2019 IEEE Special Session: Cybersecurity and Electromagnetic Systems

Cyber Resilience via Modeling & Simulation and Operations Analysis

Ambrose Kam

Lockheed Martin RMS (Moorestown, NJ)

Abstract— Driven by operational efficiency, costs and convenience, interactions between cyber world and physical systems are increasing steadily over the past two decades. Devices such as industrial control systems (ICS) are pervasive with the advent of Internet of Things and Supervisory Control and Data Acquisition systems (SCADA). Along with the complexity of the interactions comes the rise in potential of cyber threat exposure. This means that the ICS devices in our homes, offices and cars are potential attack vectors that cyber hackers could take advantage of. These threats come in various forms, targeting from the simplest API calls to the intricate interaction of subsystems. The reliability of these critical systems depends a lot on the system's cyber resilience level, which is determined by two key variables: survivability and recovery time. Originally derived the National Institute of Standards and Technology (NIST) and Accenture's cyber resilience frameworks, these 2 variables can be further broken down into 4 pillars: Preparedness, Mitigation, Response and Recovery. Directly underneath the foundation of these 4 pillars are threat assessments and vulnerability analyses.

Through university partnerships, Lockheed Martin (LM) has worked with world renowned institutions like Massachusetts Institute of Technology (MIT) and Georgia Tech (GT) to jointly research the areas of cyber risk analysis and resilience. The cornerstone of these research efforts was developing the means to understand the existing and emerging threat behaviors and their impacts on infrastructure prot6ection. LM leverages its wealth of experiences in modeling & simulation (M&S) and operations analysis (OA) capabilities. MIT brings its expertise in risk management and contribute to the research by leveraging the Situational Awareness Framework for Risk Ranking (SAFARI) platform. The MIT team investigates a risk modeling and data analytics platform that identifies risk tolerance and strategy for assessing, responding to, and monitoring cyber security risks. Georgia Tech team brings its expertise in malware behavioral analysis; through research and reverse engineering, malware behaviors can be replicated in a closed environment so that remedies could be developed and tested efficiently.

This presentation will discuss how these research efforts and industrial experiences can contribute to a more cyber resilient infrastructure through the use of M&S and OA techniques. We will also discuss our methodology in modeling cyber threats and how cyber resilience metrics can be quantified in our simulation environment.