Panel Summary:
Incentives, Markets and Information Security

Allan Friedman[1]

[1] PhD Mailboxes, Kennedy School of Government, Harvard University, 79 JFK St, Cambridge MA 02138 USA
Allan_friedman@ksgphd.harvard.edu

Economics and information security should be naturally related: the former deals with the value and distribution of scarce resources, while the latter focuses on protecting and controlling valued resources. Indeed, the observation that information security should be informed by economic theory is not new. Anderson [1] and others have explicitly highlighted the relationship, which can be seen as a natural progression from the economics of crime literature that dates back to the 1960s [2].

The discipline of economics has a set of established methods for analyzing incentives, useful for mapping questions of possession and valuation of resources into tractable, analytic frameworks. The field also has a rich tradition of "mechanism design" or how systems can be structured such that self-interested agents can be induced to behave in socially optimal fashions. Economics also offers a framework for analyzing difficult trade-offs by focusing on the underlying value. Rather than looking at the ability to prevent any sort of system subversion, benefit-cost comparison tools such as return-on-investment and externality identification allow us to examine the overall impact of action or inaction.

This panel was assembled to present a range of issues in information security that can benefit from the application of economic analysis and discuss how engineering and economics are both needed to address a wide range of pressing policy issues. It is by no means a complete description of this nascent interdisciplinary field. Further information can be found in [6] or [3].

Panel Presentations

Bazelel Gavish presented a straightforward economic analysis of a commonly discussed information security issue: spam. Gavish argues the problem stems from the low marginal cost to send messages in a digital environment, and proposes fee-based system that gives a credit to each recipient, claimable from the sender. While the general idea has been discussed before [5], this approach involved both end parties and the service providers. Gavish advocated a dynamic pricing scheme, and highlighted important areas of research for implementation.

Paul Syverson shifted the focus from mechanisms to institutions, arguing the "identity theft is about neither identity nor theft." Syverson highlighted flaws in the current state of consumer authentication, where information that has a very high value in specific contexts (a social security number can open a line of credit or obtain a new password) is undervalued by some actors, leading to arbitrage and fraud. This also introduced the concept of a security externality, where poor protection or overuse of identifying and authenticating information can raise fraud rates for other parties.

Sven Dietrich demonstrated that a single security issue like distributed denial of service (DDOS) attacks presents the opportunity for multiple levels of analysis that stem from unique features of information systems. The nature of the attack stems from the decentralized environment, where the coordination costs of a bot-net are less than the damage inflicted on the target. Networks of subverted machines also raise the question of who should bear responsibility for the damage caused, since the software manufacturer, the machine owner and local ISP could all have theoretically prevented the machine from causing damage. Dietrich even explained the networks of subverted machines were traded in illicit marketplaces, raising questions of trust and quality guarantees. While no single approach can solve the problem of DDOS attacks, each layer of analysis opens an opportunity to raise the costs, reduce the damages and mitigate harms of this critical issue.

Finally, Richard Clayton took a step back, acknowledging the importance of economics in the field of security, but tempering this enthusiasm with several observations. Using the example of email payments, he illustrated that proposed economic solutions might fall flat from simple economic or technical realities. Furthermore, economics is a nice tool, but good numbers are needed to judge efficacy. It is one thing to build internally consistent models but to further extend the field, these models should be consistent with empirical data. Clayton summed up by urging people to learn more about economics, but suggesting that it was "perhaps not yet time to change departments."

Future Directions There is little doubt that information security can be improved by better integrating economic and security theory. Acquiring better data is critical to applying theory in a policy context for both private firms and public decision-makers. Some problems may be small and tractable enough to resolve with well-informed models. The common debate about public disclosure of other's security flaws, for example, has been the focus of much attention, and it is conceivable that a consensus might be reached. Economics also serves as a useful lever with which to break apart major security issues into segments without competing incentives. Similar to Clark et al's "tussle space" theory [4], this would allow computer scientists to better address open problems without worrying about unnecessary conflicts of motivation. Finally, all involved must acknowledge that economics itself isn't the magic bullet: information security solutions, especially those at the user level, should incorporate critical findings in behavioral psychology and usability.

1. Anderson, R.: Why Information Security is Hard - An Economic Perspective. Proceedings In Proc. 17th Annual Computer Security Applications Conference (2001)
2. Becker, G. S. Crime and Punishment: An Economic Approach. The Journal of Political Economy. 76:8 (1968) 169:217
3. Camp, L.J., Lewis, S.(ed.): Economics of Information Security. Kluwer Academic Publishers, Boston MA (2004)
4. D. D. Clark, J. Wroclawski, K. Sollins, R. Braden, Tussle in Cyberspace: Defining Tomorrow's Internet, Proc. ACM SIGCOMM (2002)
5. Cranor, L.F., LaMacchia, B.A.: Spam! Communications of the ACM. 41:8 (1998)
6. Workshop on the Economics of Information Security: Past Workshops http://infosecon.net/workshop/past.php (2005)