네트워크 핑거프린팅을 이용한 OT 위협탐지 구조 설계

김민수*, 유영록**, 최경호**, 전덕조***
*목포대학교 정보보호학과
**(주)소울소프트
***(주)씨큐비스타
phoenix@mokpo.ac.kr, {young-rok.yu, cyberckh}@soulsoft.co.kr, dejeon@cqvista.com

The Design of OT Threat Detection Architecture using Network Fingerprinting

Minsoo Kim*, Young-Rok Yu**, Kyongho Choi**, Deokjo Jeon***
*Dept. of Information Security, Mokpo National University
**Soulsoft, ***CQVista Inc.

요 약

4차 산업혁명 시대에는 사이버 시스템과 물리 시스템이 연결된다. ICS(산업제어시스템)에서는 기존의 위협 외에 IT 환경에서 발생할 수 있는 보안 위협에 직면하게 된다. 따라서 OT와 IT가 결합되는 환경에서의 위협에 대한 대응 기술이 필요하다. 본 논문에서는 OT/IT 네트워크에서의 핑거프린팅을 추출하고 이를 기반으로 OT 위협을 탐지하는 구조를 설계한다. 이를 통하여 ICS에서의 보안 위협에 대응하고자 한다.

1. 서론

국가 주요 기반/산업 시설인 발전소, 공장, 댐 등에 대한 ICS(Industrial Control System) / OT(Operational Technology)에 대한 사이버 공격은 꾸준히 진행되어 왔다. OT시설이 기존 수동제어 방식에서 전자제어 시스템으로 전환하고 있다. 최근에는 IT 통신망과 시스템을 갖추게 되어, IT 통신망에서 겪에 되는 보안 위협에 노출되고 있다. 특히, 보안에 대한 전문지식이 부족하고, 보안 대응체계를 구축해보지 않은 OT 시설은 사이버 공격의 주요 목표가 되고 있다[1].

국가 기반 시설은 한번 공격을 당해서 운영이 중단될 경우에 그 피해는 엄청나게 크기 때문에 외부로부터 공격을 차단하기 위해 보안을 엄격히 강화하여야 한다. 또한 OT 통신 프로토콜뿐만 아니라 운영환경이 달라서 기존의 IT 보안 기술로는 대처하기 어려운 상황이다. 따라서 운용 가용성 보장을 최우선으로 요구하는 ICS/OT 환경에 적합한 보다 향상된 보안 기술이 필요하다. 특히 OT 시설에서 생각하지 않았던 보안 위협에 대하여 경험이 부족한 경우가 많다. 이러한 변화 속에서 보안 위협에 대응하기 위한 전략이 필요하다.

2. ICS/OT 환경

2.1 IT와 OT

OT는 산업현장의 장비, 자산, 프로세스와 여러 이벤트를 직접 모니터링하고 제어하기 위한 하드웨어 또는 소프트웨어를 말하며, 기존의 IT 기술과는 기능적 차이를 가진다. 즉 OT는 ICS, SCADA, DCS(Distributed Control System) 등의 영역으로 구성된 환경을 제어하는 기술이다[2].

ICS는 시설 장비, 공장 기계, 하드웨어 설비를 제어하는 시스템이다. SCADA는 산업현장을 모니터링하고 제어하기 위한 중앙 집중화된 시스템을 말한다. DCS는 SCADA와 기능적으로 유사하지만 분산시켜 동작을 수행한다.

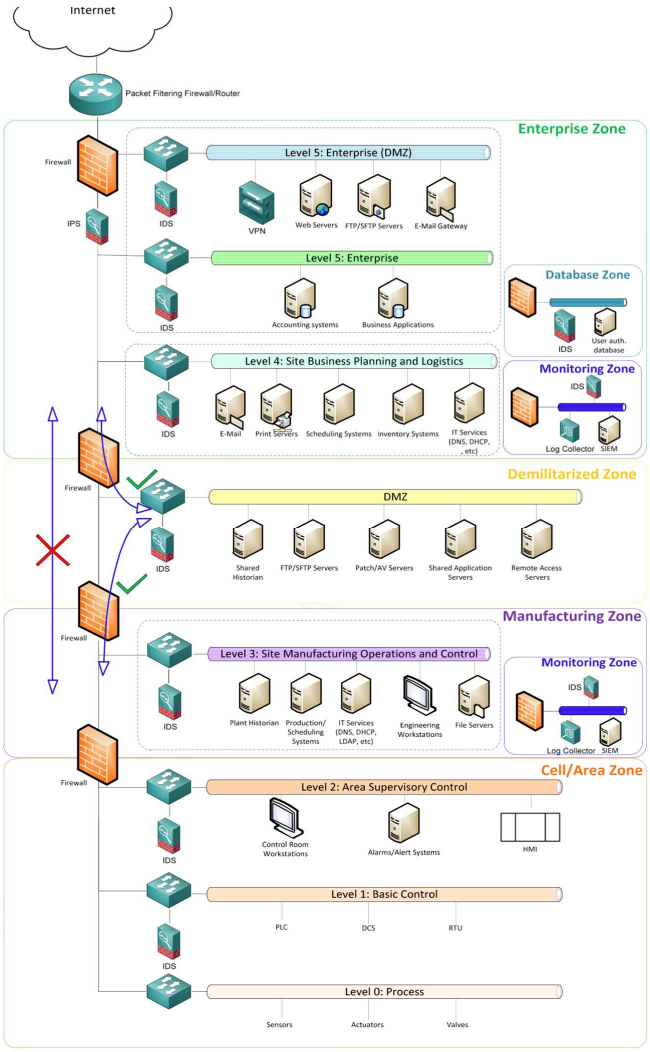
<표 1> IT와 OT의 특징 비교

항목	IT	OT
중요한 보안 요소	기밀성	가용성
위험 노출 대상	데이터	물리적 장비
실시간성	낮음	높고 민감함
구성요소의 수명주기	약5년	약20년
보안 기본 전략	데이터 보호	프로세스 보호
위협 분석 방법	위협성 기반	취약성 기반
프로토콜	글로벌 표준	독자적 특성

IT에서 보안 3요소의 우선순위는 주로 기밀성(confidentiality), 무결성(integrity), 가용성(availability)이다. 그러나 OT에서는 가용성, 무결성, 기밀성 순서로 중요하게 생각한다[3].

2.2 ICS 보안 아키텍처

SANS에서 기존에 발생한 다양한 제어시스템 대상 위협 분석을 기반으로 보안 도메인 기반 모델을 제시하였다. 6개 레벨로 구분하고 각 지역(Zone)에 따라 필요한 기능을 명시하였다[4].



(그림 1) ICS 보안 구조 (출처: SANS)

레벨4와 5는 Enterprise Zone으로 기업 IT 시스템과 응용프로그램이 사용되는 영역이다. 기업 네트워크와 DMZ에 설치되는 방화벽은 반드시 상태 추적이 가능하여야 한다. DMZ와 ICS 네트워크에는 두 개의 방화벽을 설치하여 악성행위를 차단할 수 있어야 한다.

레벨 3은 Manufacturing Zone으로 기관의 목적에 맞게 제어시스템에서 운영 결과를 출력할 수 있도록 한다. 불법적인 ICS 접근을 막기 위해서 별도의 인증과 인가 과정을 거치도록 해야 한다. 인증방식에서는 투 팩터(two-factor) 인증하는 것을 권고하고 있다.

Cell/Area Zone은 레벨 0에서 레벨 2이 해당된다. 레벨 0는 다양한 센서나 제작기기 등과 같이 레벨 1로 부터 명령어를 수신하고 명령을 수행하는 프로세스이다. 레벨 1은 다양한 센서로부터 데이터를 수집하고 알고리즘 등을 통해 명령어를 생성하여 전달하는 PLC, DCS, RTU와 같은 처리 기기가 포함된다. 처리 프로세스를 뜻한다. 레벨 2는 동일한 작업 및 요구사항을 수행하는 지역 내 시스템을 관리하기 위한 제어관리 시스템이다. HMI(Human Machine Interface), 워크스테이션, 경보 시스템 등이 포함된다.

3. OT 위협 탐지 기술 동향

3.1 다크 트레이스(DarkTrace)[5]

다크 트레이스는 프로토콜 기반이 아닌 디바이스가 발생시키는 트래픽을 통해 MITRE 정보를 조합하고 분석에 필요한 정보를 인공지능 기술로 활용하며 위협을 탐지한다. 외부의 TI(Threat Intelligence)를 활용하기보단 내부 디바이스의 행동을 비지도 학습 한 뒤 자체적으로 정상 행위를 가린다. 휴먼 에러, 제로데이 공격, 공급망 공격, 내부자의 정보유출, 악성코드 감염 등을 발견할 수 있다.

3.2 클래로티(Claroty)[6]

클래로티는 많은 연구진을 투입하여 개발하였으며, 90개가 넘는 프로토콜에 적용 가능하도록 되어 있다. SPAN 포토를 통하여 OT 미러링 학습을 할 수 있다. 별도의 에이전트 없이 OT 자산에 대한 프로파일링과 위협탐지를 수행한다. Yara 규칙이나 스노트(snort) 규칙도 지원하고 있다. 또한 실시간 이상 징후를 포착하고 선제적으로 위협 헌팅과 상관분석을 수행할 수 있다.

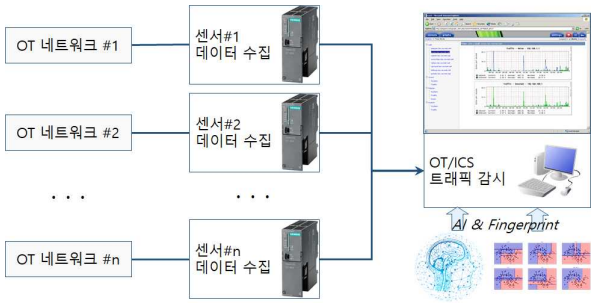
3.3 카스퍼스키랩(KasperskyLab)[7]

카스퍼스키랩에서 제안한 시스템은 팁 패킷 검사를 통해 실시간 프로세스의 통신을 분석하고, 인증되지 않는 네트워크 흐름을 감지한다. 네트워크에 연결된 OT 자산을 관리하고 산업 프로토콜의 커맨

드를 검사한다. 또한 기계학습을 통하여 이상행위를 탐지하는 기능을 포함한다. 실시간 원격 데이터와 과거 데이터를 마이닝하고, 사이버 또는 물리적 위반 사항을 자동으로 검사한다.

4. OT 위협 탐지 시스템 설계

제안하는 OT 위협탐지 시스템의 구조는 그림 2와 같다. 네트워크 트래픽을 수집하는 센서, 네트워크 핑거프린트(fingerprint)를 추출하는 모듈, 그리고 실시간 모니터링과 결과 출력을 수행하는 프로그램으로 구성된다.



(그림 2) OT 위협탐지 시스템 구조

4.1 네트워크 트래픽 수집 센서

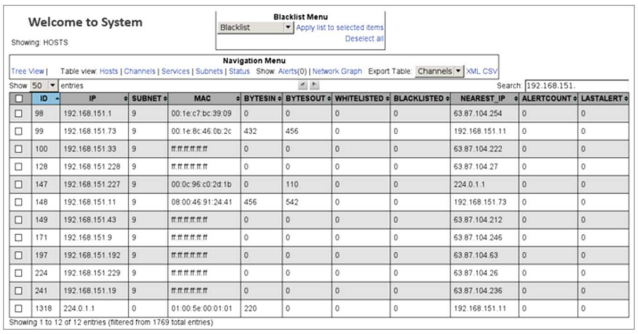
OT 센서 네트워크에서 분석에 필요한 네트워크 트래픽 데이터를 수집한다. 수집 센서는 1G 이상의 고성능 네트워크에서 트래픽을 수집하고 실시간으로 분석 및 저장할 수 있어야 한다. 이러한 센서는 ICS 환경에 적합한 형태의 하드웨어로 구성해야 한다. 또한 트래픽에서 분석이 필요한 통신 세션을 추출하여 데이터를 축약한다.

4.2 네트워크 핑거프린트 추출

네트워크 트래픽은 정상 세션과 비정상 세션으로 구분할 수 있다. 정상 세션은 평상시의 ICS/OT 환경에서 발생하는 트래픽을 설명할 수 있다. 비정상 세션은 취약점을 공격하거나 위협을 가할 수 있는 트래픽을 말한다. ICS/OT 네트워크 트래픽은 일반 IT 네트워크와 다른 특징을 가지며, 이는 이 환경의 핑거프린트로 정의할 수 있다.

4.3 인공지능 기반 위협 분석

정상 세션과 비정상 세션을 기반으로 인공지능 기술을 적용할 수 있다. 딥러닝과 같은 기계학습을 수행하여 ICS/OT 환경의 네트워크 핑거프린트에서 벗어난 트래픽을 감지할 수 있다. 이러한 트래픽에 의미를 부여하기 위해서 결정트리 알고리즘을 결합한다. 트래픽에 대한 모니터링 결과와 탐지 결과는 그림 3과 같이 그래픽 인터페이스를 통해서 보여줄 수 있다.



(그림 3) OT 트래픽 제어 UI

5. 결론

기존의 기반 시설이 인터넷으로 연결되는 환경에서 OT와 IT의 경계가 무너지고 있다. 이러한 환경의 보안 위협에 대비하여 여러 연구가 진행되고 있다. 본 논문에서는 ICS/OT 환경에서 위협을 탐지하기 위한 구조를 제안하였다. OT 네트워크에 맞는 센서를 통해 수집된 네트워크 패킷의 특징을 학습하여 실시간 탐지에 이용할 수 있는 구조이다. 본 논문에서 설계된 내용은 향후 연구를 통하여 구체적인 실증을 할 수 있을 것이다.

Acknowledgement

본 논문은 2020년도 교육부의 재원으로 한국연구재단의 지원을 받아 수행된 지자체-대학 협력기반 지역혁신 사업의 연구결과입니다.

참고문헌

[1] TATA Communications, Effective Threat Management for overcoming cyber physical security challenges, Gartner, 2019

[2] Keith Stouffer, Victoria Pillitteri, Suzanne Lightman, Marshall Abrams, and Adam Hahn, Guide to Industrial Control System (ICS) Security, NIST Special Publication 800-82, NIST, U.S. Department of Commerce

[3] 한은혜, “IT와 OT의 연계 증가에 따른 보안 취약점 개선 방안,” 정보보호학회지, 제30권 제5호, 2020년

[4] Luciana Obregon, Secure Architecture for Industrial Control Systems, SANS Institute,

2015
[5] DarkTrace, https://www.darktrace.com/en/cyber-ai/
[6] Claroty, https://www.claroty.com/
[7] Kaspersky, ttps://www.kaspersky.com/enterprise-security/industrial