Workshop on the Economics of Information Security (WEIS 2006)

Hackers, Users, Information Security

I.P.L. Png, Candy Q. Tang, Qiu-Hong Wang

Revised, May 2006

Abstract

We analyze the strategic interactions among end-users and between end-users and a hacker. We show that security efforts by end users are strategic substitutes. This explains the inertia among end-users in taking precautions even in the face of grave potential consequences. Next, we analyze the direct and indirect effects of changes in user fixing cost and the rate of enforcement against hacking. For instance, a reduction in user fixing cost would directly lead users to increase fixing effort. However, that would make them less attractive targets, and so induce less hacking, and hence, indirectly lead users to *reduce* fixing.

National University of Singapore. Corresponding author: Ivan Png, tel: +65 6516-6807; http://www.comp.nus.edu.sg/~ipng/. We thank Anindya Ghose and the anonymous referees for very helpful advice and suggestions.

1. Introduction

Information security is a critical issue of both national policy and business operations (Whitman 2003). For instance, in May 2004, Sven Jaschan created the Sasser worm to exploit a vulnerability in the Windows 2000 and XP operating systems. The Sasser worm and its variants caused hundreds of thousands of PCs to crash (ZDnet 2005). In August 2003, the Microsoft Blaster worm exploited a vulnerability in Windows 2000 and XP to infect hundreds of thousands of computers, from which it launched a "denial of service" attack on the Microsoft Windows Update server (Register 2003). During the summer of 2001, the "Code Red" worm and its successor "Code Red II" exploited a vulnerability in the Microsoft Internet Information Server to cause over $2 billion in damage (Moore et al. 2002). The threat of attack and intrusion now extends to mobile phones (Symantec 2005).

Information security depends on user efforts – to fix vulnerabilities, install and update software to detect neutralize viruses and other malicious software, install and configure firewalls, take care with file-sharing programs and email attachments, etc. Indeed, vendors and public IT agencies regularly exhort users to take more precautions and generally improve security.[1]

Information security is a critical issue only because of the activities of (unethical) hackers.[2] Industry has systematically tracked hacker behavior: "Attackers continuously look for easy targets, those that will provide them with the maximum return on the time they invest in writing malicious code" (Symantec 2005, page 55). Clearly, hacker activity depends on user behavior.

While there has been some research into the incentives of end-users (Kunreuther and Heal 2002, August and Tunca 2005), and the motivations of hackers (eg, Jordan and Taylor 1998; Van Beveren 2000), there has been little scholarly attention to the *strategic* interaction between end-users and hackers.

In this paper, we analyze the strategic interactions among end-users and between end-users and a hacker. We address two questions in particular. First, it is well known that information security poses grave potential consequences. Yet, end-users seem quite slow to take precautions (Boss 2005) – to the point that they must be exhorted and goaded by government and vendors. What explains this inertia?

Second, given the strategic interactions, how does information security vary with changes in user fixing cost and the rate of enforcement against hacking? This question is not trivial. For instance, a reduction in user fixing cost would directly lead users to increase fixing effort. However, that would make them less attractive targets, and so induce less

[1] See, for instance, US-CERT (2006).
[2] We will focus on *unethical* hackers, and, for brevity, simply refer to them as "hackers".

hacking, and hence, indirectly lead users to *reduce* fixing. Accordingly, the net effect depends on the balance between direct and indirect effects.

2. Prior Literature

Information security is an issue of tremendous concern to governments and businesses worldwide (Whitman 2003). Generally, it involves four groups of persons – users, hackers, software vendors, and security specialists such as CERT/CC. Further, it is now recognized to be as much as an issue of economic incentives as a technological problem (Anderson 2001).

Most economic analysis has focused on the policies of software vendors, CERT/CC and other security specialists to disclose security flaws and provide the appropriate patches (see, for instance, Cavusoglu, Cavusoglu, and Raghunathan 2004; Choi, Fershtman, and Gandal 2004; Nizovtsev and Thursby 2005; Arora, Caulkins, and Telang 2005; Jaisingh and Li 2005). Other analyses have focused on users' incentives to share information (Gal-Or and Ghose 2005) and implementation of detection systems (Cavusoglu, Mishra, and Raghunathan 2005).

August and Tunca (2005) consider the behavior of users, and specifically, their incentive to patch security flaws. In a finding that is reminiscent of the public-health literature on infectious diseases, they show that mandatory patching is not optimal (Brito et. al. 1991; Philipson 2001). With commercial software, the optimal policy is a subsidy on patching when security risk and patching cost are high, and no policy otherwise. However, with open-source software, the optimal policy is a subsidy on patching when both security risk and patching costs are low, and a tax on software usage otherwise.

August and Tunca (2005) assume that users consider the risk of attack when deciding whether to fix their software. This assumption is consistent with empirical analyses of crime and victim precautions. For instance, in a study of migration from urban areas, Cullen and Levitt (1999) found that each additional reported crime was associated with a decline in urban population by about one person. In particular, the migration of highly educated households and those with children was relatively more sensitive to crime.

However, in the specific context of software security, the risk of attack did not have a significant effect on experimental subjects' intention to take precautions (Boss 2005). Further, in a recent survey of residential Internet users, 78% of respondents felt "somewhat safe", "not very safe", or "not at all safe" from online threats, but only 67% protected themselves with a firewall (National Cyber Security Alliance, 2005). Apparently, users are still slow to expend effort in information security. The question is why?

Kunreuther and Heal (2002) study a positive network externality among users in taking precautions against attack. Specifically, they assumed that each user makes an all-or-nothing choice between taking precautions or not taking precautions, and that, the expected loss to any user decreases with others' precautions. They show that, for a wide range of cost and risk parameters, there are two equilibria – either all users invest in precautions or no one does. Kunreuther and Heal (2002), however, did not analyze why the expected loss to any user decreased with others' precautions, and specifically, the role of hackers.[3]

Previous research has not analyzed the economic incentives and behavior of hackers. The mentality of hackers has evolved over time, with greed, power, and revenge superseding curiosity and other benign motivations (Jordan and Taylor 1998). Importantly, Van Beveren (2000) identified two external factors that encourage hackers – the perception that hacking is seldom punished and peer approval from other hackers.

More recently, the motivation of hackers has shifted towards making money: "They often attempt to perpetrate criminal acts, such as identity theft, extortion, and fraud" (Symantec, 2005, page 4). This portends greater losses as hackers aim "to create more malicious code and that will become stealthier and more selective" (Symantec 2005, page 9).

By contrast with the previous research, we focus on the strategic interaction among end-users and between users and hackers. Our analysis shows how users' effort in fixing depends on the hacker's attacking effort and vice versa. Accordingly, we can show how changes in policy toward hackers will affect user behavior, and, also how policy changes toward users will influence hacker behavior.

3. Basic Setting

For concreteness, we consider a setting of software vulnerabilities, but note that similar conclusions apply to other contexts of information security. Consider the market for some commercial software, which is produced by a monopoly and sold at a uniform price p. (We assume a simple market structure, in order to focus on the interaction between end-users and hacker.)

End-users derive benefit, v, from use. The vendor would set price such that $v > p$, else there would be no demand. End-users differ in naivete, n, which is distributed according to the cumulative distribution function, $\Phi(n)$ between [0, 1], with 0 representing the least naïve (most sophisticated) user and 1 representing the most naïve user. All users are risk-neutral.

[3] See also Varian (2004).

A software user suffers an attack with probability $\alpha(f)\chi$, where $\alpha(f)$ is a probability that depends on the user's effort, f, in fixing the software, with the properties

$$\alpha(0)=1, \lim_{f\to\infty} a(f)=0, \frac{d\alpha}{df}<0, \frac{d^2\alpha}{df^2}>0. \quad (1)$$

and χ is a probability that measures the effectiveness of hacker effort. If the user suffers an attack, she will not derive any benefit from the software, and in addition, will suffer some harm, h.[4] The user's cost of patching the software is ncf. Each potential user decides whether to buy and, if so, chooses fixing effort to maximize her expected net benefit.

There is a single hacker, who chooses effort k in hacking, which determines the effectiveness probability $\chi=\chi(k)$, where

$$\chi(0)=0, \lim_{k\to\infty} \chi(k)=1, \frac{d\chi}{dk}>0, \frac{d^2\chi}{dk^2}<0. \quad (2)$$

The hacker derives enjoyment, e from an attack on a user, provided that he is not discovered. With enforcement probability, η, the authorities discover the hacker and then impose a penalty with monetary value, s, and prevent his enjoyment. Further, the cost of hacking effort is $c_K(k)$, where $c_K(k)$ is convex in k, and to ensure that the equilibrium outcome is not trivial, we assume that the parameters are such that

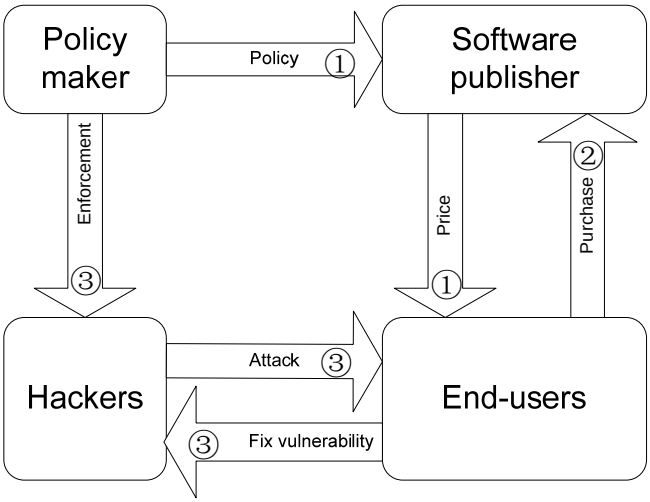
$$\chi(k) \le \frac{v}{v+h}. \quad (3)$$

The hacker chooses effort to maximize his expected net benefit. This modeling assumption is consistent with Symantec's (2005, page 55) observation that hackers direct efforts against targets that provide the maximum return on effort.

The software publisher sets price p to maximize profit. The sequence of events is as follows:

Figure 1: Sequence of events

[4] This set-up is similar to that in the literature on enforcement against copyright piracy (see, for instance, Chen and Png (2003)).

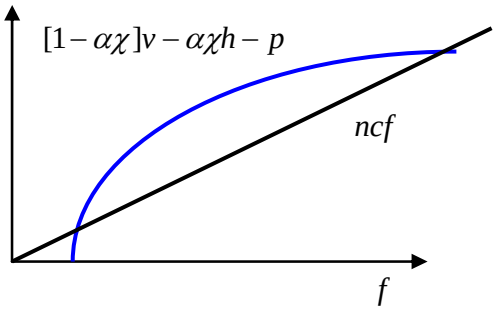


4. User-Hacker Equilibrium

Consider the end-user with type (naivete), n. If she buys the software, her expected net benefit, given the hacking level χ, would be

$$B(n \mid \chi) = [1-\alpha(f)\chi]v - \alpha(f)\chi h - p - ncf \ . \qquad (4)$$

Figure 2: User fixing effort



Maximizing with respect to f,

$$-[v+h]\chi\frac{d\alpha}{df} = nc \text{, or } \frac{d\alpha}{df} = \frac{nc}{-[v+h]\chi} \qquad (5)$$

which defines the net-benefit maximizing effort, $f(n \mid \chi)$, as a function of the user type and hacker effort. By inspection of (5), we have[5]

Observation 1. User fixing effort, f, is continuous and decreasing in naivete, n, and fixing cost, c, independent of price, p, and continuous and increasing in hacker effort, k, such that, if $k = 0$, then $f(n) = 0$, and there exists $f_\infty(n) > 0$ such that $\lim_{k\to\infty} f(n) = f_\infty(n)$.

[5] We prove all results in the Appendix.

We next characterize the demand for the software. By (4), every user for whom $B(n \mid \chi) \geq 0$ will buy the software. It is relatively straightforward to prove that $B(n \mid \chi)$ is decreasing in n. Accordingly, we have

Observation 2. Either all users buy the software or there exists a marginal user, $\hat{n}$, defined by

$$B(\hat{n}) = v - [v + h]\alpha(f(\hat{n}))\chi - p - \hat{n}cf(\hat{n}) = 0, \quad (6)$$

and such that only users with $n \leq \hat{n}$ buy the software.

The demand for the software arises from the users with $n \leq \hat{n}$, hence the quantity demanded (equal to the vendor's sales) is

$$\int_0^{\hat{n}} d\Phi(n). \quad (7)$$

The following result shows how the demand for software depends on the hacker's effort and the vendor's price.

Observation 3. The marginal user type, $\hat{n}$, is continuous and decreasing in user fixing cost, *c*, and the price, p, and continuous, decreasing and convex in the hacker's effort, k. In addition, $\lim_{k \to 0} \hat{n} = 1$ and $\lim_{k \to \infty} \hat{n} = \hat{n}_0$, where $0 \leq \hat{n}_0 \leq 1$.

Having analyzed user behavior (choices of whether to buy the software and, if so, the fixing effort) as a function of the hacker's efforts, we now consider the hacker's effort as a function of user behavior. The hacker chooses k to maximize expected net benefit,

$$H(k \mid \hat{n}, f(n)) = [1 - \eta]\int_0^{\hat{n}} \alpha(f(n))d\Phi(n) \cdot \chi(k)e - \eta s - c_K(k). \quad (8)$$

By (2) and since $c_K(k)$ is convex, the function H is concave in k. Maximizing H with respect to k, the first-order condition is

$$e[1 - \eta]\frac{d\chi}{dk}\int_0^{\hat{n}} \alpha(f(n))d\Phi(n) = \frac{dc_K}{dk}, \quad (9)$$

which characterizes the hacker's effort.

Observation 4. Hacker effort, k, is continuous and decreasing in the enforcement rate, η. Further, hacker effort, k, is continuous and increasing in the marginal user type, $\hat{n}$, and, if $\hat{n} = 0$, then $k(\hat{n}) = 0$, and there exists some $k_1 > 0$ such that if $\hat{n} = 1$, then $k(\hat{n}) = k_1$. In addition, hacker effort, k, is continuous and decreasing in user fixing effort, f, and there exists some $k_0 > 0$ such that if $f = 0$, then $k = k_0$, and there exists some $k_\infty \geq 0$ such that if $f \to \infty$, then $k = k_\infty$.

Observation 4 is consistent with expert observations. As Microsoft Internet Explorer dominated the market for Internet browsers, it became "an inviting target for hackers" and relatively less secure (cio.com 2005).

For the analysis to be meaningful, we must show that there exists a non-trivial equilibrium. To prove existence, it is useful to consider the rate at which software users are subject to security attack, conditional on hacker effectiveness, $\chi(k)$, i.e, the *conditional vulnerability* of users,

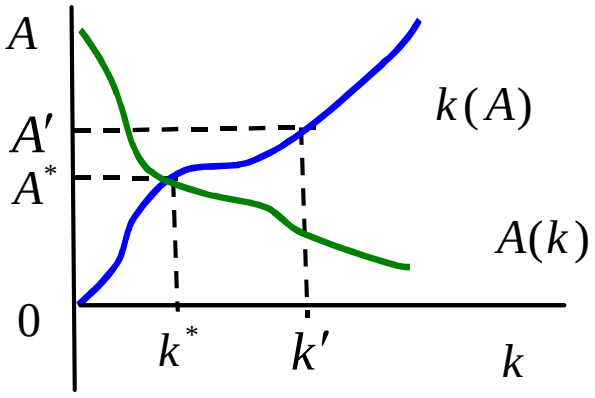
$$A(k) = \int_0^{\hat{n}(k)} \alpha(f(n \mid k)) d\Phi(n). \qquad (10)$$

Accordingly, the function $A(k)\chi(k)$ is the rate at which software users actually suffer security attack, i.e, the *effective vulnerability of users*.

Lemma 1 proves the existence of equilibrium by considering the relation between $A(k)$ and hacking effort, k. The effective vulnerability is a continuous decreasing function of hacker effort, and similarly, hacker effort is a continuous increasing function of the effective vulnerability of users. Figure 3 illustrates the result.

Lemma 1. There exists a non-trivial equilibrium between end-users and hacker, k^*, $\hat{n}(k^*)$ and $f(\hat{n}(k^*) \mid k^*)$.

Figure 3. User-hacker equilibrium



Our first substantive result focuses on the strategic interaction among end-users. Proposition 1 shows that, given hacker behavior, users' patching efforts are *strategic substitutes* (Bulow et al. 1985).

Proposition 1. Given hacker behavior, user efforts in patching are strategic substitutes: The higher the patching effort of others, the lower the patching effort of any particular individual.

By contrast with our Proposition 1, Kunreuther and Heal (2002) suggest that user efforts in security are *strategic complements*, and that the equilibrium outcome is of an all-or-nothing nature – either all users or none take precautions. By contract, our analysis implies that user efforts are strategic substitutes, hence the equilibrium outcome could involve an intermediate level of effort.

Empirical evidence appears to lend stronger support to our analysis than that of Kunreuther and Heal (2002). Table 1 reports data from an annual survey of U.S. residential computer users. It suggests that users take an intermediate level of precautions, rather than follow an all-or-nothing approach.

Table 1: User security measures

Security measure	2004	2005
Equipped with anti-virus software	85%	83%
Equipped with properly configured firewall	28%	56%
With active or open file sharing program	23%	11%
Source: National Cyber Security Alliance, 2004 and 2005.		

The impact of Lojack in the U.S. provides further suggestive empirical evidence. Lojack is a concealed device that allows police to track a stolen vehicle. Ayres and Levitt (1998) measured a significant positive externality from Lojack installation: when one owner installed Lojack, he/she significantly reduced the likelihood of the theft of *other* vehicles. Proposition 1 implies that a free-rider problem exists in user security. If other users raise their fixing effort, they will reduce the expected harm to any particular user, and she will rationally respond by reducing her fixing effort. This free-rider problem is reminiscent of that arising from concealed precautions, such as Lojack, by potential crime victims (Koo and Png 1994; Ayres and Levitt 1998).

5. Empirical Implications

The preceding analysis was "partial" in the sense that we considered only the direct effects of changes in vendor strategy and government policy, and ignored the indirect (feedback) effects through the actions of the other side of the market. We now consider the effects of changes in vendor strategy and government policy on the equilibrium between users and hackers. Accordingly, this analysis encompasses both direct and indirect effects.

Our model reveals that policy changes may induce countervailing feedback effects. Consider, for instance, an increase in the price, *p*, on the demand for software. An increase in price would directly reduce $\hat{n}$, i.e., lead some users to stop buying the software. However, the price increase will also have an indirect (consequential) effect through the effect of user choices on hacking. With fewer users buying the software, the hacker's benefit would be lower, hence he will invest less effort, which reduces the probability of attack and so raises users' expected net benefit. Thus, the indirect effect from the hacker tends to offset the direct effect of the price increase. Accordingly, the demand for software is *less elastic* than would appear from studying the direct effect alone.

Next consider an increase in enforcement, η. This directly leads the hacker to reduce his effort. However, there is also an indirect effect: users would respond to the reduced hacking by reducing their fixing effort, and also the demand for the software would increase. Accordingly, the net impact on security (as measured by the effective user vulnerability) depends on the balance of the direct and indirect effects.

Responding to public concern, software vendors have invested heavily to facilitate user fixing. For instance, in August 2004, Microsoft released Service Pack 2, to enhance user security. What would be the impact of Microsoft's action? Our analysis points to some unintended effects: specifically, actions to reduce user fixing costs need not enhance overall security. As reported in Proposition 2 below, actions to reduce user fixing costs would *enhance* overall security (as measured by effective user vulnerability) if the user fixing cost is sufficiently high, but *reduce* overall security if the user fixing cost is sufficiently low.

Proposition 2. Effective user vulnerability, χA, is decreasing in the enforcement rate, η, and increasing in the user fixing cost, c, if it is sufficiently high, but decreasing if it is sufficiently low.

Table 2 summarizes the net effect on user's fixing effort, hacker's effort and software demand with regard to change in price, p, enforcement rate, η, hacking cost, c_k, and user fixing cost, c.

Table 2. Empirical Implications

Net Effect / Change	User's fixing effort, f	Hacker's attacking effort, k	Software demand, $\hat{n}$	Conditional user vulnerability, A	Effective user vulnerability, χA
Price, p	decreasing	decreasing	decreasing	decreasing	decreasing

Fixing cost, c	$\partial A/\partial c \geq 0$	decreasing	increasing	decreasing	increasing	increasing
	$\partial A/\partial c < 0$	decreasing	decreasing	decreasing	decreasing	decreasing
Enforcement rate, η		decreasing	decreasing	increasing	increasing	ambiguous
Hacking cost, c_k		decreasing	decreasing	increasing	increasing	ambiguous

Our empirical implications are consistent with the actual impact of Service Pack 2 on information security. Since Service Pack 2 reduced user fixing costs, Table 2 predicts that it would lead users to increase security efforts. Consistent with this prediction, referring to Table 1, between 2004-05, the proportion of U.S. residential Internet users equipped with anti-virus software dropped slightly, while the proportion with properly configured firewalls *rose* from 28% to 56%, and the proportion with active or open file sharing programs dropped from 23% to 11%. Meanwhile, as for hackers, between the first halves of 2004 and 2005, the average number of attacks against Internet-linked computers fell from 78 to 57 per day (Symantec 2005).

Having analyzed the strategic interaction among end-users and between end-users and hacker, we now consider the software vendor's behavior. Insecurity of systems and software is like a degradation of product quality where the quality depends on the users' effort. In such an environment, how should a vendor set price?

By assumption, the cost of producing the software is zero, hence, by (7), the vendor's profit is

$$\Pi = p\int_0^{\hat{n}} d\Phi(n) \tag{11}$$

The profit-maximizing price is characterized by the first-order condition,

$$\frac{d\Pi}{dp} = \int_0^{\hat{n}} d\Phi(n) + p\frac{d\hat{n}}{dp}\frac{d}{dn}\Phi(\hat{n}) = 0\,. \tag{12}$$

We assume that the parameters satisfy the second order condition. Now

$$\frac{d\hat{n}}{dp} = \frac{\partial\hat{n}}{\partial p} + \frac{\partial\hat{n}}{\partial k}\frac{dk}{dp} > \frac{\partial\hat{n}}{\partial p} \tag{13}$$

since, by Observation 3, $\partial\hat{n}/\partial k < 0$, and by Table 2, $dk/dp < 0$. Intuitively, the indirect (feedback) effect of a price increase on hacker effort causes demand to be less elastic. Accordingly, by (12) and (13), the vendor should set a relatively *higher* price than in the absence of hacking.

6. Limitations and Future Work

Our analysis assumed that there was only one hacker. The key direction for future work is to analyze a setting with multiple hackers. Then, the essential issue would be how the efforts of the various hackers interact, and specifically, whether these are complementary or substitutes.

The second important limitation is that we assumed that the user's cost of fixing was exogenous. Realistically, both government and vendor affect this cost. It would be interesting to incorporate these decisions into the analysis.

Finally, it is important to apply our analytical framework to study public policy towards information security. Information security can be and are addressed from two angles – encouraging end-users to fix quickly, and enforcement against hacking. Both policies are costly. Owing to the strategic interaction, policies directed at end-users will affect hacker behavior, and enforcement against hacking will affect end-user behavior. Using our analysis, we can characterize the appropriate balance between the two policy directions from the standpoint of social welfare.

References

Anderson, Ross, "Why information security is hard – An economic perspective", *17th Annual Computer Security Applications Conference*, 2001.

Arora, Ashish, Ramayya Krishnan, Rahul Telang, and Yubao Yang, "An Empirical Analysis of Vendor Response to Software Vulnerability Disclosure", Working Paper, Heinz School of Public Policy and Management, Carnegie Mellon University, August 2005.

August, Terrence, and Tunay I. Tunca, "Network Software Security and User Incentives", Unpublished manuscript, Graduate School of Business, Stanford University, Revised, August 2005.

Ayres, Ian, and Steven D. Levitt, "Measuring the Positive Externalities from Unobservable Victim Precaution: An Empirical Analysis of Lojack," *Quarterly Journal of Economics*, Vol. 113, No. 1, 1998, 43–77.

Boss, Scott, "Control, Risk, and Information Security Precautions", Katz Graduate School of Business, University of Pittsburgh, 2005.

Brito, Dagobert L., Michael D. Intriligator, and Eytan Sheshinski, "Externalities and Compulsory Vaccinations", *Journal of Public Economics*, 45 (1991), 69-90.

Bulow, Jeremy, John Geanakoplos, and Paul Klemperer, "Multimarket Oligopoly: Strategic Substitutes and Complements," *Journal of Political Economy*, Vol. 93, No. 3, June 1985, 488-511.

Cavusoglu, Hasan, Huseyin Cavusoglu, and Srinivasan Raghunathan, "Analysis of Software Vulnerability Disclosure Policies", Unpublished manuscript, Sauder School of Business, 2004.

Cavusoglu, H., B. Mishra, B. and S. Raghunathan, "The value of intrusion detection systems in information technology security architecture", *Information Systems Research*, Vol. 16 No. 1, 2005, 28-46.

Chen, Yeh-ning, and I.P.L. Png, "Information Goods Pricing and Copyright Enforcement: Welfare Analysis", *Information Systems Research*, Vol. 14 No. 1 (March 2003), 107-123.

Cio.com, "Browser Wars: Will Firefox Burn Explorer?", http://www2.cio.com/higher/report3448.html, March 18, 2005.

Cohen, Mark A., "Measuring the Costs and Benefits of Crime and Justice", Criminal Justice 2000, Volume 4, Office of Justice Programs, US Department of Justice, Washington DC, 263-315.

Conner, K. R., R. P. Rumelt, "Software piracy: An analysis of protection strategies", *Management Science*, Vol. 37 No. 2, 1991, 125–139.

Cullen, Julie Berry, and Steven D. Levitt, "Crime, Urban Flight, and the Consequences for Cities", *Review of Economics and Statistics*, Vol. 81, No. 2 (May 1999), 159-169.

F. Pouget, M. Dacier, V.H. Pham, "Understanding Threats: a Prerequisite to Enhance Survivability of Computing Systems", *Proceedings of the International Infrastructure Survivability Workshop 2004*, Lisbon, Portugal, December 2004.

Gal-Or, Esther, and Anindya Ghose, "The Economic Incentives for Sharing Security Information", *Information Systems Research*, Vol. 16, No. 2, June 2005, 186–208.

Koo, Hui-wen, and I.P.L. Png, "Private Security: Deterrent or Diversion?" *International Review of Law and Economics*, Vol. 14, March 1994, 87-101.

Jaisingh, Jeevan, and Q. Li, "The optimal time to disclose software vulnerability: Incentive and commitment", Working Paper, Hong Kong University of Science and Technology, November 2005.

Jordan, T. and P. Taylor, "A sociology of hackers", *Sociological Review*, Vol. 46 No. 4, 1998, 757–780.

Kunreuther, Howard, and Geoffrey Heal, "Interdependent Security", *Journal of Risk and Uncertainty*, Vol. 26 Nos. 2-3, March 2003, 231-249.

Microsoft, Windows XP Service Pack 2, http://www.microsoft.com/windowsxp/sp2/default.mspx, Accessed, March 4, 2006.

Moore, David, Colleen Shannon, and J. Brown. "Code-red: a case study on the spread and victims of an internet worm", *Proceedings of the Second ACM SIGCOMM Workshop on Internet Measurement*, 2002, 273-284.

National Cyber Security Alliance, "AOL/NCSA Online Safety Study", October 2004.

National Cyber Security Alliance, "AOL/NCSA Online Safety Study", December 2005.

Nizovtsev, Dmitri, and Marie Thursby, "Economic Analysis of Incentives to Disclose Software Vulnerabilities", Working paper, 2005.

Philipson, Tomas, "Economic Epidemiology and Infectious Diseases" in Joseph Newhouse and Anthony Culyer eds., *The Handbook of Health Economics*, North Holland, 2001.

Register, "Blaster rewrites Windows worm rules", August 13, 2003 http://www.theregister.co.uk/2003/08/14/blaster_rewrites_windows_worm_rules/

Shy, O., J.-F. Thisse "A strategic approach to software protection", Journal of Economics and Management Strategy, Vol. 8, Summer 1999, 163–190.

Symantec, *Internet Security Threat Report: Trends for January 05–June 05*, Volume VIII, September 2005.

Trumbull, William N., "Who has standing in cost-benefit analysis?", *Journal of Policy Analysis and Management*, Vol. 9, 1990, 201–218.

US-CERT (United States Computer Emergency Response Team), "Why is Cyber Security a Problem?" Cyber-Security Tip ST04-001, http://www.us-cert.gov/cas/tips/ST04-001.html, Accessed, March 4, 2006.

Van Beveren, J., "A conceptual model of hacker development and motivation", *Journal of E-Business*, Vol. 1 No. 2, December 2000, 1–9.

Varian, Hal R., "System reliability and free riding", Working Paper, University of California, Berkeley, November 2004.

Whitman, Michael E., "Enemy at the gate: Threats to information security", *Communications of the ACM*, Vol. 46 No. 8, August 2003, 91–95.

Appendix

Proof of Observation 1. Differentiating (5) with respect to *c*,

$$-(v+h)\chi\frac{d^2\alpha}{df^2}\frac{\partial f}{\partial c}=n,$$

and hence, by (1),

$$\frac{\partial f}{\partial c}=\frac{n}{-[v+h]\chi\dfrac{d^2\alpha}{df^2}}<0. \tag{A1}$$

Differentiating (5) with respect to n,

$$-(v+h)\chi\frac{d^2\alpha}{df^2}\frac{\partial f}{dn}=c,$$

and hence, by (1),

$$\frac{\partial f}{\partial n}=-\frac{c}{(v+h)\chi\dfrac{d^2\alpha}{df^2}}<0. \tag{A2}$$

Differentiating (5) with respect to χ,

$$-(v+h)\frac{d\alpha}{df}-(v+h)\chi\frac{d^2\alpha}{df^2}\frac{\partial f}{\partial\chi}=0,$$

and hence, by (1),

$$\frac{\partial f}{\partial\chi}=-\frac{d\alpha/df}{\chi\dfrac{d^2\alpha}{df^2}}>0. \tag{A3}$$

By (2), $d\chi/dk>0$, hence $\partial f/\partial k>0$. If $k=0$, $\chi(Zk)=0$, hence by (5), $f(n\,|\,k=0)=0$, $\forall n\in[0,1]$. Further, if $k\to\infty$, $\chi(Zk)\to 1$, hence, by (5), $\lim_{k\to\infty} f(n)=f_\infty(n)$. [ ]

Proof of Observation 2. We first prove that $B(n)$ is monotone decreasing in n. Consider n_1 and n_2 such that $n_1<n_2$. Let user n_1 choose the fixing effort, $f(n_2)$, associated with user n_2. Since $n_1<n_2$, her expected net benefit would be

$$\begin{aligned} &v-[v+h]\alpha(f(n_2))\chi-p-n_1cf(n_2)\\ &\quad>v-[v+h]\alpha(f(n_2))\chi-p-n_2cf(n_2)\equiv B(n_2\,|k), \end{aligned} \tag{A4}$$

By (4), the fixing effort $f(n_1)$ must provide user n_1 with the maximum expected net benefit, and, in particular,

$$\begin{aligned} B(n_1\,|\,k)&=v-[v+h]\alpha(f(n_1))\chi-p-n_1cf(n_1)\\ &\geq v-[v+h]\alpha(f(n_2))\chi-p-n_1cf(n_2). \end{aligned} \tag{A5}$$

Hence, by (A4) and (A5), $B(n_1|k)>B(n_2|k)$, which is the result.

Since $B(n)$ is monotone decreasing in n, the demand of the software is described as follows. Consider the most sophisticated user, $n = 0$. By (4), her cost of fixing is zero and therefore she will choose the highest level of fixing, i.e., $f(0) \to \infty$. Under the assumption that $v > p$ and by (1), the most sophisticated user would buy since $B(0) = v - p > 0$. Consider the most naïve user, $n = 1$. If $B(1) \geq 0$, then, $B(n) > 0$ for all $n < 1$ and all other users buy the software. However, if $B(1) < 0$, the most naïve user does not buy the software, and there exists some critical level as claimed. [ ]

Proof of Observation 3. Differentiating (6) with respect to c,

$$-[v+h]\chi \frac{d\alpha(f(\hat{n}))}{df}\left[\frac{\partial f(\hat{n})}{\partial c} + \frac{\partial f(\hat{n})}{\partial n}\frac{\partial \hat{n}}{dc}\right] - \hat{n}f(\hat{n}) - cf(\hat{n})\frac{\partial \hat{n}}{dc} - c\hat{n}\left[\frac{\partial f(\hat{n})}{\partial c} + \frac{\partial f(\hat{n})}{\partial n}\frac{\partial \hat{n}}{dc}\right] = 0$$

hence, using (5),

$$\frac{\partial \hat{n}}{\partial c} = -\frac{\hat{n}}{c} < 0, \qquad \text{(A6)}$$

i.e., the marginal user, $\hat{n}$, is decreasing in *c*.

Differentiating (6) with respect to *p*,

$$-[v+h]\chi \frac{d\alpha(f(\hat{n}))}{df}\left[\frac{\partial f(\hat{n})}{\partial p} + \frac{\partial f(\hat{n})}{\partial n}\frac{\partial \hat{n}}{\partial p}\right] - 1 - cf(\hat{n})\frac{\partial \hat{n}}{\partial p} - \hat{n}c\left[\frac{\partial f(\hat{n})}{\partial p} + \frac{\partial f(\hat{n})}{\partial n}\frac{\partial \hat{n}}{\partial p}\right] = 0,$$

hence, using (5),

$$\frac{\partial \hat{n}}{\partial p} = -\frac{1}{cf(\hat{n})} < 0 \qquad \text{(A7)}$$

Differentiating (6) with respect to k,

$$-[v+h]\chi \frac{d\alpha}{df}\left[\frac{\partial f}{\partial k} + \frac{\partial f}{\partial n}\frac{\partial \hat{n}}{\partial k}\right] - [v+h]\alpha(f(\hat{n}))\frac{d\chi}{dk} - \frac{\partial \hat{n}}{\partial k}cf(\hat{n}) - c\hat{n}\left[\frac{\partial f}{\partial k} + \frac{\partial f}{\partial n}\frac{\partial \hat{n}}{\partial k}\right] = 0,$$

hence, using (5),

$$\frac{\partial \hat{n}}{\partial k} = -\frac{[v+h]\alpha(f(\hat{n}))}{cf(\hat{n})}\frac{d\chi(Zk)}{dk} < 0 \qquad \text{(A8)}$$

Further differentiating (A8) with respect to *k*,

$$\frac{\partial^2 \hat{n}}{\partial k^2} = \frac{-[v+h]\alpha(f(\hat{n}))}{cf(\hat{n})}\frac{d^2\chi}{dk^2} - \frac{[v+h]}{cf^2}\frac{d\chi}{dk}\left[\frac{\partial f}{\partial k} + \frac{\partial f}{\partial n}\frac{\partial \hat{n}}{\partial k}\right](f\frac{d\alpha}{df} - \alpha) > 0, \qquad \text{(A9)}$$

which follows from (1), (2), (A2), (A3), and (A8). By (A8) and (A9), $\hat{n}$ is decreasing and convex in k.

If $k \to 0$, then $\chi(Zk) \to 0$. Hence by (4), users' expected net benefit, $B(n) \to v - p - ncf(n)$, which is maximized with $f(n) = 0$. Thus $B(n) \to v - p$, for all *n*. Since $v > p$, all users buy the software. Accordingly, if $k \to 0$, then $\hat{n} \to 1$.

Now, if $k \to \infty$, then $\chi(k) \to 1$, hence, by (4), users' expected net benefit, $B(n) \to v - [v+h]\alpha(f(n)) - p - ncf(n)$. As proved by Observation 2, the most sophisticated user would buy the software, i.e., $B(0 \mid k \to \infty) > 0$. Consider the user with $n = 1$. If her expected net benefit, $B(1) \to v - [v+h]\alpha(f(1)) - p - cf(1) \geq 0$, then by Observation 2, $B(n) > 0$ for all *n*. Hence all users will buy the software. Otherwise, if $B(1) < 0$, then there exists some $\hat{n}_0$ such that

$$B(\hat{n}_0) \to v - [v+h]\alpha(f(\hat{n}_0)) - p - \hat{n}_0 cf(\hat{n}_0) = 0,$$

which completes the proof.

Proof of Observation 4. To simply notation, define

$$\mathrm{A}(k) \equiv \int_0^{\hat{n}(k)} \alpha(f(m \mid k))\, d\Phi(m). \tag{A10}$$

Since $d\alpha/df < 0$, then $\partial A/\partial f < 0$. Further $\partial \mathrm{A}/\partial \hat{n} > 0$. Substituting (A10) in (9), and then differentiating with respect to η,

$$eA\left[-\frac{d\chi(Zk)}{dk} + [1-\eta]\frac{d^2\chi(Zk)}{dk^2}\frac{\partial k}{\partial \eta}\right] = \frac{d^2 c_K}{dk^2}\frac{\partial k}{\partial \eta}$$

which simplifies to

$$\frac{\partial k}{\partial \eta} = \frac{e\dfrac{d\chi}{dk}A}{e[1-\eta]A\dfrac{d^2\chi}{dk^2} - \dfrac{d^2 c_K}{dk^2}} < 0. \tag{A11}$$

Similarly, differentiating (9) with respect to $\hat{n}$,

$$e(1-\eta)\frac{\partial \mathrm{A}}{\partial \hat{n}}\frac{d\chi}{dk} + e(1-\eta)\mathrm{A}(\hat{n})\frac{d^2\chi}{dk^2}\frac{\partial k}{\partial \hat{n}} = \frac{d^2 c_K}{dk^2}\frac{\partial k}{\partial \hat{n}},$$

which simplifies to

$$\frac{\partial k}{\partial \hat{n}} = \frac{e(1-\eta)\dfrac{\partial \mathrm{A}}{\partial \hat{n}}\dfrac{d\chi}{dk}}{\dfrac{d^2 c_K}{dk^2} - e(1-\eta)\mathrm{A}(\hat{n})\dfrac{d^2\chi}{dk^2}} > 0. \tag{A12}$$

When $\hat{n} = 0$, no one buys the software, it doesn't pay for the hacker to attack the software, hence $k = 0$. When $\hat{n} = 1$, all users buy the software. Since the hacker's expected net benefit, (8), is concave in k, there exists k_1 that satisfies the first order condition, (9), and maximizes the expected net benefit.

Similarly, we can show that

$$\frac{\partial k}{\partial f} = \frac{e(1-\eta)\dfrac{\partial \mathrm{A}}{\partial f}\dfrac{d\chi}{dk}}{\dfrac{d^2 c_K}{dk^2} - e(1-\eta)\mathrm{A}(\hat{n})\dfrac{d^2\chi}{dk^2}} < 0, \qquad \text{(A13)}$$

and that there exists some $k_0 > 0$ such that if $f = 0$, then $k = k_0$, and there exists some $k_\infty > 0$ such that if $f \to \infty$, then $k = k_\infty$.

Proof of Lemma 1. By Observations 1 and 3 respectively, f is increasing in k and $\hat{n}$ is decreasing in k. Accordingly, $A(k)$ is monotonically decreasing in k, regardless of the user distribution $\Phi(n)$. Further, if $k = 0$, then by (2), $\chi = 0$, hence all users would choose $f(n) = 0$ and, by (4), get $B(n \mid \chi) = v - p$. By assumption, $v - p > 0$, hence, if $k = 0$, $\hat{n} = 1$, and so, $A > 0$.

With regard to hacker effort, by Observation 4, k is monotonically increasing in A. Further, if $A = 0$ (because either $\hat{n} = 0$ or $f(n) = 0$, for all n), then the hacker will not expend any effort to attack the software, $k = 0$.

Figure 3 depicts $k(\mathrm{A})$ and $\mathrm{A}(k)$, which describe the best response functions of the hacker and users, respectively. Since the functions are continuous, they have a non-trivial intersection, say (k^*, A^*).

Given hacker effort k^*, let $\hat{n}(k^*)$ and $f(n \mid k^*)$ be the marginal user and the user fixing effort respectively. Then, by (10), the conditional vulnerability

$$A' \equiv \int_0^{\hat{n}(k^*)} \alpha(f(n \mid k^*))d\Phi(n).$$

Now, we claim that $A^* = A'$, and prove the claim by contradiction as follows.

(i) Suppose otherwise that $A' > A^*$. Then, referring to Figure 3, the function $k(\mathrm{A})$ gives the hacker's best-response effort k'. Since $k(\mathrm{A})$ is monotonically increasing in A, we have $k' > k^*$. Since $\hat{n}$ is decreasing in k and $f(.)$ is increasing in k, it follows that $\hat{n}(k') < \hat{n}(k^*)$ and $f(n \mid k') > f(n \mid k^*)$, which implies that $A' < A^*$, which contradicts the original assumption.

(ii) Suppose otherwise that $A' < A^*$. Then, referring to Figure 3, the function $k(\mathrm{A})$ gives the hacker's best-response effort k'. Since $k(\mathrm{A})$ is monotonically increasing in A, we have $k' < k^*$. Since $\hat{n}$ is decreasing in k and $f(.)$ is increasing in k, it follows that $\hat{n}(k') > \hat{n}(k^*)$ and $f(n \mid k') < f(n \mid k^*)$, which implies that $A' > A^*$, which contradicts the original assumption.

Therefore, we must have $A^* = A'$, and there exists a non-trivial equilibrium comprising k^*, $\hat{n}(k^*)$ and $f(\hat{n}(k^*)\,|\,k^*)$. [ ]

Proof of Proposition 1. Expand (12) to distinguish between the fixing effort of end-user n' denoted $f(n')$ and the efforts of all other users, f,

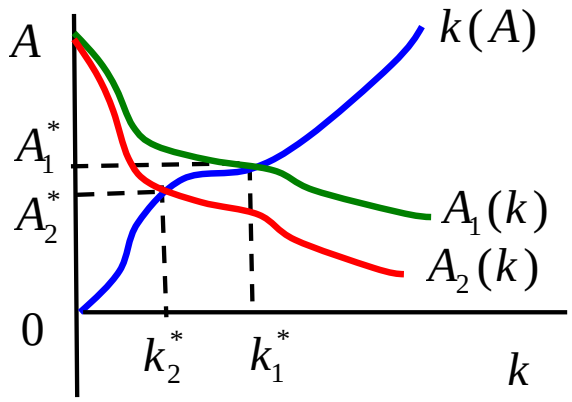
$$e[1-\eta]\frac{d\chi}{dk_i}\left[\int_{[0,n')}\alpha(f(n))d\Phi(n)+\alpha(f(n'))+\int_{(n',\hat{n}]}\alpha(f(n))d\Phi(n)\right]=\frac{dc_K}{dk_i}. \qquad \text{(A14)}$$

By (A14), an increase in fixing effort, f, by all other users except n' would reduce the term in brackets, and hence induce the hacker to reduce their effort, $\Delta k < 0$. This would imply $\Delta\chi < 0$, which in (5), shifts down the left-hand side. Therefore, user n' would reduce $f(n')$. [ ]

Proof of Proposition 2. This follows directly from the proof of Table 2, by noting that (A16) will hold, and hence $\partial A/\partial c \geq 0$, if c is sufficiently high, and not hold if c is sufficiently low.

Proof of Table 2

Figure A. Increase in price, *p*



User fixing cost, c

By Observations 1 and 4, an increase in the user fixing cost, c, directly leads users to reduce their fixing effort, f, and the software demand, $\hat{n}$. By (10), these have conflicting effects on the users' best-response function $A(k)$. By (9), the increase in the user fixing cost has no direct effect on $k(A)$. Accordingly, the net effect on hacking effort, k, and conditional vulnerability, A, depends on the sign of $\partial A/\partial c$.

Differentiating (10) with respect to c,

$$\frac{\partial A(c\,|\,k)}{\partial c}=\alpha(f(\hat{n}))\frac{\partial\hat{n}}{\partial c}\frac{d\Phi(\hat{n})}{dn}+\int_0^{\hat{n}}\frac{d\alpha}{df}\frac{\partial f(n)}{\partial c}d\Phi(n) \qquad \text{(A15)}$$

Substituting from (5), (A1), and (A6) in (A15), it follows that $\partial A/\partial c > 0$ if and only if

$$-\frac{1}{[v+h]\chi}\int_0^{\hat{n}} n\frac{d\alpha}{df}\frac{df}{d^2\alpha/df^2}d\Phi(n) \geq \frac{\hat{n}\alpha(f(\hat{n}))}{c}\frac{d\Phi(\hat{n})}{dn}. \quad \text{(A16)}$$

We analyze two cases below.

(i) $\partial A/\partial c \geq 0$. Referring to Figure A, an increase in c would lead to a new equilibrium, with higher hacking effort, $k_1^* \leq k_2^*$, higher conditional vulnerability, $A_1^* \leq A_2^*$, and hence higher effective vulnerability, $\chi(k_1^*)A_1^* \leq \chi(k_2^*)A_2^*$.

With regard to the marginal user, i.e., software demand,

$$\frac{d\hat{n}}{dc} = \frac{\partial\hat{n}}{\partial c} + \frac{\partial\hat{n}}{\partial k}\frac{dk}{dc}. \quad \text{(A17)}$$

By Observation 3, $\partial\hat{n}/\partial c < 0$ and $\partial\hat{n}/\partial k < 0$, while from above, $dk/dc > 0$. Hence, substituting in (A17), we have $d\hat{n}/dc < 0$.

Regarding the fixing effort, from above, $A_1^* \leq A_2^*$, hence

$$\frac{dA}{dc} = \alpha(f(\hat{n}))\frac{d\hat{n}}{dc}\frac{d\Phi(\hat{n})}{dn} + \int_0^{\hat{n}}\frac{d\alpha}{df}\frac{df(n)}{dc}d\Phi(n) \geq 0. \quad \text{(A18)}$$

Now, $d\hat{n}/dc < 0$, hence, substituting in (A18), it follows that $df/dc < 0$.

(ii) $\partial A/\partial c < 0$. Referring to Figure A, an increase in c would lead to a new equilibrium, with lower hacking effort, $k_1^* > k_2^*$, lower conditional vulnerability, $A_1^* > A_2^*$, and hence lower effective vulnerability, $\chi(k_1^*)A_1^* > \chi(k_2^*)A_2^*$.

With regard to fixing effort,

$$\frac{df}{dc} = \frac{\partial f}{\partial c} + \frac{\partial f}{\partial k}\frac{dk}{dc}. \quad \text{(A19)}$$

By Observation 1, $\partial f/\partial c < 0$ and $\partial f/\partial k > 0$, while from above, $dk/dc < 0$. Hence, substituting in (A19), we have $df/dc < 0$.

Regarding the marginal user, from above, $A_1^* > A_2^*$, hence

$$\frac{dA}{dc} = \alpha(f(\hat{n}))\frac{d\hat{n}}{dc}\frac{d\Phi(\hat{n})}{dn} + \int_0^{\hat{n}}\frac{d\alpha}{df}\frac{df(n)}{dc}d\Phi(n) < 0. \quad \text{(A20)}$$

Now, $df/dc < 0$, hence, substituting in (A20), it follows that $d\hat{n}/dc < 0$.

Enforcement rate, η, and hacking cost, $c_K(.)$

First, consider the effect of an increase in enforcement, η. By Observations 1 and 3, the increase in enforcement has no direct effect on the users' fixing effort or demand $\hat{n}$. Hence, by (10), the best-response function $A(k)$ remains unchanged. By Observation 4, the

enforcement increase directly leads hackers to reduce effort, hence their best-response function, $k(A)$, shifts to the left. Accordingly, in the new equilibrium, hacking effort is lower, $k_1^* > k_2^*$, and the conditional vulnerability is higher, $A_1^* < A_2^*$.

Since the increase in enforcement results in lower hacker effort, k, hence lower hacker effectiveness, $\chi(k)$, but higher conditional vulnerability, A, the impact on the effective user vulnerability, χA, depends on the balance of the effects on hackers and users.

With regard to fixing effort,

$$\frac{df}{d\eta} = \frac{\partial f}{\partial \eta} + \frac{\partial f}{\partial k}\frac{dk}{d\eta}. \qquad \text{(A21)}$$

By (5), $\partial f / \partial \eta = 0$, by Observation 1, $\partial f / \partial k > 0$, while from above, $dk / d\eta < 0$. Hence, substituting in (A21), we have $df / d\eta < 0$.

Similarly, with regard to the marginal user, i.e., software demand,

$$\frac{d\hat{n}}{d\eta} = \frac{\partial \hat{n}}{\partial \eta} + \frac{\partial \hat{n}}{\partial k}\frac{dk}{d\eta}. \qquad \text{(A22)}$$

By (6), $\partial \hat{n} / \partial \eta = 0$, by Observation 3, $\partial \hat{n} / \partial k < 0$, while from above, $dk / d\eta < 0$. Hence, substituting in (A22), we have $d\hat{n} / d\eta > 0$, which completes the proof.

The effect of an increase in the hacking cost is similar. For brevity, we omit the proof.

Price, p

By Observation 1, a price increase has no direct effect on the user's fixing effort, while, by Observation 3, the price increase directly reduces the demand, $\hat{n}$. Accordingly, by (10), for $k > 0$, the best-response function $A(k)$ shifts downward, while, by (10), for $k = 0$, $A(0)$ does not change with p. By (9), the price increase has no direct effect on $k(A)$.

Figure A depicts the new equilibrium: the users' best-response function shifts from $A_1(k)$ downward to $A_2(k)$, while the hackers' best-response function remains unchanged. In the new equilibrium, hacking effort is lower, $k_1^* > k_2^*$, and the conditional vulnerability is lower, $A_1^* > A_2^*$.

Given that the increase in price, p, leads to lower hacking effort, k, it would, by (2) result in lower hacker effectiveness, χ. Thus, the effective user vulnerability, χA, decreases with price, p.

With regard to fixing effort,

$$\frac{df}{dp} = \frac{\partial f}{\partial p} + \frac{\partial f}{\partial k}\frac{dk}{dp}. \qquad \text{(A23)}$$

By (5) $\partial f / \partial p = 0$, by Observation 1, $\partial f / \partial k > 0$, while from above, $dk / dp < 0$. Hence, substituting in (A23), we have $df / dp < 0$.

Regarding the marginal user, from above, note that

$$\frac{dA}{dp} = \frac{d\int_0^{\hat{n}} \alpha\big(f(n)\big)\, d\Phi(n)}{dp} = \alpha(f(\hat{n}))\frac{d\hat{n}}{dp}\frac{d\Phi(\hat{n})}{dn} + \int_0^{\hat{n}} \frac{d\alpha}{df}\frac{df(n)}{dp}\, d\Phi(n) < 0. \quad \text{(A24)}$$

Now, $df / dp < 0$, hence

$$\int_0^{\hat{n}} \frac{d\alpha}{df}\frac{df(n)}{dp}\, d\Phi(n) > 0.$$

Substituting in (A24), it follows that $d\hat{n} / dp < 0$, which completes the proof. [ ]