A Method to Analyze Threats and Vulnerabilities by Using a Cyber Security Test-bed of an Operating NPP

Yong Sik Kim, Choul Woong Son, Soo Ill Lee*,
KHNP Central Research Institute, Daejeon, 70 1312-gill, Yuseong-daero Yuseong-gu, Daejeon, Korea
**Corresponding author: sooill.lee@khnp.co.kr*

1. Introduction

In order to implement cyber security controls for an Operating NPP, a security assessment should conduct in advance, and it is essential to analyze threats and vulnerabilities for a cyber security risk assessment phase [1, 2].

However, a threat and vulnerability analysis is expected to be difficult for the real facilities of an operating NPP. It might be impossible to perform a penetration test or scanning for a vulnerability analysis because the test may cause adverse effects on the inherent functions of ones. This is the reason why we develop and construct a cyber security test-bed instead of using real I&C systems in the operating NPP.

In this paper, we propose a method to analyze threats and vulnerabilities of a specific target system by using a cyber security test-bed. The test-bed is being developed considering essential functions of the selected safety and non-safety system. The preliminary threats and vulnerabilities are reviewed to determine the attack scenarios for the threat and vulnerability analysis. Test-bed based vulnerability analysis will be conducted by using the high ranked attack scenarios.

2. Development of A Cyber Security Test-bed

The objective of a cyber security test-bed is to measure the performance of a target system while undergoing cyber-attack and check out the result as a vulnerability, and to find out how to implement security controls without affecting the system performance adversely. In this section, considerations and functions of the test-bed are described respectively.

2.1 Considerations for Developing a Test-bed

When developing the cyber security test-bed, security features analysis regarding specific target systems should be conducted first, i.e., main function, data communication, network architecture, known vulnerabilities and identification of critical digital assets (CDAs). After that, attack vector, threats, and vulnerabilities by exploiting those features should be analyzed so that attack scenarios could be developed.

An attack vector is a path or means by which a hacker can gain access to a computer or network server to deliver a payload or malicious outcome [3]. Attack vectors on an I&C system may include attack entry points for code injection or other cyber-attacks, such as CDAs, networks, and portable devices and media that can be attached to CDAs [4]. These attack vectors are also referred in [5].

2.2 Functions of a Test-bed

A cyber security test-bed is composed of the selected safety and non-safety system, including an analysis system. A simplified schematic for the test-bed is shown in Fig.1.

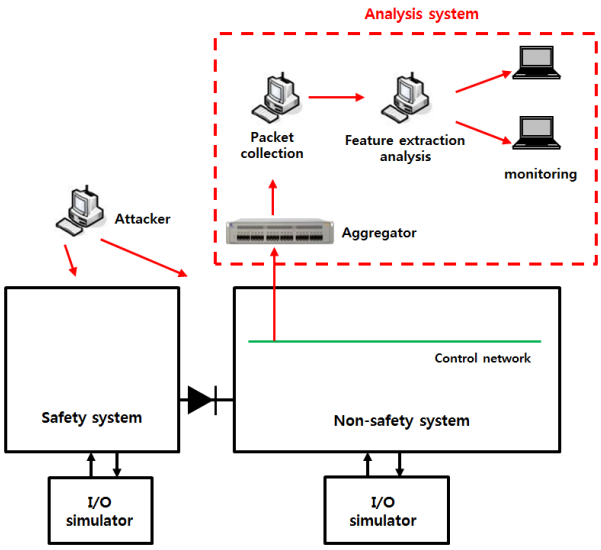

Fig. 1. Overall schematic of the cyber security test-bed

Fig. 1 shows the network connection requirement, which is one-way direction from the safety to the non-safety system, overview of the analysis system, and I/O simulators to model pseudo connection.

According to the example of scenario, it is assumed that an attacker could penetrate the non-safety system via TCP/IP network.

In order to analyze the results of penetration tests and malicious activities effectively, analysis system which is one part of the cyber security test-bed is needed. This system collects the packets of TCP/IP network via an aggregator and saves them for feature extraction analysis and monitoring.

Each I/O simulator could provide the necessary process data and handle control commands, e.g., malfunction, to the safety system and non-safety system respectively.

3. Preliminary Threats and Vulnerabilities Identification

The expected vulnerabilities are basically referred from the ISO/IEC 27005 [6] standard and categorized mainly focusing on the NPP's I&C fields as shown Table I.

Table I: Example of the vulnerabilities of NPP's I&C systems based on ISO/IEC 27005

Types	Representative vulnerabilities	Details
Software	· No or insufficient software testing · Wrong allocation of access rights · Lack of identification and authentication mechanisms like user authentication · Unnecessary services enabled	· Vulnerable function call · Insecure coding · Well-known protocol use · Lack of authentication capability
Hardware	· Lack of efficient configuration change control · Insufficient maintenance/faulty installation of storage media	· No immediate OS patch · Breach of maintenance process
Network	· Lack of proof of sending or receiving a message · Unprotected communication lines and sensitive traffic · Insecure network architecture	· Well-known protocol use · Lack of authentication capability · No secure compartmentation · No port security · No integrity check function

Actually, there are limitations to deal with all the vulnerabilities and threats on the cyber security test-bed based on the specific target systems. Table I shows the representative vulnerabilities and details. The threats corresponding to those of Table I are described as follows,

- Forging of right and theft of information by eavesdrop and sniffing
- Replay attack and theft of information by communication port
- Denial of Service (DoS)
- Vulnerability scan

4. Conclusions

This paper shows the method to analyze threats and vulnerabilities of a specific target system by using a cyber security test-bed. In order to develop the cyber security test-bed with both safety and non-safety functions, test-bed functions analysis and preliminary threats and vulnerabilities identification have been conducted. We will determine the attack scenarios and conduct the test-bed based vulnerability analysis. It is expected that test-bed based vulnerability analysis could make effectiveness how to implement adequate security controls and confirm whether the security controls make adverse impact to the inherent functions.

REFERENCES

[1] NRC regulatory guide RG 5.71, cyber security programs for nuclear facilities, January 2010.
[2] NEI 08-09 Rev.6, Cyber Security Plan for Nuclear Power Reactors, April 2010.
[3] http://searchsecurity.teachtarget.com/definition/attack-vector.
[4] J. G. Song, J. W. Lee, G. Y. Park, K. C. Kwon, D. Y. Lee, and C. K. Lee, An Analysis of Technical Security Control Requirements for Digital I&C Systems in Nuclear Power Plants, Nuclear Engineering and Technology, Vol.45, pp. 637-652, 2013.
[5] NEI 10-09 Rev.0, Addressing Cyber Security Controls for Nuclear Power Reactors, September 2011.
[6] ISO/IEC 27005 International Standard, Information technology - Security techniques – Information security risk management, Second edition, 2011.