A Study on Characteristics and Countermeasure of OT/ICS Cyberattack

Taejin Kim [a*], Taewoo Tak [a], Young-Jun Lee [a], In Jung Yoon [b]
[a]*Korea Atomic Energy Research Institute, 111, Daedeok-daero 989beon-gil, Yuseong-gu, Daejeon, Republic of Korea*
[b]*CINAMON, 86, Tongil-ro, Jung-gu, Seoul, Republic of Korea*
[*]*Corresponding author: taejinkim@kaeri.re.kr*

***Keywords :** OT/ICS*, Cyberattack, Cyber Security, Intrusion Detection System

1. Introduction

As advanced technologies have been applied in operational technology (OT) and Industrial Control System (ICS) environments for national industrial and manufacturing facilities, connections between OT and outer systems have gradually increased through some form of interface such as USB connectivity or direct networking connectivity. As ransomware attacks have recently occurred in major semiconductor manufacturers and national industrial facilities, the importance of OT cybersecurity has increased. Also, there have been several cyberattacks in the nuclear field, such as Stuxnet attack on the nuclear facility in Iran [1], a malware-based attack on the nuclear power plant in Japan [2], cyber terrorism to Korea Hydro & Nuclear Power (KHNP) in South Korea [3], a malware infection on the nuclear power plant in India [4], etc.

Recently, in nuclear field, as small modular reactor (SMR) research becomes more active, various operation methods that can have increased connectivity with outside, such as unmanned operation, autonomous operation, and so on, are being studied. Thus, we investigate the characteristics of OT and introduce characteristics and countermeasures of OT/ICS cyberattack based on general industries.

2. Characteristics of Operational Technology (OT)

OT refers to the operational domain of industries including not only ICS, but also the shared domain connected with information technology (IT). This domain includes critical national infrastructure and facilities which can pose significant threats in case for a fraction of a second.

2.1 Comparison between IT and OT

IT primarily concerns itself with data and communication, but OT focuses on behaviors and results. Thus, IT systems are inherently connected together, while OT systems are conservatively connected with closed or proprietary communication protocols. The comparison between IT and OT are described in Table I.

Table I: Comparison between IT and OT

	IT	OT
System	SCM, MES, WMS. etc.	PLC, HMI, Sensor, etc.
Role	Data or Resource Management	Industrial Control
OS	General Purpose OS (Windows, Linux, etc.)	Dedicated OS, Real-time OS
Communication	Standard protocol	Both Industrial /Standard protocol
Maintenance	Easy for patch update	Relatively hard for patch update

2.2 Difference on cybersecurity between IT and OT

Since OT and IT have different security priority and characteristics, we need to cope with different methods of IT against OT/ICS cyberattack. First, in terms of security priorities, OT emphasizes availability while IT emphasizes confidentiality. Second, when there is an incident, OT results in significant physical and economic damage, but IT incurs relatively minor economic damage. Third, while there are antivirus products available for IT, applying such products to OT is challenging. These differences on cybersecurity response between IT and OT are represented in Table II.

Table II: Cybersecurity difference for IT and OT

	IT	OT
Security Priority	Confidentiality > Integrity > Availability	Availability > Integrity > Confidentiality
Incident Effect	Minor damages such as operational inconvenience and delay	Large-scale damage such as industrial operation disruptions
Anti-virus	Available for general-purpose antivirus products	Hard to apply for general antivirus products
Network Reqs.	Crucial for overall throughput with some delays	Critical for robustness and real-time with no

	tolerated	delays

2.3 Necessity of cybersecurity for OT

First, vaccines are commonly used for IT, while specialized vaccines should be developed for OT. Second, concerning the support technology lifecycle, while IT receives support for technology every 3 to 5 years, OT faces challenges and longer timelines due to technical issues and software security validation. Third, IT can receive security updates through regular patches, but OT requires patches tailored to its specific characteristics. Fourth, OT equipment is often based on older hardware and software, which can lead to a higher number of security vulnerabilities and make security environment support more challenging. Fifth, security checks are more feasible in IT, whereas in OT, continuous operation 24/7 makes security checks more difficult.

3. Cyberattack of OT/ICS

This section describes cyberattack processes and vulnerabilities for OT/ICS.

3.1 Cyberattack process for OT/ICS

Cyberattack in OT/ICS arise with two ways: a) when they originate from IT environments or b) when unauthorized media are directly connected to OT devices.

While OT environments are generally isolated in closed networks and separated from IT networks through air gaps, there is a connection between IT network and OT management systems. If the IT network is exposed to security threats, network connection and administrator information for OT can be compromised. Furthermore, if unauthorized USBs or unauthorized laptops with mobile phone tethering are connected to OT devices, malicious code can infiltrate through bypass routes.

Once an attacker gains access to the OT environment, the spread of threats occurs rapidly due to the nature of OT systems being outdated and inadequately patched and frequent communication between systems. This can lead abnormal commands in PLCs and DCSs which originated from SCADA and HMI compromised by the attacker.

3.2 Cyberattack vulnerabilities for OT/ICS

The most common vulnerabilities on ICS in 2019 are buffer overflow and improper input validation and improper authentication and access control also occupy a big portion of vulnerabilities on ICS in Figure 1 [4]. Exploitation of vulnerabilities on ICS can lead to arbitrary code execution and unauthorized control of equipment.

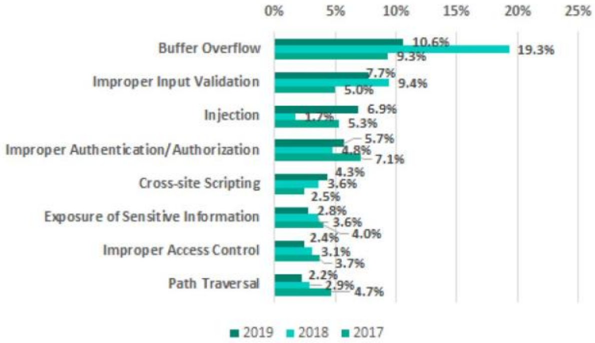

Fig. 1. Vulnerabilities on ICS [4]

The large number of vulnerabilities were identified in 2019: a) engineering software (103), b) networking devices designed for industrial environments (78), c) SCADA/HMI components (63), d) DCS (56), e) PLCs (47) [4]. The percentage of vulnerabilities are represented in Figure 2.

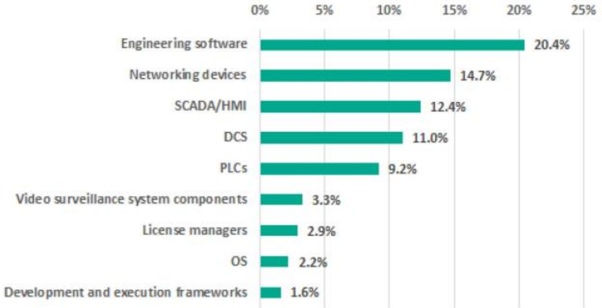

Fig. 2. Percentage of vulnerabilities in 2019 [4]

4. Intrusion Detection System for OT/ICS

This section describes types and open-source solution of intrusion detection system (IDS) for OT/ICS.

4.1 Types of IDS

The IDS is broadly classified network-based and host-based ones.

4.1.1 Network-based Detection

A network-based IDS analyzes network traffic occurring on a network to detect intrusion activities. Typically, a network-based IDS captures and analyzes network packet using network interface cards. This process involves analyzing traffic patterns on the network and identifying patterns associated with malicious code or intrusion behavior.

There are common methods for network-based IDSs:

a) Signature-based detection: This method detects patterns of known malicious code or intrusion behavior. This method is commonly used in technologies like antivirus software.

b) Behavior-based detection: This method identifies characteristic behavioral patterns of malicious code or intrusion behavior. This method is useful when patterns of malicious code or intrusion behavior are not known in advance.

c) Machine learning-based detection: This method uses machine learning techniques to detect malicious code or intrusion behavior. This method involves analyzing patterns of malicious code or intrusion behavior, automatically learning and detecting new patterns.

4.1.2 Host-based Detection

A host-based IDS detects and analyzes activities occurring within a computer. It is typically performed on a computer, where malicious code or intrusions have occurred, by installing security software to detect and analyze unauthorized activities within the computer system.

There are common methods for host-based IDSs:

a) System log analysis: This method records general activities occurring within a computer system. By analyzing the recorded logs, malicious code or intrusion attempts can be detected.

b) File system inspection: This method stores files in the file system, and then security software inspects the file system to identify files associated with malicious code or intrusion attempts.

c) Registry inspection: This method inspects the registry to detect malicious code or intrusion attempts. For reference, the registry is a database in Windows operating systems that stores critical information and can be manipulated to gain control over the system by attackers.

d) Process monitoring: This method monitors running processes to identify malicious code or intrusion attempts which attempts often create new processes to take control of a system.

4.2 Open-Source Solution of IDS

The open-source solutions are investigated by categorizing network-based and host-based ones.

4.2.1 Network-based Open-Source Solution

Here are some notable network-based open-source solutions [5]:

a) Snort: Snort is an open-source IDS developed by Sourcefire in the United States. It provides rule-based detection similar to signature-based detection, identifying malicious packets through packet analysis.

b) Suricata: Suricata is a Snort-like IDS that offers faster and more accurate detection. It supports multi-threading and multi-core processing.

c) Bro: Bro is a network security monitoring system that detects malicious activities by analyzing network traffic. It can efficiently increase detection efficiency by deeply analyzing network traffic.

d) Zeek: Zeek is the former name of Bro, a security monitoring system that enhances network security by analyzing network traffic. Zeek supports various protocols and allows the addition of detection rules through custom scripts.

e) Sagan: Sagan is an open-source Security Information and Event Management (SIEM) system that uses Snort rules to analyze log files for intrusion and anomaly detection.

4.2.2 Host-based Open-Source Solution

Here are some notable host-based open-source solutions [5][6]:

a) OSSEC: OSSEC analyzes various events occurring on a host in real-time, such as file system changes, registry activities, and log files, to detect malicious behavior. It supports multiple operating systems and offers customizable rules and randomization checks.

b) Samhain: Samhain monitors and detects changes in files, directories, processes within the system. It also analyzes system logs and network traffic to identify malicious activities.

c) OpenDLP: OpenDLP monitors internal repositories and networks to detect the unauthorized exposure of sensitive information. It helps prevent unauthorized leakage of important data within organizations.

d) ClamAV: ClamAV detects and removes malicious code from email, file systems, and the web. It employs various malware detection engines to identify a wide range of malicious code like viruses, trojans, and worms.

e) AIDE: AIDE examines the integrity of the file system to detect changes such as file modifications and deletions. It offers features like encrypted configuration files, rule-based checks, and log file analysis.

f) OpenVAS: OpenVAS detects and analyzes vulnerabilities on servers and devices within a network. It provides scan reports to users, and its vulnerability detection relies on a vulnerability database.

g) Wazuh: Wazuh detects anomalies on hosts and manages security information and event.

5. Conclusion

As cyber threats continue to evolve, cyberattacks are also occurring in the nuclear field. With the research into various operational modes such as autonomous or unmanned operation in Small Modular Reactors

(SMRs), the potential for the convergence of Information Technology (IT) and Operational Technology (OT) is increasing. Therefore, the importance of security against cyber threats in the OT environment in the nuclear field is growing. In this paper, we examine the characteristics of OT and cyberattack process and vulnerabilities of OT/ICS. Additionally, we investigate the types and solutions of IDSs for countering cyber threats in the OT/ICS environment.

ACKNOWLEDGEMENTS

This work was supported by a grant from the Ministry of Trade, Industry and Energy in Korea (No. 20224B10100140) and the Nuclear Research & Development Program of the National Research Foundation of Korea, funded by the Korean government, Ministry of Science and ICT (grant number 2020M2D5A1078133)

REFERENCES

[1] https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/

[2] https://securityaffairs.com/21109/malware/malware-based-attack-hit-japanese-monju-nuclear-power-plant.html

[3] https://www.theguardian.com/world/2014/dec/22/south-korea-nuclear-power-cyber-attack-hack

[4] Threat landscape for industrial automation systems, Kaspersky ICS CERT, H2 2019

[5] https://www.comparitech.com/net-admin/network-intrusion-detection-tools/

[6] https://en.wikipedia.org/wiki/Host-based_intrusion_detection_system_comparison