정보보호 분야에서의 사이버 레인지 기술 동향

유재학, 구기종, 김익균, 문대성†
한국전자통신연구원 정보보호연구본부
dbzzang@etri.re.kr, kjkoo@etri.re.kr, ikkim21@etri.re.kr, daesung@etri.re.kr

Trends in Cyber Range Technology in the Field of Information Security

Jaehak Yu, Kijong Koo, Ikkyun Kim, Daesung Moon†
Cyber Security Research Division, Electronics and Telecommunications Research Institute, Daejeon 34129, South Korea

요 약

최근 COVID-19 팬데믹 시대 도래로 ICT 기술 기반의 지능화된 사회실현에 대한 관심이 높아지고 있지만, 사이버 위협의 다변화로 그 범위와 피해 또한 확대되고 있다. 특히, 개인의 민감 데이터뿐만 아니라, 산업체와 공공기관의 사이버 위험성 및 노출은 심각한 문제가 발생할 수 있다. 본 논문에서는 이러한 정보보호 분야에서의 위협행위 등을 탐지, 분석, 대응할 수 있는 교육 프로그램 개발과 전문 인력양성을 위한 사이버 레인지의 국내·외 기술 동향을 살펴보고자 한다. 마지막으로, 더욱 지능화되고 발전하는 사이버 위협으로부터 이를 방지하고 대응하기 위한 사이버 레인지의 발전 방향을 논하고자 한다.

1. 서론

최근 ICT 기술로 대표되는 인공지능, 사물인터넷, 빅데이터, 5G, 정보보안 및 블록체인 등의 발전이 4차 산업혁명 시대를 견인하고 있다. 이러한 기술들의 융합은 산업 및 국방 분야를 비롯한 지능형 범죄 예방, 자율주행, 헬스케어, 드론, 스마트시티 등 다양한 분야에서 이뤄지고 있다. 하지만, 이러한 환경 또는 서비스에서의 무분별한 데이터 활용과 정보융합은 악의적인 위협 및 해킹 등의 사이버 공격에 쉽게 노출될 수밖에 없다[1, 2]. 특히, 사이버 공간에서의 보호 대상 증가, 이전보다 자동화되고 신기술로 무장한 다양한 공격 진화 등으로 보안 패러다임도 빠르게 변화하고 있다. 즉, 사이버 공간의 발전과 모바일 기기의 보급 확대, 연결성 확장, 서비스 간의 활발한 융합 등으로 디지털 전환(Digital Transformation)이 가속화되고 있는 시점에서, 사이버 해킹, 보안패치, 기술 유출 등 다양한 사이버 위협에 직면해 있다.

최근의 연구 문헌 조사에 의하면, 사이버 공간에서의 공격 고도화 및 새로운 기술로 무장한 공격 주기도 짧아지고 있는 추세이다. 따라서, 그 피해를 최소화하기 위한 전문인력 양성과 방어전략 수립에 대한 연구가 중요시되고 있다.[1, 2, 3]. 특히, 사이버 환경에서의 보안 역량을 강화할 수 있는 교육 프로그램 개발과 인력양성을 위한 사이버 레인지(Cyber Range)에 대한 필요성이 증가하고 있다. 현재까지의 사이버 레인지는 전문가의 경험에 의존한 시나리오 기반의 방식이 일반적이며, 실 환경을 반영한 보안체계 및 이기종 네트워크 등을 고려한 훈련과는 거리가 멀었다. 즉, 새로운 사이버 공격 도구, 복합적인 공격, 빠르고 다양하게 변화하는 환경을 고려한 대응 및 방어 훈련이 어려운 실정이다. 그럼에도 불구하고, 이러한 사이버 레인지 기술은 국내·외의 학계와 정부를 중심으로 활발히 연구 및 개발되고 있다[3, 4].

최근에는 사이버 공격이 AI(Artificial Intelligence)와 기술을 접목한 양상으로 발전하고 있다[5, 6]. 특히, 딥러닝(Deep Learning) 학습 및 분석에 기반한 사이버 공격이 자동화·지능화·고도화되어 공격 범위와 그 피해가 확대될 수 있다고 보고하고 있다[5]. 따라서, 사이버 레인지는 훈련 목적과 도메인 환경, 다양한 공격 시나리오에 대한 자율적인 생성과 선제적 방어 훈련으로 보안 역량 강화를 고려해

† Corresponding author

야 한다. 또한, 방어 훈련에서는 사이버 공격에 대한 즉각적인 탐지와 대응 및 분석과정을 순환적으로 재훈련하고 점진적으로 갱신할 수 있는 과정을 포함하는 것이 바람직해 보인다.

본 논문에서는 사이버 레인지의 국내·외 기술 및 연구 동향을 자세히 살펴보고, 향후 발전 방향에 대해 논하고자 한다.

2. 관련연구

COVID-19 팬데믹 시대의 도래로 원격수업 및 재택근무 등이 확대됨에 따라 디지털 환경과 서비스들을 이용하는 생활로 빠르게 변하고 있다. 이러한 사회적 변화로 물리 세계와 사이버 세계의 경계가 더욱 모호해져, 불법적인 정보 유출과 위협으로부터의 대응은 필수적인 기술로 큰 관심을 받고 있다. 특히, 전 세계 정부는 지능적인 사이버 공격으로부터 중요한 국가 인프라를 방어하고, 국민의 안전과 생명을 보호하기 위해 노력 중이다. 또한, 대응 강화를 위한 관련 법률을 정비하고 연구 및 기술개발, 전문인력을 양성하기 위해 국가 예산을 증대하고 있는 실정이다.

가트너(Gartner)[7]의 Hype Cycle For Security Operations 2021에 의하면, 2017년 AI 기술을 활용한 사이버 공격 위협 및 시뮬레이션(BAS, Breach and Attack Simulation) 기술이 처음 등장하였고, 연평균 37.8%의 고성장을 예측하였다. BAS는 실시간으로 공격 시뮬레이션 실행 및 방어기술의 효과성을 평가하는 과정을 자동화함으로써, 침투 테스트 및 모의 해킹 이슈를 극복하기 위한 위험관리 기술이다. 이러한 BAS는 미국과 유럽을 중심으로 AI 기반의 모의 해킹을 통한 중요 국가시설인 전력 및 철도 등의 보안성을 강화하는데 활용되고 있다. 침투 테스팅(Penetration Testing)은 ICT 인프라의 네트워크 시스템 보안 상태를 평가하고 보안 위협과 취약점을 의도적으로 공격하고 이를 제거하기 위한 방법이다[7, 8]. 가트너에 따르면 최근 침투 테스팅 기술이 자동화되고 있으며, 기업 또는 기관의 보안 프로세스상의 문제점들을 정의하고, 기술 장애, 취약점을 찾아 평가 및 시험하여 전반적인 보안 인식을 강화하는데 활용되고 있다. (그림 1)은 가트너의 2021년 Hype Cycle For Security Operations을 나타낸 것이다.

(그림 1) Hype Cycle For Security Operations 2021

3. 사이버 레인지 기술 동향

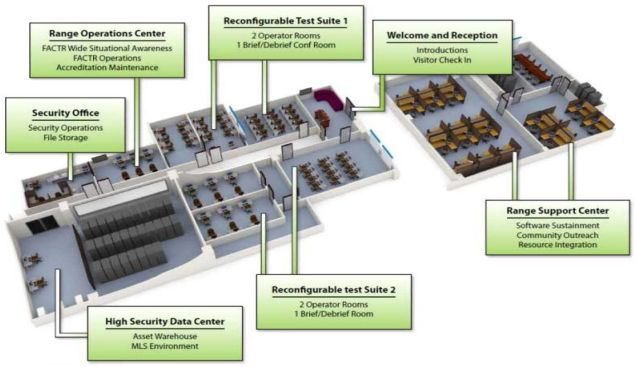
사이버 환경에서의 다양한 위협 등으로부터 안전을 보장할 수 있는 보안 역량 강화와 전문인력 양성을 위한 사이버 레인지는 필수적 기술 요소로 자리매김하고 있다. 본 절에서는 국내·외 사이버 레인지 연구 및 기술 동향을 살펴보고자 한다.

한국인터넷진흥원(KISA)의 사이버보안인재센터는 정보보호 분야의 인력양성을 목표로 시큐리티짐(Security-Gym)이라는 사이버 레인지를 운영 중이다[9]. 시큐리티짐은 이스라엘의 사이버짐(Cyber-Gym)과 미국의 NCR(National Cyber Range) 등을 참조하여 구축하였으며, 실제 환경을 모사한 가상 사이버 환경을 제공하여 훈련을 실시하고 있다. 시큐리티짐은 민간 및 공공을 비롯한 학생, 군인 등 다양한 인력을 대상으로 초급부터 고급 역량을 키울 수 있는 양방향의 공격과 방어 훈련 등을 수준에 맞춰 실시하고 있다. (그림 2)는 KISA의 사이버보안인재센터에서 운영 중인 시큐리티짐 내부 전경과 실전형 사이버 훈련 모습이다.

(그림 2) 시큐리티짐의 실전형 사이버 훈련 모습

미국 국방부 산하의 NCR은 실제 환경을 모사한 가상의 사이버 환경을 구축하고, 다양한 사이버 공격 및 취약점 분석, 대응 방안 등의 프로세스를 훈

련하는 사이버 레인지이다[2, 10]. NCR은 DARPA (미국 방사청)의 요청에 따라 개발하고 미국 국방부 획득 프로그램 및 CMF(Cyber Mission Force)를 지원하기 위한 폐쇄 루프 시스템 구조로 개발하였다. 최근에는 미군의 사이버 작전 테스트와 훈련 및 임무 리허설 등의 정보를 반영한 사이버 레인지로 활용하고 있다. (그림 3)은 미국 플로리다주 올랜도에 위치한 NCR 사이버 레인지의 시설배치를 나타내고 있다.



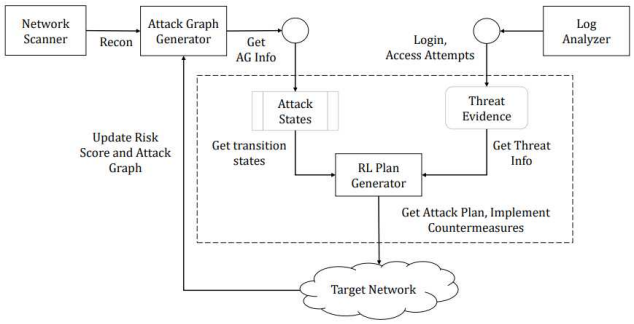
(그림 3) NCR 사이버 레인지의 시설 및 배치도

이스라엘의 사이버짐(CyberGym)은 고객에게 맞춤형 사이버 교육 솔루션을 제공하는 기업이다[11]. 사이버짐에서의 훈련에는 공격과 방어를 모니터링하고 관리하는 화이트팀, 공격을 실시하는 레드팀, 방어를 맡은 블루팀으로 구성되어 있다. 이러한 공격과 방어 훈련이 끝나면 화이트팀은 전 과정에서 수집된 데이터와 결과를 검토하고, 그동안 발견되지 않았던 취약한 영역을 보완함과 동시에 블루팀 대응에 대한 개선점 등을 설명한다. 사이버짐은 전 세계 10개 이상의 훈련장과 400여개 이상의 훈련 시나리오를 보유하고 있으며, 최근에는 가상 클라우드 아레나(Virtual Cloud Arena)로 원격 학습 환경을 제공하고 있다.

(그림 4) 사이버짐 훈련과 교육 설명 모습

(그림 4)에서는 교육생들에게 실제 시스템 환경, 인프라 및 다양한 사이버 공격으로부터 시스템을 방어하는 실습 및 결과 분석 등의 전 과정을 교육하는 모습이다.

미국의 애리조나 주립대에서는 AI를 기반으로 취약점을 자동으로 분석하고 이에 적합한 익스플로잇(Exploit)을 선정하여, 최적 조합으로 공격 시나리오를 생성하고 침투 테스팅을 실행하는 ASAP(Autonomous Security Analysis and Penetration Testing Framework) 연구를 발표하였다[6]. 우선 ASAP에서는 Nessus와 OpenVAS와 같은 상용 네트워크 스캐닝을 실행하고, 스캔 결과로 공격 그래프를 생성한다. 생성한 공격 그래프를 기반으로 자동화된 침투 테스팅을 수행하기 위한 최적 정책을 얻기 위해 DQN(Deep Q-learning Network) 기반의 강화학습 알고리즘을 적용한다. (그림 5)에서는 ASAP 구조와 데이터 흐름을 나타내고 있다.



(그림 5) ASAP 기능 구조 및 데이터 흐름도

4. 결론 및 향후 연구과제

본 논문에서는 ICT 기술로 대표되는 AI와 사이버 공격기술을 접목한 새로운 사이버 공격 및 위협에 대처할 수 있는 사이버 레인지의 연구 및 기술 동향을 살펴보았다. 특히, 딥러닝 기술을 활용한 공격 도구 생성 및 취약성 분석 등으로 사이버 공격이 자동화·지능화·고도화되어 피해 규모와 범위가 날로 확대될 것으로 예상된다. 따라서, 이러한 사이버 공격 및 위협에 대비하기 위한 지능화된 대응기술 연구개발이 필수적이다. 향후 연구과제로는 사이버 레인지에서의 훈련 목적과 훈련생의 수준, 적용 분야의 환경을 적응적으로 반영하고 최적 공격과 방어전략 수립 등을 실행할 수 있는 연구와 시스템 개발이 요구된다.

감사의 글

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임. (No. 2022-0-00961, 자가진화형 AI 기반 사이버 공방 핵심원천기술 개발)

참고문헌

[1] 이주영, 문대성, 김익균, “사이버 공격 시뮬레이션 기술 동향,” 전자통신동향분석, 한국전자통신연구원, Vol. 35, No. 1, 2020. pp. 34-48.

[2] B. Ferguson, A. Tall, D. Olsen, “National Cyber Range Overview,” 2014 IEEE Military Communications Conference, Baltimore, MD, USA, 2014, pp. 123-128.

[3] 김대식, 김용현, “사이버 레인지 운용 방안 연구,” 인터넷정보학회논문지, Vol. 18, No. 5, 2017, pp. 9-15.

[4] I. Somarakis, M. Smyrlis, K. Fysarakis, G. Spanoudakis, “Model-Driven Cyber Range Training: A Cyber Security Assurance Perspective,” Computer Security, pp. 172-184, 2019.

[5] L. Li, R. Fayad, A. Taylor, “CyGIL: A Cyber Gym for Training Autonomous Agents over Emulated Network Systems,” International Workshop on Adaptive Cyber Defense, arXiv: 2109.03331, 2021. pp. 1-8.

[6] A. Chowdhary, D. Huang, J. S. Mahendran, D. Romo, Y. Deng, A. Sabur, “Autonomous Security Analysis and Penetration Testing,” International Conference on Mobility, Sensing and Networking (MSN), Tokyo, Japan, 2020, pp. 508-515.

[7] Gartner, Available online: https://www.gartner.com/en/research/methodologies/gartner-hype-cycle, 25 April 2022.

[8] 강용석, 최국현, 신용태, 김종회, 김종배, 모의 침투 테스트 방법 및 절차의 평가 방법에 관한 연구, 한국정보통신학회 춘계종합학술대회, 2014. pp. 230-233.

[9] Security-Gym, 한국인터넷진흥원(KISA), Available online: https://www.kisa.or.kr/, 25 April 2022.

[10] National Cyber Range (NCR), USA, Available online: https://www.peostri.army.mil/national-cyber-range-ncr, 25 April 2022.

[11] CyberGym, Israel, Available online: https://www.cybergym.com/#section_1, 25 April 2022.