Contribution ID: **170** Type: **Paper**

Advancements in Hardening the Cybersecurity Posture of Nuclear Power Plant Defense-in-Depth Network Architecture

Organizations increasingly depend upon cyber-based technologies for the reliableoperation of Nuclear Power Plant (NPP) facilities through a myriad of Information Technology (IT) and Operational Technology (OT) systems. This enables the automation of industrial processes and a heightened exchange of information, however it also increases the attack surface which can be exploited by potential cyber-capable adversaries. To counter this, the International Atomic Energy Association (IAEA) proposes a defensive computer security architecture approach for strategically deploying computer networks as well as control systems through layers of securely defined levels and zones. To validate this type of architecture and to prepare for potential cyberattacks, Canadian Nuclear Laboratories (CNL) is actively performing research activities on numerous fronts. This paper will outline the advancements being made at the CNL's National Innovation Centre for Cybersecurity in collaboration with the IAEA's Coordinated Research Project (CRP) J02008, entitled 'Enhancing Computer Security Incident Analysis and Response Planning at Nuclear Facilities'.

The foundation of CNL's research in this area is a scaled down Boiler Level Control (BLC) system which integrates a software simulation of a Pressurized Water Reactor (PWR) in a feedback loop. With this experimental setup, cyberattacks can be conducted against the Programmable Logic Controllers (PLCs) managing the BLC and their supporting computing infrastructure, allowing the physical impact of cyberattacks to be measured in real-time. This segment of a NPP digital OT network is mission-critical for reliable NPP operations, and thus has significant measures in place to prevent malicious intrusion (e.g. unidirectional data diodes and no outside network connectivity). This segment is hardened but still vulnerable to insider threats, whether intentional or accidental, particularly as software changes and updates are introduced to the operational environment from engineering workstations. This paper will provide results on what type of cyberattack scenarios can affect this architectural segment, what organizational change management policies could be in place to prevent the delivery of a malicious payload, what are the symptoms of a cyberattack, and what actions could be taken in the event of a compromise.

The defensive computer security architecture paradigm puts a number of barriers in place across network segments, yet these measures may only delay a motivated Advanced Persistent Threat (APT) actor-group in a protracted cyber-intrusion campaign. Nevertheless, with enough of these obstacles to overcome, an attacker will likely leave some 'footprints' as they perform reconnaissance on the systems they are attempting to compromise. Anomaly detection tools provide a means to detect network traffic which is unaccounted for in an organization and can be used to detect an intruder. Commercial-off-the-shelf (COTS) anomaly detectors are made to be general purpose and it is unclear how they will perform in a NPP OT environment. CNL is also actively developing an anomaly detector to complement current COTS offerings. This paper will provide a benchmark of the techniques used within CNL's anomaly detector against industry standard tools applied to a configuration resembling an NPP OT environment. This will further be explored in a discussion on how a portfolio of commercially available tools could be used to secure NPP networks in a connected IT-OT Security Operations Center (SOC).

In summary, the underlying goal of this paper is to share with the international community the advancements being made at CNL for ensuring a hardened defensive posture against NPP cyberattacks. The paper will provide a description of CNL's NPP hardware-in-the-loop (HIL) architecture, an overview of its segmented computer network structure, results of penetration testing scenarios, benchmarking of custom anomaly detector tools against COTS technologies, design strategeis for an IT-OT SOC, and recommendations for how an NPP organization could react in response to a cyber-intrusion.

Gender

Male

State

Canada

Author: Mr NEAL, Christopher (Canadian Nuclear Laboratories, Polytechnique Montréal)

Co-authors: Mr TRASK, David (Canadian Nuclear Laboratories); Mr DOUCET, Richard (Canadian Nuclear Laboratories); Mr THIYAGARAJAN, Karthik (Canadian Nuclear Laboratories); Mr ADAMSON, Peter (Canadian Nuclear Laboratories); Mr DALEY, Matthew (Canadian Nuclear Laboratories); Mr FERNANDEZ, José (Polytechnique Montréal)

Presenter: Mr NEAL, Christopher (Canadian Nuclear Laboratories, Polytechnique Montréal)

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