MIS Quarterly

SPECIAL ISSUE

THE IMPACT OF MALICIOUS AGENTS ON THE ENTERPRISE SOFTWARE INDUSTRY[1]

By: **Michael R. Galbreth**
Department of Management Science
Moore School of Business
University of South Carolina
Columbia, SC 29208
U.S.A.
galbreth@moore.sc.edu

Mikhael Shor
Department of Economics
Owen Graduate School of Management
Vanderbilt University
Nashville, TN 37240
U.S.A.
mike.shor@owen.vanderbilt.edu

Abstract

In this paper, a competitive software market that includes horizontal and quality differentiation, as well as a negative network effect driven by the presence of malicious agents, is modeled. Software products with larger installed bases, and therefore more potential computers to attack, present more appealing targets for malicious agents. One finding is that software firms may profit from increased malicious activity. Software products in a more competitive market are less likely to invest in security, while monopolistic or niche products are likely to be more secure from malicious attack. The results provide insights for IS managers considering enterprise software adoption.

Keywords: Information system security, network externalities, software selection, game theory

Introduction

While the emergence of the World Wide Web has enabled unprecedented access to information, it has also created unprecedented opportunities to attack information assets. By breaching the security of enterprise systems, malicious agents can cause significant financial loss and other negative consequences. It seems reasonable to assume, then, that products with lower security against such attacks would command lower prices. This may provide incentives for software firms to minimize their products' vulnerability to attack. In this paper, we examine this assumption using a model of competition in the presence of malicious agents.

Software products with larger installed bases, and therefore more potential computers to attack, present more appealing targets for malicious agents. Attackers modify their actions based on those of their targets (Cavusoglu and Raghunathan 2004; Cremonini and Nizovtsez 2006). We incorporate the notion that adoption of a product, by increasing the product's market share, attracts more attackers. We find that, while increased vulnerability to malicious attack does often reduce the profits of software firms, this need not always be the case in a competitive environment. For an IS manager, our model provides a new perspective on the impact of malicious agents on the enterprise software industry.

[1] Peter Gutmann was the accepting senior editor for this paper. Lech Janczewski served as the associate editor.

The appendix for this paper is located in the "Online Supplements" section of the *MIS Quarterly*'s website (http://www.misq.org).

While the focus of this paper is on enterprise software, examples of malicious attacks on more familiar consumer software products can provide useful intuition for the relationship between market share and security. Consider Web browsers and the growing popularity of the Mozilla Firefox product. Taking market share from Windows Internet Explorer, Firefox has grown from a 3.5 percent market share in June 2004 (Evers 2004) to about 23 percent in July 2009 (Mossberg 2009), due in part to its perceived lower susceptibility to malicious software programs.[2] Among the small to medium-sized business market, Firefox has nearly 40 percent market share (Cherian 2007). Yet, the growth in the popularity of Firefox has led to an increase in malicious attacks directed at it (DeFelice 2006; Woo et al. 2006). This is expected given the observation by Woo et al. (2006, p. 173) that

> for web browsers with a lower percentage of the market share, such as Mozilla and Safari, the total number of vulnerabilities found is low. This does not mean that these web browsers are more secure, but merely that only a limited effort has gone into finding their vulnerabilities.

A similar explanation is provided for the lower number of discovered vulnerabilities for HTTP server products with lower market shares (Alhazmi and Malaiya 2006). A similar pattern of malicious agents following market share can be observed in PC operating systems, where Microsoft's domination has made it "the hacker target of choice" (Berghel 2003). Users of Microsoft's Windows operating system report far more virus detections than users of Apple's Mac OS X, which has a much smaller market share (Consumer Reports 2005). However, as Apple computers have surged in popularity in recent years, malicious software programs targeted at Mac OS X have become much more common (Wingfield 2006). As recently stated by an industry observer, "Popularity, it turns out, is perhaps the most important security factor in today's changing hacker world" (Maxcer 2007).

The examples of Firefox and Apple are well-known due to the ubiquity of PC operating systems and Web browsers. However, the same concept of malicious agents following market share applies to the larger domain of enterprise software, which represents a majority of the software applications market in terms of revenue (Datamonitor 2005). While analogous, the enterprise software market does differ from PC applications in several ways. First, data security is likely to be a primary consideration in deciding between competing enterprise products. Compromised enterprise-level data (e.g., about consumers, investors, suppliers) can lead to enormous financial loss and even civil and criminal action. Second, while certain PC applications exhibit positive network externalities (Brynjolfsson and Kemerer 1996), this is not always the case for enterprise IT adoption. In an enterprise context, network considerations are mostly limited to compatibility with existing intra-firm systems or specific trading partners. These are not impacted by changes in the overall market share of the package (Tam and Hui 2001). In fact, positive externalities have been empirically shown to be insignificant in some IT adoption settings (Tam and Hui 2001). Meanwhile, when malicious agents favor products with a larger installed base, this creates a negative externality from product adoption. The balance of positive and negative externalities for one national firm was described to an author by its chief technology officer when the firm chose to abandon a popular enterprise software product in favor of a much less popular one: "Yes, the [big product] comes with better support, technical info, third-party [applications], and certified IT is easier to find, but everything we get, an army of hackers and script-kiddies gets, too" (conversation with author). The implication is that the probability of a successful malicious attack on a software product is not completely captured by the security of the product, but that the negative externality caused by malicious agents' preference for discovering and attacking vulnerabilities in products with larger installed bases must be considered as well.

While attacks on information assets have been the subject of research for some time (Loch et al. 1992), the relationship between market share and the incentives of malicious agents has received little academic attention and is often overlooked in practice.[3] This represents an important area for investigation since, as pointed out by Straub (1990), the consequences of ignoring a means to prevent security breaches can be quite serious. The high cost of security breaches suggests that, although some positive externalities might exist, the overall externality in enterprise software might be negative in some cases. In fact, the data bear this out in at least one market segment: the ordering of high severity level vulnerabilities in major database applications discovered in 2007 *precisely* follows market share (SANS 2007). We explicitly

[2] Many Web users are concerned about privacy while online (Dinev and Hart 2006; Linn 2005), and security problems with Internet Explorer are well-documented: the browser had 39 published vulnerabilities in 2002 alone (Rescorla 2005).

[3] For example, Walker et al. (2005) suggest that complete standardization of U.S. health care information systems could enable savings of billions of dollars per year. Their calculations ignore, however, potential damages given the significant incentive to attack the system and access a large amount of private medical information.

capture this link between market share and software security by including a negative overall externality in our model.

Our model links an important component of the software selection process—the likelihood of malicious attack—to the market environment faced by software manufacturers. When more popular products are favored by malicious agents, product adoption creates a negative network effect for other users of the product. Negative network effects have been shown to create pricing power and soften competition between firms (Scotchmer 1985; Tiebout 1956). Our model allows for the fact that software firms can manage the strength of this negative externality by altering the security of their products. More commonly, firms purse pricing power through product differentiation (S. P. Anderson 2008). We find that competing software firms that are highly differentiated have a greater incentive to increase the security of their products than firms in more competitive environments. We demonstrate this result in the context of both horizontal and vertical differentiation.

Our model of software competition provides new insights for IS managers. For example, we define conditions under which the presence of malicious agents results in a functionally superior technology not completely capturing a market that it otherwise would. A firm with inferior technology prefers the existence of malicious agents, since this enables it to operate profitably by serving a small market that, given its small size, is unattractive to attack. We also show, perhaps in contradiction to traditional thinking regarding enterprise software, that software manufacturers engaged in fierce competition with rivals *prefer* some malicious activity as it results in increased profits for one or both firms. In these cases, software firms have a disincentive to reduce the incidence of malicious attacks. For the IS manager faced with a software selection decision, our results indicate that the nature of competition in a specific software market can provide insights into the software vendors' incentives to improve the security of their products.

Our paper is organized as follows. In the next section, we provide an overview of malicious agents and describe our approach to modeling the enterprise software selection process. In the following two sections, we develop the model in detail, assuming exogenous security choice initially, and examine the impact of malicious agents on enterprise software selection. Next, we provide results for the case of endogenous security choice, concentrating on software products that are horizontally differentiated. The "Generalizations" section formally considers vertical differentiation and relaxes several model assumptions. Finally, the contribution and insights of the model are discussed in the "Conclusions."

Malicious Agents: Motivations and Consequences

The primary motivation of malicious agents attacking information systems has changed over the years. While many early attackers were motivated by pride or prestige, there is a significant trend toward attacks with financial, political, or military goals (Cremonini and Nizovtsez 2006; Grow and Bush 2005; McHugh et al. 2000; Sullivan 2006;Wingfield 2006;Yuan 2006). These attacks have a considerable negative impact on the market value of the targeted firms (Cavusoglu, Mishra, and Raghunathan 2004). Recent research has addressed this growing security threat in a variety of ways, including examinations of security technology investment (S. P. Anderson 2008; Cavusoglu, Mishra, and Raghunathan 2005; Gordon and Loeb 2002), inter-firm information sharing (Gal-Or and Ghose 2005), vulnerability disclosure (Cavusoglu, Cavusoglu, and Raghunathan 2007), and patch releases (Arora, Caulkins, and Telang 2006; Arora et al. 2004; Arora, Telang, and Xu 2008; August and Tunca 2006, 2008; Cavusoglu, Cavusoglu, and Zhang 2008). These studies have made important contributions to the state of knowledge regarding the threat of malicious attacks on information assets, but all assume that the complete elimination of malicious activity would benefit both software firms and their consumers. As shown analytically in the following sections, this assumption may not be valid in all competitive environments.

The software security firm Symantec notes that "attackers continuously look for easy targets, those that will provide them with the maximum return on the time they invest in writing malicious code" (2005, p. 55). Empirical observations suggest rational behavior on the part of malicious agents, as their efforts are targeted at products with lower security (Cremonini and Nizovtsez 2006) and higher market share (Woo et al. 2006). These effects can be cumulative, as market share attracts attackers, who discover vulnerabilities, which attract more attackers. Perhaps a useful analogy can be drawn to security in an old-fashioned environment. Homeowners purchase safes to provide security against thieves. It is certainly not unreasonable to imagine that professional thieves practice opening safes to gain proficiency. Which safe would a thief attempt to master? He maximizes the value of his investment in safe-cracking skills by identifying vulnerabilities in the most popular models. Of course, this may result in the models with the greatest security not actually being the best at safeguarding valuables; adoption imposes a negative externality on other users of the product. This can create perverse incentives, the most intuitive being that makers of less popular models might prefer malicious activity as it reduces the competitive advantage of market leaders.

The example of safes highlights logic equally applicable to the case of software, where malicious activity has a complex impact on market dynamics. Most studies of adoption of competing technologies focus on positive network effects, building on the fundamental models of Farrell and Saloner (1985) and Katz and Shapiro (1985). In contrast, we focus on cases where, given the presence of malicious agents, the overall network effect is negative. Other work that has modeled negative externalities has generally addressed congestion issues (MacKie-Mason and Varian 1994; Varian 2004), membership in communities or clubs (Scotchmer 1985; Tiebout 1956), or two-sided markets with buyers and sellers (Galbreth et al. 2005; Parker and Van Alstyne 2005; Riggins et al. 1994; Wang and Seidmann 1995). Several papers have investigated pricing in the presence of network externalities (Hackner and Nyberg 1996; Lee and Mason 2001; Van Dender 2002), but these papers assume no differentiation between consumers.

Negative network effects have been modeled in information technology contexts.[4] For example, Asvanund et al. (2004) show that the size of a peer-to-peer network is limited by congestion costs, a form of a negative externality. MacKie-Mason and Varian (1994) also examine congestible Web resources provided either by a monopolist or under perfect competition. Nadaminti et al. (2002) and Westland (1992) examine negative network effects of intrafirm product adoption. Choi et al. (2005) propose a model of a single software firm that chooses price, investment in security, and disclosure of discovered vulnerabilities. Similar to our model, they explicitly consider the fact that larger networks are more likely to be the target of malicious activity. However, they examine only the case of a monopolist. August and Tunca (2006) present a model where consumers choose whether or not to buy given a fixed price (again, in a monopolistic setting), then choose whether or not to patch known vulnerabilities, and finally are subject to malicious attacks. Our work differs from this previous work on information system security by examining the case where competing firms choose price and vulnerability, and attackers consider both vulnerability *and* the size of the user base when targeting users. As opposed to explicitly modeling patch application, we interpret the firm's selection of vulnerability as a proxy for all costly activities to improve security, although we comment on patch application in our conclusions.

Beyond inherent security, competing software products often differ in the feature sets and user experiences they offer. Competing software products might be differentiated in the minds of consumers in two ways. First, quality differentiation implies that one product is inherently superior to the other due to factors such as stability or ease of learning. All consumers prefer one product, although they may vary in the strength of this preference (see, for example, Shaked and Sutton 1982). Second, horizontal differentiation implies that consumers differ in their preferences for the products based upon how closely a given product matches their particular needs. Generally, products contain both quality differentiated and horizontally differentiated attributes.[5] For example, a software product's stability and level of support are quality differentiated; a product that crashes less frequently than a competitor is more desirable to *all* consumers. Conversely, a product's feature set and compatibility with existing systems might be desirable to some subset of consumers, and thus is horizontally differentiated. Both types of differentiation are important to fully reflect the software selection process. In the next section, we incorporate quality differentiation into a model of horizontal differentiation. Later, in the "Generalizations" section, we show that the similar insights are obtained for a model of vertical differentiation.

Sahay and Gupta (2003) provide a detailed discussion of the primary drivers of the selection of supply chain software. They discuss the important role of both general requirements (e.g., cost, support) and company-specific requirements (e.g., critical modules, portability, integration) in the software selection process. Our model similarly breaks product differentiation into general components (quality) and company-specific ones (horizontal differentiation). For ERP software selection, van Everdingen et al. (2000) find the fit with current systems to be the most important decision criterion. They also find that general requirements such as cost and support play a role in the selection process, again confirming the value of our inclusion of relative quality parameters in addition to horizontal differentiation. Other papers also note that the software selection process involves the consideration of general factors such as price and support as well as the fit between the software and the company's unique needs (Umble et al. 2003). The calibration of such models to actual consumer tastes and purchase patterns is an active area of research in marketing, incorporating both econometric and psychometric techniques (Berry et al. 1995; Hauser and Rao 2004; McFadden 1986).

[4] We refer the reader to Li (2004) for a good conceptual discussion of negative externalities in IT adoption.

[5] We draw a distinction between vertical differentiation, where consumers have heterogeneous tastes for quality, and quality differentiation, in which all consumers agree on the value of quality.

We complement existing approaches that model incentives to invest in security. These approaches generally relate suboptimal security to inadequate consumer information and the resulting disincentive for firms to internalize the costs of security breaches. Consumers cannot always discern *a priori* the security of a product (Blakley 2002). Thus, the software market is akin to Akerlof's (1970) market for lemons, where a more secure product need not imply a higher price in the marketplace. As greater security does not raise profits, firms have no incentives to provide it (Anderson et al. 2007). Coupled with the importance of lock-in and network effects, this leads to fierce price competition among software vendors. Vendors will wait until their dominant market position is attained, and then turn their attention toward security (R. Anderson 2008). We argue that this is not the whole story. Our model shows that resolving information asymmetry does not necessarily produce an incentive to invest in security. In our model, consumers fully incorporate the expected loss due to security failures into their purchase decisions. All else equal, higher vulnerability decreases aggregate consumer willingness to pay. Firms nevertheless have inadequate incentive to secure their products. We find that products in less competitive markets (either global monopolies or local, niche monopolies) are more likely to pursue a lower overall vulnerability to attack than products in more competitive environments. Thus, the nature of competition in the software market should be a key consideration in enterprise software selection.

Model

Preliminaries

We consider competition between two firms, indexed by j in $\{1,2\}$, offering products that might be quality differentiated and/or horizontally differentiated in the minds of consumers. The average quality of each product in the minds of consumers is represented as v_j, with $v_1 > v_2 > 0$.[6] The difference between firm qualities, $v_1 - v_2$, reflects the level of quality differentiation. Horizontal differentiation is modeled using the standard approach, first proposed by Hotelling, of locating the firms at the ends of the unit line, with Firm 1 at location 0 and Firm 2 at location 1. A continuum of risk-neutral consumers is located uniformly along the unit line with total density of 1. The use of other distributions would make the problem much less tractable without changing the qualitative results. Note, however, that our model captures nonsymmetric environments, which would have a majority (as opposed to exactly half) of consumers preferring one product to the other, via v_1 and v_2. A consumer pays a transportation cost (or suffers a disutility) of $t > 0$ per unit "travelled" to a firm. Thus, t represents the degree of horizontal differentiation, and a consumer located at α suffers a disutility of $t\alpha$ if purchasing from Firm 1 and $t(1 - \alpha)$ if purchasing from Firm 2.

The utility from adopting one of the products for a consumer located at is given by

$$u_1(\alpha) = v_1 - t\alpha - p_1 - q_1(n_1)L \qquad \text{if from Firm 1} \tag{1}$$

$$u_2(\alpha) = v_2 - t(1 - \alpha) -p_2 - q_2(n_2)L \qquad \text{if from Firm 2} \tag{2}$$

where p_j is the price charged by firm j and $q_j(\cdot)$ is a user's nondecreasing probability of a successful attack by malicious agents given Firm j's measure of consumers is n_j. Unlike previous studies that have assumed a constant probability of attack (Gordon and Loeb 2002; Soo Hoo 2000), in our model this probability is a function of market share. Multiple prices might be offered in practice to different consumer segments (e.g., nonprofit versus for-profit). In our model we use a single price for ease of exposition. If multiple pricing segments exist, our model is applicable to any given segment when considered independently. Please see the "Generalizations" section for a discussion of multiple-price settings where it is unrealistic to consider segments independently. We normalize the utility from no purchase, $u_0(\alpha) = 0$. The parameter L is the expected loss caused by a successful attack and could quantify a wide variety of damages in addition to straightforward theft of cash, including compromised customer credit card information, loss of reputation, strategic losses to competitors, denial of service, etc. (Gordon and Loeb 2002). A single L to capture the loss from a malicious attack has been assumed in other models of information security (Gordon and Loeb 2002; Soo Hoo 2000), although in a later section we consider the impact that heterogeneity in L would have on the insights provided by the model. Thus, the final term in each utility function is the probability of a successful attack (which depends on market share) multiplied by the loss incurred. Firms produce at constant marginal costs which are, without loss of generality, normalized to zero. Firm profits are given by $\pi_j = p_j n_j$.

[6] If consumers are currently using an alternate technology or perhaps have the option to develop technologies in-house, then this can be interpreted as follows: the current technology has a value v_0. Each considers adopting one of two competing technologies that provide higher values than the current product ($v_1 > v_2 > v_0$). Without loss of generality, we normalize $v_0 \equiv 0$, effectively redefining $v_j^{'} = v_j - v_0$ as the relative additional value from adopting the product of Firm 1 or Firm 2.

The goal of this study is to provide insights for the case where both the prices and the security levels of the software products are chosen by each competing firm. Although our primary interest is in this case where security levels are endogenous, in the interest of expositional clarity, we assume initially that the probabilities of successful attack $q_j(\cdot)$ for all software products are identical, fixed, and known; that is, there is a single industry-wide $q(\cdot)$ and only price is directly under managerial control. Starting with this simplified model enables us to describe the basic model intuition and insights in a more manageable context. Later in the paper, we address the more interesting problem, where the choice of security level is endogenous, and show how the intuition and key insights from the simplified model extend to this context.

Since our focus is on the pricing and adoption of software, we do not explicitly model the incentives of the malicious agents here, and only assume that the probability of being attacked is linear in the size of the consumer base: $q(n_j) \equiv qn_j$, $q \leq 1$. Thus, the probability of an attack occurring is linear in market share, and q captures the *vulnerability* of the product, or the chance that an attack, once initiated, succeeds. The assumption that probability of attack is linear in market share has been effective in predicting the life-cycle of software vulnerabilities (Alhazmi and Malaiya 2005), and it is reasonable in a variety of situations, including a mercenary who is compensated per confidential record (e.g., credit card number) obtained, or a pride-motivated hacker who considers the visibility of her attack to be proportional to the number of computers she penetrates. In the appendix, we show that our main results are preserved for nonlinear functions, as well.[7]

Consider first a market without malicious agents, so that $q(\cdot) \equiv 0$. If t is sufficiently low, specifically when $t < v_1 - v_2$, all consumers prefer product 1 to product 2. If $t > v_1 - v_2$, then there exist at least some consumers who prefer the inherently inferior product 2 due to their particular needs: for example, a consumer located at $\alpha = 1$ values product 2 the amount v_2, which exceeds $v_1 - t$, the value of product 1. When malicious agents are present, the environment exhibits negative externalities from consumption. Consumers who purchase a technology increase its market size and thus increase the chance of attack.

The timing of this game is as follows. In the first period, firms simultaneously set prices for their two products (p_1 and p_2). In the second period, consumers simultaneously make their purchase decisions from among the available technologies {0,1,2} where 0 implies neither product. Each consumer purchases at most one product, although may elect not to purchase if neither product offers nonnegative utility. The resulting market sizes for each product are n_1 and n_2. In the third period, malicious agents decide on the consumers to attack. We solve for a subgame-perfect equilibrium of the game, considering first the consumer adoption decision and then the price competition among firms.

Equilibrium

The adoption decision of a consumer depends on the expected market size of each product. Denote consumers' expectations about likely market sizes by n_1^e and n_2^e. We define

$$\alpha_{12}^* = \tfrac{1}{2} + \tfrac{1}{2t}[(v_1 - v_2) - (p_1 - p_2) - q(n_1^e - n_2^e)L] \quad (3)$$

as the location of the consumer indifferent between Firm 1 and Firm 2. Similarly, we define the locations at which a consumer is indifferent between each technology and making no purchase[8]

$$\alpha_{10}^* = \tfrac{1}{t}(v_1 - p_1 - qLn_1^e) \quad (4)$$

$$\alpha_{20}^* = 1 - \tfrac{1}{t}(v_2 - p_2 - qLn_2^e) \quad (5)$$

Since a purchase implies that a consumer prefers the purchased product both to the other offering and to purchasing nothing, market sizes are given by

$$n_1 = \max(0, \min(\alpha_{12}^*, \alpha_{10}^*, 1)) \quad (6)$$

$$n_2 = \max(0, \min(1 - \alpha_{12}^*, 1 - \alpha_{20}^*, 1)) \quad (7)$$

In equilibrium, we have $n_1 = n_1^e$ and $n_2 = n_2^e$. That is, expectations must be realized. Using this, we can identify three possible market structures in the consumer adoption stage

[7] If the number of agents targeting a specific software product and the rate at which vulnerabilities are discovered both grow linearly in a product's market share, then the probability of a successful attack against a given consumer is also linear in share. A quadratic function, $q(n_j) \equiv q\beta n_j + q(1-\beta)n_j^2, \beta \in [0,1]$, provides similar insights (Corollary to Theorem 3 in the appendix).

[8] These conditions are derived from consumers' incentive compatibility (IC) and individual rationality (IR) constraints. To purchase from Firm 1, for example, these correspond to

$$u_1(\alpha) \geq u_2(\alpha) \Leftrightarrow v_1 - t\alpha - p_1 - qLn_1^e \geq v_2 - t(1-\alpha) - p_2 - qLn_2^e \quad \text{(IC)}$$

$$u_1(\alpha) \geq u_0(\alpha) \Leftrightarrow v_1 - t\alpha - p_1 - qLn_1^e \geq 0 \quad \text{(IR)}$$

Proposition 1. *In equilibrium, $n_1 > 0$ and*

$$n_1 + n_2 = 1, \quad n_2 = 0 \quad \text{if} \quad p_1 - p_2 \le (v_1 - v_2) - t - qL$$

$$n_1 + n_2 = 1, \quad n_2 > 0 \quad \text{if} \quad \begin{cases} p_1 - p_2 > (v_1 - v_2) - t - qL \\ p_1 + p_2 \le (v_1 + v_2) - t - qL \end{cases} \tag{8}$$

$$n_1 + n_2 < 1, \quad n_2 > 0 \quad \text{if} \quad p_1 + p_2 > (v_1 + v_2) - t - qL$$

The proofs of all results are left to the appendix. Proposition 1 defines three regions of the problem space. When both the difference in firms' prices ($p_1 - p_2$) and the expected loss due to attack (qL) are sufficiently small, the superior firm (Firm 1) captures the entire market. When prices are sufficiently high, some consumers forego purchase. In the intermediate case, all consumers are split between the two firms. Proposition 1 rules out the possibility of only one firm having positive market share and some consumers foregoing purchase. Intuitively, this would never be the case, since then there would be some consumers in the neighborhood of the competing firm who are not purchasing either product but could be profitably served.

The equilibrium prices and resulting market shares are characterized in the following proposition, which is discussed below.

Proposition 2. *The equilibrium prices and market shares are given by*

$$\text{if } q \le \frac{v_1 - v_2 - 3t}{3L}$$

$$\begin{aligned} p_1 &= v_1 - v_2 - t - qL & \quad n_1 &= 1 \\ p_2 &= 0 & \quad n_2 &= 0 \end{aligned} \tag{9a}$$

$$\text{if } \frac{v_1 - v_2 - 3t}{3L} < q \le \frac{v_1 + v_2 - 3t}{3L}$$

$$\begin{aligned} p_1 &= \frac{1}{3}(v_1 - v_2) + t + qL & \quad n_1 &= \frac{1}{2} + \frac{v_1 - v_2}{6(t + qL)} \\ p_2 &= -\frac{1}{3}(v_1 - v_2) + t + qL & \quad n_2 &= \frac{1}{2} - \frac{v_1 - v_2}{6(t + qL)} \end{aligned} \tag{9b}$$

$$\text{if } \frac{v_1 + v_2 - 3t}{3L} < q \le \frac{v_1 + v_2 - 2t}{2L}$$

$$\begin{aligned} p_1 &\in \left[\begin{matrix} \max\left\{\tfrac{1}{2}v_1, v_1 + \tfrac{1}{3}v_2 - t - qL\right\}, \\ \min\left\{\tfrac{2}{3}v_1, v_1 + \tfrac{1}{2}v_2 - t - qL\right\} \end{matrix} \right] & \quad n_1 &= \frac{v_1 - p_1}{t + qL} \\ p_2 &= v_1 + v_2 - t - qL - p_1 & \quad n_2 &= 1 - \frac{v_1 - p_1}{t + qL} \end{aligned} \tag{9c}$$

$$\text{if } \frac{v_1 + v_2 - 2t}{2L} < q$$

$$\begin{aligned} p_1 &= \frac{1}{2}v_1 & \quad n_1 &= \frac{v_1}{2(t + qL)} \\ p_2 &= \frac{1}{2}v_2 & \quad n_2 &= \frac{v_2}{2(t + qL)} \end{aligned} \tag{9d}$$

The nature of the equilibrium depends on which of four regions, a, b, c, or d (Equations 9a through 9d), contains q. Of course, since q is bounded ($0 \le q \le 1$), it may not be possible to find a q satisfying the conditions of all four regions. For example, consider a case with very high quality differentiation, ($v_1 - v_2$), very low horizontal differentiation, t, and arbitrary small loss, L. In this case, $\frac{v_1 - v_2 - 3t}{3L} > 1$, implying that the equilibrium will be described by Region a for all q. This is intuitive, as these parameters describe a product viewed as vastly superior by all consumers, and consumers do not face a loss from attack. Thus, regardless of the vulnerability, the superior product will capture the entire market.

The equilibrium described in Proposition 2 is unique except for a range of parameter values in Region c where a continuum of equilibria exist. Here, we briefly describe the four regions.

In Region a, Firm 1 is pricing just low enough to capture every consumer and make it impossible for Firm 2 to undercut its price. To see this, consider the consumer located furthest away from Firm 1 at $\alpha = 1$. This consumer's utility from purchasing from Firm 1 is given by $u_1(1) = v_1 - p_1 - t - qLn_1 = v_2 + qL(1 - n_1) \ge v_2$. If this consumer weakly prefers Firm 1, then so do all consumers to his left. Thus, $n_1 = 1$ and no positive price by Firm 2 would be acceptable to any consumer. In Region b, the vulnerability of the products, q, is so high that some consumers prefer a less prevalent product, in spite of the fact that this product is inferior. In this case, Firm 1 finds it too expensive to price Firm 2 out of the market, and both firms share the market. Multiple equilibria exist in Region c, a common feature of models with quality differentiated products (Shaked and Sutton 1982) as a result of corner solutions to the firms' optimization problems. In this region, a firm selecting a price must ensure that the furthest consumer it is trying to induce to purchase prefers its product both to the other firm's and to making no purchase. All equilibria in this range have the feature that this marginal consumer is indifferent between either of the two products and also indifferent between purchasing a product and making no purchase. In Region d, vulnerability is sufficiently high that it is no longer profitable for the two firms to serve the entire market. In these cases, firms will concentrate on consumers near them (in the Hotelling sense), while those consumers without a strong preference will purchase neither product.

Impact of Malicious Agents

Firms with Market Power

The regions of the problem space defined by Proposition 1 are depicted in the three unshaded quadrants of Figure 1.[9] The result of competition among two firms *without* the presence of malicious activity can be obtained from Proposition 2 when $q = 0$. Market shares and market coverage depend on the levels of horizontal and quality differentiation. For example, if quality differentiation is sufficiently strong, specifically when $(v_1 - v_2) \geq 3t$, then the equilibrium is given by (9a) for $q = 0$. The absence of malicious activity implies that the superior firm will monopolize the market (quadrant I of Figure 1) for all values of q. If horizontal differentiation is sufficiently strong, $t > \frac{1}{2}(v_1 + v_2)$, then the equilibrium is given by (9d), with each firm serving a subset of consumers (quadrant III). Intermediate levels of differentiation result in the two firms dividing the entire market between them (quadrant II).

We now examine how vulnerability, q, impacts the market. The equilibrium described in Proposition 2 suggests that, as q increases, market structure can evolve from monopolization by the superior firm (9a) to full market coverage by both firms (9b and 9c) to each firm serving only some of the available consumers (9d). That is, the presence of software vulnerabilities can move the market up and to the left in Figure 1. For example, if currently a single firm captures the entire market (quadrant I), then the negative externality imposed by increasing vulnerability makes it increasingly likely that some consumers will choose the alternative product. For a market currently in quadrant II, an increase in vulnerability might result in some consumers choosing neither product. The magnitude of the shift caused by the presence of vulnerability depends on the loss caused by a successful attack (L). If L is very small, then the existence of software vulnerabilities is little more than a nuisance, and the market is likely to remain in the same quadrant. For sufficiently large L, the market will shift to quadrant III.

As market outcomes depend on the levels of horizontal and quality differentiation, as well as the degree of vulnerability, we focus on four ranges of parameters which yield different market structures. First, for *high quality differentiation*, defined by $(v_1 - v_2) \geq 3t + 3L$ (or equivalently, $t \leq \frac{1}{3}(v_1 - v_2) - L$), the superior firm will monopolize the market for all values of q. Second, when $3t + 3L > (v_1 - v_2) \geq 3t$ (equivalently, $\frac{1}{3}(v_1 - v_2) - L < t \leq \frac{1}{3}(v_1 - v_2)$), the industry exhibits *moderate quality differentiation*. Here, whether a single firm monopolizes the market or not depends on the value of q. Third, in an industry with *high horizontal differentiation*, defined by $t > \frac{1}{3}(v_1 + v_2)$, firms price not to convince a consumer to switch from a competitor, but to entice the consumer to purchase anything at all. Thus, firms collectively serve a subset of consumers.[10] Fourth, the remaining range of parameters, $\frac{1}{3}(v_1 - v_2) < t \leq \frac{1}{3}(v_1 + v_2)$, reflect an industry with *low differentiation*. Both quality and horizontal differentiation are limited by the first and second constraints, respectively.

Next, we formally determine the profit impact of vulnerability as its level, q, increases. We begin with the case where increased vulnerability has the expected effect: reduced profitability. The following theorem states that, when the products are highly differentiated, vulnerability is undesirable.

Theorem 1. *In equilibrium*,

(i) HIGH QUALITY DIFFERENTIATION.

$$\text{If } t \leq \tfrac{1}{3}(v_1 - v_2) - L \text{, then } \frac{d\pi_j^*}{dq} \leq 0, j \in \{1,2\},$$

(ii) HIGH HORIZONTAL DIFFERENTIATION.

$$\text{If } t > \tfrac{1}{2}(v_1 + v_2) \text{, then } \frac{d\pi_j^*}{dq} < 0, j \in \{1,2\},$$

$$\text{If } \tfrac{1}{2}(v_1 + v_2) \geq t > \tfrac{1}{3}(v_1 + v_2) \text{, then } \frac{d\overline{\pi}_j^*}{dq} \leq 0 \text{ and } \frac{d\underline{\pi}_j^*}{dq} \leq 0,$$

$j \in \{1,2\}$, where $\overline{\pi}_j^*$ and $\underline{\pi}_j^*$ are the highest and lowest obtainable equilibrium profit for firm j.

When the firms are either highly quality differentiated (the average quality of Firm 1 sufficiently exceeds that of Firm 2) or highly horizontally differentiated (t is sufficiently large), profits are never increasing as vulnerability increases. See Figure 2 for an example. In these cases, software firms prefer completely secure software, or $q = 0$. In the case of high quality differentiation (case (i) in Theorem 1), the superior firm, Firm 1, captures the entire market and Firm 2's profits

[9] Only one firm having market share but not fully covering the market is ruled out by Proposition 1.

[10] In Region c, all consumers purchase, as the sum of the market shares is equal to 1. However, the consumer indifferent between purchasing the products of Firm 1 and Firm 2 is also indifferent between either purchase and no purchase, as this consumer's utility from all three decisions is zero. Thus, this class of equilibria is qualitatively similar to (9d) where firms price to make a consumer better off buying from them than buying nothing at all, rather than price to capture consumers from a competitor.

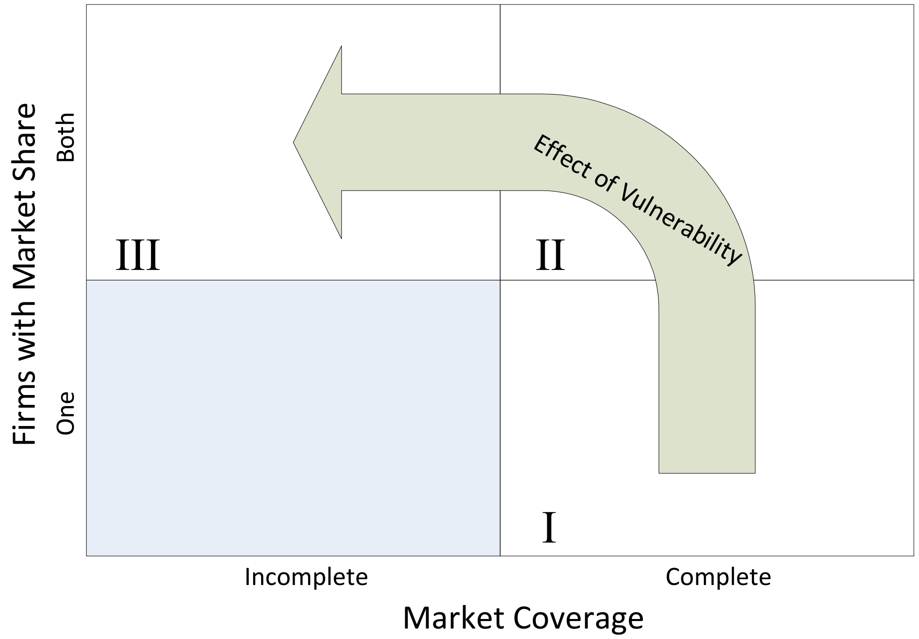
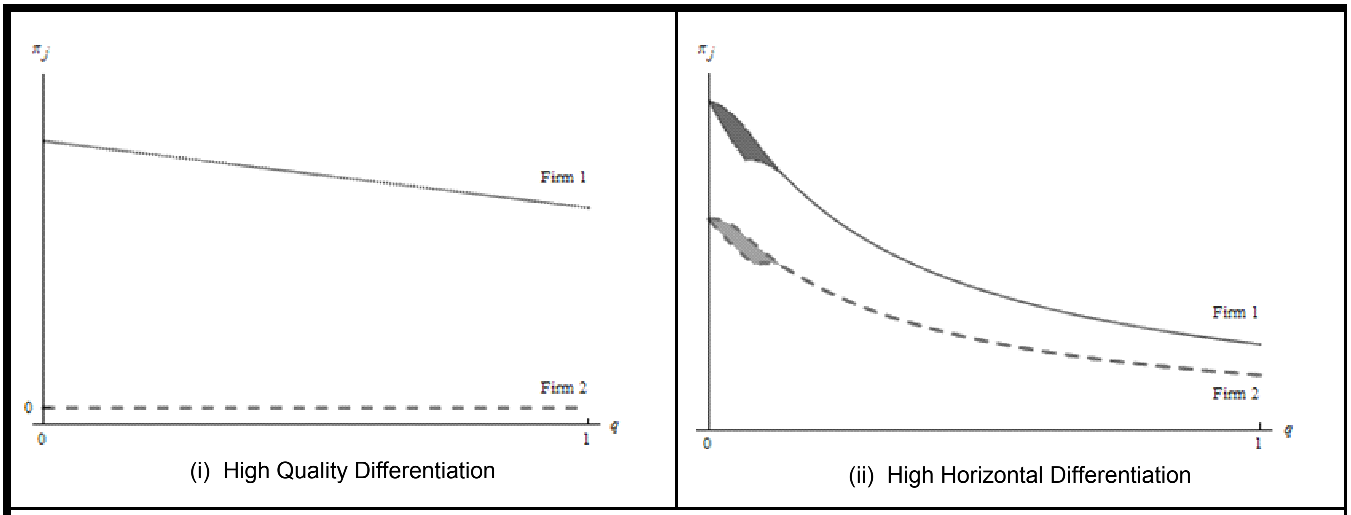


Figure 1. Market Structure and the Impact of Vulnerability



(i) High Quality Differentiation

(ii) High Horizontal Differentiation

Profits are non-increasing in *q* under both high horizontal or quality differentiation. Shaded regions indicate a continuum of equilibria.

Figure 2. Impact of Increased Malicious Activity on Profit When the Market Exhibits Differentiation

are 0. This is a monopoly that will exist regardless of the level of vulnerability. The market is in quadrant I of Figure 1 regardless of q. As vulnerability increases, the only effect is that Firm 1's product becomes less valuable to consumers, implying that the market is captured at a lower price and profit. Indeed, the equilibrium price of the superior firm (from Proposition 2), $p_1 = v_1 - v_2 - t - qL$, incorporates each consumer's expected damages from possible attacks, qL. When a firm succeeds in monopolizing the market, it fully internalizes the cost and likelihood of attack. The consumer is indifferent to vulnerability as higher vulnerability comes with exactly offsetting lower prices. Overall, with firms' profits decreasing in q and consumers indifferent to q, social welfare is maximized at $q = 0$.

Under sufficiently high horizontal differentiation (case (ii) of Theorem 1), some consumers will purchase neither product in equilibrium. Effectively, both firms are local monopolists over a subset of consumers. In this case, the firm is already in quadrant III of Figure 1 in the absence of vulnerability, so it will remain there for any positive q. Therefore, as above, increased vulnerability decreases the value of both products, resulting in lower profits. Additionally, increased vulnerability decreases consumer surplus. This occurs for two reasons, evident from (9d). First, the number of consumers purchasing each product decreases. Second, those that do purchase receive the same price independent of q and thus fully internalize the cost of higher vulnerability. In the case of local monopolists, firm and consumer interests are aligned. The second part of case (ii) in the theorem deals with a technical issue of multiple equilibria, and shows that the upper and lower bounds of possible equilibrium profits are nonincreasing for both firms.

Overall, Theorem 1 indicates that firms with local monopolies or very strong global monopolies prefer lower vulnerability in their software, since greater vulnerability simply diminishes the value of their products. In the next section, we show that this intuitively pleasing result does not always hold in more competitive settings.

A Preference for Vulnerability

Although the reduced profits from vulnerability shown above conform to conventional wisdom, this need not be the impact of vulnerability in general. In this section, we define conditions under which firms actually prefer that their software be vulnerable to attacks by malicious agents, as increased profits will result. Essentially, our results indicate that when differentiation between products is not too strong, and therefore competition is intense, vulnerability can increase the market power of the firms and enable higher profits.

First, we demonstrate that an inferior firm might prefer vulnerability because it can allow the inferior firm to gain market share.

Theorem 2. MODERATE QUALITY DIFFERENTIATION.

In equilibrium, if $\frac{1}{3}(v_1 - v_2) - L < t \leq \frac{1}{3}(v_1 - v_2)$, *then*

(i) $n_1 = 1$, $n_2 = 0$ *when* $q = 0$.

(ii) $\exists \underline{q} < 1$ *such that* $n_2 > 0$ *whenever* $q \geq \underline{q}$.

The parameter ranges of Theorem 2 result in Firm 1 monopolizing the market for some, but not all, degrees of vulnerability. When quality differentiation is moderate, the better product can still capture the entire market in the absence of vulnerability. As vulnerability rises, however, the large market share increases the probability of attack, leading some consumers to defect to the technologically inferior, but safer, product. For a sufficiently high vulnerability, the inferior firm will serve consumers in equilibrium. Thus, the better product's monopoly is not strong enough to withstand the negative network effects created by vulnerability.

The above result implies that at least one firm can potentially benefit from increased vulnerability by profiting from consumers' flight to safety. The flight from the dominant product can be viewed as a search for "security through obscurity."[11] The relatively small market share of the inferior offering from Firm 2 lowers its probability of being attacked, and this attracts some consumers (for example, the chief technology officer quoted in the "Introduction" of this paper). Thus, selecting software based only on its attributes or feature set may lead to suboptimal decisions. In some cases, adopting the inferior product with a small market share may lead to higher overall utility, given the lower probability of malicious attack.

However, it is not only the inferior firm that can benefit from increased vulnerability. Both firms can simultaneously gain, as shown in the following theorem.

Theorem 3. *In equilibrium,*

(i) *If* $\frac{1}{3}(v_1 - v_2) - L < t < \frac{1}{3}(v_1 + v_2)$, *then there exist a* $\underline{q}$ *and* $\overline{q}$, $0 \leq \underline{q} < \overline{q} \leq 1$, *such that* $\frac{d\pi_j^*}{dq} > 0$ *when* $q \in (\underline{q}, \overline{q})$, $j \in \{1,2\}$,

(ii) *if* $\frac{1}{3}(v_1 - v_2) < t \leq \frac{1}{3}(v_1 + v_2) - L$, *then* $\frac{d\pi_j^*}{dq} > 0$, $q \in [0,1]$, $j \in \{1,2\}$.

[11] This phrase has been used both to describe the relative safety of obscure technologies due to their low value to attackers and, in a context different from ours, in discussions of the costs and benefits of publicly revealing source code.

Theorem 3 defines conditions under which more vulnerability can be preferred to less by both competing firms. To provide some intuition for our results, consider competition between two nearly identical software products. In the absence of security considerations, if one competitor undercuts the price of the other, it is likely to gain most of the market. This provides a strong incentive for each firm to cut prices, leading to aggressive price competition and low profits. However, if higher market share also implies greater security risk, the dynamics of competition change. In this case, if one undercuts its rival's price, it is less likely to capture most of the consumers. Specifically, as more consumers adopt the cheaper product, they increase its probability of being attacked. The result is that some consumers might choose the more expensive, but more secure, product. In the presence of vulnerability, a price cut leads to a smaller gain in market share than would have been realized otherwise. This, in turn, reduces the incentive to cut prices. Given these dynamics, vulnerability can lead to higher prices and profits in equilibrium.

The conditions in Theorem 3(i) are the complement to those in Theorem 1 and include both moderate quality differentiation and low differentiation. In these regions, firms prefer more vulnerability precisely when all consumers make a purchase (i.e., all derive strictly positive utility) in equilibrium. More vulnerability decreases the value of both products to consumers while simultaneously softening price competition between firms. As long as all consumers continue to derive positive utility, the impact of decreased value is fully offset by the role of softer price competition, resulting in higher profits.

Part (ii) of the theorem notes an extreme case (and one that is not likely to occur in reality) where, if products are sufficiently similar, profits are *always increasing* with additional vulnerability and both firms prefer as much vulnerability as possible. The parameter ranges define a subset of low differentiation, in which the products are nearly identical. This part of the theorem contains both an upper bound on quality differentiation (first restriction on t) and an upper bound on horizontal differentiation (second restriction on t). Implicitly, the condition also requires that the loss incurred by consumers from an attack cannot be too high ($L < \frac{2}{3}v_2$). Thus, if products are very similar (in terms of quality *and* horizontal differentiation) and the loss incurred from an attack is low, then the added differentiation created by the presence of vulnerability offsets any degradation in the value of the product, and this effect is so strong that firms prefer as much vulnerability as possible.

The results above show that when neither horizontal nor quality differentiation is extreme, profits can increase with greater vulnerability. Examples of profit behavior as q increases can be seen in Figure 3. The top two panels of the figure, (a) and (b), illustrate cases when profits are increasing for only large values of q. Panel (c) corresponds to Theorem 3(ii) as profits of both firms increase over the entire range of q. Panel (d) shows profits increasing for low values of q only. Panels (e) and (f) depict cases in which profits are increasing over intermediate values of q. A more intuitive explanation of these panels may be derived from the market structures depicted in Figure 1. The market can take on only one of three general forms: a global monopoly, a competitive industry, or local monopolies. These correspond to high or moderate quality differentiation, low differentiation, and high horizontal differentiation. As vulnerabilities increase, the market outcome shifts upward and to the left in Figure 1. A monopolist becomes competitive due to the introduction of malicious agents, or a competitive market changes into a market with two local monopolists.

Clearly, if the derivative of profits with respect to q is positive at $q = 0$, then firms prefer the existence of some vulnerabilities in their software to none at all. In Figure 3, panels (c) and (d) show such cases. When profits are initially decreasing, further analysis is required to determine if firms prefer vulnerability. For example, Firm 1 prefers no vulnerability in panel (a) and a maximal amount ($q = 1$) in panel (b). Similarly, Firm 1 prefers no vulnerability in panel (e) and a moderate amount in panel (f). We address the question of whether maximum profits are achieved in the presence or absence of vulnerability in the following result.

Theorem 4. *If either of the following conditions hold:*

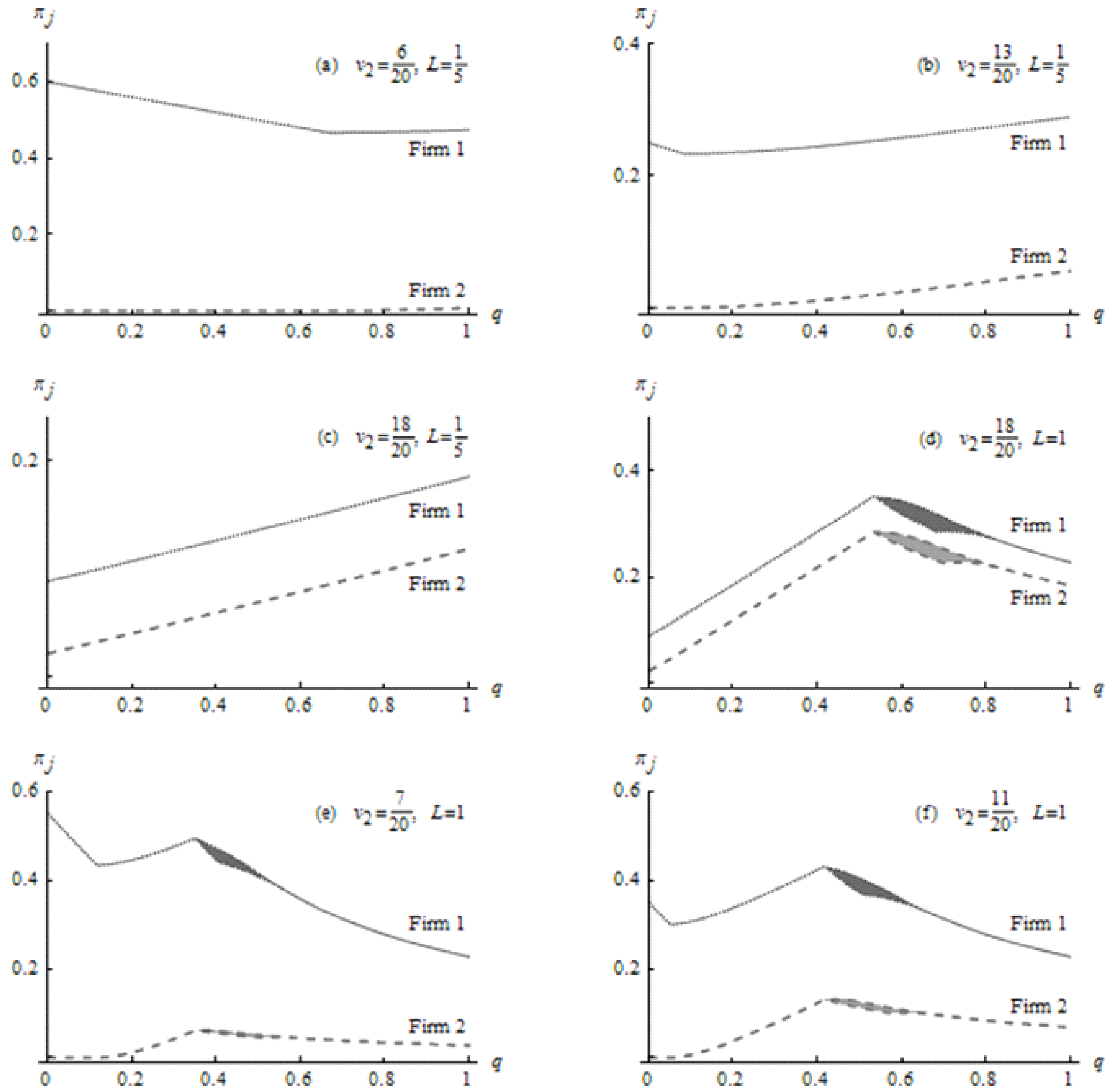
(i) LOW DIFFERENTIATION. $\frac{1}{3}(v_1 - v_2) < t \le \frac{1}{3}(v_1 + v_2)$, *or*

(ii) $\frac{v_1^2 - 3v_2^2}{3(v_1 + v_2)} < t \le \frac{1}{3}(v_1 - v_2)$ *and*

$$L > \min\left\{\frac{1}{3}(v_1 + v_2) - t,\ 2\left(\frac{1}{3}v_1 - \frac{1}{3}v_2 - t\right) + \sqrt{\left(\frac{1}{3}v_1 - \frac{1}{3}v_2 - t\right)(v_1 - v_2 - t)}\right\},$$

then both firms earn greater profits at some $q > 0$ *than when* $q = 0$.

Theorem 4 outlines conditions under which *both* firms obtain higher profits when some vulnerability is present. The conditions in case (i) of the theorem correspond precisely to situations where, in the absence of vulnerability, all consumers make a purchase and both firms have positive market share. Thus, firms are neither sufficiently horizontally nor quality



In all cases, $v_1 = 1,\ t = \frac{1}{10}$

Figure 3. Profits for Each Firm as the Probabilty of Malicious Activity Increases

differentiated. This is a highly competitive (and not uncommon) environment, since each additional consumer for one firm is a loss of a consumer to the other. Some positive amount of vulnerability is always beneficial to both firms as it, perversely, softens price competition among them. For example, imagine that, in the absence of vulnerability, a small price hike would cause a firm to lose 10 percent of its consumers. When vulnerability is present, each consumer lost actually increases the value of the product to all other consumers of that product by making it a less attractive target. In this case, the firm might lose only 8 percent of its consumers, so the incentive to raise prices is greater. Similarly, the incentive to lower prices is reduced since the firm will not capture as many consumers from its competitor. In equilibrium, these dynamics allow both firms to increase prices and capture higher profits. Case (ii) allows for higher levels of quality differentiation, and corresponds to cases where Firm 1 would be a monopoly in the absence of vulnerabilities. In the presence of vulnerabilities, the second firm enters due to its "security through obscurity" advantage. The first firm benefits from the pricing power enabled by vulnerability, even at the expense of its monopoly.

Endogenous Security Choice

In the analysis above, we characterized the conditions under which higher vulnerabilities to malicious attack can benefit software manufacturers. Of course, firms can exercise some control over the vulnerabilities of their products. We now relax the assumption of fixed and identical security of the two products, allowing security to differ across firms. We allow vulnerability, denoted by q_j, to be a variable within a firm's strategic control. Thus,

$$q_j(n_j) \equiv q_j \theta n_j \qquad (10)$$

where $\theta \in [0,1]$ is a scaling parameter.

With endogenous vulnerability levels, our model expands to four periods. First, firms simultaneously select their vulnerability level, q_j, at a cost $c_j(q_j)$, which is non-increasing and nonnegative, $c_j(\cdot) \geq 0, \frac{dc_j(q_j)}{dq_j} \leq 0, q \in [0,1]$, ensuring that lower vulnerability (better security) does not come at a lower price. Second, firms observe each others' vulnerability levels and simultaneously set prices for their two products (p_1 and p_2). Third, consumers make their purchase decisions. Finally, malicious agents decide whom to attack.

In the previous sections, we identified three possible regimes: (1) a single firm monopolizes the market when the quality differential is strong, (2) both firms share the market, with all consumers purchasing one or the other product, and (3) both firms are effectively local monopolies over consumers close to them when horizontal differentiation is strong, leaving some central consumers unserved. Thus, firms are either monopolistic (globally or locally) or engaged in competition over each consumer. With endogenous vulnerability levels, firms in both monopoly regimes effectively face a simple optimization problem, trading off the cost of extra security against the added value it provides its consumers. Consider for example the case of very high quality differentiation, when Firm 1's subsequent pricing decision would lead it to monopolize the entire market for any q_1 and q_2. Since a monopolist, by definition, is immune to changes in strategic variables of other firms, q_1 is the only relevant vulnerability level in the industry. The effect of decreasing q_1 is equivalent to the effect of a decrease in the industry q described in the previous sections. Depending on the magnitude and curvature of the cost function, the optimal solution may be interior, or could be $q_1 = 0$ or $q_1 = 1$. Similarly, the local monopolist regime has each firm selecting the optimal level of q_j to maximize the profit from its consumers. The effect is that the intuition for both the global monopolist and local monopolist regimes from the previous section, that vulnerability always decreases profits, still holds. The only change is that vulnerability choice becomes a cost–benefit analysis, balancing the higher prices a secure product brings with the costs of acquiring that security.

It remains to examine whether the result that vulnerability can *increase* profits holds when vulnerability choice is endogenous. This is addressed in the following theorem.

Theorem 5. *For any cost functions,* $c_j(q_j)$, *if* $t \leq \frac{1}{3}(v_1 + v_2) - L$, *then*

(i) *If* $\frac{1}{3}(v_1 - v_2) < t$, *then an equilibrium cannot have* $q_1 = q_2 = 0$.

(ii) *If* $(v_1 - v_2) < t$, *then the equilibrium exhibits* $q_1 = q_2 = 1$.

Further, $q_i = 1$ *is a dominant strategy.*

When software products are not very differentiated, either horizontally or in terms of quality, Theorem 5 indicates that firms will never choose to eliminate all vulnerabilities in equilibrium. Notably, even if the cost function is $c_j(\cdot) = 0$, so that eliminating vulnerabilities is costless, firms would still not elect to do so. Part (ii) of the theorem defines the extreme case (not likely to be encountered in practice) where firms have so little differentiation that each firm prefers the highest level of vulnerability possible.

When competing firms control q_j, an increase of q_j by one of the firms has two effects. First, it decreases the value of the firm's product to its own consumers, which requires it to charge lower prices. Second, it softens price competition between both firms, allowing for higher prices. Theorem 5 indicates that when firms are sufficiently similar in consumers' minds, the second effect dominates. In particular, consider two firms offering products of identical quality ($v_1 = v_2$) with t very close to zero. Since the products are not differentiated, price competition drives both prices down to their costs of production. This leaves consumers quite well off, since even the marginal consumer, who is indifferent between the two products, is receiving positive value from either product. When the vulnerability of one product increases, the entire market is still served, but the other product becomes sufficiently more valued by consumers. This allows the other firm to raise its price, allowing the initial firm to raise its price in turn. When very low differentiation creates sufficiently fierce competition, the loss of relative value due to an insecure product is fully offset by this loosening of price competition.

The above discussions only consider the cases where the marketplace will retain the same competitive structure for all levels of q_1, q_2. When this is not the case, a firm must determine its optimal profits for each market structure in turn and decide which one to pursue with its choice of p_j and q_j. For example, a firm of sufficiently higher quality must decide if it prefers a large investment in reducing vulnerability, which would give it a monopoly, or if it prefers to save on those costs and allow its competitor to enter. While the analysis of these cases is complicated by assumptions about specific functional forms of the cost function, the same intuition as provided by the exogenous vulnerability model applies.

Generalizations

There are several extensions to our model worth exploring. A complete description of the software market would incorporate vertical differentiation through heterogeneous tastes for quality, variability in the cost of loss for different consumers, and the multiple prices that software firms sometimes offer across their product lines or consumer segments. Of course, a model incorporating all of these factors would fail to offer tractable expressions. Below, we consider several of these extensions in isolation to examine the robustness of the model. For simplicity, in this section we assume an exogenous q common to both firms. Further, to focus on the most interesting cases in which competition between firms is especially intense, we assume that v_2 is sufficiently large to ensure that all consumers purchase.

Vertical Differentiation

While our model allows for a varying proportion of consumers to prefer one product's features over another, our focus has been on horizontal differentiation. Vertically differentiated products exhibit agreement among all consumers about the superiority of one over the other, but heterogeneity over the value of this superiority. Below, we demonstrate that similar insights are obtained in this context. Define the utility from adopting the product of Firm j for a consumer located at $\alpha \in [0,1]$ as

$$u_j(\alpha) = \alpha v_j - p_j - q n_j L \tag{11}$$

As before, let $q \in [0,1]$, $L > 0$, $v_1 > v_2 > 0$, α uniformly distributed. Denote the quality advantage of Firm 1 as $\Delta \equiv v_1 - v_2$. Resulting equilibrium prices and market shares are given by

$$p_1 = \frac{2}{3}\Delta + qL \qquad n_1 = \frac{2\Delta + 3qL}{3\Delta + 6qL} \tag{12}$$

$$p_2 = \frac{1}{3}\Delta + qL \qquad n_2 = \frac{\Delta + 3qL}{3\Delta + 6qL} \tag{13}$$

In the absence of any vulnerability ($q = 0$), the above yields a familiar outcome from vertical differentiation models. Firm 1 sets a higher price and captures a majority of the market. As q increases, both firms raise price. Additionally, as q increases, the firms' market shares become more equalized; the negative externality mitigates Firm 1's ability to maintain a dominant market share. Thus, as q increases, the inferior firm appreciates a higher price and higher market share. Firm 2's higher price comes at a cost of lower market share, but as the next result shows, the net effect on profit is still positive.

Theorem 6. *In the vertical differentiation model, both firms' profits are increasing in q.*

The expressions in (12) and (13) also offer some insight into the possibility of endogenous quality, where firms explicitly determine v_1 and v_2. The profits, $p_j n_j$, of both firms are increasing in Δ, the difference in firm qualities. Thus, the lower-quality firm may benefit either from an increase in the rival's quality or a decrease in its own, in keeping with the insights of Moorthy (1988) and Shaked and Sutton (1982). Additionally, the cross-partial derivatives $\frac{\partial^2 p_j n_j}{\partial \Delta \partial q}$ are negative. When competition is fiercest, so that all consumers purchase one of the two products, malicious activity serves as a substitute for differentiation in improving firms' profits. Taken together with our results in the previous sections, we find similar insights for IS managers whether vertical or horizontal differentiation most accurately reflects a given industry context.

Damages

Our model assumes that the expected loss from a successful attack, L, is identical for each consumer. This is not a critical assumption. As long as the loss is uncorrelated with consumer tastes over the two products, our qualitative results follow. For example, imagine that losses take on one of K discrete values, $L_1, \ldots, L_K$ with arbitrary element L_k. For each

L_k, there exists a full measure of consumers with density equal to d_k, $\sum d_k = 1$. Then, among the consumers with losses of L_k, the consumer indifferent between the products of Firm 1 and Firm 2 is given by an expression analogous to Equation (3):

$$\alpha_k^* = \frac{1}{2} + \frac{1}{2t}\left[\left(v_1 - v_2\right) - \left(p_1 - p_2\right) - qL_k\left(n_1^e - n_2^e\right)\right] \tag{14}$$

As all consumers purchase, by assumption, in equilibrium we have

$$n_1 = \sum_{k=1}^{K} d_k \alpha_K^* \tag{15}$$

$$= \frac{1}{2} + \frac{1}{2t}\left[\left(v_1 - v_2\right) - \left(p_1 - p_2\right)\right] - q\left(n_1^e - n_2^e\right)\sum_{k=1}^{K} d_k L_k \tag{16}$$

Thus, a single L is replaced with $E[L] = \sum_{k=1}^{K} d_k L_k$ with all other analysis proceeding as before.

If some consumers do not purchase either product in equilibrium, firms face an additional tradeoff. In particular, imagine that all consumers with relatively low L make a purchase but some with very high L do not. Then, a small increase in q provides firms with additional pricing power over the consumers with low L but decreases the value for (and thus profit from) the consumers with high L, over which each firm is a local monopolist. Whether an increase in q is beneficial for the firms will depend not only on the level of differentiation among firms, but also on the ratio of consumers with relatively high or low L.

Throughout our analysis, the probability an attack is successful, q, and the expected loss from a successful attack, L, enter multiplicatively into the utility function. This implies that reducing the chance an attack is successful by 50 percent while doubling the expected loss from a successful attack does not alter the consumer's utility. If losses are insurable, this equivalence no longer applies, as consumers may not be responsible for a loss in excess of some fixed amount. The feasibility of insurance markets for security breaches has been questioned, as these markets would suffer from severe moral hazard, very poor information, and high correlation of security risks across consumers (Anderson et al. 2007; Bohme and Kataria 2006). Nevertheless, if an insured consumer suffers some loss (perhaps a deductible) from each successful attack, or pays an insurance premium proportional to expected damages, then a consumer's expected payment still increases with market share.

Prices

Similar modifications are required to deal with situations where software firms offer products at multiple prices, in contrast to our assumption of a single price in the analysis above. If a firm markets entirely separate products, each with its own independent market segment and vulnerability, then our model should be interpreted as addressing each of these markets individually. Of course, this full separation of products and their markets is rarely realistic. Multiple versions of products often share much of the same code, so vulnerabilities found in one are likely to translate to its product-line cousins. Quantity discount licensing agreements, for example, offer an identical product at prices adjusted to different market segments (e.g., small or large firms). However, if all of these segments are highly competitive, then the incentive to increase q (or the disincentive to decrease it) exists for each product, and thus for the common code elements as well. On the other hand, if some products face intense competition while others do not, the incentive to control vulnerability will be more nuanced. In general, our results suggest that higher vulnerability along a product line will benefit products in more competitive environments but lower profits for products in less competitive environments. The incentive to lower vulnerability in shared code used across market segments would be a mixture of our results calibrated for each market and weighted by each market's contribution to profit.

Overall, our analysis of the above model extensions demonstrates the robustness of our results. The extensions considered, which in some cases might more accurately reflect reality, lead to qualitatively similar, although more nuanced, results. Other specifications are certainly possible. For example, a quadratic (rather than linear) transportation cost complicates the derived expressions, but it does not change the primary conclusion: when software firms are insufficiently differentiated in the minds of consumers, there exists an incentive to increase pricing power through higher product vulnerability.

Conclusions

The impact of malicious activity on the software industry is an important consideration for IS managers. In many cases, software firms can be expected to invest in reducing vulnerabilities to malicious attacks, as this increases the value of their products to consumers and allows for higher profits. However, we show that malicious agents can have some counterintuitive effects on the market as well.

Asvanund et al. (2004) show that congestion costs place a natural limit on a peer-to-peer network's size. Our results have an analogous interpretation: malicious agents' attraction to the more popular product can limit market share, as security fears might eventually outweigh the product's superiority in features or usability. Furthermore, our results

Table 1. Software Firm Vulnerability Preference for Different Market Structures

Market Structure	Vulnerability preference	Theorem
High quality differentiation	Higher-quality firm prefers lower vulnerability	1(i)
Moderate quality differentiation	Both firms may prefer higher vulnerability	2, 3(i)
High horizontal differentiation	Both firms prefer lower vulnerability	1(ii)
Low differentiation	Firms prefer higher vulnerability over some range of *q*	3(i)
Nearly identical products	Firms always prefer higher vulnerability	3(ii)

suggest that this limit on growth may be desirable by software manufacturers, as it allows them to compete less aggressively over consumers. In addition to enabling a firm with an inferior product to operate profitably, our results indicate that a positive level of vulnerability to malicious activity is preferred by software firms in highly competitive industries. The fiercer the competition among software vendors, the less incentive each has to decrease its vulnerability to malicious attack. Contrary to the traditional view that monopolies are less responsive to customers, monopolistic firms prefer more secure products since they can extract the value of this enhanced security through higher prices. Firms that compete over each consumer, facing a constraint on prices through the actions of their rivals, prefer to lessen price competition. The negative externality of attacks targeting higher market share achieves precisely this. A key insight for the IS manager contemplating product adoption is that a firm in a highly competitive software environment has less incentive to produce secure products than a firm in a less competitive environment. We summarize the relationship between the competitive environment and the incentives of software firms to lower the vulnerabilities of their products in Table 1. The theorem supporting each relationship is also noted in the table.

We do not envision our results as literally implying that firms will intentionally introduce security holes into their software, but we do speak to the incentives to find and diminish their presence. The common conception that software firms would gladly abolish all malicious activity if they could easily do so is perhaps overstepping. Consider, for example, the fact that adding features to software products requires additional code that might increase software vulnerabilities. Our results imply that, in highly competitive environments, software firms are more likely to add these features (i.e., increase v_j) without adequate regard for the potential increase in vulnerability, q_j. IS managers should be aware of this when considering new, feature-rich software products in a highly competitive market.

While our model furthers our understanding of the impact of malicious agents on the industries they target, we note that there are several limitations to this work. First, our results do not apply to cases where positive externalities are so strong that they trump security concerns. In these cases, insights driven by traditional research on positive network externalities would be more applicable. Second, we do not account for uncertainties regarding the application of security patches by software users. While our model does suggest that firms in competitive markets might have less incentive to encourage patching compliance, the inclusion of behavioral aspects of patch application in our model represents an interesting area for future research. Finally, our understanding of the market's impact on software security would benefit greatly from a systematic behavioral study of malicious agent incentives.

References

Akerlof, G. A. 1970. "The Market for 'Lemons': Quality Uncertainty and the Market Mechanism," *The Quarterly Journal of Economics* (84:3), pp. 488-500.

Alhazmi, O. H., and Malaiya, Y. K. 2005. "Quantitative Vulnerability Assessment of Systems Software," in *Proceedings of the 51st Annual Reliability and Maintainability Symposium*, Alexandria, VA, January 24-27, pp. 615-620.

Alhazmi, O. H., and Malaiya, Y. K. 2006. "Discovery Models for Apache and IIS http Servers," in *Proceedings of the 17th International Symposium on Software Reliability Engineering*, Raleigh, NC, November 7-10, pp. 343-352.

Anderson, R. 2008. *Security Engineering* (2nd ed.), New York: Wiley Publishing.

Anderson, R., Moore, T., Nagaraja, S., and Ozment, A. 2007. "Incentives and Information Security," *Algorithmic Game Theory*, in N. Nisan, T. Roughgarden, E. Tardos and V. V. Vazirani (eds.), New York: Cambridge University Press, pp. 633-650.

Anderson, S. P. 2008. "Product Differentiation," *The New Palgrave Dictionary of Economics Online*, S. Durlauf and L. Blume (eds.), London: Palgrave Macmillan (http://www.dictionaryofeconomics.com/article?id=pde2008_P000201)

Arora, A., Caulkins, J. P., and Telang, R. 2006. "Sell First, Fix Later: Impact of Patching on Software Quality," *Management Science* (52:3), pp. 465-471.

Arora, A., Nandkumar, A., Krishnan, R., Telang, R., and Yang, Y. 2004. "Impact of Vulnerability Disclosure and Patch Availability: An Empirical Analysis," paper presented at the Workshop on Economics and Information Security, Minneapolis, MN, May 13-14.

Arora, A., Telang, R., and Xu, H. 2008. "Optimal Policy for Software Vvulnerability Disclosure," *Management Science* (54:4), pp. 642-656.

Asvanund, A., Clay, K., Krishnan, R., and Smith, M. 2004. "An Empirical Analysis of Network Externalities in Peer-to-Peer Music Sharing Networks," *Information Systems Research* (15:2), pp. 155-174.

August, T., and Tunca, T. I. 2006. "Network Software Security and User Incentives," *Management Science* (52:11), pp. 1703-1720.

August, T., and Tunca, T. I. 2008. "Let the Pirates Patch? An Economic Analysis of Software Security Patch Restrictions," *Information Systems Research* (19:1), pp. 48-70.

Berghel, H. 2003. "Malware Month," *Communications of the ACM* (46:12), pp. 15-19.

Berry, S., Levinsohn, J., and Pakes, A. 1995. "Automobile Prices in Market Equilibrium," *Econometrica* (63:4), pp. 841-890.

Blakley, B. 2002. "The Measure of Information Security Is Dollars," paper presented at the Workshop on Economics and Information Security, Berkeley, CA, May 16-17.

Bohme, R., and Kataria, G. 2006. "On the Limits of Cyber-Insurance," in *Trust, Privacy and Security in Digital Business*, S. Fischer-Huebner, S. Furnell and C. Lambrinoudakis (eds.), Berlin: Springer Verlag, pp. 31-40.

Brynjolfsson, E., and Kemerer, C. F. 1996. "Network Externalities in Microcomputer Software: An Econometric Analysis of the Spreadsheet Market," *Management Science* (42:12), pp. 1627-1647.

Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. 2007. "Efficiency of Vulnerability Disclosure Mechanisms to Disseminate Vulnerability Knowledge," *IEEE Transactions on Software Engineering* (33:3), pp. 171-185.

Cavusoglu, H., Cavusoglu, H., and Zhang, J. 2008. "Security Patch Management: Share the Burden or Share the Damage?," *Management Science* (54:4), pp. 657-670.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2004. "The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers," *International Journal of Electronic Commerce* (9:4), pp. 69-105.

Cavusoglu, H., Mishra, B., and Raghunathan, S. 2005. "The Value of Intrusion Detection Systems in Information Technology Security Architecture," *Information Systems Research* (16:1), pp. 28-46.

Cavusoglu, H., and Raghunathan, S. 2004. "Configuration of Detection Software: A Comparison of Decision and Game Theory Approaches," *Decision Analysis* (1:3), pp. 131-148.

Cherian, J. 2007. "Mozilla's Firefox Browser Gaining in Popularity Among U.S. Small-to-Medium Businesses," *All Headline News*, March 9 (accessed March 26, 2007).

Choi, J. P., Fershtman, C., and Gandal, N. 2005. "Internet Security, Vulnerability, and Software Provision," paper presented at the Workshop on Economics and Information Security, Cambridge, MA, June 2-3.

Consumer Reports. 2005. "Net Threat Rising," *Consumer Reports*, September, pp. 12-15.

Cremonini, M., and Nizovtsez, D. 2006. "Understanding and Influencing Attackers Decisions: Implications for Security Investment Strategies," paper presented at the Workshop on Economics and Information Security, Cambridge, UK, June 26-28.

Datamonitor. 2005. "Global Application Software" (http://www.datamonitor.com/)

DeFelice, A. 2006. "Firefox a Growing Target for Hackers, *Linux Insider*, August 1 (available at http://www.linuxinsider.com/story/52152.html; accessed September 6, 2009).

Dinev, T., and Hart, P. 2006. "An Extended Privacy Calculus Model for E-Commerce Transactions," *Information Systems Research* (17:1), pp. 61-80.

Evers, J. 2004. "`Internet Explorer Loses Market Share," *Info World*, November 2 (available at www.infoworld.com/article/04/11/02/HNielosing_1.html; accessed September 6, 2009).

Farrell, J., and Saloner, G. 1985. "Standardization, Compatability and Innovation," *RAND Journal of Economics* (76:5), pp. 940-955.

Gal-Or, E., and Ghose, A. 2005. "The Economic Incentives for Sharing Security Information," *Information Systems Research* (16:2), pp. 186-208.

Galbreth, M. R., March, S. T., Scudder, G. D., and Shor, M. 2005. "A Game-Theoretic Model of E-Marketplace Participation Growth," *Journal of Management Information Systems* (22:1), pp. 295-319.

Gordon, L. A., and Loeb, M. P. 2002. "The Economics of Information Security Investment," *ACM Transactions on Information and System Security* (5:4), pp. 438-457.

Grow, B., and Bush, J. 2005. "Hacker Hunters," *Business Week*, May 30, pp. 74-82.

Hackner, J., and Nyberg, S. 1996. "Vanity and Congestion: A Study of Reciprocal Externalities," *Economica* (63:249), pp. 97-111.

Hauser, J. R., and Rao, V. 2004. "Conjoint Analysis, Related Modeling, and Applications," in *Advances in Market Research and Modeling: Progress and Prospects*, J. Wind and P. Green (eds.), New York: Kluwer Academic Publishers, pp. 141-168.

Hotelling, H. 1929. "Stability in Competition," *Economic Journal* (39:1), pp. 41-57.

Katz, M. L., and Shapiro, C. 1985. "Network Externalities, Competition, and Compatability," *American Economic Review* (75:3), pp. 424-440.

Lee, I. H., and Mason, R. 2001. "Market Structure in Congestible Markets," *European Economic Review* (45:4-6), pp. 809-818.

Li, X. 2004. "Information Cascades in IT Adoption," *Communications of the ACM* (47:4), pp. 93-97.

Linn, J. 2005. "Technology and Web User Data Privacy," *IEEE Security and Privacy* (3:5), pp. 52-58.

Loch, K. D., Carr, H. H., and Warkentin, M. E. 1992. "Threats to Information Systems: Today's Reality, Yesterday's Understanding," *MIS Quarterly* (16:2), pp. 173-186.

MacKie-Mason, J. K., and Varian, H. 1994. "Economics FAQs About the Internet," *Journal of Economic Perspectives* (8:3), pp. 75-96.

Maxcer, C. 2007. "Gates' Mac Attack: Fact vs. Fiction," *Mac News World*, March 1 (available at http://www.macnewsworld.com/story/56017.html; accessed September 6, 2009).

McFadden, D. 1986. "The Choice Theory Approach to Market Research," *Marketing Science* (5:4), pp. 275-297.

McHugh, J. A., Christie, A., and Allen, J. 2000. "Defending Yourself: The Role of Intrusion Detection Systems," *IEEE Software* (17:5), pp. 42-51.

Moorthy, K. S. 1988. "Product and Price Competition in a Duopoly," *Marketing Science* (7:2), pp. 141-168.

Mossberg, W. 2009. "In Browser Wars, the New Firefox Loses Some Edge," *Wall Street Journal*, July 16, Section D, p. 1.

Nadiminti, R., Mukhopadhyay, T., and Kriebel, C. H. 2002. "Research Report: Intrafirm Resource Allocation with Asymmetric Information and Negative Externalities," *Information Systems Research* (13:4), pp. 428-434.

Parker, G. G., and VanAlstyne, M. W. 2005. "Two-Sided Network Effects: A Theory of Information Product Design," *Management Science* (51:10), pp. 1494-1504.

Rescorla, E. 2005. "Is Finding Security Holes a Good Idea?," *IEEE Security and Privacy* (3:5), pp. 14-19.

Riggins, F. J., Kriebel, C. H., and Mukhopadhyay, T. 1994. "The Growth of Interorganizational Systems in the Presence of Network Externalities," *Management Science* (40:8), pp. 984-998.

Sahay, B. S., and Gupta, A. K. 2003. "Development of Software Selection Criteria for Supply Chain Solutions," *Industrial Management and Data Systems* (103:2), pp. 97-110.

SANS. 2007. "SANS Top-20 2007 Security Risks," SANS Institute (available at http://www.sans.org/top20/2007/; accessed April 1, 2010).

Scotchmer, S. 1985. "Profit Maximizing Clubs," *Journal of Public Economics* (27:1), pp. 25-45.

Shaked, A., and Sutton, J. 1982. "Relaxing Price Competition Through Product Differentiation," *The Review of Economic Studies* (49:1), pp. 3-13.

Soo Hoo, K. J. 2000. "How Much Is Enough? A Risk-Management Approach to Computer Security," working paper, Consortium for Research on Information Security and Policy, Stanford University (available at http://pointy.stanford.edu/pubs/11900/soohoo.pdf; accessed April 1, 2010).

Straub, D. W. 1990. "Effective IS Security: An Empirical Study," *Information Systems Research* (1:3), pp. 255-276.

Sullivan, D. 2006. "Viruses, Worms and Blended Threats," Chapter 3 in *The Definitive Guide to Controlling Malware, Spyware, Phishing, and Spam*, realtimepublishers.com (available at http://nexus.realtimepublishers.com/dgcmsps.php).

Symantec. 2005. "Internet Security Threat Report: Trends for January 05-June 05," Symantec Corporation, Cupertino, CA, September (available at http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_symantec_internet_security_threat_report_viii.pdf).

Tam, K. Y., and Hui, K. L. 2001. "A Choice Model for the Selection of Computer Vendors and its Empirical Estimation," *Journal of Management Information Systems* (17:4), pp. 97-124.

Tiebout, C. M. 1956. "A Pure Theory of Local Public Expenditures," *Journal of Political Economy* (64:5), pp. 416-424.

Umble, E. J., Haft, R. R., and Umble, M. M. 2003. "Enterprise Resource Planning: Implementation Procedures and Critical Success Factors," *European Journal of Operational Research* (146), pp. 241-257.

Van Dender, K. 2002. "Nash-Bertrand Competition in a Duopoly with Congestion," working paper, Department of Economics, University of California, Irvine online at http://www.economics.uci.edu/docs/2002-03/VanDender-01.pdf).

van Everdingen, Y., van Hillegersberg, J., and Waarts, E. 2000. "ERP Adoption by European Midsize Compaines," *Communcations of the ACM* (43:4), pp. 27-31.

Varian, H. 2004. "System Reliability and Free Riding,"in *Economics of Information Security*, in L. J. Camp and S. Lewis (eds.), New York: Springer, pp. 1-15.

Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D. W., and Middleton, B. 2005. "The Value of Health Care Information Exchange and Interoperability," *Health Affairs*, January 19, pp. W510-W518.

Wang, E. T. G., and Seidmann, A. 1995. "Electronic Data Interchange: Competitive Externalities and Strategic Implementation Policies," *Management Science* (41:3), pp. 401-418.

Westland, J. C. 1992. "Congestion and Network Externalities in the Short Run Pricing of Information Systems Services," *Management Science* (38:6), pp. 992-1009.

Wingfield, N. 2006. "'Worms' Turn on Apple Macs, Bigger Target as Sales Boom," *Wall Street Journal*, February 27, Section B, pp. 1-3.

Woo, S.-W., Alhazmi, O. H., and Malaiya, Y. K. 2006. "An Analysis of the Vulnerability Discovery Process in Web Browsers," in *Proceedings of the 10th IASTED International Conference on Computational and Systems Biology*, Dallas, TX, November 13-15, pp. 172-177 (available at http://www.cs.colostate.edu/~malaiya/pub/wooSEA_2006.pdf).

Yuan, L. 2006. "Hackers Learn to Think Like the Enemy," *Wall Street Journal*, March 23, Section B, pp. 3.

About the Authors

Michael R. Galbreth is an assistant professor of Management Science at the Moore School of Business, University of South Carolina, and the 2009/2010 Fulbright Enders Visiting Research Chair at McGill University. He received his Ph.D. from Vanderbilt University. His work has been published in *Production and Operations Management*, *Journal of Management Information Systems*, *Communications of the ACM*, *Decision Sciences*, *Interfaces*, *European Journal of Operational Research*, and others. Dr. Galbreth's research interests include sustainable operations and the interface between operations and other business disciplines. Prior to his academic career, he was a manager with KPMG Consulting, where he focused on enterprise systems development and implementation.

Mikhael Shor is an assistant professor of Economics at the Owen Graduate School of Management, Vanderbilt University. He received his Ph.D. from Rutgers University. He has published in *Games and Economic Behavior*, *Economic Theory, Contemporary Accounting Research, Journal of Management Information Systems,* and others. Dr. Shor's research interests include auction theory and behavioral and experimental economics.

MIS Quarterly

SPECIAL ISSUE

THE IMPACT OF MALICIOUS AGENTS ON THE ENTERPRISE SOFTWARE INDUSTRY

By: **Michael R. Galbreth**
Department of Management Science
Moore School of Business
University of South Carolina
Columbia, SC 29208
U.S.A.
galbreth@moore.sc.edu

Mikhael Shor
Department of Economics
Owen Graduate School of Management
Vanderbilt University
Nashville, TN 37240
U.S.A.
mike.shor@owen.vanderbilt.edu

Appendix

Proofs

Proof of Proposition 1

The proof of this proposition follows from Lemmas 1 to 4 presented below.

Lemma 1. *In equilibrium, (i)* $n_1 > 0$ *and (ii)* $n_2 = 0 \Rightarrow n_1 = 1$

Proof. (i) Assume that $n_1 = 0$. If consumers in the neighborhood of Firm 1 are not purchasing from Firm 2, then any price $p_1 < v_1$ will lead to positive sales and profits. Thus, assume that all consumers are purchasing from Firm 2. Firm 1 can make positive profits if there exists a $p_1 > 0$ such that $u_1(0) > u_2(0)$, which is equivalent to:

$$v_1 - p_1 > v_2 - p_2 - t - qL \equiv p_1 < v_1 - v_2 + p_2 + t + qL$$

Since $v_1 > v_2$, $t > 0$, and, in equilibrium, we must have $p_2 \geq 0$, a $p_1 > 0$ satisfying the above condition must exist. (ii)

If consumers in the neighborhood of Firm 2 are not purchasing from Firm 1, then any price $p_2 < v_2$ will lead to positive sales and profits. □

Lemma 2. *In equilibrium, when* $p_1 - p_2 \leq (v_1 - v_2) - t - qL$*, the consumer adoption decision is:* $n_1 = 1$*,* $n_2 = 0$*.*

Proof.

$$\begin{aligned}
\alpha_{12}^* &= \frac{1}{2} + \frac{1}{2t}\left[(v_1 - v_2) - (p_1 - p_2) - qL(n_1^e - n_2^e)\right] \\
&\geq 1 + \frac{qL}{2t}(1 - n_1^e + n_2^e) \\
&\geq 1 \\
\alpha_{10}^* &= \frac{1}{t}\left(v_1 - p_1 - qLn_1^e\right) \\
&\geq 1 + \frac{v_2 - p_2}{t} + \frac{qL}{t}(1 - n_1^e) \\
&\geq 1
\end{aligned}$$

Thus, by Equations (6) and (7), $n_1 = 1, n_2 = 0$ for any n_1^e, n_2^e. □

Lemma 3. *In equilibrium, when* $(v_1 - v_2) + p_2 - t - qL < p_1 \leq (v_1 + v_2) - p_2 - t - qL$*, the consumer adoption decision satisfies:* $n_1 + n_2 = 1, n_2 > 0$*.*

Proof.

$$\begin{aligned}
\alpha_{12}^* &= \frac{1}{2} + \frac{1}{2t}\left[(v_1 - v_2) - (p_1 - p_2) - qL(n_1^e - n_2^e)\right] \\
&\geq 1 - \frac{1}{t}(v_2 - p_2) + \frac{qL}{2t}(1 - n_1^e + n_2^e) \\
&\geq 1 - \frac{1}{t}(v_2 - p_2 - qLn_2^e) \\
&= \alpha_{20}^*
\end{aligned}$$

where the second inequality arises because $n_1 + n_2 \leq 1$. Similar reasoning demonstrates that $\alpha_{12}^* \leq \alpha_{10}^*$. By Equations (6) and (7), $n_1 + n_2 = 1$. To demonstrate that both firms have positive market share, we must show that $\alpha_{12}^* < 1$. Assume that $\alpha_{12}^* \geq 1$. This implies that $n_1 = 1, n_2 = 0$:

$$\begin{aligned}
\alpha_{12}^* &= \frac{1}{2} + \frac{1}{2t}\left[(v_1 - v_2) - (p_1 - p_2) - qL(n_1^e - n_2^e)\right] \\
&< 1 + \frac{qL}{2t}\left(1 - n_1^e + n_2^e\right) \\
&= 1
\end{aligned}$$

which is a contradiction. □

Lemma 4. *In equilibrium, when $p_1 + p_2 > (v_1 + v_2) - t - qL$, the consumer adoption decision satisfies: $n_1 + n_2 < 1$ and $n_2 > 0$.*

Proof. Reversing the proof for the first step of Lemma 3 provides: $\alpha_{10}^* < \alpha_{12}^* < \alpha_{20}^*$ which, by Equations (6) and (7), provides the first part of the lemma, that $n_1 + n_2 < 1$. Further, $n_2 = 1 - \alpha_{20}^*$. When $n_2 = n_2^e$, we have $n_2 = \frac{v_2 - p_2}{t + qL}$. That $n_2 > 0$ follows from Firm 2's profit maximization since any $p_2 < v_2$ results in positive profit. □

Proof of Proposition 2

Prices follow from Lemma 5 below, and market shares follow from Equations (6) and (7).

Lemma 5. *Firm i's best response for any price of Firm j is given by*

$$
\begin{array}{ll}
p_i(p_j) = \begin{cases} v_i - v_j + p_j - t - qL & \text{if} \quad q < \dfrac{v_i - (v_j - p_j) - 3t}{3L} \\ \frac{1}{2}(v_i - v_j + p_j + t + qL) & \text{if} \quad \dfrac{v_i - (v_j - p_j) - 3t}{3L} \le q \le \dfrac{v_i + 3(v_j - p_j) - 3t}{3L} \\ v_i + v_j - p_j - t - qL & \text{if} \quad \dfrac{v_i + 3(v_j - p_j) - 3t}{3L} < q \le \dfrac{v_i + 2(v_j - p_j) - 2t}{2L} \\ \frac{1}{2}v_1 & \text{if} \quad \dfrac{v_i + 2(v_j - p_j) - 2t}{2L} < q \end{cases} \\
p_i(p_j) \in \quad [0, \infty) \quad \text{if} \quad p_j \le v_j - v_i - t - qL &
\end{array}
$$

Proof. From Proposition 1 and Equations (6) and (7), we know that:

$$
n_1 = \begin{cases} 1 & \text{if} \quad p_1 - p_2 \le (v_1 - v_2) - t - qL \\ \frac{1}{2} + \frac{(v_1 - p_1) - (v_2 - p_2)}{2(t + qL)} & \text{if} \quad \begin{array}{l} p_1 - p_2 > (v_1 - v_2) - t - qL \\ p_1 + p_2 \le (v_1 + v_2) - t - qL \end{array} \\ \frac{v_1 - p_1}{t + qL} & \text{if} \quad p_1 + p_2 > (v_1 + v_2) - t - qL \end{cases}
$$

The corresponding derivatives of Firm 1's profit with respect to its price are:

$$
\frac{\partial \pi_1(p_1)}{\partial p_1} = \begin{cases} 1 & \text{Region 1} \\ & p_1 \le v_1 - (v_2 - p_2) - t - qL \\ \frac{v_1 - (v_2 - p_2) + t + qL - 2p_1}{2(t + qL)} & \text{Region 2} \\ & v_1 - (v_2 - p_2) - t - qL < p_1 \le v_1 + (v_2 - p_2) - t - qL \\ \frac{v_1 - 2p_1}{t + qL} & \text{Region 3} \\ & v_1 + (v_2 - p_2) - t - qL < p_1 \le v_1 \end{cases}
$$

The regions are numbered for ease of discourse. Profit is increasing over Region 1. Inspection of the derivatives reveals four possibilities: (i) profit is decreasing in Regions 2 and 3, (ii) profit is single-peaked in the interior of Region 2 and decreasing in Region 3, (iii) profit is increasing in Region 2 and decreasing in Region 3, and (iv) profit is increasing in Region 2 and is single-peaked in Region 3. These correspond to the first four cases in the lemma. In the fifth case, when $p_j \le v_j - v_i - t - qL$, Firm i cannot obtain positive market share at any price. Best responses for Firm 2 are obtained analogously. □

Proof of Theorems

The following lemma, defining conditions under which equilibrium profit is increasing in q, is used in the proofs of the theorems.

Lemma 6. *For $j \in \{1,2\}$,*

(i) *if* $q \leq \frac{v_1-v_2-3t}{3L}$, $\frac{d\pi_j^*}{dq} \leq 0$,

(ii) *if* $\frac{v_1-v_2-3t}{3L} < q \leq \frac{v_1+v_2-3t}{3L}$, $\frac{d\pi_j^*}{dq} > 0$,

(iii) *if* $\frac{v_1+v_2-2t}{2L} < q$, $\frac{d\pi_j^*}{dq} < 0$.

(iv) *if* $\frac{v_1+v_2-3t}{3L} < q \leq \frac{v_1+v_2-2t}{2L}$, $\frac{d\overline{\pi}_j^*}{dq} < 0$ *and* $\frac{d\underline{\pi}_j^*}{dq} < 0$.

where $\overline{\pi}_j^*$ and $\underline{\pi}_j^*$ are the highest and lowest obtainable equilibrium profits for firm j.

Proof. Equilibrium profits, $\pi_j^* = n_j p_j$, are obtained from Proposition 2.
(i) Profits are given by $\pi_1^* = v_1 - v_2 - t - qL$ and $\pi_2^* = 0$, which are nonincreasing in q.
(ii) Profits are given by: $\pi_j^* = \frac{1}{2}(t+qL)\left(1 + \frac{v_j-v_i}{3(t+qL)}\right)^2$, $i \neq j$. Differentiating,

$$\frac{d\pi_j^*}{dq} = \frac{1}{2}L\left[1 - \left(\frac{v_j-v_i}{3(t+qL)}\right)^2\right]$$

which is positive whenever: $q > \frac{v_j-v_i-3t}{3L}$
(iii) Profits are given by $\pi_j^* = \frac{v_j^2}{4(t+ql)}$ which is decreasing in q.
(iv) Profits are given by $\pi_j = \frac{(v_j-p_j)p_j}{t+qL}$. Differentiating with respect to q yields:

$$\frac{d\pi_j}{dq} = \left(\frac{v_j - 2p_j}{t+qL}\right)\frac{dp_j}{dq} - \frac{(v_j-p_j)Lp_j}{(t+qL)^2} \tag{A-1}$$

By Equation (9c), the set of prices that can yield either the highest or lowest equilibrium payoffs for Firm 1 is $p_1 \in \{\frac{1}{2}v_1, \frac{2}{3}v_1, v_1 + \frac{1}{3}v_2 - t - qL, v_1 + \frac{1}{2}v_2 - t - qL\}$. In the first two cases, $\frac{dp_1}{dq} = 0$ and Equation (A-1) is negative. In the last two cases, Equation (A-1) becomes:

$$\frac{d\pi_1(\in \{\overline{\pi}_1^*, \underline{\pi}_1^*\})}{dq} = -\frac{L}{(t+qL)^2}\left[(t+qL)^2 - (sv_2)^2 - sv_1v_2\right]$$

where $s \in \{\frac{1}{3}, \frac{1}{2}\}$. To complete the proof, we show that the part in brackets is positive.

$$\begin{aligned}(t+qL)^2 - (sv_2)^2 - sv_1v_2 &\geq (t+qL)^2 - \frac{v_2^2}{9} - \frac{v_1v_2}{3} \\ &> \left(\frac{v_1+v_2}{3}\right)^2 - \frac{v_2^2}{9} - \frac{v_1v_2}{3} \\ &= \frac{v_1}{9}(v_1 - v_2) > 0\end{aligned}$$

□

Proof of Theorem 1. (i) The condition $t \leq \frac{1}{3}(v_1 - v_2) - L$ implies that $q \leq \frac{v_1-v_2-3t}{3L}$ for all $q \in [0,1]$. By Lemma 6, we have that $\frac{d\pi_j^*}{dq} \leq 0$.
(ii) The condition is equivalent to $\frac{v_1+v_2-2t}{2L} < 0$ which implies that $q > \frac{v_1+v_2-2t}{2L}$. By Lemma 6, we have that $\frac{d\pi_j^*}{dq} < 0$.
(iii) The condition $t > \frac{1}{3}(v_1 + v_2)$ implies that $q > \frac{v_1+v_2-3t}{3L}$ for all $q \in [0,1]$. By Lemma 6, we have that $\overline{\pi}_j^*, \underline{\pi}_j^* < 0$. □

Proof of Theorem 2. By Proposition 2:

$$n_2 = 0 \text{ if } q \leq \tfrac{v_1-v_2-3t}{3L} \qquad \text{and} \qquad n_2 > 0 \text{ if } q > \tfrac{v_1-v_2-3t}{3L}$$

For part *(i)* of the theorem, to have $n_2 = 0$ when $q = 0$, we need $0 \leq \frac{v_1-v_2-3t}{3L}$. For part *(ii)*, we require that $1 > \frac{v_1-v_2-3t}{3L}$. These conditions are equivalent to:

$$\tfrac{1}{3}(v_1 - v_2) - L < t \leq \tfrac{1}{3}(v_1 - v_2)$$

□

Proof of Theorem 3. Define $\underline{q} \equiv \max[0, \frac{v_1-v_2-3t}{3L}]$ and $\overline{q} \equiv \min[1, \frac{v_1+v_2-3t}{3L}]$. Clearly, $\underline{q} \geq 0$ and $\overline{q} \leq 1$ and, by Lemma 6, profit is increasing whenever $q \in (\underline{q}, \overline{q})$. To show that $\underline{q} < \overline{q}$ we require:

$$\begin{aligned} & 1 > \tfrac{v_1-v_2-3t}{3L} && \text{and} && 0 < \tfrac{v_1+v_2-3t}{3L} \\ \equiv \quad & t > \tfrac{1}{3}(v_1 - v_2) - L && \text{and} && t < \tfrac{1}{3}(v_1 + v_2)\end{aligned}$$

which correspond to the conditions of part *(i)* of the theorem. The conditions in part *(ii)* imply

$$\begin{aligned} t \leq \tfrac{1}{3}(v_1 + v_2) - L \quad &\Rightarrow \quad \tfrac{v_1+v_2-3t}{3L} \geq 1 \\ t > \tfrac{1}{3}(v_1 - v_2) \quad &\Rightarrow \quad \tfrac{v_1-v_2-3t}{3L} < 0\end{aligned}$$

Therefore, $\frac{v_1-v_2-3t}{3L} < q \leq \frac{v_1+v_2-3t}{3L}$ which, by Lemma 6, implies profit is increasing for all q. □

We next consider the generality of the above results, by specifying a quadratic attack probability function which includes linearity as a special case.

Corollary 3 (quadratic attack probability). *Define*

$$q(n_j) \equiv q\beta n_j + q(1-\beta)n_j^2 \tag{A-2}$$

Where $\beta \in [0,1]$. *If*

(i) $t > \frac{1}{3}(v_1 - v_2)$, *and*

(ii) v_1 *and* v_2 *are sufficiently large so that every consumer derives strictly positive utility in equilibrium when* $q = 0$,

Then, both firms obtain maximal profit at some $q > 0$.

Proof. The consumer indifferent between Firm 1 and Firm 2 is found by solving:

$$\begin{aligned} & u_1(\alpha_{12}^*) = u_2(\alpha_{12}^*) \\ \equiv \quad & \alpha_{12}^* = \tfrac{1}{2} + \tfrac{(v_1-v_2)-(p_1-p_2)}{2t} - \tfrac{qL}{2t}\left[\beta(n_1^e - n_2^e) + (1-\beta)\left((n_1^e)^2 - (n_2^e)^2\right)\right] \end{aligned} \tag{A-3}$$

Since all consumers derive strictly positive utility when $q = 0$, by assumption, we must have $n_1^e + n_2^e = 1$ when q is sufficiently small. Equation (A-3) becomes:

$$\alpha_{12}^* = \tfrac{1}{2} + \tfrac{(v_1-v_2)-(p_1-p_2)}{2t} - \tfrac{qL}{2t}(2n_1^e - 1) \tag{A-4}$$

In equilibrium, it must be the case that $\alpha_{12}^* = n_1 = n_1^e$. Substituting into (A-4) yields

$$n_1 = \tfrac{1}{2} + \tfrac{(v_1-v_2)-(p_1-p_2)}{2(t+qL)} \tag{A-5}$$

For the above to have an interior solution ($0 < n_1 < 1$), we must have:

$$(v_1 - v_2) - (t + qL) < p_1 - p_2 < (v_1 - v_2) + (t + qL) \tag{A-6}$$

We will confirm these conditions shortly. First, equilibrium prices are obtained by differentiating $\pi_j = p_j n_j$ for each firm and solving the simultaneous equations. This yields:

$$p_j = \tfrac{1}{3}(v_j - v_i) + t + qL, \quad i, j \in \{1,2\}, i \neq j \tag{A-7}$$

The conditions in (A-6) are satisfied whenever $t + qL > \frac{1}{3}(v_1 - v_2)$ which is true by assumption (condition i). Combining (A-5) and (A-7) yields profits of:

$$\pi_j = \frac{\left[t + qL + \frac{1}{3}(v_1 - v_2)\right]^2}{2(t + qL)}$$

which is increasing in q whenever $t > \frac{1}{3}(v_1 - v_2)$. □

Proof of Theorem 4. Condition *(i)* guarantees that the profit function is initially increasing in q. In particular, it implies that

$$\tfrac{v_1 - v_2 - 3t}{3L} < 0 \leq \tfrac{v_1 + v_2 - 3t}{3L}$$

which, by Lemma 6, implies that $\left.\frac{d\pi_j^*}{dq}\right|_{q=0} > 0$.

If the profit function is initially nonincreasing, then there are two possibilities by Lemma 6. As q increases, either profit is initially nonincreasing, then increasing; or it is nonincreasing, then increasing, then decreasing:

(ii-a) nonincreasing-increasing: By Lemma 6, for profits to be nonincreasing when $q = 0$ and increasing when $q = 1$, the following conditions are required:

$$0 \leq \tfrac{v_1 - v_2 - 3t}{3L} \quad \Rightarrow \quad t \leq \tfrac{1}{3}(v_1 - v_2) \tag{A-8}$$

$$1 > \tfrac{v_1 - v_2 - 3t}{3L} \quad \Rightarrow \quad t > \tfrac{1}{3}(v_1 - v_2) - L \tag{A-9}$$

$$1 \leq \tfrac{v_1 + v_2 - 3t}{3L} \quad \Rightarrow \quad t \leq \tfrac{1}{3}(v_1 + v_2) - L \tag{A-10}$$

Firm 2's profit is 0 at $q = 0$, thus Firm 2's profit is maximized at $q = 1$. For Firm 1, maximum profit occurs either at $q = 0$ or $q = 1$ and, by Proposition 2, these are given by:

$$\pi_1^*|_{q=0} = v_1 - v_2 - t \tag{A-11}$$

$$\pi_1^*|_{q=1} = \tfrac{1}{2(t+L)} \left[\tfrac{1}{3}(v_1 - v_2) + t + L\right]^2 \tag{A-12}$$

Profit at $q = 1$ is strictly greater than profit at $q = 0$ when

$$L > 2\left(\tfrac{1}{3}v_1 - \tfrac{1}{3}v_2 - t\right) + \sqrt{\left(\tfrac{1}{3}v_1 - \tfrac{1}{3}v_2 - t\right)(v_1 - v_2 - t)} \tag{A-13}$$

Condition (A-9) is redundant as it is implied by (A-13). However, for both (A-13) and (A-10) to be satisfied, it must also be the case that

$$t > \tfrac{v_1^2 - 3v_2^2}{3(v_1 + v_2)} \tag{A-14}$$

Combining these conditions:

$$\begin{aligned} \tfrac{1}{3}(v_1 - v_2) \geq t > \tfrac{v_1^2 - 3v_2^2}{3(v_1+v_2)} \\ \tfrac{1}{3}(v_1 + v_2) - t \geq L > 2\left(\tfrac{1}{3}v_1 - \tfrac{1}{3}v_2 - t\right) + \sqrt{\left(\tfrac{1}{3}v_1 - \tfrac{1}{3}v_2 - t\right)(v_1 - v_2 - t)} \end{aligned} \tag{A-15}$$

(ii-b) nonincreasing-increasing-decreasing: By Lemma 6, we require:

$$0 \leq \tfrac{v_1 - v_2 - 3t}{3L} \quad \Rightarrow \quad t \leq \tfrac{1}{3}(v_1 - v_2) \tag{A-16}$$

$$1 > \tfrac{v_1 + v_2 - 3t}{3L} \quad \Rightarrow \quad t > \tfrac{1}{3}(v_1 + v_2) - L \tag{A-17}$$

Maximum profit can occur either at $q = 0$ or at $q = \frac{v_1+v_2-3t}{3L}$ which is the point above which profit is again decreasing in q. Firm 1's profit is given by:

$$\pi_1^*\big|_{q=\frac{v_1+v_2-3t}{3L}} = \tfrac{2v_1^2}{3(v_1+v_2)} \tag{A-18}$$

This profit exceeds the profit at $q = 0$ given by (A-11) if $t > \frac{v_1^2 - 3v_2^2}{3(v_1+v_2)}$ which is precisely the condition in (A-14). Combining these conditions, we have:

$$\begin{aligned} \tfrac{1}{3}(v_1 - v_2) \geq t > \tfrac{v_1^2 - 3v_2^2}{3(v_1+v_2)} \\ L > \tfrac{1}{3}(v_1 + v_2) - t \end{aligned} \tag{A-19}$$

Taking the union of parameter ranges in (A-15) and (A-19) yields condition *(ii)* in the theorem.

□

Proof of Theorem 5. We solve for the subgame perfect equilibrium. The consumer indifferent between Firm 1 and Firm 2 is given by

$$\alpha_{12}^* = \frac{1}{2} + \frac{1}{2t}\left[(v_1 - v_2) - (p_1 - p_2) - (q_1 n_1^e - q_2 n_2^e)L\right] \tag{A-20}$$

Following steps similar to Propositions 1 and 2, under the conditions in the theorem, we have $n_1 > 0, n_2 > 0, n_1 + n_2 = 1$ for all q_1 and q_2. Since, in equilibrium, $n_i^e = n_i$, we have

$$n_1 = \frac{(v_1 - v_2) - (p_1 - p_2) + t + q_2 L}{2t + (q_1 + q_2)L} \tag{A-21}$$

For given q_1 and q_2, firms maximize $\pi_i(p_i) = p_i n_i$ which yields the first order conditions:

$$p_i = \frac{1}{2}\left(v_i - v_j + p_j + t + q_j L\right) \quad i, j \in \{1, 2\}, i \neq j \tag{A-22}$$

From these, the equilibrium prices and market shares are given by:

$$p_1 = \frac{1}{3}(v_1 - v_2) + t + \frac{1}{3}(q_1 + 2q_2)L \qquad p_2 = \frac{1}{3}(v_2 - v_1) + t + \frac{1}{3}(q_2 + 2q_1)L \tag{A-23}$$

$$n_1 = \frac{(v_1 - v_2) + 3t + (q_1 + 2q_2)L}{6t + 3(q_1 + q_2)L} \qquad n_2 = 1 - n_1 \tag{A-24}$$

In the first stage, firms select q_i to maximize $p_i n_i - c_i(q_i)$. For $i, j \in \{1, 2\}, i \neq j$, profit as a function of q_i, q_j is given by:

$$\pi_i(q_i, q_j) = \frac{((v_i - v_j) + 3t + (q_i + 2q_j)L)^2}{9(2t + (q_i + q_j)L)} - c_i(q_i) \tag{A-25}$$

Taking the derivative with respect to q_i yields:

$$\frac{d\pi_i(q_i, q_j)}{dq_i} = [v_j - v_i + t + q_i L] \left(\frac{L(v_i - v_j + 3t + (q_i + 2q_j)L)}{9(2t + (q_i + q_j)L)^2} \right) - c_i'(q_i) \tag{A-26}$$

The fraction term is strictly positive since $t > \frac{1}{3}(v_1 - v_2)$. Also, $c_i'(q_i) \leq 0$.

(i) For an equilibrium to satisfy $q_1 = q_2 = 0$, it must be the case that the derivative of each firm's profit function at $q_1 = q_2 = 0$ must be non-positive. Consider firm 2. The expression in the brackets becomes $[v_1 - v_2 + t] > 0$. Therefore, the derivative is positive.

(ii) For $q_i = 1$ to be a dominant strategy, the derivative of profit must be increasing for all q_i, q_j. This requires that the expression in the square brackets be positive, which is true whenever $t > v_1 - v_2$. □

Proof of Theorem 6. The consumer indifferent between Firms 1 and 2 ($u_1 = u_2$) is given by

$$\alpha_{12}^* = \frac{1}{\Delta} \left[(p_1 - p_2) + qL(n_1^e - n_2^e) \right] \tag{A-27}$$

By assumption, $n_1 + n_2 = 1$ and therefore $n_1 = 1 - \alpha_{12}^*$. In equilibrium, $n_j^e = n_j$, implying

$$n_1 = \frac{\Delta - (p_1 - p_2) + qL}{\Delta + 2qL} \tag{A-28}$$

Maximizing each firm's profit, $n_j p_j$, with respect to p_j and substituting yields the expressions in (12) and (13). As both p_2 and n_2 are increasing in q, the result holds for Firm 2. For Firm 1, profits are given by $p_1 n_1 = \frac{1}{9} \frac{(2\Delta + 3qL)^2}{\Delta + 2qL}$. Differentiating with respect to q yields the result. □