사이버 훈련을 위한 위협행위 자동화 아키텍처 설계

홍수연*, 류한얼*, 김동화
LIG넥스원*, 국방과학연구소
*{suyoun.hong, haneul.ryu}@lignex1.com, dhkim@add.re.kr

Design of Automated Cyber Threat Generating Architecture for Cyber-security Training System

Hong Su-Youn*, Ryu Haneul*, Kim Donghwa
LIGNex1*, Agent of Defense Development

요 약

증가하는 사이버전 위협에 효과적으로 대응할 수 있는 인력을 양성하기 위해서는 발생하는 위협의 연계에 따른 침투 및 공격 상황을 제공하여 대응 인력이 실전적으로 훈련할 수 있도록 하여야 한다. 본 논문에서는 훈련 목적에 맞는 위협을 유기적으로 연결된 위협 체인을 자동으로 생성하고 이를 수행하기 위한 위협 행위 아키텍처 설계 방안을 제시한다.

Ⅰ. 서 론

사이버 보안 인력을 양성하기 위한 훈련은 일반적으로 훈련 대상자가 보안 전문가에 의해 발생한 사이버 위협에 대처하는 방식으로 이루어진다. 이러한 훈련에 필요한 비용을 줄이기 위해서는 보안 전문가의 역할을 자동화된 프로세스로 대체하여 인력을 최소화하기 위한 노력이 필요하다. 사이버 위협을 자동화하기 위한 연구는 실제 구축 시스템의 보안 검증을 수행하기 위해 침입 및 공격 시뮬레이션(BAS: Breach and Attack Simulation) 분야에서 발전하고 있으나 자동화된 테스트의 한계점으로 사이버 위협 간의 결과 연계를 중심으로 하는 APT 공격 절차를 제공하지는 못하며 공개된 위협을 단발적으로 시스템에 주입하는 형태이다[1]. 시스템 구축이 아닌 보안 인력의 훈련을 위해서는 위협의 연계와 그에 따른 침투 절차를 유기적으로 연결하는 것이 중요하다. 본 논문에서는 유기적으로 연결된 사이버 위협 체인을 자동으로 생성하고 이를 수행하기 위한 위협 행위 아키텍처 설계에 대해 설명한다.

Ⅱ. 본론

사이버 훈련을 위한 위협행위 자동화 아키텍처는 기본적으로 훈련 대상 시스템의 네트워크 구성 및 각 노드 정보를 알 수 있다는 가정에서부터 출발한다. 훈련 관리자에 의해 설계되는 훈련 시나리오에 있는 정보들은 사이버 훈련 전에 저작되며 위협행위 자동 발생 아키텍처는 이 정보를 활용함으로써 일반적인 사이버 위협이 진행되기 위해 취득해야하는 정보들을 획득한 것으로 간주하고 실제적인 위협을 수행할 수 있다.

그림 1. 훈련 시나리오 구성 및 포함 정보

1. 위협 행위 경로 생성 및 시나리오 구성

훈련 시나리오에 의해 위협 행위의 시작점과 최종 공격 대상 지점이 지정되면 위협행위 자동 발생 아키텍처는 주어진 네트워크 맵 시나리오의 연결 정보를 사용하여 시작점에서 최종 공격 대상 지점으로의 경로를 생성할 수 있다. 불특정 네트워크에서의 사이버 위협 진행 경로 예측은 사이버 공격 그래프 기술 분야[2]에서 연구되고 있으나 사이버 훈련을 위한 에이전트의 진행 경로 생성에서는 전체 위협 경로에 대한 예측이 필요하지 않다. 따라서 훈련의 목적에 맞도록 에이전트의 시작 위치와 최종 위협 목적 지점을 지정하고 그 사이의 노드를 도달 가능성(Reachability)만을 고려하여 선정하는 방식으로 수행한다.

경로가 생성되면 위협행위 시나리오의 최종 수행 공격 목적에 따라 최종 타겟 노드에서 실행해야 하는 마지막 위협 행위를 발생시키기 위한 이동(lateral movement)와 시스템 권한(Privilege) 획득 필요 노드를 식별할 수 있게 된다. 이동을 위해서는 웹, 메일 등의 사용자 정보가 필요한 별도의 전달 경로가 인식될 수 있으며 이는 훈련 환경 상 에이전트가 자동적으로 획득할 수 없는 사회적 정보이므로 시나리오에서 별도로 주어져야만 한다. 그 외 위협 모듈을 실행하기 위해서 획득해야 하는 정보가 있다면 다른 위협행위 모듈의 실행을 통해 해당 정보를 획득해야 한다. 본 논문에서는 훈련 목적 상 최종적으로 실행해야 하는 위협 행위를 달성하기 위해 필요한 정보들을 얻고 경로를 이동하기 위한 위협 행위들의 체인을 자동으로 생성하고 이를 실행하기 위한 개념을 제시한다.

2. 사이버 위협 체인 자동 생성

사이버 위협 체인을 자동적으로 생성하기 위해서는 위협 행위를 모듈화하고 각 모듈의 필요한 입력 정보와 생성 가능한 출력 정보, 해당 위협 모듈을 수행하기 위한 권한 정보가 필요하다. 위협 행위를 모듈화하기 위해 아키텍처 설계에서는 마이터(MITRE: 미국 에서 만든 사이버 위협 단계별 기술을 정의한 프레임워크인 마이터 어택 프레임워크(MITRE ATT&CK- Adversarial Tactics, Techniques and Common Knowledge Framework) 분류 체계[3]를 이용하였다. 그리고 해당 프레임워크에서 정

의한 위협 기술들에 대해 입력 정보와 출력 정보, 권한 정보를 추가적으로 정의하여 본 논문에서 기술하는 아키텍처에서 사용하는 위협 기술 DB로 정의한다.

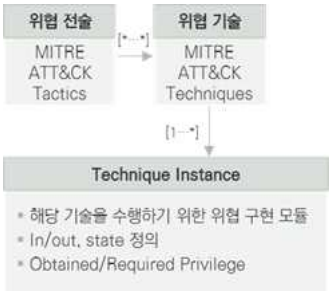

그림 2 위협 기술 DB 정보

MITRE ATT&CK에서 정의하는 기술(Technique)은 개념적인 정의로서 위협을 실제로 수행하기 위해서는 기술을 구현한 위협 모듈(Technique Instance)들을 구현하여 별도의 file DB로서 관리한다. 실제 위협을 수행하는 모듈은 수행하기 위해 필요한 정보인 입력(input), 위협 모듈을 수행함으로써 획득할 수 있는 출력(output)을 가지게 되며 해당 모듈을 실행하기 위해 필요한 권한이 정의된다.

위협 기술 DB에서 각 위협 모듈들의 입력/출력 관계가 정의되면 경로와 최종적으로 특정 노드에서 실행되어야 하는 위협을 발생시키기 위해 위협 기술 체인을 생성할 수 있다. 위협 기술 체인은 일련의 이어진 위협 모듈(Technique Instance)들의 시퀀스로서 최종 목적 기술을 발생시키기 위해 시나리오 상에 지정된 노드들을 역으로 추적하여 현재 수행하여야 하는 기술이 입력으로 필요한 정보를 발생시킬 수 있는 위협 모듈을 선택하는 작업을 재귀적으로 수행하여 최초의 시작점 노드까지 위협 체인을 생성하게 된다. 이를 pseudo code로 나타내면 아래와 같다.

```
generateAttackSeq(attack_path, final_TI)
        TI_sequence.push_front(prev_TI)
        prev_TI = final_TI
        cur_node = final_node in attack_path
        prev_node = prev_node of final_node in attack_path
        while True:
                prev_node, prev_TI = getPrevTI(cur_node, prev_node, prev_TI)
                TI_sequence.push_front(prev_TI)
                if prev_node == first_node in attack_path:
                        break
                else:
                        cur_node = prev_node
                        prev_node = prev_node of cur_node in attack_path

getPrevTI(cur_node, prev_node, prev_TI)
        if prev_TI.input == null:
                TI = lateral_move tecniques in TI_DB
                node = prev_node
        else
                for all TI in TI_DB:
                        if TI.output = prev_TI.input:
                        break
                node = cur_node

        return node, TI
```

그림 3 위협기술 체이닝 pseudo code

3. Master/Slave Agent 구조 설계

위협 경로를 구성하고 목적을 달성하기 위한 위협 행위 체인을 만들어내는 것은 시스템 전체에 대한 정보가 필요하며 한 노드에서 다음 노드로의 이동이 성공했을 경우, 다음 노드에서의 위협에 대한 명령을 내리는 것을 수행하기 위해서는 전체 네트워크 토폴로지 접근이 필요하다. 이를 위해 본 논문에서는 위협행위 자동 수행 부분을 구분하여 위협 행위의 계획을 자동적으로 결정하고 사이버 위협에 대한 명령을 내리는 역할 수행 부분을 master 에이전트의 역할로, 실제 네트워크 각 노드에서 위협을 수행하는 부분을 slave 에이전트의 역할로 할당하여 설계하였다. Master 에이전트는 훈련 환경의 네트워크 토폴로지에 포함되지 않는 별도의 VM 혹은 실제 머신에서 구동될 수 있으며 slave 에이전트와는 publish/subscribe 구조의 메시지 전달 bus를 통해 통신하도록 설계한다.

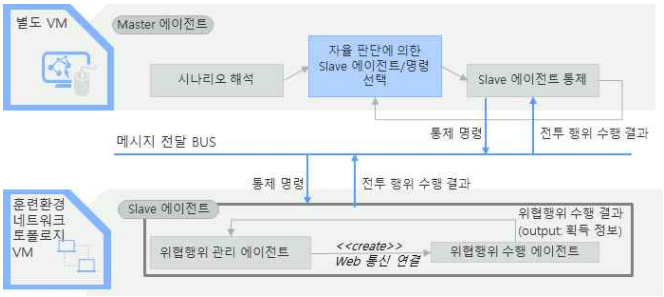

그림 4 위협행위 발생: Master/Slave 구조

Master 에이전트는 네트워크 토폴로지 정보와 위협 경로, 최종 실행 위협 기술에 대한 정보를 바탕으로 2장에서 설명한 위협행위 체이닝 알고리즘을 사용하여 slave 에이전트에 명령을 내리고 그 실행 결과에 따라 다음 실행 위협 기술을 결정한다. 만약 선택한 기술이 수행이 실패했을 경우에는 동일한 출력을 생성하는 위협 모듈을 자동적으로 선택하여 위협행위가 중단되지 않도록 한다.

Ⅲ. 결론

본 논문에서는 사이버 위협에 효과적으로 대응할 수 있는 훈련 상황 조성을 위해 훈련 목적에 맞는 위협을 자동적으로 선택하여 발생시키는 위협행위 자동화 아키텍처를 설계하여 제시하였다. 이는 위협행위에서 노드 간의 이동 시점과 시나리오 저작시 제공되어야 하는 정보들, 위협 모듈(Technique Instance)에서 정의되어야 하는 입력/출력, 상태 정보값들을 기반으로 위협행위를 훈련을 위한 단순 산발적인 행위가 아닌 APT 형태의 의미있는 위협으로서 발생시킬 수 있는 구조이다. 위협 기술 모듈의 구현 개수와 위협 기술 DB의 정보들을 계속적으로 축적한다면 master 에이전트에서 선택 가능한 위협 모듈의 폭이 넓어지게 되어 보다 현실성있고 유연한 사이버전 훈련을 위한 도구로 발전할 수 있을 것이다.

ACKNOWLEDGMENT

이 논문은 국방과학연구소의 지원으로 수행된 연구임(UC180003ED)

참 고 문 헌

[1] 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.

[2] 이주영, 문대성, 김익균, “사이버 공격 시뮬레이션 기술 동향”, 전자통신동향분석 35권 제1호, pp. 34-48, February, 2020.

[3] Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A. G., &Thomas, C. B. “MITRE ATT&CKTM: Design and philosophy.” Technical report, 2018