Contribution ID: **594** Type: **Paper**

Blue team support for EPS related cybersecurity readiness

In the context of penetration testing a Red Team of highly skilled IT security experts challenges the security posture of an IT infrastructure within an agreed upon perimeter.
They are countered by A Blue Team. The Blue Team identifies possible vulnerabilities and enforces the network security and the security of all digital devices. While the Red Team performs a cyberattack, the aim of the Blue Team is to provide strong defense against the ongoing cyberattack by improving and applying defense mechanisms. The Blue Team focuses on risk intelligence and data analyses, Distributed Denial of Service (DDoS) testing, log and memory analyses, etc. In this paper, we are focusing on Blue Team support and readiness for Electrical Power System (EPS) by providing suitable tools and methods to detect cyberattacks. Accordingly the Blue Team focus is not limited to an understanding of the IT, but comprises the target domain specific knowledge (NPP, EPS and I&C).
In the context of this paper, the main task for a Blue Team is to identify potential threat scenarios. This identification is done by observing a designated Simulink Model for the EPS of a nuclear power plant (NPP) and leads to knowledge about potential future attacks and the means to mitigate these by using suitable tools. Electrical power systems of a NPP are important not only for electricity generation and power supply to the house load but also essential to the safety and normal operation of a plant. Due to the rising degree of digitization within NPP, electrical protection devices have become more and more digitized. Hence, a cyber-attack could lead to a failure of one of the main electrical systems (e.g., electrical generator or circuit breaker) and can impact the operation of a NPP. A cyberattack could also cause malfunctions of primary or secondary cooling pumps in NPP by attacking the protection devices which are protecting the electric motor of the pump, in order to damage it. Therefore, electrical power systems inside a NPP should also be considered for cybersecurity related analyses.
Within the scope of the IAEA CRP J02008 project, we have modeled a simplified version of the EPS of a hypothetical nuclear facility called 'Asherah'. The model is implemented by using Matlab Simulink to provide a simulation base for cybersecurity related tests. The Simulink model encompasses mainly electrical systems inside a nuclear power plant. Main components involved in power generation, power supply to the main grid and to the house load, such as electrical generator, generator circuit breaker, auxiliary transformer and some cooling pumps as house load, are covered by the Simulink model.
In research work, we are connecting our Matlab Simulink model with a real piece of hardware (electrical protection relay, programmable logical controller, operating panel, etc.) to simulate the impact of a cyberattack on an electrical system (for e.g., an electrical motor driving a Feed Water Pump).
The Physical access to the components is also within the scope of the attack detection and evaluation process of the Blue Team. Electrical cabinets containing electrical protection devices (e.g., relays) and other electrical devices are placed in a room which is protected by physical access control. During maintenance or normal operation, an attacker could gain access with mischievous intention to these rooms where EPS digital devices are placed by violating physical access control. This could be achieved by stealing a person's ID to enter into the room and by cracking the password, by maintenance staff with access permission to the room combined with the use of infected software or privilege escalation etc.
For the test, we assume that the potential attacker has background knowledge of digital electrical devices. Cyberattacks (for e.g., Denial of Service, Man in the Middle attack, etc.) will be performed on the real hardware and network data and host data would be collected using different tools (for e.g., Wireshark) and later on anomaly detection would be performed as part of the Blue Team support to electrical systems to withstand against cyberattacks in future.
Beyond the integration of the interface of the EPS model with the real digital devices, a key benefit for the Blue Team is the exercising and training of "what if" scenarios. These can be simulated in the model and the model computes and shows what the impact at the overall EPS and NPP level will be. For these preparations the understanding (and mitigation) of the impact of an attack is essential, without regard on how the Red Team achieved the exploitation of a vulnerability at the IT and I&C level.

Gender

State

Germany

Primary author: Ms GUPTA, Deeksha (PhD Candidate)

Co-authors: Ms GOVINDARAJ, Dharini; Dr WAEDT, Karl; ALTSCHAFFEL, Robert (Otto-von-Guericke Universität Magdeburg)

Presenter: Ms GUPTA, Deeksha (PhD Candidate)

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