Modeling Observability in Adaptive Systems to Defend Against Advanced Persistent Threats

Cody Kinneer, Ryan Wagner, Fei Fang, Claire Le Goues, David Garlan
Security in Self-* Systems
Security in Self-* Systems
Advanced Persistant Threats (APTs)
Advanced Persistent Threats (APTs)
Tactics Techniques and Procedures (TTPs)
Tactics Techniques and Procedures (TTPs)
APT Observability
APT Observability

• Multiple attacker types
  • Goals
  • Tactics Techniques and Procedures (TTPs)
• Actions (both sides)
  • Defender faces wait or evict dilemma
  • Attacker notices defensive measures and adapts to remain hidden
Observable Eviction Game
Observable Eviction Game

- One (or none) of several APT attackers present
- Defender suspects an attack, unsure of attacker identity
- Takes place over a finite number of timesteps
- Each side has knowledge of available actions and payoff structure
Extensive Form Game
Extensive Form Game
Extensive Form Game

A1

N

Type1

A2

Type2
Extensive Form Game
Extensive Form Game

Diagram:

- Node $N$
- Type 1 branch leading to $A_1$
- Type 2 branch leading to $A_2$
Extensive Form Game

Diagram:
- Node $N$ with branches labeled $Type1$ and $Type2$.
- Player $A_1$ with branches $TTP1$ and $TTP2$.
- Player $A_2$ with branches $TTP1$ and $TTP2$.
-结局 $D$.
Extensive Form Game
Extensive Form Game
Extensive Form Game

Diagram:
- Type 1
- Node $A_1$
- Branches to $TTP1$ and $TTP2$
- Branches to $D$
Extensive Form Game
Extensive Form Game
Extensive Form Game
Extensive Form Game
Extensive Form Game

\[ TTP_1 \]

\[ \begin{array}{c}
W \\
N
\end{array} \]

\[ \begin{array}{c}
E_1 \\
E_2
\end{array} \]

\[ \begin{array}{c}
0.0, -1.0 \\
3.0, -3.5
\end{array} \]
Extensive Form Game

\[
\begin{array}{c}
E1 & E2 \\
0.0, -1.0 & 3.0, -3.5
\end{array}
\]
Extensive Form Game
Extensive Form Game

\[ TTP_1 \]

\[ W \]

\[ N \]

\[ E_1, E_2 \]

\[ 0.0, -1.0 \quad 3.0, -3.5 \]
Payoffs

• Attacker
  • Time in system
  • Suitability of TTP to goals

• Defender
  • Limit attacker utility
  • Minimize disruption to system
    • Different TTPs cause different disruption
    • Defensive measures cause varying disruption
Payoffs

\[ y_{ijk}^t = \begin{cases} 
  y_{ijk}^{t-1} \cdot (1 - q_j^{t-1}) \cdot (1 - y_j^{t-1}) & \text{if } 0 < t \leq T \\
  1 & \text{if } t = 0 \\
  0 & \text{if } t > T 
\end{cases} \]

\[ \epsilon_{ijk} = \sum_{t=1}^{T-1} \left( y_{ijk}^t \cdot \left( y_j^t \cdot (F + \tau) + (1 - y_j^t) \cdot q_j^t \cdot t \right) \right) \]

\[ + \ y_{ijk}^T \cdot \left( \chi_{jl} \cdot T + (1 - \chi_{jl}) \cdot (F + \tau) \right) \]
Extensive Form Game
Extensive Form Game
Extensive Form Game

Extensive Form Game graph with nodes and edges labeled with payoffs. The graph shows a decision tree with nodes for N, W, E1, E2, with outcomes 0.0, -1.0, 3.0, -3.5 and payoffs 1.0, -2.0.
Extensive Form Game

Diagram showing a game with nodes labeled \( N \), \( \neg Obs \), \( Obs \), and \( E1 \), \( E2 \). The payoffs are indicated at the endpoints of branches: (0.0, -1.0), (3.0, -3.5), (1.0, -2.0). The nodes \( E1 \) and \( E2 \) are connected to the payoff values (1.0, -2.0) and (3.0, -3.5).
Extensive Form Game
Solving the Game
Solving the Game
Solving the Game
Solving the Game
Solving the Game
Validation

• Does using the model result in improved utility compared to random?
• Can the OEG enable a robust defense for a range of threat landscapes?
• Is solving the OEG scalable to practically useful time horizons?
Limitations and Future Work

- High level of abstraction
- Generalizability to real world systems
- Refinement to provide automation for APT testbed
- Abstract strategy reuse and refinement
Conclusion

• Security presents unique challenges to Self-* systems
• Observable Eviction Game
• Modeling observability as a first class concern is a step towards secure self-* systems

Paper Available at:
ckinneer@cs.cmu.edu
Backup Slides
Comparison to Random
Using the model results in improvement

Nash Equilibrium

Stackelberg Equilibrium

Prior Probability of Attacker Type 1

Defender's Utility

Defender Plays
- equilibrium
- uniform random

Prior Probability of Attacker Type 1

Defender's Utility

Defender Plays
- equilibrium
- uniform random
Sensitivity Analysis
Scalability Analysis
Stackelberg Scalable on Number of Timesteps

![Graph showing Time in Seconds vs Number of Timesteps for Equilibrium, Nash, and Stackelberg strategies. The graph demonstrates a clear increase in Time in Seconds as the Number of Timesteps increases, with the Nash strategy maintaining a lower curve compared to the Stackelberg strategy.]
Evaluate Design Alternatives
Utility Change with Honeypots

Optimal Number of Decoys

Equilibrium
- nash
- stackelberg

Prior Probability of Attacker Type 1

Delta Defender's Utility

Equilibrium
- nash
- stackelberg

Prior Probability of Attacker Type 1
Strategy Change with Honeypots
Optimal Defense

- Bayesian Nash and Stackelberg equilibria

<table>
<thead>
<tr>
<th>w₀e₁</th>
<th>w₀e₂</th>
<th>e₁₀</th>
<th>e₂₀</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.68</td>
<td>0.00</td>
<td>0.00</td>
<td>0.32</td>
</tr>
</tbody>
</table>

The power of observability