Application of the Concept of Intrusion Tolerant System for Evaluating Cyber Security Enhancements

Chanyoung Lee [a], Poong Hyun Seong [a*]
[a] *Department of Nuclear and Quantum Engineering, Korea Advanced Institute of Science and Technology, 291 Daehak-ro, Yuseong-gu, Daejeon, 34141, Republic of Korea*
[*] *Corresponding author: phseong@kaist.ac.kr*

1. Introduction

Digital I&C systems have been developed and installed in operating NPP I&C systems. Cyber security concerns are increasing in the nuclear industry as new cyber-attacks on national infrastructures have become elaborate. One of the major problems is that nuclear industry is in very early stage in dealing with cyber security issues [1]. It is because that cyber security has received less attention compared to other safety problems. In addition, late adoption of digital I&C systems has resulted in lower level of cyber security advancements in nuclear industry than ones in other industries. For the cyber security of NPP I&C systems, many regulatory documents, guides and standards were already published [2]. These documents include cyber security plans, methods for cyber security assessments and comprehensive set of security controls. However, methods which can help assess how much security is improved if a specific security control is applied are not included in these documents. Hence, NPP I&C system designers may encounter difficulties when trying to apply security controls with limited structure and cost. In order to provide useful information about cyber security issues including cyber security enhancements, this paper suggests a framework to evaluate how much cyber security is improved when a specific cyber security enhancement is applied in NPPs.

2. Development of the equation of *Cyber Security Improvement*

The extent of cyber security improvement caused by security enhancement is defined as reduction ratio of the failure probability to secure the system from cyber-attack.

$$\textit{Cyber Security Improvement} = 1 - \frac{P_{Enhanced}}{P_{Current}} \quad (1)$$

Where, $P_{Current}$ is the failure probability to secure the current system from cyber-attack and $P_{Enhanced}$ is the failure probability to secure the current system from cyber-attack.

In traditional cyber security approaches, the failure probability to secure the system from cyber-attack depends on only strategy about resistance to attacks, that is, hardening for protection. However, if the resistance strategy fails, damage may follow and it may cause critical accidents.

In this study, the concept of 'intrusion tolerant system' is applied for not only prevention of cyber-attacks but also limiting the extent of damage and maintaining essential functions [3]. The concept of 'intrusion tolerant' is concerned with flexibility and survivability to cope with the events when the plant faces the unexpected extreme events. For applying the concept of intrusion tolerant system to NPP, the event tree was constructed with some assumptions.

- Only cyber-attacks that can impact to essential functions of target systems are considered in this study.
- System availability is the most important security requirement.
- It is difficult to use the concept of 'back-up system' in complicated system such as I&C system in NPP.
- It is difficult to eliminate the impact of cyber-attack with maintaining the function of attacked system.

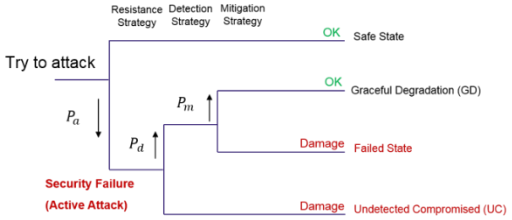

Fig. 1. Example of event tree based on the assumptions

According to behaviors of an intrusion tolerant system, three strategies were presented and described in attack progression which is a manner of attacker methodology [8].

- Resistance strategy: making exploitation of vulnerabilities difficult.
- Detection strategy: detecting an active attack in exploitation phase.
- Mitigation strategy: attempting to limit the extent of damage while maintaining the essential functions.

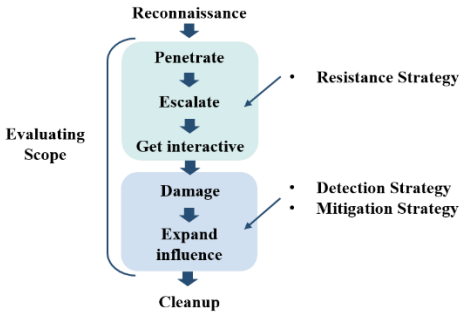

Fig. 2. Attack progression and related strategies

Once cyber-attack happens, it indicates that cyber security is failed (i.e., failure of the resistance strategy in Fig.1). In the case of 'UC state', it is caused when the detection strategy fails, and it will lead to severe accidents without any protective actions. When detection strategy succeeds, there are two possible branches. These two branches are determined whether or not the mitigation strategy succeeds. Thus, the failure probability to secure the system from cyber-attack can be estimated as follows.

$$\mathbf{P_a(1 - P_d P_m)} \tag{2}$$

Where, P_a is the probability that resistance strategy fails. P_d is the probability that a cyber attack is detected in exploitation phase. P_m is the probability that mitigation strategy succeeds.

Cyber security improvement caused by cyber security enhancement can be estimated as follows.

$$\mathbf{1 - \frac{P'_a(1-P'_d P_{m'})}{P_a(1-P_d P_m)}} \tag{3}$$

Where, P'_a, P'_d, and P'_m are the probabilities with respect of enhanced system.

Strategies for detection and mitigation are relatively clear to be defined and have mostly focused on system software modules. However, quantifying the failure probability of resistance strategy is more challenging than quantifying the probability of detection and mitigation strategies. It is because that cyber-attack is unpredictable and attack difficulty has a strong dependence on vulnerable degree of system and attacker factor such as accessibility to information.

In spite of these limitations, there have been several attempts to estimate the difficulty of actions taken by an attacker. Several cyber security researchers observed that cyber security level can be increased as the effort expended by an attacker increases [4]. With this regard, two assumptions were suggested.

- Probability of active attack is inversely proportional to difficulty of actions needed for active attack.
- Difficulty of actions is proportional to effort expended by an attacker.

With these two assumptions failure probability of resistance strategy (= probability of active attack) and effort expended by an attacker are inversely proportional to each other.

$$P_a \propto \frac{1}{\text{Effort expended by an attacker}} \tag{4}$$

The concept of 'time to compromise' was adopted in this work as a measure of effort expended by an attacker [5]. Expected value of 'time to compromise' is a function of existing vulnerabilities in a system and the attacker factor. The number of existing vulnerabilities represents vulnerable degree of a target system and the attacker factor is assumed that it depends on information accessibility. As a measure of effort, 'time to compromise' is inversely proportional to failure probability of resistance strategy (= probability of active attack).

$$P_a \propto \frac{1}{Time\ to\ Compromise(T)} \tag{5}$$

Cyber security improvement of the target system by cyber security enhancement can be replaced by adopting Eq.5 as follows.

$$\mathbf{1 - \frac{T(1-P'_d P_{m'})}{T'(1-P_d P_m)}} \tag{6}$$

3. Case Study

Various kinds of cyber-attack affect security requirements such as integrity or availability in their own ways. With this regard, cyber security enhancement should be evaluated according to possible types of attacks on a specific target system.

In this study, a target system for evaluating cyber security enhancements is the digital plant protection system (DPPS) which is a safety-critical I&C system of NPP. It can actuate a reactor trip signal to protect the core and maintain the plant in a safe shutdown condition. Because of the isolated network architecture and one way data flow, it is hard to compromise critical digital assets (CDAs) of PPS by remote access or control. However, during the maintenance and test activities, external digital devices (EWS: Engineering Work Station) may be connected to the CDAs of PPS and may provide a path for cyber- attacks. In this work, only the case of malware implementation was considered.

According to the results of cyber risk assessments of the PPS [6], possible cyber-attack types were identified in case of malware implementation on CDAs.

- A1. Dos attacks on systems communicating with a system infected by maintenance works. (DoS Attack)
- A2. System shut-down by malware infected by maintenance works. (Improper Command)
- A3. Data modification by malware infected by maintenance works. (Data Modification)

For the case study, an example of cyber security enhancement was suggested and the enhancement includes vulnerability patch and intrusion detection system (IDS).

- Suggested vulnerability patch is for the errors caused by 'flexibility of code', 'format string vulnerability' and 'insecure permission'.
- Suggested intrusion detection system (IDS) is based on 'Snort Rule' algorithm for monitoring malicious activity [7].

Before the suggested cyber security enhancement is evaluated, existing vulnerabilities in the target system were identified. Existing vulnerabilities for the operating system (OS) of sample PPS were searched at the National Vulnerability Database (NVD) [9]. 38 vulnerabilities were founded and classified into corresponding attack types. Among them, the vulnerabilities relative with remote user or leakage information are excluded because of preceded assumptions.

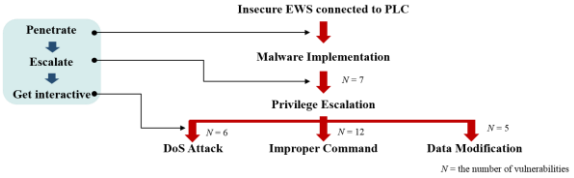

Fig. 3. Existing vulnerabilities in current system

Suggested vulnerability patch applied to enhanced system causes the reduction of the number of vulnerabilities as follows.

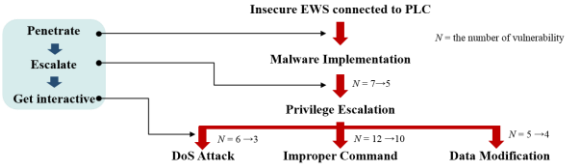

Fig. 4. Existing vulnerabilities in enhanced system

The values of '*time to compromise*' were obtained according to the number of vulnerabilities in current system and enhanced system with assumed same attacker factor, *s*. It is assumed that an attacker has 50% of knowledge of vulnerabilities in the target system (*s* = 0.5).

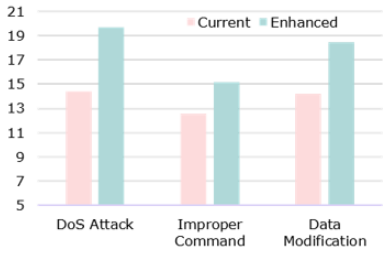

Fig. 5. Time to Compromise (*s*=0.5)

The ratios of $\boldsymbol{P_a}$ and $\boldsymbol{P_a}'$ were obtained by adopting Eq.5.

Table I: The ratios of P_a and P_a' (*s*=0.5)

	DoS Attack	Improper Command	Data Modification
$\frac{\boldsymbol{P_a}'}{\boldsymbol{P_a}} = \frac{\boldsymbol{T}}{\boldsymbol{T}'}$	0.73	0.83	0.77

With increased attack factor, the values '*Time to Compromise*' and the ratios of $\boldsymbol{P_a}$ and $\boldsymbol{P_a}'$ were obtained in same circumstances. It is assumed that an attacker has 80% of knowledge of vulnerabilities in the target system (*s* = 0.8).

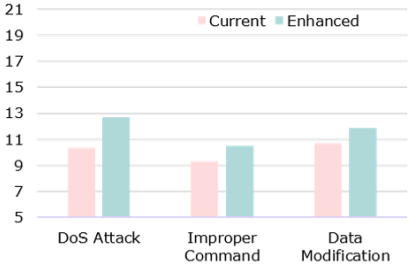

Fig. 6. Time to Compromise (*s*=0.8)

Table II: The ratios of P_a and P_a' (*s*=0.8)

	DoS Attack	Improper Command	Data Modification
$\frac{\boldsymbol{P_a}'}{\boldsymbol{P_a}} = \frac{\boldsymbol{T}}{\boldsymbol{T}'}$	0.82	0.89	0.9

According to comparison between the cases that have different attacker factors, as more information is leaked out, the effect of cyber security enhancement concerned with resistance strategy tends to be decreased.

In the current system, for all kinds of cyber-attack types, probabilities values were assumed as (P_d=0.8 P_m=0.6).

In the enhanced system probability of detection was increased due to IDS based on 'Snort Rule' algorithm. Referring to the experiments using the IDS based on 'Snort Rule' algorithm [7], the probability of detection were obtained in case by attack types. Although same detection algorithm is used, the results can be changed depending on used hardware, software and system state [10]. Hence, further researches are needed for acceptable values, but they suffice as a proof of the concept. In this work, mitigation process was not improved.

Table III: Detection probability and mitigation probability according to attack types in enhanced system

Attack Type	Probability of Detection P_d'	Probability of Mitigation P_m'
DoS Attack	100%	60%
Improper Command	89.8%	60%
Data Modification	93%	60%

With these estimated values, *cyber security improvement*, represents the extent of suggested cyber security enhancement, were calculated according to possible attack types on target system.

The attacker was assumed that has 50% of knowledge of vulnerabilities in the target system in this results (*s* = 0.5).

Table IV: *Cyber Security Improvement* caused by suggested security enhancement (*s*=0.5)

Attack Type	$\frac{P_a{}'}{P_a}$	$\frac{1-P_d{}'P_m{}'}{1-P_dP_m}$	$1-\frac{P_a{}'(1-P_d{}'P_m{}')}{P_a(1-P_dP_m)}$
DoS Attack	0.73	0.77	0.438(43.8%)
Improper Command	0.83	0.89	0.261(26.1%)
Data Modification	0.77	0.85	0.346(34.6%)

The suggested framework assesses how much security is improved when a specific enhancement is applied according to possible attack types. In addition, it can be applied to compare various security enhancement choices and set a numerical target for security level.

4. Conclusions

In order to provide useful information about cyber security issues including cyber security enhancements, this paper suggests a framework to evaluate how much cyber security is improved when a specific cyber security enhancement is applied in NPPs. The extent of cyber security improvement caused by security enhancement was defined as reduction ratio of the failure probability to secure the system from cyber-attack as Eq.1.

The concept of 'intrusion tolerant system' was applied to not only prevent cyber-attacks but also limit the extent of damage in this study. For applying the concept of intrusion tolerant system to NPP, the event tree was constructed with some assumptions. According to the event tree, the failure probability to secure the system from cyber-attack can be estimated by using Eq.2. And *cyber security improvement* caused by cyber security enhancement can be estimated as Eq.3. By comparing current system to the enhanced system, it is possible to estimate how much the system with cyber security enhancements is improved.

The framework to quantify the extent of cyber security enhancement was proposed and implemented for the case study. In this case study, a target system for evaluating cyber security enhancement is the digital plant protection system (DPPS) which is a safety-critical I&C system of NPP. Possible cyber-attack types were identified in case of malware implementation on CDAs of DPPS. For the case study, an example of cyber security enhancement was suggested. Suggested cyber security enhancement was evaluated according to possible types of attacks on the target system using the proposed framework.

However, there are some limitations to estimate the extent of cyber security enhancements because the probability of detection strategy and mitigation strategy are not determined. With further studies, it can provide useful insights to evaluate the extent of cyber security enhancements and it can be applied to compare various security enhancement choices and set a numerical target for security level.

REFERENCES

[1] Baylon, Caroline, Roger Brunt, and David Livingstone. "Cyber Security at Civil Nuclear Facilities Understanding the Risks." London: Chatham House. September 2015.

[2] Song, Jae-Gu, et al. "An analysis of technical security control requirements for digital I&C systems in nuclear power plants." Nuclear Engineering and Technology 45.5 p.637-652, 2013.

[3] Wang, Feiyi, et al. "SITAR: A scalable intrusion-tolerant architecture for distributed services." Workshop on Information Assurance and Security. Vol. 1. 2003.

[4] Scambray, J. and McClure, S., "Hacking Exposed Windows 2000: Network Security Secrets and Solutions," McGraw_Hill, 2001.

[5] Dacier, Marc, Yves Deswarte, and Mohamed Kaâniche. "Quantitative assessment of operational security: Models and tools." Information Systems Security, ed. by SK Katsikas and D. Gritzalis, London, Chapman & Hall p.179-86, 1996.

[6] McQueen, Miles A., et al. "Quantitative cyber risk reduction estimation methodology for a small SCADA control system." System Sciences, 2006. HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on. Vol. 9. IEEE, 2006.

[7] Song, Jae-Gu, et al. "A cyber security risk assessment for the design of I&C systems in nuclear power plants." Nuclear Engineering and Technology 44.8 p.919-928, 2012.

[8] Gao, Wei, and Thomas H. Morris. "On cyber attacks and signature based intrusion detection for modbus based industrial control systems." The Journal of Digital Forensics, Security and Law: JDFSL 9.1: 37, 2104.

[9] National Vulnerability Database (NVD), https://nvd.nist.gov.

[10] Kim, Man Cheol, and Seung Jun Lee. "Important factors affecting fault detection coverage in probabilistic safety assessment of digital instrumentation and control systems." Journal of Nuclear Science and Technology 51.6 p.809-817, 2014.