Cyber-Insurance Framework for Large Scale Interdependent Network[*]

Galina A. Schwartz
University of California at Berkeley
schwartz@eecs.berkeley.edu

Shankar S. Sastry
University of California at Berkeley
sastry@eecs.berkeley.edu

ABSTRACT

This article presents a framework for managing cyber-risks in large-scale interdependent networks where cyber insurers are strategic players. In our earlier work [13, 14, 12], we *imposed* that breach probability of each network node (player) is a function of two variables: player own security action and average security of all players. In this article, we formally *derive* the expression of breach probability from standard assumptions. For a homogeneous interdependent network (identical users), we provide a solution for user optimal security in environments without and with cyber insurers present. Then, we introduce a general heterogeneous network (many user types), and derive the expression for network security. Lastly, we consider the network with two user types (normal and malicious), in which we allow one user type (malicious users) to subvert monitoring by insurers, even if the insurers perfectly enforce security levels of normal users (at zero cost). Our analysis confirms a discrepancy between informal arguments that favor cyber-insurance as a tool to improve network security, rather than merely manage risks. In particular, our results support the case *against* cyber-insurance as the means of improving security. Our framework helps to identify the crucial network parameters for improving incentives to provide secure networks.

1. INTRODUCTION

The question of security incentives and optimal security risks is an integral part of studying the resilience of modern networks. In this article, we are broadly concerned with the question of how to mitigate interdependent risks to which large-scale networks are exposed, mainly due to the present-day ubiquitous connectivity. Our particular contribution is a game theoretic model, which allows to introduce competitive cyber insurers as players. The network security properties are determined as an equilibrium of the game in which players (or networked nodes) make individually optimal strategic choices, and player payoffs depend on player own choices, as well as the choices of other players, which possibly include cyber insurers. This game theoretic framework permits us to study user security choices with and without availability of cyber contracts.

Depending on the context, we will use the terms "node player" and "user" interchangeably. This will also help us to make the exposition more intuitive. Examples of nodes in networked systems include sensors, actuators, computing nodes, etc. In emerging cyber-physical networks, each node can be considered a smart networked device that is capable of making certain decisions; for e.g., a sensor deciding on its measurement strategy, an actuator deciding on a local control strategy, and a computing node choosing to perform computations. The field of networked and embedded control systems has made promising advances in designing optimal decisions for these smart devices, both in centralized and decentralized context. In this article, we assume that each node has a decision making capability that has direct connotations for the node's failure due to imperfect security of the network, and primarily due to *cyber insecurity.*

From a practical viewpoint, one can imagine numerous security choices for each smart node. Below we list some examples of the choices available to nodes: i) which specific device to install, whether to use encryption, and if so which encryption method to follow; ii) frequency of communications with other nodes, and how powerful should each communication signal, how many channels should be used for transmission; iii) whether computations are local to a node, or rely on data from other nodes; iv) whether the node location is physically secure or security is software based; v) whether node is permanently networked or could be placed off-line for maintenance and patching; vi) how frequently security updates are made, etc.

For the sake of simplicity, we do not consider multidimensional security choices in this article. Instead, we aggregate all these choices and work with one-dimensional security metrics, i.e., we will index the security of each node by a

[*]This research was supported by NSF grant CNS-1239166, which provides funding for a frontier project FORCES (Foundations of Resilient CybEr-Physical Systems), NSF grant CNS-0910711, and by TRUST (Team for Research in Ubiquitous Secure Technology), which receives support from the NSF (#CCF-0424422) and the following organizations: AFOSR (#FA9550-06-1-0244), BT, Cisco, DoCoMo USA Labs, EADS, ESCHER, HP, IBM, iCAST, Intel, Microsoft, ORNL, Pirelli, Qualcomm, Sun, Symantec, TCS, Telecom Italia, and United Technologies.

HiCoNS, April 15–17, 2014, Berlin, Germany.
Copyright 2014 ACM 978-1-4503-1263-9/12/04 ...$10.00.

value, a so-called own *security level* of a node. This level ranges between zero and one, with zero level meaning that the node is insecure, i.e., it has certainty (hundred percent chance) of a security breach, and thus, always incurs a loss. At security level of one, the node is fully secure, and no loss could occur. Such a one-dimensional security level assumes that each player optimally allocates his resources among the aforementioned security choices i) – vi). In other words, we assume that each node is capable of making the best security choices for self; i.e., the node's reaches the highest possible security level conditional on total amount of security resources that it expands.

The plan of the paper is as follows. In Section 2, we consider a network consisting of n identical nodes. In Section 3, we solve homogenous network case without cyber insurers present, and in Section 4 – with insurers. We derive an optimal cyber insurer contract. In Section 5, we compare equilibrium network security in different environments. In Section 6, we generalize to a heterogeneous network case. In Section 7, we discuss the extensions and conclude.

1.1 Literature

At present, risk management capabilities for ICT[1] are all but nonexistent [2]. Three factors that hinder cyber risk management via cyber-insurance are identified in [3]: correlations, interdependence and information asymmetries. This article combines the two latter factors and builds a framework for the analysis and comparative evaluation of cyber risk management solutions for large scale networks.

The widely held view among the researchers [2] is that network insecurity primarily caused by misaligned incentives as technology-based solutions are available, but not utilized. [5] emphasizes that information deficiencies contribute to the misaligned incentives and hence, hinder the adoption of improved security practices.

We introduce a modeling framework to investigate the possibilities of mitigating cyber risks in large scale networks. Thus, we consider the network with and without cyber-insurance, and study the effects of insurance. Our framework allows to study both problems that manifest in environments with information asymmetries: *moral hazard* (when insurers are uninformed of user security levels) and *adverse selection* (when insurers cannot distinguish different user types). In this paper, we focus on formulation of a general framework that allows to study both, adverse selection and moral hazard effects. We combine the model of large scale network, in which individual user security and network security are interdependent with ideas of asymmetric information literature, originated by Akerlof [1], Rothschild and Stiglitz [11].[2]

Due to space restrictions, we will omit technical discussion of existing cyber insurance literature. We refer an interested reader to [3], and the most recent developments will be presented in our forthcoming technical report.

2. INTERDEPENDENT NETWORK

To start, we consider a network consisting of n identical nodes (players / users). We will generalize to heterogeneous network in Section 6.

2.1 Homogeneous network

Each player i choice variable is his security level s_i to maximize his expected utility u_i:

$$E[u_i] = B_i \cdot U(W - L) + (1 - B_i) \cdot U(W) - h(s_i), \qquad (1)$$

where s_i – user security, $h(\cdot)$ – user security cost function for reaching his chosen security level, which we assume to be twice differentiable, and $h'(x), h'' \geq 0$ for every $x \in [0, 1]$, and $h(0) = 0$, $h'(0) = 0$, and $h(1) = \infty$. The intuition is that user security costs increase with security, and that improving own security level imposes an increasing marginal cost on the player, with $h(1) = \infty$ characterizing a hypothetical "perfectly secure" system. Indeed, it is realistic to assume that marginal benefit from higher security level is decreasing, whereas marginal cost of security improvements is increasing with security. $h(0) = 0$ illustrates the ease of initial security improvement, and $\lim_{x\to 1} h(x) = \infty$ illustrates the prohibitive expense of complete security. [An example of such an h is $h(x) = \frac{x^2}{1-x}$].

Players are risk-averse: $U'(\cdot) > 0$, $U''(\cdot) < 0$, and W denotes user initial wealth, L – his amount of loss, and B_i – the probability of loss (resulting from successful breach) for player i.

The reasons for keeping security costs in (1) separately from monetary wealth are two fold. First, this specification reflects that security costs are in many cases non-monetary. For example, it is hard to put a price tag on one's efforts to remember multiple passwords, and second, in today's world, security budget is frequently determined by the player's efforts to obtain the funds (or manpower) for a given, specific security need, such as performance of security updates, or increasing the frequency of backups (both these tasks require extra resources, such as manpower and equipment).

We will start with an expression for B_i standard for the literature modeling security interdependencies, as in [8, 6, 10, 7, 9, 3], and many others. To be concrete, let us borrow the specification from [10], see p. 21, where breach probability $B_i = B_i(s_1, ...s_n)$ for node i is defined as:

$$B_i(s_1, ...s_n) = 1 - s_i + s_i \prod_{j \neq i}^{n} \{q(1 - s_j)\}, \qquad (2)$$

Thus, player i face two types of attack threats, direct and indirect. A direct threat attacks player i directly, while an indirect threat results from attacks on other network nodes, $j \neq i$. Each user i have to chose his security level to mitigate against both these threats. From (2), for player i with security s_i, success probability of direct attack is $(1 - s_i)$; and success probability of indirect attack from others is $q(1-s_j)$, $j \neq i$, and $q \in (0, 1)$. parameter $q = q(n)$ is assumed to be small; the magnitude of $q(n)$ characterizes the strength of node inderdependencies of the network, with more interdependent networks having higher $g(n)$.

We argue that for large scale networks, the coherent $q(n)$ must decrease with n, because if it does not, by adding sufficiently many extra nodes to the network, B_i will reach, and then exceed 1. Therefore, such specification is unsuitable for analyzing large scale networks. Moreover, we suggest that for such networks, an assumption of $q = q(n) \to 0$ is sensible to assure that q_n remains small for any given n, where $q_n := q(n)n$.

2.2 Breaches in large scale networks

[1] Here ICT stands for information and communication technology.

[2] See [4, 15] for the literature review.

We start with (2), and derive an expression of breach probability for large scale networks with security interdependencies. As we suggested above, we assume that $q(n)n$ decreases with n, and that $g_\infty := q(n)n|_{n\to\infty}$ is small. Then, we can ignore the terms non-linear in q, and re-write (2) as:

$$B_i(s_1,...s_n) = 1 - s_i + s_i q(n) \sum_{j\neq i}^{n} (1 - s_j), \qquad (3)$$

from which we can express as:

$$B_i = 1 - s_i + s_i q_n \left\{ (1 - \ \bar{s}) - \frac{(1 - s_i)}{n} \right\}, \qquad (4)$$

where $q_n := q(n)n$ and $\bar{s}$ denotes average network security:

$$\bar{s} = \frac{1}{n} \sum_{j=1}^{n} s_j .$$

When n is high, we can ignore the last term in curly brackets:

$$B_i = B(s_i, \tilde{s}) = 1 - s_i \left[1 - q_n + \tilde{s} \right], \qquad (5)$$

where $\tilde{s} := g_\infty \bar{s}$. We will call s_i *own security* of player i, and $\tilde{s}$ – *network security*. In the limit $n \to \infty$, user i breach probability is:

$$B_i = 1 - s_i(1 - q_\infty) - s_i \tilde{s},$$

where

$$q_\infty := q(n)n|_{n\to\infty} \ \text{ and } \tilde{s} := g_\infty \bar{s}.$$

In line with common sense, from (5), no-breach probability $s_i(1 - g_\infty) + s_i\tilde{s}$ increases in both: own security (s_i) of player i, and network security $(\tilde{s} := g_\infty \bar{s})$. Parameter g_∞ is small, For more interdependent networks, the effect of interdependence on breach probability is stronger, and, by the same token, network security is more important.

In contract with our earlier work [13, 14, 12], where we *imposed* that for each player, breach probability is a function of two variables: player own security action, and average security of all players, in this paper we will formally *derive* the expression of breach probability from a standard one (3). The expression (4) is appropriate for large scale networks, and we will especially focus on its limiting case of high n, as given in (5).

This model of interdependence does not account for a possibility of correlated attack probabilities. That is, all attacks are assumed to be independent, and simultaneous attacks are ignored. In Section 7.1, we discuss the possibilities of modifying our assumptions on distribution of network risks to account for correlated (or cascading) risks. To account for correlated breach probabilities at the level of the entire network, we suggest to include an additional term high loss term.

3. HOMOGENOUS NETWORK WITH NO CYBER INSURERS: A SOLUTION

In this section, we will find individually optimal security choices of each player (i.e., Nash equilibrium) when no cyber insurers are present, and insurance contracts are unavailable. Then, each player i choice variable is security level $s_i \in [0, 1]$ which he chooses to maximize (1) with breach probability given by (3). Expected user i utility (1), can be written as:

$$U(W - L) + s_i \left[1 - q(n) \sum_{j\neq 1}^{n} (1 - s_j) \right] \cdot \Delta_0 - h(s_i),$$

where

$$\Delta_0 := \ \left[U(W) - U(W - L) \right].$$

User i optimal action (from FOC wrt s_i) is a solution of:

$$\left[1 - q(n) \sum_{j\neq i}^{n} (1 - s_j) \right] \Delta_0 - h'(s_i) \geq 0. \qquad (6)$$

We rewrite FOC as:

$$\left[1 - q_n(1 - \bar{s}) + \frac{q_n \left(1 - s_i^*\right)}{n} \right] \Delta_0 = h'(s_i^*), \qquad (7)$$

where $\Delta_0 > 0$, and we use $q_n \sum_{j\neq i}^{n} (1 - s_j) = q_n(1 - \bar{s}) - \frac{q_n(1 - s_i)}{n}$, and $q_n = \frac{q(n)}{n}$. Since user i SOC is negative, because from the proverties of the function $h''(\cdot) < 0)$ for any s_i, and thus, a single interior optimum $s_i^* = s_i^*(\bar{s})$ exists (for any fixed $\bar{s}$), and from the properties of function $h(\cdot)$, the boundaries of $s = 0$ and $s = 1$ cannot be optimal, thus, the interior maximum is indeed the optimal.

Next, let there exists an equilibrium with $\tilde{s}^*$, and let there exist two players whose optimal actions $s_i^* \neq s_j^*$. Let wlg $s_i^* > s_j^*$. Then, we can write FOC for player j as:

$$\left[1 - q_n(1 - \bar{s}^*) + \frac{q_n \left(1 - s_j^*\right)}{n} \right] \Delta_0 = h'(s_j^*), \qquad (8)$$

and subtracting (8) from (7) (FOCs for players j from FOC for player i) we obtain:

$$\frac{q_n}{n}(s_j^* - s_i^*)\Delta_0 = h'(s_i^*) - h'(s_j^*).$$

Since h' is increasing in s, for $s_i^* > s_j^*$, the right hand side is positive while the right hand side is negative. We conclude that $s_i^* = s_j^*$ and since i and j were arbitrary, player equilibrium security is identical, i.e., only symmetric equilibrium exists. This allows us to compute the equilibrium directly by setting $\bar{s} = s_i = s^*$ and using (7):

$$\Delta_0 = \frac{h'(s)}{\left[1 - \frac{(n-1)}{n} q_n(1 - s) \right]}, \qquad (9)$$

which for the limit of large n can be written as

$$\Delta_0 = R(s), \qquad (10)$$

where

$$R(s) := \frac{h'(s)}{\left[1 - q_\infty(1 - s) \right]}.$$

Equilibrium is unique, if the solution of (9) is unique. A sufficient condition for that is $R' > 0$:

$$R' = \frac{h''(s) \left[1 - q_n(1 - s) \right]}{\left[1 - q_n(1 - s) \right]^2} - \frac{h'(s) q_n}{\left[1 - q_n(1 - s) \right]^2} \geq 0,$$

$$h''(s) - q_n \left[h'(s) + (1 - s)h''(s) \right] \geq 0.$$

Further, to simplify the exposition, we will impose $R' > 0$ and restrict our attention to the case of a unique Nash equilibrium. For example, imposition of $h'''(\cdot) > 0$ results in $R' > 0$, which guarantees the uniqueness.

4. HOMOGENOUS NETWORK WITH CYBER INSURERS: A SOLUTION

Let us consider security choices of networked players (nodes) in the presence of (perfectly) competitive cyber insurers. We will define a setting following Rothschild-Stiglitz [1976], who examine equilibrium in insurance markets with adverse selection. Each insurer offers a single insurance contract in *a class of admissible contracts*, or does nothing. A Nash equilibrium is defined as a set of admissible contracts such that: i) all contracts offered at least break even; ii) taking as given the contracts offered by incumbent insurers (those offering contracts) there is no additional contract which an entrant-insurer (one not offering a contract) can offer and make a strictly positive profit; and iii) taking as given the set of contracts offered by other incumbent insurers, no incumbent can increase its profits by altering his offered contract.

The literature refers to such contracts as *competitive contracts*, because entry and exit are free, and because no barrier to entry or scale economies are present. We consider risk neutral cyber insurers, who compete with each other. In addition, following to Rothschild-Stiglitz, we assume no individual insurer can affect the network security $\tilde{s}$; thus, take each insurer takes network security as a given parameter.

We assume the following timing of the game: First (ex ante), network nodes (players) observe all contracts offered by cyber insurers; second, each node chooses which contract to accept (if any); third (ex post), the nodes choose their security level(s), (in both cases, with cyber contract or without). We assume that each cyber insurance contract includes a stipulation prohibiting the insured node to buy more than a single cyber security policy (contract).

At this point, some readers perhaps recognize that our formulation of the game does not specify whether ex ante, the players (the nodes and the insurers) have the information about ex post network security $\tilde{s}$. Still, as we demonstrate in Appendix, the game as we stated it could be solved. To proceed we will divide the problem into three steps. In Step 1, we will derive optimal security choices by the nodes under an assumption of buying contract (ρ_c, L_c). In Step 2, we will derive the contracts that are *viable* for cyber insurers. By a viable contract we mean that expected profit is non-negative, given that network nodes security choices are optimal. In Step 3, we derive an equation which solution gives equilibrium contract(s) $(\rho_c^\dagger, L_c^\dagger)$. The derivation employs an argument that only the contracts that maximize user utility will be purchased in equilibrium.

4.1 Step 1: Optimum with the contract (ρ_c, L_c)

Let there exist some given cyber contract (ρ_c, L_c) that is offered, and consider the choices of user i. Each user decides (i) which contract to purchase (in case if other, alternative contracts are offered) and (ii) which security level to choose. Since a decision to buy no insurance can be modeled as purchase of a contract $(0,0)$, we always can phrase user choice as a choice between at least two alternative contracts.

$$E[u_i] = B_i \cdot U(W - L - \rho_c + L_c) + (1 - B_i) \cdot U(W - \rho_c) - h(s_i),$$

where in general, $B_i = B_i(s_{1,} ... s_n)$, but from the derivation in Section 2.2, we have $B_i = B(s_i, \tilde{s})$.

User i expected utility with cyber-insurers present, AND assuming that he entered into a contract (ρ_c, L_c) could be written as:

$$B_i \cdot U(W - L - \rho_c + L_c) + (1 - B_i) \cdot U(W - \rho_c) - h(s_i). \quad (11)$$

From user ex post optimization (conditional on the purchase of a contract), we know that if all users indeed buy insurance, equilibrium is symmetric: the proof follows the same steps as in no-insurance case above, see Section 3. User i FOC is:

$$\Delta_{c0} = R(s, \tilde{s}), \quad (12)$$

where

$$R(s, \tilde{s}) := \frac{h'(s)}{[1 - q + \tilde{s})]} \quad (13)$$

and

$$\Delta_{c0} := [U(W - \rho_c) - U(W - \rho_c - (L - L_c))].$$

We can formulate the following proposition:

Proposition 1. *For a network with a given security $\tilde{s}$, for a user with a contract (ρ_c, L_c), with $L_c > 0$, individually optimal security $s = s^\dagger(\tilde{s}, \rho_c, L_c)$ is strictly lower than his optimal security $s = s^*(\tilde{s}, 0, 0)$ with no insurance coverage $L_c = 0$:*

$$s^\dagger(\tilde{s}, \rho_c, L_c) < s^*(\tilde{s}, 0, 0).$$

We use symmetry of user optimum $\bar{s}^\dagger = s^\dagger = s$, and $\tilde{s} = qs$:

$$\Delta_{c0} = \frac{h'(s)}{[1 - q(1 - s)]}, \quad (14)$$

Differentiating (14) wrt s, with an assumption of $h''' > 0$ we obtain that the right hand side derivative is positive:

$$\frac{h''(s)\,[1 - q(1 - s)] - h'q}{[1 - q(1 - s)]^2} > 0, \text{ if } h''' > 0. \quad (15)$$

Thus, there exists a unique user symmetric optimum for a given contract.

4.2 Step 2: Properties of viable contracts

We will use the results of Section 4.1 , in which we derive optimal user responses to a specific given contract to investigate the properties of viable cyber contracts. We will say that a contract is viable when expected insurer profit is non-negative. To assure non-negative cyber insurer profit, the following constraint has to hold

$$\rho_c = \rho_c(s_1, ... s_n, L_c) \geq B_i L_c.$$

With perfect cyber insurer competition, each insurer's expected profit is zero:

$$\rho_c = \rho_c(s_i, \tilde{s}, L_c) = B_i(s_i, \tilde{s}) L_c, \text{ with a given } \tilde{s}, \quad (16)$$

where since each insurer is small, he treats network security $\tilde{s}$ as given. A contract (ρ_c, L_c) with a premium given by (16) is called *actuarily fair contract.*

Consider some equilibrium in which $\tilde{s} = \tilde{s}^\dagger$, and assume that in this equilibrium user actions are identical: $\tilde{s}^\dagger = q_n \bar{s}^\dagger$, and $\bar{s}^\dagger = s_i^\dagger = s$. In this case, any given viable contract (ρ_c, L_c) offered for some insurers, will be accepted by all nodes due to the symmetry of their optimal action. A formal proof of symmetric optimal action mimics the proof of

Section 3. Let $s_i^\dagger(\rho_c, L_c, \bar{s})$ denote optimal response of user i with contract (ρ_c, L_c) when average security is $\bar{s}^\dagger$. Then,

$$s_i(\rho_c, L_c, \bar{s}) = \bar{s}, \tag{17}$$

because from zero profit condition (16) and (17) we can express $\rho_c(s_1, ... s_n, L_c) = \rho_c(s, L_c)$.

$$\rho_c^\dagger(s) = \rho_c^\dagger(s, L_c^\dagger) = B(s) L_c^\dagger(s), \tag{18}$$

where

$$B(s) = \left[1 - s(1-q) - (s)^2 q\right], \tag{19}$$

If users buy the same contract $(\rho_c^\dagger(s), L_c^\dagger(s))$, and network security is $\tilde{s} = q_n s$, and (14) holds:

$$R(s) = \ \Delta_{c0}.$$

Thus allows us to restate insurer problem as a problem of one independent variable, i.e., network security $\tilde{s}$ (or user security s). We will use s as an independent variable, and demonstrate that viable contract is unique, and can be determined from user optimality (14) and insurer zero profit (18). In Appendix, we prove the following result:

PROPOSITION 2. *Due to user optimum choices, for any given network security s, and if user optimal actions are symmetric (identical), there exists a unique corresponding viable contract $(\rho_c, L_c) = (\rho_c^\dagger(s), L_c^\dagger(s))$, and the derivatives $\frac{dL_c^\dagger}{ds}$ and $\frac{d\rho_c^\dagger}{ds}$ are negative.*

In Appendix, we obtain the expressions for $\frac{dL_c^\dagger}{ds}$ and $\frac{d\rho_c^\dagger}{ds}$, see (32) and (31):

$$\frac{dL_c^\dagger}{ds} = \frac{[R' + \Delta_{c1} B' L_c]}{B\Delta_{c1} - U'(W - \rho_c - L + L_c)} < 0, \tag{20}$$

and

$$\frac{d\rho_c^\dagger}{ds} = B' L_c + B\frac{dL_c^\dagger}{ds}, \text{ and } B' < 0. \tag{21}$$

Alternatively, one can express the conditions for viable contracts with L_c as an independent variable (instead of s). In some cases, such a formalization could be more intuitive, and also preferable on computational grounds. We will include it into a longer version of this paper (in preparation).

4.3 Step 3: User preferred contract(s)

Next, we derive an interior contract with which users reach maximal utility. We can demonstrate that such a contract exists (by construction). Consider an insurer a choice of a contract, such that if user optimum is symmetric $(\rho_c(s), L_c(s))$, this contract is viable for insurers, and also allows user utility to reach its maximum. Using the results of Section 4.2, to find such user preferred contract is equivalent to finding s that corresponds to this contract:

$$\max_s \{B \cdot U(W - L - \rho_c + L_c) + (1-B) \cdot U(W - \rho_c) - h(s)\}.$$

Then, insurer FOC, will determine equilibrium contract with which user utility is the highest. Let equilibrium be interior in s and user optimal actions be symmetric. Then,

$$\begin{aligned} &\{\{-s(1-q) - sq\}\,\Delta_{c0} - h'(s)\} - sq\Delta_{c0} \qquad (22) \\ &+ B\Delta_{c1}\frac{d\rho_c^\dagger}{ds} + B \cdot U'(W - L - \rho_c + L_c)\frac{dL_c^\dagger}{ds} \\ &= 0, \end{aligned}$$

where

$$\Delta_{c1} := \left[U'(W - \rho_c - (L - L_c)) - U'(W - \rho_c)\right] > 0.$$

We can combine (20) or (21) with user optimum and insurer FOC (i.e., user preferred contract), to obtain connection of L_c and s in equilibrium:

$$\frac{[B\Delta_{c1} + U'(W - \rho_c - L + L_c)]}{[B\Delta_{c1} - U'(W - \rho_c - L + L_c)]} = \frac{sqR - B\Delta_{c1}B'L_c}{B\,[R' + \Delta_{c1}B'L_c]}, \tag{23}$$

and we use (13),(19) (16) for R, B,and ρ_c:

$$R(s) := \frac{h'(s)}{[1 - q(1-s)]},$$

$$B = \left[1 - s(1-q) - (s)^2 q\right],$$

$$\rho_c = BL_c$$

to derive equilibrium contract(s) explicitly. Notice, that with a simplifying assumption of quadratic U, equilibrium equation (23) is analytically solvable: it is then quadratic in L_c.

Lastly, we have to investigate whether asymmetric user equilibrium could occur in some cases. In a longer version of this paper, we demonstrate that due to perfect insurer competition, no asymmetric user equilibrium exists. In this version, we restrict our attention by symmetric user equilibria only.

5. BENCHMARKS

5.1 Social optimum with no cyber insurers

To find a social optimum, we no longer consider and each individual's best responses, but instead find security level that maximizes cumulative expected payoff of all the users of the network. Let s^{**} denote security in social optimum. As for Nash, one can demonstrate that social optimum is symmetric. Under symmetry, social planner optimization problem becomes:

$$E[u_i] = U(W - L) + s\left[1 - q(1-s)\frac{(n-1)}{n}\right] \cdot \Delta_0 - h(s),$$

and from FOC, in social optimum, we have

$$\left\{\left[1 - q(1-s)\frac{(n-1)}{n}\right] + 2sq\frac{(n-1)}{n}\right\} \cdot \Delta_0 - h'(s) \geq 0,$$

and in interior optimum we:

$$\frac{h'(s)}{\left\{\left[1 - q(1-s)\frac{(n-1)}{n}\right] + 2sq\frac{(n-1)}{n}\right\}} = \Delta_0. \tag{24}$$

Comparison of (9) and (24), gives that social optimum coincides with Nash equilibrium only if $n = 1$. With more then one player, in Nash equilibrium (individual optimum), security is always lower than socially optimal, due to an extra term in the denominator of social planner FOC (24).

PROPOSITION 3. *In equilibrium, individually optimal user security s^* is strictly lower in social optimum:*

$$s^{**} < s^*.$$

From our analysis, Nash Equilibrium security is below socially optimal, and the gap (and thus, inefficiency) increases with network size (number of nodes) and for networks with higher interdependencies.

5.2 Optimum with vs without insurers

From the results of Sections 3 and 4, we infer that for homogenous networks the presence of insurers negatively affects security incentives:

PROPOSITION 4. *Let $s^{\dagger}$ denote user optimal security choice with a contract (ρ_c, L_c) purchased. In a symmetric interior equilibrium with non-zero coverage, user security $s^{\dagger}$ is strictly lower than user optimal choice with no insurance coverage $s^{\dagger} \leq s^*$.*

$$s^{\dagger} \leq s^*.$$

To prove Proposition 4, we compare (14) with (9) due to the fact that the right hand side of both, (14) with (9) increases with s, and left hand side is smaller with positive insurance coverage than without any coverage:

$$\Delta_{c0} \leq \Delta_0.$$

Notice, that we have not yet considered a (theoretically possible) asymmetric equilibrium where only some fraction of the nodes has positive coverage, while other nodes choose zero coverage. Then, in expectation, users with and without coverage must be indifferent between these two options. In a longer version of this paper, we prove that such configuration never occurs, and thus, equilibrium is always symmetric.

6. HETEROGENEOUS NETWORKS

Next, we consider network with n nodes / players, who can be heterogeneous. For such heterogeneous network, we will say that *two players have the same type* if their objective function (1) is identical, and (ii) both players employ identical equilibrium action(s).[3] We will assume that for each type k, the number of nodes is large. An alternative definition of a *player type* is to require (i). When for players of the same type equilibrium is symmetric, these definitions coincide. Requirement (ii) is especially appropriate for environments with multiple network nodes owned by the same player, which could result in asymmetric equilibria.

In this paper, we are limiting our attention to the case when each node chooses its action as a separate (individual) player. Let n_k be the number of type k nodes. Then:

$$\sum_{k=1}^{m} \alpha_k = 1,\ n = \sum_{k=1}^{m} n_k \text{ and } \alpha_k := \frac{n_k}{n},$$

where $m > 1$ is the number of different types of the network; the network with $m = 1$ is homogeneous network consisting of identical nodes. Each player i of type k players maximizes his expected utility:

$$E(u_{ik}) = B_{ik} \cdot U_k(W_k - L_k - \rho_c + L_c) + \\ (1 - B_{ik}) \cdot U_k(W_k - \rho_c) - h_k(s_{i_k}). \tag{25}$$

From (25), users of different types, may vary by their risk aversion (i.e., the shape of function $U = U_k(\cdot)$), security cost function $h = h_k(\cdot)$, initial wealth $W = W_k$, and $L = L_k$. Also, cyber contracts available for different types can differ by type: offered In addition, available cyber insurance contracts $(s_c, \rho_c, L_c) = (s_{ck}, \rho_{ck}, L_{ck})$ could differ with player type, and possibly, be non-zero contracts could be offered to certain user types only, but not for all the types. The types for whom cyber insurance is unavailable can be modeled as constrained to a contract with zero coverage $(0, 0, 0)$. Also, cyber insurance could be mandated for some (or all) types. In heterogeneous network, breach probabilities are defined by (2), and B_{ik} for player i of type k can be simplified (as for homogeneous network (2)), and wlg $B_{ik} = B_k$, and for $i = 1$ and $k = 1$:

$$B_1 = 1 - s_1 \\ + s_1 \left[\sum_{k \neq 1}^{m} q_k \sum_{j=1}^{n_k} (1 - s_j) + q_1 \sum_{j \neq 1}^{n_1} (1 - s_j) \right],$$

where q_k denotes indirect effect of node of type k on all other nodes; we assume that type k nodes have the same indirect effect on all others. We rewrite $B_{1k} = B_{i1} = B_1$ as:

$$B_1 = 1 - s_1 + s_1 \left[\sum_{k \neq 1}^{m} q_k(n_k) n_k (1 - \ \bar{s}_k) \right] \\ + s_1 q(n_1) n_1 \left\{ (1 - \ \bar{s}_1) - \frac{(1 - s_1)}{n_1} \right\},$$

where $\bar{s}_k = \frac{1}{n_k} \sum_{j=1}^{n_k} s_j$, is average security of type k nodes (i.e., only type k nodes securities are averaged to obtain $\bar{s}_k$).

$$B_1 = 1 - s_1 + s_1 \sum_{k=1}^{n_k} q(n_k) n_k \left\{ (1 - \ \bar{s}_k) \right\} \\ - s_1 q(n_1) n_1 \left\{ \frac{(1 - s_1)}{n_1} \right\}.$$

For high n, we ignore the last term in curly brackets:

$$B_1 = 1 - s_1 (1 - q) - s_1 \sum_{k=1}^{n_k} q_k \bar{s}_k,$$

where $\bar{s}_k = \frac{1}{n_k} \sum_{j=1}^{n_k} s_j$, and

$$q_k := q(n_k) n_k,\ q := \sum_{k=1}^{n_k} q_k,$$

and $\tilde{s} := \sum_{k=1}^{n_k} q_k \bar{s}_k$, and we will call $\tilde{s}$ *network security* for heterogeneous network.

$$B_k = 1 - s_k (1 - q) - s_k \tilde{s}. \tag{26}$$

Thus, we have shown that breach probability for the network with heterogeneous users could be expressed very similar to breach probability in the network of identical (homogeneous) users. Interestingly, when interdependence term $(q_k \equiv q)$ is the same for all types k, breach probability is identical for homogeneous and heterogeneous networks. This allows

[3] An alternative definition of a type could require that any two nodes of the same type to have identical expected utility function. When in equilibrium players with identical utilities make identical equilibrium choices, i.e., for players of the same type the equilibrium is symmetric, both definitions coincide. But our definition will be especially convenient when multiple network nodes are owned by the same player. In this paper, we will limit our attention to environments in which each node chooses its actions as a separate player.

remarkable simplification of the analysis for networks with heterogeneous types of nodes.

With identical players, we already derived breach probabilities $B_i = B_i(s_i^*, \bar{s} = s_i^*)$, when players security is optimal $s_{ik}^* = s(u, W, L, h, \bar{s} = s_i^*)$. These choices depend on player i risk-aversion, wealth, cost of security, and the amount of his loss. Similarly, breach probabilities B_i for a network with heterogeneous nodes can be derived from player security and network security, i.e., from player characteristics $U_k(\cdot), h_k(\cdot), W_k, L_k, q_k$, and network security $\tilde{s}$. Superficially (5) and (**??**) look the same, but for heterogeneous network, network security reflects the effects of different node types, by accounting their influence on others via interdependence (via q_k) and overall frequency of occurrence (via $\bar{s}_k$).

Below we will consider an important extension to two player types. It is straightforward to generalize this analysis to networks with multiple node types. For cases of multiple types of network nodes, computational algorisms based on our initial analysis should be developed. Once these steps are undertaken, these models can be fitted (parametrically) to investigate security of real cyber physical systems. In this case, the parameters of the model should be taken from data, and / or from simulations. Thereafter, with the help of testbeds the recommendations could be made for targeted (optimal) node security.

6.1 Network with two node types: A solution

We consider the network populated by two types of users, and within each type, users are identical, and for each player type, the effect on network security $\tilde{s}$ is negligible. Each user of first type, which we will call normal user type, maximizes (1) with breach probability given by (26):

Users of a second user type, whom we will call malicious, face no damage, even if attacked successfully. An example of a malicious user is a disgruntled employee. Or, malicious user could be criminal, aiming to game the system and milk the insurers.We will assume that type two users have the capabilities of subverting insurer monitoring of their security level, even when insurers could perfectly monitor (at zero cost) security levels of the normal users. Realistically, insurer monitoring is not perfect and costless. Thus, even if insurer requires the insured party to invest in security, she cannot assure that her insurees do maintain the required security level at all times. We assume that normal users are law-obedient. That is, they do not, or cannot subvert the insurer monitoring. For example, the subversion could be too costly for first user type.

Real networks undoubtedly has many users who do not care about security. These users typically have meager (or zero) losses and find it too costly to implement any security measures. We assume that a certain (fixed) fraction $\alpha \geq 0$ of network users belong to second type. Expected utility for type 2 is:

$$B_2 f(W) + (1 - B_2) f(W) - h(s) = f(W) - h(s), \qquad (27)$$

where

$$B_2 = 1 - s_2\,(1 - q) - s_2 \tilde{s},$$

From (27), for type 2, expected utility does not depend on B_2, and zero security is optimal for such users, which entails $s_2 = 0$ (and $h(0) = 0$):

$$E\left[U_{ik=2}\right] = f(W) - h(s) = f(W),$$

and

$$B_2 = 1,$$

and

$$B_1 = 1 - s_1\,(1 - q) - s_1 \tilde{s},$$

where

$$\tilde{s} := \sum_{k=1}^{n_k} q_k \bar{s}_k = q(1 - \alpha)\bar{s}_1,$$

where to simplify the exposition we let $q_1 = q_2 = q$, which gives

$$B_1 = 1 - s_1\,(1 - q) - s_1 q(1 - \alpha)\bar{s}_1.$$

For type 1 users optimal security is the same for all i $s_{i1}^m = s_1^m$, in which we use the fact that optimal action is symmetric (as demonstrated in Section 3). Optimal security $s_1^m = \bar{s}_1^m$ can be found as a solution of FOC for type 1 users:

$$\frac{h'(s_1^m)}{[(1 - q \ + q(1 - \alpha)s_1^m)]} = \Delta_0 \qquad (28)$$

From comparison with (10) which gives for s^* for the case of homogeneous network of normal users:

$$\frac{h'(s)}{[1 - q(1 - s)]} = \Delta_0.$$

and (28) we infer

$$s^* < s_1^m,$$

and

$$s^* < s_1^m$$

$$\tilde{s}^m = q(1 - \alpha)s_1^m < \tilde{s}^*.$$

To prove the last equation, consider a model of identical users with different (lower) interdependence parameter equal to $q^d = q(1 - \alpha)$. In this case, optimal security s^{d*} solves

$$\frac{h'(s^{d*})}{[(1 - q(1 - \alpha) + q(1 - \alpha)s^{d*}]} = \Delta_0, \qquad (29)$$

and comparison of (10) and (29) gives

$$s^* < s^{d*} \text{ and } \tilde{s}^* = qs^* < qs^{d*}.$$

When no malicious users are present, i.e., $\alpha = 0$, network is populated by identical normal users, (10) and (28) coincide, and $s^m = s^*$, the higher is the fraction α of malicious users, the higher is normal users optimal security investment relative to $\alpha = 0$, but network security $\tilde{s}^m$. Thus, we have shown:

Proposition 5. *With malicious users present [$\alpha \neq 0$], in equilibrium, network security is lower, and normal users' security s^m – higher than the respective values for $\alpha = 0$.*

Similarly, from comparison with a socially optimal allocation we infer:

Proposition 6. *With malicious users present [$\alpha \neq 0$], in social optimum, network security is lower, and normal users' security – higher than with $\alpha = 0$.*

From Propositions 5 and 6, we infer that although the presence of malicious users forces higher security of normal users, with malicious users explicitly included into setting, network security decreases.

7. CONCLUDING COMMENTS

Our analysis provides a rigorous derivation of cyber security contracts in a general setting, yet we demonstrated that our derivation requires only a limited amount of information. as we discuss in Section 6, our methodology generalizes to heterogeneous networks. Still, there remain several important issues that our model so far neglects. Below we briefly talk of three important avenues that we are planning to address in our future research.

Our analysis confirms a discrepancy between informal arguments that favor cyber-insurance as a tool to improve network security, rather than merely manage risks. Specifically, we observe that that in presence of cyber insurers, equilibrium network security is lower than if no cyber coverage is available. Thus, our results support that in isolation, availability if cyber-insurance does not allow to improve network security. Our framework helps to identify the crucial network parameters for improving incentives to provide secure networks.

7.1 Modeling correlated risks

Finally, some (or all) types could be subjected to additional loss(es) caused by correlated network risk (for example, risk of natural disasters (earthquakes), or risk or a terroristic attack). Such risks have very low probability $b_r \ll B_i$ of a very high loss $L_r \gg L_c$,.and even $L_r > W$. Such risks are called "catastrophic risks" or "rare events", and typically they are ignored by individual agents. Still, these risks have to be addressed at the societal level. Including these risks in utility allows to design mechanisms improving the management of these risks.

7.2 Modeling more detailed contracts

It is difficult to model multiple strategic insurer choices, and literature is dominated by the models that assume monopolistic insurers, which is not particularly realistic. Another extreme (that we pursuing in this paper) is to assume perfectly competitive market of cyber insurers, that makes insurers non-strategic due to complete lack of market power. Even papers that assume required return (load factor) do not model strategic insurer choices.

We will consider different assumptions on observability of player security and network security. And, we will consider two types of contracts: with (s_c, ρ_c, L_c), and without (ρ_c, L_c), imposition of required user security, where ρ_c – premium, L_c – amount of loss covered, and s_c a minimal security level required by the contract.

7.3 Modeling the causes of breaches

CPS risks can be broadly divided in two categories, strategic (that is driven by intended human actions), and non-strategic (that is driven by natural causes). Security policies, laws and regulations could affect both categories, albeit technical tools for the analysis are somewhat different. Your model permits to introducing attacker(s) as special player types, and examine the effects of various regulatory impositions on attacker incentives.

8. APPENDIX

Derivations for Sections 4.2 and 4.3

To prove Proposition 2, consider user FOC in a symmetric case:

$$\Delta_{c0} = R(s, \tilde{s}) = R(s),$$

where

$$\Delta_{c0} := \left[U(W - \rho_c) - U(W - \rho_c - (L - L_c))\right],$$

and we use (13) ,(19) (16) to have R, R',B, B' and ρ_c:

$$R(s) := \frac{h'(s)}{[1 - q(1 - s)]},$$

$$R'(s) = \frac{h''(s)\,[1 - q(1 - s)] - h'q}{[1 - q(1 - s)]^2},$$

$$B = \left[1 - s(1 - q) - (s)^2 q\right], \; B' = -(1 - q) - 2sq,$$

$$\rho_c = BL_c.$$

We differentiate user FOC (12) wrt s to derive the expression for $\frac{dL_c^\dagger}{ds}$

$$R' = \Delta_{c1}\frac{d\rho_c^\dagger}{ds} - U'(W - \rho_c - L + L_c)\frac{dL_c^\dagger}{ds}, \qquad (30)$$

where

$$\Delta_{c1} := \left[U'(W - \rho_c - (L - L_c)) - U'(W - \rho_c)\right] > 0,$$

and

$$\frac{d\rho_c^\dagger}{ds} = B'L_c + B\frac{dL_c^\dagger}{ds}, \text{ and } B' < 0, \qquad (31)$$

$$R' = \Delta_{c1}\left[B'L_c + B\frac{dL_c^\dagger}{ds}\right] - U'(W - \rho_c - L + L_c)\frac{dL_c^\dagger}{ds}$$

$$R' = \Delta_{c1}B\frac{dL_c}{ds} + U'(W - \rho_c - L + L_c)\frac{dL_c}{ds} + \Delta_{c1}B'L_c$$

$$\begin{aligned}&\Delta_{c1}B - U'(W - \rho_c - L + L_c)\\ &= (B - 1)\Delta_{c1} - U'(W - \rho_c) < 0\end{aligned}$$

$$\begin{aligned}&\Delta_{c1}\left[1 - s(1 - q) - (s)^2 q\right] - U'(W - \rho_c - L + L_c)\\ &= -s(1 - q) - (s)^2 q\Delta_{c1} - U'(W - \rho_c)\end{aligned}$$

$$\begin{aligned}&\underset{[+]}{\left[R' - \Delta_{c1}B'L_c\right]}\\ &= \Delta_{c1}B\frac{dL_c^\dagger}{ds} - U'(W - \rho_c - L + L_c)\frac{dL_c^\dagger}{ds},\end{aligned}$$

and we have

$$\frac{dL_c^\dagger}{ds} = \frac{[R' + \Delta_{c1}B'L_c]}{B\Delta_{c1} - U'(W - \rho_c - L + L_c)} < 0, \qquad (32)$$

and combining with (31) provides that Proposition 2 is proven.

For Step 3, we can combine (20) with the best user contract (user preferred), which we find from:

$$\begin{aligned}&\max_s \{\, B \cdot U(W - L - \rho_c + L_c)\\ &+ (1 - B) \cdot U(W - \rho_c) - h(s)\,\},\end{aligned}$$

which gives (under the assumptions of interior solution and symmetry of user equilibrium)

$$\begin{aligned}&\left\{\{-s(1-q)-sq\}\,\Delta_{c0}-h'(s)\right\}-sq\Delta_{c0}\\&+B\Delta_{c1}\frac{d\rho_c^\ddagger}{ds}+B\cdot U'(W-L-\rho_c+L_c)\frac{dL_c^\ddagger}{ds}\\&=0\end{aligned}$$

where the first curly bracket is zero (due to user optimality), and thus:

$$-sq\Delta_{c0}+B\Delta_{c1}\frac{d\rho_c^\ddagger}{ds}+B\cdot U'(W-L-\rho_c+L_c)\frac{dL_c^\ddagger}{ds}=0. \tag{33}$$

Next, we use (31) to get rid of direct dependence on $\frac{d\rho_c^\ddagger}{ds}$ in (33).

$$\begin{aligned}&-sq\Delta_{c0}+B\Delta_{c1}\left[B'L_c+B\frac{dL_c^\ddagger}{ds}\right]\\&+B\cdot U'(W-\rho_c-L+L_c)\frac{dL_c^\ddagger}{ds}\\&=0.\end{aligned}$$

$$\begin{aligned}&B^2\Delta_{c1}\frac{dL_c^\ddagger}{ds}+B\cdot U'(W-\rho_c-L+L_c)\frac{dL_c^\ddagger}{ds}\\&=sq\Delta_{c0}-B\Delta_{c1}B'L_c\end{aligned}$$

$$\begin{aligned}&B\left[B\Delta_{c1}+U'(W-\rho_c-L+L_c)\right]\frac{dL_c^\ddagger}{ds}\\&=sqR-B\Delta_{c1}B'L_c\end{aligned}$$

And then, substitute an explession (20) for $\frac{dL_c^\ddagger}{ds}$ into (33) to obtain equation connecting equilibrium $L_c^\ddagger$ and $s^\ddagger$

$$\begin{aligned}&\frac{[B\Delta_{c1}+U'(W-\rho_c-L+L_c)]}{[B\Delta_{c1}-U'(W-\rho_c-L+L_c)]}\\&=\frac{sqR-B\Delta_{c1}B'L_c}{B\left[R'+\Delta_{c1}B'L_c\right]},\end{aligned}\tag{34}$$

With a simplification to a quadratic U, equilibrium equation (34) is analytically solvable (quadratic in L_c).

References

[1] George A Akerlof. The market for 'lemons': Quality uncertainty and the market mechanism. *The Quarterly Journal of Economics*, 84(3):488–500, August 1970.

[2] R. Anderson, R. Böhme, R. Clayton, and T. Moore. Security economics and European policy. In *Proceedings of WEIS'08*, Hanover, USA, Jun. 25-28 2008.

[3] Rainer Böhme and Galina Schwartz. Modeling cyber-insurance: Towards a unifying framework. In *Proceedings of WEIS'10*, Cambridge, USA, Jun. 7-10 2010.

[4] Georges Dionne, Neil Doherty, and Nathalie Fombaron. *Adverse Selection in Insurance Markets*, chapter 7, pages 185–244. Handbook of Insurance. Boston: Kluwer Academic, 2000.

[5] Esther Gal-Or and Anindya Ghose. The economic incentives for sharing security information. Industrial Organization 0503004, EconWPA, March 2005.

[6] Geoffrey Heal and Howard Kunreuther. Interdependent security: A general model. NBER Working Papers 10706, National Bureau of Economic Research, Inc, August 2004.

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

[8] Howard Kunreuther and Geoffrey Heal. Interdependent security. *Journal of Risk and Uncertainty*, 26(2-3):231–49, March-May 2003.

[9] Mark Lelarge and Jean Bolot. Economic incentives to increase security in the internet: The case for insurance. In *INFOCOM 2009, IEEE*, pages 1494–1502, April 2009.

[10] H. Ogut, N. Menon, and S. Raghunathan. Cyber insurance and it security investment: Impact of interdependent risk. In *Proceedings of WEIS'05*, Cambridge, USA, 2005.

[11] Michael Rothschild and Joseph E. Stiglitz. Equilibrium in competitive insurance markets: An essay on the economics of imperfect information. *The Quarterly Journal of Economics*, 90(4):630–49, November 1976.

[12] Galina Schwartz, Nikhil Shetty, and Jean Walrand. Why cyber-insurance contracts fail to reflect cyber-risks. In *Allerton Conference*, pages XX – XX, 2013.

[13] N. Shetty, G. Schwartz, M. Felegyhazi, and J. Walrand. Competitive Cyber-Insurance and Internet Security. In *Workshop on Economics of Information Security 2009*, University College London, England, June 2009.

[14] Nikhil Shetty, Galina Schwartz, and Jean Walrand. Can competitive insurers improve network security? In Alessandro Acquisti, SeanW. Smith, and Ahmad-Reza Sadeghi, editors, *Trust and Trustworthy Computing*, volume 6101 of *Lecture Notes in Computer Science*, pages 308–322. Springer Berlin Heidelberg, 2010.

[15] Ralph Winter. *Optimal Insurance under Moral Hazard*, chapter 6, pages 155–183. Handbook of Insurance. Boston: Kluwer Academic, 2000.