세부 설계 내용을 pseudo code 형태로 설명하고 예제 시나리오 구동 시, 생성된 로그를 구현 결과로 제시한다.

4.1 시나리오 저작 모듈

시나리오 저작 모듈은 실행할 기술을 선택하고 해당 위협을 수행할 단말을 지정한 후, 위협을 수행하기 위해 필요한 사전 조건 및 테스트베드에 구성된 가상 머신들의 네트워크 연결 구조를 반영한 파라미터들을 입력하게 된다. 또한 실제 위협과 유사한 형태의 위협 진행을 수행하기 위해 사이버 위협의 결과인 성공/실패에 따라 다음 위협을 선택할 수 있는 분기를 두어 다른 위협 시퀀스를 진행할 수 있도록 한다.

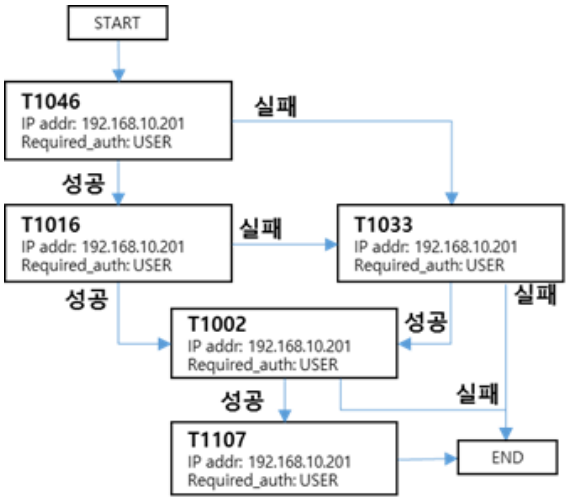

Fig. 5. Simulated attack sequence scenario

이런 형태로 작성된 사이버 위협 시나리오는 JSON (JavaScript Object Notation: 키-값 쌍으로 이루어진 데이터를 전달하는 언어 독립형 개방형 표준 포맷, 표준번

호-TTAE-OT-10.0394) 형식으로 변환되어 Master Agent에 전달된다. 이 형식의 format은 Fig. 6에 나타나 있다.

기술 단위의 기본 정보는 DB에서 저장하여 관리하도록 하며 기술을 수행하기 위한 실구현 위협 모듈을 파일 형태로 저장하고 기술 ID로 연결하여 Master Agent에서 참조할 수 있도록 DB에서 저장 위치를 관리한다. 이를 간략히 ERD(Entity Relation Diagram)으로 나타내면 Fig. 7과 같다.

```
"Nodes": [{
  "node_seq_idx": 1,
  "threat_idx" : "T1046",
  "threat_name": "Network Service Scanning",
  "succ_transition_node_idx": 2,
  "fail_transition_node_idx": 3,
  "threat_org_IP":"192.168.10.206",
  "threat_victim_IP":"192.168.10.206",
   },
  {
  "node_seq_idx": 2,
  "threat_idx" : "T1016",
  "threat_name": "System Network Connection Discovery"
  "succ_transition_node_idx": 4,
  "fail_transition_node_idx": 3,
.....
```

Fig. 6. Simulated attack scenario format

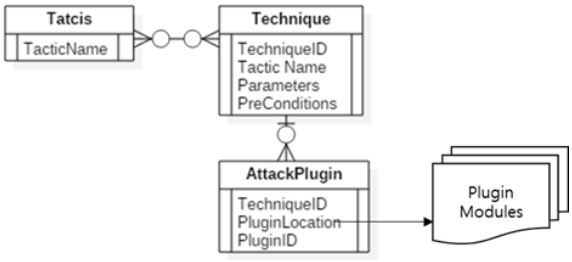

Fig. 7. Technique management DB ERD

4.2 Master Agent

Master Agent는 Fig. 6의 format으로 전달된 사이버 위협 시나리오를 해석하여 node_seq_idx를 key로 가지는 방향 그래프를 자료 구조로 생성하여 위협 시나리오를 관리한다. 시나리오에 의한 위협이 시작되면 현재 노드에서 가지고 있는 사이버 위협의 ID를 보고 위협 플러그인 DB에서 해당 모듈을 받은 후, 이를 Message bus 역할을 하는 Kafka 서버에 전달한다. 그리고 해당 모듈을 전달받은 slave agent가 위협을 수행한 후 실행 결과를 성공/실패로 판정하여 송신하면 이를 받아 다음 노드로 천이하여 다음 위협에 대한 제어 명령을 주는 흐름으로 구현되었다.

4.3 Slave Agent

Slave Agent는 Master Agent로부터 전달받은 모듈을 상위 인터페이스를 통해 실행시킨다. 상위 인터페이스는 Fig. 4에서 interface class로 명시된 AttackPlugin class에서 제공하는 추상 함수인 Execute를 수행하여 사이버 위협을 실행하고 CheckResult를 통해 수행 결과를 반환받는다. 이를 실행하는 pseudo code는 Figure. 8과 같다 .

```
def executePkt(self, jsondata):
    _module_name = "SimAttack." + _module_name
    mod = __import__( _module_name, fromlist=[''])
    _instnace = mod.script_code(_scn_idx)

   # AttackPlugin을 처리 전 선행 조건을 충족했는지 확인
   # 충족시 Execute 수행
  _instnace.Execute(_script, _extInfo)
  result = _instnace.CheckResult()
```

Fig. 8. AttackPlugin processing pseudo code

pseudo code에서 확인할 수 있듯이 AttackPlugin module은 파일명이 SimAttack.T####으로 지정되어야 하며 내부의 class name은 script_code로 통일된다. Agent를 개발하는데 사용된 python 언어는 module 동적 import를 지원하며 이를 이용하여 간단한 plugin 구조를 구현할 수 있다. 이 형식으로 작성되는 AttackPlugin 내부 구조는 Fig. 9와 같다.

```
class script_code():
    def __init__(self, _scn_idx):
        self.Threat_idx = "T1016"
        # more....

    def Execute(self, _script, _extInfo):
        # 위협 실행 script를 제어 명령의 정보를 사용하여 구성
        # 위협 행위 실행

    def CheckResult(self):
       # 실행 결과 확인
       # return True or False
```

Fig. 9. T1016 AttackPlugin pseudo code

4.4 사이버 위협 시나리오 수행 결과

모의 위협 발생기가 설계 의도와 동일하게 동작하는지를 검증하기 위하여 Fig. 10의 시스템 구성도로 가상 머신 네트워크를 구성하고 Fig. 5의 테스트용 사이버 위협 시나리오를 수행한 결과, 의도한 바와 같이 T1046, T1016, T1002, END 순서로 실행됨을 확인할 수 있었다.

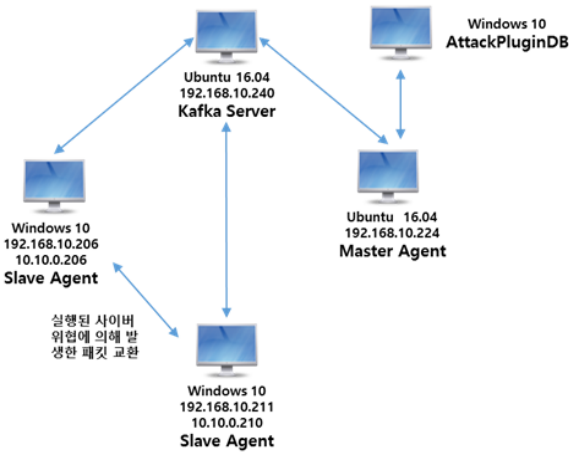

Fig. 10. Cyber attack target system structure

5. 결 론

본 논문에서는 실시간으로 진화하는 사이버 위협에 대응하는 시스템 보안 담당자의 역량을 향상시키기 위한 사이버전 훈련 시스템에 적용할 수 있는 모의 위협 발생기의 설계와 구현 예제를 제시하였다. 그리고 4장에서 기술한 바와 같이 구현 및 시험을 통해 기능이 정상적으로 동작함을 입증하였다.

본 논문에서 제시한 ATT&CK 기반 모의 위협 발생기는 선행된 사이버 위협의 성공/실패 조건에 따라 다음에 수행 가능한 사이버 위협을 선택하여 수행한다. 따라서 사이버 훈련생이 실시간으로 진행되는 사이버 위협에 대한 실시간 대응 능력을 향상시킬 수 있는 특징을 가진다. 이 특징은 시스템의 사이버 위협 대응성을 검증하는데 특화된 기존 자동화 도구와 차별되는 요소로서 사람을 훈련시키는 측면에서 강점을 지닌다.

향후에는 사이버 위협 추가가 용이하도록 설계되고 구현된 소프트웨어 구조에서 제공하는 인터페이스를 통해 활용 가능한 사이버 위협 모듈을 추가하여 더 다양한 형태의 사이버 위협 대응 훈련 지원 도구로 발전할 수 있을 것이다. 또한 도전 과제로서 Master Agent에서 사이버 위협의 목적을 달성하기 위한 위협들을 조건 기반으로 지능적으로 식별하여 자동으로 선택한 후, 실행하도록 발전시킬 수 있을 것이다.

후 기

이 논문은 민·군기술협력사업의 지원으로 수행된 연구임(UM17312RD3).

References

[1] Myung Kil Ahn, 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, 2016.

[2] B. Ferguson, A. Tall, and D. Olsen, “National Cyber Range Overview,” Proceedings of the 2014 IEEE Military Communications Conference, MILCOM ’14, pp. 123-128, Oct. 2014.

[3] T. Bonaci and J. Herron and T. YusufTo, “Make a Robot Secure: An Experimental Analysis of Cyber Security Threats Against Teleoperated Surgical Robotics,” National Science Foundation, CNS-132975 1, pp. 1-11, May 2015.

[4] SHIVAYOGIMATH, Chaitra N., “An Overview of Network Penetration Testing,” International Journal of Research in Engineering and Technology, Vol. 3, No. 3, pp. 408-413, 2014.

[5] Rossey, L. M., Cunningham, R. K., Fried, D. J., Rabek, J. C., Lippmann, R. P., Haines, J. W., & Zissman, M. A. “Lariat: Lincoln Adaptable Real-Time Information Assurance Testbed,” In Proceedings, IEEE Aerospace Conference Vol. 6, pp. 6-6, March, 2002.

[6] Applebaum, A., Miller, D., Strom, B., Korban, C., & Wolf, R. “Intelligent, Automated Red Team Emulation,” In Proceedings of the 32nd Annual

Conference on Computer Security Applications, ACM, pp. 363-373, December, 2016.

[7] Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., & Thomas, C. B., "MITRE ATT&CK™: Design and Philosophy," Technical Report, 2018.

[8] Len Bass, Paul Clements, Rick Kazman, "Software Architecture in Practice," Addison-Wesley Professional, America, 2012.

[9] Lloyd Wihl, "Training for the Combined Cyber / Kinetic Battlefield," In Proceedings of MODSIM World 2015. No. 9, pp. 1-11, March, 2015.