Science

Advanced Computing, Mathematics and Data Division Research Highlights

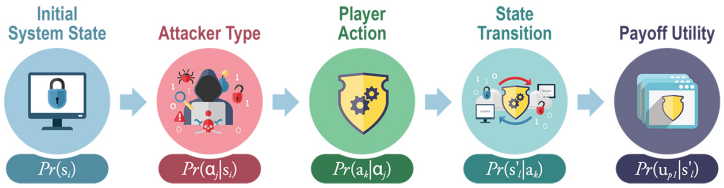
January 2016

Captured by the Game

Game theoretic approaches up the ante on defending cybersecurity resources

Results: While the notion of "players," "actions," and "payoffs" may seem more suited to Las Vegas gaming tables, game theory as a mathematical tool has steadily grown in cyber defense applications. In ongoing and progressive work being conducted under PNNL's Asymmetric Resilient Cybersecurity initiative, scientists have taken on the challenge of addressing the sources and types of uncertainty that can arise in realizing a resilient cyber system. Already, their work on quantifying uncertainties in cyber attacker payoffs within randomly determined security games has been recognized with an IEEE Best Paper award. Meanwhile, their latest publication presents a probabilistic modeling framework for representing and propagating uncertainties in cyber attacker payoffs with the added goal of increasing awareness among researchers about this problem domain.

Why it Matters: As the volume and intensity of cybersecurity incidents continue to escalate, anticipating and combating cyber system attacks becomes increasingly critical to successful system defense. Decision-makers must turn to mathematical models, such as the framework proposed in this current work, that aid in strategic planning and support effective, efficient, and preemptive protective resource allocation.



Attacker Payoff Uncertainty Quantification Framework
Enlarge Image.

Methods: In their work, the authors describe a proba¬bilistic modeling framework for representing cyber attacker payoffs, which they define as "penalties" or "rewards" based on actions, under uncertainty. A conditional probabilistic reasoning approach organizes the dependencies between different sources of cyber attacker payoff uncertainty and enables application of probabilistic theo¬ries (that involve modeling random events) to disseminate various uncertainties in the attacker payoffs.

"There are multiple sources of uncertainty that need to be addressed in trying to protect a system," explained Samrat Chatterjee, a scientist with PNNL's National Security Directorate (NSD) Operations Research Team and the paper's primary author. "For example, not being able to observe the 'overall' system at once and not knowing the attacker's capabilities or what that attacker might be after. The dilemma is in accounting for these uncertainties when you are forced to make decisions—whether you have information or not."

As such, the framework has been designed to respond to or anticipate cyber-system attacks from intelligent adversaries by enhancing cyber defender resource allocation models.

Matthew Oster, also from the NSD Operations Research Team and another co-author, suggested considering a scenario where an attacker attempts to steal data from a workstation and must navigate through multiple firewalls and servers. Basically, this attacker seeks to disrupt the system from its normal operations to a degraded state.

“The framework captures and models interdependencies between various sources of cyber attacker payoff uncertainty, including cyber system state, attacker type, player actions, and system transitions over time,” Oster said. “So, in our data breach scenario, we end up with a probabilistic representation of the potential attacker payoff that reflects uncertainty across all states, types, actions, and transitions.”

Different versions of attacker payoff probability distributions also may be used as inputs in cybersecurity games that weigh the pros and cons of engaging in a particular security resource strategy for achieving resilient cyber system designs.

Ramakrishna Tipireddy, a postdoctoral researcher with the Advanced Computing, Mathematics, and Data (ACMD) Division’s Computational Mathematics group, who contributed the mathematical formulations of probability distributions featured in the paper, explained: “The framework is flexible enough to summarize information at various levels of granularity, including a certain system state or across all states, allowing decision priorities to be made using available inputs.”

“It is not simply one size fits all,” Chatterjee added.

What’s Next? The team continues to expand and improve on its game theoretic approaches to address uncertainties within cyber defense applications and hopes their current work encourages further advancements in this complex research area.

“The primary problem in achieving cyber resilience is that there are too many uncertain variables, and we simply cannot protect every asset all of the time,” noted Mahantesh Halappanavar, a scientist with ACMD Division’s Data Sciences group. “Our new application of game theory allows for consideration of probabilities that are rigorous enough to provide useful solutions that have practical impact. Still, if we want to build systems that can remain stable and operational even when compromised, there is much more work to do.”

In addition to their already published work, the authors have two additional papers exploring uncertainties and identifying vulnerabilities using cybersecurity game concepts submitted for consideration by the 2016 IEEE International Symposium on Technologies for Homeland Security.

PNNL Research Team: Samrat Chatterjee, NSD Operations Research Team; Ramakrishna Tipireddy, Computational Mathematics, ACMD Division; Matthew Oster, NSD Operations Research Team; and Mahantesh Halappanavar, Data Sciences, ACMD Division. Sudip Saha, from Virginia Tech, also contributed to aspects of this work.

Acknowledgments: The work was supported by PNNL’s Asymmetric Resilient Cybersecurity initiative.

References:

- Chatterjee S, R Tipireddy, M Oster, and M Halappanavar. 2015. “A Probabilistic Framework for Quantifying Mixed Uncertainties in Cyber Attacker Payoffs.” *National Cybersecurity Institute Journal* 2(3):13-24. Available online: http://ncij.excelsior.edu/volume-2-number-3/.
- Chatterjee S, R Tipireddy, M Oster, and M Halappanavar. 2016. “Propagating Mixed Uncertainties in Cyber Attacker Payoffs: Exploration of Two-phase Monte Carlo Sampling and Probability Bounds Analysis.” Submitted to *2016 IEEE International Symposium on Technologies for Homeland Security*.
- Saha S, AKS Vullikanti, M Halappanavar, and S Chatterjee. 2016. “Identifying Vulnerabilities and Hardening Attack Graphs for Networked Systems.” *Submitted to 2016 IEEE International Symposium on*

Technologies for Homeland Security.

Related:

- **They've Got Game**
