Contribution ID: **606** Type: **Paper**

Toward a Game-Theoretic Metric for Nuclear Power Plant Security

Modern commercial nuclear power plants rely on the seamless integration of cyber components with underlying physical processes to achieve a profitable and safe operating environment. This integration of the cyber and physical worlds offers many improvements over traditional plant systems, such as advanced instrumentation and control techniques and improved system monitoring and diagnostics. While these technologies enable significant new capabilities, they can also introduce new vulnerabilities to plant systems.

Because the cyber and physical worlds are integrated, a successful cyber attack on a nuclear power plant could result in physical damage to the system, including severe consequences such as core damage. To protect a nuclear power plant, security engineers must determine which cyber and physical defenses are required, and the degree to which those defenses must be implemented. A method is desired to accomplish two objectives: (1) to quantify the security of nuclear power plants, and (2) to determine the defenses required to reasonably ensure the plant's safe operation.

A game-theoretic approach is proposed to develop a security metric for nuclear power plants. Game theory is a mathematical technique used to analyze the interactions of multiple decision-makers, or players. Each player has a set of strategies from which to choose. The outcome of the game is dependent on the strategies selected by all the players. Each player receives a quantified utility that is dependent on the outcome of the game. At a Nash equilibrium of the game, all players have selected strategies such that their utilities have been maximized with respect to the other players' strategies. Using game theory, we can determine which defense strategies to implement to optimize the outcome of the game.

This work applies game theory to quantify the security of nuclear power plants and prioritize security measures. The game will consider the interactions of an attacker who seeks to damage the system, and a defender who seeks to protect the system. The attacker incurs expenses to attack the system and receives a gain if the attack is successful. The defender incurs expenses to attack the system and incurs a loss if the attack is successful. Once the Nash equilibrium of the game has been determined, we can determine the probability of an undesirable outcome of the game. This probability can be compared to a desired security probability threshold to determine if the plant has been adequately protected.

It is assumed that the probability of a successful attack is dependent on the strategies selected by both players. This probability can be dependent on several factors such as the attacker's knowledge of the system and the defender's configuration of off-the-shelf components. By manipulating the factors that are within the defender's control, the probability of an undesirable outcome can be reduced. The degree of implementation of a defense can be selected such that the probability of an undesirable outcome is less than the desired probability threshold.

The game-theoretic security technique is demonstrated on a simplified pressurizer system. Failure conditions are identified for the system using fault tree analysis. Economic parameters are assumed for the attacker and defender, and the Nash equilibrium is determined. The optimal defense strategy and degree of implementation are identified to achieve a required security probability requirement.

State

United States

Gender

Primary authors: LAMB, Christopher (Sandia National Laboratories); Mr MACCARONE, Lee (Sandia National Laboratories)

Presenters: LAMB, Christopher (Sandia National Laboratories); Mr MACCARONE, Lee (Sandia National Laboratories)

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