Development of a Conceptual Framework for Supporting Cyber Situation Awareness Process 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

As the number of cyber attack cases on cyber-physical infrastructures increases, NPPs expanding the application of digital technology are no longer safe. The consequence of cyber attacks on NPPs can be amplified due to their complicated cyber-physical structures. Security defensive mechanism is not limited to preventive mechanism, but includes the detection of already compromised systems and mitigation of their subsequent damages. In safety-critical industries, the importance of response security mechanisms is more emphasized. Responsive security mechanisms have been implemented differently depending on the characteristics and purpose of the industry [1]. For example, In an Industry which regards the safety as top priority, they are designed to keep safety critical systems within available and safe range even in the face of cyber attacks. Recently, several cyber event analysis tools have been developed to support the responsive security mechanisms, and various related studies are on-going. They believe that a successful response depends on understanding of received cyber attacks in systematic and comprehensive manner [2]. When it comes to responding to cyber attacks on NPPs, security and MCR operators will conduct critical decision making together. Therefore, successful response to the cyber attacks heavily relies on their understanding of attacks with perspective of security and safety [3]. In the current NPP digital I&C interface systems, the capability of supporting the understanding of cyber attacks is still limited. There is a lack of capability to monitor cyber data and to transform the data into situation information and to construct shared common understanding between security and MCR operators. In order to solve the issue, a framework for supporting cyber situation awareness (Cyber SA) is developed in this study.

2. Challenges and Requirements for Enhancing Cyber SA Process

The concept of cyber SA is a situation awareness process concerned with intended accidents in the cyber environment [4]. A high level of cyber SA allows human decision makers to identify, to understand, and to anticipate an evolving cyber attack. Theoretically, developing cyber SA is an on going process moving from raw data to information that can guide a decision which information should be focused next. However, there are several challenges in applying the theoretical process to a real cyber environment [2].

- Cyber data to be monitored easily overwhelm the cognitive capacity of human operators.
- An abnormal cyber event has quite different symptoms at different domains.
- The time-line between an attack and its effect is unpredictable.

Although existing approaches rely on automated tools for supporting cyber SA process, these approaches only work at the lower level [5]. Higher level analysis, integrating individual information, is still done manually by human analysts, making the process labor-intensive, time-consuming, and error-prone. A supportive framework should integrate individual security perspectives into a macroscopic perspective in order to enhance Cyber SA process. A framework should be aligned with theoretical SA model to help to infer what intrusions may be going on, what consequence they may have and what actions should be taken.

3. Development of a Supportive Framework for Cyber SA

A framework is developed that integrates individual security perspectives into the macro-perspectives in terms of system processes, digital assets, and cyber attack domains. The interconnection between cross-domains descripted Fig. 1 helps to understand the meaning from one domain and to extend the meaning by correlating with other domains.

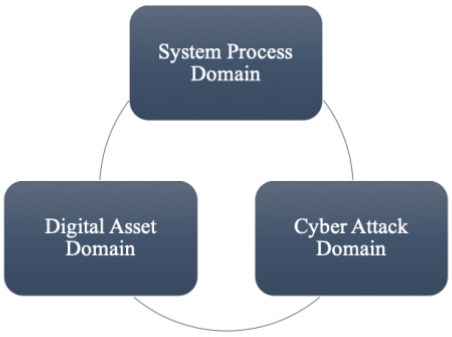

Fig. 1. Cross-Domain Correlation

In which, system process domain is a set of goal-directed (system control or protection) sequential mission flows. Digital asset domain is a collection of

digital assets, network structure and their interdependencies. Cyber attack domain is a logical sequence of malicious actions compromising and disrupting data. In modeling system process domain, It is assumed that the sequential flow within the processes can be affected by the loss of digital asset's performance. The assumption is based on the fact that System processes are performed in a sequential flow by embedded computing systems and Each sub-process is supported by some cyber resources and services provided by digital assets. In modeling digital asset domain, Digital asset's operational capacity is defined as the ability to provide cyber resource and services to system processes. The operational capacity can be affected by own faults or by dependency with other digital assets. It can also be used as an indicator of how digital assets have been affected by cyber attacks. Quality of service metrics used for checking the health of a digital asset in the IT field can be used for quantifying digital asset's operational capacity. In modeling cyber attack domain, logical and impact relationships between vulnerabilities and services provided by digital assets are reflected. Various attack graphs and IDS alert correlating methodologies are used to identify the suspected vulnerabilities and to decide whether they have been exploited or not. In addition, the Common Vulnerability Score System (CVSS) can help to understand the impact of each vulnerability exploit on services [6].

4. Application of the Framework to Response to Cyber Attacks in NPPs

When some suspicious cyber events are sensed at a NPP, the first task to do is to investigate impact on CDAs and to assess the impact on system safety. Three types of tasks for the initial response required in terms of safety impacts are defined as Fig. 2 according to the three-level SA process model.

Fig. 2. The Suggested Cyber Attack Response Process

The developed framework allows operators to understand the attacks in a comprehensive way and to conduct initial response tasks in a systematic way.

4.1 CDA Impact Assessment

CDA impact investigation includes the sub-tasks of cyber event correlation, impacted CDA identification, and CDA impact quantification. The impact on the CDA can be measured by the loss of operational capacities of digital assets, which is the result of a combination of both direct and indirect impacts. Available cyber data analysis and alert correlation methodologies and quantifying digital asset's operation capacity methodologies are being investigated.

4.2 Process Impact Assessment

Process impact assessment includes two sub-tasks of impact propagation and process impact quantification. As a cyber attack hits a CDA, the impact starts propagate through the links and reaches to some process. This propagation continues until a top-level process is affected as Fig. 3.

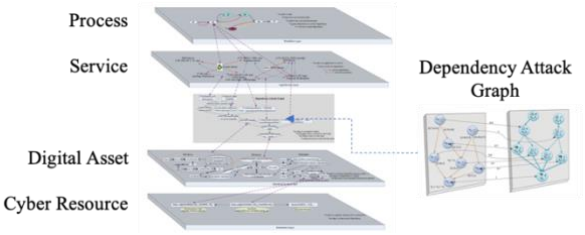

Fig. 3. Description of the Impact Propagation

The extent of impact on top-level process can be calculated by using the loss of operational capacity of each digital asset and multi-level dependency analysis.

4.3 Plausible Future Impact Projection

It is assumed that digital assets that are quite similar to those already compromised can also cause damage through the same propagation process. Aspects of asset similarity are vulnerability, configuration, location, functional, temporal, process, and usage. Quantifying the similarity requires multi-domain knowledge, including system processes and the cyber environment.

4. Conclusions

Successful response to cyber attacks heavily relies on operator's understanding of the impact in terms of security and safety. A supportive framework for cyber SA process is developed by integrating individual security perspective in terms of digital asset, cyber attack, system process. The developed framework allows operators to understand the attacks in a comprehensive way and to conduct initial response tasks in a systematic way.

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)

REFERENCES

[1] Madan, Bharat B., et al. "A method for modeling and quantifying the security attributes of intrusion tolerant systems." Performance Evaluation 56.1-4 (2004): 167-186.
[2] Endsley, Mica R., and Erik S. Connors. "Foundation and Challenges." Cyber Defense and Situational Awareness. Springer, Cham, 2014. 7-27.
[3] Vieane, Alex, et al. "Addressing human factors gaps in cyber defense." Proceedings of the Human Factors and Ergonomics Society Annual Meeting. Vol. 60. No. 1. Sage CA: Los Angeles, CA: SAGE Publications, 2016
[4] Franke, Ulrik, and Joel Brynielsson. "Cyber situational awareness–a systematic review of the literature." Computers & Security 46 (2014): 18-31.
[5] Albanese, Massimiliano, and Sushil Jajodia. "Formation of awareness." Cyber defense and situational awareness. Springer, Cham, 2014. 47-62.
[5] Mell, Peter, Karen Scarfone, and Sasha Romanosky. "Common vulnerability scoring system." IEEE Security & Privacy 4.6 (2006): 85-89.