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

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

Protection time

- Informed ground control about the highjacking

Detection time

- Excessive reaction time due to the non-responsiveness of the Swiss Air Force

Reaction time

From Physical to Time-Based Cybersecurity

- 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

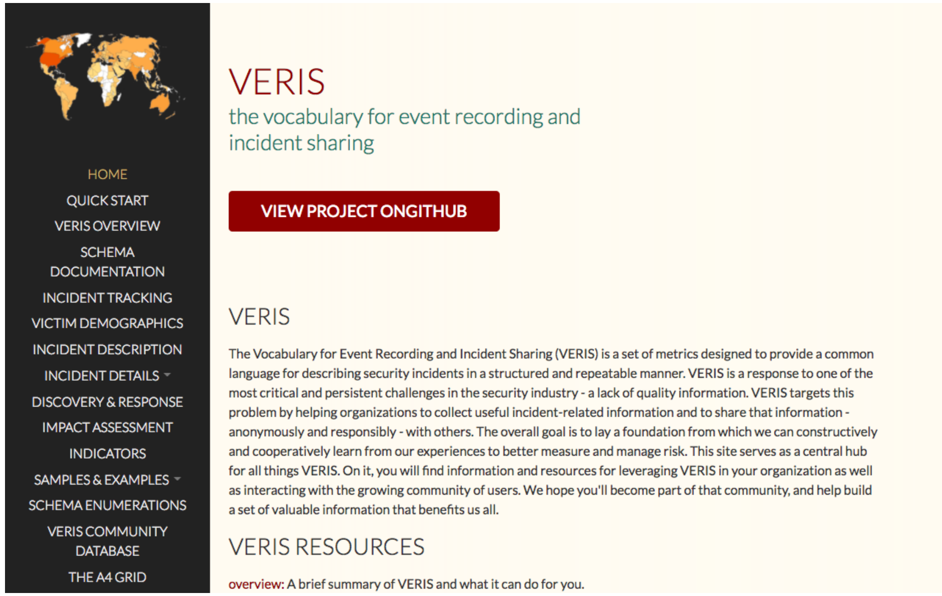
- VERIS Community Database (VCDB)
  - VERIS: Vocabulary for Event Recording and Incident Sharing
    - How to report on VCDB
  - 5,856 publicly disclosed data breaches

- Focus
  - Action
  - Timeline

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

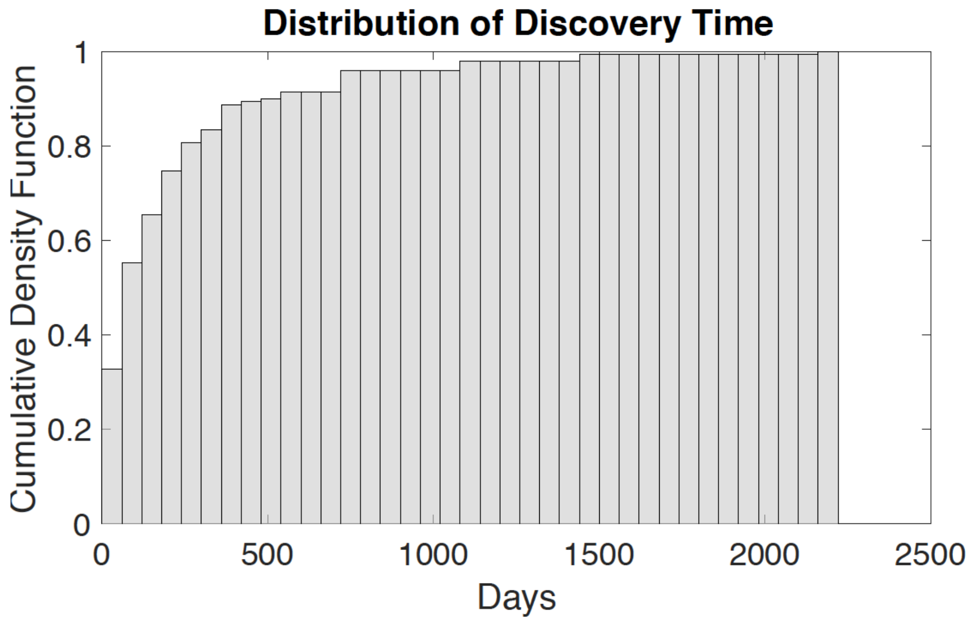
- Timeline
  - Incident date
  - Time to compromise
  - Time to exfiltration
  - Time to discovery
  - Time to containment

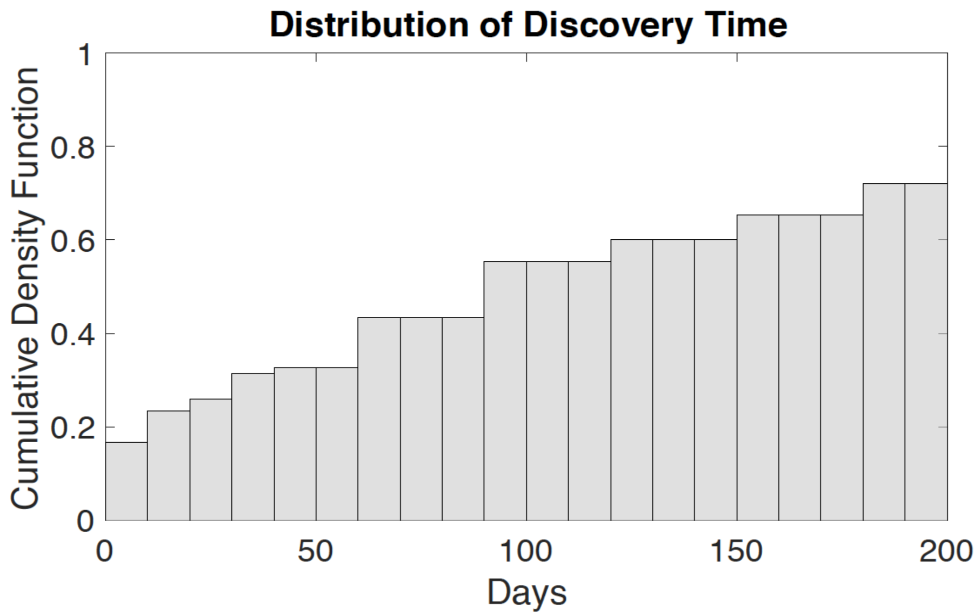
473 entries



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

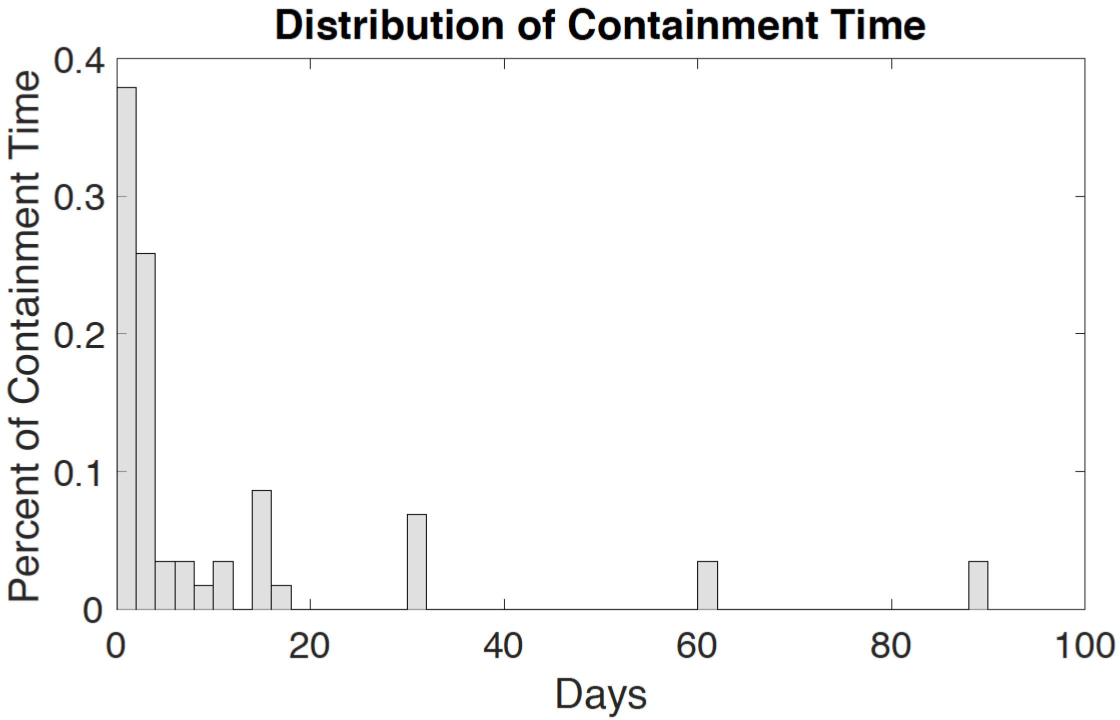
- Exfiltration time as protection time

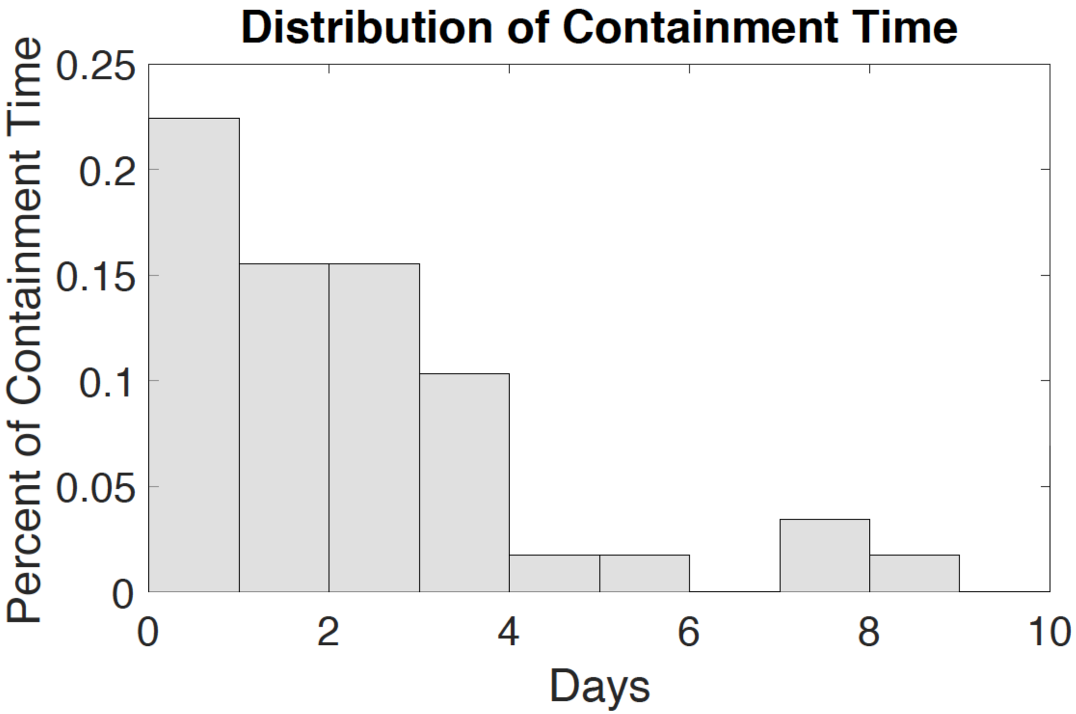
Incident Time	Discovery Time	Exfiltration Time	Containment Time
4/16/2011	Days	2 Days	Days
7/18/2011	10 Days	7 Days	-
7/24/2013	15 Days	2 Days	-
11/15/2013	1 Months	2 Weeks	-
4/15/2015	1 Year	2 Months	15 Days

- 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

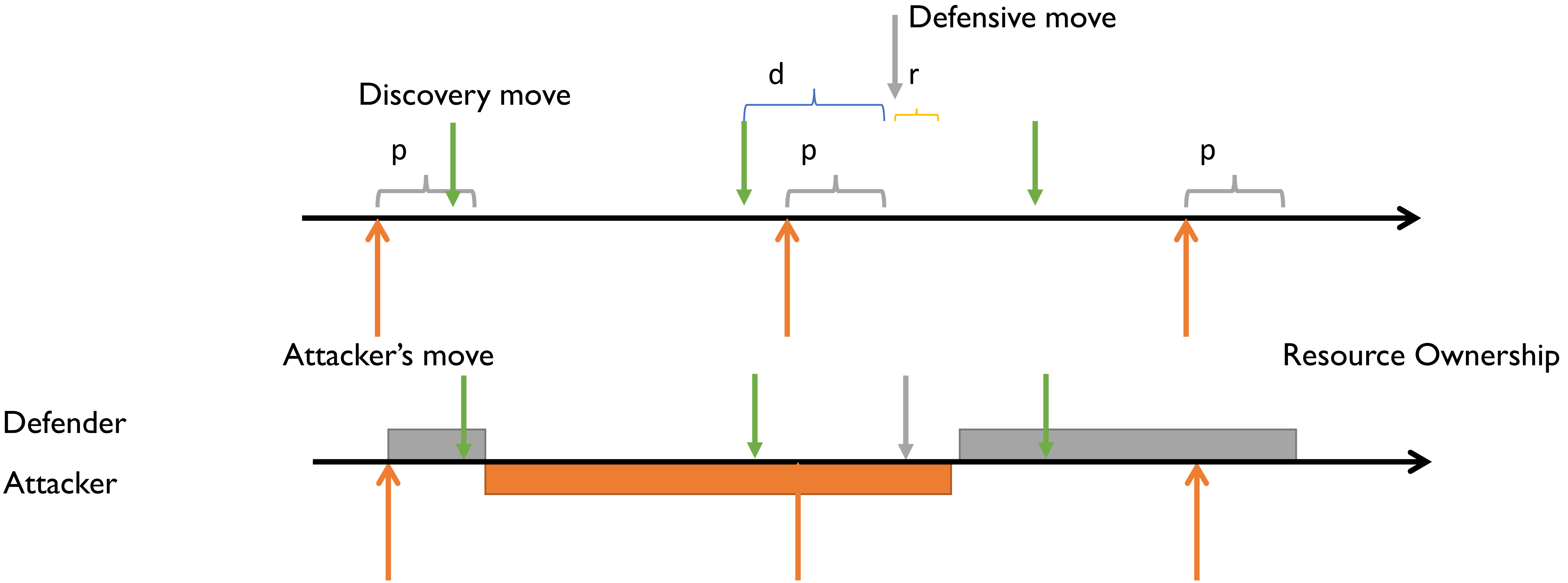
- Motivation
- Security Incident Data
- Game-Theoretic Model
- Payoff Calculation
- Results and Simulation
- Conclusion

Game-Theoretic Model

- Game-theoretic model for time-based security (TBS)
- Two-player game
  - Defender
  - Attacker
- $c_{\mathbf{A}}$ - Attacker's cost to compromise the defender's system
- $c_{\mathbf{D}}$ - Defender's cost to reset the state of the system from compromised to safe
- $c_{\mathbf{k}}$ - Defender's cost to discover whether its system has been compromised

Assumption

- **p, d, r:** Constant
- $t_{\mathbf{A}}$ - Periodicity of the attacker's attempt to compromise the system
- $t_{\mathbf{D}}$ - Periodicity of the defender checking for system compromise
- $t_{\mathbf{A}} \geq \mathbf{p} + \mathbf{d} + \mathbf{r}$ and $t_{\mathbf{D}} \geq \mathbf{p} + \mathbf{d} + \mathbf{r}$



Outline

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

Payoff Calculation

$$u_{\mathbf{D}}\left(t_{\mathbf{D}}, t_{\mathbf{A}}\right) = \boxed{\tau_{\mathbf{D}i}} - \frac{c_{\mathbf{D}}}{\boxed{\delta_{\mathbf{D}i}}} - \frac{c_{\mathbf{k}}}{t_{\mathbf{D}}}$$

$$u_{\mathbf{A}}\left(t_{\mathbf{D}}, t_{\mathbf{A}}\right) = \left(1 - \tau_{\mathbf{D}i}\right) - \frac{c_{\mathbf{A}}}{t_{\mathbf{A}}}$$

- Six cases

$$t_{\mathbf{D}} \le t_{\mathbf{A}} - \mathbf{p} - \mathbf{d} - \mathbf{r}$$

$$t_{\mathbf{A}} - \mathbf{p} - \mathbf{d} - \mathbf{r} \le t_{\mathbf{D}} \le t_{\mathbf{A}} - \mathbf{d} - \mathbf{r}$$

$$t_{\mathbf{A}} - \mathbf{d} - \mathbf{r} \le t_{\mathbf{D}} \le t_{\mathbf{A}}$$

$$t_{\mathbf{A}} \le t_{\mathbf{D}} \le t_{\mathbf{A}} + \mathbf{p}$$

$$t_{\mathbf{A}} + \mathbf{p} \le t_{\mathbf{D}} \le t_{\mathbf{A}} + \mathbf{p} + \mathbf{d} + \mathbf{r}$$

$$t_{\mathbf{D}} \ge t_{\mathbf{A}} + \mathbf{p} + \mathbf{d} + \mathbf{r}$$

Example Case

- $t_{\mathbf{D}} \leq t_{\mathbf{A}} - \mathbf{p} - \mathbf{d} - \mathbf{r}$
- $x = \frac{\mathbf{p}}{t_{\mathbf{D}}}$ $\quad \delta_{\mathbf{D}11} = t_{\mathbf{A}}$ $\quad T_{\mathbf{A}11} = t_{\mathbf{D}} + \mathbf{d} + \mathbf{r} - \frac{\mathbf{p}}{2}$
- $1 - x$ $\quad \delta_{\mathbf{D}12} = t_{\mathbf{A}}$ $\quad T_{\mathbf{A}12} = \frac{t_{\mathbf{D}} - \mathbf{p}}{2} + \mathbf{d} + \mathbf{r}$

$$\delta_{\mathbf{D}1} = x\delta_{\mathbf{D}11} + (1 - x)\,\delta_{\mathbf{D}12} = t_{\mathbf{A}}$$

$$\tau_{\mathbf{D}1} = x\tau_{\mathbf{D}11} + (1 - x)\,\tau_{\mathbf{D}12} = \frac{t_{\mathbf{A}} - \frac{t_{\mathbf{D}}}{2} - \mathbf{d} - \mathbf{r}}{t_{\mathbf{A}}}$$

Payoff

- $t_{\mathbf{A}} - \mathbf{p} - \mathbf{d} - \mathbf{r} \leq t_{\mathbf{D}} \leq t_{\mathbf{A}}$

$$\delta_{\mathbf{D}} = 2t_{\mathbf{A}} - \left(\frac{t_{\mathbf{A}} - \mathbf{p} - \mathbf{d} - \mathbf{r}}{t_{\mathbf{D}}}\right) t_{\mathbf{A}}$$

$$\tau_{\mathbf{D}} = \frac{1}{4t_{\mathbf{A}}t_{\mathbf{D}}}\left(-t_{\mathbf{A}}^2 - t_{\mathbf{D}}^2 + 4t_{\mathbf{A}}t_{\mathbf{D}} + 2\mathbf{p}t_{\mathbf{A}} - 2t_{\mathbf{D}}(\mathbf{d} + \mathbf{r}) + (\mathbf{p} + \mathbf{d} + \mathbf{r})(\mathbf{d} + \mathbf{r} - \mathbf{p})\right)$$

- Boundary point $t_{\mathbf{A}} = t_{\mathbf{D}}$

$$\delta_{\mathbf{D}} = t_{\mathbf{D}} + \mathbf{p} + \mathbf{d} + \mathbf{r}$$

Payoff

- $t_{\mathbf{A}} \leq t_{\mathbf{D}} \leq t_{\mathbf{A}} + \mathbf{p} + \mathbf{d} + \mathbf{r}$

$$\delta_{\mathbf{D}} \;=\; 2t_{\mathbf{D}} - \left(\frac{t_{\mathbf{D}} - \mathbf{p} - \mathbf{d} - \mathbf{r}}{t_{\mathbf{A}}}\right) t_{\mathbf{D}}$$

$$\tau_{\mathbf{D}} \;=\; \frac{1}{4t_{\mathbf{A}}t_{\mathbf{D}}}\left(t_{\mathbf{A}}^2 + t_{\mathbf{D}}^2 + 2\mathbf{p}t_{\mathbf{A}} - 2t_{\mathbf{D}}\left(\mathbf{d}+\mathbf{r}\right) + \left(\mathbf{p}+\mathbf{d}+\mathbf{r}\right)\left(\mathbf{d}+\mathbf{r}-\mathbf{p}\right)\right)$$

- $t_{\mathbf{D}} \geq t_{\mathbf{A}} + \mathbf{p} + \mathbf{d} + \mathbf{r}$

$$\delta_{\mathbf{D}} \;= t_{\mathbf{D}}$$

$$\boxed{\tau_{\mathbf{D}} \;=\; \frac{t_{\mathbf{A}} + 2\mathbf{p}}{2t_{\mathbf{D}}}}$$

Outline

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

Defender's Best Response

- For each value of $t_{\mathbf{A}}$, the defender's best response is:

$$BR_{\mathbf{D}}(t_{\mathbf{A}}) = \arg\max_{t_{\mathbf{D}} \in \mathcal{S}} u_{\mathbf{D}}\left(t_{\mathbf{D}}, t_{\mathbf{A}}\right)$$

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

$$\bar{t}_{\mathbf{D1}} = \sqrt{2t_{\mathbf{A}}c_{\mathbf{k}}}$$

$$\frac{c_{\mathbf{k}}}{t_{\mathbf{D}}^2} + \frac{c_{\mathbf{D}}\left(t_{\mathbf{A}}-\mathbf{p}-\mathbf{d}-\mathbf{r}\right)}{t_{\mathbf{A}}\left(2t_{\mathbf{D}}-t_{\mathbf{A}}+\mathbf{p}+\mathbf{d}+\mathbf{r}\right)^2} + \frac{1}{4t_{\mathbf{A}}t_{\mathbf{D}}^2}\left(-t_{\mathbf{D}}^2+t_{\mathbf{A}}^2-2\mathbf{p}t_{\mathbf{A}}-\left(\mathbf{p}+\mathbf{d}+\mathbf{r}\right)\left(\mathbf{d}+\mathbf{r}-\mathbf{p}\right)\right) = 0$$

$$\frac{c_{\mathbf{k}}}{t_{\mathbf{D}}^2} + \frac{c_{\mathbf{D}}t_{\mathbf{A}}}{t_{\mathbf{D}}^2\left(2t_{\mathbf{A}}-t_{\mathbf{D}}+\mathbf{p}+\mathbf{d}+\mathbf{r}\right)} - \frac{c_{\mathbf{D}}t_{\mathbf{A}}}{t_{\mathbf{D}}\left(2t_{\mathbf{A}}-t_{\mathbf{D}}+\mathbf{p}+\mathbf{d}+\mathbf{r}\right)^2} + \frac{1}{4t_{\mathbf{A}}t_{\mathbf{D}}^2}\left(t_{\mathbf{D}}^2-t_{\mathbf{A}}^2-2\mathbf{p}t_{\mathbf{A}}-\left(\mathbf{p}+\mathbf{d}+\mathbf{r}\right)\left(\mathbf{d}+\mathbf{r}-\mathbf{p}\right)\right) = 0$$

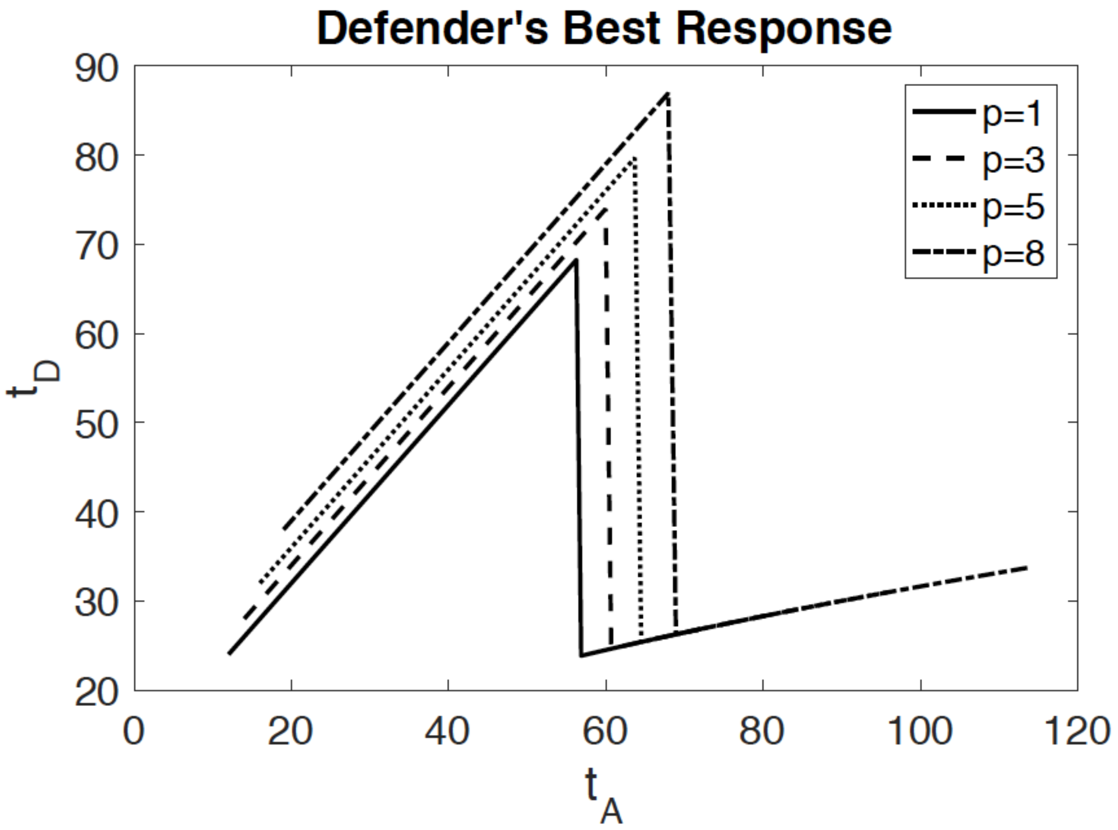
Nash Equilibrium

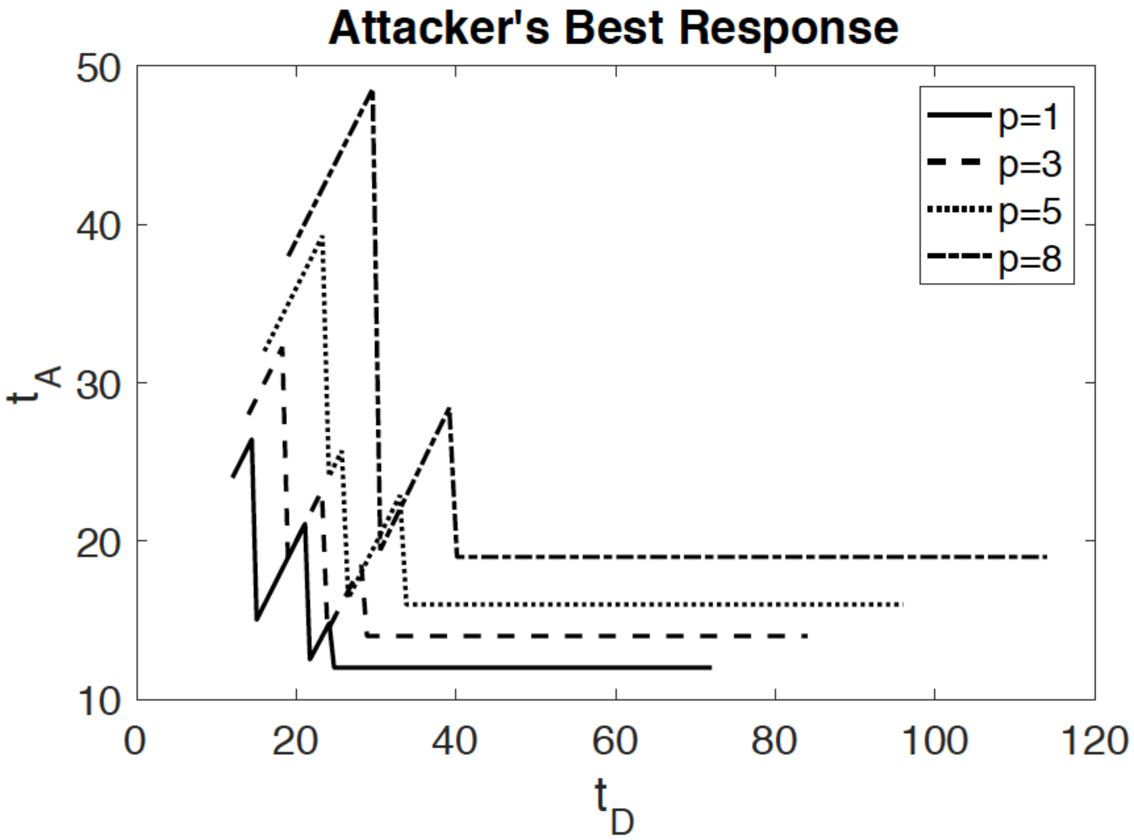
- Calculate attacker's best response

$$BR_{\mathbf{A}}(t_{\mathbf{D}}) = \arg\max_{t_{\mathbf{A}} \in \mathcal{V}} u_{\mathbf{A}}\left(t_{\mathbf{D}}, t_{\mathbf{A}}\right)$$

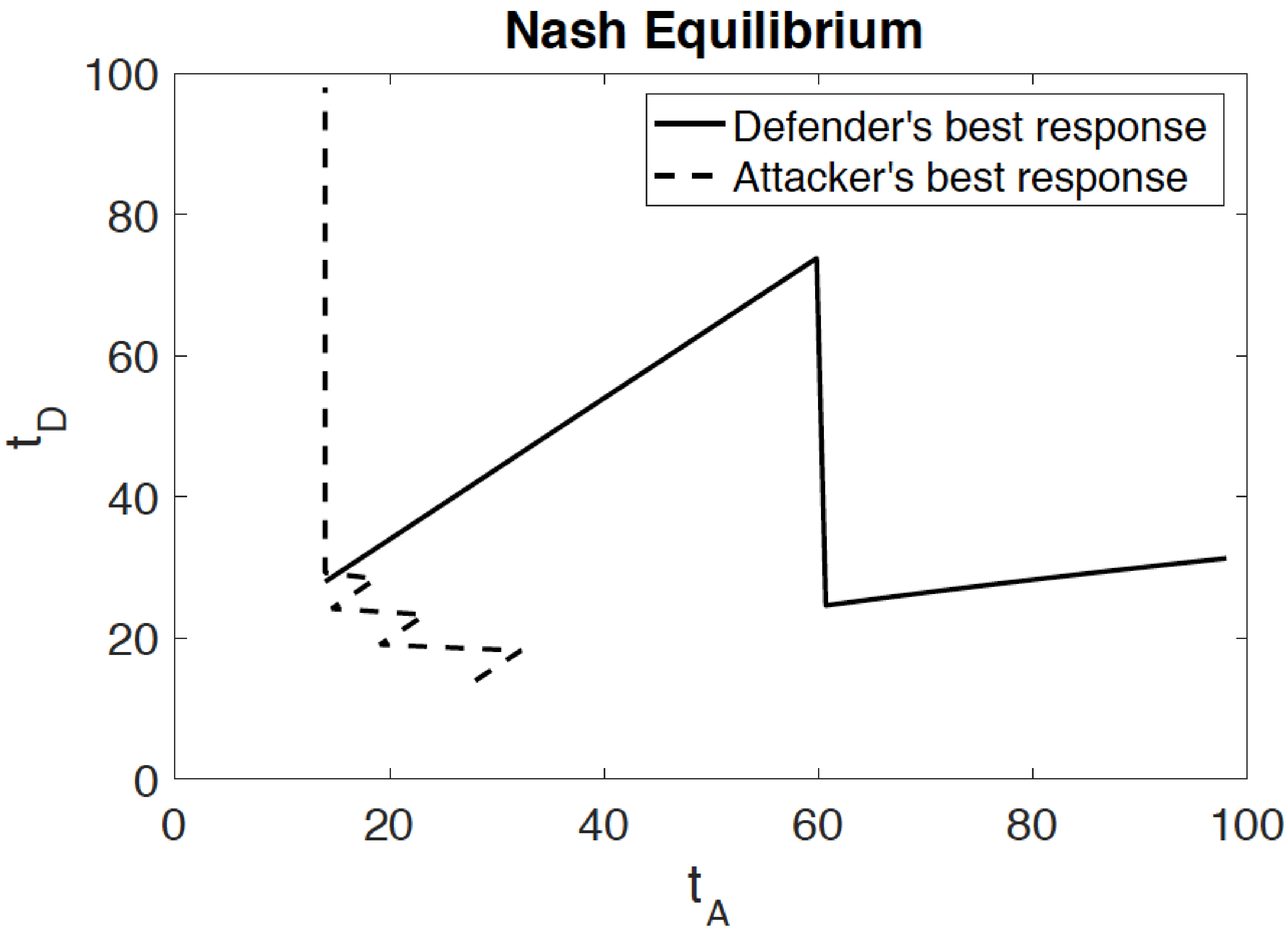
- Nash equilibrium
  - Numerically
  - Mutual best response

Simulation: p





Simulation: NE



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?