TASHAROK: Using Mechanism Design for Enhancing Security Resource Allocation in Interdependent Systems

Mustafa Abdallah[1], Parinaz Naghizadeh[2], Daniel Woods[3], Issa Khalil[4], Timothy Cason[1], Shreyas Sundaram[1], and Saurabh Bagchi[1]

1: Purdue University; 2: Ohio State University; 3: University of Innsbruck; 4: Qatar Computing Research Institute

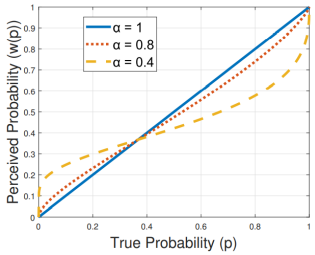
Introduction

- Interdependent systems, such as the power grid, consist of a large number of assets managed by multiple stakeholders (i.e., defenders)
- Defenders have to judiciously allocate their (often limited) security budget to reduce their security risks
- Particularly challenging for large-scale systems, i.e., with huge number of assets
- Security investments critically depend on:
  - ❑ How human decision-makers perceive the risk (probability) of being attacked successfully
  - ❑ Degree of interdependency among different CPS defenders

Research Question:
For large-scale interdependent systems, can we mitigate the impacts of suboptimal security investments allocated by human defenders and enhance system's security cost?

Motivation

- Humans overweight low probabilities and underweight large probabilities
- Probability weighting functions transform true probabilities p into perceived probabilities $w(p)$
- Example: Prelec [1998] weighting function:
  $w(p) = \exp(-(-\ln(p))^{\alpha})$
  where parameter $\alpha \in (0,1]$



- The dashed lines shows the non-linear perception of the probability of successful attack by behavioral defender.
- The solid line gives the perception of rational defender who perceives the probability of attack in a true manner (correctly)
  - There is a cross-over point such that the true probability is the same as the perceived probability where probabilities greater than this point is underweighted and probabilities less than this point is over weighted
  - Therefore, TASHAROK uses this probability weighting function to identify whether the defender is a rational decision-maker or not

Our Contributions: TASHAROK

- Proposes a security investment guiding technique for guiding defenders in interdependent systems
- Adapts two mechanism designs for interdependent security games modeled by attack graphs
- Shows a rigorous investigation of the impacts of behavioral perceptions of security risk and selfishness of PNE decision-making on system security
- Analyzes the different parameters that affect the mechanism outcomes for four real-world interdependent systems, such as types of defense mechanisms, the tax amount under central regulation, voluntary participation, and sensitivity of edges

Model Overview

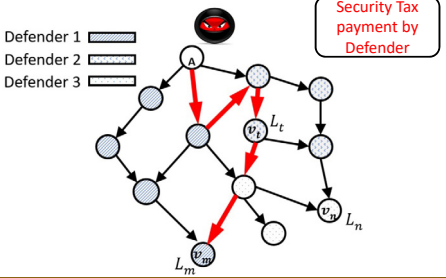
- **Security risk of an asset:** probability of attack on the asset on the path that has the highest probability of success for the attacker
- The cost of defender D_k is given by

$$C_k(x) \triangleq \sum_{v_m \in V_k} L_m \left(\max_{P \in \mathbb{P}_m} \prod_{(u_i u_j) \in P} w(p_{ij}(x)) \right)$$

- Each player misperceives the risk on each edge
- Mechanism Design Setup

$$C_k(\mathbf{x}, \mathbf{t_k}) = C_k(\mathbf{x}) + t_k$$

Security Tax payment by Defender



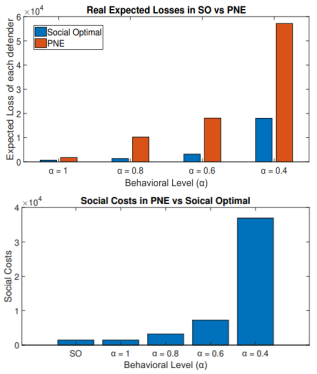
Properties of Mechanism Design

- **Theorem:** The Behavioral Games possess a Pure Nash Equilibrium (PNE) for $0 < \alpha < 1$
- **Theorem:** The tax-based incentive mechanisms cannot implement the socially optimal solution, while guaranteeing weak budget balance, in all instances of interdependent security games
- **Theorem:** Under Externality mechanism, the tax paid by defender D_k is a decreasing function in behavioral level α_k (i.e., , the behavioral defender pays more taxes compared to a rational defender)

Evaluation

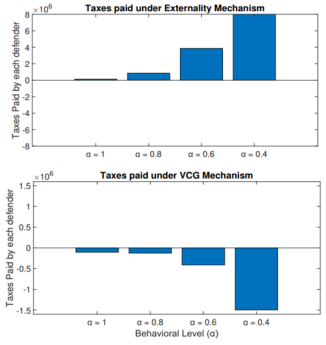
- We evaluate our model on four real-world systems:
  - ❑ Distributed energy resource (DER) and SCADA industrial control system, following NIST guidelines
  - ❑ Voice-over-IP (VoIP) and E-commerce systems

Defense Mechanism (Social Optimal VS PNE)



- The socially optimal solution is **more efficient for the system and for each defender** as well
- **66.8% reduction in total loss** if both defenders are highly behavioral ($\alpha = 0.4$)
- Social Planning is **more beneficial for behavioral stakeholders**

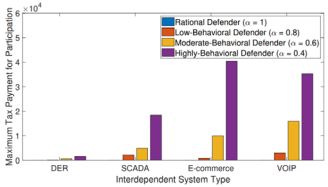
Effect of Behavioral Bias on Tax Payment



- In Externality mechanism, each defender pays **tax amount proportional to her benefit of other defenders investments**
- Under the VCG Mechanism, **the player receives payment due to her contribution on enhancing social cost**

Key Insight:
The amount of taxes increases as the stakeholders (defenders) become more behavioral

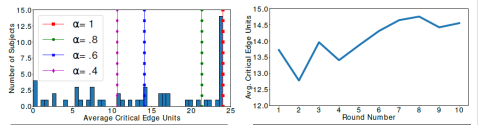
Voluntary Participation in Central Mechanism



- We consider **both compulsory and voluntary participation**
- **Behavioral defenders participate under higher tax amount**

Human Subject Experiments

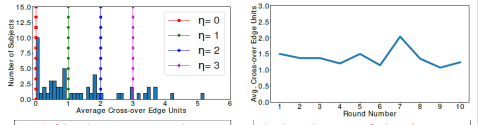
A) Probability Weighting Bias



24% of the subjects makes rational decisions
76% of the subjects are behavioral

20.45% makes worse decisions in later rounds, 45.45% exhibits no learning across rounds, 34.10% improves their investments.

B) Spreading Heuristics Bias



18.5% of the subjects are non-spreaders
81.5% of the subjects are spreaders

This shows the average of subjects' investments on the crossover edge in each round, which shows a weak downward trend.

Prior Work

- Majority of existing work has focused on classical game theoretic models of rational decision making on large scale systems modelled by attack graphs [Sheyner-IEEE Security and Privacy 02], while we [Abdallah- IEEE S&P 22] analyze behavioral models of decision making in these systems
- A notable departure from classical economic models within the security and privacy literature is in [Acquisti-IEEE Security and Privacy 09], which identifies the effects of behavioral decision making on individual's personal privacy choices.
- The problem of security resource allocation under behavioral decision-making was studied [Abdallah-TCNS20]. However, this work has not taken into account the mitigation of such suboptimal security investments.
- The work [Naghizadeh-INFOCOM16] provides a theoretical treatment of mechanism design in certain specific classes of interdependent security games. That research, however, does not consider the more realistic attack scenarios (i.e., considered no dependencies) and systems that we consider here and did not consider behavioral bias.

Acknowledgments

This work is supported by NSF SaTC grant CNS-1718637, and Purdue WHIN center. Any opinions, findings, and conclusions or recommendations expressed here are those of the authors and do not necessarily reflect the views of the funding agencies.

References

[1] Oleg Sheyner, Joshua Haines, Somesh Jha, Richard Lippmann, and Jeannette M Wing. "Automated generation and analysis of attack graphs". In IEEE Symposium on Security and Privacy, pp. 273-284, IEEE, 2002.

[2] Mustafa Abdallah, Daniel Woods, Parinaz Naghizadeh, Issa Khalil, Timothy Cason, Shreyas Sundaram, and Saurabh Bagchi "TASHAROK: Using Mechanism Design for Enhancing Security Resource Allocation in Interdependent Systems." IEEE Symposium on Security and Privacy (SP), San Francisco, 2022.

[3] Alessandro Acquisti. "Nudging privacy: The behavioral economics of personal information." IEEE security and privacy, 2009.

[4] Mustafa Abdallah, Parinaz Naghizadeh, Ashish Hota, Timothy Cason, Saurabh Bagchi, and Shreyas Sundaram, "Behavioral and game-theoretic security investments in interdependent systems modeled by attack graphs" IEEE Transactions on Control of Network Systems, vol 7, pp. 1585-1596, 2020.

[5] Parinaz Naghizadeh and Mingyan Liu, "Exit equilibrium: Towards understanding voluntary participation in security games," in IEEE INFOCOM 2016-The 35th Annual IEEE International Conference on Computer Communications. IEEE, 2016, pp. 1-9.