When to Invest in Security? Empirical Evidence and a Game-Theoretic Approach for Time-Based Security

Sadegh Farhang
College of Information Sciences and Technology
The Pennsylvania State University
farhang@ist.psu.edu

Jens Grossklags
Chair for Cyber Trust
Technical University of Munich
jens.grossklags@in.tum.de
Outline

- Motivation
- Security Incident Data
- Game-Theoretic Model
- Payoff Calculation
- Results and Simulation
- Conclusion
Motivation

- Early morning, February 17, 2014
- Highjacked Flight ET-702
- Landed in Geneva at 6:02am local time

- No escort from Swiss Air Force
  - Does not operate
    - Before 8am weekdays
    - During lunch time
    - During weekends
Focus on Time Aspect

- Pilot stealthily took ownership of a plane at a particular **day** and **time**
- Direct the plane to his target destination
- Informed ground control about the highjacking
- Excessive reaction time due to the non-responsiveness of the Swiss Air Force

**Protection time**

**Detection time**

**Reaction time**
Capturing complexity of security situations with time-based security

- **Protection time (p):** Amount of time the attacker needs to execute her attack successfully

- **Detection (discovery) time (d):** Required time for the defender to detect that his system has been stealthily compromised

- **Reaction time (r):** Required time for the defender to reset his defense mechanisms in order to recreate a safe system state
Outline

- Motivation
- Security Incident Data
- Game-Theoretic Model
- Payoff Calculation
- Results and Simulation
- Conclusion
Security Incident Data

- Shed light on the question of the actual timing of security incidents and responses by looking into empirical data sources

- Available field data sources
  - Not necessarily matching our definitions precisely
  - But provide some indication of the magnitude of these parameters

- Relevant industry report data
  - Verizon's annual Data Breach Investigations Report (DBIR)
VCDB

- VERIS Community Database (VCDB)
  - VERIS: Vocabulary for Event Recording and Incident Sharing
  - How to report on VCDB
  - 5,856 publicly disclosed data breaches

- Focus
  - Action
  - Timeline

- Timeline
  - Incident date
  - Time to compromise
  - Time to exfiltration
  - Time to discovery
  - Time to containment

- Action
  - Malware: 439
  - Hacking: 1655
  - Total: 1795

473 entries
Discovery Time

- 325 entries with non-empty discovery time
  - 150 with exact values for discovery time
- Average: 198.2539 days
  - Max: 6 years
  - Min: 10 hours
Protection Time

- Exfiltration time as protection time

<table>
<thead>
<tr>
<th>Incident Time</th>
<th>Discovery Time</th>
<th>Exfiltration Time</th>
<th>Containment Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>4/16/2011</td>
<td>Days</td>
<td>2 Days</td>
<td>Days</td>
</tr>
<tr>
<td>7/18/2011</td>
<td>10 Days</td>
<td>7 Days</td>
<td>-</td>
</tr>
<tr>
<td>7/24/2013</td>
<td>15 Days</td>
<td>2 Days</td>
<td>-</td>
</tr>
<tr>
<td>11/15/2013</td>
<td>1 Months</td>
<td>2 Weeks</td>
<td>-</td>
</tr>
<tr>
<td>4/15/2015</td>
<td>1 Year</td>
<td>2 Months</td>
<td>15 Days</td>
</tr>
</tbody>
</table>

- Protection time < discovery time
Reaction time

- Containment time as reaction time
- Average: 10.4504 days
Implications

- Other Datasets
  - Web Hacking Incidents Database (WHID)
  - Privacy Rights Clearinghouse

- Actual details with respect to timing information are insufficient to draw robust conclusions

- Significant omission of cybersecurity-related data collection

- Further work in this direction
Outline

- Motivation
- Security Incident Data
- Game-Theoretic Model
- Payoff Calculation
- Results and Simulation
- Conclusion
Game-Theoretic Model

- Game-theoretic model for time-based security (TBS)

- Two-player game
  - Defender
  - Attacker

- $C_A$ - Attacker’s cost to compromise the defender’s system

- $C_D$ - Defender’s cost to reset the state of the system from compromised to safe

- $C_k$ - Defender’s cost to discover whether its system has been compromised
Assumption

- $p, d, r$: Constant
- $t_A$: Periodicity of the attacker’s attempt to compromise the system
- $t_D$: Periodicity of the defender checking for system compromise
- $t_A \geq p + d + r$ and $t_D \geq p + d + r$
Outline

- Motivation
- Security Incident Data
- Game-Theoretic Model
- Payoff Calculation
- Results and Simulation
- Conclusion
Payoff Calculation

\[ u_D(t_D, t_A) = \tau_{D_i} - \frac{C_D}{\delta_{D_i}} - \frac{C_k}{t_D} \]

\[ u_A(t_D, t_A) = (1 - \tau_{D_i}) - \frac{C_A}{t_A} \]

- Six cases

1. \( t_D \leq t_A - p - d - r \)
2. \( t_A \leq t_D \leq t_A + p \)
3. \( t_A + p \leq t_D \leq t_A + p + d + r \)
4. \( t_A - p - d - r \leq t_D \leq t_A - d - r \)
5. \( t_A - d - r \leq t_D \leq t_A \)
6. \( t_D \geq t_A + p + d + r \)
Example Case

- \( t_D \leq t_A - p - d - r \)
- \( x = \frac{p}{t_D} \quad \delta_{D11} = t_A \quad T_{A11} = t_D + d + r - \frac{p}{2} \)
- \( 1 - x \quad \delta_{D12} = t_A \quad T_{A12} = \frac{t_D-p}{2} + d + r \)

\[ \delta_{D1} = x \delta_{D11} + (1 - x) \delta_{D12} = t_A \]

\[ \tau_{D1} = x \tau_{D11} + (1 - x) \tau_{D12} = \frac{t_A - \frac{t_D}{2} - d - r}{t_A} \]
Payoff

- \( t_A - p - d - r \leq t_D \leq t_A \)

\[
\delta_D = 2t_A - \left( \frac{t_A - p - d - r}{t_D} \right) t_A
\]

\[
\tau_D = \frac{1}{4t_A t_D} ( -t_A^2 - t_D^2 + 4t_A t_D + 2pt_A - 2t_D (d + r) + (p + d + r)(d + r - p) )
\]

- Boundary point \( t_A = t_D \)

\[
\delta_D = t_D + p + d + r
\]
Payoff

- \( t_A \leq t_D \leq t_A + p + d + r \)

\[ \delta_D = 2t_D - \left( \frac{t_D - p - d - r}{t_A} \right) t_D \]

\[ \tau_D = \frac{1}{4t_At_D} \left( t_A^2 + t_D^2 + 2pt_A - 2t_D (d + r) + (p + d + r) (d + r - p) \right) \]

- \( t_D \geq t_A + p + d + r \)

\[ \delta_D = t_D \]

\[ \tau_D = \frac{t_A + 2p}{2t_D} \]
Outline

- Motivation
- Security Incident Data
- Game-Theoretic Model
- Payoff Calculation
- Results and Simulation
- Conclusion
Defender’s Best Response

- For each value of $t_A$, the defender’s best response is:

$$BR_D(t_A) = \arg \max_{t_D \in S} u_D(t_D, t_A)$$

$$S(t_A) = \{ \bar{t}_{D1}, \bar{t}_{D2}, \bar{t}_{D3} \} = \{ p + d + r, t_A - p - d - r, t_A, t_A + p + d + r \}$$

$$\bar{t}_{D1} = \sqrt{2t_A c_k}$$

$$\frac{c_k}{t_D^2} + \frac{c_D(t_A - p - d - r)}{t_A(2t_D - t_A + p + d + r)^2} + \frac{1}{4t_A t_D^2} (-t_D^2 + t_A^2 - 2pt_A - (p + d + r)(d + r - p)) = 0$$

$$\frac{c_k}{t_D^2} + \frac{c_D t_A}{t_D^2(2t_A - t_D + p + d + r)} - \frac{c_D t_A}{t_D(2t_A - t_D + p + d + r)^2}$$

$$+ \frac{1}{4t_A t_D^2} (t_D^2 - t_A^2 - 2pt_A - (p + d + r)(d + r - p)) = 0$$
Nash Equilibrium

- Calculate attacker’s best response

\[ BR_A(t_D) = \arg \max_{t_A \in V} u_A(t_D, t_A) \]

- Nash equilibrium
  - Numerically
  - Mutual best response
Simulation: p

Defender's Best Response

Attacker's Best Response
Simulation: NE

Nash Equilibrium

- Defender's best response
- Attacker's best response
Outline

- Motivation
- Security Incident Data
- Game-Theoretic Model
- Payoff Calculation
- Results and Simulation
- Conclusion
Conclusion

- Empirical evaluation of timing of security incidents
  - Protection time
  - Reaction time
  - Discovery time

- Time-based security framework
  - Game-theoretic model
  - Analysis

- Future work:
  - Extend model
    - \( p, d, r \): Random variable
  - Field data
Thank you.

Questions?