

Economics of Security

Jens Grossklags

College of Information Sciences and Technology
Pennsylvania State University

NSF Trustworthy Computing Workshop
Arlington, VA, October 27-29, 2010



Incentives and defense behavior

- Security landscape
 - Threats are real, wide-spread, and intractable
 - Business owners and users are concerned
 - Technologies are available
 - But:
 - 82% do not create backups regularly
 - 42% lost data in 2008
 - 58% have no firewall installed
 - Investing too little? Or even too much?
 - Economic incentives → Growing research community

Building an economic framework to tackle these questions



Short answer

Benefit of Security $>$ Cost of Security



Goal: Build a security framework

Cases that have enough structure to enable more intuitive statements about characteristics of equilibria.

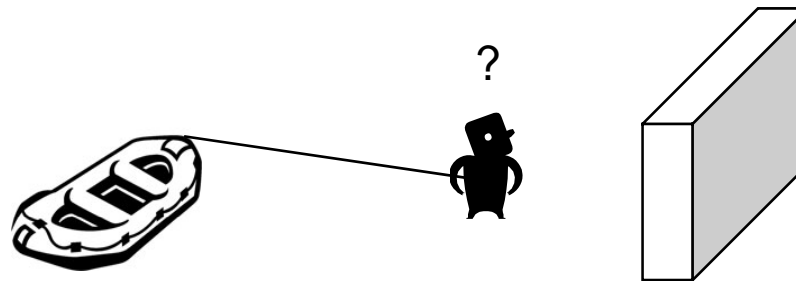
(Cornes and Sandler, 1996)

- Variety of security threats and responses
 - Capture important security interactions met in practice
 - Finite number of important economic factors



Decouple security strategies

- Decouple security strategies
 - **Self-protection** (e.g., patching system vulnerabilities)
 - Protection level determined by all participants of a network.
 - *Interdependency (e.g., Public good [Varian, 2004])*
 - **Self-insurance** (e.g., backup technologies)
 - Individual level of loss reduction
 - *Private good [Ehrlich and Becker, 1972]*
 - **Passivity**



[WWW 2008]



An example – Bear races

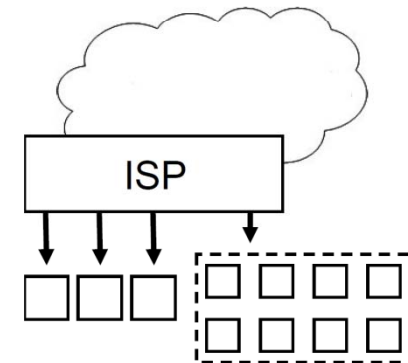
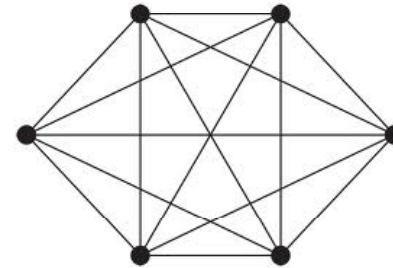


[ACM EC 2008, ACM SIGCOMM PINS 2004]



Context

- Connectedness
 - Correlation
 - Propagation
- Structure and Dependency
 - User-Admin relationships
 - User-ISP relationships
 - Cloud Computing



[TRUST 2010]



What is the correct solution approach?



Information and Bounded rationality

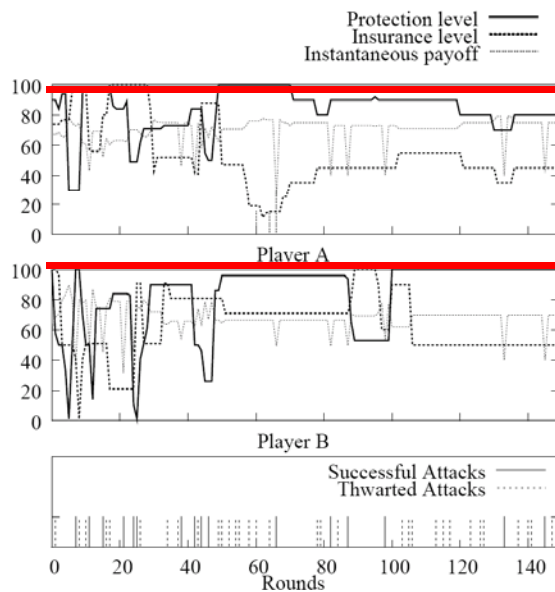
- What do we know?
 - Parameters
 - Types of players
 - Structure of network
- Who are we?
 - Near-sighted, myopic, time-inconsistent
 - Near rational, satisficing
 - Simplification: Naïve vs. sophisticated

[GameNets 2009, GameSec 2010, ACM SIGCOMM PINS 2004, FC 2010]

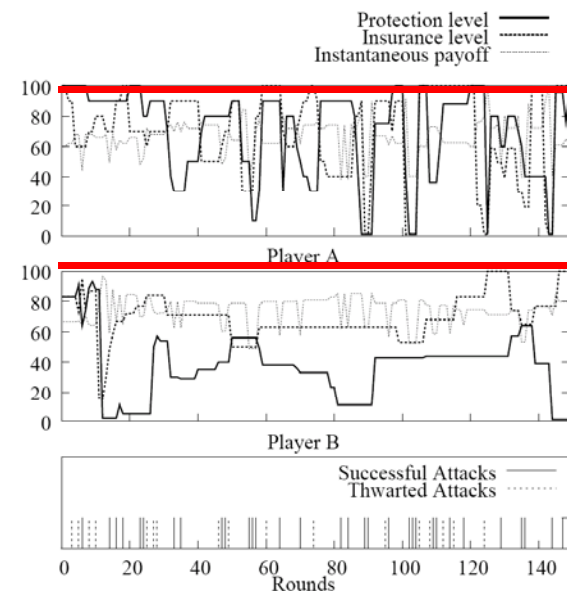


Understanding decision-makers

- Behavioral study
 - Laboratory experimentation with human subjects



**Pareto-optimal
payoff**
Vs.
Actual payoff



[USENIX UPSEC 2008]



Empirical data and economic research

- Measurement
 - Specific threats (e.g., spam) [GTNoise Lab]
 - Cybercrime [ICSI/UCSB]
- Merge with economic research
 - Event studies [Romanosky, Telang, and Acquisti, 2010]
 - Topology data [LCA, EPFL]
 - Connectivity and airline data [Kearns and Ortiz, 2004]
 - Estimation of structural parameters



Let's not forget about **privacy**

- Behavioral privacy research
 - Surveys and experiments to demonstrate and explain inconsistency between attitudes and behavior
 - Social status and demand for privacy and security
- Factors:
 - Asymmetric uncertainty and ambiguity
 - Non-monetary valuation by users
 - Monetary valuation of information by companies vs. human right

[Acquisti and Grossklags, 04 - ...]



Summary of methodology

1. Formal analysis
 - Game-theoretic predictions
 - Impact of various parameters
2. Experimental research
 - Controlled lab and online experiments
 - Behavioral modeling
3. Field data measurement
 - Acquisition of attacker data (criminal markets goods, advertisements, ...)
 - Acquisition of investment patterns
4. Testing intervention mechanisms
 - Incentives, legal issues, public policy



Related Publications

- J. Grossklags, N. Christin, and J. Chuang. Secure or Insure? A Game-Theoretic Analysis of Information Security Games. [WWW'08](#).
- J. Grossklags, B. Johnson. Uncertainty in The Weakest Link Security Game. [GAMENETS '09](#).
- J. Grossklags, B. Johnson and N. Christin. When Information Improves Information Security. [FC'10](#).
- J. Grossklags, B. Johnson and N. Christin. The Price of Uncertainty in Security Games. [WEIS'09/SPRINGER'10](#).
- B. Johnson, J. Grossklags, N. Christin and J. Chuang. Are Security Experts Useful? Bayesian Nash Equilibria for Network Security Games with Limited Information. [ESORICS'10](#).
- B. Johnson, J. Grossklags, N. Christin and J. Chuang. Uncertainty in Interdependent Security Games. [GAMESEC'10](#).
- J. Grossklags, S. Radosavac, A. Cárdenas and J. Chuang. Nudge: Intermediaries' Role in Interdependent Network Security. [TRUST'10](#).



A vertical chain of metal links is positioned on the left side of the slide, extending from the top to the bottom. The background is a blue gradient that is lighter in the center and darker at the top and bottom. The text is overlaid on the right side of the chain.

Questions?

Contact: jensg@ist.psu.edu

**Thanks to Ed Felten, Nicolas Christin,
Alessandro Acquisti, Benjamin Johnson,
John Chuang, Deirdre Mulligan, Hal Varian and
Teck-Hua Ho.**