https://kiisc.or.kr

2022년 한국정보보호학회 동계학술대회

CISC-W'22

Conference on Information Security and Cryptography-Winter 2022

2022년 11월 26일 (토) | 국민대학교

- 학술대회 등록대: 미래관 자율주행 스튜디오 (4층)
- 개회식/정기총회: 본부관 (1층)

Proceedings

주최 한국정보보호학회 Korea Institute of Information Security & Cryptology

주관 KMU 국민대학교 KOOKMIN UNIVERSITY

후원 국가정보원 NATIONAL INTELLIGENCE SERVICE, 과학기술정보통신부, 행정안전부, KISA 한국인터넷진흥원, ETRI 한국전자통신연구원 Electronics and Telecommunications Research Institute, NSR 국가보안기술연구소 National Security Research Institute, KiSTi 한국과학기술정보연구원 Korea Institute of Science and Technology Information www.kisti.re.kr, 지란지교시큐리티, PILAB

한국정보보호학회
Korea Institute of Information Security & Cryptology

조직 맞춤형 사이버 공방 훈련을 위한 가상 인프라 변이 생성 프레임워크

노주영*, 이세한*, 박기웅†

* 세종대학교 시스템보안연구실 (지능형드론 융합전공) (대학원생)
† 세종대학교 정보보호학과 (교수)

Virtual Infrastructure Mutagenesis Framework for Customized-Organization Cyber Warfare Training

Joo-Young Roh*, Se-Han Lee*, Ki-Woong Park†

* SysCore Lab. (Convergence Engineering for Intelligent Drone), Sejong University (Graduate Student)
† Dept. of Computer and Information Security, Sejong University (Prof.)

요 약

사이버 공격 및 침해사건의 수가 증가함에 따라 공격에 대한 신속한 방어 및 대응의 필요성이 증가하고 있다. 이는 사이버 보안 능력을 갖춘 전문가의 양성과 탐지 및 대응을 위한 방어전략을 요구한다. 사이버 훈련장을 통해 방어전략을 갖춘 전문가를 양성하고 있지만, 기존 시스템에서는 가상훈련 시스템의 자원의 한계, 시나리오 기반의 실습 콘텐츠 개발 및 운영 비용적인 문제 등에 있어서 어려움을 겪는다. 이를 보완하기 위해서 본 논문에서는 사이버 훈련장 가상 인프라 생성 기술에 딥러닝 기술을 적용하여 능동적이고 효율적인 훈련장 생성 및 관리 프레임워크를 제안하고자 한다. 이는 지능화되고 있는 사이버 위협에 대응하고 훈련 목적에 부합한 인프라를 구축하여 기존 교육 프로그램의 운영을 재정비하고 개선할 수 있을 것으로 기대한다.

I. 서론

현대의 사이버 공격이 점차 고도화되면서 다양한 공격들로 인해 공공기관과 기업들이 피해를 받고 있다. 특히 새로운 패턴의 사이버 공격의 출현 빈도가 증가하면서[1] 이에 따른 대응 훈련의 중요도가 높아지게 되었고, 정부와 주요 기업들 또한 방어전략과 보안 인력 양성에 대한 중요성을 제시하고 있다[2]. 대응 훈련에서의 주요 문제점 중 하나로, 실질적인 사이버 환경 구성 및 이기종 시스템에 따르는 사이버 환경이 조성되어야 하는데, 이는 운영자가 사이버 위협 대응 훈련환경을 매번 구성하는 데 비용적인 측면과 전문가의 분석에 있어서 한계에 다다르고 있다.

오늘날 사이버 훈련장은 전문가들의 경험을 바탕으로 만들어진 시나리오를 통해 문제를 풀어나가는 방법이 일반적이다[2]. 이러한 훈련 방법은 새로운 사이버 공격 도구, 복합적인 무차별 공격, 실제 환경에 대한 공격 등에 대응이 어렵고 급변하는 최신 환경이나 서비스에 적용하지 못한다는 단점을 가진다. 또한, 훈련 시나리오는 실행에 있어서 위험부담과 요구조건이 따르기에 독단적으로 실행이 불가하다. 그리고 실행 환경 요건과 훈련자의 지식, 기술 수준을 고려하지 않고 설계되는 경우 난이도 조절 실패로 시나리오 활용이 불가능하다. 따라서, 현 시대의 필요한 사이버 훈련장은 공격과 방어 시나리오의 능률적인 생성과 훈련 목적에 따른 환경 구성을 갖춰야 한다. 이를 통해 선제적 조치와 방어 훈련을 수행함으로써 능동적인 수행 능력을 향상하고 공격에 대한 탐지·분석·대응·예방 등을 방어전략으로 갖추며 이를 순환적으로 실행함으로써 재훈련할 기회를 가질 수 있도록 해야 한다. 본 논문에서는 이러한 기회들

†교신저자: 박기웅 (세종대학교 정보보호학과 교수)
본 논문은 2020년 국방과학연구소에서 주관하는 미래도전국방기술 연구개발사업(UD210029TD)의 지원으로 수행된 연구임.

을 자동화하고 현실성 있는 훈련을 위해 조직 맞춤형 사이버 공방 훈련을 위한 가상 인프라 변이 생성 프레임워크를 제안한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 프레임워크 제안을 위해 관련된 연구에 대해 설명한다. Ⅲ장에서는 프레임워크의 시스템 구성도와 변이 생성 과정을 설명하고, Ⅳ장에서는 결론 및 향후 연구계획에 대하여 설명한다.

II. 관련 연구

본 장에서는 기존의 사이버 보안 훈련 시스템 훈련장 생성 방법에 대하여 설명하고, 제안하고자 하는 프레임워크에서 활용이 가능한 딥러닝 엔진을 소개한다.

2.1 기존의 사이버 공방 훈련 시스템 훈련장

기존에 이용되는 사이버 공방 훈련을 위한 가상 인프라 생성으로 대표적인 방법으로 SecGen[3], APG(Automatic Problem Generation)[4] 등이 활용되고 다양한 기관에서 사이버 공방 훈련장 설계 및 구축 연구를 진행하고 있다[5].

SecGen은 사이버 공방 훈련자들이 보안 침투 테스트 기술을 배울 수 있도록 취약한 환경을 가진 가상 머신을 생성한다. 가상 머신은 훈련자에게 해킹 대상을 공유하는 효과적인 방법이며 모의 해킹, CTF(Capture-The-Flag), 보안 목적의 교육에 사용된다. 이 시스템은 시나리오 기반으로 생성되기 때문에 가상 머신을 만들게 되면 정적인 환경이 구성되며, 임의의 가상 머신을 생성하기 때문에 훈련자에게 적합한 시나리오를 내어주는 것에 한계가 있다.

APG는 기존 문제들의 매개 변수를 바탕으로 훈련자에게 다양한 공방 훈련 시나리오를 제공하지만, 이는 CTF 대회 목적을 위한 생성기이므로 사이버 공방 훈련 목적으로 만드는 훈련장을 제공하기에는 적합하지 않다.

위의 시스템들 외에도 가상 머신을 이용하여 시나리오 형태의 문제들을 설계하고 구축하는 연구들은 진행하고 있다[5].

2.2 딥러닝 엔진

딥러닝(Deep Learning)은 기계학습의 한 분야로 다량의 데이터를 바탕으로 연속된 신경망 계층 구조를 통해 의미 있는 내용 또는 기능을 배우는 데 강점이 있으며, 기존의 데이터로부터 새로운 데이터를 학습하는 방식이다. 딥러닝 모델은 데이터 학습을 위해 수백 개의 연속된 층을 가지고 있다. 이 층들을 모두 훈련 데이터에 노출하고 다양한 알고리즘을 통해 데이터를 자동으로 학습시킨다[6].

본 논문에서는 가상 인프라 변이 생성 프레임워크에서 활용할 수 있는 두 가지 비지도 학습 딥러닝 엔진으로서 GAN(Generative Adversarial Networks)과 GPT(Generative Pre-trained Transformer)에 대하여 설명한다.

2.2.1 GAN(Generative Adversarial Networks)

딥러닝 엔진 중 하나인 GAN[7]은 생성자(Generator)와 판별자(Discriminator)로 이루어져 있다. 생성자는 학습할 데이터를 입력받아 유사한 새로운 데이터를 생성하고 변이시키며, 판별자는 입력 데이터와 생성된 새로운 데이터를 구별한다. 생성자는 기존의 학습한 데이터와 유사한 데이터를 만들도록 훈련하고, 판별자는 기존 데이터와 새롭게 생성된 데이터를 구별하도록 훈련한다. GAN은 실제 사람의 얼굴 이미지 데이터 셋에서 사람과 유사한 얼굴 이미지를, 실제 글씨 이미지에서 유사한 글씨 콘텐츠를 만들어낼 수 있다[8].

관련 연구로는 GAN을 이용하여 텍스트를 변형시키고 생성해내는 Text-GAN[9]의 연구가 진행되고 있으며, 텍스트 기반의 코드 복제 및 탐지를 위해 만들어낸 SCCD-GAN[10]의 연구도 진행되고 있다.

2.2.2 GPT(Generative Pre-trained Transformer)

GPT는 생성적 사전학습 변환기로 OpenAI 社에서 만든 비지도 학습, 생성적 사전학습이 통합된 인공지능 엔진이다[11]. GPT는 온라인 빅데이터를 이용하여 대용량의 라벨링 되지 않은 데이터로 사전학습 모델을 만들고, 후에 실제 행동을 위한 라벨 데이터로 전이 학습을 수행하는 방법으로 사용한다. 따라서 방대한 학습 데이터 및 매개 변수로 미리 학습된 모델을 바탕으로 다른 학습 모델과는 다르게 적은 용량의 학습 데이터로 원하는 결과를 빠르게 얻을

수 있다. 실제로 GPT를 활용하여 번역기, 언어 관련 문제, 상황에 맞는 글짓기, 요청한 문장에 따른 프로그래밍, 대화 등이 가능하다[12].

III. 사이버 공방 훈련을 위한 가상 인프라 변이 생성 프레임워크

본 논문에서는 능동적이고 효율적인 사이버 공방 훈련장 생성 및 관리를 위해 가상 인프라 변이 생성 프레임워크를 제안하고자 하며 그 구성도는 [그림 1]과 같다.

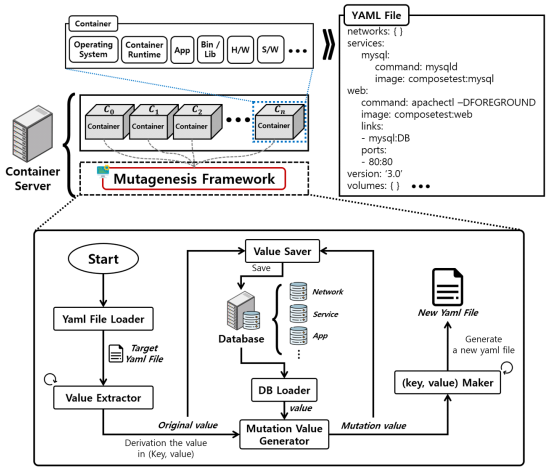

그림 1. 사이버 공방 훈련 가상 인프라 변이 생성 프레임워크 구성도

사이버 공방 훈련 운영자는 취약점이 존재하는 컨테이너를 마크업 코드로 작성하여 인프라 파일을 구성한다. 마크업 코드에는 여러 형태가 존재하지만, 본 논문에서는 Key와 Value로 이루어져 있는 YAML[13] 파일을 사용한다.

YAML 파일이 생성되면 해당 파일에서 각 코드의 역할(시스템 설정, 네트워크 설정, DB 설정, 스토리지, 추가 요구 S/W 등)에 따라 분류한다. Key와 Value 쌍에서 'Value Extractor'로부터 Value를 추출하여 데이터베이스에 저장하고 데이터셋을 확보한다. 충분한 학습 데이터가 확보되면 딥러닝 엔진의 'Mutation Value Generator'가 'DB Loader'를 통해 학습된 데이터를 가져와서 요구하는 파라미터 값과 함께 새로운 Value를 만들어내고 변이된 Value를 다시 데이터셋에 추가함과 동시에 $(Key, Value)$ 쌍을 만들어주는 'Maker'를 통해 결합하여 새로운 YAML 파일을 얻어낸다. 새로운 YAML 파일을 바탕으로 변이된 컨테이너 환경이 구성되며 운영자는 훈련자에게 이를 활용하여 새로운 사이버 공방 훈련환경을 제공할 수 있다.

본 프레임워크 내 YAML 파일 변이 생성 과정은 [그림 2]와 같다.

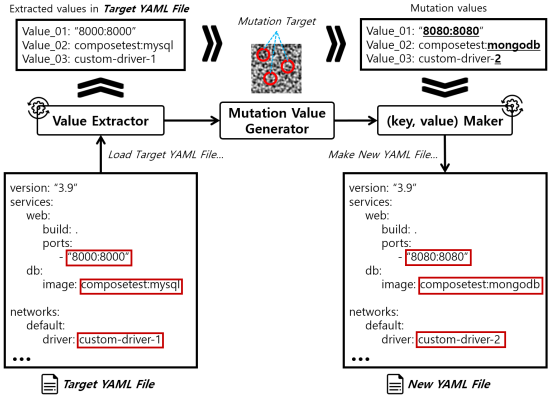

그림 2. YAML 파일 내 Value 추출 및 변이 과정

우선 'YAML File Loader'를 통해 컨테이너 서버 내 다양한 컨테이너 환경 구성 파일 중 하나를 선택하여 가져온다. 이후 'Value Extractor'를 통해 $(Key, Value)$ 쌍에서 Value를 추출하여 변이시킬 준비를 한다.

본 예시에서는 네트워크 서비스 구성 레이블 중 포트 번호와 데이터베이스 타입, 네트워크 드라이버 Value에 대해 변이하는 것을 보여준다.

추출된 다양한 Value 및 기존에 미리 학습된 다양한 Value를 바탕으로 'Mutation Value Generator'에서 새로운 변이 Value를 생성하고, 'Maker'를 통해 기존 Key와 변이된 Value를 결합하여 새로운 YAML 파일을 만들게 된다. 최종적으로 새로운 YAML 파일을 토대로 새로운 환경의 인프라가 구축되어 훈련자에게 새로운 사이버 공방 훈련환경을 제공할 수 있다.

IV. 결론

오늘날 정부와 주요 기업에서는 효과적인 사이버 공방 훈련을 위한 가상 인프라 구축에 많은 인력과 자원을 투자하고 있다. 하지만 제한된 자원과 급변하는 사이버 공격에 실시간으로

대응할 수 있는 인프라가 충분히 구축되지 않아 훈련에 어려움을 겪고 있다.

본 논문에서는 조직 맞춤형 사이버 공방 훈련을 위한 가상 인프라 변이 생성 프레임워크를 제안하였다. 이는 급변하는 사이버 공격에 대응하는 훈련 프로그램 내에 가상 환경의 인프라를 구축하고 사이버 공방 훈련 인프라의 변이 생성을 자동화하는 모델로 활용이 가능할 것으로 기대된다. 향후 연구를 통해 딥러닝 엔진이 코드를 학습하고 필요한 코드를 구현하여 만든 데이터 셋을 바탕으로 인프라를 만드는데 효율적이고 능동적인 클라우드 환경 자동화 플랫폼을 개발하고자 한다.

[참고문헌]

[1] 한국인터넷진흥원, 사이버 위협 동향 보고서 (2022년 상반기), 2022.07.

[2] Hetong JIANG et al., Pandora: A Cyber Range Environment for the Safe Testing and Deployment of Autonomous Cyber Attack Tools, 8th International Symposium (SSCC 2020), Vol.1364, pp.1-20, Feb., 2021.

[3] Z. Cliffe Schreuders et al., Security Scenario Generator (SecGen): A Framework for Generating Randomly Vulnerable Rich-scenario VMs for Learning Computer Security and Hosting CTF Events, 2017 USENIX Workshop on Advances in Security Education, Aug., 2017.

[4] J. Burket et al., Automatic Problem Generation for Capture-the-Flag Competitions, 2015 USENIX Summit on Gaming, Games, and Gamification in Security Education, Aug., 2015.

[5] 최영한 외 8명, 사이버위기 경보 기반 사이버 방어 훈련장 설계 및 구축 연구, 한국정보보호학회 논문지, 제30권 제5호, pp.805-821, 2020.10.

[6] Y. Bengio et al., Representation Learning: A Review and New Perspectives, IEEE transactions on Pattern Analysis and Machine Intelligence, Vol.35, No.8, pp.1798-1828, Aug., 2013.

[7] I. Goodfellow et al., Generative adversarial networks, Communications of the ACM, Vol.63, No.11 pp.139-144, Nov., 2020.

[8] Youngjoo Jo, Jongyoul Park, SC-FEGAN: Face Editing Generative Adversarial Network With User's Sketch and Color, Proceedings of the IEEE/CVF International Conference on Computer Vision, pp.1745-1753, Oct., 2019.

[9] Y. Zhang et al., Adversarial Feature Matching for Text Generation, Proceedings of the 34th International Conference on Machine Learning, Vol.70, pp.4006-4015, Aug., 2017.

[10] K. Xu, Y. Liu, SCCD-GAN: An Enhanced Semantic Code Clone Detection Model Using GAN, 2021 IEEE 4th International Conference on Electronics and Communication Engineering, pp.16-22, Dec., 2021.

[11] A. Radford et al., Improving Language Understanding by Generative Pre-Training, pp.1-12, 2018.

[12] N. Nguyen, S. Nadi, An empirical evaluation of GitHub copilot's code suggestions, Proceedings of the 19th International Conference on Mining Software Repositories, pp.1-5, May, 2022.

[13] O. Ben-Kiki, C. Evans, B. Ingerson, YAML Ain't Markup Language (YAMLTM) version 1.2, YAML Language Development Team, Oct., 2021.