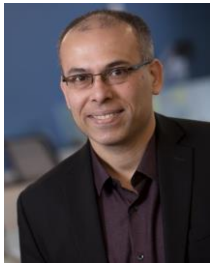
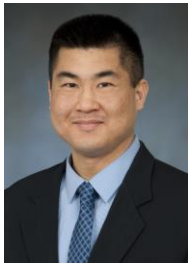
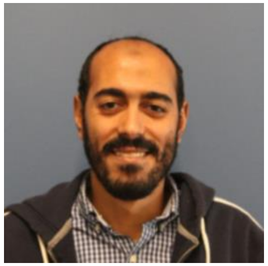
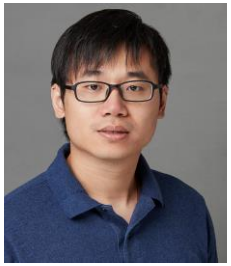
Game Theory and Distributed System Security

Co-leads: Saurabh Bagchi (Purdue University & KeyByte)
Kevin Chan (Army Research Lab)

Scribes: Mustafa Abdallah (Purdue University)
Xing Gao (U of Delaware)

Slides: https://bit.ly/satc22pres2 Survey: https://bit.ly/satc22postsurvey

Topic Context: Status and Gap

- There has been significant work in understanding vulnerabilities in large-scale distributed systems and putting technological patches to address specific classes of vulnerabilities.
  - However, the works often lack understanding of the impact of cascading attacks or mitigation on the resilience of the overall system.
  - Due to the large legacy nature of many distributed infrastructures and budgetary constraints, a complete re-architecting and strengthening of the system is often not possible.
  - Rather, rational decisions need to be made to strengthen parts of the system, taking into account the risks and the interdependencies among the assets.

Topic Context: Open Questions

- While static game theory has been extensively studied for several decades, the large-scale distributed systems present critical challenges that preclude the direct application of existing theory.
  - Specifically, there is a need for new techniques to account for both the interdependencies and the dynamical nature of the subsystems.
  - Furthermore, some of these dynamical subsystems may be complex in their own right (e.g., a perception system that employs multi-modal sensors) and may only be represented by simulation models.
- Questions
  - Can the security community extend traditional game theory to develop tractable analysis and design techniques that can be applied to security of large-scale interdependent distributed systems?
  - Can the community learn from behavioral economics where human biases are taken into account in decision making?
  - Can that be incorporated into traditional game theory to understand the effect of biases on security decision making and possible mitigation actions.

Analytical Directions

Near term
Medium term

- Personalized learning
  - Different individuals learning differently at different rates
  - Human vs machine learning
- Incorporating biases and incomplete information
  - Cognitive biases of human players
  - Asymmetric knowledge, asymmetric capabilities
  - Partial cooperation/collusion among players
- Scalability and Tractability
  - Rigorous approximation of game theoretic formulation
  - Allows one to produce bounds for best-case/worst-case outcomes
  - Use epidemic theory to analyze effect of cascading attacks
  - Handles case of large numbers of players
- Incorporating stochastic behavior in game theoretic formulation
  - Machine learning integrated with game theory
  - Failures and attacks are inherently stochastic in nature

Systems Directions

Near term

Medium term

- Resource-aware defenses
  - Different nodes have different capabilities and available resources
  - Calibrate defense mechanism using (possibly dynamic) node-specific attributes
  - Cost of attack may also be varying, e.g., cost to corrupt data
- Security guarantees are a function of current system state
  - Guarantees are a function of number and capability of attackers and defenders rather than an absolute
  - Dynamic property varying with the system state
  - Hardware degrades, software ecosystem changes over time
  - Function of level of collusion among attackers (non Byzantine+Byzantine attackers)
- Designing for security in the tradeoff space of (performance, resource usage) and security
  - Example: Use hardware-level virtualization rather than containers
  - Specialized functions reducing attack surface
  - Makes debugging easier

Integration Directions

Near term
Medium term

- Security of distributed systems in CPS domain
  - Interdependent systems
  - Nodes embedded in physical environment and subject to environmental effects
  - Some parts of system are opaque to defenders
- Continuous verification
  - Are our models and practical software instantiations generating useful results even under attacks and perturbations
  - Use sparse human feedback online
  - Use incremental verification/testing methodologies
  - Verification of highly non-linear ML models
- Integrated evaluation environments
  - Some common base, then specialization for different domains
  - Evaluate different action spaces and mechanism designs
  - Evaluate red/blue team, educate policy makers using results
  - Evaluate different capabilities of attackers/defenders