# Voluntary Participation in Cyber-insurance Markets

Parinaz Naghizadeh and Mingyan Liu

**Abstract** The study of cyber-insurance, both as a method for transferring residual cyber-security risks, and as an incentive mechanism for internalizing the externalities of security investments in interdependent systems, has received considerable attention in the literature. On one hand, it has been shown that competitive insurance markets, even though ensuring user participation, fail to improve the overall network security. On the other hand, existing literature illustrates how a monopolist insurer can induce socially optimal behavior (under a binary decision model). Nevertheless, participation in the latter market is assumed to be mandatory. In this work, we ask the question of whether socially optimal security investments can be incentivized through non-compulsory insurance. To do so, we will not consider the competitive market model due to its inefficiencies, and focus instead on the role of a monopolist profit-neutral insurer acting as a regulator in implementing the socially optimal investment profile. We first propose an insurance design mechanism that allows a continuous decision model, and then study users' participation incentives. We show that due to the non-excludable nature of security, there may exist scenarios in which it is impossible to guarantee that users voluntarily purchase insurance. We discuss the implication of this impossibility and possible ways to circumvent it.

## 1 Introduction

The use of insurance, or more precisely *cyber-insurance* as it is referred to in the realm of computer security, as a means of mitigating cyber-attack losses and enhancing the reliability of computer systems has been receiving increasd attention both in the literature, as well as in practice, as suggested by the growing market for cyber-insurance contracts.

Department of Electrical Engineering and Computer Science, University of Michigan, Ann Arbor, e-mail: {naghizad,mingyan}@umich.edu

There are currently over 30 insurance carriers offering cyber-insurance contracts in the US [2, 19]. Many insurers have reported growths of 10-25% in premiums in a 2012 survey of the market [2], with some carriers reporting even higher rates. For example, one carrier reports an increase of 33% from 2011 to 2012 in the number of clients purchasing their contracts [16]. The total amount of premiums written are estimated to be between $500M and $1bn [19]. Typical premiums are estimated to start from $10k -$25k and go as high as $50M [2, 19]. These contracts are reported to have an average of $16.8M limits [16], with some coverage limits up to $200M-$300M [19]. We refer the interested reader to [1, 2, 19] for additional information on both the US and the UK insurance markets, as well as common types of coverage offered through these policies, and the typical exclusions.

Aside from the use of cyber-insurance as a risk transfer mechanism, i.e., as a means of managing residual security risks, insurance has been considered as a potential solution to the problem of under-investment in security in interdependent systems.

### *1.1 Sub-optimality of security investments*

In general, the effort exerted by a user, entity, or network, to secure its system, not only protects that user from security breaches, but also improves the security posture of other users connected to it, by decreasing the likelihood of an indirect attack originating from the former entity. Accordingly, users' investments in security in such systems are often viewed as a *public good* with *positive externalities*. Within this context, a strategic user out of self-interest may not only choose to ignore the externality of its actions on others, but can further choose to free-ride on others' efforts, resulting in an overall under-investment in security, which then leads to lower overall levels of security.

The problem of (under-)investment in security by an interconnected group of strategic users, both in general as well as in the context of computer security, has been extensively studied in the framework of game theory, see e.g. [5, 8, 11–13, 23], and is often formulated as an Interdependent Security (IDS) game. In the majority of the literature, under-investment in security is verified by finding the levels of effort exerted in a Nash equilibrium of the IDS game, and comparing them with the socially optimal levels of investment.

This under-investment problem motivates the study of mechanisms for improving network security, and ideally, driving the system to its socially optimal state (see [12] for a recent survey). Below we briefly summarize the literature on cyber-insurance as a potential method for enhancing a system's security by incentivizing user cooperation.

## 1.2 Cyber-insurance as an incentive mechanism

The study of cyber-insurance both as a method for mitigating cyber-security risks and as an incentive mechanism for internalizing the externalities of security investments has received considerable attention, see e.g. [3, 4, 6, 10–12, 14, 15, 18, 22]. In addition to the classic insurance problems of adverse selection (higher risk users seek more protection) and moral hazard (users lower their investment in self-protection after being insured), the design of cyber-insurance contracts is further complicated by the risk interdependencies and the possibility of correlated damages in an interconnected system.

The literature on cyber-insurance has mainly focused on one of the two market environments of competitive or monopolistic insurers. On one hand, it can be shown that in competitive insurance markets, the introduction of insurance contracts not only fails to improve, but can further worsen network security relative to a no-insurance scenario [18, 22]. This is because contracts offered in such markets are optimal from the viewpoint of *individual* users, whereas socially optimal contracts should be designed by keeping *social* welfare in mind. On the other hand, it is shown that by engaging in premium discrimination, a monopolistic profit-neutral cyber-insurer can induce socially optimal security investments in an interdependent system where security decisions are binary [6, 15, 18].[1]

Despite the shortcomings of competitive markets in implementing socially optimal solutions, a competitive approach to insurance contract design provides the benefit that the participation of users in the market will be guaranteed, as their self-interest is satisfied. In contrast, although [6, 15, 18] implement the socially optimal solution in the binary decision framework, participation is assumed to be mandatory, e.g., users are enforced through policy mandates to purchase insurance.

In the remainder of this chapter, we ask the question of whether socially optimal security efforts can be incentivized through non-compulsory insurance? That is, we take on the latter viewpoint on insurance markets, focusing on implementing the socially optimal investment profile in an IDS game by considering a monopolist profit-neutral insurer, i.e., an insurance regulator, and study users' participation incentives in these markets.

## 1.3 Main contributions

In this chapter, we take a mechanism design approach to the security investment problem, and present a message exchange process through which users converge to an equilibrium where they make the socially optimal levels of investment in security.

[1] We note that the term "monopolistic" generally implies the use of exclusive market power for profit maximization, while in our model this monopolistic insurer is profit-neutral, essentially acting as a *regulator* through insurance means [3]. This use of the term however is consistent with literature in this area, see e.g., [6, 15, 18]. For this reason we will henceforth use the terms "insurance regulator" and "monopolistic insurer" interchangeably.

The proposed method, which is adapted from the externality mechanism proposed by Hurwicz in [7], is applicable to a general model of interdependence, and captures heterogeneity in users' preferences, costs, and their importance to the system. In particular, this model allows for continuous levels of effort. Therefore, our work complements the existing results in [6, 15, 18], by introducing a mechanism that achieves similar benefits in a non-binary setting.

More importantly, our other goal in this paper is to elucidate the nature of participation incentives in the insurance market with security interdependencies. We show that with a general model of interdependencies and as a result of the non-excludable nature of security as a public good, the insurance regulator may not be able to guarantee that users voluntarily purchase protection form the market. These constraints have not been specifically addressed in the literature on monopolistic cyber-insurance [6, 15, 18]. Therefore, to the best of our knowledge, this is the first work to study users' voluntary participation in cyber-insurance markets.

### *1.4 Chapter organization*

The rest of this chapter is organized as follows. We present our model and main assumptions in Section 2, and introduce our proposed insurance mechanism in Section 3. Further illustration using two numerical simulations in provided in Section 4. We discuss users' participation incentives in Section 5, followed by further interpretation of our observations and possible remedies in Section 6. Section 7 concludes the chapter.

## 2 Model and Preliminaries

Consider a collection of $N$ users, referred to as the system. Each user $i$ can choose a non-negative level of investment on security measures or protection, denoted by $x_i$, and incur a cost of $h_i(x_i)$. We assume $h_i : \mathbb{R} \to \mathbb{R}_+$ is differentiable, strictly increasing, and strictly convex, for all $i$. Intuitively, this means that security measures get increasingly costly as their effectiveness increases.

Let $\mathbf{x} := (x_1, x_2, \ldots, x_N)$ denote the *profile* of users' security investments. We denote user $i$'s *security risk* function by $f_i(\mathbf{x})$. The security risk function models the probability that a successful security attack on a particular user occurs, and may vary among different users depending on their security interdependencies.

Let $L_i$ denote user $i$'s losses in case a security breach occurs. Note that users may be able to decrease their potential losses by investing in *self-insurance* measures (e.g. data backup) [5, 9]. If such options are available to users, $L_i$ will denote the *residual* losses of user $i$, i.e., losses that can not be mitigated through self-insurance alone. The expected losses of an individual in the system is therefore given by $L_i f_i(\mathbf{x})$.

We assume $f_i : \mathbb{R}^N \to \mathbb{R}_+$ is differentiable, strictly decreasing in all $x_j$, and strictly convex in all $x_j$, for all $i, j$. This assumption states that the security risk decreases as the investment in security increases. In particular, $\partial f_i/\partial x_j < 0,\ j \neq i$ models the positive externality of security investments. The assumption of convexity means that while initial investment in security offers considerable protection, the rate of risk reduction slows down at higher investment levels, as there is no security measure that could fully prevent malicious activities [8, 12].

The utility function of user $i$ is thus given by:

$$u_i(\mathbf{x}) = -L_i f_i(\mathbf{x}) - h_i(x_i)\ . \tag{1}$$

The strategic game $(\{1,2,\ldots,N\}, \{x_i \geq 0\}, \{u_i(\cdot)\})$ among the $N$ utility-maximizing users will be referred to as the Interdependent Security (IDS) game.

The Nash equilibria (NE) of IDS games have been extensively studied in the literature. These studies often point out to the inefficiency of these NE as compared to the socially optimal (SO) levels of investment in security. The socially optimal profile of security investments $\mathbf{x}^*$ is the profile of investments that maximizes the social welfare, and is determined by the solution to the following centralized optimization problem:

$$\max_{\mathbf{x} \succeq 0} \quad \sum_{i=1}^{N} u_i(\mathbf{x})\ . \tag{2}$$

Given the model assumptions, our IDS game has a unique socially optimal solution. Our goal in Section 3 is to design insurance contracts, the purchase of which will induce this socially optimal investments by the users without directly solving the above centralized problem.

To do so, we will focus on an insurance regulator who offers insurance contracts $(\rho_i, I_i)$ where the two elements are interpreted as follows: $\rho_i$ is the premium paid by user $i$, and $I_i$ the indemnification payment or coverage provided to user $i$ if an incident occurs. The utility of a user $i$ when purchasing insurance is thus given by:

$$u_i(\mathbf{x}, \rho_i, I_i) = -(L_i - I_i) f_i(\mathbf{x}) - h_i(x_i) - \rho_i\ . \tag{3}$$

We note that the insurer may offer partial coverage ($I_i < L_i$), full coverage ($I_i = L_i$), or additional compensation ($I_i > L_i$) in case of a loss. In the latter case, a negative $L_i - I_i$ implies an additional *reward* to user $i$.

We should emphasize that the assumption of a monopolist insurer is key in our setting. Our focus is on implementing the socially optimal investment profile in an IDS game; we thus do not consider a competitive market model due to its inefficiencies and instead investigate the role of a monopolist insurer. It should be noted that a contract may include additional terms such as deductible, premium discount for being incident-free, separate coverage for catastrophic events, etc. However, we shall show that an insurer can implement the socially optimal solution using the most simple contracts consisting only of a premium and a coverage level. The potential benefits of introducing additional dimensions is discussed in Section 6.

The expected profit of the insurer offering a set of contracts $\{(\rho_i, I_i)\}_{i=1}^N$ is given by:

$$P = \sum_i \rho_i - \sum_i I_i f_i(\mathbf{x}) \ . \tag{4}$$

We will further assume that the insurer is profit neutral. This assumption is common in the mechanism design literature, often referred to as the *budget balance* condition in mechanisms that use monetary taxation.[2] In our context the role of the monopolist insurer may very well be played by a government agency, in which case profit-neutrality becomes a natural assumption. Consequently, we are interested in insurance contracts satisfying $\sum_i \rho_i = \sum_i I_i f_i(\mathbf{x})$. Given this, the socially optimal solution to (2) is the same whether we input (1) or (3) as users' utility functions.

## 3 Insurance Contract Design

In this section, we present a mechanism that can achieve the socially optimal solution to (2). A decentralized mechanism is specified by a game form $(\mathscr{M}, g)$.

- The message space $\mathscr{M} := \Pi_{i=1}^N \mathscr{M}_i$ specifies the set of permissible messages $\mathscr{M}_i$ for each user $i$.
- The outcome function $g : \mathscr{M} \to \mathscr{A}$ determines the outcome of the game based on the users' messages. Here, $\mathscr{A}$ is the space of all security investment, premium, and coverage profiles, i.e., $(\mathbf{x}, \boldsymbol{\rho}, \mathbf{I})$.

The game form, together with the utility functions (3), define a game, given by $(\mathscr{M}, g(\cdot), \{u_i(\cdot)\})$. We will henceforth refer to this as the *regulated IDS game* or the IDS game induced by the mechanism. We say the message profile $\mathbf{m}^*$ is a Nash equilibrium of this game, if

$$u_i(g(m_i^*, \mathbf{m^*}_{-i})) \geq u_i(g(m_i, \mathbf{m^*}_{-i})), \qquad \forall m_i, \ \forall i \ . \tag{5}$$

The components of our mechanism are as follows.

Each user $i$ provides a message $m_i := (\mathbf{x}_i, \boldsymbol{\pi}_i)$ to the insurer. $\mathbf{x}_i \in \mathbb{R}^N$ denotes user $i$'s proposal on the public good, i.e., it proposes the amount of security investment to be made by everyone in the system, referred to as an *investment profile*. $\boldsymbol{\pi}_i \in \mathbb{R}_+^N$ denotes a *pricing profile* which suggests the equivalent amount to be paid by everyone. As illustrated below, this is used by the insurer to determine the insurance contracts of all users. Therefore, the pricing profile is user $i$'s proposal on the private good.

[2] In fact, it is easy to see that a *profit making* monopolist insurer can only make the voluntary participation constraints even harder to satisfy, as this profit could have been used to incentivize user cooperation. As we aim to understand participation incentive in this study, we will adopt the profit neutrality assumption.

The outcome function $g(\cdot)$ takes the message profiles $\mathbf{m} := \{m_1, m_2, \ldots, m_N\}$ as input, and determines the security investment profile $\hat{\mathbf{x}}$ and an intermediate *net payment* profile $\hat{\mathbf{t}}$ as follows:

$$\hat{\mathbf{x}}(\mathbf{m}) = \frac{1}{N}\sum_{i=1}^{N} \mathbf{x}_i \ , \tag{6}$$

$$\begin{aligned}\hat{t}_i(\mathbf{m}) = &(\boldsymbol{\pi}_{i+1} - \boldsymbol{\pi}_{i+2})^T \hat{\mathbf{x}}(\mathbf{m}) \\ &+ (\mathbf{x}_i - \mathbf{x}_{i+1})^T \mathrm{diag}(\boldsymbol{\pi}_i)(\mathbf{x}_i - \mathbf{x}_{i+1}) \\ &- (\mathbf{x}_{i+1} - \mathbf{x}_{i+2})^T \mathrm{diag}(\boldsymbol{\pi}_{i+1})(\mathbf{x}_{i+1} - \mathbf{x}_{i+2}), \forall i.\end{aligned} \tag{7}$$

In (7), for simplicity $N+1$ and $N+2$ are treated as 1 and 2, respectively. Once the net payment profile $\hat{\mathbf{t}}$ is calculated, the insurer determines the optimal contracts $\{(\hat{\rho}_i, \hat{I}_i)\}_{i=1}^N$ based on the following equations:

$$\hat{\rho}_i - \hat{I}_i f_i(\hat{\mathbf{x}}) = \hat{t}_i \ , \ \forall i \ . \tag{8}$$

The choice of the term "net payment" should now be clear from (8): it determines the difference between premium payed and expected coverage received. Notice also that by (7), we have $\sum_i \hat{t}_i = 0$. Together with (4), this implies that the profit-neutrality condition of the insurer is automatically satisfied through this construction. What this means is that the insurer will not be spending resources or making profit, as the users whose net payment $\hat{t}_i$ is positive will be financing the insurance coverage for those who have negative net payments. The above equations may have many solutions, each of which results in an optimal contract. The choice lies with the insurer, e.g., it may offer full coverage in return for a high premium, or a lower-premium contract with partial coverage. Note that users are not able to change either their premium or their coverage level directly, but can potentially alter their net payment $\hat{t}_i$ through their message.

It is worthwhile to highlight an alternative interpretation for the intermediate net payment profile $\hat{\mathbf{t}}$. Even though the profile $\hat{\mathbf{t}}$ has been used as a stepping stone in finding the optimal insurance contracts in our proposed mechanism, one could simply view this profile as a monetary taxation/reward to incentivize optimal user behavior. Our previous work on the proposed mechanism in the context of IDS games [17], as well as similar decentralized mechanisms proposed in [7, 21], are based on this interpretation.

## *3.1 An intuitive explanation*

Intuitively, the above mechanism operates as follows. The investment profile $\hat{\mathbf{x}}$ gives the levels of investment suggested by the insurer for each player. This vector is derived by taking the average of all users' proposals for the public good. To ensure that these proposals are consistent, and eventually match the socially optimal levels

of investment, the insurer designs the insurance contracts according to (7) and (8). To highlight this feature, we consider the three terms in (7) separately.

First, we note that a user $i$ can only affect the first term $(\boldsymbol{\pi}_{i+1}-\boldsymbol{\pi}_{i+2})^T\hat{\mathbf{x}}(\mathbf{m})$ in its net payment by altering its proposal on the investment profile. We will illustrate the role of this term shortly. The second term in (7) is included to punish discrepancies among users' proposals on the investment profile by increasing their net payment in case of disagreement. Lastly, the third term, which is independent of user $i$'s message, is included to satisfy the profit-neutral constraint of the insurer. As discussed in the proof of Theorem 1, the last two terms will be zero at an equilibrium of the regulated IDS game. Nevertheless, the inclusion of these terms is required to ensure convergence to the socially optimal solution, and also for balancing the insurer's budget.

We now highlight the role of the first term in (7), and its close relation to the positive externality effects of users' actions. As shown in the proof of Theorem 1, at the equilibrium $\mathbf{m}^*$ of the regulated IDS game, the net payment of a user $i$ reduces to $\hat{t}_i = \mathbf{l}_i^{*T}\hat{\mathbf{x}}(\mathbf{m}^*)$, where $\mathbf{l}_i^* := \boldsymbol{\pi}_{i+1}^* - \boldsymbol{\pi}_{i+2}^*$. If net payments are determined according to these prices, the socially optimal investments $\hat{\mathbf{x}}(\mathbf{m}^*)$ will be individually optimal as well, i.e.,[3]

$$\hat{\mathbf{x}}(\mathbf{m}^*) = \arg\min_{\mathbf{x}\succeq 0} \quad L_i f_i(\mathbf{x}) + h_i(x_i) + \mathbf{l}_i^{*T}\mathbf{x}\ . \tag{9}$$

As a result, for all $i$, and all $j$ for which $\hat{x}_j \neq 0$, the Karush-Kuhn-Tucker (KKT) conditions on (9) yield:

$$l_{ij}^* = -L_i \frac{\partial f_i}{\partial x_j}(\hat{\mathbf{x}}(\mathbf{m}^*))\ . \tag{10}$$

The interpretation is that by implementing this mechanism, each user $i$ will be financing part of user $j \neq i$'s insurance contract. According to (10), this amount is proportional to the positive externality of $j$'s investment on user $i$'s utility.

## *3.2 Analysis of the insurance mechanism*

We close this section by establishing the optimality of our proposed mechanism. Note that to prove this optimality, we first need to show that a profile $(\hat{\mathbf{x}}(\mathbf{m}^*), \hat{\boldsymbol{\rho}}(\mathbf{m}^*), \hat{\mathbf{I}}(\mathbf{m}^*))$, derived at the NE $\mathbf{m}^*$ of the regulated IDS game, is the socially optimal solution to the centralized problem (2). Furthermore, as the procedure for convergence to NE is not specified, we need to verify that the optimality property holds *for all Nash equilibrium* of the message exchange process. This guarantees that the outcome will converge to the socially optimal solution regardless of the realized NE. These two requirements are established in Theorem 1 below.

[3] See proof of Theorem 1 presented later in this section for the derivation of this result.

**Theorem 1.** *Let* $(\hat{\mathbf{x}}(\mathbf{m}^*), \hat{\boldsymbol{\rho}}(\mathbf{m}^*), \hat{\mathbf{I}}(\mathbf{m}^*))$ *be the investment, premium, and coverage profiles obtained at the Nash equilibrium* $\mathbf{m}^*$ *of the regulated IDS game* $(\mathscr{M}, g(\cdot), \{u_i(\cdot)\})$. *Then,* $\hat{\mathbf{x}}$ *is the optimal solution to the centralized problem* (2). *Furthermore, if* $\bar{\mathbf{m}}$ *is any other Nash equilibrium of the proposed game, then* $\hat{\mathbf{x}}(\bar{\mathbf{m}}) = \hat{\mathbf{x}}(\mathbf{m}^*)$.

*Proof:* Let $\mathbf{m}^*$ be a Nash equilibrium of the message exchange process, resulting in an allocation $(\hat{\mathbf{x}}, \hat{\boldsymbol{\rho}}, \hat{\mathbf{I}})$. Assume user $i$ updates its message from $m_i^* = (\boldsymbol{\pi}_i^*, \mathbf{x}_i^*)$ to $m_i = (\boldsymbol{\pi}_i, \mathbf{x}_i^*)$, that is, it only updates the pricing vector proposal. Therefore, according to (6), $\hat{\mathbf{x}}$ will remain fixed, while based on (7), the second term in $\hat{t}_i$ will change. The change of this term can in turn affect the choice of either $\hat{\rho}_i$, $\hat{I}_i$, or both. First note that a user $i$'s utility (3) can be re-written as follows:

$$\begin{aligned} u_i(\mathbf{x}, \rho_i, I_i) &= -L_i f_i(\mathbf{x}) - h_i(x_i) - (\rho_i - I_i f_i(\mathbf{x})) \\ &= -L_i f_i(\mathbf{x}) - h_i(x_i) - t_i \ . \end{aligned} \tag{11}$$

Using (11) and the fact that if $\mathbf{m}^*$ is an NE, unilateral deviations are not profitable, we have:

$$\begin{aligned} & (\mathbf{x}_i^* - \mathbf{x}_{i+1}^*)^T \mathrm{diag}(\boldsymbol{\pi}_i^*)(\mathbf{x}_i^* - \mathbf{x}_{i+1}^*) \\ \leq \ & (\mathbf{x}_i^* - \mathbf{x}_{i+1}^*)^T \mathrm{diag}(\boldsymbol{\pi}_i)(\mathbf{x}_i^* - \mathbf{x}_{i+1}^*), \quad \forall \boldsymbol{\pi}_i \succeq 0. \end{aligned} \tag{12}$$

Hence, from (12) we conclude that for all $i$:

$$\mathbf{x}_i^* = \mathbf{x}_{i+1}^* \quad \text{or} \quad \boldsymbol{\pi}_i^* = \mathbf{0} \ . \tag{13}$$

Using (13) together with (7) we conclude that at equilibrium, the second and third terms of a user's net payment vanish. Denoting $\mathbf{l}_i^* := \boldsymbol{\pi}_{i+1}^* - \boldsymbol{\pi}_{i+2}^*$, we get:

$$\hat{t}_i(\mathbf{m}^*) = \mathbf{l}_i^{*T} \hat{\mathbf{x}}(\mathbf{m}^*) \ . \tag{14}$$

Now consider users' utility functions at the NE $\mathbf{m}^*$. Since unilateral deviations are not profitable, a user's utility (11) should be maximized at the NE, i.e., for any choice of $\mathbf{x}_i$ and $\boldsymbol{\pi}_i \succeq 0$:

$$\begin{aligned} & L_i f_i(\hat{\mathbf{x}}(\mathbf{m}^*)) + h_i(\hat{x}_i(\mathbf{m}^*)) + \mathbf{l}_i^{*T} \hat{\mathbf{x}}(\mathbf{m}^*) \\ \leq \ & L_i f_i\Big(\frac{\mathbf{x}_i + \sum_{j \neq i} \mathbf{x}_j^*}{N}\Big) + h_i\Big(\frac{x_{ii} + \sum_{j \neq i} x_{ji}^*}{N}\Big) + \mathbf{l}_i^{*T} \frac{\mathbf{x}_i + \sum_{j \neq i} \mathbf{x}_j^*}{N} \\ + \ & (\mathbf{x}_i - \mathbf{x}_{i+1}^*)^T \mathrm{diag}(\boldsymbol{\pi}_i)(\mathbf{x}_i - \mathbf{x}_{i+1}^*) \ . \end{aligned} \tag{15}$$

If we choose $\boldsymbol{\pi}_i = \mathbf{0}$ and let $\mathbf{x}_i = N \cdot \mathbf{x} - \sum_{j \neq i} \mathbf{x}_j^*$, where $\mathbf{x}$ is any vector of security investments, we get:

$$L_i f_i(\hat{\mathbf{x}}(\mathbf{m}^*)) + h_i(\hat{x}_i(\mathbf{m}^*)) + \mathbf{l}_i^{*T} \hat{\mathbf{x}}(\mathbf{m}^*) \leq L_i f_i(\mathbf{x}) + h_i(x_i) + \mathbf{l}_i^{*T} \mathbf{x}, \quad \forall \mathbf{x} \ . \tag{16}$$

To show that the Nash equilibrium $\mathbf{m}^*$ results in a socially optimal allocation, we sum up (16) over all $i$, and use the fact that $\sum_i \mathbf{l}_i^* = \mathbf{0}$ to get:

$$\sum_{i=1}^{N} u_i(\hat{\mathbf{x}}(\mathbf{m}^*)) \geq \sum_{i=1}^{N} u_i(\mathbf{x}), \quad \forall \mathbf{x} \,. \tag{17}$$

Therefore, $\hat{\mathbf{x}}(\mathbf{m}^*)$ is the optimal solution to problem (2). Furthermore, any insurance contract determined using (8) and the intermediate net payment profile $\hat{\mathbf{t}}(\mathbf{m}^*)$ can be chosen as the insurance contract in the optimal solution. Finally, since our choice of the NE $\mathbf{m}^*$ has been arbitrary, the same proof holds for any other NE, and thus all NE of the mechanism result in the optimal solution to problem (2). ■

We next establish the converse of the above theorem in Theorem 2, i.e., given an optimal investment profile, there exists an NE of the proposed game which implements this solution; the proof is given in the appendix.

**Theorem 2.** *Let $\mathbf{x}^*$ be the optimal investment profile in the solution to the centralized problem* (2)*. Then, there exists at least one Nash equilibrium $\mathbf{m}^*$ of the regulated IDS game $(\mathscr{M}, g(\cdot), \{u_i(\cdot)\})$ such that $\hat{\mathbf{x}}(\mathbf{m}^*) = \mathbf{x}^*$.*

## 4 Numerical Examples

In this section we present two numerical examples to illustrate how the proposed insurance contracts affect users' actions, security risks, costs, and ultimately, the security and societal costs of the interconnected system. In particular, this is done under two different risk models. Throughout this section, for consistency and ease of presentation, we assume users' costs are linear in their investment, i.e., $h_i(x_i) = c_i x_i$, where $c_i > 0$ is the unit cost of investment. Users will be indexed according to their costs, such that $c_1 < c_2 < \ldots < c_N$.

### *4.1 Example 1: a weighted total effort model*

We first assume users' risk functions are given by a *weighted total effort* model [12, 23],

$$f_i(\mathbf{x}) = \exp(-\sum_{j=1}^{N} a_{ij} x_j), \tag{18}$$

where $a_{ij}$ determines the degree of externality of user $j$'s investment on user $i$'s security risks. Let $A := [a_{ij}]$ denote the *interdependence matrix* containing these weights. Under these assumptions, a user $i$'s utility function is given by:

$$u_i(\mathbf{x}, I_i, \rho_i) = -(L_i - I_i)\exp(-\sum_{j=1}^{N} a_{ij}x_j) - c_i x_i - \rho_i \ .$$

The simulations are based on an instance of this problem with the following parameters. Consider a collection of $N = 10$ users. Assume that the unit costs of investment for the firms are generated randomly, such that $c_1 < c_2 < \ldots < c_N$. We let $L_i = L = \$50M$, $\forall i$, that is, we assume all firms are subject to a similar maximum loss of \$50M in case of a security breach. Finally, we generate the interdependence matrix $A$ at random, with the only constraint that $a_{ii} > a_{ij}$, $\forall i,\ j \neq i$. This implies that a user's security is primarily affected by its own expenditure in security measures.

Figure 1 illustrates the expected losses $L_i f_i(\mathbf{x})$ of user $i$ under both the Nash equilibrium and the socially optimal outcome. In this example, we see that implementing the proposed insurance contracts not only leads to risk transfer, but it also incentivizes risk reduction.[4] Figure 2 shows the change in users' expenditure in security after the contracts are purchased. It can be seen that as expected, the socially optimal solution requires users with lower cost in security improvement to make higher investments.

As the insurer is profit-neutral, this higher effort by the main investors is compensated by other users' premium payments. Indeed, as illustrated in Figure 3, the net payment of the main investors 1 and 2 are negative, to be covered by the positive net payment of the remaining users. In essence, the social optimality derives from the fact that users that are more effective and efficient in their security spending are being paid by less efficient users to do so on their behalf. The insurer in this context serves as a *coordinator* or *facilitator*.

Interestingly, the net payment of several users are negligible. This is consistent with our observations in Figures 1 and 2, where the expected loss and expenditures of these users are also negligible at the socially optimal outcome. As a result, the insurance contracts for these users are the degenerate contracts with zero premium and coverage. Similarly, based on Figure 1, the probability of large losses are negligible for users 1 and 2. In this case, offering an indemnification payment to these users is unnecessary. The insurer can in turn allocate the premium surplus from other users to the main investors as additional funds to be spent in security. Finally, the insurer can offer full coverage to users 5 and 7 (i.e. $I_i = L = \$50M$), in return for premiums of \$4.7M and \$7M, respectively.

Overall, the introduction of the proposed insurance contracts reduces the costs of all users in security, as illustrated in Figure 4, where costs are given by $-u_i(\mathbf{x}^*)$ for user $i$. This figure illustrates a component-wise improvement in users' costs as a result of implementing the proposed mechanism. This means that the profit-neutral insurer does not necessarily need to make some users worse off in order to improve social welfare. Figure 5 illustrates the improvement in social welfare following the implementation of insurance. Numerically, as a result of risk reduction following the purchase of insurance contracts, we see savings of close to \$40M in social costs.

[4] It is worth mentioning that this is not necessarily the case when a system moves from the Nash equilibrium to the socially optimal solution. A socially optimal solution is meant to minimize social costs, and therefore it may result in higher risks/losses for some users.

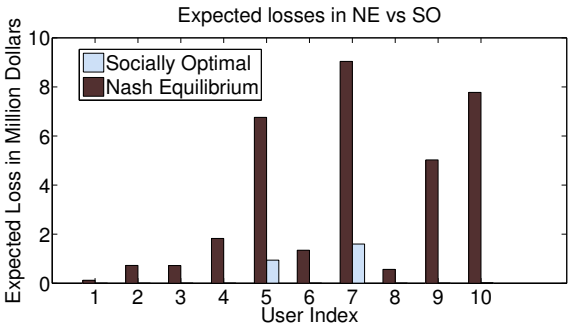


**Fig. 1** Expected Losses - Weighted Total Effort

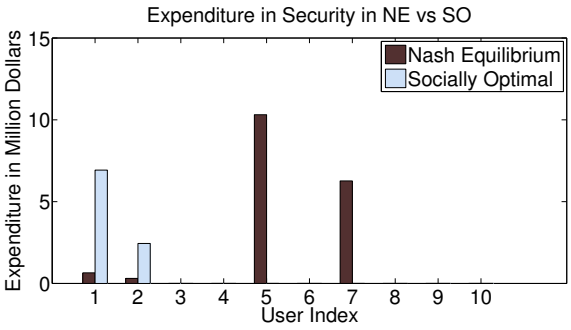


**Fig. 2** Expenditure in Security - Weighted Total Effort

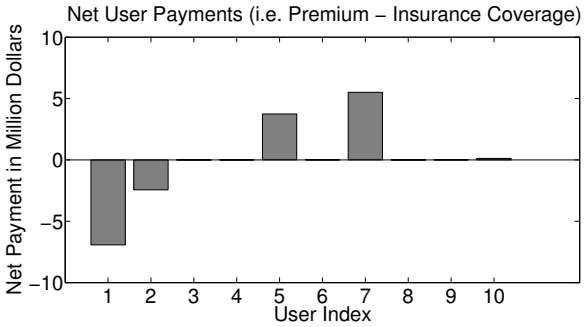


**Fig. 3** Net Payments - Weighted Total Effort

## *4.2 Example 2: a weakest link model*

We now assume users' risk functions are determined by the *weakest link* model $f_i(\mathbf{x}) = \exp(-\min_j x_j)$ [12, 23]. Intuitively, this model states that an attacker can compromise the security of an interconnected system by taking over the least protected machine. To use this model in our proposed framework, we need a

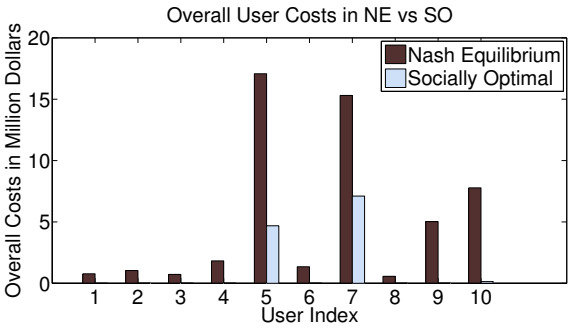


**Fig. 4** Expected Costs - Weighted Total Effort

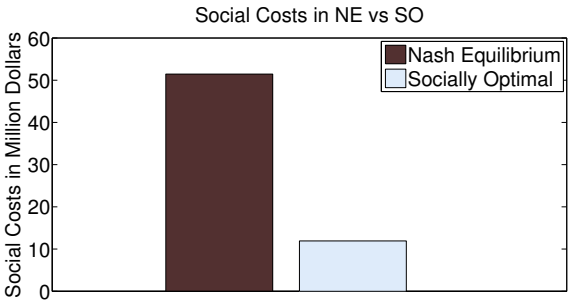


**Fig. 5** Social Costs - Weighted Total Effort

continuous, differentiable approximation of the minimum function. Let $\min_j x_j \approx -\frac{1}{\gamma}\log\sum_j \exp(-\gamma x_j)$, where the accuracy of the approximation is increasing in the constant $\gamma > 0$. User $i$'s utility function is thus given by:

$$u_i(\mathbf{x}, I_i, \rho_i) = -(L_i - I_i)(\sum_{j=1}^{N} \exp(-\gamma x_j))^{1/\gamma} - c_i x_i - \rho_i \ .$$

The simulations are based on an instance of this problem with the following parameters. We again consider $N = 10$ users, with unit costs of investment generated randomly, such that $c_1 < c_2 < \ldots < c_N$. Also, $L_i = L = \$50M$, $\forall i$. We note that the weakest link game has multiple Nash equilibrium, in which all users invest in the same (sub-optimal) amount in security. We pick the NE with investment levels at the mean of all these possible NE.

Figure 6 illustrates the expected losses $L_i f_i(\mathbf{x})$ of users $i$. Again, we see that implementing the proposed insurance contracts has incentivized risk reduction. Figure 7 shows the change in users' expenditure in security after the contracts are purchased. Note that at an equilibrium of the weakest-link game, all users exert an identical level of effort [23]. Therefore, to arrive at this same optimal level of investment, users with higher costs are required to spend more in security measures.

As a result, one expects the users with lower costs to aid this transition. Indeed, as illustrated in Figure 8, the net payment of the higher cost users are negative, to be covered by the positive net payment of the lower cost users. Users' insurance contracts can now be determined according to their net payments. For example, user 3 will be receiving full coverage $I_3 = \$50M$ in return for a \$2M premium, while user 7 receives full coverage $I_7 = \$50M$, but pays a zero premium.

We again observe a component-wise reduction in users' costs, as illustrated in Figure 9, along with improvement in social welfare leading to savings of close to \$35M in social costs, Figure 10.

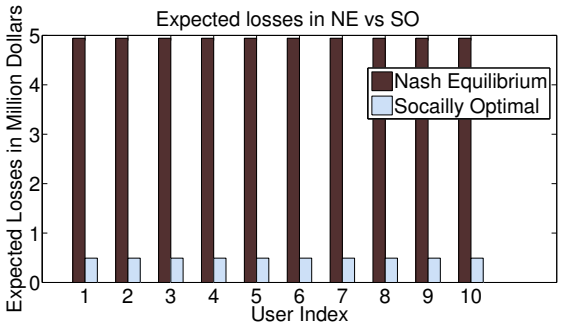


**Fig. 6** Expected Losses - Weakest Link

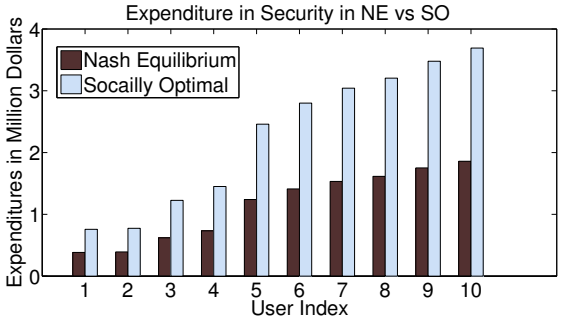


**Fig. 7** Security Expenditure - Weakest Link

## 5 On Voluntary Participation

The message exchange process proposed in Section 3, as well as the mechanisms proposed in [6, 15, 18], take users' participation in the insurance market for granted.

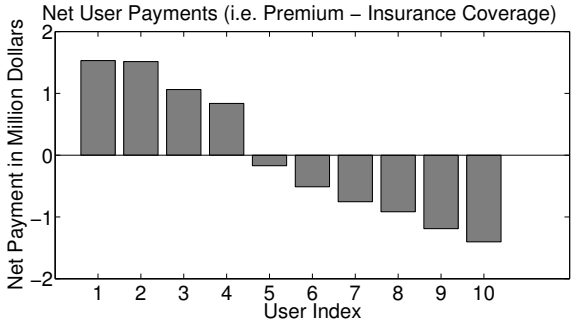


**Fig. 8** Net Payments - Weakest Link

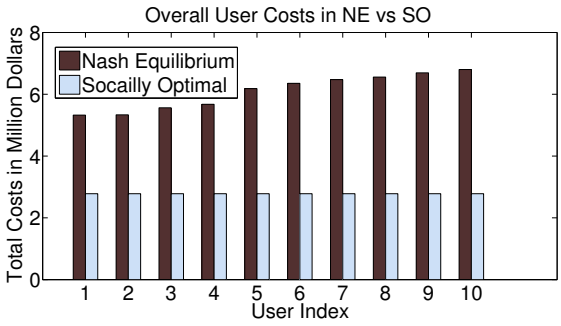


**Fig. 9** Expected Costs - Weakest Link

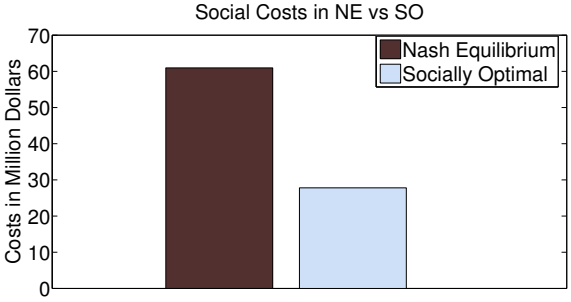


**Fig. 10** Social Costs - Weakest Link

While this could be ensured through certain external incentive mechanisms, e.g., a government agency could make participation in cyber-insurance a prerequisite to receiving funding or business opportunities, it is generally more desirable to make this incentive to participate a built-in property of the mechanism itself. If this can be accomplished then the mechanism not only induces socially optimal resource allocation, but offers incentive for each individual user to participate in the mechanism.

Within this context there are two desirable conditions/constraints that we would like a mechanism to satisfy. The first is the commonly studied *individual rationality* (IR) condition which states that users should prefer the existence of the mechanism to the previous state of anarchy. The second is the less frequently invoked *voluntary participation* (VP) condition referred to by [20], which states that a user should prefer participation in the mechanism to staying out, given everyone else in the environment participates.

Satisfying individual rationality in the current context, although desirable, does not guarantee the implementation of the insurance contracts, as voluntary participation of users in the insurance market needs to be ensured as well. In this section, we further illustrate the difference of the two constraints in the current setting, and study the voluntary participation constraint of the users under the insurance mechanism.

## *5.1 The non-excludable public good*

Strategic users' decisions regarding participation in a given mechanism is influenced not only by the structure of the induced game form, but also by the actions available to them when opting out. A common assumption in the majority of public good and resource allocation problems, including those on decentralized mechanisms similar to the one presented in Section 3 [7, 21], is that users get a *zero* share (of the public good or allotted resources) when opting out. Following this assumption, the individual rationality and voluntary participation constraints of such mechanisms are equivalent, and are rather trivially satisfied.

However, a similar line of reasoning is not applicable to our problem. This is because at issue is the provision of a *non-excludable* public good: in an inter-connected system, an individual benefits from improved security of its neighbors (the positive externality) regardless of its own decision on whether to adopt a certain measure. Specifically in the context of an IDS game, even when opting out, a user can still enjoy the positive externalities of other users' investments (although these may be lower as the mechanism has now only partial coverage), choose its optimal action accordingly, and possibly avoid spending resources on insurance. Thus to ensure voluntary participation in this regulated IDS game is not as trivial as in previous studies.

Indeed, we next present a counter-example which shows that there may exist users to whom the benefits of staying out exceeds that of participation. Thus such a user is better off acting as a "loner", who refuses to participate in the mechanism, and later best-responds to the socially optimal strategy of the remaining $N-1$ users who did participate. It would be natural to expect these $N-1$ users to also revise their strategy (investments) in response to this loner's best response, resulting in a game between the loner and the remaining $N-1$ users. In this example we will compare the loner's utility in the socially optimal solution when participating in the mechanism, versus the utility it gains as the outcome of the game described above.

### *5.2 A negative example*

Consider a collection of $N$ users. The cost function of each user $i$ is given by a linear function $h_i(x_i) = c_i x_i$, where $c_i > 0$ is the unit cost of investment. Choose $c_1 < c_2 < \ldots < c_N$. Assume the risk function of user $i$ is given by $f_i(\mathbf{x}) = \exp(-\sum_{j=1}^{N} x_j)$ (an instance of the total effort model [23]). Finally, for simplicity, let $L_i = 1,\ \forall i$. The utility function of a user $i$ purchasing the insurance contract $(\rho_i, I_i)$ is therefore given by:

$$u_i(\mathbf{x}, \rho_i, I_i) = -(1 - I_i)\exp(-\sum_{j=1}^{N} x_j) - c_i x_i - \rho_i \ . \tag{19}$$

It is easy to show [17, 23] that with a total effort model, the user with the smallest cost will exert all the effort, while all other users will free-ride on the positive externality of this investment. Therefore, we can find the equilibrium of the game under different conditions as follows.

**Socially optimal outcome:** When all $N$ users participate in the mechanism, it is clear that under the optimal solution to problem (2) user 1 will exert all the effort. The first order optimality condition suggests that this optimal investment is given by the solution to the equation:

$$N\exp(-x_1^*) - c_1 = 0 \implies \exp(-x_1^*) = \frac{c_1}{N} \ .$$

Intuitively, user 1's investment in this case corresponds to the amount it would make if it were the only user in the system with a unit cost $\frac{c_1}{N}$. This will thus be referred to as user 1's *equivalent cost* in this $N$-player total effort game. Therefore, the socially optimal profile of investments $\mathbf{x}^*$ is such that:

$$\exp(-x_1^*) = \frac{c_1}{N}, \quad x_j^* = 0,\ \forall j > 1 \ .$$

**User 1's VP condition:** If user 1 chooses to stay out, user 2 will be the player with the lowest cost in the $N-1$ player game, investing according to the equivalent cost of $\frac{c_2}{N-1}$. Whether user 1 will invest in security or free-ride on the externalities depends on user 2's level of investment. When $c_1 > \frac{c_2}{N-1}$, user 1 will have a higher cost, and thus will prefer to free-ride on user 2's investment. The equilibrium levels of investment $\hat{\mathbf{x}}$ of this game will thus be:

$$\exp(-\hat{x}_2) = \frac{c_2}{N-1}, \quad \hat{x}_j = 0,\ \forall j \neq 2 \ .$$

**User $k$'s VP condition, for $k \geq 2$:** Finally, if any user other than 1 decides to stay out, user 1 will continue exerting all the effort, but the level of security will be determined according to the higher equivalent cost of $\frac{c_1}{N-1}$. The equilibrium levels of security $\tilde{\mathbf{x}}$ will decrease such that:

$$\exp(-\tilde{x}_1) = \frac{c_1}{N-1}, \quad \tilde{x}_j = 0, \, \forall j > 1 \, .$$

We can now use the above analysis to determine the voluntary participation conditions of all users. For user 1 to voluntarily participate in the mechanism, we need $u_1(\mathbf{x}^*, \rho_1^*, I_1^*) \geq u_1(\hat{\mathbf{x}})$. This in turn leads to:

$$-\exp(-x_1^*) - c_1 x_1^* - \rho_1^* + I_1^* \exp(-x_1^*) \geq -\exp(-\hat{x}_2) \, .$$

Rearranging, we see that user 1's insurance contract should satisfy:

$$-\rho_1^* + I_1^* \frac{c_1}{N} \geq c_1 (\frac{1}{N} - \ln \frac{c_1}{N}) - \frac{c_2}{N-1} \, . \tag{20}$$

For any other user $k \geq 2$, the voluntary participation condition is:

$$-\exp(-x_1^*) - \rho_k^* + I_k^* \exp(-x_1^*) \geq -\exp(-\tilde{x}_1) \, .$$

Rearranging, we conclude that user $k$'s insurance contracts, which in fact requires these users to finance the insurance contract for user 1, should be worth the extra security:

$$\rho_k^* - I_k^* \frac{c_1}{N} \leq \frac{c_1}{N(N-1)} \, . \tag{21}$$

To satisfy the insurer's profit-neutral constraint, we need $\sum_j \rho_j^* = \frac{c_1}{N} \sum_j I_j^*$, which can be written as $-\rho_1^* + I_1^* \frac{c_1}{N} = \sum_{j=2}^N \rho_j^* - I_j^* \frac{c_1}{N}$. Using this, together with (21), we conclude:

$$-\rho_1^* + I_1^* \frac{c_1}{N} \leq \frac{c_1}{N} \, . \tag{22}$$

For (20) and (22) to be consistent, we need to satisfy the following condition:

$$c_1 (\frac{1}{N} - \ln \frac{c_1}{N}) - \frac{c_2}{N-1} \leq \frac{c_1}{N} \, .$$

Choose any $c_1 < c_2 < 1$ and $c_1 > \frac{c_2}{N-1}$. If $N \geq 3$, then $c_1 \ln(\frac{c_1}{N}) + \frac{c_2}{N-1} < 0$, which means that the VP conditions for user 1 and users $k \geq 2$ cannot be simultaneously satisfied.

## 6 Discussion

We have thus found an example where not all users will voluntarily participate in the insurance mechanism. Note that the existence of the counter example in Section 5.2 does not depend on how the insurance contracts are designed; it is simply a

consequence of not being able to simultaneously satisfy individuals' self-interest, social optimality, and the insurer's profit-neutrality.[5]

Intuitively, this impossibility arises from the fact that to achieve socially optimal investments, one (or more) of the users is required to increase its investment level, thus demanding compensation in the form of insurance coverage. Nevertheless, the added security is not enough to incentivize the remaining users to finance this coverage, especially as they are able to free-ride on a slightly lower security level if they opt out. Conversely, the main investor may prefer to opt out of the mechanism if the compensation offered to them is not high enough. In this case, this user may choose to free-ride on the externality of the (lower) security by the next main investor.

### *6.1 A numerical example*

The following numerical example highlights both of these possible complications under our proposed mechanism. Again assume users' risk functions are given by the weighted total effort model, $f_i(\mathbf{x}) = \exp(-\sum_{j=1}^{N} a_{ij}x_j)$. Let $A := [a_{ij}]$ denote the randomly generated interdependence matrix containing the weights $a_{ij}$.

The simulations are based on an instance of this problem with the following parameters. Consider a collection of $N = 5$ users. Assume that the unit costs of investment for the users are generated randomly, such that $c_1 < c_2 < \ldots < c_N$. We let $L_i = L$, $\forall i$, that is, we assume all users are subject to a similar maximum loss in case of a security breach.

Figure 11 illustrates the investments of users in security measures with and without insurance contracts. It is easy to see that users 2, 3, and 5 are the main investors in the mechanism, while users 1 and 4 are the free-riders. Users' costs when purchasing insurance and acting as loners is illustrated in Figure 12. Notice that in this problem instance, user 2 is motivated to contribute as a main investor, while users 3 and 5 are not compensated enough to do so. Similarly, free-rider 4 is willing to pay a high premium in return for the added protection, while free-rider 1 would rather stay out and benefit from the positive externalities from the improved security of the remaining 4 users.

[5] Our approach in deriving this result is similar to that in [20, Section 2], in which the authors present a counter-example to show the impossibility of achieving voluntary participation in Lindahl mechanisms for provision of a public good with a constant return to scale technology. The authors then establish a more rigorous proof of the impossibility, by showing the inconsistency in the set of problem constraints [20, Section 4]. It would be interesting to establish the impossibility result in the current IDS problem using a similar approach.

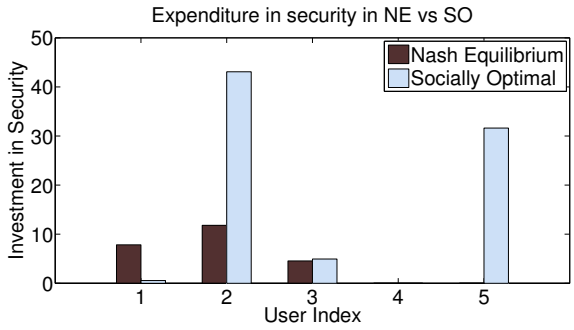


**Fig. 11** Users' investments in security with or without insurance

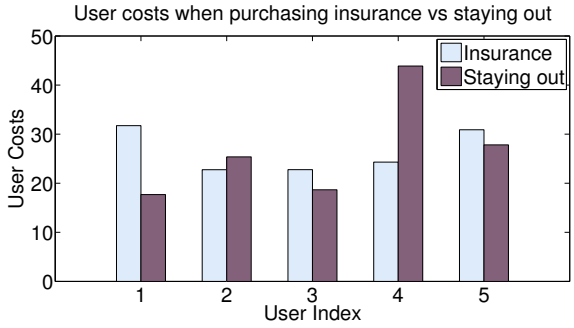


**Fig. 12** Users' costs when participating vs acting as loners

## *6.2 A positive example*

We next identify a family of problem instances in which the insurance mechanism of Section 3 does satisfy the voluntary participation constraints of users.

Consider the same interdependency model detailed in the counter-example in Section 5.2. As mentioned, since users with utility functions given by (19) are subject to similar losses, only the user with the smallest cost will invest in security, while the remaining users free-ride. We want to ensure that all users, i.e. both the main security investor and the free-riders, prefer participating in the proposed mechanism to unilaterally staying out.

First note that the net payments of users in our proposed mechanism can be determined according to (10), and are given by:

$$t_i^* = -\sum_j x_j^* \frac{\partial f_i}{\partial x_j}(x^*) - c_i x_i^* \ .$$

Substituting $f_i(\mathbf{x}) = -\exp(-\sum_j x_j)$, the utility of users when all $N$ participate in the mechanism will reduce to:

$$u_i(\mathbf{x}^*, \rho_i^*, I_i^*) = -\frac{c_1}{N}(1+x_1^*), \forall i \ .$$

**Users' VP constraints:** Using the analysis from the previous section, for a user $j \geq 2$ to voluntarily participate in the mechanism, we need $u_j(\mathbf{x}^*, \rho_j^*, I_j^*) > u_j(\hat{\mathbf{x}})$, which yields:

$$\frac{c_1}{N}(1+x_1^*) < \frac{c_1}{N-1} \Rightarrow \quad \ln\frac{N}{c_1} < \frac{1}{N-1} \quad (\text{VP}_\text{j}) \ .$$

On the other hand, when user 1 steps out, one of the following outcomes is realized:

**a.** If $c_1 < \frac{c_2}{N-1}$, user 1 will continue investing in security, with an investment given by $\exp(-\bar{x}_1) = c_1$. User 1's VP constraint in this case is:

$$\frac{c_1}{N}(1+x_1^*) < c_1(1+\bar{x}_1) \Rightarrow \ln c_1 < 1 - \frac{\ln N}{N-1} \ \ (\text{VP}_{1\text{a}}).$$

**b.** If $\frac{c_2}{N-1} < c_1 < c_2$, user 2 will invest in security, while all other users, including user 1, free-ride. The level of security provided is given by $\exp(-\hat{x}_2) = \frac{c_2}{N-1}$, leading to the following VP condition for user 1:

$$\frac{c_1}{N}(1+x_1^*) < \frac{c_2}{N-1} \qquad (\text{VP}_{1\text{b}}) \ .$$

**Ensuring voluntary participation:** For voluntary participation to hold in a problem instance, we need to have ($\text{VP}_\text{j}$), and either ($\text{VP}_{1\text{a}}$) or ($\text{VP}_{1\text{b}}$) satisfied.

($\text{VP}_\text{j}$) and ($\text{VP}_{1\text{a}}$) hold simultaneously if and only if:

$$N = 2, \quad \frac{2}{e} < c_1 < \frac{e}{2}, \quad c_2 > c_1 \ .$$

($\text{VP}_\text{j}$) and ($\text{VP}_{1\text{b}}$) hold if and only if $N, c_1, c_2$ satisfy:

$$c_1 > N\exp(-\frac{1}{N-1}), \quad c_1 < c_2 < (N-1)c_1 \ .$$

## *6.3 Potential solutions*

As shown in the previous positive example, we may identify classes of problems in which the mechanism in Section 3 satisfies users' voluntary participation constraints. In general, it may be possible to alleviate the participation issues by injecting external resources into the system (i.e. relaxing the insurer's budget balance condition), implementing a sub-optimal equilibrium (i.e. relaxing the social optimality condition), restricting the space of utility functions (i.e. designing separate contracts for different classes of risk functions), or settling for a mechanism with partial coverage. These remain interesting directions of future research.

If the above alternatives are not desirable, and voluntary participation cannot be guaranteed, one may also resort to policy mandate to induce users to purchase insurance in order to achieve social optimality. It should be noted that policy mandate is different from existing mechanisms that dictate users' *investments* [12], in that even under mandate, constant enforcement of users' actions is not needed, as it is individually optimal for users to exert the socially optimal effort once contracts are purchased.

An alternative to policy mandate is in the form of other financial incentives, including those already mentioned such as business opportunities or tax credits. It is also conceivable for the monopolist insurer (especially if played by a government agency) to guarantee the VP condition by offering separate coverage for rare but catastrophic security losses. As this type of coverage (acting in much the same way as relief for loss due to war or natural disasters) would be otherwise unavailable, it provides additional incentive for a user who might otherwise consider opting out.

## 7 Conclusion

We have considered the issue of users' voluntary participation in mechanisms achieving socially optimal solutions in IDS games using insurance contracts consisting of premiums and coverage levels, or equivalently, using monetary taxation/rewards. We argue that with positive externalities, the incentive to stay out and free-ride on others' investments can make users' participation incentives much harder to satisfy when designing contracts. We further discuss the implication of this result and possible remedies.

It remains an interesting question whether there are more sophisticated forms of the contracts (e.g., with additional dimensions such as deductibles, maximum coverage, premium discounts for incident-free users) which might satisfy all requirements, or whether this is a more fundamental challenge in designing mechanisms involving positive externalities.

**Acknowledgements** The authors would like to thank the anonymous reviewers of WEIS 2014 for useful comments and suggestions. This work is supported by the Department of Homeland Security (DHS) Science and Technology Directorate, Homeland Security Advanced Research Projects Agency (HSARPA), Cyber Security Division (DHS S&T/HSARPA/CSD), BAA 11-02 via contract number HSHQDC-13-C-B0015.

## Appendix

**Proof of Theorem 2:** This proof is technically similar to those presented in [7, 21]. Consider the optimal security investment profile $\mathbf{x}^*$ in the solution to the centralized

problem (2). Our goal is to show that there indeed exists a Nash equilibrium $\mathbf{m}^*$ of the mechanism for which $\hat{\mathbf{x}}(\mathbf{m}^*) = \mathbf{x}^*$.

Let $C_i(\mathbf{x}) := L_i f_i(\mathbf{x}) + h_i(x_i)$ denote the costs associated with the security investment and expected losses of user $i$. We start by showing that given the investment profile $\mathbf{x}^*$, it is possible to find a vector of personalized prices $\mathbf{l}_i^*$, for each $i$, such that,

$$\arg\min_{\mathbf{x}\succeq 0} \quad C_i(\mathbf{x}) + \mathbf{l}_i^{*T}\mathbf{x} = \mathbf{x}^* \ . \tag{23}$$

First, note that since $\mathbf{x}^*$ is the optimal solution to (2), it should satisfy the following KKT conditions, where $\boldsymbol{\lambda}_i \in \mathbb{R}_+^N, \ \forall i$:

$$\begin{aligned} \sum_{i=1}^{N} (\nabla C_i(\mathbf{x}^*) - \boldsymbol{\lambda}_i^T) = \mathbf{0} \ , \\ \boldsymbol{\lambda}_i^T \mathbf{x}^* = 0 \quad \forall i \ . \end{aligned} \tag{24}$$

Choose $\mathbf{l}_i^* = -\nabla C_i(\mathbf{x}^*) + \boldsymbol{\lambda}_i^T$. Then,

$$\mathbf{l}_i^* + \nabla C_i(\mathbf{x}^*) - \boldsymbol{\lambda}_i^T = \mathbf{0} \ . \tag{25}$$

Equations (24) and (25) together are the KKT conditions for the convex optimization problem:

$$\min_{\mathbf{x}\succeq 0} \quad C_i(\mathbf{x}) + \mathbf{l}_i^{*T}\mathbf{x} \ . \tag{26}$$

The KKT conditions are necessary and sufficient for finding the optimal solution to the convex optimization problem (26), and thus we have found the personalized prices satisfying (23).

We now proceed to finding a Nash equilibrium $\mathbf{m}^*$ resulting in the socially optimal solution $\mathbf{x}^*$. Consider the message profiles $m_i^* = (\boldsymbol{\pi}_i^*, \mathbf{x}_i^*)$, for which $\mathbf{x}_i^* = \mathbf{x}^*$, and the price vector proposals $\boldsymbol{\pi}_i^*$ are found from the recursive equations:

$$\boldsymbol{\pi}_{i+1}^* - \boldsymbol{\pi}_{i+2}^* = \mathbf{l}_i^*, \quad \forall i \ . \tag{27}$$

Here, $\mathbf{l}_i^*$ are the personalized prices defined at the beginning of the proof. The set of equations (27) always has a non-negative set of solutions $\boldsymbol{\pi}_i^* \succeq 0, \ \forall i$. This is because starting with a large enough $\boldsymbol{\pi}_1^*$, the remaining $\boldsymbol{\pi}_i^*$ can be determined using:[6]

$$\boldsymbol{\pi}_i^* = \boldsymbol{\pi}_{i-1}^* - \mathbf{l}_{i-2}^*, \quad \forall i \geq 2 \ . \tag{28}$$

Now, first note that by (26), for all choices of $\mathbf{x} \succeq 0$, and all users $i$, we have:

$$C_i(\mathbf{x}^*) + \mathbf{l}_i^{*T}\mathbf{x}^* \leq C_i(\mathbf{x}) + \mathbf{l}_i^{*T}\mathbf{x} \ . \tag{29}$$

[6] In (28), $\mathbf{l}_0^*$ is interpreted as $\mathbf{l}_N^*$.

Particularly, if we pick $\mathbf{x} = \frac{\mathbf{x}_i + \sum_{j \neq i} \mathbf{x}_j^*}{N}$,

$$C_i(\mathbf{x}^*) + \mathbf{l}_i^{*T}\mathbf{x}^* \leq C_i(\frac{\mathbf{x}_i + \sum_{j \neq i} \mathbf{x}_j^*}{N}) + \mathbf{l}_i^{*T}\frac{\mathbf{x}_i + \sum_{j \neq i} \mathbf{x}_j^*}{N} \ . \tag{30}$$

Also, since by construction $\mathbf{x}_i^* = \mathbf{x}_{i+1}^*$, $\forall i$, the inequality is preserved for any choice of $\boldsymbol{\pi}_i \succeq 0$, when the two remaining net payment terms from (7) are added in as follows:

$$\begin{aligned}
&C_i(\mathbf{x}^*) + \mathbf{l}_i^{*T}\mathbf{x}^* + (\mathbf{x}_i^* - \mathbf{x}_{i+1}^*)^T \mathrm{diag}(\boldsymbol{\pi}_i^*)(\mathbf{x}_i^* - \mathbf{x}_{i+1}^*) \\
&-(\mathbf{x}_{i+1}^* - \mathbf{x}_{i+2}^*)^T \mathrm{diag}(\boldsymbol{\pi}_{i+1}^*)(\mathbf{x}_{i+1}^* - \mathbf{x}_{i+2}^*) \\
\leq\ & C_i(\frac{\mathbf{x}_i + \sum_{j \neq i} \mathbf{x}_j^*}{N}) + \mathbf{l}_i^{*T}\frac{\mathbf{x}_i + \sum_{j \neq i} \mathbf{x}_j^*}{N} + (\mathbf{x}_i - \mathbf{x}_{i+1}^*)^T \mathrm{diag}(\boldsymbol{\pi}_i)(\mathbf{x}_i - \mathbf{x}_{i+1}^*) \\
&-(\mathbf{x}_{i+1}^* - \mathbf{x}_{i+2}^*)^T \mathrm{diag}(\boldsymbol{\pi}_{i+1}^*)(\mathbf{x}_{i+1}^* - \mathbf{x}_{i+2}^*).
\end{aligned} \tag{31}$$

Equation (31) can be more concisely written as:

$$u_i(g(m_i^*, \mathbf{m}^*{}_{-i})) \geq u_i(g(m_i, \mathbf{m}^*{}_{-i})) \ , \quad \forall m_i = (\boldsymbol{\pi}_i, \mathbf{x}_i),\ \forall i \ . \tag{32}$$

We conclude that the messages $m_i^* = (\boldsymbol{\pi}_i^*, \mathbf{x}^*)$ constitute an NE of the proposed mechanism. In other words, the message exchange process will indeed have an NE which implements the socially optimal solution of problem (2). ■

## References


1. Arimic. Airmic review of recent developments in the cyber insurance market. 2013.
2. Betterley. The betterley report: Cyber/privacy insurance market survey. June 2012.
3. R. Böhme and G. Schwartz. Modeling cyber-insurance: Towards a unifying framework. In *WEIS*, 2010.
4. L. A. Gordon, M. P. Loeb, and T. Sohail. A framework for using insurance for cyber-risk management. *Communications of the ACM*, 46(3):81–85, 2003.
5. J. Grossklags, N. Christin, and J. Chuang. Secure or insure?: a game-theoretic analysis of information security games. In *Proceedings of the 17th international conference on World Wide Web*, pages 209–218. ACM, 2008.
6. A. Hofmann. Internalizing externalities of loss prevention through insurance monopoly: an analysis of interdependent risks. *The GENEVA Risk and Insurance Review*, 32(1):91–111, 2007.
7. L. Hurwicz. Outcome functions yielding walrasian and lindahl allocations at nash equilibrium points. *The Review of Economic Studies*, 46(2):217–225, 1979.
8. L. Jiang, V. Anantharam, and J. Walrand. How bad are selfish investments in network security? *IEEE/ACM Transactions on Networking*, 19(2):549–560, 2011.
9. B. Johnson, R. Böhme, and J. Grossklags. Security games with market insurance. In *Decision and Game Theory for Security*, pages 117–130. Springer, 2011.
10. J. P. Kesan, R. P. Majuca, and W. J. Yurcik. The economic case for cyberinsurance. 2004.
11. H. Kunreuther and G. Heal. Interdependent security. *Journal of Risk and Uncertainty*, 26(2-3):231–249, 2003.
12. A. Laszka, M. Felegyhazi, and L. Buttyán. A survey of interdependent security games. *CRYSYS*, 2, 2012.

13. M. Lelarge. Economics of malware: Epidemic risks model, network externalities and incentives. In *47th Annual Allerton Conference on Communication, Control, and Computing*, pages 1353–1360. IEEE, 2009.
14. M. Lelarge and J. Bolot. Cyber insurance as an incentive for internet security. WEIS, 2008.
15. M. Lelarge and J. Bolot. Economic incentives to increase security in the internet: The case for insurance. In *INFOCOM 2009, IEEE*, pages 1494–1502. IEEE, 2009.
16. Marsh. Benchmarking trends: More companies purchasing cyber insuracne. March 2013.
17. P. Naghizadeh and M. Liu. Closing the price of anarchy gap in the interdependent security game. *Information Theory and Applications Workshop (ITA)*, 2013.
18. R. Pal, L. Golubchik, K. Psounis, and P. Hui. Will cyber-insurance improve network security: A market analysis. In *IEEE INFOCOM*, 2014.
19. S. Romanosky. Comments to the department of commerce on incentives to adopt improved cybersecurity practices. April 2013.
20. T. Saijo and T. Yamato. Fundamental impossibility theorems on voluntary participation in the provision of non-excludable public goods. *Review of Economic Design*, 14(1-2):51–73, 2010.
21. S. Sharma and D. Teneketzis. A game-theoretic approach to decentralized optimal power allocation for cellular networks. *Telecommunication Systems*, 47(1-2):65–80, 2011.
22. N. Shetty, G. Schwartz, M. Felegyhazi, and J. Walrand. Competitive cyber-insurance and internet security. In *Economics of Information Security and Privacy*, pages 229–247. Springer, 2010.
23. H. Varian. System reliability and free riding. *Economics of information security*, pages 1–15, 2004.