허니팟 자동화 방안: 디지털 트윈과 MITRE ATT&CK TTP 매핑을 통하여

박준영*, 김종현†

*세종대학교 (학부생, 교수)

Automating Honeypots through Digital Twins and MITRE ATT&CK TTP Mapping

Jun-Yeong Park*, Jonghyun Kim†

*Sejong University (Undergraduate student, Professor)

요 약

본 연구는 디지털 트윈(Digital Twin, DT) 기술을 활용하여 기존 허니팟의 한계를 극복할 수 있는 능동형 사이버 기만 시스템인 '디지털 트윈 허니팟(DT Honeypot)'을 설계하고 실험적으로 검증한 것이다. 이를 위해 본 연구는 원본 시스템의 변화를 복제 시스템에 실시간으로 적용하는 디지털 트윈의 실시간 반영적 특성을 허니팟과 결합하고, 그로 인해 생기는 데이터 유출 부담을 최소화하기 위해 허구화 모듈을 작성 및 적용했다. 또한, 공격자의 공격을 실시간 모니터링해 MITRE ATT&CK 프레임워크의 TTP(Tactics, Techniques, and Procedures)와 매핑하는 모듈을 통해 공격 유형에 따른 적절한 계층의 가짜 시스템을 노출하도록 해 공격자에게 노출되는 가짜 자산의 범위를 최소화했다. 본 연구의 실험 결과, DT Honeypot은 기존 정적 허니팟보다 더 높은 안정성과 유연성을 제공하며, 기존 허니팟과 달리 스스로 변화함에 따라 기만 시스템 유지 비용을 줄이고, 디지털 트윈을 사용한다는 점에서 생기는 문제점을 보완해 능동적 보안 시스템으로 기능할 수 있음을 입증했다.

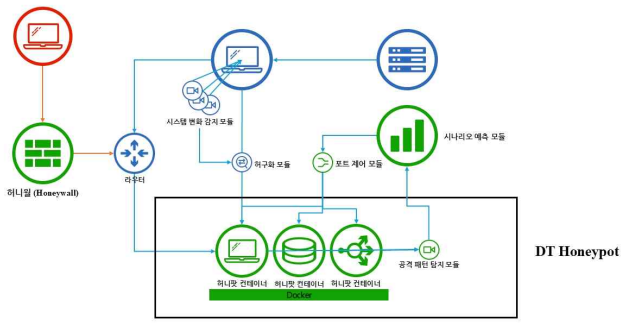
I. 서론

사이버 보안 분야에서 기존의 허니팟 시스템은 단발적이고 정적인 특성으로 인해공격자가 기만 환경을 쉽게 인식할 수 있고, 이로 인해 유지 비용이 높다는 한계를 가진다. 따라서 본 연구는 디지털 트윈(Digital Twin, DT) 기술의 실시간 반영 특성을 활용해 허니팟 업데이트에 드는 자원의 부담을 줄이고, 공격자의 탐색 패턴에 따라 동적으로 기만 환경을 변화시키는 디지털 트윈 허니팟(DT Honeypot)을 설계하고 실험적으로 검증한다. DT는 실시간 데이터를 기반으로 가상 환경을 재현하며, MITRE ATT\&CK 프레임워크의 TTP 매핑을 통해 공격자의 행위 흐름을 예측한다. 본 논문은 이를 통해 기존의 정적 허니팟 시스템보다 높은 안정성과 유연성을 제공하는 능동적 보안 시스템을 구현하고, 그 효과를 평가한다.

II. 관련 연구

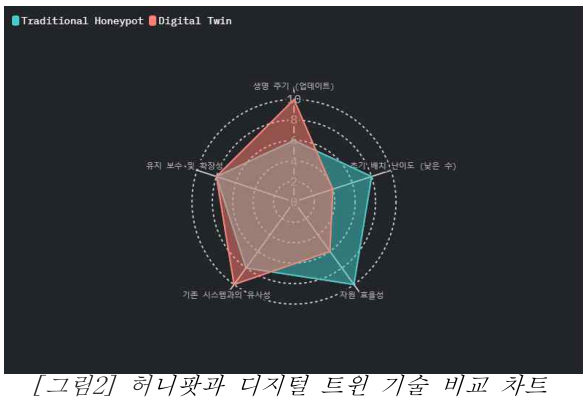
국외에서 디지털 트윈을 활용한 허니팟 시스템에 관한 연구는 새로운 접근법으로 주목받고 있다. Yigit 등은 스마트 항만에서의 외부 공격을 탐지하고 분석하기 위해 디지털 트윈을 활용한 허니팟인 'TwinPot'을 구축하였다[1]. 그러나 이 연구는 이미 사용 중인 디지털 트윈과 디지털 트윈 기반 허니팟이 독립적이라는 점이 한계로 지적된다. 또한, Nintsiou 등은 디지털 트윈을 활용한 실시간 데이터 기반 허니팟 시스템을 제안하였다[2]. 이 시스템은 APT (Advanced Persistent Threat) 공격 탐지 기능을 제공하지만, 공격 완화보다는 위협 분석에 초점이 맞춰진 연구로 평가된다.

이와 같은 한계점들은 디지털 트윈을 활용한 기만 전략이 아직 실용화되기 어려운 이유로 지적된다. Heluany 등은 디지털 트윈과 사이버 기만의 결합 가능성을 탐구하고, 기존 연구들이 대부분 이론적 수준에 그치고 있다는 점을 강조하였다[3]. 이러한 한계를 극복하기 위해,



[그림1] 디지털 트윈 허니팟의 구조 제안안

Suhail 등은 'INCEPTION'이라는 디지털 트윈 기반의 자동화된 기만 전략 조정 플랫폼을 제안 및 실험하였다[4]. 이 플랫폼은 앞선 연구들의 한계점을 보완했지만, 허구화된 디지털 트윈을 기반으로 매번 허니팟을 새로 배포한다는 점에서 실시간 반응성이 떨어진다는 한계를 지닌다. 따라서 기만 환경이 효율적이고 동적으로 변화할 수 있는, 높은 유연성과 적응성을 제공하는 기만 시스템 개발이 필요하다.



[그림2] 허니팟과 디지털 트윈 기술 비교 차트

III. DT Honeypot 시스템

3.1 디지털 트윈과 허니팟 기술 평가

[그림2]는 전통적 개념의 허니팟과 디지털 트윈 기술을 생명 주기, 유지 보수 및 확장성, 기존 시스템과의 유사성, 자원 효율성, 초기 배치 난이도라는 공통 평가 지표로 비교한 차트이다. 디지털 트윈은 실제 시스템과의 실시간 동기화를 기본으로 해 생명 주기(10점)와 시스템 유사성(10점) 면에서 허니팟(각 6점, 8점)을 크게 상회하며, 유지 보수 및 확장성에서 디지털 트윈은 유지 보수가 까다롭지만 확장성에 유리하고, 허니팟은 경량 구조에 의해 유지 보수에 유리하지만, 확장성이 유연하지 못하다는 점에서 유사한 수준(각 8점)을 유지한다. 또한, 허니팟은 시스템 유사성이 떨어질수록 컴퓨터 자원과 인적 자원의 투자가 적으므로 자원 효율성(10점)과 초기 배치 난이도(8점)에서 디지털 트윈(각 6점, 4점)보다 유리하다. 따라서 이러한 평가에 따라 두 기술의 장점을 아우르는 새로운 형태의 기만 시스템인 DT Honeypot을 제안한다.

3.2 DT Honeypot 핵심 요소 분석

DT Honeypot 구현을 위해 본 연구는 '행위 재연', '구조 거짓 재현', '실시간 상호작용'의 세 가지 핵심 요소를 제안하며, 이를 위한 구체적 설계 방안을 마련하였다. 먼저, 원본 시스템의 DB, 시스템 로그, 파일 및 네트워크 정보를 허구화하여 계층별 허니팟을 도커 컨테이너로 구성해 시스템 구조를 거짓으로 재현한다. 동시에, 원본 시스템 모니터링을 통해 실시간으로 실제 시스템의 변화를 허니팟에 반영해 사용자 행위를 재연하는 동적인 허니팟을 구현한다. 또한, 공격 행위를 MITRE ATT&CK의 TTP 정보와 실시간으로 매핑해 탐지된 행위에 따라 해당 계층 컨테이너의 포트를 동적으로 제어함으로써 공격자에게 노출되는 시스템 구성 요소를 유동적으로 조절하도록 설계하였다.

3.3 DT Honeypot 검증 실험 설계

본 연구는 위에서 제안한 DT Honeypot의 핵심 요소들이 실제 환경에서 효과적으로 작동하는지를 검증하기 위해 실험을 설계하였다. 실험

에 사용된 원본 시스템은 WSL2 기반의 Ubuntu 20.04이며, 해당 시스템의 내부 구조와 데이터를 허구화한 뒤, 계층별 허니팟을 도커 컨테이너로 구성하였다. 또한, 원본 시스템의 변화를 실시간으로 감지하여 Docker API를 통해 컨테이너 구성 요소에 반영함으로써, 동적으로 변화하는 허니팟을 구현하였으며, 공격자는 외부 포트를 통해 도커 네트워크에 진입한다. 공격자는 공개된 웹 서버 취약점을 스캔한 후 RCE (Remote Code Execution) 취약점을 이용해 셸을 획득, 내부 DB에 접근해 계정을 덤프하는 시나리오를 따른다. 시나리오 예측 모듈은 공격자의 행위 로그를 기반으로 MITRE ATT&CK 프레임워크에 따라 TTP를 실시간 매핑하고, 예측된 공격 흐름에 따라 자동으로 컨테이너의 포트 노출을 조정한다. 위와 같이 설계한 실험을 바탕으로 컨테이너로의 원본 시스템 변화 반영 여부, 컨테이너 포트 조정 여부 및 정확도, TTP 매핑 정확도를 고려하여 DT Honeypot의 실용 가능성을 평가한다.

IV. 실험 결과

DT Honeypot은 디지털 트윈 기술에 따라 높은 현실성을 나타내면서도 허구화된 데이터로 지속 가능한 기만 환경을 보여주었다. 또한, TTP 자동 매핑을 통해 공격자의 공격 전략을 효과적으로 예측해 공격자의 의심을 줄이고, 더욱 긴 시간 동안 상호작용을 유도할 수 있을 것으로 보인다. 또한, ‘Apache 서버의 노출된 로그 경로 시나리오’와 ‘Nginx 리버스 프록시 설정 오류 시나리오’의 추가적인 공격 시나리오 실험을 통해 다양한 상황에서 성공적으로 TTP를 매핑하고 해당하는 허니팟 컨테이너의 포트 노출을 조정할 수 있음을 확인해 DT Honeypot의 대응 능력을 확인하였다.

V. 결론

본 연구는 디지털 트윈 기술을 허니팟에 적용하여 고현실성 허니팟을 구축하고, 원본 시스템의 변화를 스스로 적용 및 업데이트하는 동적 허니팟을 구체화하였다. 더불어 MITRE ATT&CK 기반 TTP 매핑을 통해 공격자의 행위 흐름을 예측해 이에 맞는 기만 자산 컨테이너를 자동으로 노출함으로써 기존 허니팟의 정적 한계를 극복했다. 또한, 기존 연구들이 디지털 트윈과 허니팟을 따로 인식한 것과 달리 두 기술을 하나로 통합하면서 디지털 트윈 기반 허니팟의 새로운 방향성을 제시하였다. 이를 통해 디지털 트윈이 차세대 사이버 기만 기술의 핵심 요소로 기능할 수 있음을 확인하였다. 기존의 상용 허니팟과의 비교 분석을 통한 정량적으로 평가하고 공격 시나리오 적응 능력을 검증한다면 디지털 트윈 허니팟의 가용성을 확인할 수 있을 것이다.

[참고문헌]

[1] Yigit, Y., Kinaci, O. K., Duong, T. Q., & Canberk, B. (2023). TwinPot: Digital Twin-assisted Honeypot for Cyber-Secure Smart Seaports. 2023 IEEE International Conference on Communications Workshops (ICC Workshops), 740 - 745.

[2] Nintsiou, M., Grigoriou, E., Karypidis, P. A., Saoulidis, T., Fountoukidis, E., & Sarigiannidis, P. (2023). Threat intelligence using Digital Twin honeypots in Cybersecurity. 2023 IEEE International Conference on Cyber Security and Resilience (CSR), 530 - 537.

[3] Heluany, J., Amro, A., Gkioulos, V., & Katsikas, S. (2024, April). Interplay of Digital Twins and Cyber Deception: Unraveling Paths for Technological Advancements. 2024 IEEE/ACM 4th International Workshop on Engineering and Cybersecurity of Critical Systems and 2024 IEEE/ACM Second International Workshop on Software Vulnerability (EnCyCriS/SVM), 20 - 28.

[4] Suhail, S., Iqbal, M., & McLaughlin, K. (2024). Digital-Twin-Driven Deception Platform: Vision and Way Forward. IEEE Internet Computing, 28(4), 40 - 47.