# Economic Incentives to Increase Security in the Internet: The Case for Insurance

Marc Lelarge
INRIA-ENS
France
Email: marc.lelarge@ens.fr

Jean Bolot
SPRINT
USA
Email: bolot@sprint.com

***Abstract*—Entities in the Internet, ranging from individuals and enterprises to service providers, face a broad range of epidemic risks such as worms, viruses, and botnet-driven attacks. Those risks are interdependent risks, which means that the decision by an entity to invest in security and self-protect affects the risk faced by others (for example, the risk faced by an individual decreases when its providers increases its investments in security). As a result of this, entities tend to invest too little in self-protection, relative to the socially efficient level, by ignoring benefits conferred on by others.**

**In this paper, we consider the problem of designing incentives to entities in the Internet so that they invest at a socially efficient level. In particular, we find that insurance is a powerful incentive mechanism which pushes agents to invest in self-protection. Thus, insurance increases the level of self-protection, and therefore the level of security, in the Internet. As a result, we believe that insurance should be considered as an important component of risk management in the Internet.**

## I. Introduction

The infrastructure, the users, and the services offered on the Internet are all subject to a wide variety of risks, both malicious (such as denial of service attacks, intrusions of various kinds, phishing, worms and viruses, etc) and non-intentional (such as overloads or denial of service caused by flash crowds). The approach typically taken to manage those risks has been to accept the loss when it occurs, and in parallel to develop and deploy methods to reduce the likelihood of loss, reduce the impact of the risk and therefore reduce the severity of the damages. In practice, this has led to a vast industry, and a large scale effort in the research community, centered around tools and techniques to detect threats and anomalies and to protect the network infrastructure and its users from the negative impact of those anomalies, along with efforts in the area of security education in an attempt to minimize the risks related to the human factor.

Comparatively very little attention has been focused, and work been done, on an alternative approach to handling risks, namely the transfer of risk to another entity through contract or hedging. A widely known way to do that in many areas of modern life is through insurance. There, the risk is transferred to an insurance company, in return for a fee which is the insurance premium.

The Internet has become a fundamental infrastructure of modern economies, yet ”Internet insurance” is still in its infancy. Cyberinsurance, or the insurance of computer risks in general (without much focus on network environments specifically) was proposed more than 10 years ago [16] but popularized only recently [25], [26]. The authors in [13], [14] make the the economic case for insurance, arguing that insurance results in higher security investments (and therefore increases the global level of safety), that it encourages standards for best practices to be at the socially optimum level, and that it solves a market failure (namely the absence of risk transfer opportunity), and they see the emerging market for cyberinsurance as a validation of the case they make in the paper.

The market for cyberinsurance started in the late 90’s with insurance policies offered by security software companies partnering with insurance companies as packages (software + insurance). The insurance provided a way to highlight the (supposedly high) quality of the security software being sold, and to deliver a ”total” risk management solution (risk reduction + residual risk transfer), rather than the customary risk reduction-only solution; see for examples solutions offered by Cigna (Cigna’s Secure System Insurance) or Counterpane/Lloyd’s of London [8]. More recently, insurance companies started offering stand-alone products (e.g. AIG’s NetAdvantage [1]). Reference [21] provides a recent and comprehensive description of the history and the current state of computer insurance.

Using insurance in the Internet raises a couple of challenging issues, caused by specific properties of the Internet and other large scale networked systems. The first challenge is caused by correlations between risks, which makes it difficult to spread the risk across customers - a sizable fraction of worm and virus attacks, for example, tend to propagate rapidly throughout the Internet and inflict correlated damages to customers worldwide [24], [31]. The second challenge is because entities in the Internet face interdependent risks, i.e. risks that depends on the behavior of other entities in the network, and thus the reward for a user investing in security depends on the general level of security in the network. In this paper, we focus on interdependent risks such as those caused by propagating worms, viruses or bot networks, where damages can be caused either directly by a user, or indirectly via the user’s neighbors.

Bot networks are now a prevalent form of malware with a wide variety of malicious applications including spam, phishing, distributed denial of service, click fraud, data harvesting, password cracking, online reputation inflation and adware installation among others. We explore botnets in detail in Section II-C.

Correlated and interdependent risks have only very recently started being addressed in the literature [4], [5], [7], [12], [15]. Reference [15] considers the situation of agents faced with interdependent risks and proposes a parametric game-theoretic model for such a situation. In the model, agents decide whether or not to invest in security and agents face a risk of damage which depends on the state of other agents. They show the existence of two Nash equilibria (all agents invest or none invests), and suggest that taxation or insurance would be ways to provide incentives for agents to invest (and therefore reach the ”good” Nash equilibrium), but they do not analyze the interplay between insurance and security investments. The model in [15] is extended in [12] to include compulsory insurance offered by a monopolistic insurer.

A more general two-level model was developed and analyzed in [18] and [19]- there, one model describes the spread of malware and another level the economic model for the agents. However, that model did not include insurance. Its main conclusion is that the agents invest too little in self-protection relative to the socially efficient level. A similar result is well-known in public economics: in an economy with externalities, the equilibrium outcomes is generally inefficient [28], [20]. This fact seems very relevant to the situation observed on Internet, where under-investment in security solutions and security controls has long been considered an issue. Security managers typically face challenges in providing justification for security investments, and in 2003, the President’s National Strategy to Secure Cyberspace stated that government action is required where ”market failures result in under-investment in cybersecurity” [30]. The main reason for this situation is that the possible loss cannot be avoided completely by a self-protection investment: a residual (indirect) risk remains. This risk depends on the behavior of other agents. Those who invest in self-protection incur some cost and in return receive some individual benefit through the reduced individual expected loss. But part of the benefit is public: the reduced indirect risk in the economy from which everybody else benefits. The model in [18] and [19] allows to model these network externalities and shows that a tipping phenomenon is possible: in a situation of low level of self-protection, if a certain fraction of the population chooses to invest in security, then it can trigger a large cascade of adoption of security features.

Our work in this paper analyzes the conditions under which insurance could encourage the agents to individually self-protect and possibly leading to a cascading phenomenon of adoption of self-protection. It builds in part on the models of [12], [15], [18], [19] but differs from those because it models all three desirable characteristics of an Internet-like network, namely correlated risks, interdependent agents, and a general model of a network with the realistic topology of a sparse random graph, and it derives general results about the state of the network and the behavior of the agents with and without insurance being available. Our main result is that without regulation insurance (in a competitive market or with one monopoly) is not a good incentive for self-protection and we provide possible rules to ensure viability of insurance companies and increase the level of security of the network.

The rest of the paper is organized as follows. In Section II, we introduce a model of agents subject to epidemic risks when insurance in not available. In Section III, we augment the model from Section II to include insurance, and we discuss the interplay between self-protection and insurance. In Section IV, we present our main results in the case of a general network, subject to epidemic risks, in the presence of insurance. In Section V, we prove the theorems behind our main results of Section IV. In Section VI, we discuss our results and conclude the paper.

## II. A MODEL FOR EPIDEMIC RISKS WITHOUT INSURANCE

In this section, we consider the case of economic agents (namely, agents that attempt to optimize some kind of utility function) subject to epidemic risks, when insurance is not available. We describe a model and give an example of application: botnets. In the next section, we augment this model to include an insurance market. We then solve that model to obtain our main results for this paper.

Our models in this and the next section include two components, so to speak: one component describes the economic model of the agents, the other component describes the spread of the security risk (worm or malware spread, virus attack...) among the agents. We consider simple one-period probabilistic models for the risk, in which all decisions and outcomes occur in a simultaneous instant.

### A. *Economic model for the agents*

We model agents using the classical expected utility model: the decision maker who bears risk, maximizes some kind of preference functional that evaluates the level of his satisfaction. This functional is taken as his expected utility. We assume that agents are rational and that they are risk averse, i.e. their utility function is concave (see Proposition 2.1 in [10]). Risk averse agents dislike mean-preserving spreads in the distribution of their final wealth. As explained below, it is an essential assumption when dealing with problem of insurance.

We denote by $w$ the initial wealth of the agent. The *risk premium* $\pi$ is the maximum amount of money that one is ready to pay to escape a pure risk $X$, where a pure risk $X$ is a random variable such that $\mathbb{E}[X] = 0$. The risk premium corresponds to an amount of money paid (thereby decreasing the wealth of the agent from $w$ to $w - \pi$) which covers the risk; hence, $\pi$ is given by the following equation:

$$u[w - \pi] = \mathbb{E}[u[w + X]].$$

Each agent faces a potential loss $\ell$, which we take in this paper to be a fixed (non-random) value. We denote by $p$ the probability of loss or damage. There are two possible final states for the agent: a good state, in which the final wealth of the agent is equal to its initial wealth $w$, and a bad state in which the final wealth is $w-\ell$. If the probability of loss is $p>0$, the risk is clearly not a pure risk. The amount of money $m$ the agent is ready to invest to escape the risk is given by the equation:

$$pu[w-\ell]+(1-p)u[w]=u[w-m] \qquad (1)$$

We clearly have $m>p\ell$ thanks to the concavity of $u$. We can actually relate $m$ to the risk premium defined above: $m=p\ell+\pi[p;\ell,w]$. We will often use the simplified notation $\pi[p]=\pi[p,\ell,w]$, when no confusion is possible.

An agent can invest some amount in self-protection. Each agent has a binary choice regarding self-protection: if it decides to invest in self-protection, we say that the agent is in state $S$ (as in Safe or Secure). If the agent decides not to invest in self-protection, we say that it is in state $N$ (Not safe). If the agent does not invest, its probability of loss is $p^N$. If it does invest, for an amount which we assume is a fixed amount $c$, then its loss probability is reduced and equal to $p^S<p^N$.

In state $N$, the expected utility of the agent is $p^N u[w-\ell]+(1-p^N)u[w]$; in state $S$, the expected utility is $p^S u[w-\ell-c]+(1-p^S)u[w-c]$. Using the definition of risk premium, we see that these quantities are equal to $u[w-p^N\ell-\pi[p^N]]$ and $u[w-c-p^S\ell-\pi[p^S]]$, respectively. Therefore, the optimal strategy is for the agent to invest in self-protection only if the cost for self-protection is less than the threshold

$$c<(p^N-p^S)\ell+\pi[p^N]-\pi[p^S]. \qquad (2)$$

### B. Epidemic risks for interconnected agents

Our model for the spread of the attack is an elementary epidemic model. Agents are represented by vertices of a graph and face two types of losses: direct and indirect (i.e. due to their neighbors). We assume that an agent in state $S$ has a probability $p^-$ of direct loss and an agent in state $N$ has a probability $p^+$ of direct loss with $p^+\geq p^-$. Then any infected agent contaminates neighbors independently of each others with probability $q^-$ if the neighbor is in state $S$ and $q^+$ if the neighbor is in state $N$, with $q^+\geq q^-$.

Special cases of this model are examined in [18], where $q^+=q^-$, and in [22], where agents in state $S$ are completely secure and cannot have a loss, i.e. $p^-=q^-=0$.

We assume that all agents have the same initial wealth $w$ and that the size of the possible loss is fixed to $\ell$ (i.e. does not depend if it is direct or indirect and is the same across the population). We consider a heterogeneous population, where agents differ only in self-protection cost. The cost of protection should not exceed the possible loss, hence $0\leq c_i\leq\ell$. We model this heterogeneous population by taking the sequence $(c_i, i\in\mathbb{N})$ as a sequence of i.i.d. random variables independent of everything else.The cost $c_i$ is known to agent $i$ and varies among the population. We will consider random families of graphs $G^{(n)}$ with $n$ vertices and given vertex degree [6]. All our results are related to the large population limit ($n$ tends to infinity). In all cases, we assume that the family of graphs $G^{(n)}$ is independent of all other processes.

We now explain how the equilibria of this game are computed. Note that the stochastic process of the losses depends on the state of the agent but her strategic choice given by (2) depends on the probabilities of experiencing a loss in state $N$ and $S$. Clearly, the decision made by the agent depends on the information available to her. As in [18] and [19], we will assume that only a global information is available to the agents. More precisely, if $\gamma$ is the fraction of the population investing in self-protection (in state $S$) then one can compute $p^{N,\gamma}$ and $p^{S,\gamma}$ which are the corresponding probabilities of loss averaged over the population, conditionally on the decision to invest in self-protection $S$ or not $N$. We assume that these quantities are known to each agent so that the decision to invest in self-protection for agent $i$ becomes

$$c_i<c^\gamma, \qquad (3)$$

with $c^\gamma=(p^{N,\gamma}-p^{S,\gamma})\ell+\pi[p^{N,\gamma}]-\pi[p^{S,\gamma}]$. In particular, we can now compute the fraction of population investing in self-protection as a function of these $p^{N,\gamma}$ and $p^{S,\gamma}$, so that the equilibria of the game are given by a fixed point equation, see [18], [19] and [17] for a connection with the standard concept in the economic literature of fulfilled expectations equilibrium.

### C. An example: Botnets

We now show how our model captures the main features of viruses, worms or botnets. The relevance of studying botnets is accredited by the last Symantec Internet Security Threat Report: “Effective security measures implemented by vendors, administrators, and end users have forced attackers to adopt new tactics more rapidly and more often. Symantec believes that such a change is currently taking place in the construction and use of bot networks. Between July 1 and December 31, 2007, Symantec observed an average of 61,940 active bot-infected computers per day, a 17 percent increase from the previous reporting period. Symantec also observed 5,060,187 distinct bot-infected computers during this period, a one percent increase from the first six months of 2007.”

A bot is an end-user machine containing software that allows it to be controlled by a remote administrator called the bot herder via a command and control network. Bots are generally created by finding vulnerabilities in computer systems, exploiting these vulnerabilities with malware and inserting malware into those systems. The bots are then programmed and instructed by the bot herder to perform a variety of cyber- attacks. When malware infects an information system, two things can happen: something can be stolen and the infected information system can become part of a botnet. When an infected information system becomes part of a botnet it is then used to scan for vulnerabilities in other information systems connected to the Internet, thus creating a cycle that rapidly infects vulnerable information systems.

Our model is particularly well-suited to analyze such threats. Recall that we defined two types of losses: direct losses could model the attack of the bot herder who infects machines when he detects it lacks a security feature and then indirect losses would model the contagion process taking place without the direct control of the bot herder. Note that the underlying graph would model the propagation mechanism as file sharing executables or email attachment. In particular it does not necessary correspond to a physical network but it can also be a social network.

Clearly our model is a very simplified model of botnets observed on the Internet. However, security threats on the Internet are evolving very rapidly and our model captures their main features which are more stable.

## III. Model for epidemic risks with insurance

We now analyze the impact of the availability of insurance on the level of investment in self-protection chosen by the agent.

### A. Interplay between insurance with full coverage and self-protection

Consider first the case when a fraction $\gamma$ of the population is in state $S$ and an agent $i$ such that Equation (3) is satisfied, namely it is best for her to invest in self-protection. We assume that the agent can choose between insurance with full coverage at a cost $\wp$ and self-protection. Clearly if the agent chooses full coverage, she will not spend money on self-protection since losses are covered and the utility becomes $u[w-\wp]$. In the case of optimal self-protection, the utility has been computed above: $u[w-c_i-p^{S,\gamma}\ell-\pi[p^{S,\gamma}]]$ since Equation (3) holds. Hence the optimal strategy for the agent is to use insurance if

$$\wp - p^{S,\gamma}\ell - \pi[p^{S,\gamma}] < c_i \tag{4}$$

We see that in this simple case, where only full insurance is available, some agents who would have invested in self-protection if there was no insurance, now take a full coverage and do not invest any more in self-protection. In other words, insurance with full coverage and fixed premium is a negative incentive to self-protection.

We will solve this issue in the sequel but before that, we describe the model of the insurer. We assume that the insurer is risk-neutral and maximizes expected profit. In the case of full coverage the expected profit for the insurer is $\wp - p^{N,\gamma}\ell$ times the fraction of population with a cost $c_i$ satisfying (4). In particular, for the profit to be positive, we need $\wp > p^{N,\gamma}\ell$ and that there exists agents $i$ such that

$$\wp < c_i + p^{S,\gamma}\ell + \pi[p^{S,\gamma}] \leq p^{N,\gamma}\ell + \pi[p^{N,\gamma}].$$

Now if there is only one monopolistic insurer, he will choose $\wp \in (p^{N,\gamma}\ell; p^{N,\gamma}\ell + \pi[p^{N,\gamma}])$ in order to optimize his profit. We will also consider the case where the insurance market is perfectly competitive, in which case only insurers proposing the premium $\wp = p^{N,\gamma}\ell$ will sell insurance and make zero profits. It corresponds to the conventional definitions of competitive equilibrium which assume market clearing, zero profits and the existence of prices.

### B. The basic insurance model

As explained above, the combination of insurance and self-protection raises the problem of what is referred to as moral hazard. Moral hazard occurs when agents or companies covered by insurance take fewer measures to prevent losses from happening, or maybe even cause the loss (and reap the insurance benefits from it). This happens if the insurer is unable to observe the actions of the insured agent, which could result in negligence by the latter.

As we will see if the premium does not depend on whether or not the agent invests in self-protection, then insurance can become a negative incentive to self-protection. This fact is well-known in the economic literature and it is due to the fact that insurance reduces the impact of a loss. Demand for insurance and expenditures on self-protection are negatively related. However, as Ehrlich and Becker [9] have shown, market insurance and self-protection can complement in the sense 'that the availability of the former could increase the demand for the latter', if the insurer can observe the protection level of the insured (in practice, for the insurer to audit self-protection practices and the level of care that the agent takes to prevent the loss) and tie the premium to the amount of self-protection. In order to raise the social level of self-protection, the insurer may engage in premium discrimination. In particular, he may design different contracts for different risk types, relying on the policyholders' categorization: he may offer a premium rebate for low risk agents, and/or he may impose a premium loading for high risk agents and let agents voluntarily decide whether or not to invest in self-protection. The sequence of the considered game between the insurer and its customers may then be seen as follows: at a first stage, the insurer offers appropriate contracts including a premium loading and/or rebate. At a second stage, the customers chooses a contract and decide simultaneously whether or not to invest in prevention.

There is another solution to moral hazard problem: incomplete coverage against loss [27]. Incomplete coverage gives an individual a motive to prevent loss by exposing him to some financial risk.

Our general model of insurance covers both cases and we present it now: with insurance, agent's income, in the event of a loss is increased, while if there is no loss, it is reduced. To an agent who invests in self-protection, the insurer offers the premium $\wp[S]$ and the (net) benefit $\beta[S]$ so that her income in the two states, no loss and loss are: $w-c-\wp[S]$ and, $w-c-\ell+\beta[S]$.

To an agent who does not invest in self-protection, he offers the premium $\wp[N]=\wp[S]+x$ and the benefit $\beta[N]=\beta[S]-y$. We then consider two cases:

- if insurer has perfect information about the level of security of the agents and thus we ignore possible problems associated with moral hazard, then $x$ and $y$ are allowed to be positive in which case it corresponds to a premium penalty (loading).
- if insurer has no information about the level of security of the agents, then we impose $\wp[S]=\wp[N]=\wp$ and $\beta[S]=\beta[N]$ by setting $x=y=0$.

### C. Epidemic risks for interconnected agents with insurance

We now explain how the equilibria of this game with insurance are computed. We first define the set of feasible contracts: those $\{\wp[S], \beta[S], x, y\}$ for which expected profits (for the insurer) are non-negative over the whole population, i.e.

$$\gamma\left((1-p^{S,\gamma})\wp[S] - p^{S,\gamma}\beta[S]\right) \\ +(1-\gamma)\left((1-p^{N,\gamma})\wp[N] - p^{N,\gamma}\beta[N]\right) \geq 0,$$

which can be rewritten as:

$$\begin{aligned} \wp[S](1-p^{\gamma}) - \beta[S]p^{\gamma} & & \\ +(1-\gamma)(x(1-p^{N,\gamma}) + yp^{N,\gamma}) &\geq& 0, \end{aligned} \tag{5}$$

where $p^{\gamma} = \gamma p^{S,\gamma} + (1-\gamma)p^{N,\gamma}$ is the probability of loss.

We will consider two cases:

- case (i): insurer observes with perfect accuracy the level of self-protection of the agents and offers only full coverage contracts: $\beta = \ell - \wp$.
- case (ii): insurer does not observe the level of self-protection of the agents and offers any insurance contracts.

In case (i), note that because only full coverage is offered, we have $\beta[N] = \beta[S] - y = \ell - \wp[S] - x = \ell - \wp[N]$, so that $x = y$. Hence the insurance contracts depend on only two parameters: $\wp[S] = \wp$ and $x$ and all other quantities are derived from these parameters. In particular, if there is a monopolistic insurer, his revenue with market clearing is given by (5):

$$R(\gamma, \wp, x) = \wp - \ell p^{\gamma} + (1-\gamma)x. \tag{6}$$

Suppose a market with many risk neutral insurers being in competition to attract customers and suppose insurers act so as to maximize expected profits. The only policies that will survive in the market are those that yield zero expected profits to insurers and, given this constraint, the highest possible expected utility to agents. Now consider an insurer offering a contract with $x > 0$, then by lowering $x$, he will attract more customers (in state $N$) and increases his profit. As a consequence, at the equilibrium we must have $x = 0$. Hence if there is a competitive insurance market, we require that $x = 0$ and $R(\gamma, \wp, 0) = 0$.

In case (ii), since $x = y = 0$, the insurance contracts depend on only two parameters: $\wp[S] = \wp$ and $\beta[S] = \beta$. As in case (i), if there is a monopolistic insurer, his revenue with market clearing is

$$R(\gamma, \wp, \beta) = \wp(1-p^{\gamma}) - \beta p^{\gamma}. \tag{7}$$

If there is a competitive insurance market, we require that $R(\gamma, \wp, \beta) = 0$.

Now the procedure to compute the equilibria of the game is similar to the one described in Section II-B. For a fraction $\gamma$ of the population investing in self-protection (in state $S$), one can compute the probabilities $p^{N,\gamma}$ and $p^{S,\gamma}$. From these quantities (known to the agents), we can predict the strategic behavior of each agent, namely to invest or not in self-protection and/or to take or not an insurance. In particular, we are able to compute the fraction of population investing in self-protection as a function of these $p^{N,\gamma}$ and $p^{S,\gamma}$, so that the equilibria of the game are given by a new fixed point equation (see Section V for a more formal treatment). In the case of a monopolistic insurer, his revenue can be computed thanks to (6) or (7). In the case of a competitive insurance market, only equilibria satisfying the zero profit condition are valid. In particular, it is possible that equilibria with a monopolist insurer exist whereas, no equilibrium exists in a competitive market.

Summary of notations:

- $c_i$ and $\ell_i = \ell$ are the cost of self-protection and the amount of loss for agent $i$.
- $p^{+} > 0$ is the probability of direct loss when not investing in self-protection (state $N$).
- $p^{-} < p^{+}$ is the probability of direct loss when investing in self-protection (state $S$).
- $q^{+}$ is the probability of contagion in state $S$.
- $q^{-} \leq q^{+}$ is the probability of contagion in state $N$.
- $\gamma$ is the fraction of the population investing in self-protection.
- when a fraction $\gamma$ is in state $S$, $p^{S,\gamma}$ and $p^{N,\gamma}$ are the respective probabilities of loss conditioned on being in state $S$ and in state $N$.
- $p^{\gamma} = \gamma p^{S,\gamma} + (1-\gamma)p^{N,\gamma}$ is the probability of loss averaged over the whole population.
- an insurance contract is a couple of a premium and a benefit: insurer offers a contract $(\wp[S], \beta[S])$ to agents in state $S$ and $(\wp[S] + x, \beta[S] - y)$ to agents in state $N$:
  - in case (i), there is no moral hazard and only full coverage: $\beta[S] = \ell - \wp[S]$. $\wp[S] = \wp$, $x = y$.
  - in case (ii), there is moral hazard: $x = y = 0$.

## IV. Main results

Humans are the weakest link in security but cannot be directly programmed to perform. Rather their autonomy must be respected as a design constraint and incentives provided to induce desired behavior [2], [17], [29]. In this section we answer the following fundamental questions:

1) what is the range of parameters of the insurance contracts ensuring that the introduction of insurance cannot decrease the level of self-protection in the network?
2) under which conditions can the introduction of insurance increase the level of self-protection in the network?

Answering these questions is a crucial point in a possible development of insurance markets for the Internet and its users. Our model yet simple allows to get insights on the limits and benefits of insurance for such epidemic risks. It also raises several issues (discussed in Section VI) concerning a possible implementation of insurance viewed as a mechanism to increase the adoption of security measures Internet-wide.

We say that insurance is a good incentive for self-protection if for any fraction $\gamma$ of the population investing in self-protection, the incentive for any agent to invest in self-protection increases when insurance is introduced. We now consider different scenarios and their impact on the level of self-protection in the network. Proofs of the propositions are given in Section V.

### A. Competitive insurance market

*Proposition 1:* In cases (i) and (ii) and in a competitive insurance market, insurance is not an incentive for self-protection.

In case (ii), Proposition 1 shows that moral hazard is a limit to insurance for epidemic risks, since there is an inverse relationship between risk prevention and insurance coverage. In this case, the level of risk prevention will be inefficient. Anticipating this low degree of prevention, insurers will raise their premium rate, inducing policyholders to reduce their coverage: no insurance can be an (inefficient) equilibrium.

In case (i), there is no problem of moral hazard since insurers can engage in premium discrimination but they will actually not engage in such a premium discrimination. Suppose, they did tie the premium to the amount of self-protection, then an insurer could come into the market and offer an insurance contract to agents in state $S$ only. It is easy to see that he will make a positive profit because he will benefit from the low probability of loss for those agents and not bear the costs needed to achieve this high level of security.

Our Proposition 1 sustains the following general claim:

*Claim 1:* Network externalities cannot be internalized in a competitive insurance market.

This claim is also substantiated by [12]. Claim 1 shows that there is a need for public intervention. A possibility is the enforcement of norms for risk prevention. This is the case for environmental risks in which ships transporting chemical products have to satisfy several safety requirements that are imposed by regulatory agencies. Automobile driving norms are also standard as speed limits, alcohol-free driving... Note that these norms are mostly organized by a regulatory agency rather than by insurers. One reason is due to the combination of negative externalities and limited liability [11]. If there are more than one agency supervising the implementation of norms, the information among the different agencies should be pooled.

### B. Monopolistic Insurer

We assume now that there is a risk-neutral monopolistic insurer maximizing expected profit:

*Proposition 2:* In cases (i) and (ii), a monopolistic insurer is not a good incentive for self-protection.

It follows from the proof of this proposition that the following phenomenon occurs: starting form a situation without insurance, the insurer attracts only agents in state $S$. Then among this fraction of the population, the agents with the highest cost for self-protection choose to take an insurance without self-protection (even if the premium is higher).

Propositions 1 and 2 explain in part the actual situation where cyberinsurance seems not to have ’taken off’. There are various reasons and we will discuss some in Section VI. But it seems reasonable to think that insurance can actually take off only if it is a good incentive for self-protection, otherwise losses will be very big and highly correlated among the network, making the claims harder to reimburse. With this point of view, the right question to ask is not anymore: is insurance a good incentive for self-protection? but: what would be a framework which would allow insurance to exist? There is no such economic framework today (at least specific to the Internet) and as a consequence cyberinsurance is still in its infancy. The definition of such a framework is a vast question which seems to be a promising research area. The model designed in previous sections is our main contribution to this research agenda. It allows to capture the main features of the problem and is tractable enough to give some insights on the way to alter the economic incentives in order to solve the problem.

### C. Insurance as a good incentive

In order for insurance to be a good incentive, we need to find the good rules to regulate the market. We explore this issue now.

*Proposition 3:* If there is no moral hazard, there exists a threshold $t$ such that in a competitive insurance market where the premium loading is forced to exceed $t$, then insurance is an incentive to self-protection.

There is a simple way, to enforce such a rule thanks to a tax: agents choosing not to invest in self-protection have to pay a tax $t$. This argument substantiates the following claim:

*Claim 2:* Implementing a tax for individuals not investing in self-protection could enable an insurance market for the Internet and its users.

It might actually be technically possible to implement such a tax system. However there is still an economic issue. A collected tax should be returned to the agents for example by refunding taxes equally to all users, otherwise the total cost incurred to the network can actually be larger than without tax. In other words, the social optimum is attained only if the collected tax is returned to the network. Hence the implementation of such a tax system should be able to return some money or a good to the end users.

Our next proposition solves this issue and shows that if insurance is provided by a monopolistic insurer who does not maximize his expected profit, then insurance is a good incentive to self-protection. Moreover, there is no need to return money to the agents, since the insurance contract can be provided at a fair premium, meaning that the insurer makes zero profit.

*Proposition 4:* If there is no moral hazard, insurance provided at a fair premium to agents in state $S$ is a good incentive.

Note that in all cases, there is a fundamental requirement, namely the insurer should be able to observe the level of self-protection of the agents. Both the cost and the potential usefulness of observations of self-protection measures may depend on when the observations are made, either ex ante, when a policy is purchased or ex post, when a claim is presented. We do not deal with this issue in this paper. Our model deals with the case, where there is an exact observation made by the insurer. But one could add some noise on this observation. Our main methodology will carry on but details will change. In the case of moral hazard, when no observation can be made by the insurer, the design of an insurance scheme with good incentive is an open problem. This issue is left for a future research.

## V. Mathematical Analysis

### A. General framework

In this section, we consider the case of Erdös-Rényi graphs $G^{(n)} = G(n, \lambda/n)$ on $n$ nodes $\{0, 1, \dots, n-1\}$, where each potential edge $(i, j)$, $0 \le i < j \le n-1$ is present in the graph with probability $\lambda/n$, independently for all $n(n-1)/2$ edges. Here $\lambda > 0$ is a fixed constant independent of $n$. This class of random graphs has received considerable attention in the past. We refer to [18] and [19] to see how our results extend to random graphs with asymptotic given degree. The main features of the solution are still valid in these different cases.

Following Proposition 1 of [19] (see also Section 4.1) we define $h(\gamma)$ as the unique solution in $[0, 1]$ of

$$h = 1 - \gamma(1-p^-)e^{-\lambda q^- h} - (1-\gamma)(1-p^+)e^{-\lambda q^+ h}.$$

Then, we define

$$\begin{aligned} p^{N,\gamma} &= 1 - (1-p^+)e^{-\lambda q h(\gamma)}, \\ p^{S,\gamma} &= 1 - (1-p^-)e^{-\lambda q h(\gamma)}. \end{aligned}$$

By Proposition 4 of [18] or Section 3.3 of [19], we know that these quantities are the asymptotics as $n \to \infty$ of the probabilities of loss conditioned on being in $N$ and $S$ respectively, when the fraction of the population investing in self-protection is $\gamma$.

Thanks to these quantities, we compute the utility for all possible cases, for a fixed $\gamma$:

- $(I, S)$: the agent pays for insurance and invests in self-protection, then her utility is given by
$$\begin{aligned} u^{(I,S)} &= (1-p^{S,\gamma})u[w - c_i - \wp[S]] \\ &\quad + p^{S,\gamma}u[w - c_i - \ell + \beta[S]] \\ &= u[w - c_i - p^{S,\gamma}\ell - \zeta], \end{aligned}$$
where $\nu^S = \wp[S] - \ell + \beta[S]$ and $\zeta = \pi[p^{S,\gamma}; \nu^S] + (1 - p^{S,\gamma})\wp[S] - p^{S,\gamma}\beta[S]$.
- $(I, N)$: the agent pays for insurance but does not invest in self-protection, then her utility is given by
$$\begin{aligned} u^{(I,N)} &= (1-p^{N,\gamma})u[w - \wp[N]] \\ &\quad + p^{N,\gamma}u[w - \ell + \beta[N]] \\ &= u[w - p^{N,\gamma}\ell - \eta], \end{aligned}$$
where $\nu^N = \wp[N] - \ell + \beta[N]$ and $\eta = \pi[p^{N,\gamma}; \nu^N] + (1 - p^{N,\gamma})\wp[N] - p^{N,\gamma}\beta[N]$.
- $(NI, S)$: the agent does not pay for insurance but does invest in self-protection, then her utility is given by
$$\begin{aligned} u^{(NI,S)} &= (1-p^{S,\gamma})u[w - c_i] \\ &\quad + p^{S,\gamma}u[w - \ell - c_i] \\ &= u[w - c_i - p^{S,\gamma}\ell - \pi[p^{S,\gamma}]]. \end{aligned}$$
- $(NI, N)$: the agent does not pay for insurance nor invests in self-protection, then her utility is given by
$$u^{(NI,N)} = u[w - p^{N,\gamma}\ell - \pi[p^{N,\gamma}]].$$

TABLE I
Utility with insurance and self-protection

| | |
|---|---|
| $(I, S)$ | $u[w - c_i - p^{S,\gamma}\ell - \zeta]$ |
| $(I, N)$ | $u[w - p^{N,\gamma}\ell - \eta]$ |
| $(NI, S)$ | $u[w - c_i - p^{S,\gamma}\ell - \pi[p^{S,\gamma}]]$ |
| $(NI, N)$ | $u[w - p^{N,\gamma}\ell - \pi[p^{N,\gamma}]]$ |

The utility for all possible cases is summarized in Table 1. The first column denotes the choice made by an agent. It is denoted by the pair $(U, V)$, where $U = I$ means that the agent pays for insurance and $U = NI$ otherwise, and $V = S$ means that the agent invests in self-protection and $V = N$ otherwise.

We see that if $\zeta < \pi[p^{S,\gamma}]$, then $(I, S)$ always dominates $(NI, S)$. For $(I, S)$ to dominate $(I, N)$, we need $c_i < (p^{N,\gamma} - p^{S,\gamma})\ell + \eta - \zeta$. For $(I, S)$ to dominate $(NI, N)$, we need $c_i < (p^{N,\gamma} - p^{S,\gamma})\ell + \pi[p^{N,\gamma}] - \zeta$. For $(I, N)$ to dominate $(NI, N)$, we need $\eta < \pi[p^{N,\gamma}]$. For $(NI, S)$ to dominate $(NI, N)$, we need the standard condition: $c_i < c^\gamma = (p^{N,\gamma} - p^{S,\gamma})\ell + \pi[p^{N,\gamma}] - \pi[p^{S,\gamma}]$. We define

$$c^\gamma[\zeta, \eta] := (p^{N,\gamma} - p^{S,\gamma})\ell + \min(\eta - \zeta; \pi[p^{N,\gamma}] - \zeta).$$

so that if $\zeta < \pi[p^{S,\gamma}]$, for $c_i < c^\gamma[\zeta, \eta]$, the strategy $(I, S)$ is dominant and if $\zeta \ge \pi[p^{S,\gamma}]$ and $c_i < c^\gamma[\zeta, \eta]$, then the strategy $(NI, S)$ is dominant. For $c_i > c^\gamma[\zeta, \eta]$, either $(I, N)$ or $(NI, N)$ dominates. Note that in this last case, there is no incentive to invest in self-protection. In other words, in the presence of insurance, agent $i$ will decide to invest in self-protection if and only if $c_i < c^\gamma[\zeta, \eta]$. This last relation has to be compared to Equation (3).

In particular, from $p^{N,\gamma}, p^{S,\gamma}, \wp[S], \beta[S], x, y$, we can now compute the fraction $f(p^{N,\gamma}, p^{S,\gamma}, \wp[S], \beta[S], x, y)$ of the population investing in self-protection, namely the agents such that $c_i < c^\gamma[\zeta, \eta]$. Then, the possible equilibria are characterized by the fixed point equation: $\gamma = f(p^{N,\gamma}, p^{S,\gamma}, \wp[S], \beta[S], x, y)$.

### B. Conditions for Insurance as a good incentive

We say that insurance is a good incentive for self-protection if $c^\gamma[\zeta, \eta] \ge c^\gamma$ for all $\gamma$. In words, it implies that for any fraction $\gamma$ of the population investing in self-protection, the incentive for any agent to invest in self-protection increases when insurance is introduced.

Then we have:

$$c^\gamma[\zeta, \eta] \ge c^\gamma \Leftrightarrow \left\{ \begin{array}{rcl} \pi[p^{S,\gamma}] & \ge & \zeta, \text{ and,} \\ \eta - \zeta & \ge & \pi[p^{N,\gamma}] - \pi[p^{S,\gamma}]. \end{array} \right. \qquad (8)$$

We now look at the different cases studied.

### C. Analysis of case (i)

Note that we have $\nu^N = \nu^S = 0$, $\zeta = \wp - p^{S,\gamma}\ell$ and $\eta = \wp + x - p^{N,\gamma}\ell$. Hence Equation (8) becomes:

$$\left\{ \begin{array}{rcl} \wp & \le & p^{S,\gamma}\ell + \pi[p^{S,\gamma}], \text{ and,} \\ x & \ge & c^\gamma. \end{array} \right. \qquad (9)$$

In a competitive insurance market, we must have $x = 0$ which contradicts the second equation of (9) as soon as $p^{N,\gamma} > p^{S,\gamma}$ which is implied by $p^- < p^+$. Hence the first part of Proposition 1 follows.

We now look when insurance is a dominant strategy. For $(I,S)$ to be dominant, we need to have

$$\begin{aligned} \zeta &\leq \pi[p^{N,\gamma}], \text{ and,} \\ c_i &\leq (p^{N,\gamma} - p^{S,\gamma})\ell + \min(\eta - \zeta; \pi[p^{N,\gamma}] - \zeta). \end{aligned}$$

For $(I,N)$ to be a dominant strategy, we need to have

$$\begin{aligned} \eta &\leq \pi[p^{N,\gamma}], \text{ and,} \\ c_i &\leq (p^{N,\gamma} - p^{S,\gamma})\ell + \eta - \pi[p^{S,\gamma}], \text{ and,} \\ c_i &\geq (p^{N,\gamma} - p^{S,\gamma})\ell + \eta - \zeta. \end{aligned}$$

First assume that the insurer chooses $\eta > \pi[p^{N,\gamma}]$, then $(I,N)$ is never dominant and the insurer will attract only agents in state $S$ such that $c_i \leq (p^{N,\gamma} - p^{S,\gamma})\ell + \pi[p^{N,\gamma}] - \zeta$ and the profit made by the insurer for any such customer is exactly $\zeta$. In particular, in a competitive market, we know that $\zeta = 0$ and hence agents with $c^\gamma < c_i \leq (p^{N,\gamma} - p^{S,\gamma})\ell + \pi[p^{N,\gamma}]$ will invest in self-protection, hence increasing the fraction of the population in state $S$. In this case, insurance is an incentive for self-protection. Note that

$$\begin{aligned} \eta > \pi[p^{N,\gamma}] \quad &\Leftrightarrow \quad \wp + x - p^{N,\gamma}\ell > \pi[p^{N,\gamma}] \\ &\Leftrightarrow \quad x > (p^{N,\gamma} - p^{S,\gamma})\ell + \pi[p^{N,\gamma}], \end{aligned}$$

and Proposition 4 follows.

Now consider the case where the (monopolistic) insurer chooses $\eta \leq \pi[p^{N,\gamma}]$. As a result we see that agents with $c_i \leq (p^{N,\gamma} - p^{S,\gamma})\ell + \eta - \zeta$ choose $(I,S)$ and provide a revenue of $\zeta \leq \pi[p^{N,\gamma}]$ to the insurer and agents with $c_i \in [(p^{N,\gamma} - p^{S,\gamma})\ell + \eta - \zeta, (p^{N,\gamma} - p^{S,\gamma})\ell + \eta - \pi[p^{S,\gamma}]]$ choose $(I,N)$ and provide a revenue of $\eta$ to the insurer.

Hence we see that, the optimal choice for $\eta$ for the insurer is actually $\eta = \pi[p^{N,\gamma}]$ and then Proposition 3 follows.

### *D. Analysis of case (ii)*

We have $\zeta = \pi[p^{S,\gamma}] + (1 - p^{S,\gamma})\wp - p^{S,\gamma}\beta$ and $\eta = \pi[p^{N,\gamma}] + (1 - p^{N,\gamma})\wp - p^{N,\gamma}\beta$. Hence Equation (8) becomes:

$$\left\{ \begin{array}{rcl} \wp + \beta &\leq& 0, \text{ and,} \\ (1 - p^{S,\gamma})\wp &\leq& p^{S,\gamma}\beta. \end{array} \right. \tag{10}$$

Recall (7) that $R(\gamma, \wp, \beta) = \wp(1 - p^\gamma) - \beta p^\gamma$.

In a competitive insurance market, we must have $R(\gamma, \wp, \beta) = 0$. However, we have

$$R(\gamma, \wp, \beta) \geq 0 \Leftrightarrow \wp(1 - p^\gamma) \geq \beta p^\gamma,$$

and since $p^\gamma < p^{S,\gamma}$ (for $\gamma < 1$), we see that it is in contradiction with the second equation of (10). The corresponding statement of Propositions 1 for case (ii) follows.

The proof of Proposition 2 for case (ii) follows the same argument as in previous section. In particular, it is always optimal for the insurer to choose $\eta = \pi[p^{N,\gamma}]$ and then to optimize $\zeta$.The insurer now get a revenue $(1-p^{N,\gamma})\wp - p^{N,\gamma}\beta$ from the agents with $c_i \in [(p^{N,\gamma} - p^{S,\gamma})\ell + \pi[p^{N,\gamma}] - \zeta, c^\gamma]$.

## VI. Discussion and Implications

In this work, we focused on quantifying the benefits of managing epidemic risks, such as those caused by the spread of worms and viruses in the Internet, using insurance. Our analysis leads us to conclude that insurance can be a powerful mechanism to increase the level of self-protection, and therefore the overall security, in the network (see Propositions 3and 4). Furthermore, it appears to be an attractive proposition and a growth opportunity for insurance companies since risks are not decreasing but the importance of the Internet infrastructure is increasing.

However, we also found that, moral hazard problem could be a barrier for insurance (Proposition 1). Therefore, the analysis suggests a winning combination, namely a regulated market (so that insurance companies can prosper while still offering fair premiums to agents) which provides a clear benefit (namely an overall increase in Internet security). Given the benefits of insurance, and the increasing strategic importance of the Internet, it seems likely that insurance will play a role, possibly a key role, in Internet security in the future.

However, we have found that mentioning Internet insurance rapidly attracts comments about the uniqueness of the Internet environment, and in particular questions around the estimation of damages. The assumption is that estimating damages in the Internet is so difficult and fraught with peril that insurance is not inevitable at all, but rather destined to remain a niche or an oddity. We first note that reliably estimating damages is indeed an important task because it controls the profit (or the ruin) of the insurer and the incentives for agents to invest in self-protection. Also, it is true that quantifying risks for a good or an optimal premium value is difficult because the assets to be protected are intangible (such as a company stock price), because damages might be visible only long after a threat or an attack was identified (e.g. easter egg with timed virus or exploit in a downloaded piece of software), because risk changes can occur quickly (zero day attacks), and because evaluating the insurability (and the level of protection) of new and existing customers is likely to be a complex and time intensive task. However, the insurance industry has been dealing with those problems for decades or centuries in other areas of life - if warships can be insured in time of war (as indeed they can), it is difficult to argue convincingly that Internet risks and damages absolutely cannot be insurable. Questions about damage estimation might also be the wrong questions. A better question might be how to help insurers do a better job, i.e. how the current Internet might be used to help insurers do a better job of estimating damages, and how to evolve the Internet or create a new design that will make that job even easier. One way suggested by the discussion above on estimating damages would be to develop metrics and techniques for that purpose. Another, related way is to develop metrics for the security related issues of interest. Some interesting propositions have been made in that sense, for example the cost to break metric described in [25], but we believe this is an important area ripe for further research (see also [3]). Note that metrics of interest are not limited to core security metrics such as cost to break, but need to be developed for all relevant activities facing threats and risks.

We conclude by noting that deploying large scale insurance solutions in the Internet raises several systems and architectural issues. In particular, it will require new processes and fresh approach to some Internet components. Insurance relies heavily on authenticated, audited, or certified assessments of various kinds to avoid fraud or other issues such as the moral hazard examined earlier in the paper. This argues, along with security logs and metrics, for effective and efficient ways to measure and report those metrics during the lifetime of an insurance contract (for example, a declaration of security investments and settings at signup time, possible audits while the contract is effective, and a certified assessment post-damage of the security settings and responses during the attack or infection).

Finally, we believe that the design of insurance policies for realistic Internet scenarios raises exciting research questions, with opportunities for contributions that can impact the evolution of the Internet and the evolution of the industry of risk management on the Internet.

## REFERENCES

[1] American International Group, Inc. netAdvantage http://www.aignetadvantage.com/

[2] R. Anderson. Why information security is hard-an economic perspective. *Proceedings of the 17th Computer Security Applications Conference, 2001. ACSAC 2001.*, pages 358-365, 2001.

[3] J. Aspnes, J. Feigenbaum, M. Mitzenmacher, D. Parkes. Towards better definitions and measures of Internet security. *Proc. Workshop on Large-Scale-Network Security and Deployment Obstacles*, Landsdowne, VA, March 2003.

[4] R. Böhme. Cyber-insurance revisited. *Proc. of Workshop on the Economics of Information Security (WEIS)*, 2005.

[5] R. Böhme and G. Kataria. Models and measures for correlation in cyber-insurance. *Proc. of Workshop on the Economics of Information Security (WEIS)*, 2006.

[6] B. Bollobas. Random Graphs *Cambridge university Press*, 2001.

[7] J. Bolot and M. Lelarge. A New Perspective on Internet Security using Insurance. *INFOCOM Mini-Conf.* 2008.

[8] http://www.counterpane.com/pr-lloydssl.html

[9] I. Ehrlich and G. S. Becker. Market insurance, self-insurance, and self-protection. *The Journal of Political Economy*, 80(4):623–648, 1972.

[10] C. Gollier. *The Economics of Risk and Time.* MIT Press, 2004.

[11] C. Gollier. Some aspects of the economics of catastrophe risk insurance. *CESifo working paper 1409*, 2005.

[12] 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.

[13] J. Kesan, R. Majuca, and W. Yurcik. The economic case for cyberinsurance. In *Securing Privacy in the Internet Age*, A. Chander et al., Eds., Stanford University Press, 2005.

[14] J. Kesan, R. Majuca, and W. Yurcik. Cyberinsurance as a market-based solution to the problem of cybersecurity:a case study. *Proc. WEIS 2005*, Harvard, MA, June 2005.

[15] H. Kunreuther and G. Heal. Interdependent security: the case of identical agents. *Journal of Risk and Uncertainty*, 26(2):231–249, 2003.

[16] C. Lai, G. Medvinsky and C. Neuman Endorsments, licensing, and insurance for distributed systems services. *Proc. 2nd ACM Conf. Computer and Comm. Security (CCS)*, Fairfax, VA, Nov. 1994.

[17] M. Lelarge. Economics of Malware: Epidemic Risks Model, Network Externalities and Incentives. *Fifth bi-annual Conference on The Economics of the Software and Internet Industries*, Toulouse, Jan. 2009.

[18] M. Lelarge and J. Bolot. Network externalities and the deployment of security features and protocols in the Internet. *Proc. ACM Sigmetrics 2008*, pages 37-48, Annapolis, MD, 2008.

[19] M. Lelarge and J. Bolot. A Local Mean Field Analysis of Security Investments in Networks. *Proc. ACM NetEcon 2008*, pages 25-30, Seattle, USA, 2008.

[20] L. Jiang, V. Anantharam and J. Walrand. Efficiency of Selfish Investments in Network Security. *Proc. ACM NetEcon 2008*, pages 31-36, Seattle, USA, 2008.

[21] R. P. Majuca, W. Yurcik, and J. P. Kesan. The evolution of cyberinsurance. *Information Systems Frontier*, 2005.

[22] T. Moscibroda, S. Schmid and R. Wattenhofer. When selfish meets evil: byzantine players in a virus inoculation game. *PODC '06: Proceedings of the twenty-fifth annual ACM symposium on Principles of distributed computing*, 35–44, 2006.

[23] J. Mossin. Aspects of rational insurance purchasing. *Journal of Political Economy*, 76:553–568, 1968.

[24] S. Saniford, D. Moore, V. Paxson, N. Weaver. The top speed of flash worms. *Proc. ACM Workshop Rapid Malcode WORM'04*, Fairfax, VA, Oct 2004.

[25] B. Schneier. Insurance and the computer industry. *CACM*, vol. 44, no. 3, March 2001.

[26] B. Schneier. Computer security: It's the economics, stupid. *Proc. WEIS 2002*, Berkeley, CA, May 2002.

[27] S. Shavell. On Moral Hazard and Insurance. *The Quarterly Journal of Economics*, (93)4:541–562, 1979.

[28] H. Varian. System Reliability and Free Riding. *WEIS* 2004.

[29] R. Wash and J. K. MacKie-Mason. Security when people matter: structuring incentives for user behavior. *ICEC '07: Proceedings of the ninth international conference on Electronic commerce*, pages 7-14, Minneapolis, MN, USA, 2007.

[30] White House. "National Strategy to Secure Cyberspace", 2003. Available at whitehouse.gov/pcipb.

[31] C. Zou, W. Gong, D. Towsley. Code Red worm propagation modeling and analysis. *Proc. 9th ACM Conf. Computer Comm. Security CCS'02.*, Washington, DC, Nov 2002.