Application of a Model-driven Security State Estimation Method for Cybersecurity Incident Detection and Response in 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 to NPP I&C systems has not only increased the system efficiency, but also raised cybersecurity problems. Regulatory agencies have issued cybersecurity planning guidelines requiring all nuclear facilities to prevent cyberattacks and have sufficient response capabilities [1]. Although several researches have been conducted for assessing the cyber risks of NPPs or evaluating the efficacy of cybersecurity controls in NPPs, there has not been much research on response capabilities. The cybersecurity guidance encourages ongoing management to periodically discover potential vulnerabilities and apply security patches. However, it may take more than several months to apply a patch in NPPs, which may expose many operating digital systems with known vulnerabilities to advanced persistent threats [2]. Since it is impossible to identify and prevent all intentional and evolving cyber-attacks, the preventive cybersecurity plan may not be sufficient. When a cyber-attack occurs and preventive protection fails, responsive protection is the last barrier to keep the plants safe. Without responsive protection, multiple safety barriers, such as automatic protections and operator interventions, can be failed by cyber-attacks. However, NPP cybersecurity plans for responsive protection have not been elaborated yet, and related training and experience are insufficient.

In order to ensure the safety of NPPs under cyber-attacks, the time required from cyber intrusion to damage isolation must be minimized. On the other hand, post-incident response tasks, such as cause analysis and restoration, should be conducted after the plant has been safely shut down. In this regard, it is necessary to develop a system that can support cybersecurity incident detection and initial response process.

2. Analysis

The cybersecurity incident detection and response in a large-scale system is cyclic processes in which a series of decision-makings are conducted repeatedly [3]. Security incident handlers are responsible for monitoring real-time security data to determine what has happened and validating possible security incidents. When the handlers believe that a security incident has occurred, they should rapidly conduct an initial analysis to determine the mitigation scope. If a nuclear power plant is suspected to be under cyber-attacks, the plant must be safely shut down before physical abnormal events occur, and appropriate countermeasures must be taken to prevent the spread of damage [4].

However, the limited observability in cyber environment can degrade the cybersecurity incident detection and response performance [5]. Limitation of the use of advanced security technologies used in the IT field creates multiple blind spots. Information from anomaly detection systems is not intuitive and contains potential errors. Even, some of the monitoring and detection data can be easily lost or manipulated by attackers. Detection through user observation is an "after-the-fact" activity, which may delay response and induce a degree of risk.

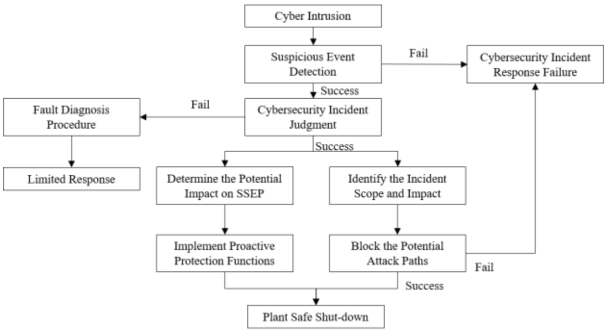
Cyber Intrusion
Suspicious Event Detection
Fail
Cybersecurity Incident Response Failure
Success
Fault Diagnosis Procedure
Fail
Cybersecurity Incident Judgment
Success
Limited Response
Determine the Potential Impact on SSEP
Identify the Incident Scope and Impact
Implement Proactive Protection Functions
Block the Potential Attack Paths
Fail
Success
Plant Safe Shut-down

Fig. 1. The Suggested Cybersecurity Incident Response Flow Chart in NPPs

Given the numerous possible effects, the detection procedures have been designed in the ICS field to detect malicious cyber events as early as possible [6]. The basic actions involved with detection are routine monitoring, inspection, and transition to the mitigation procedures. Each event diagnostic procedure identifies one or more integrity check items which are to be completed in order of subjective judgments. However, detection and diagnostic procedures can also delay the necessary response actions.

3. Development

When observations are limited, model-driven online analysis methods can be used to support the detection and response processes. In a model-driven online estimation approach, knowledge of digital I&C systems and cybersecurity can be used to estimate current security state by correlating real-time data. It can compensate for uncertainty of cyber data and prioritize necessary inspection tasks.

The security state dynamics, which describes evolving security states within cyber environment, can be modeled by attack-graphs based on knowledge of digital I&C system structures and knowledge of cybersecurity. In this study, a quantitative form of security states is defined as a set of compromised security conditions. A set of compromised security conditions can be interpreted as a current progress of an attack against a particular attack target. The conditional dependency attack-graph concept is adopted to reflect the logical dependencies between current security states and feasible transitions [7]. In a conditional dependency attack-graph, exploitation can only be attempted if all pre-conditions are enabled, and the outcome of the attempt determines whether the post-conditions are enabled or not.

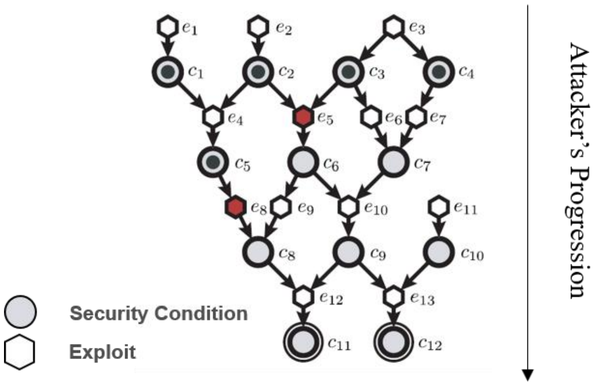

Fig. An Example of Security State [8]

Assuming the state transitions and observations are dictated by probability distributions, the security state dynamic follows a partially observable Markov decision process (POMDP). POMDP is an agent decision process in which it is assumed that the system dynamics are determined by an agent's decision, but the agent cannot directly observe the underlying state. Belief distribution indicates the probability distribution that the current security status is in each security state. The likelihood of various state trajectories with the current belief can be reasoned, which allows to prescribe optimized response actions. The optimal response actions may often include not only defensive actions, but also information gathering tasks that are taken purely because they improve the agent's estimate of the current state, thereby allowing it to make better decisions in the future. The belief is updated through subsequent inspection and observation until the extent of uncertainty of belief distribution within the acceptable range. Although the POMDP algorithm can be used to obtain an optimized set of defensive and observative actions, the extent allowable uncertainty in decision making should vary depending on the situation, and an appropriate level will be determined through further study.

4. Summary and Conclusion

Cybersecurity incident response in large systems is a cyclical decision process that iteratively makes a series of analysis and mitigation actions. In NPPs, security response teams need to make their initial security response actions in time to ensure plant safety while maintaining the system availability. The security state dynamics, which describes evolving security states within cyber environment, is modeled a model-driven security state estimation method. The conditional dependency graph concept is adopted to determine the security state for the next time step based on the current security state and the behavior of the attack. Assuming the state transitions and observations are dictated by probability distributions, the security state dynamic follows the POMDP algorithm. However, the extent allowable uncertainty in decision making should vary depending on the situation, and an appropriate level will be determined through further study.

REFERENCES

[1] US Nuclear Regulatory Commission. "Regulatory Guide 5.71." Cyber Security Programs for Nuclear Facilities, Washington, DC (2010).

[2] Baylon, Caroline, Roger Brunt, and David Livingstone. Cyber Security at Civil Nuclear Facilities: Understanding the Risks: Chatham House Report. Chatham House for the Royal Institute of International Affairs, 2015.

[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] Miehling, Erik, Mohammad Rasouli, and Demosthenis Teneketzis. "Optimal defense policies for partially observable spreading processes on Bayesian attack graphs." Proceedings of the Second ACM Workshop on Moving Target Defense. 2015.

[6] US Department of Defense, Environmental Research Programs. "Advanced Cyber Industrial Control System Tactics, Techniques, and Procedures, ACI TTP", (2018)

[7] Miehling, Erik, Mohammad Rasouli, and Demosthenis Teneketzis. "A dependency graph formalism for the dynamic defense of cyber networks." 2017 IEEE Global Conference on Signal and Information Processing (GlobalSIP). IEEE, 2017.

[8] Miehling, Erik, Mohammad Rasouli, and Demosthenis Teneketzis. "A POMDP approach to the dynamic defense of large-scale cyber networks." IEEE Transactions on Information Forensics and Security 13.10 (2018): 2490-2505.