Contribution ID: **282** Type: **Paper**

The Asherah Nuclear Power Plant Simulator (ANS) as a training tool at the Brazilian Guard Cyber Exercise

Brazil performed a singular cyber defence exercise in 2018 (from 3 to 6, July 2018): the first Cyber Guardian Exercise (EGC –Exercicio Guardiao Cibernetico). That exercise brought together 23 organizations, from the public and private sectors, in the first national drill towards increasing of performance and stability of cyber security of Brazilian critical infrastructure [1]. The University of Sao Paulo (USP) participants of the International Atomic Energy Agency (IAEA) Coordinated Research Project (CRP) "Enhancing Computer Security Incident Response at Nuclear Facilities"(J02008) took part of that drill by planning the EGC nuclear cyber attackers'scenarios.

The second EGC will take place from 2-4 of July, 2019, in Brasilia, Brazil's capital. Besides public and private organizations from the finance (Itau Private Bank, Caixa Economica, Central Bank of Brazil, Bank Santander etc); nuclear (Eletronuclear, Industrias Nucleares do Brasil, National Energy Commission (CNEN)); and defence sectors (Brazil's Federal Police, Brazilian Army, Brazilian Navy and Brazilian Air Force); the electric sector (Eletrobras, Itaipu Binacional etc) will also be participating. It is expecting that the number of participating will increase to more than 40 organizations.

Under the IAEA CRP J02008, the USP research team has been developing a nuclear power plant (NPP) simulator suitable for digital research, cyber security assessment and computer security measures development. The NPP model is based on a pressurized water reactor (PWR) implemented using Matlab/Simulink. The Matlab/Simulink model, the Asherah NPP Simulator (ANS), simulates nuclear processes and controller's system dynamics. The ANS is the heart of a comprehensive hardware in the loop (HIL) simulation environment, the ANS Test Bed (ATB). The ATB has advanced operational technology (OT) and information and technology (IT) capabilities.

This simulator was designed based on a 2,772 MWt PWR Babcock & Wilcox (B&W) [2] [3] [4] [5]. The ANS integration capabilities include network connection by means of the open communication protocol Modbus and of the open cross-platform machine-to-machine OPC Unified Architecture (OPC-UA) protocol. Two USP developed interfaces allow that simulated subsystems can be replaced by their real counterparts. ANS is the adequate tool for cyber security training.

The ANS has been developed to allow digital OT and IT research, to enhance cyber security response and prevention by capturing thermo hydraulics, neutronics and corporate knowledge on plant operation. By designing a first-of-a-kind NPP simulator that allows exchange of hardware and software and the capture of process and network data, we are extending the ability of engineers to incorporate their operational knowledge on cyber security.

During the 2 EGC, the USP research team will be presenting the ANS capabilities as a research tool. In addition, two cyber attack scenarios exercises, hardware-based schemes, will be performed for the nuclear community to point it out the ANS training capabilities. Practical cyber security exercises are an effective procedure to teach the specifies of OT and IT security.

The ATB HIL scenarios includes four virtual machines (VM) running:

- ANS: Windows 7,
- IPFire firewall: Linux Appliance,
- Network Time Protocol server (NTP): CentOS Linux, and
- ScadaBR [6]: Windows 7.

Moreover, the reactor power controller and the pressurizer pressure controller will be running in a programmable logic controller (PLC) S7 1200. There are three subnets within the ATB training scenario.

One of the attack scenario considers a third party authorized worker connecting a laptop for maintenance, an engineering unauthorized workstation remote access, the exploitation of network vulnerabilities that lead to changes in the PLC behavior. The control of reactivity function is compromised and the facility impact is accessed after the attack. Both training schemes are set up to guide the students through all the necessary steps to understand the importance of training: objectives of the exercise, network topology, dynamic of the attack and lessons learned. The overall goal is to go through the security wheel of secure, improve, monitor, test and improve.

The exercise are set up to go from the technical point of view to realistic situations by including a logical flow of events. The realism of the exercise are based on the attacker's goal towards a successful reactor power sabotage.

REFERENCES

[1] https://dialogo-americas.com/en/articles/brazilian-army-conducts-unprecedented-cyberdefense-exercise. Acessed on May 1st, 2019.

[2] U.S. Nuclear Regulatory Commission (NRC). Backgrounder on the Three Mile Island Accident. www.nrc.gov/reading-rm/doc-collections/fact-sheets/3mile-isle.html. Accessed on September, 16 2017.
[3] K.N. Ivanov et al. Pressurized Water Reactor Main Steam Line Break (MSLB) Benchmark. Volume I: Final Specifications. Organization for Economic Co-Operation and Development (OECD), Nuclear Energy Agency (NEA) (1999).
[4] Busquim e Silva, R.A., "Implications of advanced computational methods for reactivity initiated accidents in nuclear reactors", University of Sao Paulo, PhD Thesis, 2015.
[5] Busquim e Silva, R.; Ferreira Marques, A.L.; Cruz, J.J.; Marques, R.P.; Piqueira, J.R.C. Use of State Estimation Methods for Instrumentation and Control Cyber Security Assessment in Nuclear Facilities. International Conference on Nuclear Security: Commitments and Actions, Vienna –Austria, 2016.
[6] http://www.scadabr.com.br/ Acessed on May 10, 2019.

State

Brazil

Gender

Male

Primary author: Dr BUSQUIM E SILVA, Rodney (University of Sao Paulo)

Co-authors: Mr CORREA, Diego Alves (University of Sao Paulo); Mr ANTUNES, Felipe Ramos (University of Sao Paulo); Prof. PIQUEIRA, José Roberto Castilho (University of Sao Paulo); Mr SOUZA, Francisco Carlos Salles de (University of Sao Paulo); Prof. MARQUES, Ricardo Paulino (University of Sao Paulo)

Presenter: Dr BUSQUIM E SILVA, Rodney (University of Sao Paulo)

Track Classification: CC: Information and computer security considerations for nuclear security