Cyber-Insurance as a Signaling Game: Self-Reporting and External Security Audits

Aron Laszka (Univ. of Houston), Emmanouil Panaousis (Univ. of Surrey), Jens Grossklags (Tech. Univ. of Munich)

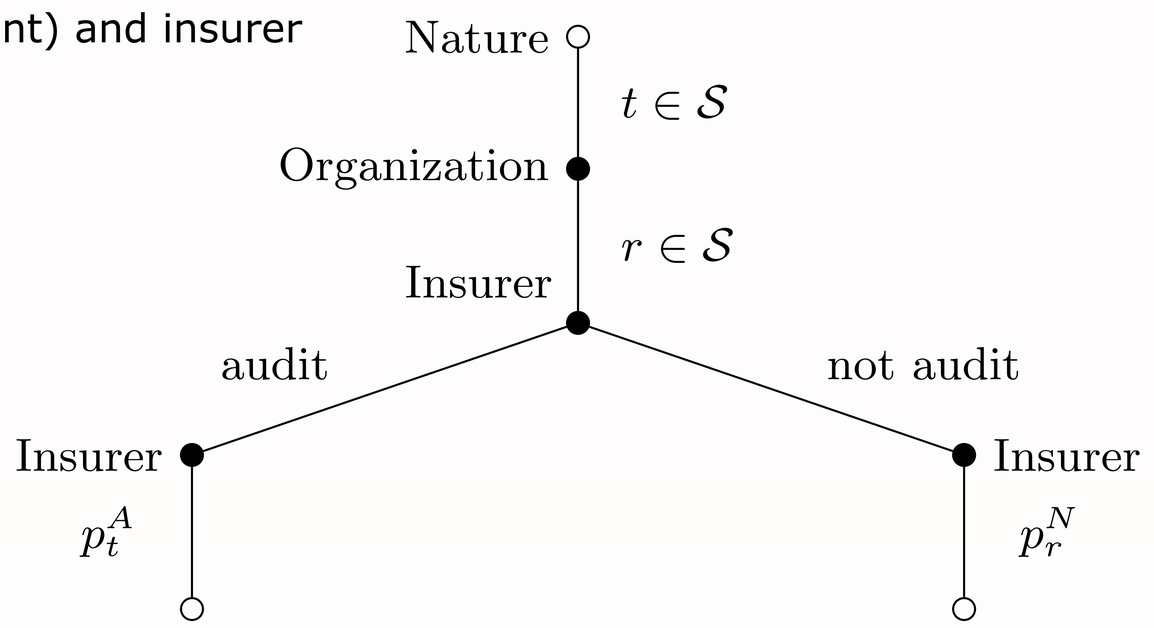
Motivation and Overview

- Cyber-insurance market is growing rapidly and is expected to reach **$14 billion** by 2022
- However, the market faces many challenges, such as **information asymmetry** between insurers and clients
- Information asymmetry causes adverse selection, which **increases insurance premiums** and **decreases adoption**
- Insurer may use **security audits** to overcome information asymmetry, but these audits can be very expensive
- We introduce a **game-theoretic model** to study the potential clients' self-reporting and the insurer's auditing decisions
- We present **numerical results** showing how less expensive and more effective audits alleviate information asymmetry

Stages and Strategies

- Two-player signaling game between organization (potential client) and insurer

1. Organization's **security level** $t \in S$
   - chosen at random by Nature to model uncertainty
   - known by the organization, but not by the insurer
   - insurer knows only the probability distribution
2. Organization **reports security level** $r \in S$ to the insurer
3. Insurer decides whether to **perform a security audit**
   - audit reveals the true security level t, but costs C
4. Insurer chooses **premium** p to ask from the client
5. Client decides whether to **purchase insurance**

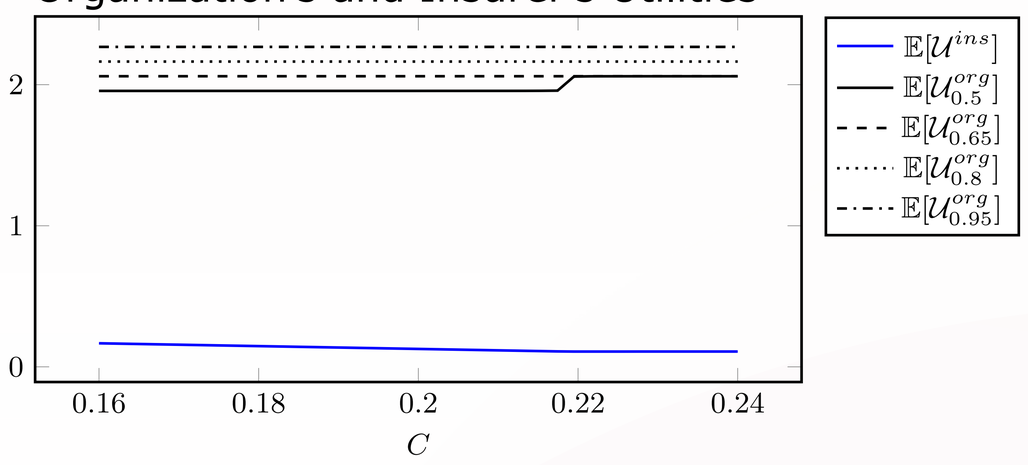


Utilities and Solution Concept

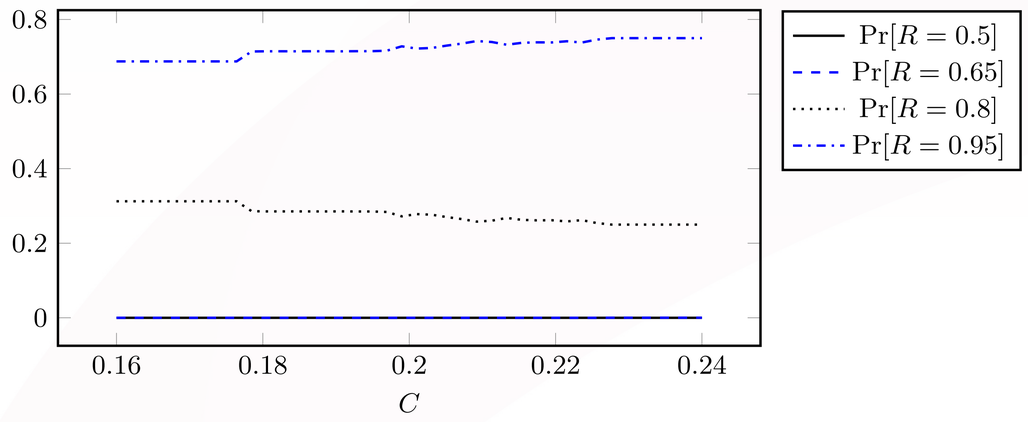
- Organization's utility
  - with insurance coverage: $\mathcal{U}_t^{org,acc}(p) = U(W - p)$
  - without insurance coverage: $\mathcal{U}_t^{org,rej} = (1-t) \cdot U(W - L) + t \cdot U(W)$
- Insurer's utility
  - with audit: $\mathcal{U}^{ins,aud}(t,p) = (p - (1-t) \cdot L) \cdot 1_{\{\text{insurance accepted}\}} - C$
  - without audit: $\mathcal{U}^{ins,noaud}(t,p) = (p - (1-t) \cdot L) \cdot 1_{\{\text{insurance accepted}\}}$
- Solution concept: perfect Bayesian Nash equilibrium: mixed profile $(\boldsymbol{\rho}^*, (\boldsymbol{a}^*, \boldsymbol{p}^{N*}, \boldsymbol{p}^{A*}))$ is equilibrium if
  - for each security level t, the client plays a best response: $\boldsymbol{\rho}^{t*} \in \operatorname{argmax}_{\boldsymbol{\rho}^t} \mathbb{E}\left[\mathcal{U}_t^{org}\right](\boldsymbol{\rho}^t, \boldsymbol{a}, \boldsymbol{p}^N, \boldsymbol{p}^A)$
  - insurer plays a best response: $(\boldsymbol{a}^*, \boldsymbol{p}^{N*}, \boldsymbol{p}^{A*}) \in \operatorname{argmax}_{(\boldsymbol{a}, \boldsymbol{p}^N, \boldsymbol{p}^A)} \sum_{t \in \mathcal{S}} \Pr[T = t \mid R = r] \Big[a_r \cdot \mathcal{U}^{ins,aud}(t, p_t^A) + (1 - a_r) \cdot \mathcal{U}^{ins,noaud}(t, p_r^N) \Big]$

Numerical Results

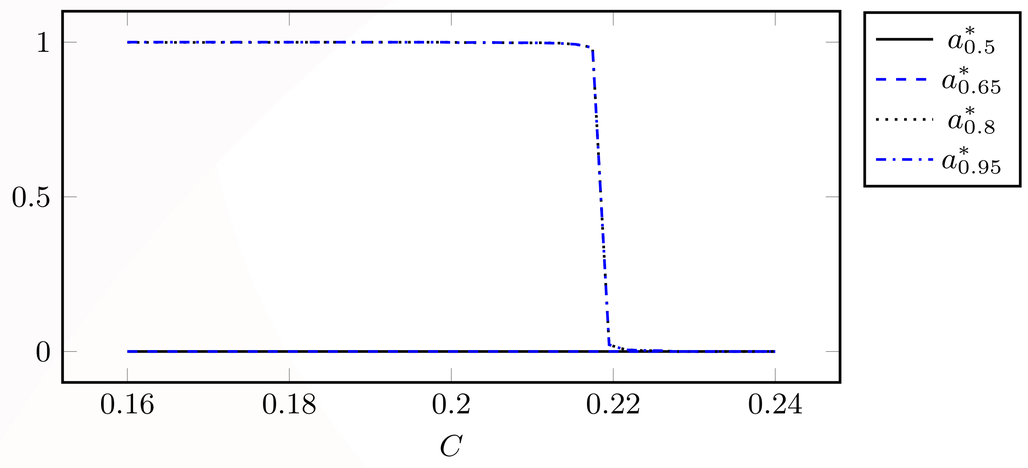
Organization's and Insurer's Utilities



Probability of Reporting Security Level $r = R$



Audit Probability for Reported Level $r = R$



Conclusion

- We introduced a novel model to study self-reported security levels, audit decisions, and adverse selection
- In future work, we plan to characterize the equilibria, consider forensic investigations after an incident and security investments