Uncertainty in the Weakest-Link Security Game

Jens Grossklags and Benjamin Johnson

Abstract— **Individuals in computer networks not only have to invest to secure their private resources from potential attackers, but have to be aware of the existing interdependencies that exist with other network participants. Indeed, a user's security is frequently negatively impacted by protection failures of even just one other individual, the *weakest link*.**

In this paper, we are interested in the impact of bounded rationality and limited information on user payoffs and strategies in the presence of strong weakest-link externalities.

As a first contribution, we address the problem of bounded rationality by proposing a simple but novel modeling approach. We anticipate the vast majority of users to be unsophisticated and to apply approximate decision-rules that fail to accurately appreciate the impact of their decisions on others. Expert agents, on the other hand, fully comprehend to which extent their own and others' security choices affect the network as a whole, and respond rationally.

The second contribution of this paper is to address how the security choices by users are mediated by the information available on the severity of the threats the network faces. We assume that each individual faces a randomly drawn probability of being subject to a direct attack. We study how the decisions of the expert user differ if all draws are common knowledge, compared to a scenario where this information is only privately known.

We further propose a metric to quantify the value of information available: the payoff difference between complete and incomplete information conditions, divided by the payoff under the incomplete information condition. We study this ratio metric graphically and isolate parameter regions where being more informed creates a payoff advantage for the expert agent.

I. Introduction

Security practitioners frequently draw the analogy between the strength of protective measures and the weakest-link interdependency.[1] In general, interdependencies occur when the security actions of a given user have an effect on the rest of the users in the network, in part or as a whole. Specifically, in the weakest-link externality an attacker is able (after approaching her target) to identify the least protected point in the system of interconnected resources in which the target is embedded. Depending on the type and security actions of defenders the weaknesses of a system can be costly to circumvent, and of surprising variety.

On the one hand, technology and code quality are often the culprits of (un)predictable weaknesses in the chain of defense. The increasing complexity of software products (for example, because of code bloat and feature creep) leaves little doubt that most publicly available software products include several significant security vulnerabilities [13]. But even sophisticated and thoroughly tested security software and protocols (e.g., certain hard disk encryption packages) can sometimes be broken with non-standard attacks [21], or large-scale brute-force efforts [26]. Legal, regulatory and law enforcement requirements can also put limits on security effectiveness (e.g., through mandatory escrow of encryption keys or inclusion of back doors in hardware and software technologies) [4].

On the other hand, many observers argue that the "human factor is truly security's weakest link" [28]. First, insiders may maliciously interfere with data and network security to the disadvantage of other individuals [31]. Second, an abundance of incidents involving lost and stolen property (e.g., laptops and storage devices), as well as individuals' susceptibility to deception and social engineering are evidence of breaches characterizing weakest-link vulnerabilities. Third, users may out of convenience, cognitive limitations or economic considerations engage in insecure practices. The most common example is the prevalent use of weak passwords in organizations reported in many empirical and behavioral studies [5], [35].[2] Password misuse can sometimes be remedied, but it "only requires one indiscretion to destroy a secret" [8] such as the identities of members of a darknet (for filesharing purposes).

The last observations can be generalized to the variety of security precautions that users can implement to safeguard their individual systems, and to limit the potential negative externalities that their peers have to endure. Recent studies show that users frequently fail to deploy, or upgrade security technologies, or to carefully preserve and backup their valuable data [24], [30], which leads to considerable monetary losses to both individuals and corporations every year.

In this paper, we continue the investigation of the weakest-link security problem from an economic perspective. Prior work includes the seminal study by Hirshleifer [22], Varian's investigation of public goods functions in the context of security and reliability [34], and our own prior work [18], [19]. In all of these studies end users rationally undertake a cost-benefit analysis and decide for or against certain security

J. Grossklags is with the School of Information, University of California, Berkeley, CA 94720, USA jensg@ischool.berkeley.edu

B. Johnson is with CyLab, Carnegie Mellon University, Pittsburgh, PA 15213, USA johnsonb@andrew.cmu.edu

[1] See, for example, an interview with a security company CEO conducted by the New York Times (September 12, 2007), "Who needs hackers," available at http://www.nytimes.com/2007/09/12/technology/techspecial/12threat.html, stating that: "As computer networks are cobbled together [...] the Law of the Weakest Link *always* seems to prevail."

[2] For example, the analysis of a leaked password data set from phpbb.com revealed that 16% of passwords matched a person's first name, 14% of passwords were patterns on the keyboard, 4% were variations of the word "password" etc. Analysis available as online article "PHPBB Password Analysis" at: http://www.darkreading.com/blog/archives/2009/02/phpbb_password.html.

actions with implications for overall system security [14], [32].

With the current analysis we want to emphasize two issues of relevance for security decision-making. First, the risk management explanation overemphasizes the rationality of the involved consumers [7], [23]. In practice, consumers face the task to "prevent security breaches within systems that sometimes exceed their level of understanding" [3]. And second, the amount of information users may be able to acquire, is limited so that users have to implement their security strategy under considerable uncertainty [1].

As a first contribution, we address the problem of bounded rationality by proposing a simple but novel modeling approach. We anticipate the vast majority of users to be *unsophisticated (or naïve)*, and to apply approximate decision-rules that fail to accurately appreciate the impact of their decisions on others [1]. In particular, we assume non-expert users to conduct a simple self-centered cost-benefit analysis, and to neglect interdependencies. Such users would secure their system only if the vulnerabilities being exploited can cause a direct annoyance to them (e.g., their machine becomes completely unusable), but would not act when they cannot perceive or understand the effects of their insecure behavior (e.g., when their machine is used as a relay to send moderate amounts of spam to third parties).

In contrast, a *sophisticated (or expert)* user fully comprehends to which extent her own and others' security choices affect the network as a whole, and responds rationally. We study the strategic optimization behavior of such an expert user in an economy of naïve end users for the weakest-link interdependency by applying a decision-theoretic approach [6], [15].

The second contribution of this paper is to address how the security choices by users are mediated by the information available on the severity of the threats the network faces. We assume that each individual faces a randomly drawn probability of being subject to a direct attack. We study how the decisions of the expert user differ if all draws are common knowledge, compared to a scenario where this information is only privately known. With this approach we provide two important baseline cases for the impact of the expert agent.

We further propose a metric to quantify the value of information available to the agents. Specifically, we conduct a graphical analysis of a ratio metric for the total expected payoff for the expert user considering the two information conditions. By evaluating this metric for a range of parameters, we can determine when being less informed does not significantly jeopardize an expert user's payoff.

The rest of this paper is organized as follows. We first discuss selected work related to our analytic model and describe the model in detail, including our assumptions about agent behaviors and information conditions (Section II). Then, we present our methodology and formal decision-theoretic analysis in Section III. We discuss the results and their implications, and our metric approach to the measurement of information inefficiencies and conduct a preliminary graphical analysis in Section IV. Finally, we are offering concluding remarks in Section V and describe our plans for future work in Section VI.

II. Description of decision-theoretic model

We base our model on our previously proposed framework [18], and extend it to the case of an economy consisting of an expert user and several unsophisticated users. Our analysis significantly differs from prior decision-theoretic approaches that we summarize briefly in the following.

A. Relation to other decision-theoretic approaches

Gordon and Loeb present a model that highlights the trade-off between perfect and cost-effective security [15]. They consider the protection of an information set that has an associated loss if compromised, probability of attack, and probability that an attack is successful. They show that an optimizing firm will not always defend highly vulnerable data, and only invest a fraction of the expected loss. Cavusoglu *et al.* [6] consider the decision-making problem of a firm when attack probabilities are externally given compared to a scenario when the attacker is explicitly modeled as a strategic player in a game-theoretic framework. Their model shows that if the firm assumes that the attacker strategically responds then in most considered cases its profit will increase.

B. Model overview

Self-protection and self-insurance. In practice, the arsenal of a defender may include several actions to prevent successful compromises and to limit losses that result from a breach [10]. In Grossklags *et al.* we provide a model that allows a decoupling of investments in the context of computer security [18]. On the one hand, the perimeter can be strengthened with a higher protection investment (e.g., implementing or updating a firewall). On the other hand, the amount of losses can be reduced by introducing self-insurance technologies and practices (e.g., backup provisions). Formally, player i chooses a self-insurance level $0 \leq s_i \leq 1$ and a protection level $0 \leq e_i \leq 1$. $b \geq 0$ and $c \geq 0$ denote the unit cost of protection and self-insurance, respectively, which are homogeneous for the agent population. So, player i pays be_i for protection and cs_i for self-insurance.

Interdependency. We focus in this work on the weakest-link security game which is an example for tightly coupled networks [22], [34]. In a tightly coupled network all defenders will face a loss if the condition of a security breach is fulfilled whereas in a loosely coupled network consequences may differ for network participants. The interdependency is modeled with a public goods "contribution" function that characterizes the effect of e_i on agent's utility U_i, subject to the protection levels chosen (contributed) by *all* other players [34]. The weakest-link contribution function is defined as $H = \min(e_i, e_{-i})$, where, following common notation, e_{-i} denotes the set of protection levels chosen by players other

than i. We require that H be defined for all values over $(0,1)^N$.

Attack probabilities, network size and endowment. Each of $N \in \mathbb{N}$ agents receives an endowment M. If she is attacked and compromised successfully she faces a loss L. We restrict our attention to cases with $N \geq 2$, and $0 \leq b, c \leq L \leq M$; that is, there is no bankruptcy due to security attacks. We assume that each agent i draws an individual attack probability p_i ($0 \leq p_i \leq 1$) from a uniform random distribution. This models the heterogeneous preferences that attackers have for different targets, due to their economic, political, or reputational agenda. The choice of a uniform distribution ensures the analysis remains tractable, while already providing numerous insights. We conjecture that different distributions (e.g., power law) may also be appropriate in practice.

C. Player behavior

At the core of our analysis is the observation that expert and non-expert users differ in their understanding of the complexity of networked systems. Indeed, consumers' knowledge about risks and means of protection with respect to privacy and security can be quite varied [1], and field surveys separate between high and low expertise users [33].

Sophisticated (expert) user. Advanced users can rely on their superior technical and structural understanding of computer security threats and defense mechanisms when they select an adequate security strategy [9]. In the present context, expert users, for example, have less difficulty to conclude that the problem of safeguarding a corporate network is indicative of a weakest-link optimization problem [18]. Accordingly, a sophisticated user correctly understands her utility to be dependent on the weakest-link interdependencies that exist in the network:

$$U_i = M - p_i L(1 - s_i)(1 - \min(e_i, e_{-i})) - be_i - cs_i \ .$$

Naïve (non-expert) user. Average users underappreciate the interdependency of network security goals and threats [1], [33]. We model the *perceived* utility of each naïve agent to only depend on the direct security threat and the individual investment in self-protection and self-insurance. The investment levels of other players are *not* considered in the naïve user's decision making, despite the existence of interdependencies. We define the perceived utility for a specific naïve agent j as:

$$PU_j = M - p_j L(1 - s_j)(1 - e_j) - be_j - cs_j \ .$$

Clearly, perceived and realized utility actually differ: by failing to incorporate the interdependencies of all agents' investment levels in their analysis, naïve users may achieve sub-optimal payoffs that actually are far below their own expectations. This paper does not aim to resolve this conflict, and, in fact, there is little evidence that users will learn the complexity of network security over time [33]. We argue that non-expert users would repeatedly act in an inconsistent fashion. This hypothesis is supported by findings in behavioral economics that consumers repeatedly deviate from rationality, however, in the same predictable ways [25].

Binary strategies. We further restrict the actions available to each agent (of either type) to make the analysis tractable. Instead of picking a continuous protection level $0 \leq e_i \leq 1$, agents only have the choice between $e_i = 0$ ("do not protect") or $e_i = 1$ ("protect"). Likewise, the parameter space for s_i is restricted to a binary choice $s_i \in \{0, 1\}$. While this may seem a very strong restriction, prior analysis [18], [19] showed that, for all models we look at, efficient Nash equilibria are all of the form $(e_i, s_i) \in \{(0,0), (0,1), (1,0)\}$ (respectively, "passivity," "full self-insurance," and "full protection") for all agents i, even when agents can choose e_i and s_i from a continuous spectrum of values. Further, in practice many security choices are presented to individuals in discrete format. For example, users have to decide whether to procure and install a new security technology [27], [29], or whether they want to apply a particular patch [2].

D. Information conditions

Our analysis is focused on the decision making of the expert user subject to the bounded rational behaviors of the naïve network participants. That is, more precisely, the expert agent maximizes their expected utility subject to the available information about other agents' drawn threat probabilities and their resulting actions. Two different information conditions may be available to the expert agent:

Complete information: Actual draws of attack probabilities p_j for all $j \neq i$, and her own drawn probability of being attacked p_i.

Incomplete information: Known probability distribution of the unsophisticated users' attack threat, and her own drawn probability of being attacked p_i.

Therefore, the expert agent can accurately infer what each agent's investment levels are in the complete information scenario. Under incomplete information the sophisticated user has to develop an expectation about the actions of the naïve users.

III. Decision-theoretic analysis

Agents have three main strategies at their disposal. That is, they may either prefer to invest in protection, or self-insurance, or they can remain passive. The basic approach of our analysis is to conduct pairwise comparisons between the three strategies and to derive the conditions for the important parameters under which each of the strategies is optimal.

A. Basic methodology

In the remainder of this discussion, we will always use the index i to denote the expert player, and $j \neq i$ to denote the naïve players. Our analysis proceeds via the following five-step procedure.

1) Determine player i's payoff within the weakest link game for selected strategies of passivity, full self-insurance, and full protection.
2) Determine the conditions on the game's parameters (b, c, L, N, p_i, and if applicable, p_j for $j \neq i$) under which player i should select each strategy.

3) Determine additional conditions on the parameters such that the probability (relative to p_i) of each case, as well as the expected value of p_i within each case can be easily computed.
4) Determine player i's total expected payoff relative to the distribution on p_i and all other known parameters.
5) In the case of complete information, eliminate dependence on p_j for $j \neq i$ by taking, within each parameter case, an appropriate expected value.

B. Examples of computation

In the remainder of this section we exemplify this method by highlighting the more difficult cases in the analysis.

Step 1: Payoff computation

Table I records the payoffs for the expert player given the choice between the three security strategies. Each entry in this table is determined by substituting the specified information condition and selected strategy into the basic utility function for player i,

$$U_i = M - p_i L(1 - \min(e_i, e_{-i}))(1 - s_i) - be_i - cs_i. \quad (1)$$

As a result of these computations we derive case functions. To make the information easier to present and manipulate, we have included case divisions as row labels, so that all entries can be expressed in a simple closed form. For example, to compute the payoff for full protection with *complete* information, we substitute $(e_i, s_i) = (1, 0)$ into Equation 1 to get:

$$M - b - p_i L(1 - \min_{j \neq i} e_j). \quad (2)$$

Our assumptions about players $j \neq i$ is that they play the naïve strategy. That is, they protect fully if and only if $b \leq c$ and $b \leq p_j L$. Hence,

$$\min_{j \neq i} e_j = \begin{cases} 1 & \text{if } b \leq c \text{ and } \frac{b}{L} \leq \min_{j \neq i} p_j \\ 0 & \text{otherwise} \end{cases}. \quad (3)$$

The payoff for full protection with complete information can thus be expressed as the case equation:

$$U_i = \begin{cases} M - b & \text{if } b \leq c \text{ and } \frac{b}{L} \leq \min_{j \neq i} p_j \\ M - b - p_i L & \text{otherwise} \end{cases}. \quad (4)$$

By subdividing the various cases, we get the closed form expressions listed in Table I.

Next, we consider the case of *incomplete* information. If $c < b$, then we know none of the naïve players will protect, so the payoff for player i will always be:

$$M - b - p_i L. \quad (5)$$

If $b \leq c$, however, player i's utility depends on the unknown information $\min_{j \neq i} e_j$. The best we can do with the information we have is to compute an expected utility for player i by evaluating:

$$M - b - p_i L(1 - E[\min_{j \neq i} e_j]) \quad (6)$$

(following Equation 2). Since $\min_{j \neq i} e_j$ takes values in $\{0, 1\}$, its expected value is just $Pr[\min_{j \neq i} e_j = 1]$, which (using Equation 3 and the assumption $b \leq c$) is the probability that all the drawn p_j's are greater than $\frac{b}{L}$, and this in turn is equal to $\left(1 - \frac{b}{L}\right)^{N-1}$. So the (expected) payoff for protection under incomplete information and $b \leq c$ is

$$M - b - p_i L \cdot \left(1 - \left(1 - \frac{b}{L}\right)^{N-1}\right). \quad (7)$$

Step 2: Strategy selection

Now that the payoffs for each strategy have been explicitly recorded, we seek to determine which of the three potential strategies maximizes the payoff for player i, relative to all known parameters.

In the case $c < b$, the payoff expressions from Table I are simple, and do not depend on the information conditions (i.e., complete or incomplete). In this case, the payoff for protection $M - b - p_i L$ is always (weakly) dominated by the payoff for passivity $M - p_i L$; hence it is never advantageous in the case $c < b$ for player i to choose protection. The choice then is between self-insurance and passivity, with self-insurance the preferable option when $p_i > \frac{c}{L}$, and passivity the better option if $p_i < \frac{c}{L}$. In the case $p_i = \frac{c}{L}$, the payoffs for passivity and self-insurance are the same; for consistency we adopt the convention that under these circumstances the expert prefers to self-insure.

When $b \leq c$ in the case of complete information, determining the strategy selection conditions is still relatively easy. When $b \leq c$ and $\min_{j \neq i} p_j < \frac{b}{L}$, the payoffs for all three strategies are the same as above, and thus the strategy selection conditions are also the same as above. In the case $b \leq c$ and $\frac{b}{L} \leq \min_{j \neq i} p_j$, the payoff for protection is now $M - b$. Thus, assuming that $b \leq c$ the payoff for self-insurance $M - c$ is always (weakly) dominated by the payoff for protection. Hence, the expert reasonably selects between protection $M - b$ and passivity $M - p_i L$, with protection preferable when $p_i > \frac{b}{L}$ and passivity preferable when $p_i < \frac{b}{L}$. In the case of a tie $p_i = \frac{b}{L}$ we follow the convention that the expert selects protection.

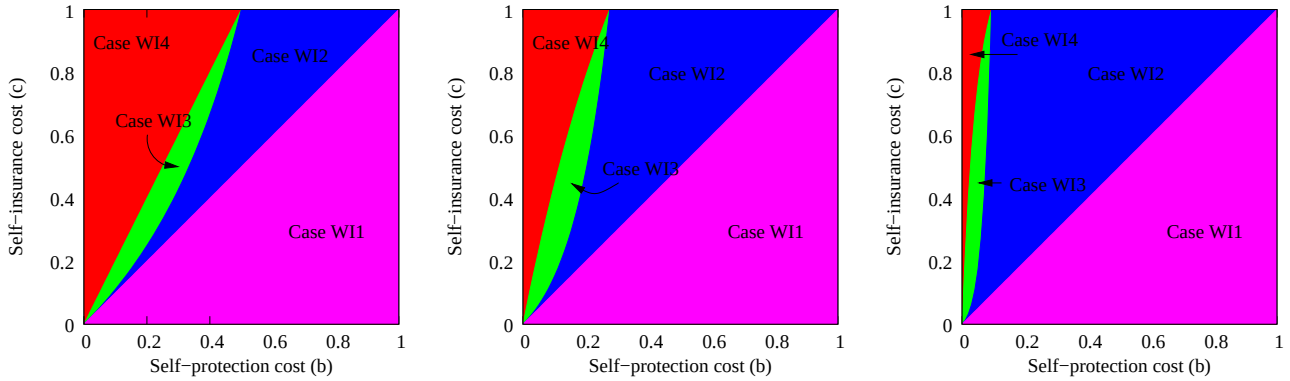
The case $b \leq c$ with limited information is the more difficult case. To determine the optimal strategy for player i, we must select the maximum of the payoffs for passivity: $M - p_i L$, self-insurance: $M - c$, and protection: $M - b - p_i L(1 - (1 - b/L)^{N-1})$. We should choose passivity if it is better than self-insurance or protection, i.e. $M - p_i L > M - c$ and $M - p_i L > M - b - p_i L(1 - (1 - b/L)^{N-1})$. We should choose self-insurance if it is better than passivity or protection, i.e. $M - c \geq M - p_i L$ and $M - c > M - b - p_i L(1 - (1 - b/L)^{N-1})$. We should choose protection if it is preferable to passivity or self-insurance, i.e. $M - b - p_i L(1 - (1 - b/L)^{N-1}) \geq M - p_i L$ and $M - b - p_i L(1 - (1 - b/L)^{N-1}) \geq M - c$.

Re-writing the above inequalities as linear constraints on p_i, we choose passivity if $p_i \leq c/L$ and $p_i \leq \frac{b}{L(1-(1-b/L)^{N-1})}$; we choose self-insurance if $p_i > c/L$ and $p_i > \frac{c-b}{L(1-(1-b/L)^{N-1})}$; and we choose protection if

TABLE I

WEAKEST LINK SECURITY GAME: PAYOFFS FOR DIFFERENT STRATEGIES UNDER DIFFERENT INFORMATION CONDITIONS

	Case	Information Type	Payoff Passivity	Payoff Self-Insurance	Payoff Protection
	$c < b$	Complete	$M - p_i L$	$M - c$	$M - b - p_i L$
	$b \leq c$ and $\min_{j \neq i} p_j < \frac{b}{L}$	Complete	$M - p_i L$	$M - c$	$M - b - p_i L$
	$b \leq c$ and $\frac{b}{L} \leq \min_{j \neq i} p_j$	Complete	$M - p_i L$	$M - c$	$M - b$
	$c < b$	Incomplete	$M - p_i L$	$M - c$	$M - b - p_i L$
	$b \leq c$	Incomplete	$M - p_i L$	$M - c$	$M - b - p_i L \left(1 - \left(1 - \frac{b}{L}\right)^{N-1}\right)$



(a) $N = 2$ **(b)** $N = 5$ **(c)** $N = 25$

Fig. 1. **Cases for incomplete information conditions** (The highlighted regions indicate the four cases identified in Table II. The x-axis covers values for protection cost b, and the y-axis shows self-insurance cost c. The loss penalty is fixed at $L = 1$. Displayed are graphs for three different network sizes.)

$\frac{c-b}{L(1-(1-b/L)^{N-1})} \leq p_i \leq \frac{b}{L(1-(1-b/L)^{N-1})}$.

For simplicity of computation, we would like to have our decision mechanism involve only a single inequality constraint on p_i. To obtain this sub-result it is necessary and sufficient to determine the ordering of the three terms: $\frac{c}{L}$, $\frac{b}{L(1-(1-b/L)^{N-1})}$, and $\frac{c-b}{L(1-(1-b/L)^{N-1})}$.

It turns out that there are only two possible orderings for these three terms. The single inequality

$$c < \frac{b}{(1-b/L)^{N-1}} \tag{8}$$

determines the ordering: $\frac{c}{L} < \frac{c-b}{L(1-(1-b/L)^{N-1})} < \frac{b}{L(1-(1-b/L)^{N-1})}$; while the reverse of Inequality 8 determines the reverse ordering on all three terms. This observation suggests we should add sub-cases under $b \leq c$ depending on which of these two inequalities holds. See Table II.

Within each new sub-case the criterion for selecting the strategy that gives the highest payoff can now be represented by a single linear inequality on p_i. If $c \leq \frac{b}{(1-b/L)^{N-1}}$, then passivity is preferable as long as $p_i < c/L$; (because the new case conditions also guarantee $p_i < \frac{b}{L(1-b/L)^{N-1}}$). Similarly, self-insurance wins if $p_i \geq c/L$. Protection will never be preferred in this case because we cannot have

$$\frac{c-b}{L\left(1-(1-b/L)^{N-1}\right)} \leq p_i \leq \frac{b}{L\left(1-(1-b/L)^{N-1}\right)}$$

when we also have $\frac{b}{(1-b/L)^{N-1}} < \frac{c-b}{L\left(1-(1-b/L)^{N-1}\right)}$. The computations for the case $\frac{b}{(1-b/L)^{N-1}} < c$ are similar; the results are recorded in Table II.

Step 3: Case determination

Now that we have written down the payoffs and conditions, it should be a straightforward task to write down an expression for the expert player's total expected payoff, by taking an expected value over all possibilities for p_i and (where applicable) p_j. Unfortunately, writing such an expression at this point in the process requires considering additional cases, essentially because some of the conditions on p_i from the previous step may not be compatible with the requirement that p_i is a probability in $[0, 1]$. Because the computation of a total expected payoff is already somewhat cumbersome, we take an additional step to produce an efficient set of case constraints such that all the probabilities and expected values necessary to compute the total expected payoffs can be written in closed form given the additional breakdown of cases.

Consider the various linear constraints on p_i from Table II. Because we have assumed from the onset that $0 \leq b, c \leq L$, the only difficulty arises with the case $\frac{b}{\left(1-\frac{b}{L}\right)^{N-1}} < c$ under the conditions of incomplete information. Here (referring to Table II for the values) we must introduce additional cases to determine how the quantities $\frac{b}{L\left(1-\frac{b}{L}\right)^{N-1}}$ and $\frac{c-b}{L\left(1-\left(1-\frac{b}{L}\right)^{N-1}\right)}$ relate to 1, and to each other.

From the case assumption $\frac{b}{\left(1-\frac{b}{L}\right)^{N-1}} < c$ we can deduce that $\frac{b}{L\left(1-\frac{b}{L}\right)^{N-1}}$ is both less than 1 and also less than $\frac{c-b}{L\left(1-\left(1-\frac{b}{L}\right)^{N-1}\right)}$. Hence, it remains to know the greater of

TABLE II

WEAKEST LINK SECURITY GAME: CONDITIONS TO SELECT PROTECTION, SELF-INSURANCE OR PASSIVITY STRATEGIES

	Case	Information Type	Conditions Passivity	Conditions Self-Insurance	Conditions Protection
	$c < b$	Complete	$p_i < \frac{c}{L}$	$p_i \geq \frac{c}{L}$	NEVER!
	$b \leq c$ and $\min_{j \neq i} p_j < \frac{b}{L}$	Complete	$p_i < \frac{c}{L}$	$p_i \geq \frac{c}{L}$	NEVER!
	$b \leq c$ and $\frac{b}{L} \leq \min_{j \neq i} p_j$	Complete	$p_i < \frac{b}{L}$	NEVER!	$p_i \geq \frac{b}{L}$
	$c < b$	Incomplete	$p_i < \frac{c}{L}$	$p_i > \frac{c}{L}$	NEVER!
	$b \leq c \leq \frac{b}{\left(1-\frac{b}{L}\right)^{N-1}}$	Incomplete	$p_i < \frac{c}{L}$	$p_i \geq \frac{c}{L}$	NEVER!
	$\frac{b}{\left(1-\frac{b}{L}\right)^{N-1}} < c$	Incomplete	$p_i < \frac{b}{L\left(1-\frac{b}{L}\right)^{N-1}}$	$p_i > \frac{c-b}{L\left(1-\left(1-\frac{b}{L}\right)^{N-1}\right)}$	$\frac{b}{L\left(1-\frac{b}{L}\right)^{N-1}} \leq p_i \leq \frac{c-b}{L\left(1-(1-\frac{b}{L})^{N-1}\right)}$

1 or $\frac{c-b}{L\left(1-\left(1-\frac{b}{L}\right)^{N-1}\right)}$, and this is not determined by our previous case conditions. We thus add this relation as an additional case consideration, rewriting $\frac{c-b}{L\left(1-\left(1-\frac{b}{L}\right)^{N-1}\right)} < 1$ for consistency as the following linear inequality on c yields

$$c < b + L\left(1 - \left(1 - \frac{b}{L}\right)^{N-1}\right).$$

Figure 1 includes three plots of the four distinct cases for the incomplete information condition as functions of b and c, with fixed L and N, helping us to see more directly how the parameters inform the case conditions.

Step 4: Total payoff computation

Now that the cases are established so that all best-strategy decisions can be made by evaluating a simple linear inequality on p_i, it is straightforward to compute the probability (over p_i) that each decision is reached, given a set of fixed parameters (other than p_i). These probabilities are recorded in Table III. It is now also easy to compute the expected value of p_i within each decision case, but we have not included a separate table of expected p_i here because they are more complicated to display and only serve as an intermediate step during the process of payoff computation.

The total payoff for each parameter case is computed by evaluating (Probability of passivity · Expected payoff for passivity) + (Probability of self-insurance · Expected payoff for self-insurance) + (Probability of protection · Expected payoff for protection). As an example, we compute the total expected payoff for the parameter case $b \leq c$ and $\frac{b}{L} \leq \min_{j \neq i} p_j$. Here we have:

$$\begin{aligned}
&\text{Payoff}[passivity] \cdot Pr[passivity] \\
&+ \text{Payoff}[insurance] \cdot Pr[insurance] \\
&+ \text{Payoff}[protection] \cdot Pr[protection] \\
&= [M - E[p_i] \cdot L] \cdot \left[\frac{b}{L}\right] + [M - c] \cdot [0] + [M - b] \cdot \left[1 - \frac{b}{L}\right] \\
&= \left[M - \left(\frac{b}{2L}\right) \cdot L\right] \cdot \left[\frac{b}{L}\right] + [M - b] \cdot \left[1 - \frac{b}{L}\right] \\
&= M - \frac{b^2}{2L} - b + \frac{b^2}{L} \\
&= M - b + \frac{b^2}{2L}
\end{aligned}$$

The appropriate derivations for each of the remaining parameter cases and information conditions are omitted due to space considerations, but the results are recorded in Table IV.

Step 5: Eliminating dependence on other players

The results in Table IV give the total expected payoffs for player i conditioned on all parameters other than p_i. In the case of complete information, these results depend on known information about p_j for other players j. To facilitate a comparison of expected payoffs between complete and incomplete information, we seek to eliminate the dependence on p_j for the expert with complete information. We do this by taking an additional expected value over all the p_j. Because the p_j's only occur in two case conditions this is relatively straightforward and requires only one computation.

We get an expected payoff for complete information in the case $b \leq c$ by computing (the probability that we are in the sub-case $b \leq c$ and $\min_{j \neq i} p_j < \frac{b}{L}$ times the payoff for this case) + (the probability that we are in the sub-case $b \leq c$ and $\frac{b}{L} \leq \min_{j \neq i} p_j$ times the probability that we are in *this* case). We have:

$$\begin{aligned}
&\text{Probability}_{p_j : j \neq i}\left[\min_{j \neq i} p_j < \frac{b}{L}\right] \cdot \text{ExPayoff[that case]} \\
&+ \text{Probability}_{p_j : j \neq i}\left[\frac{b}{L} \leq \min_{j \neq i} p_j\right] \cdot \text{ExPayoff[that case]} \\
&= \left(1 - \left(1 - \frac{b}{L}\right)^{N-1}\right) \cdot \left[M - c + \frac{c^2}{2L}\right] \\
&+ \left(1 - \frac{b}{L}\right)^{N-1} \cdot \left[M - b + \frac{b^2}{2L}\right] \\
&= M - c + \frac{c^2}{2L} + \left(c - \frac{c^2}{2L}\right)\left(1 - \frac{b}{L}\right)^{N-1} \\
&- \left(b - \frac{b^2}{2L}\right)\left(1 - \frac{b}{L}\right)^{N-1} \\
&= M - c + \frac{c^2}{2L} + \left(c - b - \frac{c^2 - b^2}{2L}\right)\left(1 - \frac{b}{L}\right)^{N-1} \\
&= M - c + \frac{c^2}{2L} + (c - b)\left(1 - \frac{c+b}{2L}\right)\left(1 - \frac{b}{L}\right)^{N-1}
\end{aligned}$$

This gives us an expected payoff for the case $b \leq c$ under complete information conditions that we can directly

TABLE III

WEAKEST LINK SECURITY GAME: PROBABILITIES TO SELECT PROTECTION, SELF-INSURANCE OR PASSIVITY STRATEGIES

	Case	Information Type	Probability Passivity	Probability Self-Insurance	Probability Protection
WC1	$c < b$	Complete	$\frac{c}{L}$	$1 - \frac{c}{L}$	0
WC2a	$b \leq c$ and $\min_{j \neq i} p_j < \frac{b}{L}$	Complete	$\frac{c}{L}$	$1 - \frac{c}{L}$	0
WC2b	$b \leq c$ and $\frac{b}{L} \leq \min_{j \neq i} p_j$	Complete	$\frac{b}{L}$	0	$1 - \frac{b}{L}$
WI1	$c < b$	Incomplete	$\frac{c}{L}$	$1 - \frac{c}{L}$	0
WI2	$b \leq c \leq \frac{b}{\left(1-\frac{b}{L}\right)^{N-1}}$	Incomplete	$\frac{c}{L}$	$1 - \frac{c}{L}$	0
WI3	$\frac{b}{\left(1-\frac{b}{L}\right)^{N-1}} < c$ and $c < b + L\left(1 - \left(1 - \frac{b}{L}\right)^{N-1}\right)$	Incomplete	$\frac{b}{L\left(1-\frac{b}{L}\right)^{N-1}}$	$1 - \frac{c-b}{L\left(1-\left(1-\frac{b}{L}\right)^{N-1}\right)}$	$\frac{c-b}{L\left(1-(1-\frac{b}{L})^{N-1}\right)} - \frac{b}{L\left(1-\frac{b}{L}\right)^{N-1}}$
WI4	$\frac{b}{\left(1-\frac{b}{L}\right)^{N-1}} < c$ and $b + L\left(1 - \left(1 - \frac{b}{L}\right)^{N-1}\right) \leq c$	Incomplete	$\frac{b}{L\left(1-\frac{b}{L}\right)^{N-1}}$	0	$1 - \frac{b}{L\left(1-\frac{b}{L}\right)^{N-1}}$

TABLE IV

WEAKEST LINK SECURITY GAME: TOTAL EXPECTED GAME PAYOFFS, CONDITIONED ON OTHER PLAYERS

	Case	Information Type	Total Expected Payoff for player i (conditioned on other players)
WC1	$c < b$	Complete	$M - c + \frac{c^2}{2L}$
WC2a	$b \leq c$ and $\min_{j \neq i} p_j < \frac{b}{L}$	Complete	$M - c + \frac{c^2}{2L}$
WC2b	$b \leq c$ and $\frac{b}{L} \leq \min_{j \neq i} p_j$	Complete	$M - b + \frac{b^2}{2L}$
WI1	$c < b$	Incomplete	$M - c + \frac{c^2}{2L}$
WI2	$b \leq c \leq \frac{b}{\left(1-\frac{b}{L}\right)^{N-1}}$	Incomplete	$M - c + \frac{c^2}{2L}$
WI3	$\frac{b}{\left(1-\frac{b}{L}\right)^{N-1}} < c < b + L\left(1 - \left(1 - \frac{b}{L}\right)^{N-1}\right)$	Incomplete	$M - c + \frac{b^2}{2L\left(1-\frac{b}{L}\right)^{N-1}} + \frac{(c-b)^2}{2L\left(1-\left(1-\frac{b}{L}\right)^{N-1}\right)}$
WI4	$\frac{b}{\left(1-\frac{b}{L}\right)^{N-1}} < b + L\left(1 - \left(1 - \frac{b}{L}\right)^{N-1}\right) \leq c$	Incomplete	$M - b - \frac{L}{2}\left(1 - \left(1 - \frac{b}{L}\right)^{N-1}\right) + \frac{b^2}{2L\left(1-\frac{b}{L}\right)^{N-1}}$

compare with the cases for incomplete information. The final results for comparison are presented in Table V.

IV. RESULTS

In the previous section we derived total expected payoffs for the expert user under complete and incomplete information conditions. As some of these results contain as many as five variables the chief goal of this section is to provide the reader with a more meaningful and practically relevant interpretation. We highlight several important features from the tabulated results, and include several graphs to help identify important patterns.

Result 1: *The expert always receives the same or higher payoff with complete information compared to having incomplete information.*

Our graphs in Figure 2 give evidence of this result, and we could also derive it algebraically by comparing pairwise the expressions in Table V. For explanatory purposes, we offer a more subtle and more general argument involving the way we have modeled the information conditions. Fix values for all the information parameters $p_1, \ldots, p_n, b, c, L, M, N$. In the case of complete information, the expert selects an optimal strategy that maximizes her payoff given the values of these parameters. By the definition of a maximum, the strategy selected by the expert with incomplete information cannot result in a higher payoff (assuming the same fixed parameter values). The result we wish to show now follows from the fact that taking expected values preserves inequalities. I.e., the total expected payoff under incomplete information cannot exceed that of complete information.

Result 2: *When self-insurance cost are lower than protection expenses then defender strategies and payoffs are identical for both information conditions.*

When self-insurance is priced lower than protection, there is no cost incentive for the other players to choose protection. Hence, the additional knowledge about the naïve users' security risks does not give any advantage to the expert player, or change her security strategy.

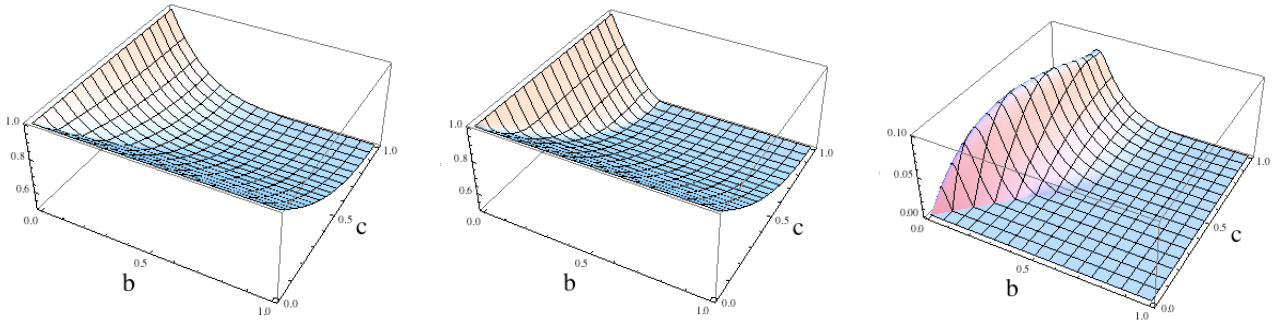
Result 3: *When protection is cheaper than self-insurance information matters.*

In order to quantify this statement, we require a definition. We define the **value of information** in the weakest-link security game to be the payoff difference between complete

TABLE V

WEAKEST LINK SECURITY GAME: TOTAL EXPECTED GAME PAYOFFS, NOT CONDITIONED ON OTHER PLAYERS

	Case	Information Type	Total Expected Payoff for player i (not conditioned on other players)
WC1	$c < b$	Complete	$M - c + \frac{c^2}{2L}$
WC2	$b \leq c$	Complete	$M - c + \frac{c^2}{2L} + (c-b)\left(1 - \frac{c+b}{2L}\right)\left(1 - \frac{b}{L}\right)^{N-1}$
WI1	$c < b$	Incomplete	$M - c + \frac{c^2}{2L}$
WI2	$b \leq c \leq \frac{b}{\left(1-\frac{b}{L}\right)^{N-1}}$	Incomplete	$M - c + \frac{c^2}{2L}$
WI3	$\frac{b}{\left(1-\frac{b}{L}\right)^{N-1}} < c < b + L\left(1 - \left(1 - \frac{b}{L}\right)^{N-1}\right)$	Incomplete	$M - c + \frac{b^2}{2L\left(1-\frac{b}{L}\right)^{N-1}} + \frac{(c-b)^2}{2L\left(1-\left(1-\frac{b}{L}\right)^{N-1}\right)}$
WI4	$\frac{b}{\left(1-\frac{b}{L}\right)^{N-1}} < b + L\left(1 - \left(1 - \frac{b}{L}\right)^{N-1}\right) \leq c$	Incomplete	$M - b - \frac{L}{2}\left(1 - \left(1 - \frac{b}{L}\right)^{N-1}\right) + \frac{b^2}{2L\left(1-\frac{b}{L}\right)^{N-1}}$
WN1	$c < b$	Naive	$M - c + \frac{c^2}{2L}$
WN2	$b \leq c$	Naive	$M - b + \frac{b^2}{2L} - \frac{L}{2}\left(1 - \frac{b^2}{L^2}\right)\left(1 - \left(1 - \frac{b}{L}\right)^{N-1}\right)$



(a) *Payoff under Complete Information* **(b)** *Payoff under Incomplete Information* **(c)** *The Difference*

Fig. 2. **Payoff Comparison of Complete and Incomplete Information Conditions:** with $L = M = 1$ and $N = 5$. (The first two plots show that under either information condition payoff is high when protection or self-insurance is cheap; and payoff is lower when protection and self-insurance are both expensive. The difference between information conditions is shown in the third graph. Observe the substantial change of scale. The difference between the payoffs is less than 10% of the best-case payoff, and less than 20% of the worst-case payoff.)

and incomplete information conditions, divided by the payoff under the incomplete information condition.

$$\frac{\text{Payoff[Complete]} - \text{Payoff[Incomplete]}}{\text{Payoff[Incomplete]}} \tag{9}$$

This ratio is 0 in cases where information does not matter, and it increases, potentially (though not actually) without bound, as information becomes more significant. With this definition in hand, we can give three additional results addressing the value of information. We first give an absolute upper bound on the value of information; secondly, we address how the value of information is affected by self-insurance and protection costs; and thirdly, we determine how the value of information holds up as the number of other players increases.

Result 4: *While information does matter, the value of information is bounded, and is in fact never overwhelmingly significant.*

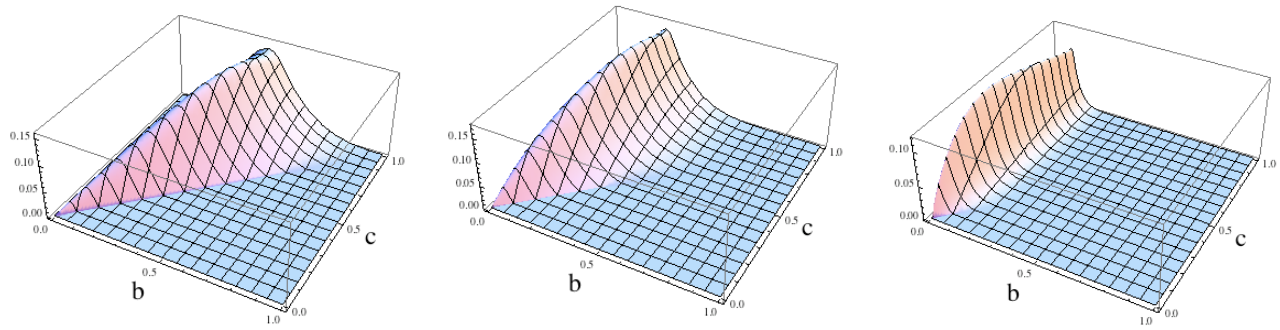
In particular, for all parameter settings, the value of information as we have defined it never exceeds 0.18; that is to say that the difference in payoff between complete and incomplete information is never more than 18% of the total expected payoff under incomplete information. Interestingly, the value of information reaches its highest point at a local maximum with $N = 4$ and a value of about 0.1787. We have not included the full range of plots or the algebraic reductions necessary to demonstrate this assertion, but as an example, Figure 3 plots the value of information as a function of b and c, with $L = M = 1$ fixed and for a range of N.

Result 5: *For the value of information to be noticeable, the costs of self-insurance and protection must be selected from a restrictive range of values. Furthermore, these restrictions become more severe as the number of players increases.*

For example, with an increase in the number of players, information has a significant value only when protection costs are very small. This feature is evidenced by the sequence of graphs in Figure 3.

Self-insurance and protection must be "well-priced", for security choices to be interesting and challenging. Conversely, if these costs are not "well-priced", then security choices are obvious without additional security-related information. This observation suggests that there may be value in restricting our attention to those values of protection and self-insurance costs that maximize the value of information. By doing so we can more easily see how the value of information depends on the potential losses and the number of players.

Result 6: *As long as protection and self-insurance costs are chosen to meet appropriate restrictions, the value of*



(a) $N = 2$ **(b)** $N = 5$ **(c)** $N = 25$

Fig. 3. **The Value of Information, as measured by the ratio:** $\frac{\text{Payoff[Complete]} - \text{Payoff[Incomplete]}}{\text{Payoff[Incomplete]}}$ with $L = M = 1$. (The three plots offer one measure of the value of information, in terms of protection costs b and self-insurance costs c. Observe the similarity to the case conditions in Figure 1. The value of information is always highest in the same case condition, case WI3, the case in which passivity, self-insurance, and protection are all viable options.)

information remains bounded away from zero, even with many players.

In particular, as the number of players increases, there remains a choice of self-insurance and protection costs such that the value of information is at least 0.1; or to say it another way, there always exist some self-insurance and protection costs such that an expert without relevant security information could expect to add 10% to her total expected payoff by gaining that information.

To illustrate this result, we fix $L = M = 1$ and consider the maximum, over all b, c with $0 \leq b, c \leq L$, of the *value of information* normally considered as a function of b, c, L, M, N. These restrictions give us a function in the single variable N. Figure 4 plots this function for N going from 2 to 200. As can be seen from the graph, the value of information approaches a constant (very close to 0.11) as N increases.

V. Concluding remarks

This paper extends the framework of our previous security model to accommodate limited information and bounded rationality. In conducting a comprehensive case analysis of this scenario, we have built a framework in which further extensions of our model can be more easily studied [20]. Our main computational achievement takes the form of expected payoffs for an expert user under two security information conditions. Comparing these expected payoffs is complicated because they involve functions of five parameters. To assist with interpretation, we offer a further graphical and numerical analysis to isolate key features in these payoffs and draw out practical implications. We also develop a concrete metric for measuring the value of information. The upshot is that information matters, to an extent. The overall significance of information compared to other factors may be limited, and there may only be an isolated set of costs for which complete information gives a significant advantage, but those costs always exist even in large networks.

VI. Future work

First, we are currently extending our analysis to different forms of security interdependencies. Following our own prior work [18], we are considering best-shot and total effort contribution functions [20].

Second, we intend to further explore the applicability of different metrics to measure the value of information. In particular, we interested in studying worst-case outcomes for difference, payoff-ratio, and cost-ratio metrics.

Third, we are developing a set of laboratory experiments to conduct user studies and attempt to measure the differences between perfectly rational behavior and actual strategies played [16]. Preliminary results are available for the weakest-link game with incomplete information [17].

Finally, we want to mention our interest in a more detailed exploration of the incentives of attackers. We have studied a simple scenario with an endogenously modeled strategic attacker [12]. However, we intend to conduct a more thorough analysis to study opportunities for attack deterrence and avoidance, and to better understand the interactions between competing self-interested malefactors [11].

VII. Acknowledgments

We thank Paul Laskowski, John Chuang, Nicolas Christin and the anonymous reviewers for their helpful comments to an earlier version of this paper. All remaining errors are our own. This work is supported in part by the National Science Foundation under ITR award ANI-0331659 (100x100). Jens Grossklags' work is also funded through a University of California MICRO project grant in collaboration with DoCoMo USA Labs.

References

[1] A. Acquisti and J. Grossklags. Privacy and rationality in individual decision making. *IEEE Security & Privacy*, 3(1):26–33, January–February 2005.

[2] T. August and T. Tunca. Network software security and user incentives. *Management Science*, 52(11):1703–1720, November 2006.

[3] D. Besnard and B. Arief. Computer security impaired by legitimate users. *Computers & Security*, 23(3):253–264, May 2004.

[4] M. Blaze. Protocol failure in the escrowed encryption standard. In *Proceedings of the 2nd ACM Conference on Computer and Communications Security (CCS)*, pages 59–67, Fairfax, VA, November 1994.

[5] K. Bryant and J. Campbell. User behaviours associated with password security and management. *Australasian Journal of Information Systems*, 14(1):36–63, November 2006.

[6] H. Cavusoglu, S. Raghunathan, and W. Yue. Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems*, 25(2):281–304, Fall 2008.

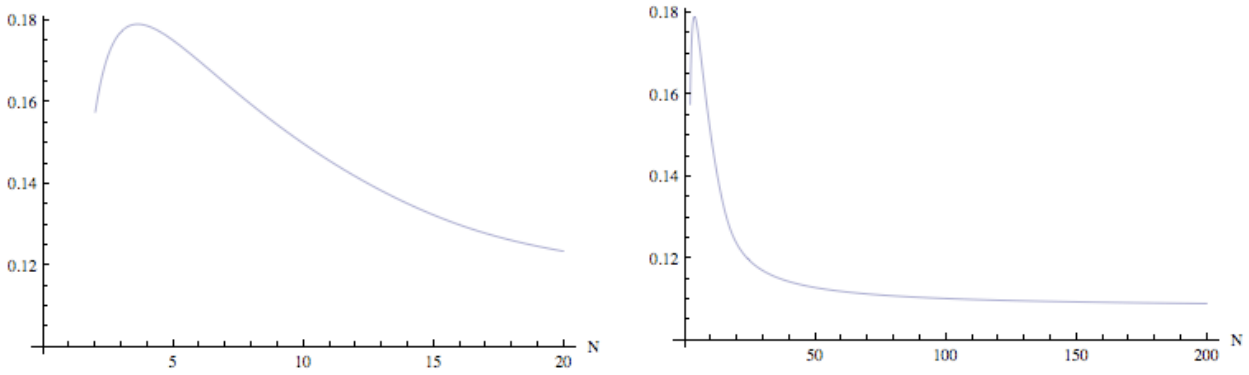


Fig. 4. **The Value of Information, as measured by the ratio: $\frac{\text{Payoff[Complete]} - \text{Payoff[Incomplete]}}{\text{Payoff[Incomplete]}}$, presented as a function of** N, with $L = M = 1$, and b, c selected to maximize the ratio. (The same function is shown using two different scales to illustrate both local and global features.)

[7] N. Christin, J. Grossklags, and J. Chuang. Near rationality and competitive equilibria in networked systems. In *Proceedings of ACM SIGCOMM'04 Workshop on Practice and Theory of Incentives in Networked Systems (PINS)*, pages 213–219, Portland, OR, August 2004.

[8] R. Cornes and T. Sandler. *The theory of externalities, public goods, and club goods*. Cambridge University Press, Cambridge, UK, 1986.

[9] D. Dörner. *The Logic Of Failure: Recognizing And Avoiding Error In Complex Situations*. Metropolitan Books, 1996.

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

[11] J. Franklin, V. Paxson, A. Perrig, and S. Savage. An inquiry into the nature and causes of the wealth of internet miscreants. In *Proceedings of 14th ACM Conference on Computer and Communications Security (CCS)*, pages 375–388, Alexandria, VA, October/November 2007.

[12] N. Fultz and J. Grossklags. Blue versus red: Towards a model of distributed security attacks. In *Proceedings of the 13th International Conference Financial Cryptography and Data Security (FC'09)*, Christ Church, Barbados, February 2009.

[13] D. Geer, C. Pfleeger, B. Schneier, J. Quarterman, P. Metzger, R. Bace, and P. Gutmann. Cyberinsecurity: The cost of monopoly. how the dominance of microsoft's products poses a risk to society, 2003. Available from Computer & Communications Industry Association at `http://www.ccianet.org/papers/cyberinsecurity.pdf`.

[14] L. Gordon and M. Loeb. *Managing Cyber-Security Resources: A Cost-Benefit Analysis*. McGraw-Hill, New York, NY, 2006.

[15] L.A. Gordon and M. Loeb. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4):438–4572, November 2002.

[16] J. Grossklags. Experimental economics and experimental computer science: A survey. In *Workshop on Experimental Computer Science (ExpCS'07), ACM Federated Computer Research Conference (FCRC)*, San Diego, CA, June 2007.

[17] J. Grossklags, N. Christin, and J. Chuang. Predicted and observed user behavior in the weakest-link security game. In *Proceedings of the 2008 USENIX Workshop on Usability, Psychology, and Security (UPSEC'08)*, San Francisco, CA, April 2008.

[18] J. Grossklags, N. Christin, and J. Chuang. Secure or insure? A game-theoretic analysis of information security games. In *Proceedings of the 2008 World Wide Web Conference (WWW08)*, pages 209–218, Beijing, China, April 2008.

[19] J. Grossklags, N. Christin, and J. Chuang. Security and insurance management in networks with heterogeneous agents. In *Proceedings of the 9th ACM Conference on Electronic Commerce (EC'08)*, pages 160–169, Chicago, IL, July 2008.

[20] J. Grossklags, B. Johnson, and N. Christin. When information improves information security. Technical report, UC Berkeley & Carnegie Mellon University, CyLab, February 2009. Available as CMU-CyLab-09-004 technical report at `http://www.cylab.cmu.edu/research/techreports/tr_cylab09004.html`.

[21] A. Halderman, S. Schoen, N. Heninger, W. Clarkson, W. Paul, J. Calandrino, A. Feldman, J. Appelbaum, and E. Felten. Lest we remember: Cold boot attacks on encryption keys. In *Proceedings of the 17th USENIX Security Symposium*, pages 45–60, San Jose, CA, August 2008.

[22] J. Hirshleifer. From weakest-link to best-shot: the voluntary provision of public goods. *Public Choice*, 41(3):371–386, January 1983.

[23] C. Jaeger, O. Renn, E. Rosa, and T. Webler. *Risk, uncertainty, and rational action*. Earthscan Publications, London, UK, 2001.

[24] Kabooza. Global backup survey: About backup habits, risk factors, worries and data loss of home PCs, January 2009. Available at: `http://www.kabooza.com/globalsurvey.html`.

[25] D. Kahneman and A. Tversky. *Choices, values and frames*. Cambridge University Press, Cambridge, UK, 2000.

[26] O. Kerr. The fourth amendment in cyberspace: Can encryption create a reasonable expectation of privacy? *Connecticut Law Review*, 33(2):503–533, Winter 2001.

[27] H. Kunreuther and G. Heal. Interdependent security. *Journal of Risk and Uncertainty*, 26(2–3):231–249, March 2003.

[28] K. Mitnick and W. Simon. *The Art of Deception: Controlling the Human Element of Security*. Wiley Publishing, Indianapolis, IN, 2002.

[29] T. Moscibroda, S. Schmid, and R. Wattenhofer. When selfish meets evil: Byzantine players in a virus inoculation game. In *Proceedings of the 25th Annual Symposium on Principles of Distributed Computing (PODC 2006)*, pages 35–44, Denver, CO, July 2006.

[30] NCSA/Symantec. Home user study, October 2008. Available at: `http://staysafeonline.org/`.

[31] M. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, and A. Moore. Insider threat study: Illicit cyber activity in the banking and finance sector. Technical report, CERT Coordination Center, Software Engineering Institute, June 2005. Technical report No. CMU/SEI-2004-TR-021. Available at `http://www.sei.cmu.edu/pub/documents/04.reports/pdf/04tr021.pdf`.

[32] B. Schneier. *Beyond Fear*. Springer Verlag, New York, NY, 2006.

[33] J. Stanton, K. Stam, P. Mastrangelo, and J. Jolton. Analysis of end user security behaviors. *Computers & Security*, 2(24):124–133, March 2005.

[34] H.R. Varian. System reliability and free riding. In L.J. Camp and S. Lewis, editors, *Economics of Information Security (Advances in Information Security, Volume 12)*, pages 1–15. Kluwer Academic Publishers, Dordrecht, The Netherlands, 2004.

[35] M. Zviran and W. Haga. Password security: An empirical study. *Journal of Management Information Systems*, 15(4):161–186, Spring 1999.