CHALLENGE

Effective cyber defense requires characterization of system state, knowledge of attacker and defender activities, and the relationship between them in order to make effective decisions. However, in the real world, there is imperfect knowledge of both attacker and defender behavior, so one must think in terms of uncertainties. The Rendezvous approach enables users to explore attacker and defender scenarios in the presence of system and attack related uncertainties, and recommends best choice options for defense.

APPROACH

Rendezvous is a decision-support engine that generates optimal cyber defense recommendations in a dynamic setting with imperfect information. Behind the scenes, the tool uses game theory to evaluate consequences and outcomes of adversary and defender actions. This is done without assuming perfect knowledge of either the attacker or the state of the system. The attacker’s perspective is explored using a wide range of attack classes, and the defender’s actions can be tuned to match the environment of the defender. System state transitions are based on attack and defense options within a Markovian setting. Mathematical solvers within a simulation setting generate recommended defense actions based on the results of an ensemble of games.

A flexible recommendation engine, providing decision support to human-focused or automated systems with special emphasis on capturing uncertainty in state measures.

Given data, models, and assumptions, we compute a distribution of policies (1), assign initial belief about the cyber-system state (2), recommend an action based on the computed policies and initial belief (3), observe final system state based on executed action (4), and update the system state belief based on current belief, action, and observation (5).
METHODOLOGY

Inspired by advances in solving strategic card games such as poker, the Rendezvous approach consists of reformulating mathematical games that account for imperfect information for use in cybersecurity decision-support. In this setup, a simulated defender repeatedly interacts with multiple attack classes under partially observable conditions. Uncertainty is characterized through stochastic state transition and observation models. In addition to recommendations for defender action, recommended policies (mapping of actions to states) are also generated. Using the transition and attacker’s policy models, transition and reward models for the defender are developed. The defender summarizes all their past information in a compact form, and every time the defender executes an action and receives an observation, that form is updated. Mathematical solvers are implemented within a simulation setting to run multiple times for a class of models, while accounting for imperfect information and partial observability. As a result, policies and actions generated are based on an ensemble of games. A simulated defender maps actions to states and determines actions that will provide the most favorable outcomes in a time-varying setting.

IMPACT

In the real world with imperfect information and multiple sources and types of uncertainties associated with cyber systems, the Rendezvous decision-support action recommendation engine generates optimal cyber defense actions that operators may choose from to maximize the system’s ability to continue mission critical operations. The recommendation engine is flexible and tunable to fit specific operating environments; may consist of defensive, offensive, or deceptive strategies; and can be tailored for attack surface reduction/shifting, dynamic proactive defense, as well as adaptive intrusion response needs.

Workflow for dynamic decision-support implementation

Contacts

Sam Chatterjee, Ph.D.
Principal Investigator
(509) 375-3957
samrat.chatterjee@pnnl.gov

Chris Oehmen
Initiative Lead
(509) 375-2038
chris.oehmen@pnnl.gov