

Can Competitive Insurers improve Network Security?

Nikhil Shetty, Galina Schwartz, Jean Walrand

Electrical Engineering

and Computer Sciences

University of California, Berkeley

Berkeley, California 94720

Email: {nikhils, schwartz, wlr}@eecs.berkeley.edu

Abstract—The interdependent nature of security on the Internet causes a negative externality that results in under-investment in technology-based defences. Previous research suggests that, in such an environment, cyber-insurance may serve as an important tool not only to manage risks but also to improve the incentives for investment in security. This paper investigates how competitive cyber-insurers affect network security and user welfare. We utilize a general setting, where the network is populated by identical users with arbitrary risk-aversion and network security is costly for the users. In our model, a user’s probability to incur damage (from being attacked) depends on both his security and the network security.

First, we consider cyber-insurers who cannot observe (and thus, affect) individual user security. This asymmetric information causes moral hazard. If an equilibrium exists, network security is always worse relative to the no-insurance equilibrium. Though user utility may rise due to a coverage of risks, total costs to society go up due to higher network insecurity.

Second, we consider insurers with full information about their users’ security. Here, user security is perfectly enforceable (zero cost). Each insurance contract stipulates the required user security and covers the entire user damage. Still, for a significant range of parameters, network security worsens relative to the no-insurance equilibrium. Thus, although cyber-insurance improves user welfare, in general, competitive cyber-insurers may fail to improve network security.

I. INTRODUCTION

Today, the Internet serves as the primary communication platform for both individuals and businesses. At present, due to the nearly universal connectivity, a huge amount of wealth is accessible online and the Internet has become a preferred destination for criminals. However, the Internet, which was originally conceived to be an academic network, has failed to address many of these security problems. Due to the ease of accessibility and programmability of end-systems, unwary end users’ computers are routinely infected with malware. Network vulnerabilities are easy to exploit and infected computers are used for future crimes, resulting in an interdependent security environment.

Technology-based defense and enforcement solutions are available, but a consensus among security researchers [1] is that the existing security problems cannot be solved by technological means alone. Indeed, these security problems

primarily result from misaligned incentives of the networked parties with respect to their security. Users under-invest in security since they are not accountable for the true societal costs of their actions, which causes a negative externality.

Existing research [2]–[7] indicates that *risk management* in general and cyber-insurance in particular are potentially valuable tools for security management. In this paper, we focus on the effects of cyber-insurers on network security and user welfare, in a general setting with interdependent security and asymmetric information (between users and insurers). We believe that these features of the environment induce socially suboptimal network security, and complicate the management of security risks.

In our model, all users are identical. Their wealth is identical and they suffer identical damage if cyber-attack on them is successful. The user’s probability of being attacked depends on both the *user security level* and the *network security level*, which individual users take as given. Thus, there is an externality due to which, individually optimal user security level is lower than the socially optimal one.

First, we investigate the effects of information asymmetry in the presence of interdependent security. Though our model allows to study both moral hazard (when insurers are not aware of user security levels) and adverse selection (when insurers cannot distinguish different user types), in this paper, we address only moral hazard. In this case, we find that cyber-insurance fails to improve the network security level though it may improve user utility, if an equilibrium exists. Next, we assume no information asymmetry between the insurers and the users. We demonstrate that user utility is higher with insurance, but surprisingly, even in this case, the network security level is not necessarily higher. On reverse, in many cases, network security worsens with insurers.

The paper is organized as follows. In Section II, we describe the related work. In Section III, we propose and analyze the base model. In Section IV, we add competitive insurers to our base model, and consider two cases: with non-contractible individual security levels, and with required individual security level included into user’s insurance contract. In Section V, we discuss the intuition behind our results, and in Section VI, summarize our findings and conclude. The technical details are relegated to Appendix.

II. RELATED WORK

We build on the seminal ideas about the role of information in insurance markets [8],¹ which we combine with the ideas of interdependent security originated by [10]–[12].²

Previous work such as [2] focus on the effects of correlated risks on cyber-insurance. However, in our setting, we emphasize that interdependent security is a focal feature, which shapes the incentives for Internet security [7], [15]. Although security interdependence is present in other contexts (such as terrorist attacks [20]), network security is especially prone to these effects because many millions of users are interlinked.

The authors in [7] investigate cyber-insurance with a simple two-user model of security interdependence in the presence of a single insurer. They suggest that a mandatory cyber-insurance will provide users the necessary incentives to adopt better security practices and improve network security as a whole. Their model does not incorporate the fact that the Internet involves a large number of players and cyber-insurance, in general, will not be provided by a monopolist (whether socially benevolent or not). We model security interdependence for a large number of users and present the analysis in the case where cyber-insurers compete with each other. Our results indicate that [7] does not directly extend to cases with multiple users and competitive cyber-insurers.

In [21], we propose a simple model, which the current paper extends to general functions. In [21], we use specific functional forms to illustrate most of the results. Here, we prove that our old results extend to any network of identical risk-averse users, with arbitrarily risk-aversion and costly network security, where user cost of improving his security level is characterized by an arbitrary function with decreasing returns to security investment.

III. MODEL

We consider a network populated by N homogeneous (i.e., identical) users, each of whom possesses a wealth $W > 0$. In the absence of network security problems, user i utility U_i is:

$$U_i = f(W),$$

where the function f is increasing and concave ($f' > 0$, and $f'' \leq 0$), reflecting that user wealth W has a positive but decreasing marginal benefit for the user.

In the presence of network security problems, we assume that a user i incurs a monetary damage $D \in (0, W)$ when he is successfully attacked, and we let p_i denote the probability of successful attack. We assume that the probability p_i depends on two factors: the *security level* $s_i \in [0, 1]$ chosen by user i and the *network security level* $\bar{s} \in [0, 1]$, which depends on the security choices of all network users. We define the network security level $\bar{s}$ as the average security level in the network:

$$\bar{s} = \frac{1}{N} \sum_{i=1, \dots, N} s_i.$$

Further, we assume N to be large, i.e., each user has a negligible effect on $\bar{s}$ and takes the network security level as given. Then, we define the probability p_i of a successful attack on user i as

$$p_i = (1 - s_i)(1 - \bar{s}),$$

where the second term $(1 - \bar{s})$ can be viewed as the probability of an attack in the network and the first term $(1 - s_i)$ can be viewed as the probability of success of such an attack on user i .

We assume that, for any user i , achieving individual security s_i entails a cost $h(s_i)$. We let h be an increasing convex function ($h', h'' \geq 0$), with $h(0) = 0$ representing a completely insecure user and $h(1) = \infty$ characterizing the costs required to maintain a “perfectly secure” system. The intuition is that user security costs increase with security, and that improving security level imposes an increasing marginal cost on the user. Additionally, for expositional convenience, we impose $h'(0) = 0$, to ensure positive user investments $s_i > 0$.

Thus, the expected user utility can be expressed as

$$U_i = (1 - p_i) \cdot f(W) + p_i \cdot f(W - D) - h(s_i). \quad (1)$$

To simplify the exposition, we introduce the vulnerability of player i , $v_i = 1 - s_i$ and the network *vulnerability* level $\bar{v} = 1 - \bar{s}$. Then, the expected utility of user i is:

$$U_i = (1 - v_i \bar{v}) \cdot f(W) + v_i \bar{v} \cdot f(W - D) - g(v_i), \quad (2)$$

where $g(v_i) = h(1 - v_i)$. This gives us: $g' \leq 0$, $g'' \geq 0$, and $g(1) = 0$, $g'(1) = 0$ and $g(0) = \infty$.

A. Social Optimum

We assume that, in the social optimum, aggregate user utility is maximized. In Appendix, we show that the socially optimal security level is identical for all users: $v_i = v$. Then, $\bar{v} = v$, and from (2), we have:

$$U^{soc} = (1 - v^2) \cdot f(W) + v^2 \cdot f(W - D) - g(v). \quad (3)$$

In any social optimum, $\frac{\partial U^{soc}}{\partial v} = 0$, from which we have:

$$2v^{soc} [f(W) - f(W - D)] = -g'(v^{soc}), \quad (4)$$

and since $\frac{\partial^2 U^{soc}}{\partial v^2} < 0$, the socially optimal vulnerability level is unique.

B. Nash Equilibrium

We assume that all parameters are known to users. As discussed above, a user takes the network vulnerability $\bar{v}$ as given and chooses his vulnerability v_i to maximize his utility given by (2). Taking the partial derivative of (2) with respect to v_i , and equating to zero, $\frac{\partial U_i}{\partial v_i} = 0$, we obtain:

$$\bar{v} [f(W) - f(W - D)] = -g'(v_i). \quad (5)$$

From the properties of the function g , the solution of equation (5) is unique, from which vulnerability choice is identical for all users. Hence, in equilibrium, all users have identical

¹See [9] for the literature review.

²See also [3], [13]–[19]. This list is by no means exhaustive.

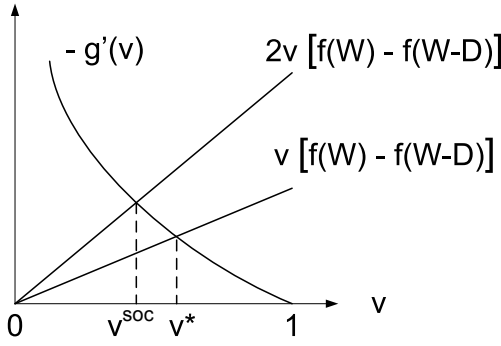


Fig. 1. Nash Equilibrium Vs Social Optimum

security (vulnerability) level, which we denote by v^* . Then, $\bar{v} = v^*$ and the following holds:

$$v^* [f(W) - f(W - D)] = -g'(v^*). \quad (6)$$

As in the case of social optimum, equilibrium vulnerability level is unique. Thus, in equilibrium, user security investments are identical and positive. Optimal investment increases when the damage D increases relative to wealth W . From (2) and (6), the equilibrium expected utility is:

$$U^* = f(W) + v^* g'(v^*) - g(v^*). \quad (7)$$

Comparing (4) and (6), we observe that since the LHS in (4) grows twice as fast as in (6) (see Fig. 1), we must have the following proposition:

Proposition 1: Individually optimal user security is strictly positive, and it is strictly lower than the socially optimal one ($v^{soc} < v^*$ or $s^{soc} > s^*$).

The expected per user loss due to network insecurity is:

$$(v^*)^2 D,$$

which is higher than the expected per user loss in the social optimum: $(v^{soc})^2 D$. Thus, in our model, users under-invest in security relative to a socially optimal level and this negative externality results in higher losses to society. In the next section, we will add competitive cyber-insurers to our base model and study how the presence of cyber-insurer affects network security.

IV. INSURANCE

Equilibrium is defined in a way similar to [8], where insurance equilibrium is examined in the markets with adverse selection. Each insurer offers a single insurance contract in a class of admissible contracts, or does nothing. A Nash equilibrium is defined as a set of admissible contracts such that: i) all contracts offered at least break even; ii) taking as given the contracts offered by incumbent insurers (those offering contracts) there is no additional contract which an entrant-insurer (one not offering a contract) can offer and make a strictly positive profit; and iii) taking as given the set of

contracts offered by other incumbent insurers, no incumbent can increase its profits by altering his offered contract.

The literature referred to such contracts as “competitive,” because entry and exit are free, and because no barrier to entry or scale economies are present. Thus, we will consider insurance firms (insurers), who are risk neutral and compete with each other. In addition to these equilibrium conditions, we assume that individual insurers cannot affect the network vulnerability, and thus, take it as given.

Let ρ be the premium charged to a user and L be the amount of loss covered by the insurer. Let user vulnerability be v and network vulnerability be $\bar{v}$. The user pays the premium both when he is attacked and when he is not, but is covered a loss L when the attack occurs successfully. Thus, with probability $v\bar{v}$, the user is successfully attacked and receives utility $[f(W - D + L - \rho) - g(v)]$ and with probability $(1 - v\bar{v})$, he obtains utility $[f(W - \rho) - g(v)]$. Denoting $U(v, \bar{v}, \rho, L)$ as the corresponding expected user utility,

$$U(v, \bar{v}, \rho, L) = (1 - v\bar{v}) \cdot f(\tilde{W}) + v\bar{v} \cdot f(\tilde{W} - \tilde{D}) - g(v), \quad (8)$$

where

$$\tilde{W} = W - \rho \text{ and } \tilde{D} = D - L.$$

The utility in (8) coincides with the no-insurance case if $\rho = 0, L = 0$. When v is identical for all users, we have $\bar{v} = v$, and:

$$U(v, v, \rho, L) = (1 - v^2) \cdot f(\tilde{W}) + v^2 \cdot f(\tilde{W} - \tilde{D}) - g(v). \quad (9)$$

A. Non-contractible User Security

In this subsection, we assume that insurers do not know, and have no control over user security level. This occurs when it is impossible (too costly) for the insurers to monitor the users' vulnerability v . Hence, the contract offered by an insurer will be of the form (ρ, L) , i.e., the insurer sets the premium and the amount of coverage, and stipulates that no additional coverage can be purchased.

Note that the user is free to choose his required vulnerability here. Hence, users will choose the vulnerability level to maximize their utility, given the network security level. Thus, in the presence of competitive insurers, users choose which contract to buy, if any, and the corresponding vulnerability that maximizes their utility. In equilibrium, no user wishes to deviate from his equilibrium contract to any other contract or to not buying any insurance. We denote the equilibrium values in this non-contractible security case by the superscript $\dagger$.

1) *Social Planner:* We assume that the social planner's objective is to maximize aggregate user utility with the constraint that the equilibrium contracts must not be loss-making. When social planner offers some contract(s), the users optimal choices could be described as if they play a game as in Section III-B, but with wealth $\tilde{W} = W - \rho$ and damage $\tilde{D} = D - L$. In Appendix, we show that a social planner will offer a single contract (ρ, L) only. Then, user optimal choice is given by (6):

$$v^{\dagger soc} [f(\tilde{W}) - f(\tilde{W} - \tilde{D})] = -g'(v^{\dagger soc}). \quad (10)$$

To maximize aggregate user utility, the social planner's contract must solve the following optimization problem:

$$\max_{\rho, L} U(v^{\dagger soc}, v^{\dagger soc}, \rho, L),$$

subject to (10) and budget constraint $\rho - (v^{\dagger soc})^2 L \geq 0$. In Appendix, we show that all users buy this insurance. No user deviates to not buying, when other users have bought the insurance.

With the insurance provided by a social planner, user utility is higher, but, the vulnerability $v^{\dagger soc}$ is also higher than in the no-insurance Nash equilibrium:

$$v^{\dagger soc} > v^*. \quad (11)$$

2) *Competitive Insurance*: Insurers offer contracts (ρ, L) , and users maximize their utility by choosing the contracts and a corresponding preferred security levels, given the network security. In Appendix, we show that in any equilibrium, the following proposition holds:

Proposition 2: With competitive insurers present, and non-contractible user security, in equilibrium, the security is always worse than the security in the no-insurance Nash equilibrium ($\bar{v}^\dagger > v^*$ or $\bar{s}^\dagger < s^*$).

Thus, we demonstrated that although insurers may allow users to reach a higher utility, the network security is strictly lower with insurers. The favorable effect of insurers on user utility is not free of cost for the society. The presence of insurers negatively impacts network security level, which increase the losses from network insecurity. Expected per user loss due to the insurers' presence increases relative to the no-insurance Nash equilibrium by $\Delta^\dagger$ given by:

$$\Delta^\dagger = [(\bar{v}^\dagger)^2 - (v^*)^2] D.$$

This is what one expects when insurers cannot monitor user security level. Since user risk is covered, users tend to under-invest in security. Next, we study the case where the insurer has perfect information about, and can perfectly enforce the security of his insured users.

B. Contractible User Security

Here, we assume that the insurers can monitor their insured users' vulnerability v at zero cost. Thus, we permit the contracts that specify user's required v . Let (v, ρ, L) be a contract that sets the premium ρ , the coverage L , and requires user vulnerability to be at most v . We denote the equilibrium values in this contractible security case by the superscript $\ddagger$.

1) *Social Planner*: We assume that the social planner's objective is to maximize aggregate user utility with the constraint that the equilibrium contracts must not be loss-making. In Appendix, we demonstrate that the social planner offers a single contract (v, ρ, L) only. Thus, $\bar{v} = v$, and to maximize total utility, the contract offered by the social planner must be a solution to the following optimization problem:

$$\max_{v, \rho, L} U(v, v, \rho, L), \text{ s.t. } v^2 L \leq \rho.$$

In Appendix, we show that the solution $(v^{\ddagger soc}, \rho^{\ddagger soc}, L^{\ddagger soc})$ is unique and satisfies:

$$\begin{aligned} (v^{\ddagger soc})^2 L^{\ddagger soc} &= \rho^{\ddagger soc} \\ L^{\ddagger soc} &= D \\ 2v^{\ddagger soc} D f'(W - (v^{\ddagger soc})^2 D) &= -g'(v^{\ddagger soc}). \end{aligned} \quad (12)$$

Thus, the optimal contract makes no profit and offers full coverage. The social planner choice $v^{\ddagger soc}$ is given by (12).

2) *Competitive Insurance*: In this case, insurers offer contracts (v, ρ, L) . In equilibrium, if the network vulnerability is $\bar{v}$, then all equilibrium contracts must yield equal utility $U(v, \bar{v}, \rho, L)$ for the user. If there exists a contract (v, ρ, L) that an insurer can offer and improve this user utility, it is preferred by the users and users will deviate and buy that contract. Hence, in equilibrium, the contracts chosen by the insurers must maximize $U(v, \bar{v}, \rho, L)$. In Appendix, we prove the following proposition:

Proposition 3: With competitive insurers present, and security level contractible, in equilibrium, profits are zero ($v^{\ddagger 2} L^\ddagger = \rho^\ddagger$), and full coverage is offered ($L^\ddagger = D$). The equilibrium contract is unique and in this equilibrium, the security is always worse than what will be chosen with a socially optimum insurance ($v^\ddagger > v^{\ddagger soc}$). Also, compared to the no-insurance equilibrium, security is worse ($v^\ddagger > v^*$) except when the damage D is a small fraction of the wealth W . Users are strictly better off with insurers than when no insurers are present ($U^\ddagger > U^*$).

When security level is observable by the insurers, insurer presence allows to improve user welfare, but not necessarily the network security. Unless the damage is a small fraction of the wealth, with cyber-insurance, expected per user loss from network insecurity increases compared to the no-insurance Nash equilibrium by $\Delta^\ddagger$, where:

$$\Delta^\ddagger = [(\bar{v}^\ddagger)^2 - (v^*)^2] D.$$

Thus, for a significant range of parameters, the losses to society may increase when insurance is available.

V. DISCUSSION

Our basic model captures the effects of interdependent security on network security. It highlights the incentive misalignment for end-user security investments, and captures a well known gap between individually and socially optimal user incentives for security (free-riding effect). We use this model to investigate the effects of the presence of competitive cyber-insurance on user utility and network security level.

We consider competitive cyber-insurance under two cases - one in which information asymmetry between the insurer and the user is present and the other in which it is absent. When this information asymmetry is present, the insurer is unable to observe and hence enforce any contract based on the user security level. Thus, we consider the two extreme cases (worst and best respectively) for cyber-insurance under the current network structure. We expect a real-life cyber-insurance to be

intermediate between the two, reflecting the fact that cyber-insurers may have some information about user vulnerability but may not know/monitor user security level perfectly.

When information asymmetry is present, we show that the moral hazard problem becomes relevant. Here, users are insured and their risks are covered. No conditions are imposed on user security, because even if they were, they cannot be enforced. In this case, users tend to further under-invest in security and the network security worsens in the presence of cyber-insurers, as is expected. Though the total user utility of the network has increased due to user risk being covered, the total damages (costs) to society have increased due to the lower security levels.

When no information asymmetry is present between users and insurers, we show that competitive cyber-insurers cover the complete user risk. However, even in this case, due to competitive pressures, in equilibrium, these insurers choose a security level that is lower than the socially optimum level. In this case, cyber-insurers free-ride on the security levels of their competitors to bring down the network security level. In fact, for a significant range of parameters, the network security level may be lower than the security level without insurance. Thus, again, though user utility goes up, the total damages to society may increase.

Note that in the second case, there is no information asymmetry between the insurers and the users. However, there is still information asymmetry between the insurers themselves since they cannot coordinate on their contracted security levels. Insurers could have reached a better equilibrium via cooperation, but this is unlikely because they cannot ensure that a deviant insurer will not try to attract more users by having a lax user contract. This free-riding may be difficult to detect and prevents improvement in the network security level.

Our assumption of identical users is simplistic, and does not hold in the actual Internet. But, adding user and insurer heterogeneity to our setting only increases informational asymmetries. When insurers could separate users of different types, our results should continue to hold for every user sub-type present in a heterogeneous market. When insurers are unable to distinguish between users with different types, missing markets are likely, as [8] demonstrate. And, the presence of different insurer types brings adverse selection problems, such as the “lemon problem” [22], also leading to missing markets.

To conclude, we suggest that, for cyber-insurance to be an effective tool for improvement of network security, we need to solve two information asymmetries, not one. The traditional information asymmetry between insurers and users may be tackled by better monitoring and enforcing security best practices (via software certification techniques, for example). However, the information asymmetry between insurers also needs to be resolved. One way this may be achieved is via a mandate on the required user security in insurance contracts. Lower security interdependence may also be achieved by lowering or degrading inter-insurer connectivity. However, such solutions may not be socially viable.

VI. CONCLUSION

In this paper, we investigate the effects of competitive cyber-insurers on network security and welfare. We highlight the impact of asymmetric information in the presence of network externalities and address the effects of interdependent security on the market for cyber-risks. The existing literature attributes cyber-insurance a significant role in cyber-risk management; it especially emphasizes positive effects of cyber-insurance market on security incentives. We find that, on reverse, the presence of competitive cyber-insurers, in general, weakens user incentives to improve security.

Though insurance improves the utility for risk-averse users, it does not serve as an incentive device for improving security practices. Indeed, insurance is a tool for risk management and redistribution, not necessarily a tool for risk reduction. To sum up, we argue that a combination of interdependent security and information asymmetries hinder cyber-insurance from performing the function of a catalyst for improvement of network security.

ACKNOWLEDGMENTS

The authors would like to thank the members of the NetEcon group at UC Berkeley, specially Mark Felegyhazi, John Musacchio, Libin Jiang, Assane Gueye and Jiwoong Lee for their helpful comments and suggestions.

APPENDIX

Social Optimum with No Insurance

In the social optimum, the goal is to maximize aggregate user utility given by

$$U^{agg} = \sum_{i=1 \dots N} [(1 - v_i \bar{v})f(W) + v_i \bar{v}f(W - D) - g(v_i)],$$

where $\bar{v} = \frac{\sum_{i=1 \dots N} v_i}{N}$. To optimize this expression, we take the partial derivative w.r.t. v_j for some $j \in 1, \dots, N$ and equate to zero:

$$\begin{aligned} \frac{\partial U^{agg}}{\partial v_j} &= 0 \\ \sum_{i=1 \dots N} \left[\frac{v_i}{N} \{f(W - D) - f(W)\} \right] + \dots \\ \dots \bar{v} \{f(W - D) - f(W)\} - g'(v_j) &= 0 \\ 2\bar{v} \{f(W) - f(W - D)\} &= -g'(v_j). \end{aligned} \quad (13)$$

Since (13) is identical for all j , all users must be assigned an identical vulnerability to maximize the aggregate utility.

Proposition 2

Social Planner: First, we show that the social planner will offer a single contract in equilibrium only. Assume the reverse, and let there exist an equilibrium with network security $\bar{v}$, and at least two equilibrium contracts (ρ_1, L_1) and (ρ_2, L_2) . Without loss of generality, let $v_1 > \bar{v} > v_2$.

Then, for any user with contract (ρ_1, L_1) optimal v_1 is the same as in the base model with $\tilde{W}_1 = W - \rho_1$ and $\tilde{D}_1 =$

$D - L_1$, and thus v_1 is identical for all users with contract (ρ_1, L_1) and is given from (5):

$$\bar{v} [f(\tilde{W}_1) - f(\tilde{W}_1 - \tilde{D}_1)] = -g'(v_1). \quad (14)$$

Using (5), all these users' utility U_1 can be written as

$$U_1 = f(\tilde{W}_1) + v_1 g'(v_1) - g(v_1), \quad (15)$$

Similarly, for all users with contract (ρ_2, L_2) we have:

$$U_2 = f(\tilde{W}_2) + v_2 g'(v_2) - g(v_2).$$

Taking the derivative of $vg'(v) - g(v)$ w.r.t. v , we get

$$g'(v) - g'(v) + vg'' = vg'' \geq 0, \quad (16)$$

which implies that $vg'(v) - g(v)$ increases with v .

Now, consider instead a single contract (ρ, L_1) such that optimal user vulnerability in the base model with $\tilde{W} = W - \rho$ and $\tilde{D}_1 = D - L_1$ is v_1 , i.e., from (6),

$$v_1 [f(\tilde{W}) - f(\tilde{W} - \tilde{D}_1)] = -g'(v_1). \quad (17)$$

Comparing the LHS of (14) and (17), we infer that, since $v_1 > \bar{v}$, $\tilde{W} > \tilde{W}_1$ and hence $\rho < \rho_1$. Comparing the user utility with this single contract (ρ, L_1) with (15), we have

$$U = f(W - \rho) + v_1 g'(v_1) - g(v_1) > U_1 = U_2,$$

since $\rho < \rho_1$. Thus, this single contract (ρ, L_1) permits the social planner to achieve higher user utility and will be preferred to the two contracts (ρ_1, L_1) and (ρ_2, L_2) . Hence, we have proven that only a single contract will be offered in the social planner optimum.

Second, we demonstrate that the network vulnerability with the optimal contract $(\rho^{\dagger soc}, L^{\dagger soc})$ is higher than in the no-insurance Nash equilibrium, i.e., $v^{\dagger soc} \geq v^*$. We know that $U^{\dagger soc}$ must be higher than U^* since U^* can always be reached by the planner offering the contract $(\rho, L) = (0, 0)$:

$$U^{\dagger soc} \geq U^*.$$

Next, for any contract (ρ, L) with optimal vulnerability v , similar to (15), the user's utility can be written as

$$U = f(W - \rho) + vg'(v) - g(v). \quad (18)$$

From $\rho > 0$, the monotonicity of $vg' - g$ from (16), (18) and (7), we infer that $U^{\dagger soc} \geq U^*$ holds only if

$$v^{\dagger soc} > v^*.$$

Last, we show that all users purchase this insurance. If a user i deviates to no-insurance, she obtains $U(v_i, v^{\dagger soc}, 0, 0)$, which is highest for $v_i = \tilde{v}$ determined from $\frac{\partial U(v_i, v^{\dagger soc}, 0, 0)}{\partial v_i} = 0$, which gives:

$$v^{\dagger soc} [f(W) - f(W - D)] = -g'(\tilde{v}). \quad (19)$$

Since $v^{\dagger soc} \geq v^*$, comparing the LHS of (19) and (6), we have

$$\tilde{v} \leq v^* \leq v^{\dagger soc}.$$

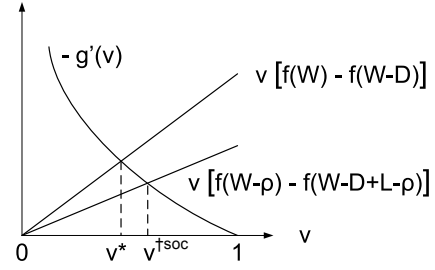


Fig. 2. Nash Equilibrium Vs Social Optimum for Non-contractible Insurance

Next, we write $U(\tilde{v}, v^{\dagger soc}, 0, 0)$ using (19):

$$U(\tilde{v}, v^{\dagger soc}, 0, 0) = f(W) + \tilde{v}g'(\tilde{v}) - g(\tilde{v}). \quad (20)$$

Comparing with (7) using the monotonicity of $vg' - g$ derived in (16), we conclude that, since $\tilde{v} \leq v^*$, the user utility from deviation $U(\tilde{v}, v^{\dagger soc}, 0, 0)$ must be lower than U^* . Therefore,

$$U(\tilde{v}, v^{\dagger soc}, 0, 0) \leq U^* \leq U^{\dagger soc},$$

giving us the required result that no user will deviate and not buy insurance.

Competitive Insurers: In the case of competing insurers, there may exist multiple contracts in equilibrium. However, the resulting network vulnerability $\bar{v}^\dagger$ will not be lower than the vulnerability in the Nash equilibrium v^* . Indeed, assume the reverse: $\bar{v}^\dagger < v^*$. Let (ρ_1, L_1) be some contract adopted by a non-zero fraction of users in this equilibrium.

From (5), replacing W by $\tilde{W}_1 = W - \rho_1$ and D by $\tilde{D}_1 = D - L_1$, we get an expression for the vulnerability v_1 chosen by users who adopt the contract (ρ_1, L_1) :

$$\bar{v}^\dagger [f(\tilde{W}_1) - f(\tilde{W}_1 - \tilde{D}_1)] = -g'(v_1). \quad (21)$$

Note that $\rho_1 \leq L_1$, i.e., the premium must be lower than the coverage, else deviating from this contract to no-insurance gives higher utility to the users. Hence, $[f(\tilde{W}_1) - f(\tilde{W}_1 - \tilde{D}_1)] \leq [f(W) - f(W - D)]$.

From our assumption that $\bar{v}^\dagger \leq v^*$, we observe that the LHS of (21) is lesser than the LHS of (6) which implies that $v_1 \geq v^*$. (See Fig. 3.) However, the choice of (ρ_1, L_1) was arbitrary among all the contracts in equilibrium. Hence, the user adopting any contract in equilibrium will choose vulnerability not lower than v^* . This gives us $\bar{v}^\dagger \geq v^*$, which contradicts our assumption. Hence, $\bar{v}^\dagger \geq v^*$ in the competitive equilibrium as well.

Proposition 3

Social Planner: First, we show that a social planner will offer a single contract in equilibrium only. Indeed, assume the reverse. Let the social planner offer two contracts (The proof for more contracts is similar.) (v_1, ρ_1, L_1) and (v_2, ρ_2, L_2) to a fraction α and $(1 - \alpha)$ of the population respectively. Thus,

$$\bar{v} = \alpha v_1 + (1 - \alpha) v_2.$$

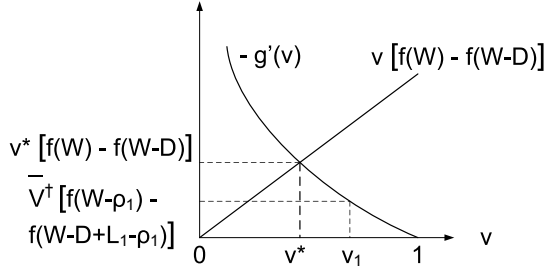


Fig. 3. Deviation v_1 in Competitive Non-contractible Insurance

From the budget constraint, we have

$$\alpha\rho_1 + (1 - \alpha)\rho_2 \geq \alpha v_1 \bar{v} L_1 + (1 - \alpha)v_2 \bar{v} L_2.$$

From (8), we observe that the contracts with $L_1 = L_2 = D$ offer users a higher utility. Hence, we will only focus on the contracts (v_1, ρ_1, D) and (v_2, ρ_2, D) for the rest of the proof. In this case, the budget constraint becomes

$$\alpha\rho_1 + (1 - \alpha)\rho_2 \geq \alpha v_1 \bar{v} D + (1 - \alpha)v_2 \bar{v} D = \bar{v}^2 D. \quad (22)$$

From (8), the aggregate utility with the contracts (v_1, ρ_1, D) and (v_2, ρ_2, D) will be:

$$U^{agg} = \alpha[f(W - \rho_1) - g(v_1)] + (1 - \alpha)[f(W - \rho_2) - g(v_2)].$$

Since both f and $(-g)$ are concave functions (and $f' > 0$),

$$\begin{aligned} U^{agg} &< f(W - \{\alpha\rho_1 + (1 - \alpha)\rho_2\}) - g(\bar{v}) \\ &\leq f(W - \bar{v}^2 D) - g(\bar{v}), \end{aligned}$$

where the second inequality comes from (22).

$f(W - \bar{v}^2 D) - g(\bar{v})$ is the utility obtained from the contract $(\bar{v}, \bar{v}^2 D, D)$. Hence, there exists the single contract $(\bar{v}, \bar{v}^2 D, D)$ which always provides a higher aggregate user utility than all contracts (v_1, ρ_1, L_1) and (v_2, ρ_2, L_2) .

Thus, the social planner offers only a single contract. This contract must be a solution to the following optimization problem:

$$\begin{aligned} \max_{v, \rho, L} & U(v, v, \rho, L) \\ \text{s.t.} & v^2 L \leq \rho \text{ and } v \leq 1. \end{aligned}$$

Next, we write the Lagrangian:

$$LAN = U(v, v, \rho, L) - \lambda_1(v^2 L - \rho) - \lambda_2(v - 1).$$

Let $\tilde{W} = W - \rho$ and $\tilde{D} = D - L$. Taking the derivatives of LAN w.r.t. v , L and ρ and equating to 0 gives us the following equations.

$$\begin{aligned} \frac{\partial LAN}{\partial v} &= \frac{\partial U(v, v, \rho, L)}{\partial v} - 2\lambda_1 v L - \lambda_2 = 0, \\ \left[-2v(f(\tilde{W}) - f(\tilde{W} - \tilde{D}) - g'(v)) \right] - 2\lambda_1 v L - \lambda_2 &= 0. \end{aligned} \quad (23)$$

$$\begin{aligned} \frac{\partial LAN}{\partial L} &= \frac{\partial U(v, v, \rho, L)}{\partial L} - \lambda_1 v^2 = 0, \\ v^2 f'(\tilde{W} - \tilde{D}) - \lambda_1 v^2 &= 0. \end{aligned} \quad (24)$$

$$\begin{aligned} \frac{\partial LAN}{\partial \rho} &= \frac{\partial U(v, v, \rho, L)}{\partial \rho} + \lambda_1 = 0, \\ -v^2 f'(\tilde{W} - \tilde{D}) - (1 - v^2)f'(\tilde{W}) + \lambda_1 &= 0. \end{aligned} \quad (25)$$

Further, from complementary slackness, we have

$$\lambda_1(v^2 L - \rho) = 0, \quad (26)$$

$$\text{and } \lambda_2(v - 1) = 0. \quad (27)$$

Note that $v \neq 0$, since that would require infinite security costs for the users. Hence, from (24), we conclude that $\lambda_1 = f'(\tilde{W} - \tilde{D}) > 0$ and thus, constraint (26) binds:

$$v^2 L = \rho. \quad (28)$$

Equating λ_1 from (24) and (25), we obtain:

$$f'(\tilde{W} - \tilde{D}) = v^2 f'(\tilde{W} - \tilde{D}) + (1 - v^2)f'(\tilde{W}). \quad (29)$$

Note that $v \neq 1$ because $g'(1) = 0$ and even a tiny decrease in v increases the expected benefit without increasing costs. Thus, from (29),

$$L = D. \quad (30)$$

Next, we can substitute (28) and (30) into (24) to get $\lambda_1 = f'(W - v^2 D)$. Also, $\lambda_2 = 0$, since $v < 1$. Substituting λ_1 , λ_2 , (28) and (30) into (23), we get

$$-g'(v) = 2vDf'(W - v^2 D). \quad (31)$$

Since the LHS is monotone decreasing while the RHS is monotone increasing, $v^{\ddagger soc} (< 1)$ is the unique solution to (31).

With $L = D$, and $\rho = v^2 D$ user utility at any v can be expressed as

$$U(v, v, v^2 D, D) = f(W - v^2 D) - g(v).$$

Maximum utility is reached at $\frac{dU(v)}{dv} = 0$:

$$-2vDf'(W - v^2 D) - g'(v) = 0, \quad (32)$$

and maximum is unique, because $\frac{d^2 U(v)}{dv^2} < 0$:

$$4v^2 D^2 f''(W - v^2 D) - 2Df'(W - v^2 D) - g''(v) < 0,$$

due to the properties of the functions f and g . Thus, there exists a unique social planner's optimum contract.

Competitive Insurers: First, we notice that in any equilibrium, due to competition, for any insurer, profit is zero, i.e. $\rho = v\bar{v}L$ for any equilibrium contract (v, ρ, L) . If $\rho > v\bar{v}L$, some entrant insurer could offer a contract $(v, \tilde{\rho}, L)$ s.t. $\rho > \tilde{\rho} > v\bar{v}L$. From (8), the contract with a lower premium and same L , v and $\bar{v}$ improves user utility.

Second, full coverage, i.e. $L = D$ will be offered due to competition. Indeed, the contract $(v, v\bar{v}D, D)$ offers users the highest utility. To see this, consider the family of contracts $(v, v\bar{v}L, L)$ for $L \leq D$. From (9), the utility $U(v, \bar{v}, v\bar{v}L, L)$ will be $(1 - p)f(W - pL) + pf(W - pL - D + L) - g(v)$,

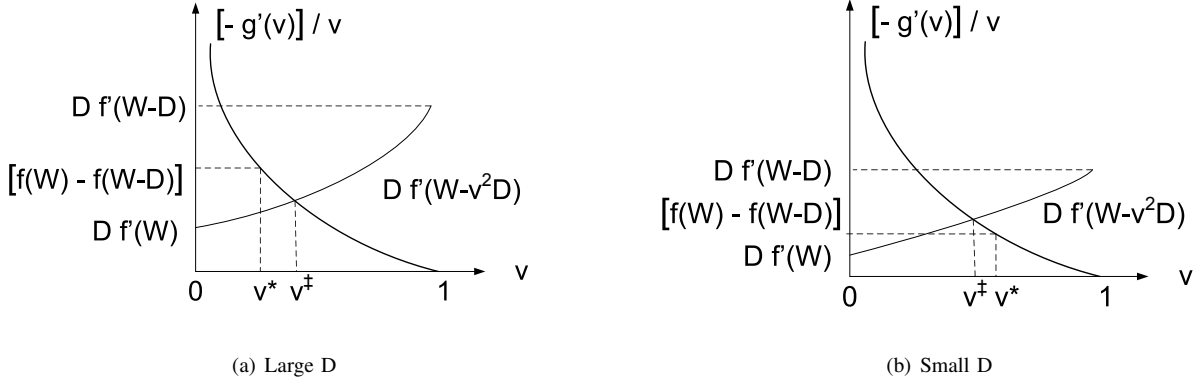


Fig. 4. Competitive Equilibrium with Contractible Security

where $p = v\bar{v}$. Differentiating w.r.t. L , and equating to 0, we get

$$p(1-p)f'(W-pL) = p(1-p)f(W-pL-D+L).$$

If $p \neq 0$ or 1, then $L = D$, which gives the required result. Henceforth, we restrict our analysis to contracts $(v, v\bar{v}D, D)$ only.

Third, in any equilibrium, user utility from deviation to no-insurance gives user a strictly lower utility. Indeed, assume the reverse. Consider a contract $(v_1, v_1\bar{v}D, D)$ that has a non-zero number of users adopting it in equilibrium. If a customer of this contract prefers to deviate to v_i with no insurance, then his utility without insurance must be greater than the utility with insurance contract, i.e., $U(v_i, \bar{v}, 0, 0) \geq U(v_1, \bar{v}, v_1\bar{v}D, D)$. Consider an entrant insurer who offers a contract $(v_i, v_i\bar{v}D, D)$ (full coverage at actuarially fair price). Adopting this contract improves user utility, which conflicts our equilibrium assumptions. Therefore, the utility from deviation to no-contract must be strictly lower than with a contract, and thus, all users strictly prefer to buy insurance.

Fourth, we prove that equilibrium contract is unique. Consider an equilibrium with network security $\bar{v}$. An entrant insurer could offer a contract $(\tilde{v}, \tilde{v}\bar{v}D, D)$ that maximizes $U(\tilde{v}, \bar{v}, \tilde{v}\bar{v}D, D) = f(W - \tilde{v}\bar{v}D) - g(\tilde{v})$. To determine $\tilde{v}$ at which user utility is the highest we differentiate

$$\begin{aligned} \frac{\partial}{\partial \tilde{v}} U(\tilde{v}, \bar{v}, \tilde{v}\bar{v}D, D) &= \frac{\partial}{\partial \tilde{v}} (f(W - \tilde{v}\bar{v}D) - g(\tilde{v})) = 0, \\ f'(W - \tilde{v}\bar{v}D)(-\bar{v}D) - g'(\tilde{v}) &= 0, \end{aligned}$$

and since the second derivative is always negative:

$$f''(W - \tilde{v}\bar{v}D)(\bar{v}D)^2 - g''(\tilde{v}) < 0,$$

user utility reaches its maximum at a single point $\tilde{v}$ only, which is exactly the contract offered in equilibrium. Thus, we have $\tilde{v} = \bar{v} = v^\dagger$, and in any equilibrium, all users buy an identical contract $(v^\dagger, (v^\dagger)^2D, D)$, determined from

$$-g'(v^\dagger) = v^\dagger D f'(W - (v^\dagger)^2D). \quad (33)$$

The unique $v^\dagger$ is strictly less than 1 since $f'(W-D) > 0$. (If $f'(W-D) = 0$, then $f(W) = f(W-D)$ and insurance

does not improve user utility and is hence redundant.) Since the RHS of (31) is twice the RHS of (33), we conclude that $v^\dagger \geq v^{\dagger soc}$, i.e., the equilibrium security under competitive insurers is worse than under a social planner.

Next, we determine how $v^\dagger$ compares to v^* . We rewrite (33) as

$$\frac{-g'(v^\dagger)}{v^\dagger} = Df'(W - (v^\dagger)^2D), \quad (34)$$

and compare with the Nash equilibrium by rewriting (6) as:

$$\frac{-g'(v^*)}{v^*} = f(W) - f(W-D). \quad (35)$$

Note that, from $f'' \leq 0$, we have $f'(W) \leq \frac{f(W) - f(W-D)}{D} \leq f'(W-D)$. Also, $f'(W - v^2D)$ is an increasing function of v , and $\frac{-g'(v)}{v}$ is decreasing. Hence, if $Df'(W - v^{*2}D) < f(W) - f(W-D)$ then $v^\dagger > v^*$ else $v^\dagger \leq v^*$. Thus, if the marginal benefit from full coverage offered at v^* is lower than the average loss of benefit per unit damage, insurance does not improve the security level.

Fig. 4 depicts the solution of (34). From the figure, it is clear that only when D becomes small, the network security level in the equilibrium with insurers exceeds security level of no-insurance equilibrium. Note that when D is small, v^* is also large. Thus, competitive insurers improve network security only when equilibrium vulnerability in no-insurance equilibrium is high.

REFERENCES

- [1] R. Anderson, R. Böhme, R. Clayton, and T. Moore, "Security economics and european policy," in *Proceedings of WEIS'08*, Hanover, USA, Jun. 25-28 2008.
- [2] R. Böhme, "Cyber-insurance revisited," in *Proceedings of WEIS'05*, Cambridge, USA, 2005.
- [3] L. A. Gordon, M. Loeb, and T. Sohail, "A framework for using insurance for cyber-risk management," *Communications of the ACM*, vol. 46, no. 3, pp. 81-85, 2003.
- [4] R. P. Majuca, W. Yurcik, and J. P. Kesan, "The evolution of cyberinsurance," ACM Computing Research Repository, Tech. Rep. CR/0601020, 2006.
- [5] K. Soohoo, "How much is enough? a risk-management approach to computer security," Ph.D. dissertation, Stanford University.
- [6] S. E. Schechter, "Computer security strength and risk: a quantitative approach," Ph.D. dissertation, Cambridge, MA, USA, 2004, adviser-Smith, Michael D.

- [7] J. Bolot and M. Lelarge, "A new perspective on internet security using insurance," *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, pp. 1948–1956, April 2008.
- [8] M. Rothschild and J. E. Stiglitz, "Equilibrium in competitive insurance markets: An essay on the economics of imperfect information," *The Quarterly Journal of Economics*, vol. 90, no. 4, pp. 630–49, November 1976. [Online]. Available: <http://ideas.repec.org/a/tpr/qjecon/v90y1976i4p630-49.html>
- [9] J. E. Stiglitz, "Information and the change in the paradigm in economics," *American Economic Review*, vol. 92, no. 3, pp. 460–501, June 2002. [Online]. Available: <http://ideas.repec.org/a/aea/aerev/v92y2002i3p460-501.html>
- [10] H. Kunreuther and G. Heal, "Interdependent security," *Journal of Risk and Uncertainty*, vol. 26, no. 2-3, pp. 231–49, March-May 2003. [Online]. Available: <http://ideas.repec.org/a/kap/jrisku/v26y2003i2-3p231-49.html>
- [11] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Trans. Inf. Syst. Secur.*, vol. 5, no. 4, pp. 438–457, 2002.
- [12] K. Hausken, "Returns to information security investment: The effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability," *Information Systems Frontiers*, vol. 8, no. 5, pp. 338–349, 2006.
- [13] J. Grossklags, N. Christin, and J. Chuang, "Secure or insure?: a game-theoretic analysis of information security games," in *WWW '08: Proceeding of the 17th international conference on World Wide Web*. New York, NY, USA: ACM, 2008, pp. 209–218.
- [14] H. Varian, "System reliability and free riding," in *Workshop on the Economics of Information Security, WEIS 2002*, Cambridge, USA, 2002.
- [15] H. Ogut, N. Menon, and S. Raghunathan, "Cyber insurance and it security investment: Impact of interdependent risk," in *Proceedings of WEIS'05*, Cambridge, USA, 2005.
- [16] W. S. Baer and A. Parkinson, "Cyberinsurance in it security management," *IEEE Security and Privacy*, vol. 5, no. 3, pp. 50–56, 2007.
- [17] M. Fisk, "Causes and remedies for social acceptance of network insecurity," in *Proceedings of WEIS'02*, Berkeley, USA, 2002.
- [18] P. Honeyman, G. Schwartz, and A. V. Assche, "Interdependence of reliability and security," in *Proceedings of WEIS'07*, Pittsburg, PA, 2007.
- [19] A. Hofmann, "Internalizing externalities of loss prevention through insurance monopoly: an analysis of interdependent risks," *Geneva Risk and Insurance Review*, vol. 32, no. 1, pp. 91–111, 2007.
- [20] H. C. Kunreuther and E. O. Michel-Kerjan, "Evaluating the effectiveness of terrorism risk financing solutions," National Bureau of Economic Research, Inc, NBER Working Papers 13359, Oct. 2007. [Online]. Available: <http://ideas.repec.org/p/nbr/nberwo/13359.html>
- [21] N. Shetty, G. Schwartz, M. Felegyhazi, and J. Walrand, "Competitive Cyber-Insurance and Internet Security," in *Workshop on Economics of Information Security 2009*, University College London, England, June 2009.
- [22] G. A. Akerlof, "The market for 'lemons': Quality uncertainty and the market mechanism," *The Quarterly Journal of Economics*, vol. 84, no. 3, pp. 488–500, August 1970. [Online]. Available: <http://ideas.repec.org/a/tpr/qjecon/v84y1970i3p488-500.html>