Development of a Quantitative Method for Evaluating Cybersecurity Incident Response Capability based on the NPP Cyber Kill-Chain Model

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

Recently, due to the expansion of the digital technology application in NPP I&C systems and the increasing number of cyber-attacks on the national infrastructure, concerns about cybersecurity have been raised in the nuclear industry. In response to these issues, the related nuclear cybersecurity legislations have been enacted and cybersecurity regulatory guidelines have been published by several standards and regulatory bodies. The nuclear regulatory bodies require all nuclear facilities to be sufficiently protected from cyber-attacks and to have the capability to detect, mitigate, and recover from the damage [1]. In the nuclear society, several researches have been conducted to develop methods for assessing cyber risks of NPPs or for evaluating the efficacy of cybersecurity controls in NPPs [2].

Recently, the importance of response-based protection strategies has been emphasized based on the fact that it is impossible to identify and prevent all intentional and evolving cyber threats [3]. Considering that NPPs can be exposed to advanced persistent threats targeting national infrastructures, prevention-based protection strategies may not be sufficient. The NIST has published a practical cybersecurity incident handling guide to help organizations to respond effectively and efficiently to the incidents. The IAEA also has developed a guideline for cybersecurity incident response plan for ensuring the availability of safety critical systems and rapid restoration from damages [4]. However, a systematic security incident response strategy for timely detection and mitigation has not been established in the nuclear industry [5]. It is because that the structure of NPP I&C systems is highly complicated and security knowledge is limited, and the dynamics of systems under cyber-attacks is determined by the unpredictable attacker's behaviors. In addition, the incident response is required to maximize long-term benefit rather than short-term benefit.

In order to improve the capability of cybersecurity incident response, a quantitative method for evaluating the effectiveness of embedded response techniques against cyber threats is developed in this study.

2. Analysis

A method for evaluating the cybersecurity incident response capability in NPPs is developed with the integrated perspective of cybersecurity and physical safety. Insufficient or excessive security functions may cause negative effect on system safety or reliability, so the response techniques and their deployment must be designed in a way to ensures the NPP safety. The first step in development is to analyze what stages of intelligent cyberattacks targeting nuclear power plants. The reason for this analysis is that various types of intrusion response techniques were developed to stop each detailed stage of cyber-attacks, and it is important to systematically analyze the effects of those functions.

According to several cyber kill-chain models, the lifecycle of a digital system is modeled as Fig. 1. The security state transition process model consists of normal, penetrated, compromised, recovering, and security failure state [6]. In this model, a state in which a cyber-attack is in progress is detected and recovered back to its normal state by proactive detection and mitigation techniques, or it can be contained and eradicated by containment and incident response techniques. However, if a compromised state remains for a certain period of time without being detected, it goes into the security failure state that cannot be returned to the normal state without system shut-down.

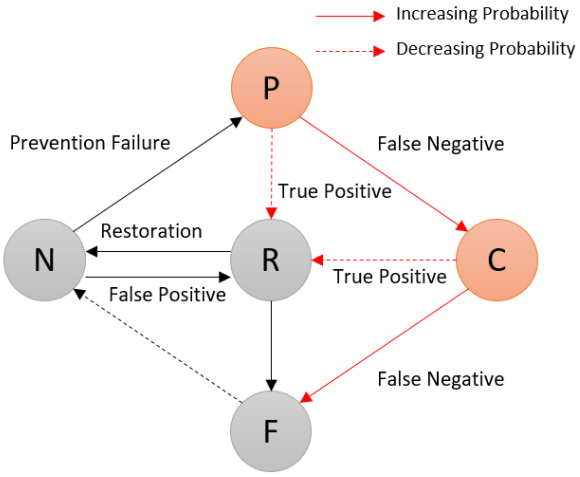

Fig. 1 Security State Transition Process Model

3. Development

The semi-Markov process (SMP) modeling method is applied to estimate the probability of the intrusion response failure when some preventive failures are assumed. The time spent in each state and the state transition rate are in the form of a probability distribution, and it is assumed that the performance of restoration depends on the previous security state.

The probability of security state transitions in the direction of the attack process depends on the performance of the deployed detection techniques and the assumed adversary tactics and techniques [7]. The performance of detection techniques depends on the sets of detection threshold and the amount of computing resources allocated to monitor the certain security conditions [8]. In addition, the likelihood of being detected decreases over time, because intelligent attack patterns tend to collect system information and to disguise as a normal state while the attack is in progress.

The probability of transitioning from the 'Recovering' state to the 'Normal' state or the 'Security Failure' state has a different distribution depending on what the previous state was.

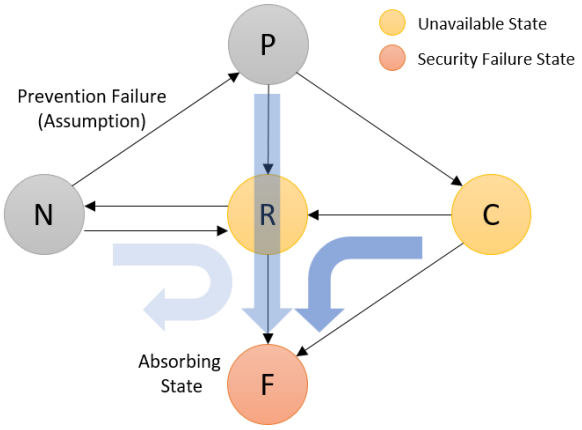

Fig.2 Analysis Using the Semi-Markov Process Model

Using the semi-Markov process model, intrusion response failure probability can be estimated as following equation.

$$\frac{v_F s_F}{\sum_{i\in\{N,P,R,C\}} v_i s_i}$$

In which, v_k is steady state probability of k state in the SMP model, and s_k is the expected sojourn time of the process in state k.

The developed method can be used to maximize the synergy effect of detection technologies that detect an attack not only in the incubation period, but also in the manifestation period. The developed method can also support quantitative dependability analysis which helps to prevent the loss of system availability due to drastic detection thresholds or excessive usage of computing resources. The purpose of future case study is to determine the optimized parameters of each detection technology that can meet both system availability and reliability requirements.

4. Conclusion

A quantitative method for evaluating the effectiveness of cybersecurity incident response techniques is developed with the integrated perspective of system security and plant safety. The intrusion response failure probability was estimated using the semi-Markov process model. The developed method can help assess how much security and safety can be improved by security incident response techniques, and can be applied to select appropriate response techniques among various options in advance. In addition, it can help security designers establish a specific target of effectiveness level that they must achieve. However, the developed method has following limitations. The performance estimation of mitigation techniques needs to be more elaborated, and the effectiveness of propagation containment response techniques was not considered yet. In addition, the active response actions conducted by operators need to be considered.

ACKNOWLEDGEMENTS

This work was supported by the Development of Cyber Security Test and Validation Technology for Nuclear I&C System of the Korea Institute of Energy Technology Evaluation and Planning (KETEP) grant funded by the Korea government Ministry of Trade, Industry and Energy.
(No. 20171510102100)

REFERENCE

[1] US Nuclear Regulatory Commission. "Regulatory Guide 5.71." Cyber Security Programs for Nuclear Facilities, Washington, DC (2010).
[2] Lee, Chanyoung, Ho Bin Yim, and Poong Hyun Seong. "Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept." Annals of Nuclear Energy 112 (2018): 646-654.
[3] Cichonski, Paul, et al. "Computer security incident handling guide." NIST Special Publication 800.61 (2012): 1-147.
[4] International Atomic Energy Agency. "Computer Security Incident Response Planning at Nuclear Facilities TDL005 (NST-038)", (2016).
[5] Zhao, Yunfei, et al. "Finite-horizon semi-markov game for time-sensitive attack response and probabilistic risk assessment in nuclear power plants." Reliability Engineering & System Safety (2020): 106878.
[6] Hahn, Adam, et al. "A multi-layered and kill-chain based security analysis framework for cyber-physical systems." International Journal of Critical Infrastructure Protection 11 (2015): 39-50.
[7] Lalropuia, K. C., and Vandana Gupta. "Modeling cyber-physical attacks based on stochastic game and Markov processes." Reliability Engineering & System Safety 181 (2019): 28-37.
[8] Mitchell, Robert, and Ray Chen. "Effect of intrusion detection and response on reliability of cyber physical systems." IEEE Transactions on Reliability 62.1 (2013): 199-210.