Necessity of Establishing a Security model for Cyber Threat Assessment

Seungmin KIM [a,] Kookheui Kwon [a*]
[a,a*]*Korea Institute of Nuclear nonproliferation And Control(KINAC), Division of Cyber Security, 1418 Yuseong Daero, Daejeon, Korea*
[*]*Corresponding author: vivacita@kinac.re.kr*

1. Introduction

With the increase in cyber threat events and the advancement of cyber attack technology throughout the industry, importance of cybersecurity and cyber threat assessment in nuclear facilities is also increasing. The purpose of this paper is to present the need to develop a threat assessment model to enhance cybersecurity of nuclear facilities [1,2].

2. Typical cyber security model & Necessity of cyber security model

KINAC (Korea Institute of Nuclear nonproliferation And Control), which carries out cybersecurity regulations on nuclear facilities in Korea, evaluates whether critical digital assets of nuclear facilities can be protected from cyber threats. To this end, KINAC collect and analyze threat information on new cyber threats to prepare cyber security threat assessment reports, reset DBT(Design Basis Threat) according to the prepared threat assessment, and evaluate whether the cybersecurity system of nuclear facilities is appropriate through inspection and training. With the advancement of cyber attack technology, more systematic threat assessment strategies are needed, and many security companies are analyzing and preparing for cyber threats through the establishment of cybersecurity models [3]. Typical security models include Cyber Kill Chain and MITRE's ATT&CK framework.

2.1 Cyber Kill chain

Cyber Kill Chain aims to minimize the damage of APT (Advanced Persistent Threat) attacks, and is a security model based on "kill chain", an aggressive defense system that preemptively attacks by detecting enemy missile attacks. Considering that cyberattacks are carried out in a series of procedures, it is a multi-stage defense strategy that mitigates or delays threats by identifying the attack stage from the attacker's perspective and taking appropriate security techniques and measures at each stage. Cyber kill chain are divided into five major stages: Reconnaissance: Infiltrate target infrastructure, secure a stronghold, and conduct long-term reconnaissance. Weaponization and delivery: gather information and gain privileges to achieve attack targets. Exploitation/installation: create and install exploit malware. Commands/Control: Run Commands Remotely. Actions on Objectives: Take actions to achieve their objectives [4].

Figure 1 shows the results of the application of major cyber attacks to kill chains selected by ENISA(European Union Agency for Network and Information Security) [5].

By applying cyber attacks to kill chains, defenders can establish strategies to prevent cyber attacks.For example, DoS (Denial of Service) attacks correspond to the reconnaissance and weaponization stages of the kill chain, so applying mitigation measures equivalent to reconnaissance and weaponization to the CDA to protect DoS attacks can prevent DoS attacks.

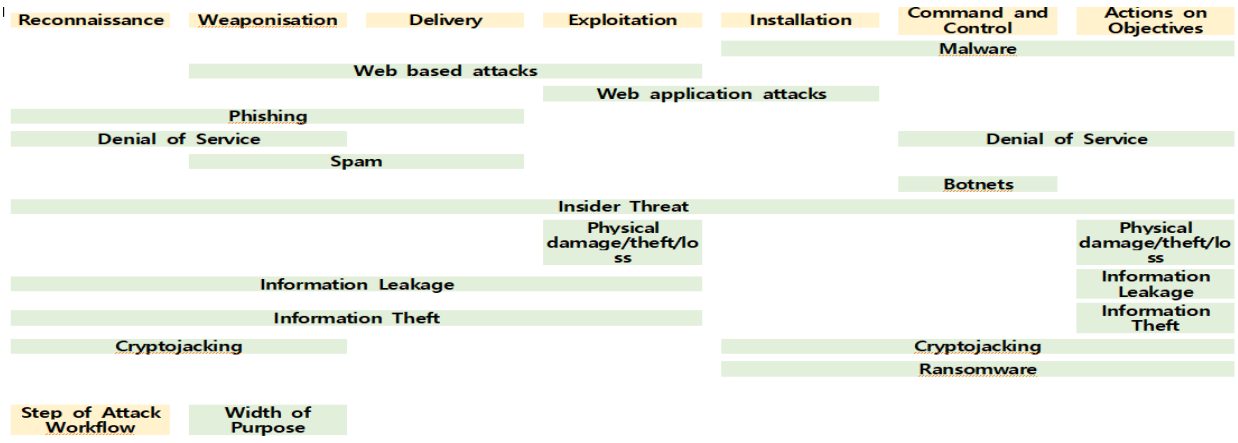
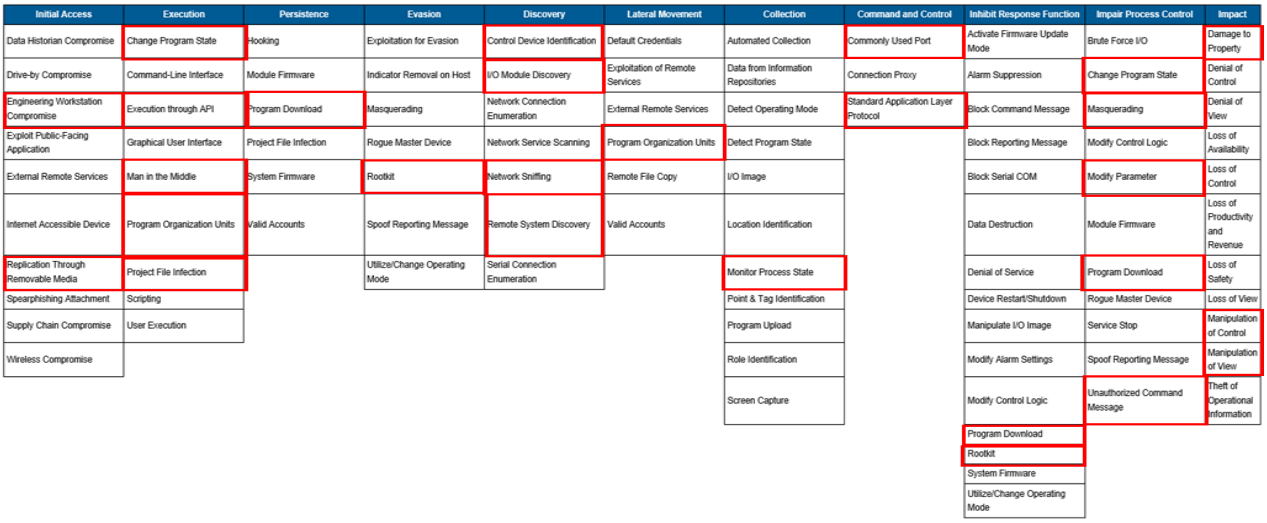


Fig. 1. ENISA's cyber kill chain for each cyber threat



Initial Access	Execution	Persistence	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Data Historian Compromise	Change Program State	Hooking	Exploitation for Evasion	Control Device Identification	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Drive-by Compromise	Command-Line Interface	Module Firmware	Indicator Removal on Host	I/O Module Discovery	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Change Program State	Denial of Control
Engineering Workstation Compromise	Execution through API	Program Download	Masquerading	Network Connection Enumeration	External Remote Services	Detect Operating Mode	Standard Application Layer Protocol	Block Command Message	Masquerading	Denial of View
Exploit Public-Facing Application	Graphical User Interface	Project File Infection	Rogue Master Device	Network Service Scanning	Program Organization Units	Detect Program State		Block Reporting Message	Modify Control Logic	Loss of Availability
External Remote Services	Man in the Middle	System Firmware	Rootkit	Network Sniffing	Remote File Copy	I/O Image		Block Serial COM	Modify Parameter	Loss of Control
Internet Accessible Device	Program Organization Units	Valid Accounts	Spoof Reporting Message	Remote System Discovery	Valid Accounts	Location Identification		Data Destruction	Module Firmware	Loss of Productivity and Revenue
Replication Through Removable Media	Project File Infection		Utilize/Change Operating Mode	Serial Connection Enumeration		Monitor Process State		Denial of Service	Program Download	Loss of Safety
Spearphishing Attachment	Scripting					Point & Tag Identification		Device Restart/Shutdown	Rogue Master Device	Loss of View
Supply Chain Compromise	User Execution					Program Upload		Manipulate I/O Image	Service Stop	Manipulation of Control
Wireless Compromise						Role Identification		Modify Alarm Settings	Spoof Reporting Message	Manipulation of View
						Screen Capture		Modify Control Logic	Unauthorized Command Message	Theft of Operational Information
								Program Download		
								Rootkit		
								System Firmware		
								Utilize/Change Operating Mode		

Fig. 2. Stuxnet analyzed through MITRE Framework

2.2 MITRE ATT&CK Framework

MITRE is a non-profit organization overseeing the vulnerability database CVE(Common Vulnerabilities and Exposures), providing an information-based security framework for cyber attack tactics and techniques called ATT&CK, Adversarial Tactics, Techniques, and Common Knowledge. ATT&CK matrix for ICS consists of 11 tactics (initial access, execution, etc.) and 81 techniques (data historian compromise, external remote services, etc.). Figure 2 shows the application of Stuxnet to the MITRE ATT&CK ICS framework, a cyber threat that has caused physical damage to Iranian nuclear facilities, and the red box is a techniques used in STUXNET.

2.3 Necessity of Cyber Security Model

The first expected effect of establishing cyber security model for nuclear facilities is that it is easy to identify which attack techniques an attacker used at what stage (tactic) based on threat information collected through the built security model. Furthermore, cumulative attack techniques allow defenders to identify threat trends, which can be exploited to refine DBT reassessment and attack techniques. For example, if Tactic and Technique, which have been used most frequently for three years, are Initial access's supply chain compromise, it can assess whether DBT will reset the DBT by identifying whether it currently includes the technologies used in Supply chain compromise.

The second expected effect of establishing cyber security model for nuclear facilities is that it is possible to assess the impact of nuclear facilities on cyber threats. Matching the technical security controls of KINAC/RS-015 with the general mitigation corresponding to the technique corresponding to each tactic can determine whether the technique can be prevented or not. If there is no control corresponding to the general mitigation, the addition of the relevant control may enhance the nuclear facility cyber security system. The following is an example of Stuxnet. The technique used for the initial access (tactic) of Stuxnet is Engineering Workstation Compromise, and in general Mitigation, there are Authorization Enforcement/ Network Allowlists/ Antivirus, Antimalware/ Encrypt Sensitive Information/ Network Segmentation/ Update Software/ Audit / Filter Network Traffic, etc. The controls corresponding to the technical security controls of KINAC/RS-015 are Data flow enforcement, Network access control, Wireless Access Restrictions, Access control for portable and mobile devices, and Auditable vents, etc [3].

The third expected effect of establishing cyber security model for nuclear facilities is that the highly frequent tactics and techniques derived from threat trend analysis can verify whether a defense system has been established through regular inspections and training. It is expected to be able to list the types of cyber attacks that can be applied.

3. Conclusions

This paper suggests the need and expected effectiveness of establishing a security model that reflects the characteristics of nuclear facilities for cyber threat assessment of nuclear facilities, using two representative security models as examples. By establishing a cybersecurity model that reflects the characteristics of nuclear facilities, threat trends can be identified, DBT revision can be made, and effective defense system can be established from cyber attacks. KINAC will utilize previously analyzed cyber threat information to establish a nuclear facility security model.

REFERENCES

[1] Seungmin Kim, KookHeui Kwon, “Cyber Security Strategy for Nuclear Power Plant through Vital digital Assets,” 2019.
[2] INFCIRC/225/Rev.5 (IAEA Nuclear Security Series No. 13), “Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities”, IAEA, Vienna, 2001.
[3] KINAC, KINAC. "RS-015." Technical Standard on Cyber Security for Computer and Information System of Nuclear Facilities (2016).
[4] Tarun Yadav, Rao Arvind Mallari, Technical A pects of Cyber Kill Chain, Third International Symposium on Security in Computing and Communications (SSCC’15). Vol 536, 2015.
[5] ENISA, ENISA Threat Landscape Report (2017), 2017.
[6] MITRE, MITRE ATT&CK framework for ICS, 2020.