Contribution ID: **220** Type: **Interactive Content Presentation**

Computer Security & Threat Analysis: Minimizing The Attack Surface

Nuclear and radiological facilities are digitizing elements of security and operational systems in order to improve performance, effectiveness and efficiency while reducing cost of ownership. These digital elements have greatly increased the interconnectivity between traditionally disparate systems such as components in physical protection systems (PPS), nuclear material control & accounting systems (NMAC), as well as other security and operational systems at a nuclear power plant. The migration to digital technology, along with the increased interconnectivity, has introduced new vulnerabilities. These vulnerabilities, which may go unobserved and undetected, present a new landscape of opportunity for potential threat actors targeting nuclear and radiological facilities.

Recent advances in adversarial modeling have generated new and valuable perspectives on existing and emerging threat characteristics, capabilities, and potential attack vectors. The models identify elevated security risks of a threat actor incorporating cyber based attack tools into theft and sabotage scenarios. The risks are particularly pronounced for insider threats that can leverage legitimate access and authorized privileges to conduct maloperations and/or introduce malware to achieve attack scenario goals.

There is a demand from member states and global subjective matter experts for actionable intelligence that can help define accurate prescriptive measures related to how cyber security guidance should be implemented. The landscape of referenceable case studies specific to cyber / physical attacks on nuclear instrumentation and control is poorly populated even though there is an abundance of information on both general non-nuclear cyber security events and physical attack methods.

To address this need, researchers selected actual cyber security attack methods and fused them with well-known insider and physical attack trends. As a result, plausible attack use cases were developed to demonstrate how after-action analysis can be performed to define how a threat actor could use combined cyber/physical methods to accomplish their goal of creating a nuclear reportable event. The goal being to create use cases applicable to the nuclear industry. The presentation will include analysis of cyber event investigation, artifact analysis, attack tree modeling and a comprehensive discussion on how NSS 33-T can be used to proactively defend against the adversarial methods and tactics illustrated in the use cases.

State

United States

Gender

Male

Authors: FABRO, MARK (LOFTY PERCH); NICKERSON, Charles (Idaho National Laboratory)

Presenters: FABRO, MARK (LOFTY PERCH); NICKERSON, Charles (Idaho National Laboratory)

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