Pacific Northwest
NATIONAL LABORATORY
Proudly Operated by Battelle Since 1965

Optimization and Stochastic Algorithms for Asymmetric Resilient Infrastructure

CHALLENGE

Recent cybersecurity incidents involving data theft from the U.S. Office of Personnel Management, have heightened the importance of designing resilient cyber systems that can support mission goals when compromised. Securing any system on a continual basis against attacks is an ongoing challenge. System defenders typically have limited protective resources that need to be effectively allocated to thwart attackers operating at relatively low costs. Game-theoretic approaches are increasingly being adopted for such cybersecurity challenges. To effectively deploy such methods one must account for uncertainties in attack types and cyber system operational behaviors over time, which is the challenge that we address in this project.

Developing a mathematical framework to enable defenders with limited budget to gain asymmetrical advantage over attackers

CURRENT PRACTICE

Previous literature on cybersecurity indicates further scope for development of attacker payoff uncertainty quantification methods. This includes addressing aleatory and epistemic uncertainties in: (1) attacker types and their plans, and (2) system behavior under varying attack conditions. In the physical security domain, probability distributions and intervals have been proposed to address attacker payoff uncertainties. However, in the cyber domain there are also uncertainties associated with the state of the system following an attack that should be incorporated within the uncertainty framework. Inspired by the advances in the physical security domain, and the challenges within a cyber-setting, we present an integrated attacker payoff uncertainty quantification framework.

Proposed payoff uncertainty quantification framework

U.S. DEPARTMENT OF
ENERGY

APPROACH

Game-theoretic approaches can be used to solve several cybersecurity problems. However, several sources and types of uncertainty impacting cyber attacker payoffs (defined as a penalty or reward based on actions) make game-theoretic solutions challenging. These uncertainties arise due to randomness or lack of knowledge associated with cyber system operational behaviors, attacker types, and attack and defense actions over time. In this project we propose a probabilistic modeling framework for representing cyber attacker payoffs under uncertainty. We develop a conditional probabilistic reasoning approach to organize the dependencies between a cyber system's state, attacker type, player actions, and state transitions.

The payoff uncertainty quantification framework is based on systems analysis, probability theory, and utility theory. Within this framework, uncertainty is modeled through marginal, joint, and conditional probability distributions associated with parameters of a stochastic cybersecurity game (see Figure). There are five elements within this modeling framework:

1. Probability of initial cyber system state
2. Probability of attacker type
3. Probability of player action choices
4. Probability of cyber system state transitions over time
5. Probability of attacker payoff utility. An underlying assumption here is that the cyber system is already compromised; as a result, issues related to sensing during an attack are beyond the scope of this study.

IMPACT

Game-theoretic approaches have been used to solve a broad class of problems related to cybersecurity such as intrusion detection and intrusion prevention, risk assessment, wireless jamming problems, and cyber resilience. These methods are applicable to a broad set of users from cyber defenders to system architects. However, a fundamental limitation of these approaches is the lack of information and mathematical methods to handle uncertainty. Consequently, the unified mathematical framework proposed and developed in this project will have significant impact on a wide variety of cybersecurity solutions based on game theory.

Contact

Mahantesh Halappanavar
Principal Investigator
(509) 372-5987
hala@pnnl.gov

Samrat Chatterjee
Co-Principal Investigator
(509) 375-3957
samrat.chatterjee@pnnl.gov

Pacific Northwest
NATIONAL LABORATORY

Proudly Operated by Battelle *Since 1965*