Cybersecurity Training: Simulation of a Cyber Attack at a Radiotherapy Clinic

Rodney Busquim e Silva
International Atomic Energy Agency
r.busquim@iaea.org

Ricardo Paulino Marques
Universidade de São Paulo
ricardomarques@usp.br

José Roberto Castilho Piqueira
Universidade de São Paulo
piqueira@lac.usp.br

Abstract

This paper presents the simulation of a cobalt-60 radiotherapy clinic, which offers cancer treatment using a teletherapy unit (TTU), that was developed for conducting computer security training and exercises. The simulator allows the execution of two independent cyber-attacks: a ransomware of personal information and the compromise of an access control system (ACS), and the ability of training or exercise participants to recognize and respond to such attacks. This clinic is part of a regional hospital in a fictious country, and includes a teletherapy treatment room, a control room, designed as controlled areas, and a waiting room. The simulated computer-based systems comprise a simplified treatment planning system (TPS), a simulation of the TTU, an ACS and IT equipment. The ACS manages physical access to the premises, and provides images of a CCTV camera, using Modbus and TCP/IP protocols. The TPS has an HMI that allows the operator to configure and control a TTU treatment session, and a database with patient personal information. The ACS has an HMI that allows the training or exercise participants to open and close doors and have access to the CCTV camera. This simulator was developed using Docker containers to reduce the overhead associated with each participant accessing their own simulated environment. It also allows participants real-time access to simulated network data packets using the Wireshark application. This simulation was developed and first used as part of the IAEA Regional Training Course on Computer Security for Industrial Control Systems (25–29 April 2022 and 05-09 December 2022), and it was also the basis of a scenario deployed during a major Brazilian critical infrastructure exercise, Cyber Guardian Exercise 4.0 (16-19 August 2022). The outcomes of both events related to the use of the simulator were: increased learning experience as the participants had access to exercise hands-on environment while sharing remote supervision; enhanced training capability to illustrate the cyber-security challenges of facilities handling radioactive or nuclear materials; and increased instructor capacity to facilitate discussions on the application of computer security measures (technical, administrative and physical) based on the IAEA guidance on computer security.

1. Introduction

Cyber-attacks are malicious acts with the intent of stealing, altering, preventing access to or destroying a specified target through unauthorized access to a susceptible computer-based system [1]. For example, a cyber-attack targeting sensitive information about the design of the physical protection system (PPS) could facilitate the coordinated use of both cyber-attack and physical attack aiming sabotage.

Simulators specially designed for cyber physical assessments are key tools for addressing the facility impact arising from a cyber-attack [2]. Simulators can be an essential tool for cyber security training as they allow the participants to recognize that computer security is required for the prevention and detection of, response to and recovery of computer-based systems from cyber-attacks. This includes, for example, the understanding that computer security incident response [3] comprehends the detection and analysis, the mitigation (containment, eradication and recovery) and post-accidents activities. Simulators also facilitate

discussions on the application of physical, administrative and technical control measures to maintain the preventive and protective measures. They also allow the application of IAEA computer security guidance [1] [4] [[5] [6], which includes recommendations (among others) on the application of computer security risk management; on the establishment of a computer security program (CSP); and on the definition and implementation of a defensive computer security architecture (DCSA) that provides for defence-in-depth and applies computer security measures in a graded approach.

This work presents the simulation of a cobalt-60 radiotherapy clinic, which offers cancer treatment using a teletherapy unit (TTU) developed for computer security training and exercises. The simulator offers the possibility of performing two independent cyber-attacks: a ransomware of personal information and the compromise of an access control system (ACS). The trainees interact with the simulator, recognize and respond to such attacks. The trainers are able to guide discussion on how IAEA computer security concepts should be applied to facilities that handle radioactive materials.

This training tool was developed using Docker containers to reduce the overhead associated with each participant accessing their own simulated environment. This approach allows participants real time access to network data packets using the Wireshark application.

2. Radiotherapy Clinic

The Gula Regional Hospital (GRH) is a fictitious hospital that provides specialized medical services, including medical services using radioactive materials. It serves both the fictitious Republic of Anshar and its fictitious neighboring countries. These fictitious entities were created by IAEA for use in exercises, training courses, demonstrations, etc.

GRH has two main wings, the radiography and radio-oncology wings, that have blood irradiators, which uses Cesium (Cs-137) Chloride Salt for processing blood for transfusion, and a teletherapy unit (TTU), which uses cobalt-60 to generate an external beam of gamma rays for cancer treatment. GRH serves about 600 patients per day during the work week.

The GRH oncology radiotherapy clinic addresses the Republic of Anshar need to deliver specialized medical services for cancer treatment in the region. Teletherapy, or external beam radiotherapy, is a form of radiotherapy where the patient lies on a couch and an external source of ionizing radiation is pointed at a particular part of the body. The TTU is a medical equipment capable of performing this treatment. Figure 1 shows the new TTU acquired by GRH.

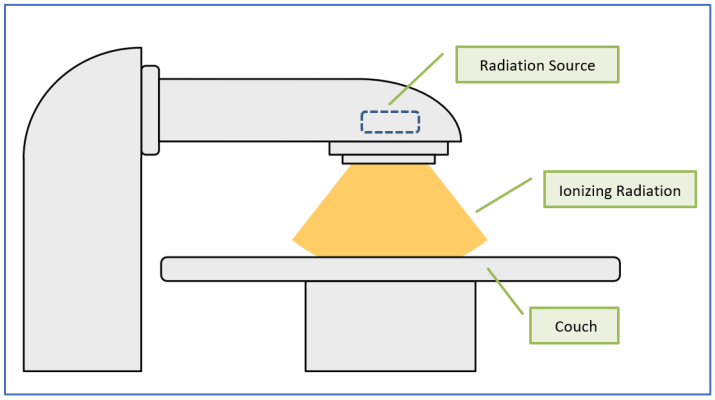

Figure 1: GRH TTU

The GRH radiotherapy clinic layout has a waiting room, a control room (operator) and a bunker where the TTU is located [7]. The diagram in Figure 2 shows the Oncology Wing Radiotherapy Clinic layout.

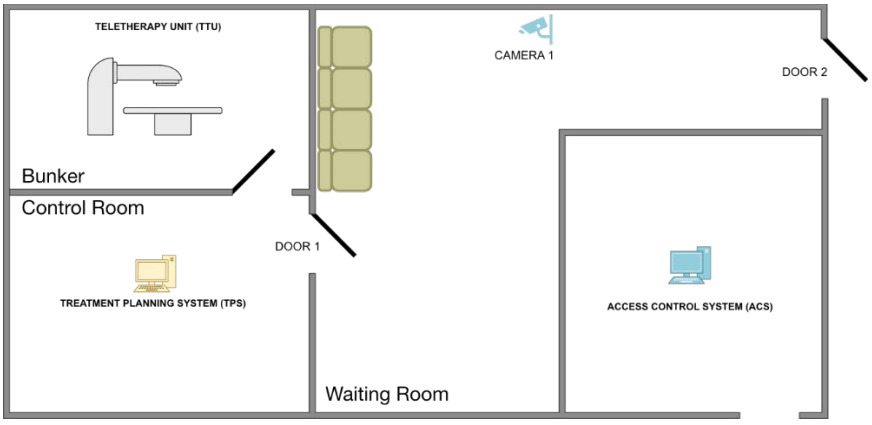

Figure 2: Oncology Wing Radiotherapy Clinic

The two main computer-based systems at the GRH radiotherapy clinic are:

- Treatment Planning System (TPS), connected to the TTU.
- Access Control System (ACS) that controls physical access to the facility.

The TPS is a system used to calculate technical parameters such energy, dose, and duration of the radiotherapy treatment needed to deliver a safe and effective dose distribution. The ACS provides monitoring and control of the movement of people in a facility, and complements other security and emergency management systems.

The TPS has a Human-Machine Interface (HMI) terminal that allows the operator to configure and control a treatment session. The HMI allows the operator to interact with the TTU. The TPS also has a database with patient records and other personal information. The access to the treatment facility must be controlled as the TTU contains Co-60, which is done using a simple ACS that allows an operator to open and close the facility doors, and monitor the waiting room with a CCTV camera. Figure 3 presents the TPS and ACS simplified interfaces.

The ACS manages physical access to the premises, and provides images of a CCTV camera. The ACS HMI allows the trainees to open and close the doors. ACS uses Modbus and TCP/IP protocols.

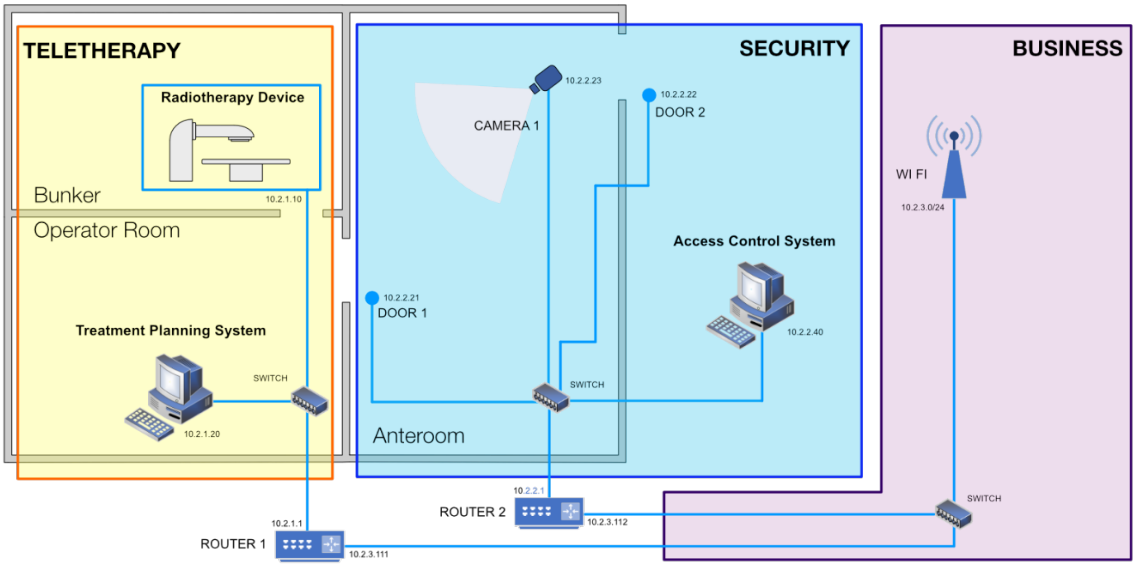

Figure 3: TPS and ACS HMIs

2.1. Network Diagram

The computer-based systems in the radiotherapy clinic are connected through three internal networks: a password protected staff WIFI network used by patients and staff; a PPS network used exclusively by the ACS; and a TTU network used locally by the TPS and the TTU. The radiotherapy network diagram is shown in Figure 4.

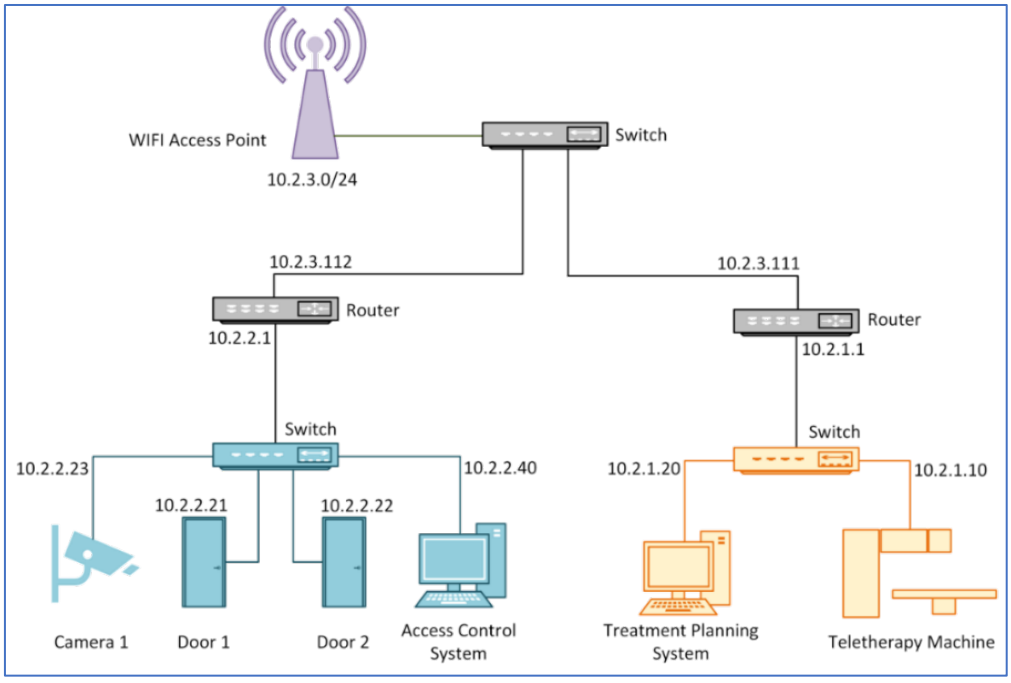

Figure 4: Oncology Wing Radiotherapy Clinic Network

3. Training Dynamics

The simulator allows participants to, on their own time and following the exercise description, get familiarized with the simulation, look at the network baseline, trigger the attacks and see their impact. The storyline that supports the activity includes the information that the adversary had access to the network and systems information, and had the knowledge, resources and time to plan and conduct the attack.

The training scenario consists of a blended attack against the radiotherapy clinic ACS, and a ransomware campaign on the teletherapy unit TPS, with the following steps:

1. The adversary obtains access to the staff WIFI network.
2. The adversary creates a specialized malware based on collected knowledge and detected vulnerabilities of the network and connected systems.
3. The adversary executes the malware from a terminal in the WIFI network.
4. Malware execution compromises the following systems and devices:
    a. Camera 1, by exploring a vulnerability similar to Devil's Ivy (CVE-2017-9765), freezing the camera.
    b. Doors, by performing a data injection attack, sending repeated commands to unlock the doors at a much higher rate than the ACS.
5. The path is open for the adversary to intrude the facility undetected and potentially gain access to the radiological sources.
6. On a parallel move, the adversary exploits vulnerabilities of the TPS, gains access to the system and encrypts files with important patient's information by performing a ransomware attack.

The scenario and the simulation system were developed for and first used as part of the IAEA Regional Training Course on Computer Security for Industrial Control Systems (25–29 April 2022 and 05-09 December 2022), and were also the basis of a scenario deployed for the Brazilian Cyber Guardian Exercise 4.0 (16-19 August 2022).

4. Lessons Learned and Outcomes

Lessons learned at both events related to the use of this simulator can be summarized as:

1. Realistic dynamic simulation environments improve the learning experience by providing credible scenarios and convincing detailed attack evidences in real time under trainer supervision.
2. Realistic real-time simulated attacks lead to improved knowledge on the prevention and detection of, response to and recovery of computer-based systems from cyber-attacks.
3. A simulated environment improves the training capability to illustrate the cyber-security challenges of facilities handling radioactive or nuclear materials in comparison with table top exercises.
4. Adequate cyber-attack scenarios and exercise simulated tools allow the direct application of the IAEA nuclear security guidance and contribute to their understanding.
5. Understanding of the application of relevant IAEA computer security guidance is much improved with the aid of an environment capable of producing realistic outcomes, including physical consequences of cyber-attacks to nuclear facilities.
6. Discussions are facilitated by the availability of a system capable of illustrating the application of computer security measures (technical, administrative and physical) in real-time and relating it to relevant guidelines.

7. The use of a virtualized container-based framework for the simulators makes possible the straightforward deployment of an exercise scenario without major computational requirements, being a tool especially convenient for hands-on training courses.
8. Docker container implementations reduce dramatically the overhead associated with starting and running instances when compared to the use of virtual machines.

The main outcomes of the events can be summarized as follows:

a) Increased awareness of cyber threats to nuclear facilities and facilities that handle radioactivity materials among governmental authorities, operators and other stakeholders.
b) Increased participants' knowledge on the prevention and detection of, response to and recovery of computer-based systems from cyber-attacks.
c) Improved computer security capability building, making use of relevant IAEA computer security guidance.
d) Improved capability to identify and prioritize potential computer security gaps in real life facilities.
e) Shared information regarding the resources, capabilities, tools, and planning needed to prepare for, conduct, and evaluate computer security exercises.

The events were very positively evaluated. For instance, for CGE 4.0 the overall evaluation performance by the participants was 4.95 of 5.0, with many participants stating they would directly apply the lessons learned within their organizations.

5. Conclusions

The use of simulators such as the GRH radiotherapy clinic for conducting computer security exercises brings benefits such as:

a) Readiness, as it allows for automatic deployment of exercise scenarios with self-guided procedures and without major computational requirements.
b) Efficiency, as it allows each team to have access to their own real-time exercise environment with a realistic simulation scenario, improving the participants' experience.
c) Flexibility, as the use of simulator allows the inclusion of specific requirements within the exercise cyber-attack scenario.

The use of a specially designed simulator allowed the development of very realistic and complex scenarios quickly and easily deployed. The Docker container-based technology allowed each participant to have access to their own independent immersive environment. This increased the learning experience when compared with table top exercises, and facilitate discussion on the application of computer security measures. Finally, the use of such tools is a promising alternative for future training and exercises.

References

[1] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Techniques for Nuclear Facilities, IAEA Nuclear Security Series No. 17-T (Rev. 1), IAEA, Vienna (2021).

[2] Busquim e Silva et al. Integration of the Asherah NPP Simulator into a Closed-Loop Digital Twin Environment for Cybersecurity Assessment. 12th NPIC&HMIT (2021).

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

[4] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security for Nuclear Security, IAEA Nuclear Security Series No. 42-G, IAEA, Vienna (2021).

[5] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security of Instrumentation and Control Systems at Nuclear Facilities, IAEA Nuclear Security Series No. 33-T, IAEA, Vienna (2018).

[6] INTERNATIONAL ATOMIC ENERGY AGENCY, Computer Security Approaches to reduce Cyber Risks in the Nuclear Supply Chain, IAEA Vienna (2022).

[7] INTERNATIONAL ATOMIC ENERGY AGENCY, Radiotherapy Facilities: Master Planning and Concept Design Considerations, IAEA Human Health Reports No. 10, IAEA, Vienna (2014).