Analyzing Self-Defense Investments in Internet Security Under Cyber-Insurance Coverage

Ranjan Pal
Department of Computer Science
Univ. of Southern California
Email: rpal@usc.edu

Leana Golubchik
Department of Computer Science
Univ. of Southern California
Email: leana@usc.edu

***Abstract*—Internet users such as individuals and organizations are subject to different types of epidemic risks such as worms, viruses, and botnets. To reduce the probability of risk, an Internet user generally invests in self-defense mechanisms like antivirus and antispam software. However, such software does not completely eliminate risk. Recent works have considered the problem of residual risk elimination by proposing the idea of cyber-insurance. In this regard, an important decision for Internet users is their amount of investment in self-defense mechanisms when insurance solutions are offered.**

In this paper, we investigate the problem of self-defense investments in the Internet, under *full* and *partial* cyber-insurance coverage models. By the term 'self-defense investment', we mean the monetary-cum-precautionary cost that each user needs to invest in employing risk mitigating self-defense mechanisms, *given* that it is fully or partially insured by the Internet insurance agencies. We propose a general mathematical framework by which co-operative and non-co-operative Internet users can decide whether or not to invest in self-defense for ensuring both, individual and social welfare. Our results show that (1) co-operation amongst users results in more efficient self-defense investments than those in a non-cooperative setting, under a full insurance coverage model and (2) partial insurance coverage motivates non-cooperative Internet users to invest more efficiently in self-defense mechanisms when compared to full insurance coverage.

***Keywords:* cyber-insurance, Internet risks, self-defense investments, cyber-insurance coverage, co-operative and non-co-operative users**

I. Introduction

The Internet has become a fundamental and an integral part of our daily lives. Billions of people nowadays are using the Internet for various types of applications that demand different levels of security. For example, commercial and government organizations run applications that require a high level of security, since security breaches would lead to significant financial damage and loss of public reputation. On the other hand, an ordinary individual, for instance, generally uses a computing device for purposes that do not demand strict security requirements. There are other Internet applications running as well, which require intermediate levels of security. However, all these applications are running on a network, that was built under assumptions, some of which are no longer valid for today's applications, e.g., that all users on the Internet can be trusted and that the computing devices connected to the Internet are static objects. Today, the Internet comprises of both, good and malicious users. The malicious users perform illegal activities, are able to affect many users in a short time period, and at the same time reduce their chances of being discovered. Presently the users protect themselves through anti-spam software, firewalls, and other add-ons. However, new worms, viruses, and botnets emerge rapidly, and as a result these self-protection tools are not always effective security solutions. They only aid an Internet user in partially reducing its risk.

Little attention has been paid to an alternative approach to handling risks, specifically that of transferring risk to a different entity. An example of such a widely popular technique in modern life is insurance [3]. The risks are transferred to insurance companies, in return for a fee, i.e., the insurance premium. For instance, the works in [5][6][1] discuss cyber-insurance, in general, but without much focus on Internet insurance. In several recent papers [10][9][8][14], the authors show that (1) insurance would increase security on the Internet, (2) investments in both self-defense mechanisms and insurance schemes are quite inter-related in maintaining a socially efficient level of security on the Internet, and (3) without regulation, insurance is not a good incentive for self-defense. The work in [10] also gives conditions for jointly ensuring viability of insurance companies and improving network security. In a recent work [11], the authors have investigated risk management using cyber-insurance under different information availability scenarios between the insurer and the user, with respect to user security levels. In a stark contrast to existing works, they show that under all possible situations there is no market for cyber-insurance on the Internet (i.e., cyber-insurance increases individual user utility but *weakens* user incentives to improve overall network security). The authors define the network security level as the the probability that Internet users are attacked. They however, do not consider the interplay of self-defense investments and cyber-insurance investments, which plays an important part in improving user security levels. It is not surprising that the probability of users not being attacked may not be improved using cyber-insurance[1], but the judicious investments in both, self-defense and cyber-insurance can definitely improve individual user security, i.e., the probability of attacks *being successful* will

[1] The intentions of malicious users to attack the network generally do not change, unless there are mechanisms to track and punish them. Cyber-insurance does not provide a mechanism to track and punish the guilty.

be lowered, leading to a robust Internet (improving social welfare).

To the best of our knowledge, none of the previous efforts in [10][9][8][14][11] consider the *co-operative and the non-cooperative* nature of network users and the *effect* this has on the overall level of security and appropriate user self-defense investments. We note that the case of co-operating users is important for the following reasons: (1) It invites an opportunity for a user to benefit from the positive externality[2] that its investment poses on the other users in the network, and (2) Although, the majority of Internet users today are non co-operative and selfish in nature, i.e., they are primarily interested in maximizing their own performance without caring for the overall system performance, there exist Internet applications where co-operation amongst users is encouraged (e.g., distributed file sharing in peer-to-peer environments, multicasting, and efficient network resource sharing). Although, in such applications Internet users co-operate to improve performance, it is *not evident* that the same users are incentivized to co-operate on their security parameters (e.g., self-defense investment) as well.

Hence in this paper, we investigate the problem of appropriate self-defense investments under insurance regulation[3], *given* that Internet users are *fully* or *partially* covered by Internet insurance and that Internet users can be both, co-operative and non-co-operative *with respect* to their self-defense investment amounts. The contributions of our work are as follows:

- We quantitatively analyze an n-agent model, using *botnet* risks as a representative application, and propose a general mathematical framework through which co-operative and non-co-operative Internet users can decide whether to invest in self-defense mechanisms, given that each user is fully insured (see Section III). Our framework is applicable to all risk types that inflict direct and/or indirect losses to users.
- Under full insurance coverage, we perform a mathematical comparative study to show that co-operation amongst Internet users results in better self-defense investments when the risks faced by the users in the Internet are interdependent (see Section IV). We use basic concepts from both, co-operative and non-co-operative game theory to support the claims we make in Sections III and IV. Our results are applicable to co-operative (e.g., distributed file sharing) and non-cooperative Internet applications where a user has the option to be either co-operative or non-cooperative with respect to security parameters.
- We mathematically prove that in situations where co-operation amongst network users is not feasible at all, partial insurance coverage motivates users to invest more in self-protection when compared to full insurance coverage, thereby resulting in an increase in overall social welfare (see Section V).

We note that in practice, currently there exists virtually no insurance-like risk management capabilities in the present Internet [12]. However, cyber-insurance is a hot topic in Internet security and is being considered seriously by the research community for a potential solution to risk-free security guarantees for the next generation Internet [7]. We firmly believe that with the evolution of the Internet over time, the concept will become real and prove beneficial in the long run.

II. Economic Model

In this section we describe our proposed model. To ground the discussion in real systems, we first give a brief description of a representative application. That is, for purposes of clarity and ease of presentation, we first describe a representative application, namely that of ‘botnets’, as this is a reasonably rich and representative example of Internet threats. However, we would like to note that our approach can be applied to other applications with direct/indirect risk scenarios (for instance, such as worms and viruses).

A. Representative application

A bot is an end-user machine containing code that can be controlled by a remote administrator (bot herder) via a command and control network. Bots are created by finding vulnerabilities in computer systems. The vulnerabilities are exploited with malware and the malware is then inserted into the systems. A bot herder can subsequently program the bots and instruct them to perform various types of cyber-attacks. A malware infected computing device is susceptible to information theft from it. The infected device can become part of a botnet and in turn can be used to scan for vulnerabilities in other computer systems connected to the Internet, thus creating a cycle that rapidly infects vulnerable computer systems. Hence, bots result in both direct and indirect losses. Direct losses result when the bot herder infects machines that lack a security feature, whereas indirect losses result due to the contagion process of one machine getting infected by its neighbors.

Risks posed by bots are extremely common and spread rapidly. In a recent study, Symantec corporation observed approximately five million distinct bot-infected computers within a period of just six months between July, 2007 and December, 2007[10]. Here, we assume that Internet users could buy insurance from their Internet service providers (ISPs) to cover the risks posed by botnets. For instance, the coverage could be in the form of money or protection against lost data.

B. Model

We consider n identical[4] rational risk-averse users in a network. The users could be (1) entirely non co-operative in nature, i.e., the network supports Internet applications where users are not incentivized to co-operate with other users in

[2] An externality is a positive (external benefit) or negative (external cost) impact on a user not directly involved in an economic transaction.

[3] The term ‘insurance regulation’ refers to the act of making sure that insurance contracts are enforced by concerned parties in a proper and legal manner.

[4] In general, Internet users are not identical. However, our aim in this paper is to study certain general investment trends which we show, remain intact even if users are heterogenous.

any capacity (e.g., web surfing) or (2) co-operative to a variable degree, i.e, the network supports Internet applications where users co-operate with other users in some capacity to improve overall system performance but may or may not co-operate entirely. The users could either voluntarily co-operate by sharing information with other network users about their intentions to invest in self-defense, or be bound to co-operate due to a network regulation which requires participating users to share self-defense investment information. Each user has initial wealth w_0 and is exposed to a substantial risk of size R with a certain probability p_0. (Here, risk represents the negative wealth accumulated by a user when it is affected by botnet threats.) We also assume there exist markets for self-defense and cyber-insurance.

A user investing in self-defense mechanisms reduces its risk probability. For an amount x, invested in self-defense, a user faces a risk probability of $p(x)$, which is a continuous and twice differentiable decreasing function of investment, i.e., $p'(x) < 0$, $p''(x) > 0$, $lim_{x\to\infty}p(x) = 0$, and $lim_{x\to\infty}p'(x) = 0$.

The investment x is a function of the amount of security software the user buys and the effort it spends on maintaining security settings on its computing device. In addition to investing in self-defense mechanisms, a user may also buy *full* or *partial* cyber-insurance coverage at a particular premium to eliminate its residual risk. A user *does not* buy insurance for high probability low risk events because 1) these events are extremely common and does not cause sufficient damage to demand insurance solutions and 2) the insurance company also has reservations in insuring every kind of risk for profit purposes. We assume that the insurance market is perfectly competitive with no barriers to entry and exit, which results in actuarially fair premiums. We also account for the fact that the system does not face the moral hazard problem, i.e., a user insulated from risk does not behave differently from the way it would behave if it were fully exposed to the risk.

An Internet user apart from being directly affected by threats may be indirectly infected by the other Internet users. We denote the indirect risk facing probability of a user i as $q(\overrightarrow{x}_{-i}, n)$, where $\overrightarrow{x}_{-i} = (x_1, ..., x_{i-1}, x_{i+1}, ..., x_n)$ is the vector of self-defense investments of users other than i. An indirect infection spread is either 'perfect' or 'imperfect' in nature. In a perfect spread, infection spreads from a user to other users in the network with probability 1, whereas in case of imperfect spread, infection spreads from a user to others with probability less than 1. For a perfect information spread $q(\overrightarrow{x}_{-i}, n) = 1 - \prod_{j=1,j\neq i}^{n}(1 - p(x_j))$, whereas in the case of imperfect spread, $q(\overrightarrow{x}_{-i}, n) < 1 - \prod_{j=1,j\neq i}^{n}(1 - p(x_j))$. In this paper, we consider perfect spread only, without loss of generality because the probability of getting infected by others in the case of imperfect spread is less than that in the case of perfect spread, and as a result this case is subsumed by the results of the perfect spread case. Under perfect spread, the risk probability of a user i is given as

$$p(x_i) + (1 - p(x_i))q(\overrightarrow{x}_{-i}, n) = 1 - \prod_{j=1}^{n}(1 - p(x_j))$$

and its expected final wealth upon facing risk is denoted as $w_0 - x_i - (1 - \prod_{j=1}^{n}(1 - p(x_j)) \cdot IC) - R + IC$, where $(1 - \prod_{j=1}^{n}(1 - p(x_j)) \cdot IC$ is the fair premium and IC denotes the insurance coverage. In this paper, we use the terms 'final wealth' and 'expected final wealth' interchangeably. The aim of a network user is to invest in self-defense mechanisms in such a manner so as to maximize its expected utility of final wealth.

III. Mathematical Framework for Full Insurance Coverage

In this section, we assume full cyber-insurance coverage and propose a general mathematical framework for deciding on the appropriate self-defense investment of an Internet user. We model the following risk management scenarios: (1) users do not co-operate and do not get infected by other users in the network, (2) users co-operate and may get infected by other users in the network, (3) users do not co-operate but may get infected by other users in the network, and (4) users co-operate but do not get infected by other users in the network. We note that Case 4 is a special case of Case 2 and thus is subsumed in the results of Section III-B.

A. Case 1: No Co-operation, No Infection Spread

Under full insurance, the risk is equal to the insurance coverage, and users determine their optimal amount of self-defense investment by maximizing their level of final wealth, which in turn is equivalent to maximizing their expected utility of wealth [4]. We can determine the optimal amount of self-defense investment for each user i by solving for the value of p that maximizes the following constrained optimization problem:

$$argmax_{x_i}FW_i(x_i) = w_0 - x_i - p(x_i)R - R + IC$$

or

$$argmax_{x_i}FW_i(x_i) = w_0 - x_i - p(x_i)R$$

subject to

$$0 \leq p(x_i) \leq p_0,$$

where FW_i is the final wealth of user i and $p(x_i)R$ is the actuarially fair premium for full insurance coverage. Taking the first and second derivatives of FW_i with respect to x_i, we obtain

$$FW_i'(x_i) = -1 - p'(x_i)R$$

$$FW_i''(x_i) = -p''(x_i)R < 0$$

Thus, our objective function is globally concave. Let x_i^{opt} be the optimal x_i obtained by equating the first derivative to 0. Thus, we have:

$$p'(x_i^{opt})R = -1. \qquad (1)$$

Economic Interpretation: The left hand side (LHS) of Equation (1) is the marginal benefit of investing an additional dollar in self-protection mechanisms, whereas the right hand side (RHS) denotes the marginal cost of the investment. A user equates the LHS with the RHS to determine its self-defense investment.

Conditions for Investment: We first investigate the boundary costs. The user will not consider investing in self-defense if $p'(0)R \geq -1$ because its marginal cost of investing in any defense mechanism, i.e., -1, will be relatively equal to or lower than the marginal benefit when no investment occurs. In this case, $x_i^{opt} = 0$. If the user invests such that it has no exposure to risk, $x_i^{opt} = \infty$. When $p'(0)R < -1$, the costs do not lie on the boundary, i.e., $0 < x_i^{opt} < \infty$, and the user invests to partially eliminate risk (see Equation (1)).

B. Case 2: Co-operation, Infection spread

Under full insurance coverage, user i's expected final wealth is given by

$$FW_i = FW(x_i, \overrightarrow{x}_{-i}) = w_0 - x_i - (1 - \prod_{j=1}^{n}(1-p(x_j)))R$$

When Internet users co-operate, they jointly determine their optimal self-defense investments. We assume that co-operation and bargaining costs are nil. In such a case, according to Coase theorem [13], the optimal investments for users are determined by solving for the socially optimal investment values that maximize the aggregate final wealth (AFW) of all users. Thus, we have the following constrained optimization problem:

$$argmax_{x_i, \overrightarrow{x}_{-i}} AFW = nw_0 - \sum_{i=1}^{n} x_i - n(1 - \prod_{j=1}^{n}(1-p(x_j)))R$$

$$0 \leq p_i(x_i) \leq p_0, \forall i$$

Taking the first and the second partial derivatives of the aggregate final wealth with respect to x_i, we obtain

$$\frac{\partial}{\partial x_i}(AFW) = -1 - np'(x_i) \prod_{j=1, j\neq i}^{n} (1-p(x_j))R$$

$$\frac{\partial^2}{\partial x_i^2}(AFW) = -np''(x_i) \prod_{j=1, j\neq i}^{n} (1-p(x_j))R < 0$$

The objective function is globally concave, which implies the existence of a unique solution $x_i^{opt}(\overrightarrow{x}_{-i})$, for each $\overrightarrow{x}_{-i}$. Our maximization problem is symmetric for all i, and thus the optimal solution is given by $x_i^{opt}(\overrightarrow{x_{-i}^{opt}}) = x_j^{opt}(\overrightarrow{x_{-j}^{opt}})$ for all $j = 2, ..., n$. We obtain the optimal solution by equating the first derivative to zero, which gives us the following equation

$$np'(x_i^{opt}(\overrightarrow{x}_{-i})) \prod_{j=1, j\neq i} (1-p(x_i))R = -1 \qquad (2)$$

Economic Interpretation: The left hand side (LHS) of Equation (2) is the marginal benefit of investing in self-defense. The right hand side (RHS) of Equation (2) is the marginal cost of investing in self-defense, i.e., -1. We obtain the former term of the marginal benefit by internalizing the positive externality[5], i.e., by accounting for the self-defense investments of other users in the network. The external well-being posed to other users by user i when it invests an additional dollar in self-defense is $-p'(x_i)\prod_{j=1,j\neq i}^{n}(1-p(x_i))$. This is the amount by which the likelihood of each of the other users getting infected is reduced, when user i invests an additional dollar.

Conditions for Investment: If $np'(0)\prod_{j=1,j\neq i}^{n}(1 - p(x_j))R \geq -1$, it is not optimal to invest any amount in self-defense because the marginal cost of investing in defense mechanisms is relatively equal to or less than the marginal benefit of the joint reduction in risks to individuals when no investment occurs. In this case, the optimal value is a boundary investment, i.e., $x_i^{opt}(\overrightarrow{x}_{-i}) = 0$. If the user invests such that it has no exposure to risk, $x_i^{opt} = \infty$. In cases where $np'(0)\prod_{j=1,j\neq i}^{n}(1-p(x_j))R < -1$, the optimal probabilities do not lie on the boundary and the user invests to partially eliminate risk (see Equation (2)).

C. Case 3: No Co-operation, Infection Spread

We assume that users do not co-operate with each other on the level of investment, i.e., users are selfish. In such a case, the optimal level of self-defense investment is the pure strategy Nash equilibria of the normal form game, $G = (N, A, u_i(s))$, played by the users [2]. The game consists of two players, i.e., $|N| = n$; the action set of G is $A = \prod_{i=1}^{n} \times A_i$, where $A_i \, \epsilon \, [0, \infty]$, and the utility/payoff function $u_i(s)$ for each player i is their individual final wealth, where $s \, \epsilon \prod_{i=1}^{n} \times A_i$. The pure strategy Nash equilibria of a normal form game is the intersection of the best response functions of each user [2].

We define the best response function of user i, $x_i^{best}(\overrightarrow{x}_{-i})$, as

$$x_i^{best}(\overrightarrow{x}_{-i}) \, \epsilon \, argmax_{x_i} FW_i(x_i, \overrightarrow{x}_{-i}),$$

where

$$FW_i(x_i, \overrightarrow{x}_{-i}) = w_0 - x_i - (1 - \prod_{j=1}^{n}(1-p(x_j)))R$$

Taking the first and second partial derivative of $FW_i(x_i, \overrightarrow{x}_{-i})$with respect to x_i and equating it to zero, we obtain

$$\frac{\partial}{\partial x_i}(FW_i(x_i, \overrightarrow{x}_{-i})) = -1 - p'(x_i) \prod_{j=1, j\neq i}^{n} (1-p(x_j))R$$

$$\frac{\partial^2}{\partial x_i^2}(FW_i(x_i, \overrightarrow{x}_{-i})) = -p''(x_i) \prod_{j=1, j\neq i}^{n} (1-p(x_j))R < 0$$

Thus, our objective function is globally concave, which implies a unique solution $x_i^{best}(\overrightarrow{x}_{-i})$ for each $\overrightarrow{x}_{-i}$. We also observe that a particular user i's strategy complements user j's strategy for all j, which implies that only *symmetric* pure

[5] Internalizing a positive externality refers to rewarding a user, who contributes positively and without compensation, to the well-being of other users, through its actions.

strategy Nash equilibria exist. The optimal investment for user i is determined by the following equation:

$$\frac{\partial}{\partial x_i}(FW_i(x_i, \overrightarrow{x}_{-i})) =$$
$$-1 - p'(x_i) \prod_{j=1, j\neq i}^{n} (1 - p(x_j))R = 0 \qquad (3)$$

Economic Interpretation: The left hand side (LHS) of Equation (3) is the marginal benefit of investing in self-defense. The right hand side (RHS) of Equation (3) is the marginal cost of investing in self-defense, i.e., -1. Since the users cannot co-operate on the level of investment in self-defense mechanisms, it is not possible for them to benefit from the positive externality that their investments pose to each other.

Conditions for Investment: If $p'(0)\prod_{j=1,j\neq i}^{n}(1-p(x_j))R \geq -1$, it is not optimal to invest any amount in self-defense because the marginal cost of investing in defense mechanisms is greater than the marginal benefit of the joint reduction in risks to individuals when no investment occurs. In this case, the optimal value is a boundary investment, i.e., $x_i^{best}(\overrightarrow{x}_{-i}) = 0$. If the user invests such that it has no exposure to risk, $x_i^{opt} = \infty$. In cases where $p'(0)\prod_{j=1,j\neq i}^{n}(1-p(x_j))R < -1$, the optimal probabilities do not lie on the boundary and the user invests to partially eliminate risk (see Equation (3)).

Multiplicity of Nash Equilibria: Due to the symmetry of our pure strategy Nash equilibria and the increasing nature of the best response functions, there always exists an odd number of pure-strategy Nash equilibria, i.e., $x_i^{best}(\overrightarrow{x}_{-i}^{best}) = x_j^{best}(\overrightarrow{x}_{-j}^{best})$ for all $j = 2, \ldots, n$.

IV. Comparative Study

In this section, we compare the optimal level of investments in the context of various cases discussed in the previous section. Our results are applicable to Internet applications where a user has the option to be either co-operative (e.g., distributed file sharing applications) or non-cooperative with respect to security parameters.

A. Case 3 versus Case 1

(3) The following lemma gives the result of comparing Case 3 and Case 1.

Lemma 1. *If Internet users do not co-operate on their self-defense investments (i.e., do not account for the positive externality posed by other Internet users), in any Nash equilibrium in Case 3, the users inefficiently under-invest in self-defense as compared to the case where users do not cooperate and there is no infection spread.*

Proof. In Case 1, the condition for any user i not investing in any self-defense is $-p'(0)R \leq 1$. The condition implies that $-1-p'(0)\prod_{j=1,j\neq i}^{n}(1-p(x_j))R < 0$ for all $\overrightarrow{x}_{-i}$. The latter expression is the condition for non-investment in Case 3. Thus, for all users i, $x_i^{opt} = 0$ in Case 1 implies $x_i^{best} = 0$ in Case 3, i.e., $x_i^{opt}(\overrightarrow{x_{-i}^{opt}}) = x_i^{best}(\overrightarrow{x_{-i}^{best}}) = 0, \forall i$. The condition for optimal investment of user i in Case 1 is $-1-p'(x_i)R = 0$. Hence, $-1 - p'(x_i)\prod_{j=1,j\neq i}^{n}(1 - p(x_j))R < 0$, for all x_{-i}. Thus, in situations of self-investment for user i, $x_i^{opt} > 0$ in Case 1 implies $0 \leq x_i^{best} < x_i^{opt}$, for all x_{-i}, in Case 3, i.e., $x_i^{opt}(\overrightarrow{x_{-i}^{opt}}) > x_i^{best}(\overrightarrow{x_{-i}^{best}}) \geq 0, \forall i$. Therefore, under non-cooperative settings, a user always under-invests in self-defense mechanisms. ■

B. Case 3 versus Case 2

The following lemma gives the result of comparing Case 3 and Case 2.

Lemma 2. *Under environments of infection spread, an Internet user co-operating with other users on its self-defense investment (i.e., accounts for the positive externality posed by other Internet users), always invests at least as much as in the case when it does not co-operate.*

Proof. In Case 2, the condition for any user i not investing in any self-defense mechanism is $-1 - np'(0)(1 - p(0))^{n-1}R \leq 0$. The condition also implies that $-1 - np'(0)(1 - p(0))^{n-1}R \leq 0$. The latter expression is the condition in Case 3 for an Internet user not investing in any self-defense mechanism. Thus, for all users i, $x_i^{opt} = 0$ in Case 2 implies $x_i^{best} = 0$, for all Nash equilibrium in Case 3, i.e., $x_i^{opt}(\overrightarrow{x_{-i}^{opt}}) = x_i^{best}(\overrightarrow{x_{-i}^{best}}) = 0, \forall i$. The condition for optimal investment of each user i in Case 2 is $-1-np'(x_i^{opt}(\overrightarrow{x_{-i}^{opt}})(1-p(x_i^{opt}(\overrightarrow{x_{-i}^{opt}}))^{n-1}R = 0$. The latter expression implies $-1 - p'(x_i^{opt}(\overrightarrow{x_{-i}^{opt}})(1 - p(x_i^{opt}(\overrightarrow{x_{-i}^{opt}}))^{n-1}R < 0$. Hence $x_i^{opt}(\overrightarrow{x_{-i}^{opt}}) > x_i^{best}(\overrightarrow{x_{-i}^{best}}) \geq 0, \forall i$. Therefore, under environments of infection spread, a user in Case 3 always under invests in self-defense mechanisms when compared to a user in Case 2. ■

C. Case 2 versus Case 1

The following lemma gives the result of comparing Case 2 and Case 1.

Lemma 3. *In any n-agent cyber-insurance model, where $p(0) < 1 - \sqrt[n-1]{\frac{1}{n}}$, it is always better for Internet users to invest more in self-defense in a co-operative setting with infection spread than in a non-co-operative setting with no infection spread.*

Proof. In Case 1, the condition for any user i not investing in any self-defense is $-p'(0)R \leq 1$. The condition implies that $-1-np'(0)(1-p(0))^{n-1}R \leq 0$ for all $p_0 < 1 - \sqrt[n-1]{\frac{1}{n}}$. Thus, for all i, $x_i^{opt}(\overrightarrow{x_{-i}^{opt}}) = 0$ in Case 1 implies $x_i^{opt}(\overrightarrow{x_{-i}^{opt}}) \geq 0$ in Case 3 if and only if $p_0 < 1 - \sqrt[n-1]{\frac{1}{n}}$. In situations of non-zero investment

$$-1 - np'(x_i(\overrightarrow{x}_{-i}))(1 - p(x_i(\overrightarrow{x}_{-i}))^{n-1})R >$$
$$-1 - p'(x_i(\overrightarrow{x}_{-i})), \forall i, \forall x_i(\overrightarrow{x}_{-i}),$$

if and only if $p(x_i(\overrightarrow{x}_{-i})) < 1 - \sqrt[n-1]{\frac{1}{n}}$. Hence,

$$-1 - np'(x_i^{opt}(\overrightarrow{x_{-i}^{opt}})(1 - p(x_i^{opt}(\overrightarrow{x_{-i}^{opt}}))^{n-1})R >$$
$$-1 - p'(x_i^{opt}(\overrightarrow{x_{-i}^{opt}})), \forall i,$$

where $x_i^{opt}(\overrightarrow{x_{-i}^{opt}})$ is the optimal investment in Case 2. Since the expected final wealth of a user in Case 1 is concave in $x_i(\overrightarrow{x}_{-i})$, $x_i^{opt}(\overrightarrow{x_{-i}^{opt}})$ in Case 2 is greater than $x_i^{opt}(\overrightarrow{x_{-i}^{opt}})$ in Case 1. Thus, we infer that investments made by users in Case 2 are always greater than those made by users in Case 1 when the risk probability is less than a threshold value that decreases with increase in the number of Internet users. Hence, in the limit as the number of users tends towards infinity, the lemma holds for all p_0. ■

The basic intuition behind the results in the above three lemmas is that internalizing the positive effects on other Internet users leads to better and appropriate self-defense investments for users. We also emphasize that our result trends hold true in case of heterogenous network users because irrespective of the type of users, co-operating on investments always leads to users accounting for the positive externality and investing more efficiently. The only difference in case of heterogenous network user scenarios could be the value of probability thresholds i.e., $p(0)$ (this value would be different for each user in the network), under which the above lemmas hold.

Based on the above three lemmas, we have the following theorem.

Theorem 1. *If Internet users cannot contract on the externalities, in any Nash equilibrium, Internet users inefficiently under-invest in self-defense, that is compared to the socially optimal level of investment in self-defense. In addition, in any Nash equilibrium, a user invests less in self-defense than if they did not face the externality. Furthermore, if $p(0) < 1 - \sqrt[n-1]{\frac{1}{n}}$, the socially optimal level of investment in self-defense is higher compared to the level if Internet users did not face the externality.*

Proof. The proof follows directly from the results in Lemmas 1, 2, and 3. ■

V. Mathematical Framework for Partial Insurance Coverage

In the previous section, we proved that Internet users inefficiently under-invest in self-defense mechanisms if they do not co-operate with other users in a network. In this section, we show that in non-cooperative environments, charging a deductible on the user insurance amount (partial cyber-insurance), results in improvement in individual and social welfare when compared to the case in Section III-C. The intuition behind charging a deductible is that each user will bear part of its own loss and therefore is more likely to invest more in self-defense mechanisms than if it had full cyber-insurance coverage. Since our goal is to simply show that partial cyber-insurance in a non-cooperative network setting improves welfare, for ease of exposition we analyze a two-user model to arrive at our result. We denote the users as i and j. Our result is applicable to a network with any number of users.

A. Case A: No Co-operation, No Infection Spread

Under partial insurance, users determine their optimal amount of self-defense investment by maximizing their expected utility of final wealth, which is *not* equivalent to maximizing the expected final wealth [4]. Thus, we have to perform our analysis based on utility functions rather than based on the expected value of final wealth.

Let $U()$ be an increasing and concave utility function for each user in the network such that $U' > 0$ and $U'' < 0$. We can determine the optimal amount of self-defense investment for each user i by solving for the value of p_i that maximizes the following constrained optimization problem:

$$argmax_{p_i} UFW(p_i) = U(w_0 - x(p_0 - p_i) - p_i \cdot (R - D))$$
$$0 \leq p_i \leq p_0,$$

where UFW is the utility of final wealth of a user, $x(\Delta p)$, a function of the difference of p_0 and p_i, represents user i's cost of reducing the risk probability from p_0 to p_i, $\Delta p = p_0 - p_i$, and $0 < D < R$ is the deductible in cyber-insurance. We assume that x is monotonically increasing and twice differentiable with $x(0) = 0$, $x'(0) > 0$, and $x''(0) > 0$, and $p_i \cdot (R - D)$ is the actuarially fair premium for user i's partial insurance coverage. Taking the first and second derivatives of UFW with respect to p_i, we obtain

$$UFW'(p_i) = U'(A) \cdot B,$$

where

$$A = w_0 - x(p_0 - p_i) - (R - D),$$
$$B = [x'(p_0 - p_i) - (R - D)]$$
$$UFW''(p_i) = U''(A) \cdot B^2 + C \cdot U'(A) < 0,$$

and

$$C = [-x''(p_0 - p_i) - (R - D)]$$

Thus, our objective function is globally concave with p_i^{opt} being the optimal p_i obtained by equating the first derivative to 0. According to our hypothesis, $U'() > 0$. Thus, any user will not consider investing in self-defense if $x'(0) \geq R - D$ because its marginal cost of investing in any defense mechanism will be relatively equal or higher than its benefit of reducing the expected risk. In this case, $p_i^{opt} = p_0$. If $x'(p_0) < R - D$, then $p_i^{opt} = 0$ because the marginal cost of completely eliminating the probability of risk is small relative to the magnitude of the risk itself. In this case, the user will invest such that it has absolutely no exposure to risk. When $x'(0) < R - D < x'(p_0)$, the probabilities do not lie on the boundary, i.e., $0 < p_i^{opt} < p_0$, and the user invests to partially eliminate risk. It is evident that with $D > 0$ the condition for investment in self-defense mechanisms is more relaxed than that in Section III-A. Thus, a user having partial insurance coverage is more motivated to invest in self-defense mechanisms under non-cooperative scenarios. The following lemma states our result.

Lemma 4. *In a 2-user network, where the users are not incentivized to co-operate, a positive deductible on the insurance coverage always motivates the users to invest more in self-defense mechanisms as compared to a full insurance coverage scenario.*

Proof. The proof follows directly from the reasoning in the previous paragraph. ■

B. Case B: No Co-operation, Infection Spread

As mentioned earlier, enforcing a deductible in partial insurance coverage scenarios may lead to better self-defense investments on part of Internet users and in turn contribute to social and individual welfare. In this section, we derive conditions for optimally charging a strictly positive deductible, and show that welfare is indeed improved when compared to a non-cooperative scenario with full insurance coverage.

Similarly to Section III-C, under partial insurance coverage, user i's expected utility of final wealth is determined as

$$UFW_i = UFW_i(p_i, p_j, D) = \alpha + \beta,$$

where

$$\alpha = (1-p_i)(1-p_j)U(w_0 - x(\Delta p_i) - P(D))$$

and

$$\beta = (p_i + (1-p_i)p_j)U(w_0 - x(p_0 - p_i) - P(D) - D)$$

We define $P(D)$ as the actuarially fair premium, and it is expressed as

$$P(D) = (p_i + (1-p_i)(R-D)$$

We denote the best response of user i under a deductible as the solution to the following constrained optimization problem:

$$p_i^{bestD}(p_j, D) \,\epsilon\, argmax_{p_i} UFW(p_i, p_j)$$

$$0 \leq p_i, p_j \leq 1$$

Then, the following lemma states the conditions for strictly positive deductibles.

Lemma 5. *For a 2-user network, given that $x''(p_0 - p_i^{best}) > R$, the optimally enforced deductible is strictly positive if and only if, for each user i: (i) $(1-p_i^{best})^2 R > (1-(1-p_i^{best}))^2 x''(p_0 - p_i^{best})$, and (ii) $p_i^{best} < 1 - \sqrt{\frac{1}{2}}$, where p_i^{best} is the risk probability in a Nash equilibrium, under full insurance coverage.*

Proof. Let $p^{bestD}(D)$ denote the symmetric pure strategy Nash equilibrium of the optimization problem defined in this section, i.e., $p^{bestD}(D) = p_i^{bestD}(p_j^{best}(D), D) = p_j^{bestD}(p_i^{best}(D), D)$. The Nash equilibrium satisfies the first order condition given by

$$E1 + E2 + E3 = 0, \tag{4}$$

where

$$E1 = (1 - p^{bestD}(D)) \cdot (\alpha 1 - \beta 1),$$

$$E2 = K1 \cdot \alpha 2,$$

$$E3 = K2 \cdot \alpha 3,$$

$$\alpha 1 = U(w_0 - x(p_0 - p^{bestD}(D)) - P(D) - D),$$

$$\beta 1 = U(w_0 - x(p_0 - p^{bestD}(D)) - P(D)),$$

$$K1 = (1 - p^{bestD}(D))^2 \cdot K11,$$

$$K11 = (x'(p_0 - p^{bestD}(D)) - (1 - p^{bestD}(D))(R - D)),$$

$$\alpha 2 = U'(w_0 - x(p_0 - p^{bestD}(D)) - P(D)),$$

$$K2 = p^{bestD}(D)(2 - p^{bestD}(D)) \cdot K11,$$

$$\alpha 3 = U'(w_0 - x(p_0 - p^{bestD}(D)) - P(D) - D),$$

Substituting $D = 0$, in the first order condition, we obtain

$$x'(p_0 - p^{bestD}(0)) - (1 - p^{bestD}(0))R = 0$$

For a particular D, the expected utility of final wealth for user i is

$$UFW_i(p^{bestD}(D), p^{bestD}(D), D) = I + J,$$

where

$$I = (1 - p^{bestD}(D))^2 \cdot \zeta$$

and

$$J = 2 - p^{bestD}(D))p^{bestD}(D) \cdot \eta$$

$$\zeta = U(w_0 - x(p_0 - p^{bestD}(D)) - P(D))$$

$$\eta = U(w_0 - x(p_0 - p^{bestD}(D)) - P(D) - D)$$

Taking the first derivative of the expected utility with respect to D and substituting $D = 0$, we obtain

$$\frac{\partial UFW_i(p^{bestD}(D), p^{bestD}(D), D)}{\partial D}_{D=0} = G \cdot UT*,$$

where

$$G = -p^{\prime bestD}(0)(1 - p^{bestD}(0))R$$

and

$$UT* = U'(w_0 - x(p_0 - p^{bestD}(0)) - P(0))$$

We determine the sign of the first derivative of the expected utility by implicitly differentiating the first order condition with respect to D and evaluating it to 0. We obtain the following relation

$$p^{\prime bestD}(0)(R - x''(p_0 - p^{\prime bestD}(0))) = 0$$

From the above relation, we observe that $p^{\prime bestD}(0) = 0$ if and only if $(R - x''(p_0 - p^{\prime bestD}(0))) \neq 0$. We also note that when $D = 0$, the Nash equilibria of the non-cooperative game coincides with those when full insurance coverage is offered. We now prove that in a 2-user non-cooperative network with infection spread, and under full insurance coverage, $x''(p_0 - p'^{best}(0)) > R$ is a condition satisfied under all Nash equilibria. We define the best response function of user i, $p_i^{best}(p_j)$, as

$$p_i^{best}(p_j)\, \epsilon\, argmax_{p_i} FW_i(p_i, p_j) = w_0 - x(\Delta p_i) - P_R(i)R$$

where $P_R(i) = p_i + (1 - p_i)p_j$. Taking the first derivative with respect to p_i and equating it to zero, we obtain

$$x'(p_0 - p_i^{best}(p_j)) - (1 - p_j)R = 0$$

Differentiating again with respect to p_j, we obtain

$$-p_i^{best'}(p_j) \cdot x''(p_0 - p_i^{best}(p_j)) + R = 0$$

Therefore,

$$p_i^{best'}(p_j) = \frac{R}{x''(p_0 - p_i^{best}(p_j))} > 0$$

Since $0 < p_i^{best'}(p_j) < 1, x''(p_0 - p'^{best}(0)) > R$, for all symmetric pure Nash equilibria. Thus,

$${\frac{\partial UFW_i(p^{bestD}(D), p^{bestD}(D), D)}{\partial D}}_{D=0} = 0$$

We now determine the sign of the second derivative of expected utility of final wealth evaluated at $D = 0$. The second derivative evaluated at $D = 0$ gives

$${\frac{\partial^2 UFW_i(p^{bestD}(D), p^{bestD}(D), D)}{\partial D}}_{D=0} = E + F, \qquad (5)$$

where

$$\begin{aligned} &E = \\ &-p''^{bestD}(0)(1 - p^{bestD}(0))RU' \times \\ &(w_0 - x(p_0 - p^{bestD}(0)) - P(0)) \end{aligned}$$

and

$$F = (1 - p^{bestD}(0))^2 p^{bestD}(0)(2 - p^{bestD}(0)) \cdot UT,$$

where

$$UT = U''(w_0 - x(p_0 - p^{bestD}(0)) - P(0))$$

Double differentiating the first order condition, in Equation (4), implicitly with respect to D, and substituting $D = 0$ we get the value of $p''^{bestD}(0)$ as

$$p''^{bestD}(0) = \frac{M}{Z}, \qquad (6)$$

where M equals

$$(1 - p^{bestD}(0))(1 - 2(1 - p^{bestD}(0))^2) \cdot UT$$

and

$$Z = (R - x''(p_0 - p^{bestD}(0))) \cdot UT$$

It is evident from Equation (6) that a value of $p''^{bestD}(0) < 1 - \sqrt{\frac{1}{2}}$ ensures $p''^{bestD}(0) < 0$. Hence, for such a value of $p''^{bestD}(0)$, small deductible amounts increase the self-defense investment of Internet users and in turn contributes to an improvement in both, social and individual welfare when compared to the case of non-cooperation with full insurance coverage.

Substituting Equation (6) into Equation (5), we obtain

$${\frac{\partial^2 UFW_i(p^{bestD}(D), p^{bestD}(D), D)}{\partial D}}_{D=0} = \gamma \cdot \delta$$

where

$$\gamma = 1 - (1 - p^{bestD}(0))^2 - \frac{(1 - 2(1 - p^{bestD}(0))^2)R}{(R - x''(p_0 - p^{bestD}(0)))})$$

and

$$\delta = (1 - p^{bestD}(0))^2 U''(w_0 - x(p_0 - p^{bestD}(0)) - P(0))$$

A strictly positive deductible is positive if and only if

$${\frac{\partial^2 UFW_i(p^{bestD}(D), p^{bestD}(D), D)}{\partial D}}_{D=0} > 0$$

and that occurs if and only if

$$(1 - p_i^{bestD})^2 R > (1 - (1 - p_i^{bestD}))^2 x''(p_0 - p_i^{bestD}). \blacksquare$$

The basic intuition behind our results is that additional investments in self-defense create an external benefit through the positive externality that exists between the Internet users. Our stated theorems specify the conditions under which this benefit outweighs the cost of users bearing part of the risk. Our results are scalable when n users are present in the network. It can be conjectured that in the limit when $n \to \infty$, positive deductibles result for all Nash equilibria p^{bestD}. More generally, we also *conjecture* that in a network with n users, positive deductibles result for $p^{bestD} < 1 - \sqrt[n]{\frac{1}{n}}$. Based on Lemmas 4 and 5, we state the following theorem summarizing our results.

Theorem 2. *In a 2-user network, positive deductibles always motivate non-cooperative users to invest more in self-defense investments when compared to full coverage scenarios, and thereby help in increasing individual and social welfare when there is no infection spread; they do so in cases of infection spread if and only if* $p^{bestD} < 1 - \sqrt{\frac{1}{2}}$.

Proof: The proof follows directly from the results in Lemmas 4 and 5. $\blacksquare$

VI. Conclusions and Future Directions

In this paper, we investigated the problem of self-defense investments in the Internet, under the *full insurance* and *partial insurance* coverage models. We showed that (1) co-operation amongst users results in more efficient self-defense investments than those in a non-cooperative setting, under a full insurance coverage model and (2) partial insurance motivates non-cooperative Internet users to invest efficiently in self-defense mechanisms.

Cyber-insurance is a relatively new area of research, with many open questions in both, theoretical and systems directions. For instance, one could consider the presence of informational asymmetry between the insurer and the insured. The problem is more on the insurer side as the insured have the freedom to hide information from the insurer. This might lead to poor and unprofitable business models on behalf of the cyber-insurance company. One could also consider using intermediary organizations between the insurer and the insured to make sure that there are minimal or no informational asymmetries between the insurer and the insured, which would result in a transparent environment within which Internet users could make correct and appropriate investments.

There are also interesting directions to pursue in the context of distributed systems. For instance, we note that in cooperative scenarios, distributed applications could consider adding information, to already existing protocol messages, indicating whether or not a particular user/node (participating in the application) has invested in cyber-insurance. For example, we could imagine a peer-to-peer file downloading application, where users joining the peer-to-peer overlay could include (in their join messages) information about the protection in which they have invested; of course, such information could also be "piggybacked" on update messages which are typical of distributed applications. Moreover, we could imagine modifying peer-to-peer protocols to include a bias towards exchanging data with nodes that do invest in protection - e.g., nodes could be (a) more biased towards being neighbors (in the overlay) of nodes that do invest in protection and/or (b) more biased towards exchanging data with nodes that invest in protection. It would also be interesting to consider whether adding information about the level of investment is useful in such applications and what are the possible effects, on the applications, of providing such information as well as the degree of user truthfulness needed in such information in order to produce positive effects. In this regard, we could look at truth binding *mechanism design* models in games. Lastly, it would also be interesting to explore how our model could be applied (or adapted) in the context of mobile and wireless networks. Although presently our model does not consider user mobility, it may still provide interesting insights as we do not make assumptions that prevent its applicability in such a domain.

VII. Acknowledgements

We would like to sincerely thank Professor Konstantinos Psounis for his insightful comments. We would also like to thank the anonymous reviewers for their feedback, used in improving the paper. This work was supported in part by the USC Provost Fellowship, the IBM Faculty Award, and the NSF 0540420 and 0917340 grants.

References

[1] B.Schneier. Its the economics, stupid. In *WEIS*, 2002.

[2] D.Fudenberg and J.Tirole. *Game Theory*. MIT Press, 1991.

[3] H.Kunreuther and G.Heal. Interdependent security. *Journal of Risk and Uncertainty*, 26, 2002.

[4] I.Ehrlick and G.S. Becker. Market insurance, self-insurance, and self-protection. *Journal of Political Economy*, 80(4), 1972.

[5] J.Kesan, R.Majuca, and W.Yurcik. *The economic case for cyberinsurance: In Securing Privacy in the Internet Age*. Stanford University Press, 2005.

[6] J.Kesan, R.Majuca, and W.Yurcik. Cyberinsurance as a market-based solution to the problem of cybersecurity: A case study. In *WEIS*, 2005.

[7] J.Walrand. *Personal Communication*.

[8] M.Lelarge and J.Bolot. Cyber insurance as an incentive for internet security. In *WEIS*, 2008.

[9] M.Lelarge and J.Bolot. A new perspective on internet security using insurance. In *IEEE INFOCOM*, 2008.

[10] M.Lelarge and J.Bolot. Economic incentives to increase security in the internet: The case for insurance. In *IEEE INFOCOM*, 2009.

[11] N.Shetty, G.Schwarz, M.Feleghyazi, and J.Walrand. Competitive cyber-insurance and internet security. In *WEIS*, 2009.

[12] R.Anderson, R.Boehme, R.Clayton, and T.Moore. Security economics and european policy. In *WEIS*, 2008.

[13] R.H.Coase. The problem of social cost. *Journal of Law and Economics*, 3, 1960.

[14] S.Radosavac, J.Kempf, and U.C.Kozat. Using insurance to increase internet security. In *ACM NetEcon*, 2008.