Modeling Security Decisions as Games

Chris Kiekintveld

University of Texas at El Paso

.. and MANY Collaborators
Decision Making and Games

- Research agenda: improve and justify decisions
  - Automated intelligent agents
  - Decision support tools

- Challenges
  - Modeling decisions
  - Uncertainty
  - Scalable algorithms
  - Multiple agents
  - Learning

Game Theory
Examples of Games

- Chess
- Backgammon
- Poker
- Auctions
- Sponsored search
- Security
- Network protocols
- Video games
- Financial markets

...
Many Targets      Few Resources

How to assign limited resources to defend the targets?

*Security Games*
Applications: Deployed Security Assistants

Ports & port traffic
US Coast Guard

Airports, flights
TSA, FAMS, Airport Police

Metro trains
LA Sheriff’s/TSA

Environmental Crime
US Coast Guard/World bank
ARMOR: Deployed at LAX August 2007

- “Assistant for Randomized Monitoring Over Routes”
- LAWA: Los Angeles World Airports police
  - Problem 1: Schedule vehicle checkpoints
  - Problem 2: Schedule canine patrols

ARMOR-Checkpoints    ARMOR-K9
### Available Canines

<table>
<thead>
<tr>
<th>Available Teams</th>
<th>Morning (AM)</th>
<th>Evening (PM)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sunday</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Monday</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Tuesday</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Wednesday</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Thursday</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Friday</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Saturday</td>
<td>6</td>
<td>6</td>
</tr>
</tbody>
</table>

### Days to Schedule

- **July, 2009**
- Today: 7/30/2009

- Set All: Morning (AM) 6, Evening (PM) 6

Generate Schedule
Key Issues

- Intelligent, adaptive attackers
  - Surveillance, insider threats
  - *Unpredictable* schedules
- Diverse targets
  - *Varying* consequences, vulnerabilities
  - *Non-uniform*, weighted randomization
- Uncertainty about attackers
  - *Multiple groups with different capabilities*
  - *Uncertain* preferences and motivations
  - *Bayesian* reasoning
Fundamentals: Utilities (Payoffs)

- How can we characterize consequences?
  - Utilities measure magnitudes of preferences
  - Real numbers to measure value

- Decision makers have preferences over outcomes
  - May include indifference relationships
  - Should be complete, rational

“Rational” preferences can be represented as utility functions
Fundamentals: Probabilities

- How can we characterize risk?
  - Probabilities measure *likelihood* of events
  - Formal way to reason about uncertainty
  - Ratio of positive/total events

- Reasons for uncertainty
  - Ignorance/incomplete knowledge
  - Laziness/complexity
  - Strategic unpredictability

- Reasoning about evidence
  - Bayes Rule
Fundamentals: Decision Rules

- Maximize expected value
  - *Weight the value for each outcome by likelihood*
  - *Assumes risk neutrality*
- Maxmin value
  - *Maximize the worst-case value*
  - *“Paranoid” solution*
- Minimize regret
  - *Minimize “opportunity loss”*
  - *How much better could I have done?*
- What if there are multiple decision makers?
  - *Game theory/adversarial reasoning*
Security Game

2 players
2 targets
1 defender resource

Target 1 | Target 2
---|---
1, -1 | -2, 2
-1, 1 | 2, -1
Security Game

2 players
2 targets
1 defender resource

<table>
<thead>
<tr>
<th></th>
<th>Target 1</th>
<th>Target 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target 1</td>
<td>1, -1</td>
<td>-2, 2</td>
</tr>
<tr>
<td>Target 2</td>
<td>-1, 1</td>
<td>2, -1</td>
</tr>
</tbody>
</table>

Play this game against several different opponents
Play at least twice as the defender, and twice as the attacker
Game Solutions

Best Response

<table>
<thead>
<tr>
<th></th>
<th>Target 1</th>
<th>Target 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target 1</td>
<td>1, -1</td>
<td>-2, 2</td>
</tr>
<tr>
<td>Target 2</td>
<td>-1, 1</td>
<td>2, -1</td>
</tr>
</tbody>
</table>
## Game Solutions

### Best Response

<table>
<thead>
<tr>
<th></th>
<th>Target 1</th>
<th>Target 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target 1</td>
<td>1, -1</td>
<td>-2, 2</td>
</tr>
<tr>
<td>Target 2</td>
<td>-1, 1</td>
<td>2, -1</td>
</tr>
</tbody>
</table>
Game Solutions

Best Response

<table>
<thead>
<tr>
<th>Target 1</th>
<th>Target 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target 1</td>
<td>1, -1</td>
</tr>
<tr>
<td></td>
<td>-2, 2</td>
</tr>
<tr>
<td>Target 2</td>
<td>-1, 1</td>
</tr>
<tr>
<td></td>
<td>2, -1</td>
</tr>
</tbody>
</table>
### Game Solutions

**Mixed Strategy**

<table>
<thead>
<tr>
<th></th>
<th>Target 1</th>
<th>Target 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>50%</td>
<td>1, -1</td>
<td>-2, 2</td>
</tr>
<tr>
<td>Target 1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>50%</td>
<td>-1, 1</td>
<td>2, -1</td>
</tr>
<tr>
<td>Target 2</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Nash Equilibrium

A mixed strategy for each player such that no player benefits from a unilateral deviation.
Nash Equilibrium

A mixed strategy for each player such that no player benefits from a unilateral deviation.
Stackelberg Equilibrium

Attackers use surveillance in planning attacks

Defender commits to a mixed strategy

\[
\begin{array}{c}
\{0.1,0.9\} \\
\text{...} \\
(-0.9, 0.9) \quad (1.8, -0.9) \\
\{0.5,0.5\} \\
(0, 0) \quad (0, -0.5)
\end{array}
\]
### Standard (Compact) Security Game

**Targets**

<table>
<thead>
<tr>
<th></th>
<th><img src="image.png" alt="Airplane 1" /></th>
<th><img src="image.png" alt="Airplane 2" /></th>
<th><img src="image.png" alt="Airplane 3" /></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Reward</strong></td>
<td>5</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td><strong>Penalty</strong></td>
<td>-5</td>
<td>-1</td>
<td>-2</td>
</tr>
<tr>
<td><strong>Reward</strong></td>
<td>5</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td><strong>Penalty</strong></td>
<td>-3</td>
<td>-1</td>
<td>-6</td>
</tr>
</tbody>
</table>

**Identical Resources**

Payoffs for a target depend only on coverage of that target.
### Standard (Compact) Security Game

<table>
<thead>
<tr>
<th>Targets</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="Airplane" /></td>
<td><img src="image2.png" alt="Airplane" /></td>
<td><img src="image3.png" alt="Airplane" /></td>
<td></td>
</tr>
<tr>
<td><strong>Reward</strong></td>
<td>5</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td><strong>Penalty</strong></td>
<td>-5</td>
<td>-1</td>
<td>-2</td>
</tr>
<tr>
<td><img src="image4.png" alt="Thief" /></td>
<td><img src="image1.png" alt="Airplane" /></td>
<td><img src="image2.png" alt="Airplane" /></td>
<td></td>
</tr>
<tr>
<td><strong>Reward</strong></td>
<td>5</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td><strong>Penalty</strong></td>
<td>-3</td>
<td>-1</td>
<td>-6</td>
</tr>
</tbody>
</table>

**Defender strategy:** decide probability to cover each target, subject to resource limitation

If there is no coverage, which target is attacked?
ARMOR: Multiple Adversary Types

- *Uncertainty* about attacker payoffs (different adversaries)
- Bayesian game models

<table>
<thead>
<tr>
<th>P=0.3</th>
<th>P=0.5</th>
<th>P=0.2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Term #1</td>
<td>Term #2</td>
<td>Term #1</td>
</tr>
<tr>
<td>Term #1</td>
<td>5, -3</td>
<td>-5, 5</td>
</tr>
<tr>
<td>Term #2</td>
<td>-1, 1</td>
<td>2, -1</td>
</tr>
</tbody>
</table>

Uncertainty about attacker payoffs (different adversaries)

Bayesian game models

<table>
<thead>
<tr>
<th>Term #1</th>
<th>Term #2</th>
<th>Term #3</th>
<th>Term #4</th>
<th>Term #5</th>
</tr>
</thead>
<tbody>
<tr>
<td>111</td>
<td>121</td>
<td>112</td>
<td>211</td>
<td>...</td>
</tr>
<tr>
<td>3.3, -2.2</td>
<td>2.3,...</td>
<td>2.3,...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>-3.8, 2.6</td>
<td>...,...</td>
<td>...,...</td>
<td>...</td>
<td>222,...</td>
</tr>
</tbody>
</table>
ARMOR Results

ARMOR v/s Non-weighted (uniformed) Random for Canines

- ARMOR: 6 canines
- ARMOR: 5 canines
- ARMOR: 3 canines
- Non-weighted: 6 canines
Questions?