Methodology to Estimate Attack Graph System State from a Simulation of a Nuclear Research Reactor

Title	Methodology to Estimate Attack Graph System State from a Simulation of a Nuclear Research Reactor
Publication Type	Conference Paper
Year of Publication	2018
Authors	Nichols, W., Hawrylak, P. J., Hale, J., Papa, M.
Conference Name	2018 Resilience Week (RWS)
Date Published	aug
Keywords	attack graph, attack graph system state, Attack Graphs, composability, cyber-physical system, Cyber-physical systems, cybersecurity, Databases, formal verification, graph theory, hybrid attack graph, Inductors, Metrics, nuclear engineering computing, nuclear research reactor, Predictive models, pubcrawl, resilience, Resiliency, safety-critical applications, safety-critical software, SCADA System Security, security of data, security testing, state estimation, Temperature sensors, Tools, verification procedure, Vulnerability Evaluation
Abstract	Hybrid attack graphs are a powerful tool when analyzing the cybersecurity of a cyber-physical system. However, it is important to ensure that this tool correctly models reality, particularly when modelling safety-critical applications, such as a nuclear reactor. By automatically verifying that a simulation reaches the state predicted by an attack graph by analyzing the final state of the simulation, this verification procedure can be accomplished. As such, a mechanism to estimate if a simulation reaches the expected state in a hybrid attack graph is proposed here for the nuclear reactor domain.
DOI	10.1109/RWEEK.2018.8473465
Citation Key	nichols_methodology_2018

Databases Predictive models safety-critical software security of data tools resilience Temperature sensors pubcrawl Metrics Resiliency composability graph theory Cybersecurity cyber-physical systems attack graph attack graph system state cyber-physical system formal verification hybrid attack graph Inductors nuclear engineering computing nuclear research reactor safety-critical applications SCADA System Security security testing state estimation verification procedure Vulnerability Evaluation attack graphs