Study on the improvement and analysis of cyber security exercise on nuclear power plant

Ickhyun Shin
Korea Institute of Nuclear Nonproliferation and Control, 1534 Yuseong-daero, Yuseong-gu, Daejeon City, 34054
ihshin@kinac.re.kr

1. Introduction

Since cyber attacks detect undiscovered vulnerabilities first and carry out attacks that exploit them, cyber security prevention measures alone cannot prevent them 100 percent. Therefore, a cyber security incident response system is needed to minimize adverse effects in the event of cyber attacks, and the incident response system should be evaluated and response capabilities should be strengthened through regular cyber security trainings and exercises. South Korea's nuclear facilities have been conducting cyber security exercises based on threat response scenarios in earnest since 2016 under the revised Act on Physical Protection and Radiological Emergency (APPRE). Cyber Design Basis Threat (DBT), which is the basis of the exercise scenario, presents the attributes of cyber threat, which differ in many ways from the threat attributes in traditional physical DBT. Cyber threats, in particular, differ from physical threats in that they are not quantifiable, have no concept of delaying after detecting an attack, and are not easy to track attackers. In addition, physical protection exercise, e.g., force-on-force exercise, involves the infiltration of actual nuclear power plant by forming an attack group, while cyber security exercise cannot create real situation such as malware infection on an operating computer-based system. In this paper, the differences between physical and cyber threats, and force-on-force exercise and cyber security exercise are presented to draw out ways to improve cybersecurity exercise.

2. Cyber security vs Physical Protection

2.1 Purpose of Cyber Security Exercise

The purpose of cyber security and physical protection is to prevent sabotage of nuclear facilities and nuclear materials and theft of nuclear materials, and to quickly detect and minimize consequences if a threat occurs. The exercise is intended to verify incident response plan and capabilities in order to respond effectively in a real attack situation. Cyber security exercise verifies various incident response phases such as detection, analysis, containment, eradication, recovery and post-incident activity.

2.2 Cyber Threats vs Physical Threats

Developing scenarios on which training is based, whether cyber security or physical, requires a threat attribute defined in DBT, which varies between physical threat and cyber threat. Some of the different factors that the cyber security has are as follows;

1) No concept of delay: the traditional physical protection concept, i.e., detection, delay, response, does not apply exactly in the field of cyber security. In particular, for cyber security, there is no concept of delay because most computer system have already compromised when they detected a cyber attack. With respect to the response, cyber security focus on incident investigation and tracking while physical protection deals with actual engagement

2) Hard to track cyber attack: It is hard for investigators to identify cyber attackers since hackers can erase their traces of an attack and can travel multiple servers. However physical attackers normally leave their marks.

3) Unknowing insider: In the case of a physical attack, it is possible to facilitate an attack with the cooperation of an insider, but in the case of a cyber attack, it is possible to break through the closed network without having to engage an insider. In other words, if an engineer inadvertently infects a USB or laptop that is brought in by an engineer with access to a closed network, the system can be deactivated by the engineer authorized to access the internal system without the need for an intentional insider. The paralysis of Nonghyup bank's computer network in April 2011 is the incident that was caused by unintended insider.

4) Cyber threats that are difficult to quantify: In the case of physical protection, threat attributes such as the type of weapons used, the force of explosives, and number of adversaries can be quantified, but such quantification is difficult for cyber security. For this reason, it is difficult to divide the boundaries between DBT and Beyond DBT in the case of cyber security, and therefore the boundaries between the roles and responsibilities of the state and nuclear reactor licensees are vague.

5) Supply chain security: Physical protection protects areas such as protected areas and vital areas, but in the case of cyber security, systems that perform important functions such as safety function, security function, and emergency preparedness function should be protected from cyber attack. And it is very import to implement cyber security measures, e.g., temper proof seals, hash function, during the delivery of computer based system

who perform those functions since malicious code or manipulated data can be inserted during transfer.

2.3 Force-on-Force vs Cyber security Exercise

There are also several differences between cyber security exercise and force-on-force exercise. The biggest difference is that for force-on-force exercise, the penetration group and the response group are organized to evaluate facility's incident response system consisting of detection, delay and response through actual penetration, as well as to evaluate the performance of the physical protection system corresponding to each detection, delay and response [1]. However, cyber security scenario doesn't include actual cyber compromise since operational and safety problems can arise if cyber breaches of the actual operating system are made. Thus, the technical assessment of the effectiveness of cyber security systems, e.g., firewall, intrusion detection system, and cyber security controls implemented on computer systems is even more difficult. In the case of a physical attack scenario, the attack target area, i.e., vital area, sabotage of which can lead to a core damage, should be set up and this can be identified through probabilistic risk assessment (PRA). In addition, the most vulnerable paths from the outside of the facility to the vital areas are also needed to be developed. The path is reflected in the exercise scenario and can be used in the design phase for the construction of a nuclear power plant. However, neither the digital assets, cyber compromise of which can lead to a core damage, nor the most vulnerable paths from outside to the digital assets are identified

3. Improvement of Cyber Security Exercise

The purpose of cyber security for nuclear facilities under the APPRE is to protect the lives and property of the people. To this end, cyber attacks to cause sabotage are prevented, and cyber security exercise should be conducted to assess whether the incident response system is appropriate to respond to the greatest threats that could cause sabotage and whether it has sufficient technical capabilities. Some of the improvement for cyber security exercise to achieve that purpose is suggested as follows;

1) When developing cyber attack scenarios for exercise, it is very important to consider most attractive targets which can lead to a serious damage such as radiological sabotage. It is studied that the vital digital assets which, if compromised, can lead to a core damage by using PRA methodology including fault tree and event tree analysis [2]. These vital digital assets should be the threat scenario targets for cyber security exercise.

2) Attack vectors and pathways from outside to the vital digital assets should also be considered when developing cyber security exercise scenarios. One of the ways to develop attack pathways is to use tools such as "ATT&CK for Enterprise" which is developed by MITRE corporation. This tool is an adversary model for describing adversary action to compromise system and was derived from cyber kill chain developed by Lockheed Martin [3].

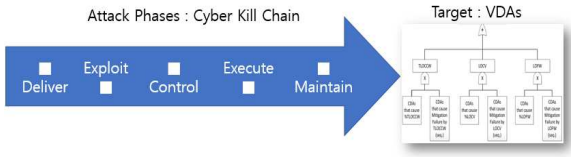

Fig. 1. Attack phases and target for scenarios

3) In the case of physical protection, the penetration is carried out by actually cutting the outer fence to reflect the actual situation as much as possible. Since it is difficult for cyber security to carry out direct attacks, a Mockup system needs to be deployed as an alternative. The plant will be able to assess its technical capabilities in the areas of response, such as detection, investigation and analysis, by utilizing a Mockup system.

3. CONCLUSIONS

In this paper, the differences between physical and cyber threats and exercises were presented to derive ways to improve cyber security exercise. Cyber security exercise should be planned and conducted based on threat scenarios which lead to most serious problem, i.e., radiological sabotage. Thus, vital digital assets should be identified and should be a target for the scenario. Then attack path to the target should also be developed using certain tools. Finally, the exercise should be done in an mockup system to reflect real environment and assess technical capability.

REFERENCES

[1] M. Koh, M. Jung, The Dvelopoment of a Scientific Evaluation System of FOF Exercise for Performance-based Regulation in Nuclear Security, KNS Spring Meeting, 2015
[2] K. Kwon, H. Kim, S. Kim, Research on Vital Digital Assets for Nuclear Cyber Security, ANS 2017 International Topical Meeting on Probabilistic Safety Assessment and Analysis, 2017
[3] ATT&CK for Enterprise, MITRE Corporation, http://attack.mitre.org/resources/enterprise-introduction, 2018