

System-Aware Cyber Security Architecture

Rick A. Jones
Systems and Information
Engineering
University of Virginia
Charlottesville, VA, 22904
Phone: 434-260-1531
Email: raj2u@virginia.edu

Barry Horowitz (PI)
Systems and Information
Engineering
University of Virginia
Charlottesville, VA, 22904
Phone: 434-924-0306
Email: bh8e@virginia.edu

Presentation Abstract

The presentation will begin with a description of System-Aware Cyber Security, an architectural formulation that embeds security solutions as tightly coupled parts of the system to be protected through reusable security services in order to mitigate the growing risk posed by insider and supply chain attacks. An architectural approach that integrates fault tolerant system concepts with advanced cyber security concepts is introduced. This will include an overview of several reusable security services, including (1) the ability significantly increasing the difficulty for adversaries by avoiding a monoculture environment through the integration of a diverse set of redundant subsystems involving hardware and software components provided by multiple vendors, (2) the development of subsystems that are capable of rapidly changing their attack surface through hardware and software reconfiguration (configuration hopping) in response to perceived threats, (3) data continuity checking services for isolating faults and permitting moving surface control actions to avoid continuing operations in a compromised configuration, and (4) forensic analysis techniques for rapid post-attack categorization of whether a given fault is more likely the result of a cyber attack than other causes (i.e. natural failure). To illustrate how these System-Aware security services could potentially deter and/or defend against insider and supply chain attacks, an example System-Aware security solution is presented. This example will focus on protecting a nuclear power turbine control system from two specific threats, including a discussion of how the security services employed would increase the difficulty to an adversary and a high-level assessment of the benefits and cost. In addition, an initial outline for a methodology for comparing and assessing System-Aware security architectures will be presented. This will include an overview of the legacy of work in the field of safety that serves as a basis for the methodology and a description of the proposed methodology. Finally, we will summarize future research that is necessary to facilitate implementation across additional domains critical to the nation's interest.