Learning about Protecting Distributed Infrastructure from Behavioral Economists

Saurabh Bagchi
ECE & CS, Purdue University

Joint work with:
ECE: Shreyas Sundaram, Mustafa Abdallah
Economics: Tim Cason, Daniel Woods

Supported by NSF SaTC grant CNS-1718637 (2017-20)
Security is Only Too Human

• Security of large-scale systems (such as the power grid, industrial plants, and communication and computer networks) depend critically on human decisions.

• A few thousand papers on optimal decision making for protecting interconnected systems.

• But relies on classical economic models of perfectly rational and optimal behavior for human decision-makers.

• But behavioral economics shows humans are only partly rational and thus, consistently deviate from the above-mentioned classical models.
Behavioral Weighting Function

- Human perceptions of rewards and losses can differ substantially from their true values.
- These perceptions can have a significant impact on the investments made to protect the systems that the individuals are managing.

- Humans overweight low attack probabilities and underweight large attack probabilities.
- Example: Prelec [1998] weighting function:
  - \( w(x) = \exp(-(-\ln(x))^\alpha) \)
  - where parameter \( \alpha \in (0,1] \).
What’s Nobel Got to Do With It?

Richard Thaler (2017 Economics Nobel Laureate): “I discovered the presence of human life in a place not far, far away, where my fellow economists thought it did not exist: the economy.”

Prospect theory as a model of decision making under risk as a counterpoint to expected utility theory.
Our Research Direction

- **Game-theoretic framework** involving attack graph models of large-scale interdependent systems and multiple defenders
- Each human defender misperceives the probabilities of successful attack in the attack graph
- We characterize impacts of such misperceptions on the security investments made by each defender

- The cost of a defender $D_k$ is:

$$C_k(x) = \sum_{u_m \in V_k} L_m \left( \max_{P \in \mathcal{P}_m} \prod_{(u_i, u_j) \in P} w(p_{i,j}(x)) \right)$$
Initial Observations

- Both games (vertex based and path based) have **Convex cost function** given a convex decreasing probability function.
- Both games have a **Pure Nash Equilibrium (PNE) state**.
- In each game, we can compute the best response by solving a convex optimization problem.
- They have **different investment decisions** than standard security game which maximizes expected utility.
- A rational player **can benefit** from a biased player.

Both players rational

Player 2 biased

Overall Loss = 18.1436

Overall Loss = 0.3616