ICS/SCADA 시스템에 대한 ICS-ATT&CK 기반의 위협 분석 방안 연구

안명길 이정륜

중앙대학교

lovedew@cau.ac.kr jrlee@cau.ac.kr

Research on Threat Analysis Methodology based on ICS-ATT&CK for ICS/SCADA system

Myung Kil Ahn Jung-Ryun Lee

Chung-Ang University

요 약

폐쇄망으로 운영되어 비교적 안전하다고 인식되는 산업제어시스템인 ICS/SCADA 시스템도 사이버 공격에 노출될 수 있으며, 이에 대한 사전 위협 분석을 통해 능동적인 대비가 필요하다. 본 논문에서는 MITRE에서 제공하는 ATT&CK for ICS 프레임워크를 분석하고, ICS/SCADA 시스템에 대한 ATT&CK for ICS 기반의 위협 분석 방안을 제시하고자 한다.

Ⅰ. 서 론

사이버 공격에 대응하기 위해 많은 노력을 기울이고 있음에도 불구하고, 고도화된 새로운 유형의 공격은 지속적으로 출현하고 있다[1]. 폐쇄망으로 운영되어 비교적 안전하다고 인식되는 산업제어시스템인 ICS(Industrial Control System) 및 SCADA(Supervisory Control and Data Acquisition) 시스템도 사이버 공격에 노출될 수 있으며, 이에 대한 사전 위협 분석을 통해 능동적인 대비가 가능하다.

본 논문에서는 ICS/SCADA 시스템의 특성을 분석하고, ICS/SCADA 시스템에 특화된 선진국의 사이버 보안 테스트베드를 살펴본다. 또한, MITRE에서 제공하는 산업용 제어 시스템을 대상으로 한 ATT&CK for ICS 프레임워크를 분석하고, ICS/SCADA 시스템에 대한 ATT&CK for ICS 기반의 위협 분석 방안을 제시하고자 한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 ICS/SCADA 시스템 관련 특성 및 테스트베드를 살펴보고, Ⅲ장에서는 제안하는 ATT&CK for ICS 기반의 위협 분석 방안을 기술한다. Ⅳ장에서는 향후 연구에 대해 기술하고 결론을 맺는다.

Ⅱ. ICS/SCADA 시스템 특성 및 테스트베드 분석

1. ICS/SCADA 시스템

ICS/SCADA 시스템의 표준 모델이라고 할 수 있는 Purdue 모델은 미국 산업계 및 Purdue대에서 공동으로 정립한 참조 모델(Reference Model)로서, 그 개략적인 구조는 그림 1[2]과 같다. 가장 하부의 레벨 0에 센서, 액츄에이터 등의 물리 장치가 위치하며, 레벨 1, 2에는 공정 수행/스케쥴링/제어를 담당하는 콘트롤러/PLC 등의 장치가 존재한다. 레벨, 1, 2의 경우 정보체계와 전용장치가 혼재되어 있는 영역으로, 하이브리드 영역으로 정의된다. 레벨 3 이상은 정보체계 영역으로, 서버/호스트 등의 컴퓨터 시스템을 통해 산업제어망에 대한 감시 및 관리를 수행한다. 주로 폐쇄망으로 운용된다.

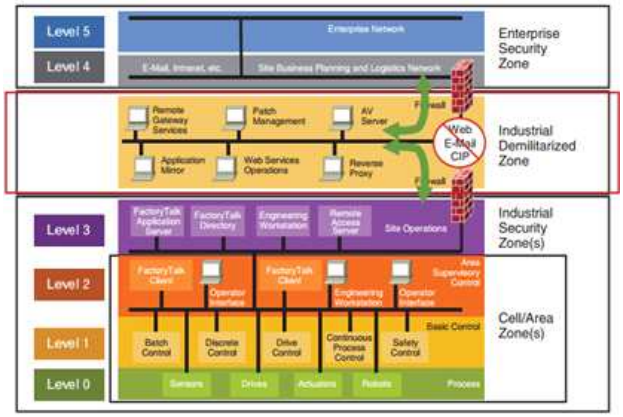

그림 1. Purdue 참조 모델

2. ICS/SCADA 시스템에 특화된 사이버 보안 테스트베드

Queen's Universityt의 ICS/SCADA 테스트베드 프레임워크[3]는 자동화 스크립트를 통해 인터페이스나 원격터미널을 에뮬레이팅하여 SCADA 네트워크를 모사한다. 물리적인 하드웨어와의 상호작용을 지원하여 스마트 그리드, 화력 발전소 등 다양한 시나리오에 적용할 수 있다.

QUT(Queensland University of Technology)의 SCADA Cyber Security Laboratory[4]는 세계 최초로 구축된 ICS/SCADA 테스트베드 중 하나로서, 상수도, 변전소, 철도 제어 등 다양한 산업용 시스템의 목업 모델 및 컨트롤러를 배치해 연구를 수행하고 있다.

Claroty[5]는 이스라엘에서 개발한 SCADA 전문 관제체계로서, 방화벽, IPS 등 기존 정보보호장비로는 탐지할 수 없는 ICS/SCADA 체계에 대한 다양한 위협을 모니터링하고 가시화 한다.

Ⅲ. ATT&CK for ICS 기반의 위협 분석 방안

1. MITRE ATT&CK for ICS

MITRE ATT&CK [6] 프레임워크는 Adversarial Tactics, Techniques, and Common Knowledge로서, 사이버 공격 사례를 기반으로 한 공격자의 행위 모델이다. 공격 목적에 해당하는 Tactics과 목적을 달성하기 위한 구체적인 방법에 해당하는 Technique으로 구성되며 매트릭스 형태로 제시된다. 엔터프라이즈, 모바일, ICS 시스템에 대한 각각의 매트릭스를 제공한다.

ATT&CK for ICS 는 전력, 운송 등의 부문에 걸쳐 안전한 산업용 제어 시스템을 설계하기 위해 활용되며, 주요 기관에서 발표한 위협 분석 보고서, 연구논문, 실제 산업 보안 사고를 바탕으로 정의된다. ATT&CK for ICS 매트릭스는 그림 2와 같다.

Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
I/O Image		Block Serial COM	Modify Parameter	Loss of Control

그림 2. ATT&CK for ICS의 Tactic과 Technique 일부

Inhibit Response Function Tactic은 프로세스 및 제품에 대한 보호 수단을 방해하기 위한 목적으로 정의된다. 인명 손실, 장비 파괴 및 생산 중단을 위한 안전 조치가 비정상적으로 동작하도록 유도한다. 알람 경보 및 응답을 방해하는 것을 목표로 하며. 공격자는 시스템 논리를 수정 또는 업데이트하거나 서비스 거부로 응답을 완전히 막을 수도 있다. 프로그램, 논리, 장치 및 통신의 예방, 파괴, 조작 또는 수정이 발생할 수 있다.

관련 Technique들은 이러한 목적을 달성하기 위한 구체적인 방법들을 기술한다. Alarm Suppression Technique은 위급 상황이 발생한 경우 운용자에게 알람을 주기 위한 경보 기능을 방해하기 위한 공격 방법이며, Block Command Message는 명령의 실행을 방해하기 위해, 명령 메시지가 전달되지 못하도록 차단하는 공격 방법으로 구성된다.

2. ATT&CK for ICS 기반의 위협 분석 방안

산업용 제어 시스템이 폐쇄망으로 운용된다고 하더라도, CD나 USB 같은 내부 장비 인터페이스를 통해 악성코드가 유입될 수 있다. 또한, 유지보수를 통한 침투나 공급사슬(Supply Chain)을 통해 악성코드의 유입도 가능하다. 이러한 취약성에 의해 사이버 공격에 노출될 수 있으며, 사전 위협 분석을 통한 능동적인 대비를 수행해야 한다.

산업용 제어 시스템에 ATT&CK for ICS에서 제시하는 다양한 공격 목적과 공격 방법을 수행하여 사이버 보안을 위한 공격 에뮬레이션을 수행할 수 있다. 하지만, 현장에서 실제 운용하고 있는 ICS/SCADA 시스템에서 이를 수행하는 것은 많은 제약이 따른다. 따라서, ICS/SCADA 시스템의 가상화는 필수적이다.

이를 위해, 디지털 트윈(Digital Twin)[7][8] 개념이 필요하며, ICS/SCADA 시스템에 대한 디지털 복제로서, 수명주기 전체에 걸쳐 대상 객체 요소들의 속성/상태를 유지하고 실제와 동일하게 동작할 수 있는 가상의 환경을 구축해야 한다. 이를 기반으로 다양한 위협 분석 및 모의 실험을 수행할 수 있으며, 현재 Purdue 참조모델 기준 레벨에 따른 점진적인 가상화를 위해 노력하고 있다.

ICS/SCADA 시스템 테스트베드를 기반으로 ATT&CK for ICS에서 제시하는 다양한 공격 목적과 방법을 활용하여, 그림 3과 같이 위협 분석을 수행할 수 있다.

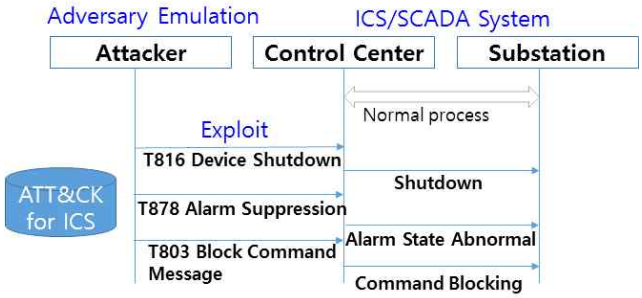

그림 3. ATT&CK for ICS 기반의 위협 분석

Tactic과 Technique을 활용하여 공격 체인을 구성하고, 공격자의 최종 목적을 달성하기 위한 과정을 모의한다. 이러한 사전 위협 분석을 통해 시스템의 안전성은 좀 더 높아질 것이다. 또한, 새롭게 출현하는 위협은 ATT&CK for ICS에 계속 업데이트 되고 있으며 지속적 분석이 가능하다.

Ⅳ. 결론

본 논문에서는 ICS/SCADA 시스템의 특성을 분석하고, ICS/SCADA 시스템에 특화된 선진국의 사이버 보안 테스트베드를 살펴보았다. 또한, ATT&CK for ICS 프레임워크를 분석하고, ICS/SCADA 시스템에 대한 ATT&CK for ICS 기반의 위협 분석 방안을 제안하였다.

무기체계 분야로 확대하여 관련 연구가 지속될 것이며, 위협 분석 및 기술 검증, 실전적 훈련 환경 구축에 활용될 것으로 기대한다.

ACKNOWLEDGMENT

이 논문은 중앙대학교 및 UM17312RD3의 지원으로 수행된 연구임.

참 고 문 헌

[1] AhnLab, ASEC REPORT, Vol.98, 2020.

[2] Pascal Ackerman, Industrial Cybersecurity, Packt, Oct. 2017

[3] Helge Janicke, Kevin Jones, Thomas Brandstetter, 4th International Symposium for Industrial Control System & SCADA Cyber Security Research, Queen's University, Belfast Paperback, 2016

[4] Rodofile, Nicholas, Radke, Kenneth, & Foo, Ernest, Real-time and interactive attacks on DNP3 critical infrastructure using Scapy, 13th Australasian Information Security Conference, pp. 67-70, 2015

[5] The Claroty, Claroty platform for ICS / SCADA Security, Available at https://claroty.com/

[6] MITRE, ATT&CK, Available at https://attack.mitre.org.

[7] Gartner Research, Gartner's Top 10 Strategic Technology Trends for 2017, October 2016.

[8] 이광기, 유호동, 김탁곤, 디지털 트윈 기술 발전방향, KEIT PD Issue Report, Vol.18-9, Sep. 2018.