Development of a Framework for Improving the Cyberattack Prevention and Response Capabilities of NPPs

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

The application of digital and automation technologies has raised the cyber security concerns in the nuclear industry. It was proved that cyberattacks are possible in NPPs even the internal network is separated from the external one. Regulatory bodies require all nuclear facilities to have sufficient prevention and response capability. However, difficulties still exist when deciding which security controls are needed and defining appropriate security control requirements [1]. The main reasons are; practical examples for the application of security controls are not available to system designers, and methods that can help assess how much security is improved if a specific control is applied are not included. In particular, the requirement that the performance and reliability of safety-rated digital systems must not be degraded by cyber security controls is not well addressed.

In addition, security prevention measures are not effective enough to protect NPPs from cyberattacks [2]. Prevention measures cannot continue to be effective against evolving cyberattacks and cannot be upgraded immediately due to the NPP operating conditions. In addition, Prevention measures can be breached by information leakage or spiteful insiders. Existing NPP emergency operating procedures are not enough for responding to cyberattacks. In addition, cyberattack response plans form the IT industry cannot be used in NPPs. Therefore, if a cyber-attack occurs in an NPP, the MCR operators are faced with the task of diagnosing uncertain situations and taking an action in a short time without detailed response procedures. In this study, a framework that can improve the cyberattack prevention and response capabilities of NPPs is developed.

2. Improvement of Prevention Capability of NPPs

In the previous study [3], a quantitative method for evaluating the efficacy of security controls for NPP I&C systems is developed based on the intrusion tolerant concept. The intrusion tolerant concept is applied to the evaluation method because availability of system's safety functions is the first priority in the nuclear industry. ''How much the system is intrusion-tolerant" means that to what extent does the system provide the minimum level of safe operation when facing unexpected intrusions. Based on intrusion tolerant strategies, an event tree was constructed, and an efficacy indicator is defined as a reduction ratio of failure probability of intrusion tolerant strategies: the resistance strategy, the detection strategy, and the graceful-degradation strategy. Among these three strategies, quantifying failure probability of the resistance strategy is more challenging than the other two strategies because its relation with the attack-difficulty. The attack-difficulty has a strong dependence on unexpected and abstract factors such as attacker's skills and accessibility to information of the target system. For this reason, the model of mean time to compromise was adopted to estimate abstract variables.

However, one of the other important considerations is that the performance and reliability of safety-grade software system must not be degraded by the cyber security controls. In the previous study [4], a cyber security control V&V process model is developed based on the concept of adaptive focusing testing to improve the application process of cyber security controls more efficiently. In the developed model, fault-proneness of each security control is estimated, and the extent of fault-proneness is considered when conducting verification tests. For the quantitative estimation of fault-proneness of each security control, the security control entropy model is developed by revising the existing software change entropy model. The developed model considers two kinds of complexity dimensions in terms of structural and semantic complexity. The developed security control entropy model also allows for the analysis of fault-proneness analysis at not only security control level, but also digital device level and functional requirement group level.

3. Improvement of Response Capability of NPPs

An IAEA guideline recommends that a course response actions must be planned and taken according to the severity level of plant security state [5]. However, the guideline describes neither how to estimate the current severity state nor how to plan a course of response actions. A security state can be defined as a set of compromised attack conditions, which allows operators to understand how far the cyberattack has progressed. However, security states cannot be observed directly and is also hard to be inferred using the highly uncertain and incomplete cyber anomaly alarms. To overcome the difficulties associated with identifying the current security state, a security state estimation method is developed using hidden Markov Models (HMMs) in the previous study [6]. Since training data sets required for constructing HMMs are hard to be obtained in the nuclear cyber security field, a knowledge-based method

is developed for constructing HMMs that can be optimized online. After a cyberattack is initiated and a series of security alarms are observed, the most suitable HMM could be selected among the constructed HMMs by using an online evaluation module. Using the selected model, a decoding module can estimate the current security state. The architecture of the adopted security state estimation method is illustrated in Fig. 1.

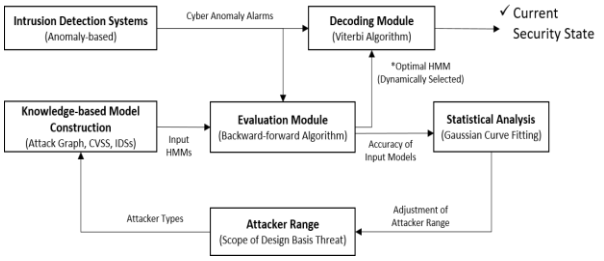

Fig. 1. Architecture of the security state estimation method [6]

Based on the feedback architecture, the selected model and estimated security state could be updated upon the generation of a new security alarm. By using the adopted security state method, the current security state and previous transition path can be estimated even if there are false-negative and false-positive alarm errors. In addition, it can also predict which security failure states can be reached and how long it will take to reach them.

Although the current security state can be estimated, operators may have difficulties in planning cyberattack response actions. The response plan must include taking security and safety response actions and be optimized with a long-term perspective. In addition, the response plan must be adjusted according to dynamic patterns of a cyberattack. In the previous study [7], a security state-based cyberattack response planning method is developed using the Markov decision process model. Based on the temporal response margin analysis, available response actions are modeled as actions that can increase the available response time or decrease the response time required to ensure plant safety. The response reward of an action is quantified as an increase in the response margin time. By modifying the existing action-value function and adopting the Monte-Carlo tree search algorithm, the developed method can help to establish optimal response plans that can maximize the response margin time and minimize the time required for the implementations.

4. Conclusion

Previous nuclear security researches focused on prevention. However, there are still difficulties when it comes to deciding which security controls are needed and to defining appropriate security control requirements for NPPs. The developed methods for evaluating efficacy and fault-proneness of security controls can help assess not only the degree to which system security can be improved if specific cyber security techniques are applied, but also the influence of the security techniques on the target system in terms of system reliability. In addition, it is expected that the suggested method can be applied to select appropriate security controls among various options in advance. Furthermore, by evaluating cyber security techniques quantitatively, the method can also be applied to establish a specific target of efficacy level that system can achieve.

In NPPs, operators may face two problems in planning a course of cyberattack response actions. First, it is difficult to cope with the uncertainty associated with the current security state and attacker type. This difficulty is solved by adopting a security state estimation method developed in the previous study. Second, it is difficult to establish and coordinate response plans. This difficulty is also solved by applying the concept of security state-based response planning. The integration of the adopted security state estimation method and the developed response planning method is expected to enable operators to quickly respond to cyberattacks and protect NPPs from cyberattacks.

ACKNOWLEDGEMENTS

This research was supported by the National R&D Program through the National Research Foundation of Korea (NRF) funded by the Korean Government. (MSIP: Ministry of Science, ICT and Future Planning)
(No. NRF-2016R1A5A1013919)

REFERENCES

[1] 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,” Nucl. Eng. Technol., vol. 45, no. 5, pp. 637–652, 2013.
[2] Y. Zhao, L. Huang, C. Smidts, and Q. Zhu, “Finite-horizon semi-Markov game for time-sensitive attack response and probabilistic risk assessment in nuclear power plants,” Reliab. Eng. Syst. Saf., vol. 201, no. August 2019, p. 106878, 2020.
[3] C. Lee, H. Bin Yim, and P. H. Seong, “Development of a quantitative method for evaluating the efficacy of cyber security controls in NPPs based on intrusion tolerant concept,” Ann. Nucl. Energy, vol. 112, pp. 646–654, 2018.
[4] C. Lee, S. M. Han, and P. H. Seong, “Development of a quantitative method for identifying fault-prone cyber security controls in NPP digital I & C systems,” Ann. Nucl. Energy, vol. 142, p. 107398, 2020.
[5] IAEA, Computer Security Incident Response Planning at Nuclear Facilities. 2016.
[6] C. Lee, Y. Ho Chae, and P. Hyun Seong, “Development of a method for estimating security state: Supporting integrated response to cyber-attacks in NPPs,” Ann. Nucl. Energy, vol. 158, p. 108287, 2021.
[7] C. Lee, Y. H. Chae, and P. H. Seong, “Development of a Cyber Response Strategy Establishment Method for Minimizing the Potential Risk from Cyber-Attacks in NPPs,” in Proceedings of the 12th Nuclear Plant Instrumentation, Control and Human-Machine Interface Technologies, 2021, pp. 1234–1241.