

Introduction to the Economics of Cybersecurity

The challenges of cybersecurity

- early and current generation of hackers
- biggest challenge facing in the future
- information security breaches entail direct and indirect costs
- trust in electronic transactions
- information and communications technologies have permeated all aspects of society
- reaching an appropriate level of information security is difficult

- factors that endanger information security:
 - more and more of players required to provide advanced communication systems
 - national and international broadband connectivity
 - complexity of attacks
 - social networks, new mobile devices and applications, and the emergence of new services related to cloud computing

Economics of Cyber Security

- Market players make their own tradeoffs regarding what kind of security measures they deem appropriate and rational, given their business model
- security failures are the outcome of rational economic decisions
- some level of insecurity is economically justifiable
- key question is whether the costs and benefits perceived by market players are aligned with social costs and benefits of an activity
- security decisions of a market player may be rational for that player but its course of action may impose costs on other market players
- These costs are typically not taken into account by the market player making the initial decision, causing an externality → lead to sub-optimal outcomes if left unaddressed

- Security externality is a key concept, but economics offers a broader framework to make sense of security issues
- Dominance in software markets can be due to network externalities
- → the more people use certain software, the more valuable it becomes and the more users it attracts → effects on security
- To become dominant, platform vendors may be reluctant in implementing security restrictions for complementary products
- large providers are more or less immune to such forms of peer pressure and have weaker incentives to act against security problems

- Looking at security issues in terms of costs and benefits also helps to put broader security questions in perspective
- Where we have better evidence that economic damage is indeed rising, fraud levels may actually be diminishing

Main themes of this special issue

- Public awareness campaigns: divergent opinions
 - Support: consumers are clueless facilitators of crime (by publishing personal data)
 - Resistance: consumers are victims (public and private organizations want to distract from their faults)
- Key question: who benefits more from publicity available information on security incidents, the attackers or the defenders?
 - Study impact of publicity available information on phishing websites
 - Conclusion: strategic disclosure of incident information can actually help defenders (depending on procedure)

- Cloud computing: security risks
 - Could be used as new platforms for malice
 - Customers: cannot easily assess security policies and precautions of providers

- Cyber attacks cannot be solved by end users
 - Study: government subsidies for cleaning computers
 - Approximately 1\$/person

- Role of information availability in enhancing cybersecurity
 - based on European institutional and regulatory of framework for cybersecurity
 - 3 measures:
 - Information sharing about treats
 - Information sharing about information security breaches
 - Measures that increase information security competence
- Role of resource public key infrastructure (decentralized)
 - Routing protocols weren't designed to ensure data security
 - Solution: resource public key infrastructure: reduce resulting vulnerabilities