A Behavioral Game Modeling Cyber Attackers, Defenders, and Users

Sarah Kusumastuti\textsuperscript{1,2}, Jinshu Cui\textsuperscript{1,2}, Arjun Tambe\textsuperscript{1}, and Richard S. John\textsuperscript{1,2}

\textsuperscript{1}Center for Risk and Economic Analysis of Terrorism Events (CREATE) 
\textsuperscript{2}Department of Psychology 
University of Southern California
Outline

• Motivation of a three-way behavioral game
• Experiment Design
• Simulation
3-Player Cyber Security Game
Sequential Cyber Security Game with Simultaneous Play

- Cyber Attacker Chooses Strategy Under Uncertainty
- Uncertainties
  - Defender (System) Defense
  - User Defense (Compliance) and Response
  - Exogenous Uncertainties
Alternatives and Interactions

**Attacker:**
- Alternatives:
  1. Expend resources to obtain a capability/search for system’s vulnerability
  2. Attack the system
  3. Attack individual users
- Long-term (system) vs. short-term (user)

**Defender:**
- Alternatives: 3 security levels
- tradeoff between protecting both system and users and user compliance

**User:**
- Alternative: 3 security levels
- Protect users
Influence Diagram

- Decisions

- Outcomes

- Exogenous variables
Components that Differentiate Players

• Heuristics and Biases
  – sensitive to experience
  – sunk cost effects
• Multiple objectives
  – attacker: maximize financial gains, maximize fear, minimize chance of detection
  – defender: maximize protection, minimize efforts, maximize user compliance
  – user: maximize productivity, maximize protection
• Risk Attitudes
  – risk averse, risk seeking, risk neutral
## Parameters – Attacker

<table>
<thead>
<tr>
<th>Attack system</th>
<th>Attacker</th>
<th>probability of success (%)</th>
<th>cost</th>
<th>reward if succeed</th>
<th>penalty if fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>first step: obtain capability</td>
<td></td>
<td>50</td>
<td>$0.5</td>
<td>$0</td>
<td>$0</td>
</tr>
<tr>
<td>second step: attack database</td>
<td>Defender: low</td>
<td>70</td>
<td>$0.5</td>
<td>$5</td>
<td>$2</td>
</tr>
<tr>
<td></td>
<td>Defender: medium</td>
<td>50</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Defender: high</td>
<td>30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attack user</td>
<td>Defender: low</td>
<td>90</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>User: low</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>User: medium</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>User: high</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defender: medium</td>
<td>User: low</td>
<td>60</td>
<td>$0.5</td>
<td>$1</td>
<td>$0</td>
</tr>
<tr>
<td></td>
<td>User: medium</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>User: high</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Defender: high</td>
<td>User: low</td>
<td>30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>User: medium</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>User: high</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Parameters – Defender

<table>
<thead>
<tr>
<th>Defender</th>
<th>protection rate (%)</th>
<th>cost</th>
<th>penalty if fail</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>protect system</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>low</td>
<td>30</td>
<td>$0.25</td>
<td>$2</td>
</tr>
<tr>
<td>medium</td>
<td>50</td>
<td>$0.5</td>
<td>$2</td>
</tr>
<tr>
<td>high</td>
<td>70</td>
<td>$1</td>
<td>$2</td>
</tr>
<tr>
<td><strong>protect user</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>low</td>
<td>User: low</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User: medium</td>
<td>40</td>
<td>$0.25</td>
</tr>
<tr>
<td></td>
<td>User: high</td>
<td>70</td>
<td></td>
</tr>
<tr>
<td>medium</td>
<td>User: low</td>
<td>20</td>
<td>$0.5</td>
</tr>
<tr>
<td></td>
<td>User: medium</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User: high</td>
<td>80</td>
<td></td>
</tr>
<tr>
<td>high</td>
<td>User: low</td>
<td>30</td>
<td>$1</td>
</tr>
<tr>
<td></td>
<td>User: medium</td>
<td>60</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User: high</td>
<td>90</td>
<td></td>
</tr>
</tbody>
</table>
## Parameters – User

<table>
<thead>
<tr>
<th>User</th>
<th>protection rate (%)</th>
<th>cost</th>
<th>penalty if fail</th>
</tr>
</thead>
<tbody>
<tr>
<td>low</td>
<td>Defender: low</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Defender: medium</td>
<td>20</td>
<td>$0</td>
</tr>
<tr>
<td></td>
<td>Defender: high</td>
<td>30</td>
<td>$1</td>
</tr>
<tr>
<td>medium</td>
<td>Defender: low</td>
<td>40</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Defender: medium</td>
<td>50</td>
<td>0.5</td>
</tr>
<tr>
<td></td>
<td>Defender: high</td>
<td>60</td>
<td>$1</td>
</tr>
<tr>
<td>high</td>
<td>Defender: low</td>
<td>70</td>
<td>$1</td>
</tr>
<tr>
<td></td>
<td>Defender: medium</td>
<td>80</td>
<td>$1</td>
</tr>
<tr>
<td></td>
<td>Defender: high</td>
<td>90</td>
<td>$1</td>
</tr>
</tbody>
</table>
Scenario

• “Tegrat” is a very popular online store in the US. Customers can shop online with their Tegrat Accounts. “Lisi”, a group of phishing attackers are choosing from two ways to obtain customers’ online payment information at Tegrat.

• Lisi can obtain customers’ payment information one by one by targeting on individual accounts. Using multiple phishing techniques the attackers can obtain usernames and passwords of individual accounts and then get access to those accounts and gather payment information. They can also obtain hundreds of payment information with one-time attacking by targeting on the accounts owned by Tegrat’s online system database administrators. However, Lisi need to first “locate” those administrators, for instance, locate their email address, devices, IP address, etc. After locating the administrators who have access to Tegrat’s database, Lisi can use the same phishing techniques and procedures to get access to Tegrat’s database. Lisi can then seize a large amount of payment card data from the database. In a word, Lisi need to choose from generic attacks that play the numbers game, hoping to get victims on volume and focused attacks that have a small number of targets, and keep taking shots until they get a hit.
Scenario

• On the other hand, Tegrat has several ways to protect their users’ payment data. The simplest one is to require longer passwords when logging in from both their administrators and online customers. They can also install two-factor authentication besides requiring longer passwords, which forces all logins to enter a second, one-time password in addition to their usual credentials. A third way is to require a new password different from used passwords every week besides longer passwords requirement and two-factor authentication.

• To protect themselves from phishing attack, online customers also have three measures. They can either never click on the links in emails and instead type the address into address bar, or scan their computers every week in addition to the first measure, or even use a different password for every online account in addition to the second measure.
Game Simulation (with Python)

- 3 strategies of attacker:
  - Mainly attacking defender
  - Mainly attacking user
  - Attacks evenly (moderate strategy)

- 2 types of strategies for user and defender
  - Mainly high
  - Mainly low

- Total 3x2x2=12 simulations

- For a game of 20 rounds, n=1000
Attacker Strategy: Mainly attack defender
User Payoff for Attacking Defender Strategy

- Defender Low/User High
- Defender High/User High
- Defender Low/User Low
- Defender High/User Low

Density

N = 1000  Bandwidth = 0.155
Attacker Strategy: Mainly attack user
Defender Payoff for Attacking User Strategy

- Defender Low/User High
- Defender High/User High
- Defender Low/User Low
- Defender High/User Low

N = 1000  Bandwidth = 0.3374
User Payoff for Attacking User Strategy

- Defender Low/User High
- Defender High/User High
- Defender Low/User Low
- Defender High/User Low

Density

N = 1000  Bandwidth = 0.1572
Attacker Strategy: Moderate strategy
User Payoff for Moderate Attacker Strategy

- Defender Low/User High
- Defender High/User High
- Defender Low/User Low
- Defender High/User Low

Density

N = 1000  Bandwidth = 0.1611
Findings Summary

• Payoff distribution is relatively invariant to attacker strategy
• For the defender, user strategy matters more when the defender is on the mainly high strategy
• For the user, a high defender causes more variation in payoff
• Generally, a high strategy is undesirable for both defender and user
Plan

• Bots
• Three-player interacting game
• Manipulations: defender and user’s strategies
• In lab and online