An Introduction to Key Themes in the Economics of Cyber-Security

Neil Gandal

Tel Aviv University and CEPR

July 13, 2006

Abstract

In this brief paper, I discuss key themes in the budding literature on the economics of cyber-security. My primary focus is on how economics incentives affect the major issues and themes in information security.

I thank Jay P. Choi, Chaim Fershtman, Jacques Lawarree, Shlomit Wagman, several anonymous reviewers from WEIS 2005 and this encyclopedia, and seminar participants from WEIS 2005 for their helpful comments. A research grant from Microsoft is gratefully acknowledged. Any opinions expressed are those of the author.

1. Introduction

It's become commonplace to receive warnings about killer viruses. Some of these are hoaxes, but several real viruses have done significant damage. According to the Economist magazine,[1] the Blaster worm and SoBig.F viruses of 2003 resulted in $35 Billion in damages. Weaver and Paxson (2004) suggest that a worst case worm could cost anywhere from $50 Billion to $100 Billion. And it appears that the time between the announcement of a software vulnerability and the time in which an attack that exploits the vulnerability is launched has declined significantly. According to the Economist, the time from disclosure to attack was six months for the Slammer worm (January 2003), while the time from disclosure to attack for the Blaster worm (August 2003) was only three weeks.

The Slammer, Blaster, and Sobig.F worms exploited vulnerabilities even though security patches or updates eliminating the vulnerabilities had been released by Microsoft. That is, although the updates were widely available, relatively few users applied them. Indeed, a 2004 survey found the following:[2]

- 80 percent of the computers connected to the Internet are infected with spyware.
- 20 percent of the machines have viruses.
- 77 of those surveyed thought that they were very safe or somewhat safe from online threats, yet 67 percent did not have updated antivirus software.
- 2/3 of all computer users had no firewall protection.

In this short paper, I discuss key themes in the budding literature at the "intersection" of computer science/engineering issues and the economics incentives associated with cyber security and software provision. My primary focus is on how economic incentives affect

[1] http://www.economist.co.uk/science/displayStory.cfm?story_id=2246018.
[2] From the article "Home Web Security Falls Short, survey Shows" by John Markoff, October 25, 2004, available at http://www.staysafeonline.info/news/safety_study_v04.pdf.

the major issues and themes in information security.[3] A quick introduction to the topic can be found at Ross Anderson's "Economics and Security Resource Page."[4] Another source of information is the annual Workshop on Economics and Information Security (WEIS).[5]

2. Two Key Phenomena: Security Externalities and Network Effects

Two key phenomena relevant for the economics of cyber security issues are (I) a security externality and (II) a network effect that arises in the case of computer software.

2.1 Security Externality

Unprotected computers are vulnerable to being used by hackers to attack other computers. There is a lack of incentive for each user in the system to adequately protect against viruses in his system, since the cost of the spread of the virus is borne by others. That is, computer security is characterized by a positive "externality." If I take more precautions to protect my computer, I enhance the security of other users as well as my own. Such settings lead to a classic free-rider problem. In the absence of a market for security, individuals will choose less security than the social optimal. Solutions to the free-rider problems have been addressed in many settings. Hence, I do not elaborate on this issue here.

2.2 Network Effects

A network effect arises in computer software. The benefits of computer software typically depend on the number of consumers who purchase licenses to the same or compatible software. A direct network effect exists when increases in the number of consumers on the network raise the value of the good or service for everyone on the

[3] Legal issues are surveyed by Grady and Francesco (forthcoming 2006). Readers interested in the economics of privacy should see the web page maintained by Alessandro Acquisti: http://www.heinz.cmu.edu/~acquisti/economics-privacy.htm.

[4] See http://www.cl.cam.ac.uk/users/rja14/econsec.html. For a wealth of articles on computer security, see Bruce Schneier's web page at http://www.schneier.com/essays-comp.html.

[5] The first conference was held in 2002. Websites for the 2002-2005 conferences are included in the list of references.

network. The most common examples are communication networks such as telephone and email networks.

A network effect also exists when individuals consume a "hardware" good and complementary software. In such a system, the value of the hardware good increases as the variety of compatible software increases. Increases in the number of users of compatible hardware lead to an increase in demand for compatible software, which provides incentives for software vendors to increase the supply of software varieties. This in turn increases the benefit of all consumers on the hardware/software or virtual network. Examples of markets where virtual network effects arise are consumer electronics, such as CD players and compact discs and computer operating systems and applications programs.

Given the importance of interconnection in information technology networks, the economics of compatibility and standardization has become mainstream economics. For an introduction to network effects and policy issues, see Gandal (2002) and Church and Gandal (2006).

Network effects are typically thought to benefit consumers and firms that have coalesced around a standard. However, network effects may contribute to security problems. Large networks are more vulnerable to security breaches, precisely because of the success of the network. In part because of its large installed base, Microsoft's Internet Explorer is likely more vulnerable to attack than the Mosaic's "Firefox" Browser. This is because the payoff to hackers from exploiting a security vulnerability in Internet Explorer is much greater than the payoff to exploiting a similar vulnerability in Firefox. I will explore the implications of this "negative network effect" in section 3.2.

3. Research on the Economics of Cyber Security

A significant portion of the research in the economics of cyber security focuses on the creation of markets. I briefly survey this research in sections 3.1. In section 3.2, I discuss research on the incentives of software vendors regarding the provision of security.

3.1 Intermediaries and Markets for Software Vulnerabilities

The Computer Emergency Response Team/Coordination Center (CERT/CC) is a center for Internet security in the Software Engineering Institute at Carnegie Mellon University. Although CERT/CC is not a public agency, it acts as an intermediary between users who report vulnerabilities to CERT/CC and vendors who produced the software and the patches. When informed by a user about a vulnerability, CERT/CC conducts research into the matter. If the user has indeed uncovered a security vulnerability, CERT/CC then informs the software vendor and gives it a 45 day "vulnerability window." This allows the firm time to develop a security update. After the 45 day period, CERT/CC will typically disclose the vulnerability even if a security update has not been made available.

Recently, a private market for vulnerabilities has developed where firms such as iDefense and Tipping Point/3Com act as intermediaries, paying those who report vulnerabilities and providing the information to software users who have subscribed to the service.

There is a growing literature on markets for vulnerability. Camp and Wolfram (2004) heuristically discuss this issue of markets for vulnerabilities. Schechter (2004) formally models the market for vulnerabilities and Ozment (2004) shows how such a market can function as an auction. Kannan and Telang (2004) develop a model with four participants – an intermediary, a benign agent who can identify software vulnerabilities, an attacker, and software users – and ask whether a market based mechanism is better than the setting in which a public agency acts as an intermediary.

In the work discussed in this section, there is no role for software vendors. Software vendors that deal directly with benign agents would likely reduce the need for such intermediary markets.

3.2 Examining Incentives for Software Vendors

In this section, I discuss research that includes software vendors in the models. Arora, Telang, and Xu (2004) theoretically examine the optimal policy for software vulnerability disclosure. The software vendor strategy is limited to whether it will release a patch and if so when to release the patch. August and Tunca (2005) have a strategic software vendor as well, but the vendor strategy is limited to pricing the software. Nizovtsev and Thursby (2005) examine the incentives of software firms to disclose vulnerabilities in an open forum.

Choi, Fershtman, and Gandal (2006) examine how software vulnerabilities affect the firms that develop the software and the consumers that license software. They model three decisions of the firm: An upfront investment in the quality of the software to reduce potential vulnerabilities, a policy decision whether to announce vulnerabilities, and a license price for the software. They also model two decisions of the consumer: whether to license the software and whether to apply a patch. While this model provides a base, further research is needed to examine incentives for software vendors to invest in security.

3.3 Empirical Work in the Economics of Cyber Security

To the best of my knowledge, there are only a few empirical papers in the economics of cyber security. Here I briefly mention a few recent papers. Arora, Nandkumar, Krishnan, Telang, and Yang (2004) examined 308 distinct vulnerabilities and showed that disclosure of vulnerabilities increases the number of attacks per host and installing security updates decreases the number of attacks per host. Arora, Krishnan, Telang, and Yang (2005) find that disclosure deadlines are effective. They find that vendors respond more quickly to vulnerabilities that are processed by CERT/CC than to vulnerabilities not handled by CERT/CC.

3.4 Data for Empirical Work

In many fields, theoretical work progresses much more quickly than empirical work, in part due to the dearth of data. There is clearly an untapped potential for empirical work in the economics of Internet security, since the National Vulnerability Database (NVD), which is assembled by the Computer Security Division of the National Institute of Science and Technology (NIST) is available on line at http://nvd.nist.gov/statistics.cfm.

High quality data are available at the level of the vulnerability as well as at the industry or firm level. The data include information about severity of the vulnerability, the impact of the vulnerability, as well as information on the vulnerability type. This database was employed by Arora, Nandkumar, Krishnan, Telang, and Yang (2004) and Arora, Krishnan, Telang, and Yang (2005).

Suggestions for empirical work can be found by examining the summary statistics available from the NVD. They show that while the number of vulnerabilities in the NVD increased from 1858 in 2002 to 3753 in 2005, the number of "high severity" vulnerabilities has roughly stayed the same during that period.[6] According to the NVD, severe vulnerabilities constituted about 48% of all vulnerabilities in 2002, 33% of all vulnerabilities in 2004, and 23.5% of all vulnerabilities in 2005. These data suggest a fall in the percentage of high severity vulnerabilities as a percentage of all vulnerabilities.

The data further show that vulnerabilities that enable unauthorized access and derive from input validation error, i.e., from either buffer overflow or boundary condition error account for a large and growing percentage of all "high severity" vulnerabilities. While they accounted for approximately 50% of all "high severity" vulnerabilities during 1995-2001, they accounted for 60% of all "high severity" vulnerabilities in 2002-2004. In 2005, they accounted for 72% of all "high severity" vulnerabilities.

[6] The NVD defines a vulnerability to be "high severity" if (i) it allows a remote attacker to violate the security protection of a system (i.e. gain some sort of user, root, or application account), (ii) it allows a local attack that gains complete control of a system, or (iii) it is important enough to have an associated CERT/CC advisory or US-CERT alert. See http://nvd.nist.gov/faq.cfm.

It would be helpful for researchers to try to determine what is driving these and other trends. These simple statistics suggest that interdisciplinary empirical is likely to be quite fruitful. Economists may be able to identify trends in the data, but without collaboration with Computer Scientists and Engineers, it will not be possible to understand the implications of these numbers. Hopefully such work will be forthcoming in the not too distant future.

References:

August, T., and T. Tunca, "Network Software Security and User Incentives," Stanford University mimeo, 2005.

American Online and the National Cyber Security Alliance, *AOL/NCSA Online Safety Study*, October 2004.

Arora, A., Telang, R., and H. Xu, "Optimal Policy for Software Vulnerability Disclosure," Carnegie Mellon Working Paper, 2004

Arora, A., A. Nandkumar, R Krishnan, R Telang, and Y Yang (2004), "Impact of Vulnerability Disclosure and Patch Availability — An Empirical Analysis", 3rd Workshop on Economics and Information Security, Minneapolis, May 13-15. http://www.dtc.umn.edu/weis2004/telang.pdf.

Arora, A., Krishman, R., Telang, R, and Y.Yang, "An Empirical Analysis of Vendor Response to Software Vulnerability Disclosure, mimeo, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=786128.

Anderson, R., (2001), "Why Information Security is Hard," available at http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/econ.pdf.

Camp, L.J., and C. Wolfram, "Pricing Security," in L.J. Camp and S. Lewis, eds., Economics of Information Security, vol. 12, Advances in Information Security. Springer-Kluwer, 2004.

Choi, J., Fershtman, C., and N. Gandal, "Internet Security, Vulnerability Disclosure, and Software Provision," 2006 mimeo.

Church, J., and N. Gandal, "Platform Competition in Telecommunications," 2006, pps. 117-153, in The Handbook of Telecommunications Volume 2, M. Cave, S. Majumdar, and I. Vogelsang editors, Elsevier.

Gandal, N., "Compatibility, Standardization, & Network Effects: Some Policy Implications," 2002, *Oxford Review of Economic Policy*, 18: 80-91.

Grady, M. and P. Francesco, "The Law and Economics of Cybersecurity: An Introduction," Cambridge University Press, forthcoming 2006, available at http://ssrn.com/abstract=622985.

Kannan, K., and R. Telang, "Market for Software Vulnerabilities? Think Again," Carnegie Mellon Working Paper, 2004.

Nizovtsev, D., and M. Thursby, "Economic Analysis of Incentives to Disclose Software Vulnerabilities," mimeo, available at http://infosecon.net/workshop/pdf/20.pdf.

Ozment, A., "Bug Auctions: Vulnerability Markets Reconsidered," mimeo, available at http://www.dtc.umn.edu/weis2004/ozment.pdf

Schechter, S., "Computer Security, Strength and Risk: A Quantitative Approach," 2004, available at http://www.eecs.harvard.edu/~stuart/papers/thesis.pdf

Weaver, N., and V. Paxson, 2004, "A Worst Case Worm," available at http://www.dtc.umn.edu/weis2004/weaver.pdf.

WEIS 2002: Held at UC-Berkeley. Papers are available at http://www.sims.berkeley.edu/resources/affiliates/workshops/econsecurity/.

WEIS 2003: Held at the University of Maryland. Papers are available at http://www.cpppe.umd.edu/rhsmith3/agenda.htm.

WEIS 2004: Held at the University of Minnesota. Papers are available at http://www.dtc.umn.edu/weis2004/agenda.html.

WEIS 2005: Held at Harvard University. Papers are available at http://infosecon.net/workshop/schedule.php.