Contribution ID: **215** Type: **Paper**

Blended Threat Nuclear-Cyber Scenario Development

Monday, February 10, 2020 12:00 PM (15 minutes)

One challenge of the risk management process for cyber security within nuclear facilities is understanding how to create scenarios to test deployed security controls that are representative of how threat actors operate. The challenge to creating these scenarios is centered on three issues. First, the complexity of systems and components (assets) at nuclear facilities makes for an expansive attack surface, so the number of viable attack pathways is difficult to approach with any confidence. Second, the nature of cyber-attacks and cyber-campaigns has evolved to include cyber-enabled physical attacks and physical-enabled cyber-attacks, which blends together attack types which have traditionally been treated separately. Third, threat actor capabilities vary depending upon the resources they have available to them and their domain experience. Our paper provides for a methodology to create blended threat nuclear-cyber scenarios for use during research, assessments, and exercises in support of risk management and training objectives.

Our methodology was derived through a series of International Atomic Energy Agency (IAEA) consultancy series and a multi-year research project on detecting events within nuclear facilities that may indicate that a cyber-attack is taking place. The first step in our methodology was to agree upon an attack and defense framework that would allow us to describe each scenario in a common way. This normalized scenario development vocabulary is critical for adoption. The next step was to choose an approach to representing the tactics and techniques used by cyber actors (both attackers and defenders) and so we integrated the MITRE ATT&CK model into our scenario development process. This vocabulary is abstractly represented such that both cyber and physical attacks can be represented across a common attack and defense framework. The third step in our methodology was to develop a series of interactions that would be created using the framework objects as defined. The last step of the methodology was to provide reference implementations for research, field assessments, and exercises such that specific threat actor capabilities can be layered on top of each step of the methodology.

Gender

Male

State

United States

Authors: HEWES, Mitchell (IAEA); SPIRITO, Christopher (Idaho National Laboratory)

Presenter: SPIRITO, Christopher (Idaho National Laboratory)

Session Classification: IAEA Coordinated Research Programmes for Information and Computer Security

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