Economics of Information Security

Several years ago, a number of researchers began to realize that many security systems fail not so much for technical reasons as from misplaced incentives. Often the people who could protect a system were not the ones who suffered the costs of failure. Hospital medical-records systems provided comprehensive billing-management features for the administrators who specified them, but were not so good at protecting patients' privacy. Automatic teller machines suffered from fraud in countries like the United Kingdom and the Netherlands, where poor regulation left banks without sufficient incentive to secure their systems, and allowed them to pass the cost of fraud along to their customers. And one reason the Internet is insecure is that liability for attacks is so diffuse.

Ross Anderson
University of Cambridge

Bruce Schneier
Counterpane Internet Security

In all of these examples, the economic considerations of security are more important than the technical considerations.

Economic aspects of security

More generally, many of the most basic security questions are at least as much economic as technical. Do we spend enough keeping hackers out of our computer systems? Or do we spend too much? For that matter, do we spend appropriate amounts on police and army services? And are we spending our security budgets on the right things? In the shadow of 9/11, such questions have acquired a heightened importance.

Economics can actually explain many of the puzzling realities of Internet security. Firewalls are common; email encryption is rare: not because of the relative effectiveness of the technologies, but because of the economic pressures that drive companies to install them. Companies rarely publicize information about intrusions because of economic incentives against doing so. And an insecure operating system is the international standard, in part because its economic effects are largely borne not by the company that builds the operating system, but by the customers that buy it.

Some of the most controversial cyberpolicy issues also sit squarely between information security and economics. Take, for example, the issue of digital rights management. Is copyright law too tight—or not tight enough—to maximize society's creative output? And if it isn't tight enough, will DRM technologies actually benefit the music industry or the technology vendors? Is "trusted computing" a good idea, or just another way for Microsoft to lock its customers into Windows, Media Player, and Office? Any attempt to answer these questions becomes rapidly entangled with both information security and economic arguments.

For all these reasons, interest in "security economics" has grown rapidly among information security researchers and economists. Here we offer six articles selected from the 18 presented at the third annual Workshop on Economics and Information Security, which was held 13–14 May 2004 at the University of Minnesota.

The articles

One of the hot debates in security economics is about vulnerability disclosure. Those in the open-source and free-software communities argue that openness helps the defender more, while proprietary software vendors claim that openness is more valuable to attackers. The two opening articles in this issue present these opposing viewpoints from the economic perspective.

Eric Rescorla's article "Is Finding

Security Holes a Good Idea?" argues that because large modern software products such as Windows contain many security bugs, removing an individual bug makes little difference to the likelihood that an attacker will find exploits later in a product's life. However, a significant number of exploits are based on vulnerability information disclosed, whether explicitly by researchers or implicitly when manufacturers ship patches. Rescorla therefore argues that, unless discovered vulnerabilities are significantly correlated, it's best to avoid vulnerability disclosure and minimize patching. This is a novel and disturbing argument against openness; interestingly, it centers on vulnerability statistics—which we might be able to measure empirically over time.

Ashish Arora and Rahul Telang argue for openness in "Economics of Software Vulnerability Disclosure." Their thesis is that software vulnerability disclosure policies should, in some cases, be more aggressive to push vendors into investing more in patch management. Their analysis proceeds from an idealized software life cycle in which they consider a single representative vulnerability, rather than looking at vulnerability statistics; thus, their work does not necessarily contradict Rescorla's. Together, these two articles will doubtless drive further research regarding this important policy and engineering issue.

In "Privacy and Rationality in Individual Decision Making," Alessandro Acquisti and Jens Grossklags present the latest work on another hot topic: the economics of privacy. The authors use consumer psychology tools to investigate why users' stated privacy preferences differ from their behaviors. The article explores bounded-rationality models, incomplete information theory, and various psychological distortions. For example, consumers tend to take a short-term view of privacy; they discount future risks too deeply, paying particularly little attention to the far off future.

Hal Varian, Fredrik Wallenberg, and Glenn Woroch delve into a narrow but important topic in their article, "The Demographics of the Do-Not-Call List." They used the US Freedom of Information Act to obtain data on the more than 60 million Americans who signed up for the FCC's telephone-sales blacklist. Analyzing the data by district, they extract information about what privacy means to different population groups (which they break down by income, race, number of children, home ownership, and so on). The results raise new, interesting questions: for example, highly educated people with mortgages are more likely to sign up for the do-not-call list, but is that because wealthier households get more calls, or because they value their time more?

In "Toward Econometric Models of the Security Risk from Remote Attacks," Stuart Schechter discusses the problems of trying to model network attacks in the same way that economists interested in crime build economic models of housebreaking. Many of the variables concerning computer or system security risk are hard to pin down, and change rapidly. For example, an analysis of attackers' incentives and costs comes up against the difficulty of assessing products' security strengths. A market for security vulnerability information might bring some clarity here.

Finally, George Danezis and Ross Anderson analyze the economics of censorship resistance. If you're designing a peer-to-peer network to resist attacks from the music industry, what is the trade-off between solidarity and dispersal? Should file swappers pool their resources in centralized systems, forcing the music industry to either close all or none at all; or would a federation of fan clubs be better so that not all could be attacked at once? This is an interesting model for a wide range of conflict games.

These six articles that follow provide a sample of the security economics field as of May 2004. If you find them intriguing, the fourth international workshop on information security economics will take place at Harvard from 2–4 June 2005 (www.infosecon.net/workshop). □

Bruce Schneier *is one of the world's foremost security experts and chief technical officer of Counterpane Internet Security. His most recent book is* Beyond Fear: Thinking Sensibly about Security in an Uncertain World. *You can subscribe to his email newsletter,* Crypto-Gram, *at www.schneier.com.*

Ross Anderson *is a professor of security engineering at the University of Cambridge and one of the founders of the study of security economics. His research interests also include cryptography, protocols, hardware tamper-resistance and peer-to-peer systems. He is the author of the textbook* Security Engineering—A Guide to Building Dependable Distributed Systems. *Contact him via www.ross-anderson.com.*