Stackelberg vs. Nash in Security Games: An Extended Investigation of Interchangeability, Equivalence, and Uniqueness

Daniel Redelmeier

5 November 2015
Problem

- Attacker knows Defender strategy:
  - Strong Stackelberg Equilibrium

- Attacker does not know Defender strategy:
  - Nash Equilibrium

- Given some uncertainty, what model should we use? Does it matter?
Applications

- LAX ARMOR

- FAMS
  - Scheduling constraints: tours of flights, location/timing

- Other applications:
  - Transport Security Administration GUARDS
  - US Coast Guard
  - Network security
Paper Contributions

1. Nash equilibria are interchangeable in security games

2. If SSAS property holds, Defender SSE $\subset$ NE

3. If attackers can attack multiple targets, then SSE $\not\subset$ NE

4. Design explicit extensive-form game model to account for uncertainty
Nash Equilibria are Interchangeable

• Idea of proof: convert to a zero-sum game

• Assume defender utilities are negative of attacker utilities (zero-sum)
If SSAS property, defender SSE ⊆ NE

- SSAS: Subsets of Schedules Are Schedules
  - Schedule: some set of targets that can be defended by a single resource
  - E.g. 4 targets: \{1, 0, 1, 0\} is a possible schedule
  - If SSAS, \{1, 0, 0, 0\} is also a schedule

- Minimax: decision rule that maximizes worst-case reward of player who goes first

- Idea of proof: SSE ⊆ MM, MM = NE
  - Therefore SSE ⊆ NE
Unique SSE/NE strategy?

• Property: defender has homogenous resources that can cover only one target each

• Example: LAX

• Idea of proof:
  – Show there is unique MM strategy
  – Therefore there is a unique SSE/NE strategy
SSE ≠ NE with Multiple Attacker Resources

- Counterexample:

<table>
<thead>
<tr>
<th></th>
<th>t₁</th>
<th>t₂</th>
<th>t₃</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Def</strong></td>
<td>C</td>
<td>U</td>
<td>C</td>
</tr>
<tr>
<td><strong>Att</strong></td>
<td>0</td>
<td>-2</td>
<td>-9</td>
</tr>
<tr>
<td>5</td>
<td>6</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>

- Intuition: Attacker will attack t₁, Defender does not want second attacker to attack t₂
- t₁ is defended in NE profile, t₂ is defended in SSE profile with two attackers
- NE profile: {⟨1,0,0⟩, ⟨1,1,0⟩}
- Stackelberg profile: {⟨0.5, 0.5, 0⟩, ⟨1,0,1⟩}
Experiment Design

• Several variables:
  – Number of attacker resources
  – Number of defender resources
  – Size of schedules that defenders can cover
  – Number of schedules

• For every setting, 1000 games with 10 targets
• Random attacker and defender payoffs
Experiment Results

- 3 attacker resources:
Modelling Uncertainty

Figure 3: Extensive form of the larger game in which the defender is uncertain about the attacker’s ability to observe.
Discussion Questions

• In the extensive-form game model, $p$ would likely have a large margin of error under real circumstances. How much does this matter?

• The authors mention that their contributions in the field of security games may also have applications in computer network security. How might this be modeled? Are there applications outside of security games?

• When discussing the problem of the defenders not knowing the attacker's utility function, the authors use Bayesian games as a possible solution. However, they state that “Bayesian games are practical only for small security games, because they depend on writing out the complete action space for each player, which is of exponential size in security games.” Could an action-graph model help in this case?