Developing a Training Program for IAEA ITC on Computer Security in a Nuclear Facility

Jeong-ho Lee
KINAC, 1534 Yuseong-daero, Yuseong-gu, Daejeon, Korea, 34054
friend25kr@kinac.re.kr

1. Introduction

As growing global concern on computer security[1] in a nuclear facility, IAEA decided to develop a new computer security training program. Even though having several training programs on computer security, IAEA took a different approach for the new training program. This training program is more inclined to "technical" awareness. It aimed to develop a training program not just only to raise awareness on computer security, but ambitiously also to familiarize computer security technologies. Moreover, it took a step further to cover computer security in a nuclear facility. Also, IAEA would like to set up footholds to implement the training program.

KINAC volunteered to take a part in developing the training program and setting up training environment at INSA. It was a good chance for KINAC to share its knowledge and experience on computer security regulation for years. As well, it opened another opportunity for KINAC to take a part in and learn lessons from international computer security expert community.

While participating the IAEA's ambitious project, KINAC tried to reflect its knowledge and experience to the program. KINAC aimed to come up with the program that helps international trainees to understand computer security in a nuclear facility. For the purpose, KINAC developed training modules on how computer security measures are applied to functions of a nuclear facility. At first, KINAC designed hypothetical nuclear facilities and defined their computer-based system networks based on facilities' functions. Then, training modules are developed dealing with computer security issues on the computer-based system networks of nuclear facilities. In this paper, we would like to introduce KINAC's efforts working with IAEA to develop the training program for nuclear security perspectives.

2. Training Program Scheme

A training program requires to provide trainees to clues on what computer security would like in a nuclear facility. The program developers defined two hypothetical nuclear facility. One is a research reactor facility, and the other is a nuclear power plant. The research reactor facility, which has simple safety systems, is designed for introduce facility functions, basic computer security concepts, and their relations. The other nuclear power plant will be used for the training module on computer security incident response.

The first part of the program is about basics of computer security in a hypothetical research reactor. Then, the subject of the program is moved to computer incident response and its post activities. Incident response and post activity require to apply almost every basic concepts of computer security. After covering basics of computer security in a hypothetical research reactor, the subjects of the training are moved to incident response and post activities in control systems of a hypothetical nuclear power plant.

3. Hypothetical Nuclear Facilities

Two hypothetical nuclear facilities are designed for the training. The first hypothetical facility is a research reactor facility named "Shapash Nuclear Research Institute (SNRI)". The other is a nuclear power plant called "Asherah Nuclear Power (ANP)."

The training purpose of SNRI is to guide trainees to computer security in a nuclear facility [1, 5, 6]. A design principle of SNIR is to have overall characteristics of a nuclear facility as simple as possible. Important factors for the training are information security [2], network vulnerability assessment and management, and computer security on physical protection system and safety control system.

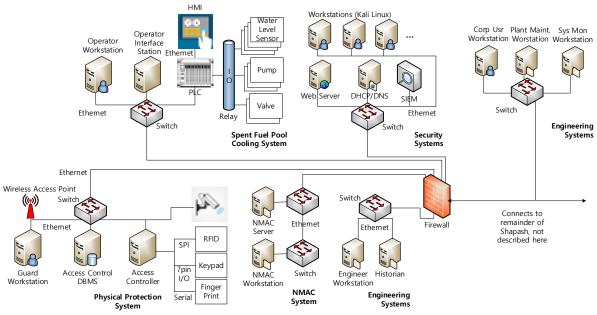

Figure 1. The Network Architecture of SNRI

[1] IAEA decided to use the term, "computer security" instead of cyber security in the nuclear security series. This paper will use the term along with IAEA guidelines.

Based on those design requirements, the computer-based network of SNRI consists of six subnetworks as presented in the Figure 1:

- NMAC [2] [3] Systems: information systems that contains nuclear material stored and used at SNRI.
- Physical Protection Systems (PPS): security systems for monitoring surveillance camera and controlling access of SNRI
- Spent fuel pool cooling (SFPC) systems: control systems of spent fuel cooling function at SNRI
- Engineering Systems: auxiliary control systems and logging systems for operational data from the control systems (SFPS)
- Corporate Systems: operational systems for managing, control, and managing control systems (SNRI)
- Security Systems: computer security monitoring system to manage vulnerabilities of computer-based systems and to detect computer security incidents

Another hypothetical facility, Ashara Nuclear Power (ANP) is used for training of compute security incident response [4] on control systems. Training requirements of ANP are to present how threat might be applied to a nuclear facility and to provide training environment to detect, analyze and eradicate a computer security incident.

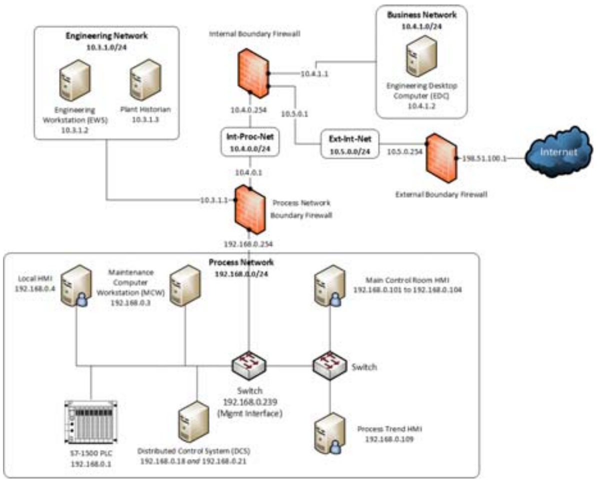
Engineering Network
10.3.1.0/24
Engineering Workstation (EWS) 10.3.1.2
Plant Historian 10.3.1.3
Internal Boundary Firewall
10.4.1.1
Business Network
10.4.1.0/24
Engineering Desktop Computer (EDC) 10.4.1.2
10.4.0.254
10.5.0.1
Int-Proc-Net
10.4.0.0/24
Ext-Int-Net
10.5.0.0/24
10.5.0.254
198.51.100.1
Internet
External Boundary Firewall
10.4.0.1
10.3.1.1
Process Network Boundary Firewall
192.168.0.254
Process Network
192.168.0.0/24
Local HMI 192.168.0.4
Maintenance Computer Workstation (MCW) 192.168.0.3
Main Control Room HMI 192.168.0.101 to 192.168.0.104
Switch
Switch 192.168.0.239 (Mgmt Interface)
S7-1500 PLC 192.168.0.1
Distributed Control System (DCS) 192.168.0.18 and 192.168.0.21
Process Trend HMI 192.168.0.109

Figure 2. The Network Architecture of ANP

Based on the training requirements, ANP network is made up with three subnetworks:

- Business Networks: a system to assist ANP employees' daily business
- Engineering Networks: systems for configuration management and operational data logging
- Process Network: systems consisting of controlling systems and monitoring systems

The ANP network does not look like a real network architecture for a nuclear power plant. It is designed as simple as possible only fit for the training scenario and getting rid of redundant elements from SNRI network.

4. Training Program

Training modules were developed based on the hypothetical facilities. The developed training program contains general computer security along with its characteristics in nuclear security. In this section, we would like to describe our effort on how to distinguish computer security in nuclear facilities.

As it is discussed, the first part of the training program deals with basics computer security concept based on SNRI. One of basic lessons is that computer security in a nuclear facility requires to understand facility function and operations.

NMAC systems is stored nuclear material information, types, amount, and location of nuclear materials. The information is sensitive[3] because it can be used for unauthorized removal. The information is usually managed by operational staffs. As well, security guards are using the information to verify authorized nuclear material transportation. Those functional or operational requirements are not so much different from general database systems used in a business world.

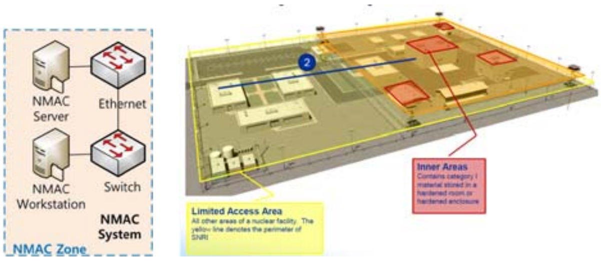
NMAC Server
Ethernet
NMAC Workstation
Switch
NMAC System
NMAC Zone
2
Limited Access Area
All other areas of a nuclear facility. The yellow line denotes the perimeter of SNRI
Inner Areas
Contains category I material stored in a hardened room or hardened enclosure

Figure 3. NMAC Network and Physical Layout

However, implementation of computer security measures requires operational knowledge on a nuclear facility. Even though network architecture of NMAC subnetwork looks simple (the left side in the Figure 3), there are more to consider (the right side in the Figure 3). For instance, operational staffs are supposed to manage the NMAC data in secure area (inner area in the Figure 3). However, security guards refer the data at the less secure area (limited access area in the Figure 3). As well, there is long transmission between two places.

Considering those operational aspects, computer security measures should be put in place as depicted in the Figure 4.

1. Stronger access control measures at the NMAC workstation used by security guards

[2] NMAC: Nuclear Material Accountancy and Control

[3] In the training program, NMAC information is provided as an example of sensitive information to be protected.

2. Secure and one-way transmission from protected area to limited access area
3. Information security measures (for example, cryptography) and access control measures

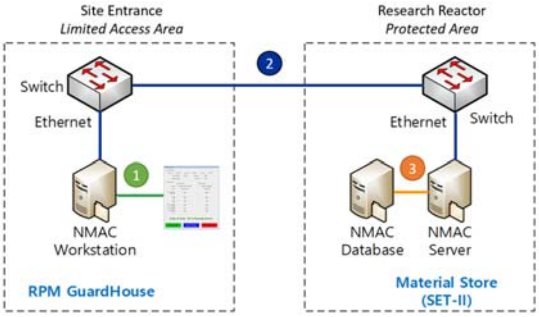

Figure 4. Security Measures for NMAC Systems

Physical Protection Systems (PPS) are used for intrusion detection and access control to SNRI. PPS consists of third-party products such as CCTV camera, and so on. Open source information on CCTV cameras can be used for an adversary to misconfigure or misdirect surveillance cameras. As well, PPS manages access information such as credentials or biometric information. If the information is compromised, an adversary might take advantage to access SNRI. We designed PPS hands-on for PPS training modules as show in the Figure 5.

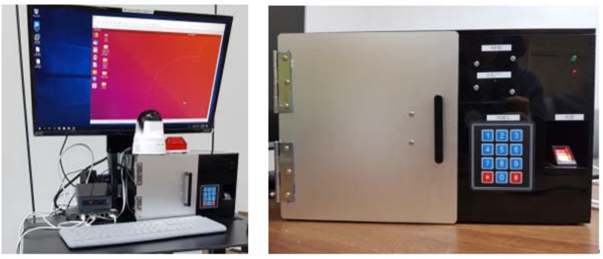

Figure 5. PPS Hands-on

Main function of Spent Fuel Pool Cooling (SFPC) Systems is to remove residual heat from spent fuel. It carries out the function by maintaining the amount of coolant and its temperature. SFPC systems is important because it is sensitive safety system. Also, it has a control system, which is different from general purpose computer-based system. A control system can be easily compromised by a malicious act because of their real-time attributes and limitation of computational power. We designed SPFC hands-on for the training using a commercial PLC as shown in the Figure 6. In the training scenario, we demonstrate that the function of coolant level maintenance can be compromised by continuous reverse, unauthorized but legitimate, PUMP activation commands. Even though every system in the SFPC systems was intact, unauthorized network element, such as a laptop or tablet PC, can compromise whole system functions.

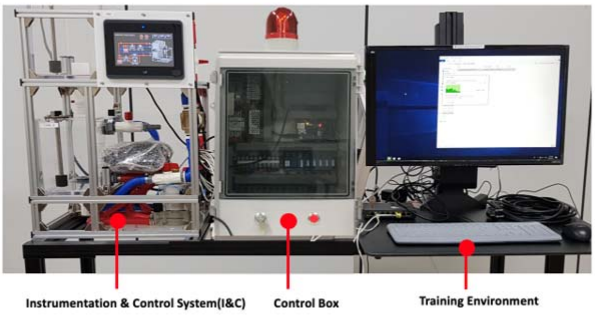

Figure 6. SFPC Hands-on

A critical safety system like SFPC systems has auxiliary systems for emergency and monitoring system of its operations. Those systems are spatially or remotely located. Hence, SFPC systems are required to be access from engineering systems or corporate systems. Also, SFPC systems need to log its operational data in an independent system according to safety regulatory requirement. Those functional requirements can create vulnerabilities, which might open opportunities for an adversary. Computer security measures are required to put in place to compensate those vulnerabilities. The training module are developed to introduce the compensating technical measures such as a firewall, OSSIM, OSSEC, and so on. Those technical measures secure computer-based networks in SNRI to isolate subnetwork allowing only required connections and to detect intrusions to a system/subnetwork.

The second part of the training moves its subject to computer security incident response based on the new facility, ANP. The incident response training is based on an incident scenario. The training scenario is:

- The CEO of ANP meets one of adversaries who disguises himself as a salesman in a software company. The CEO decides to introduce a software that the disguised salesman recommended.
- The IT team of ANP install the software, which has a planted malware, in the ANP business network.
- The malware in the software succeeds to obtain access to engineering workstation in the ANP engineering network. Then, the malware retrieves data from the workstation and sends back to an adversary.
- An adversary learns from the obtained data that ANP plans to upgrade a maintenance computer workstation in the ANP process network. A new hardware is about to deliver to ANP. The adversary compromises the supply chain and succeeds to implant unauthorized communication device, which will allow him to remotely access the maintenance computer, to the hardware.
- The implanted maintenance computer is put in place. The adversary activates unauthorized control commands to a pump in a ANP condenser.

Based on the scenario, we create PCAP files that simulate every step of the scenario. We create the MCR and condenser mock-up to demonstrate the scenario as shown in the Figure 7. With tangible hardware and PCAP file, trainees are asked to analyze an adversary's techniques and tactics.

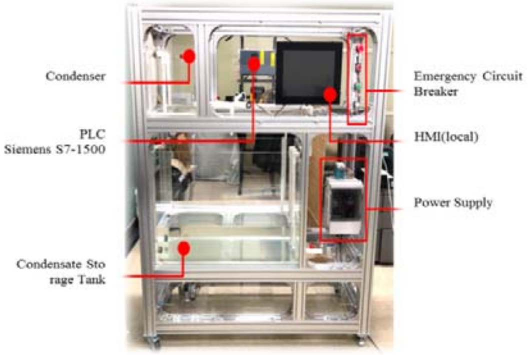

Figure 7. Condenser Mock-up

5. Training Environment

From the perspective of the training implementation, the training program is developed in two parts. One is lectures and the other is exercises. The training program is designed to provide changes for trainee to feel and touch tools addressed in the lecture.

Exercises are developed for this purpose. In the exercise, trainees can look closely into the NMAC database and feel the differences between unencrypted data and encrypted data. Also, trainees can manipulate access credentials to allowing an unauthorized person to access or to disallowing an authorized person to access. They exploit opensource data from web to compromise security cameras in an exercise. Even they can scan the whole SNRI network to find system/vulnerabilities.

We create the whole SNRI network based on virtual machine technology. Then, we connect PPS and SFPC hands-on equipment to SNRI network to increase reality. The training environment is created to host five groups with six trainees. To meet the target, we create five independent and designated SNRI network.

We create the SNRI network based on open source software (as much as possible):

- Trainee Workstation: Kali linux
- Database (NMAC, PPS): MariaDB, DBeaver
- Firewall: pfSense
- OSSIM/OSSEC: AilenVault, OpenOSSEC
- Network Scan: NMAP
- Vulnerability Management: Metasploit
- Network Analysis: Wireshark

As well, we used commercial software such as:

- Microsoft Windows 7, Sysinternals
- VMware ESXi, vSphere, vCenter

Five independent SNRI network were configured as depicted in the Figure 8. It requires much knowledge and effort on network engineering and VMware technology.

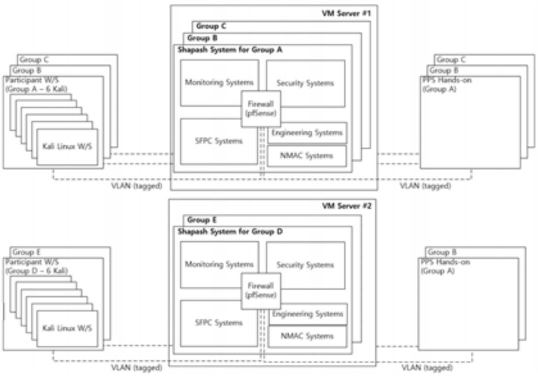

Figure 8. Training Environment

6. Training Program Evaluation

Based on developed the training program, we successfully conducted an international training course (ITC) in November 2019. After the ITC, we had reviewed meeting with IAEA and international experts who involved in the ITC based on trainees' evaluations.

The evaluation result tells "everything is in it, but too much". Based on the evaluation result, the main remaining task seems that we need work on reduce the burden of the course work, especially for trainees from non-English speaking states. We will work on revise the training program in this year for the next upcoming training course.

REFERENCES

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security at Nuclear Facilities, IAEA Nuclear Security Series No. 17, IAEA, Vienna (2011)

[2] INTERNATIONAL ATOMIC ENERGY AGENCY, Security of Nuclear Information, IAEA Nuclear Security Series No. 23-G, IAEA, Vienna (2015)

[3] INTERNATIONAL ATOMIC ENERGY AGENCY, Use of Nuclear Material Accounting and Control for Nuclear Security Purposes at Facilities, IAEA Nuclear Security Series No. 25-G, IAEA, Vienna (2015)

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Incident Response Planning at Nuclear Facilities, Technical Document (Non-serial Publications), IAEA, Vienna (2016)

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, Draft Implementing Guide (NST045), IAEA, Vienna (2016)

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, Draft Implementing Guide (NST047), IAEA, Vienna (2017)