Scarcity of user information and the link between computer security and reliability[1]

Galina A. Schwartz
University of California, Berkeley
Peter Honeyman
University of Michigan, Ann Arbor
Ari Van Assche
HEC Montréal

Abstract

This paper studies manufacturer incentives to invest in the improvement of reliability and security of a software system when (i) reliability and security failures are caused by the same errors in the development of the software components and (ii) naive users find it too costly to distinguish between these two classes of system failures. We trace the effects of these informational imperfections and discuss how the resulting supply and demand externalities affect manufacturer investments. When users cannot distinguish between reliability and security failures and investment in system security is driven by the weakest link, the standard for optimal due care then depends on manufacturer characteristics with respect to both security and reliability. In this case, imposition of a due care standard based solely on reliability or on security becomes socially suboptimal.

JEL Codes: D82, L14, D40.

Key words: computer security, computer reliability, information inefficiencies, free-riding, externalities

[1] Updated version: May 18, 2009. We are grateful to Weston Andros Adamson, J. Bruce Fields, Niels Provos, Dug Song, and Terence P. Kelly for insights on the technical details of software production. We thank Jean Walrand, John Musaccio and Hal Varian for useful comments.

1. Introduction

This paper studies manufacturer incentives to invest in software system reliability and security when users are unable to distinguish between failures caused by security or reliability faults. By far, most users lack the expert knowledge required to make this distinction, and therefore find it too costly to identify (i) the manufacturer responsible for a system failure and (ii) whether a system failure is caused by a reliability failure (i.e., a non-malicious programming error) or a security failure (i.e., a malicious attack by a malevolent party). As a result, manufacturer incentives to invest in system reliability and security are socially suboptimal due to public good features on both the supply and demand side.

Our paper is related to a growing literature that has considered the incentives for the provision of system reliability or system security.[2] Varian (2004) approaches system reliability as a problem of public good provisioning and analyzes the ensuing free-rider problem for various functional forms. He investigates possibilities to alleviate the resulting underinvestment in system reliability through fines, due care standards, and legal liability. Anderson (2001), and Kunreuther and Heal (2003) focus on the incentives to invest in system security. Anderson (2001) and Anderson and Moore (2006) connect with principal-agent theory arguments to demonstrate that when the parties charged with protecting systems are not the parties who bear the costs of breached security, security is suboptimally low.[3] Kunreuther and Heal (2003) and Heal and Kunreuther (2004) consider network environments where the security choices of one agent affect the risks faced by others. Their setup is applicable to software system security since the risk that a hacker attacks a system depends not only on a specific manufacturer's investment in improving security, but also on the actions of other manufacturers of the system. They demonstrate that such environments are also prone to free-riding, i.e., the agents' privately optimal investments in system security are suboptimally low from a social standpoint.

[2] See Soohoo (2000) and Schechter (2004) for a quantitative approach to the role of economic incentives in securing cyber-space. Also see Anderson and Moore (2006); Anderson et al. (2008) for a recent literature review.

[3] In the literature addressing the principal-agent problem (see Tirole (1999)), informational imperfections (costs) due to the presence of principal-agent conflict lead in many cases to environments mathematically equivalent to ones with free-riding.

Our paper extends the existing literature by considering manufacturer incentives to invest in system reliability and security jointly. This is an important research question because (i) reliability and security failures are often caused by the same errors in the design of the software components and (ii) it is too costly for naive users to distinguish between both types of system failures. We argue that it is therefore necessary to address investment incentives into reliability and security jointly.[4]

Consistent with the existing literature, Section 2 shows that manufacturers underinvest because system reliability and security depend not only on the investment of an individual manufacturer, but also on the actions of the other component producers. We call this supply side inefficiency *manufacturer information inefficiency*; the literature frequently refers to such inefficiencies as *free-riding*. In addition, we show that informational imperfections on the demand side due to untenable user costs to distinguish between reliability and security failures lead to further inefficiencies. To our knowledge, ours is the first attempt to model both types of inefficiencies simultaneously. Our joint analysis of reliability and security leads to policy recommendations that differ from the recommendations of prior models.

In Section 3, we apply our framework by using specific functional forms for system security and reliability. Consistent with the information technology literature, we assume that the expected number of security failures in a system depends solely on the parameters of the bottleneck manufacturer, i.e. that manufacturer whose bugs have the highest likelihood to create a security failure. We model the system's expected number of reliability failures as a weighted sum of the number of bugs in the individual products of which the system is comprised. We show that in systems with homogeneous products and a relatively high probability for the weakest link's bugs to create a security (rather than a reliability) failure, all manufacturers invest in system reliability and security by matching their component security to that of the weakest link. However, in systems with highly heterogeneous products, only a "strongest link" manufacturer will invest in system reliability and security. Our analysis thus provides insight

[4] We have also stressed this point in Honeyman et al. (2007).

into the patterns of manufacturer investment in system reliability and security, depending on the parameters of products of which the system is comprised.

The remainder of this paper is organized as follows. In Section 2, we outline the relevant technological environment and present the general model. In Section 3, we use specific functional forms to find the equilibrium of the game and demonstrate the intuition of our model. In Section 4, we summarize and conclude.

2. Model

2.1. Environment of the Model

Modern software system typically consist of hundreds of distinct software products produced by dozens of manufacturers. Using such a software system thus involves the concurrent consumption of several software products. User demand for a software system depends on numerous parameters, such as technical characteristics, reliability, security, and the legal environment. In this paper, we treat all system parameters except reliability and security as exogenous. We state the following definitions:

Definition 1. *A* ***software system failure*** *is a malfunction in a user's software system due to an error or weakness in the design, implementation, or operation of a system.*

Definition 2. *A software system failure is classified as a* ***security failure*** *if it is caused by malicious unauthorized access to the user's system. Otherwise, it is classified as a* ***reliability failure****.*

For example, according to Definition 1, a buffer overflow is a system failure since it causes the system to operate incorrectly. According to Definition 2, the buffer overflow is a security failure if it is caused by a malicious attack by hackers, but it is a reliability failure if it is caused by a non-malicious programming or operational error.[5]

For the intuition behind Definitions 1 and 2, consider a hypothetical fully secure world, where no security threat exists. For example, let all users be authorized to access everything on the network. Then, no unauthorized access

[5] The 1988 Morris worm attack, the 2002 Slapper worm attack that infected thousands of Linux- based web servers, and the 2003 Slammer and Blaster worm attacks on Windows PCs all exploited buffer overflow vulnerabilities.

is possible. In such a world, all system failures will be classified as reliability failures.

Next, assume that there are two disjoint fully secure networks (as described above) with users belonging to network N1 or N2, but not to both. Here, too, all system failures will be classified as reliability failures. Now, let us connect these two networks, and suppose that network N1 user U1 employs his web access to gain unauthorized access to network N2 resources. According to our Definition 2, a system failure on N2 caused by U1's unauthorized access is classified as a security failure. Moreover, if in the process of achieving unauthorized access to N2 resources, U1 causes a failure on N1, this failure will also be classified as a security failure.

This suggests that system reliability and security ought to be analyzed jointly since reliability and security failures result from the same bugs and cannot necessarily be distinguished by a user. We introduce the concept of "robustness," which reflects both reliability and security features of a software system:[6]

Definition 3. *Software system* ***robustness*** *is inversely related to the number of system failures.*

Three types of agents affect system robustness: software manufacturers, users, and hackers. A manufacturer can increase system robustness by investing in the enhancement of the security and reliability of his own software component. Users can affect system robustness through demand. Hackers can hamper system robustness by attacking system weaknesses.

In this paper, we focus on manufacturer incentives to invest when users lack information about causes of a specific system failure. We ignore other factors by assuming that users have identical preferences for system robustness and that their systems are equally susceptible to hacking. We do not model hacker incentives, but treat them as exogenous.

Manufacturer incentives to invest in system robustness are affected by two types of informational deficiencies faced by the users. Due to the high cost of information acquisition, users find it too costly to (i) determine which manufacturer's software component has caused a system failure and (ii) whether the

[6] The term software system robustness closely matches the term "information assurance" from the computer science literature (see for example Galin (2003).)

system failure was caused by a reliability or security failure. A number of legal and technological factors contribute to these informational deficiencies. On the technological side, they include the complexity of typical network systems, unavailability of proprietary source code for many software products, legislation preventing the disclosure of flaws in commercial software (e.g., the Digital Millennium Copyright Act or DMCA), and hackers' actions to cover their tracks. On the legal side, software manufacturers' lack of legal liability tends to nullify user incentives to collect information and resolve the informational deficiency.

In our model, the production of a software system requires M inputs (software components), each produced by a separate manufacturer. We assume that the system's price is determined by user willingness to pay, which depends on the number of expected system failures. The manufacturers divide the gross revenue according to an exogenous sharing rule. In this respect, our setup follows agency literature, where the players' surplus sharing is determined from their Nash bargaining, and player bargaining powers are exogenous.

While the first type of informational deficiency is well-established, the existing literature has paid scant attention to the second type. We therefore emphasize the conjecture that is central for our model:

Conjecture 1. *It is too costly for users to distinguish between system reliability failures and systems security failures.*

While numerous measures of software vulnerability exist (for example US government maintains the "National Vulnerability" database), and enormous amounts of security related data are collected by private parties, the current consensus of security researchers is that usage of this data is limited. In many cases, only obsolete data is easily available, see Anderson et al. (2008) review.

Also, our paper importantly limits its attention to naïve users, who are unaware of many existing data sources. Moreover, even when an educated user is aware that data sources exist, it is prohibitively costly (time wise) to use these resources. Judging by our personal experience, it is too costly.

Perhaps, it will be more precise to assume that a certain fraction of (but not all) users is subject to such informational constraints. Still, we suggest that this fraction of uninformed users is close to 100 percent. We believe that only security professionals regularly use the databases to find out security characteristics of specific applications. Most rank-and-file users, from whom the bulk of demand originates, are ignorant of these tools. Indeed, in practice, such users have no habit of checking with these databases when they are shopping for a new computer system.

Conjecture 1 has an important ramification for user demand: users base their willingness to pay on the joint measure of system robustness, not on the separate measures of system reliability and security.

To emphasize the relevance of system failures to consumer choices, let us make an analogy with auto purchases. The Yugo was more prone to failure than a comparable Honda, which influenced consumer demand and manufacturer pricing. Indeed, at present, Apple's market share is increasing relative to the PC despite an unfavorable cost differential. Anecdotal evidence suggests that user preference for a system with fewer failures is part of the impetus driving PC users to switch to the Mac.

2.2. Outline of the Model

We consider a one-shot game G of M players (manufacturers). [7] Consumers are not players: they take no actions and are described by their demand.

Demand Side

Let f^r and f^s denote the expected number of reliability and security failures for a system, and f the expected total number of system failures:

$$f = f^r + f^s.$$

According to Definition 3, f characterizes system robustness: a system gets more robust when f decreases. Due to Conjecture 1, user willingness to pay for the system should depend on the expected total number of system failures f, but not on f^r and f^s separately. Thus, we infer:

Corollary 1. *When it is prohibitively costly for users to distinguish between reliability and security failures, their willingness to pay for a system depends solely on the expected total number of system failures f.*

[7] The assumption of a non-repeated game reflects the current technological reality where rapid changes make even *ex post* costs of information revelation prohibitively high. Thus, informational deficiencies of today's highly dynamic technological environment prevent manufacturers from forming durable reputation for system robustness.

We assume that users are identical and their systems are equally susceptible to hacking. Let $p(f)$ denote the representative user's willingness to pay for the system with f expected failures. We assume that $p(f)$ is decreasing and concave in the number of system failures:

$$p' = \frac{\partial p(f)}{\partial f} < 0, \quad p'' = \frac{\partial p^2(f)}{\partial f^2} \leq 0.$$

Simply put, a representative user prefers a more robust system. When the total number of expected failures decreases, a user's willingness to pay drops more for each additional reduction in the number of failures. We assume the market size for software system as exogenous, i.e., unaffected by manufacturer choice of system robustness. Since users are identical, and aggregate market size exogenous, we normalize the market size to 1, in which case aggregate willingness to pay for the system for all users is equal to the willingness for an individual user: $p(f)$.

Supply Side

The system is comprised of products (components) from M heterogeneous manufacturers. Each manufacturer can improve system robustness by investing in fixing his product's bugs. Let $\mathbf{x} = x_1, ..., x_M$ be the vector of system bugs, with its m-th component x_m denoting the number of bugs for the m-th manufacturer, and $x_m \in (0, \infty)$. For any system, the expected number of reliability and security failures are functions of $\mathbf{x}$:

$$f(\mathbf{x}) = f^r(\mathbf{x}) + f^s(\mathbf{x}),$$

with $f(\mathbf{x})$ weakly increasing and convex in x_m:

$$f' = \frac{\partial f(\mathbf{x})}{\partial x_m} \geq 0, \qquad f'' = \frac{\partial^2 f(\mathbf{x})}{\partial x_m^2} \geq 0. \tag{1}$$

That is, when the number of bugs x_m of the m-th manufacturer increases, the entire system becomes weakly less robust; when a manufacturer's product is more buggy (i.e., at higher x_m), an increase in x_m leads to an increased number of additional system failures.

A manufacturer can improve system robustness by investing in fixing bugs. Let the m-th component q_m of the vector $\mathbf{q} = q_1, ..., q_M$ denote the m-th manufacturer's investment in improving system robustness. We assume that this investment is irreversible and affects only his own bugs. The number of bugs of the m-th manufacturer is weakly decreasing in his investment:

$$\frac{\partial x_m}{\partial q_m} \leq 0, \qquad \frac{\partial^2 x_m}{\partial (q_m)^2} \geq 0. \tag{2}$$

Let $\mathbf{a} = (\mathbf{q}, \mathbf{x})$ denote the vector of manufacturer actions, with its m-th component being the m-th manufacturer actions. Manufacturers choose their actions simultaneously and independently to maximize expected profit Π_m:

$$\Pi_m = \max_{a_m = (q_m, x_m)} \left[S_m - r^m q_m \right], \tag{3}$$

where S_m is the m-th manufacturer's surplus, and r^m is his return on investment in the outside option.

We do not directly model manufacturer competition with potential entrants, who could offer applications substitutable for the m-th manufacturer one. The presence of substitutes is likely to affect manufacturer surplus sharing, perhaps resulting in lower surplus shares for the manufactures whose applications have highly competitive substitutes. To simplify, in our model the ownership sharing is exogenous.

The surplus S_m is equal to:

$$S_m = \alpha^m p(f),$$

where α^m is the m-th manufacturer's ownership share of gross aggregate surplus $p(f)$. We treat ownership shares as exogenous. Clearly,

$$\sum_{m=1}^{M} \alpha^m = 1,$$

because gross aggregate surplus S equals user aggregate willingness to pay

$$S = \sum_{m=1}^{M} S_m = p(f).$$

To summarize, we model manufacturer incentives to invest in system robustness as a game G of M players, in which they act simultaneously and independently, and each chooses actions $a_m = (q_m, x_m)$ to maximize his profit given by equation (3). For the given functions P and f**,** the game G has $2 \times M$ parameters: α^m, r^m, where $m = 1, ...M$. All parameters of the game are common knowledge. The functions p and $\mathbf{x}$ are well-behaved, i.e., they are continuous and two times continuously differentiable for $q_m, x_m \in (0, \infty)$. We assume that players coordinate on Pareto efficient subgame perfect Nash equilibrium, and use such an equilibrium as the solution concept for our game.[8] Let the superscript * denote equilibrium outcomes and payoffs. We use superscripts to indicate parameters, and subscripts to indicate choice variables. Using equation (1) and (2), robustness f can be connected to investments q_m, and we have the following:

Proposition 1. *The expected number of system failures is non- increasing and convex in the m-th manufacturer's investment in system robustness:*

$$\frac{\partial f(\mathbf{x})}{\partial q_m} \leq 0, \qquad \frac{\partial^2 f(\mathbf{x})}{\partial (q_m)^2} \geq 0.$$

Proof. Follows from combining equations (1) and (2). ■

From Conjecture 1, users base their demand on f, and not on f^r and f^s separately. As a result, a manufacturer's return to investment in system robustness depends on its impact on f. Thus, from Proposition 1, S could be expressed as a function of q_m.

Proposition 1 permits us to express manufacturer optimization in the game G as his choice of optimal q_m, with x_m uniquely determined by q_m. Once we have proven Proposition 1, vector $\mathbf{x}$ may appear an unnecessary complication of the notation: indeed, x_m can be recovered from q_m. We want to stress that $\mathbf{x}$ is an essential feature of our setup, and it would be impossible to present our results without $\mathbf{x}$. Although the functions f^r and f^s may behave very differently with

[8] We do not prove an existence of an equilibrium of our game for a general case. In Section 3, we do demonstrate equilibrium existence for a specific functional form of f^r and f^s, and a linear relation between x_m and q_m.

$\mathbf{x}$, naturally, both depend on the same bugs – $\mathbf{x}$. If instead we had introduced f^r and f^s as functions of $\mathbf{q}$, it would be hard to justify the point that investment decisions about fixing reliability and security flaws are interdependent.

In Section 3, we express f as a function of q_m, relying on concrete specifications of f^r and f^s, for which dependence on x_m closely follows the existing literature. We use Brady et al. (1999); Anderson (2002), to provide a technology driven justification of our chosen relationship between x_m and q_m. The resulting dependence of f on q_m is complex (equation (A-1)), and hardly intuitive, despite the fact that we derive it from standard assumptions about reliability and security failures and about costs of reducing such failures.

2.3. Information Inefficiencies

We pointed out in Section 2.1 that users face two informational deficiencies: they find it too costly to (i) determine which manufacturer's software component has caused a system failure and (ii) whether the system failure is caused by a reliability or security failure. We refer to the first informational imperfection as *manufacturer information inefficiency,* and to the second as *hacker information inefficiency.*

Manufacturer Information Inefficiency

When it is too costly for the user to determine which software product caused the system failure, manufacturers are subject to information inefficiency which causes a standard free-riding problem. We label the related inefficiencies as *manufacturer information inefficiency.* To demonstrate this, one can compare optimal investments of individual manufacturers and of a social planner.

We assume perfect price discrimination of the users, and zero consumer surplus as a result. Thus, in our model, social surplus coincides with aggregate manufacturer surplus. The social planner's objective V is to maximize aggregate manufacturer surplus:

$$V = \max_{\mathbf{a}} \left[\sum_{m=1}^{M} \Pi_m(\mathbf{a}) \right] = \max_{\mathbf{a}} \left[\sum_{m=1}^{M} S_m(\mathbf{a}) - \mathbf{rq} \right], \qquad (4)$$

where $\mathbf{r} = r^1, ..., r^M$ is a vector of manufacturer outside options.

By comparing the first-order conditions that can be derived from equations (3) and (4), it is straightforward to see that socially optimal marginal return on investment is lower than that for the individual manufacturer. Thus, manufacturers invest less than is socially optimal due to an inherent manufacturer free-rider problem.

Hacker Information Inefficiency

When Conjecture 1 holds, users do not distinguish whether a system failure is security or reliability driven. Thus, their willingness to pay for any two systems with equal expected total number of failures is identical. In reality, however, security and reliability failures may have different effects on the user utilities because expected utility losses can differ for reliability and security failures. With complete information about failure's origin, user willingness to pay depends on security and reliability failures separately. This implies that the informational imperfections highlighted by Conjecture 1 lead to an additional inefficiency. We call this inefficiency *hacker information inefficiency* because it is due to the user's inability to distinguish whether a failure is due to hackers or manufacturers.

Let $\hat{G}$ denote the game with perfectly distinguishable security and reliability failures, and let "hat" denote its equilibrium outcomes and payoffs. We can formulate the following proposition:

Remark 1. *For any equilibrium of the subgame $\hat{G}$, with investment restricted to equilibrium investment of the game G, consumer willingness to pay for the system is at least as high as in the equilibrium of the game G.*

Proof. In the game $\hat{G}$, user willingness to pay for the system $\hat{P}$ is the function of two variables, f^r and f^s: $\hat{P}(f^r, f^s)$. In the game G reliability and security failures are indistinguishable, so user willingness to pay for two systems with the same total number of expected failures f is equal to their willingness to pay for the less costly of the two systems:

$$P(f) = \min_{f^r, f^s} \hat{P}(f^r, f^s), \text{ such that } f^r + f^s = f.$$

Thus, we have:

$$P(f) \leq \hat{P}(f^r, f^s), \text{ for any } f^r, f^s \text{ such that } f^r + f^s = f.$$

■

It follows from Remark 1 that aggregate manufacturer profits are at least as high as in the game G. Thus, resolving hacker information inefficiency improves aggregate manufacturer profits even if manufacturer information inefficiency remains intact.

Note that *hacker information inefficiency* can be present even when there is no *manufacturer information inefficiency*, i.e., when the system is produced by a social planner. Similarly, *manufacturer information inefficiency* can be present even when there is no *hacker information inefficiency.*

Policy Implications

In general, standard policy recommendations aiming to alleviate manufacturer information inefficiency do not address the hacker information inefficiency problem. This is sub-optimal for two reasons. First, it implies that an important source of inefficiencies – hacker information inefficiency – remains. Second, in the presence of hacker information inefficiency, the traditional policy recommendations addressing manufacturer information inefficiency might become ineffective. For example, a standard policy recommendation to resolve manufacturer information inefficiency is to impose limited legal liability on the agent responsible for the system failure. In the presence of hacker information inefficiency, however, courts face difficulty in determining whether a manufacturer or a hacker is responsible for system failure. This limits the usability of manufacturer legal liability for resolving manufacturer information inefficiency.

In Section 3, we apply our framework by considering specific functional forms for system security and reliability. This allows us to derive an optimal due care level based on $\mathbf{x}$ (or $\mathbf{q}$), i.e., we show that the social optimum can be achieved without imposition of separate reliability and security due care levels.

3. Applying the Model

In the remainder of the paper, we adopt a specific functional form for the function f to illustrate our model in a concrete environment. Since reliability and security failures are driven by different usage patterns, one expects that functional forms for f^r and f^s differ. Hackers take advantage of a product with the greatest potential of creating a system failure. Accordingly, we assume:

$$f^s(\mathbf{x}) = \max_{m=1}^{M} \omega^m x_m, \tag{5}$$

where $\omega^m < 1$ is the probability that the m-th manufacturer's product induces a security failure. Thus, the number of security failures of the system is determined by the least secure manufacturer, i.e., by the manufacturer with the largest expected number of security failures. Our assumption that "hackers take advantage of a product with greatest potential of creating a system failure" (aka "the weakest link") is made to illustrate the point. Although it is reasonable in many cases, which makes it popular in the literature (see Varian (2004), Hausken (2006), Grossklags et al. (2008)), it is clearly not universally applicable; see for example, Kunreuther and Heal (2002, 2003); Heal and Kunreuther (2004); Hofmann (2007) for other functional forms of interdependent security.

We assume that the system's expected number of reliability failures is a weighted sum of the number of bugs in the individual products from which the system is comprised:

$$f^r(\mathbf{x}) = \sum_{m=1}^{M} \theta^m x_m, \tag{6}$$

where $\theta^m < 1$ is the normalized incidence of bugs in the m- th manufacturer's product that induce a reliability failure. Varian (2004) refers to the cases described by equations (5) - (6) as "weakest link" and "total effort" functional forms. Equation (6) captures the fact that reliability failures tend to be isolated for each system product, and that the total number of reliability failures is a sum of reliability failures of individual manufacturers.

Brady et al. (1999); Anderson (2002) use reliability growth models to demonstrate that when the number of bugs is sufficiently large, reduction in the mean time between failures (MTBF) becomes proportionate to effort invested. We use their results to justify our assumption that the number of bugs that the m-th manufacturer fixes is proportional to his investment:

$$x_m = \bar{x}^m - \gamma^m q_m, \text{ and } \gamma^m > 0, \tag{7}$$

where $\bar{x}_m$ denotes the m-th manufacturer's component-specific number of bugs when he invests zero to improve system robustness. We can say that higher γ^m reflects lower manufacturer costs of improving his product robustness.

We assume that at zero manufacturer investment $\mathbf{q} = \mathbf{0}$, all products are equally secure, for any two manufacturers m and n:

$$\omega^m \bar{x}^m = \omega^n \bar{x}^n. \tag{8}$$

To simplify the analysis, let:

$$\lim_{f \to 0} P'(f) = 0, \tag{9}$$

i.e., if the prospect of system failure is negligible, users are unwilling to pay extra for improved system robustness. The latter assumption permits us to avoid the unrealistic corner solution where it is optimal for at least one manufacturer to fix all his bugs.

Equations (5) – (9) permit us to prove that the equilibrium of the game G exists. To assure the uniqueness of the equilibrium, we impose that for any two manufacturers m and n:

$$\frac{r^m}{\gamma^m \alpha^m \theta^m} \neq \frac{r^n}{\gamma^n \alpha^n \theta^n}. \tag{10}$$

Intuitively, if the cost benefit ratios of a pair of manufacturers are identical, there will be multiple equilibria with identical robustness.

Next, we define three levels of system robustness that can occur in equilibrium: $\bar{f}$, f_w and f_t. Let $\bar{f}$ denote the level of system robustness when no manufacturers invest ($\mathbf{q} = \mathbf{0}$ and $\bar{\mathbf{x}} = (\bar{x}^1, ..., \bar{x}^M)$):

$$f(\bar{\mathbf{x}}) = \bar{f} = \bar{f}^r + \bar{f}^s,$$

where from equations (5) and (6):

$$\bar{f}^r = \sum_m^M \theta^m \bar{x}^m \qquad \text{and} \qquad \bar{f}^s = \max[\omega^m \bar{x}^m].$$

Let f_t and f_w denote the levels of system robustness for which the following equations hold:

$$-P'(f_t) = \min_{m=1}^M \left[\frac{r^m}{\gamma^m \alpha^m \theta^m} \right], \tag{11}$$

and

$$-P'(f_w) = \max_{m=1}^M \left[\frac{r^m}{\gamma^m \alpha^m (\theta^m + \omega^m)} \right]. \tag{12}$$

We call f_t *the strongest link system robustness* since it corresponds to the level of system robustness at which the manufacturer with the lowest marginal cost-benefit ratio of investing in system robustness is at his profit-maximizing level of investment. Intuitively, at this level of system robustness, the manufacturer with the lowest cost-benefit ratio is the only one with incentives to contribute in the improvement of system robustness. Thus, we will call him the strongest link and identify the parameters associated with him with superscript t.

We call f_w *the weakest link system robustness* since it corresponds to the level of system robustness at which the manufacturer with the highest marginal cost-benefit ratio is as his profit-maximizing investment. Intuitively, at this level of system robustness, the manufacturer with the highest marginal cost-benefit ratio has less incentive to invest in system robustness than others. We will call him the weakest link and identify the parameters associated with him with superscript w.

By using the three levels of system robustness, we characterize the equilibrium of the game G:

Theorem 1. *There exists a unique equilibrium of game G. The equilibrium number of system failures is equal to* $\min\{\bar{f}, f_t, f_w\}$.

Proof. See Appendix. ■

The proof of Theorem 1 gives three different scenarios of equilibrium, which differ in their structure and equilibrium levels of robustness $\bar{f}$, f_w or f_t.

Scenario 1 corresponds to $\min\{\bar{f}, f_t, f_w\} = \bar{f}$. In Scenario 1, in equilibrium, no manufacturer invests in system robustness: $\mathbf{q}^* \equiv 0$ and $f^* = \bar{f}$. We call

Scenario 1 the *no investment equilibrium.*

Scenario 2 corresponds to $\min\{\bar{f}, f_t, f_w\} = f_t$. In Scenario 2, only the strongest link makes positive equilibrium investment, and $f^* = f_t$, where

$$-P'(f^*) = \frac{r^t}{\gamma^t \alpha^t \theta^t}. \tag{13}$$

This scenario mimics Varian (2004) “total effort” prototype case, in which only the strongest link invests to improve system reliability, and his investment q_t^* can be found from equation (13). We call Scenario 2 the *reliability-driven equilibrium.*

Lastly, Scenario 3 corresponds to $\min\{\bar{f}, f_t, f_w\} = f_w$. In Scenario 3, all manufacturers' equilibrium investments are positive, and $f^* = f_w$, where:

$$-P'(f^*) = \frac{r^w}{\gamma^w \alpha^w (\theta^w + \omega^w)}, \tag{14}$$

In this scenario, every manufacturer other than the weakest link invests to match the weakest link's security level. Then, in equilibrium, each manufacturer investment is positive, and his product is as secure as the weakest link product:

$$\omega^m x_m^* = \omega^w x_w^*. \tag{15}$$

Equations (7) and (15) permit us to express q_m^* via q_w^* :

$$q_m^* = \frac{\omega^w \gamma^w}{\omega^m \gamma^m} q_w^*, \tag{16}$$

to express f^* as a function of q_w^*:

$$f^* = \bar{f} - \omega^w \gamma^w q_w^* \left[\sum_m \frac{\theta^m}{\omega^m} + 1 \right],$$

and to use equation (14) to find q_w^*. The equilibrium investments q_m^* of all other manufacturers can then be calculated from equation (16). In this scenario, our model thus reverts to Varian (2004) “weakest link ” prototype case. We call this the *security-driven equilibrium.*

3.1. Parameter Analysis

In the environment described by equations (5) - (6), every manufacturer (other than the weakest and the strongest links) either invests nothing or just enough so that the number of her expected security failures matches the weakest link manufacturer's number of failures. Using equations (11) and (12), we identify the likely parameters of the weakest and the strongest link:

Remark 2. *Ceteris paribus, the strongest link manufacturer is likely to have a higher α, γ and θ, and a lower r. Ceteris paribus, the weakest link manufacturer is likely have a lower α, γ, θ and ω, and a higher r.*

To understand Remark 2, we can analyze the role of manufacturer security and reliability characteristics (ω^m and θ^m) on the identification of the strongest and weakest links. To simplify, assume for a moment that all manufacturer parameters other than ω^m and θ^m are identical: $r^m \equiv r, \gamma^m \equiv \gamma$ and $\alpha^m \equiv \alpha$. Then, from equation (12), the weakest link is the manufacturer with the lowest $\theta^m + \omega^m$. Thus, the weakest link is the manufacturer whose bugs are the least likely to create a system failure. This is because the weakest link has a smaller benefit from investing in the improvement of system robustness than other manufacturers due to the low probability of system failures induced by his product. From equation (11), the strongest link is the manufacturer with the highest θ^m. In other words, he is the manufacturer whose bugs are the most likely to create a reliability failure. Intuitively, this is because the strongest link has a larger benefit from investing in the improvement of system robustness than other manufacturers due to a high probability of failures induced by his product.

We can conduct a similar analysis to identify the role of ownership share α^m. Assume that manufacturers differ only in α^m. Then, the manufacturer with the lowest ownership share α^m is the weakest link, since he has the lowest incentive to invest in the improvement of system robustness. On the other hand, the manufacturer with the highest α^m is the strongest link, since he has the most incentive to invest in the improvement of system robustness.

Finally, we can use Remark 2 to address how manufacturer parameters determine which equilibrium Scenario will occur. From Theorem 1, there is a *security-driven equilibrium* if $f_w \leq f_t$.[9] This will occur if:

$$\frac{\omega^w}{\theta^w} \geq \frac{\frac{r^w}{\gamma^w \alpha^w \theta^w}}{\frac{r^t}{\gamma^t \alpha^t \theta^t}} - 1. \tag{17}$$

The right-hand side of equation (17) is nonnegative since, from equation (11), the weakest link's cost-benefit ratio of investing into system reliability is (by definition) larger than that of strongest link. Equation (17) implies that there is a *security-driven equilibrium* if (i) the strongest and weakest links have similar cost- benefit ratios in investing in system reliability, and (ii) the probability that the weakest link's bugs will create a security failure relative to a reliability failure is large. If the weakest and strongest links have very different cost-benefit ratios and if the weakest link's bugs are relatively more likely to create reliability failures, then there is a *reliability-driven equilibrium.*

3.2. Social Optimum and Due Care

We can derive the socially optimal outcome by solving the social planner's problem given by equation (4). From the first-order conditions, the socially optimal robustness $f^{\circledast}$ guarantees that the following equation holds:

$$-P'(f^{\circledast}) = \sum_m \frac{r^m}{\gamma^m(\theta^m + \omega^m)}. \tag{18}$$

From equations (7) and (8), in a socially optimal outcome, manufacturer investments should be connected with each other, similar to equation (15). Thus, without loss of generality, we can express $q_m^{\circledast}$ via $q_1^{\circledast}$:

$$q_m^{\circledast} = \frac{\omega^1 \gamma^1 q_1^{\circledast}}{\omega^m \gamma^m}, \tag{19}$$

Substituting equation (19) into equations (5) - (6) lets us express $f^{\circledast}$ as a function of $q_1^{\circledast}$:

$$f^{\circledast} = \bar{f} - \omega^1 \gamma^1 q_1^{\circledast} \left[\sum_m \frac{\theta^m}{\omega^m} + 1 \right]. \tag{20}$$

Equation (20) can then be combined with equation (18) to derive $\mathbf{q}^{\circledast}$.

[9] In the remaining analysis, we ignore the case of the *no investment equilibrium.*

A comparison of equation (18) (which describes social optimum) with equations (13) or (14) (which describe individually optimal outcomes) gives:

$$f^{\circledast} \leq f^{*} \text{ and } q_m^{\circledast} \leq q_m^{*}.$$

Thus, manufacturers invest less than is socially optimal due to an inherent manufacturer free-rider problem.

Individual optimization will be socially optimal only if manufacturers have identical cost-benefit ratios $\frac{r^m}{\gamma^m \alpha^m (\theta^m + \omega^m)}$. If manufacturers are not identical, the social optimum can be attained through the imposition of a "due care level"of $\mathbf{q}_{\mathbf{m}}^{\circledast}$.[10] In this case, any manufacturer who invests below the "due care level" is required to compensate others for their losses from system failures.

It is important to note that the imposition of a "due care level" of investment is feasible despite the presence of hacker information inefficiency. This is because the "due care level" of investment is a function of total system failures, and not of reliability and security failures separately.

4. Conclusion

This paper analyzes manufacturer incentives to invest in software system reliability and security when (i) reliability and security failures are caused by the same bugs, and (ii) users are unable to distinguish between security and reliability failures due to prohibitive costs of differentiating such failures. In Section 2, we trace the suboptimality of manufacturer incentives to invest to two distinct free riding problems, which we call manufacturer information inefficiency and hacker information inefficiency. Our results suggest that the presence of a hacker *information inefficiency* problem might invalidate traditional policies recommended to alleviate manufacturer *information inefficiency.*

In Section 3, we apply our model using specific functional forms consistent with the information technology literature. For system security, we opt for the prototype case of "weakest link "since hackers tend to take advantage the most vulnerable components to attack a system. For system reliability, we opt for the

[10] A formal proof is identical to Varian (2004).

prototype case of “total effort” since it captures the focal feature that reliability failures are relatively isolated from the network. We infer that in systems with homogeneous products and relatively high probability that the weakest link’s bugs will create a security failure, all manufacturers invest positively and each matches the security of her component to that of the weakest link. Otherwise, only the strongest link manufacturer invests in system robustness.

To sum up, our model traces reliability and security failures to the same source – software bugs. We emphasize user inability to distinguish between security and reliability failures, and model the interplay of system reliability and security. While our assumptions can be found in the literature individually, we are not aware of other analysis that make these assumptions simultaneously.

Appendix

Proof of Theorem 1

Using equations (5) - (7), we rewrite the m-th manufacturer objective as:

$$\Pi_m = \max_{q_m} \left[\alpha^m P \left(\sum_{m}^{M} \theta^m \left(\bar{x}^m - \gamma^m q_m \right) + \max_{m=1}^{M} \omega^m \left(\bar{x}^m - \gamma^m q_m \right) \right) - r q_m \right]. \tag{A-1}$$

Let $\bar{f}$ denote system robustness when $\mathbf{q} = \mathbf{0}$, that is: $\bar{f} = \bar{f}^r + \bar{f}^t$, where from equations (5) and (6), $\bar{f}^r$ and $\bar{f}^t$ are:

$$\bar{f}^r = \sum_{m}^{M} \theta^m \bar{x}^m \text{ and } \bar{f}^t = \max\{\omega^m \bar{x}^m\}.$$

Let f_m^t and f_m^w denote the respective solutions of equations:

$$-P'(f_m^t) = \frac{r^m}{\gamma^m \alpha^m \theta^m} \tag{A-2}$$

and

$$-P'(f_m^w) = \frac{r}{\gamma^m \alpha^m (\theta^m + \omega^m)}. \tag{A-3}$$

From Proposition 1, for each manufacturer (and given investments of other manufacturers), there exists a unique investment q_m^t (and q_m^w) that this manufacturer invests to achieve a specific number of system failures f_m^t (or f_m^w).

Clearly, ceteris paribus, for each m, the number of system failures that solves equation (A-3) is lower than the respective number that solves equation (A-2):

$$f_m^w < f_m^t.$$

We define f_t and f_w as:

$$f_t = \min_{m=1}^{M} f_m^t \text{ and } f_w = \max_{m=1}^{M} f_m^w;$$

we call the manufacturer with the lowest f_m^t the *strongest link*, and the highest f_m^w the *weakest link*. For the strongest link:

$$-P'(f_t) = \min_{m=1}^{M} \left[\frac{r^m}{\gamma^m \alpha^m \theta^m} \right], \tag{A-4}$$

and for the weakest link:

$$-P'(f_w) = \max_{m=1}^{M} \left[\frac{r^m}{\gamma^m \alpha^m (\theta^m + \omega^m)} \right]. \tag{A-5}$$

Intuitively, the strongest link is the manufacturer whose A-2) corresponds to the most robust system, and the weakest link whose (A-3) – to the least robust system. The remainder of the proof is by construction. We construct an equilibrium whose uniqueness follows from properties of the underlying functions. We distinguish three scenarios, each leading to a different equilibrium configuration.

Scenario 1: If $\min[\bar{f}, f_t, f_w] = \bar{f}$, then for any manufacturer, his marginal benefit from investing at $f = \bar{f}$ is lower than his marginal cost. Since in our game each manufacturer's marginal benefit from investment increases with f, and his cost is constant (due to linearity of (7)), at any $f < \bar{f}$, positive investment is suboptimal. Thus, in equilibrium, no manufacturer invests. The only equilibrium is $\mathbf{q}^* = \mathbf{0}$ and $f^* = \bar{f}$, and from (A-1) we have: $P^* = P(\bar{f})$.

Scenario 2: If $\min[\bar{f}, f_t, f_w] = f_t$, only the strongest link manufacturer in equilibrium chooses a positive level of investment. No other manufacturer invests because the marginal benefit of investing at f_t is smaller than the marginal cost. Thus, the strongest link's first order condition provides that in equilibrium:

$$-p'(f^*) = \min_{m=1}^{M} \frac{r^m}{\gamma^m \alpha^m \theta^m} = \frac{r}{\gamma^t \alpha^t \theta^t}.$$

From the properties of P and f, we have a unique equilibrium in which:

$$f^* = f_t,$$

and the strongest link manufacturer is the only one with $q_t^* > 0$.

Scenario 3: If $\min[\bar{f}, f_t, f_w] = f_w$, each manufacturer invests so that his expected number of security failures matches that of the weakest link manufacturer. To demonstrate this, we observe that the strongest link's marginal benefit of investing in system reliability is smaller than its marginal cost when $f_w < f_t$. As a result, all manufacturers match their investments to that of the weakest link. Since $f_w < \bar{f}$, all manufacturers choose positive investments that solve the following system of equations:

$$\omega^m \left(\bar{x}^m - \gamma^m q_m\right) = \omega^w \left(\bar{x}^w - \gamma^w q_w\right) : m \neq w \tag{A-6}$$

and:

$$-P'(f^*) = \frac{r}{\gamma^w \alpha^w (\theta^w + \omega^w)}. \tag{A-7}$$

From the properties of P and f, a unique equilibrium exists with $f^* = f_w$.

With the weakest link determined by (A-5), we use (A-6) to express q_m via q_w:

$$q_m = \frac{\omega^w \gamma^w q_w}{\omega^m \gamma^m}. \tag{A-8}$$

Substituting equation (A-8) in equation (A-1) and using equations (5), (6) and (7) provides q_w^* as a solution of the following equation:

$$f^* = \bar{f} - \omega^w \gamma^w q_w \left(\sum_{m=1}^{M} \frac{\theta^m}{\omega^m} + 1 \right). \tag{A-9}$$

Linearity of equation (7) and the properties of the function P assure the uniqueness of q_w^*, and the conditions of Scenario 3 assure its existence. From the properties of the functions P and f, the solution (A-7) - (A-9) provide equilibrium investments of other manufacturers, the existence and uniqueness of which are immediate. Thus, our construction yields a unique equilibrium for Scenario 3.

From the analysis of Scenarios 1 – 3, there exists a unique equilibrium for any underlying parameters of the game, which completes the proof. ■

References

Anderson, R., 2001. Why information security is hard an economic perspective. In: Proc. 17th Ann. Computer Security Applications Conf. Assoc. for Economic Service, pp. 358–365.

Anderson, R., 2002. Security in open versus closed systems - the dance of boltzmann, coase and moore. In: In Conference on Open Source Software Economics. MIT Press, pp. 1–15.

Anderson, R., Böehme, R., Clayton, R., Moore, T., Jun. 25-28 2008. Security economics and european policy. In: Proceedings of WEIS'08. Hanover, USA.

Anderson, R., Moore, T., 2006. The economics of information security. Science 314 (5799), 610–613.
URL http://www.sciencemag.org/cgi/content/abstract/314/5799/610

Brady, R. M., Anderson, R. J., Ball, R. C., 1999. Murphy's law, the fitness of evolving species, and the limits of software reliability. Computer Laboratory Technical Report 471, Cambridge University.
URL http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-471.pdf

Galin, D., 2003. Software qurality assurance: from theory to implementation. Addison-Wesley.

Grossklags, J., Christin, N., Chuang, J., 2008. Secure or insure?: a game-theoretic analysis of information security games. In: WWW '08: Proceeding of the 17th international conference on World Wide Web. ACM, New York, NY, USA, pp. 209–218.

Hausken, K., 2006. Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. Information Systems Frontiers 8 (5), 338–349.

Heal, G., Kunreuther, H., Aug. 2004. Interdependent security: A general model. NBER Working Papers 10706, National Bureau of Economic Research.

Hofmann, A., 2007. Internalizing externalities of loss prevention through insurance monopoly: an analysis of interdependent risks. Geneva Risk and Insurance Review 32 (1), 91–111.

Honeyman, P., Schwartz, G., Assche, A. V., 2007. Interdependence of reliability and security. In: Proceedings of WEIS'07. Pittsburg, PA.

Kunreuther, H., Heal, G., Apr. 2002. Interdependent security: The case of identical agents. NBER Working Papers 8871, National Bureau of Economic Research.

Kunreuther, H., Heal, G., 2003. Interdependent security. Journal of Risk and Uncertainty 26 (2-3), 231–49.

Schechter, S. E., 2004. Computer security strength and risk: a quantitative approach. Ph.D. thesis, Cambridge, MA, USA, adviser-Smith, Michael D.

Soohoo, K., 2000. How much is enough? a risk-management approach to computer security. Ph.D. thesis, Stanford University.

Tirole, J., July 1999. Incomplete contracts: where do we stand? Econometrica 67 (4), 741–782.
URL http://ideas.repec.org/a/ecm/emetrp/v67y1999i4p741-782.html

Varian, H. R., 2004. System reliability and free riding. In: in Economics of Information Security, Kluwer. Kluwer Academic Publishers, pp. 1–15.