Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies

By
Marco Cremonini
and
Dmitri Nizovstev*

WASHBURN UNIVERSITY
SCHOOL OF BUSINESS
WORKING PAPER SERIES
Number 68

April 2006

Washburn University
School of Business
1700 SW College Ave.
Topeka, KS 66621
785-670-1308
www.washburn.edu/sobu

*Marco Cremonini is assistant professor of information systems at the University of Milan, Italy. Dmitri Nizovtsev is assistant professor of economics at the School of Business at Washburn University, Topeka, Kansas. Comments should be directed to Dmitri Nizovtsev, School of Business, Washburn University, 1700 SW College Ave. Topeka, Kansas 66621, 785-670-1599, dmitri.nizovtsev@washburn.edu.

Understanding and Influencing Attackers' Decisions: Implications for Security Investment Strategies

Marco Cremonini
Dept. of Information Technology
University of Milan, Italy
cremonini@dti.unimi.it

Dmitri Nizovtsev
School of Business
Washburn University, USA
dmitri.nizovtsev@washburn.edu

Abstract
We consider a model of economic behavior of attackers for the case when they are able to obtain complete information about the security characteristics of each target and the case when such information is unavailable. We find that if attackers are able to distinguish targets by their security characteristics and switch between multiple alternative targets, then the direct effect of security measures, represented by the strengthened technical protection of networked assets, is complemented by a behavioral effect resulting from more effort being put into attacks on systems with low security level than on systems with high security level. Ignoring that effect would result in underinvestment in security or misallocation of security resources. We also find that systems with better levels of protection have stronger incentives to reveal their security characteristics to attackers whereas poorly protected systems prefer to hide their characteristics. Those results have important implications for security practices and policy issues.

1. Introduction

The importance of developing quantitative models of computer security has been widely recognized in research fields such as economics (Gordon&Loeb, 2005) and computer science (Schechter, 2004, Liu&Zang, 2005). More specifically, quantitative techniques for evaluating attackers' behavior have been fruitfully applied in the area of dependable computing (Avizienis et al., 2000, Nicol et al., 2004). The reason is that dependability researches traditionally shifted their focus from analyzing static design properties and development processes of systems to analyzing the interaction with the operational environment (Littlewood et al., 1993, Avizienis et al., 2004). From the security perspective, one of the main components of the operational environment is the behavior of attackers. Several models of attackers' behavior have been proposed (Jonsson&Olovsson, 1997, Ortalo et al., 1999, McDermott, 2005).

The importance of developing quantitative models of computer security has been widely recognized in economics (Gordon&Loeb, 2005) and computer science (Schechter, 2004, Liu&Zang, 2005). Researchers in the field of dependable computing have also shifted their focus from analyzing static design properties and development processes of systems to analyzing the interaction with the operational environment, which includes security requirements as well (Littlewood et al., 1993, Avizienis et al., 2004). From the security perspective, one of the main components of the operational environment is the behavior of attackers. Quantitative techniques for evaluating attackers' behavior have been fruitfully applied (Avizienis et al., 2000, Nicol et al., 2004) and several models of attackers' behavior have been proposed (Jonsson&Olovsson, 1997, Ortalo et al., 1999, McDermott, 2005). However, attacker's behavior in the aforementioned works is modeled as exogenous (as a probabilistic distribution of intrusion occurrences or such statistics as the average time between breaches). No clear assumptions have been made about the principles attacker's behavior is based on.

Contrary to the aforementioned approach that treats attackers' behavior as exogenous, we consider the case in which attackers are assumed to behave economically (that is, choose their actions optimally based on comparison of their costs to benefits). That view of attackers as rational agents is not entirely new and is consistent with several theoretical and empirical studies. Some prior work has recognized that attackers act strategically either by rationally selecting their targets or in response to targets' actions (Jajodia&Miller, 1993; NIST, 2002). Leeson and Coyne (2006) make a distinction between fame-driven and profit-driven attackers,[1] with the former attracted by the possible notoriety and the latter focused on gaining monetary rewards, and conclude that the two groups must be analyzed separately. In the past the stereotypical view of an attacker was mainly that of a fame-driven individual (Denning, 1990). Even more recently the "15 minutes of fame" was claimed to be one of the biggest motivation for attackers (Curry, 2002). However, while fame-driven attackers are certainly still numerous, ample evidence exists that economically-minded attackers are posing a much more serious threat to corporate information security. For instance, a pronounced shift toward financially motivated intrusions (Sieberg, 2005) and, as a result, an increase in the average losses caused by unauthorized access to information and theft of proprietary information (Gordon et. al., 2005) have been recently witnessed.

The novelty of our work is in developing an analytical model of the behavior of an attacker that rationally chooses his course of action based on cost-benefit analysis. Such analysis involves considerations of the expected reward and the cost of achieving it, which includes the opportunity cost of staying at a given target. The last factor, represented by the alternatives to the current target, has often been overlooked in analyses of attacker behaviors and defense strategies. Our work specifically focuses on modeling the way in which the behavior of an economically-minded attacker can be influenced by security measures implemented at potential targets and the ways in which such an interaction may affect the choice of security practices.

Our results show that the presence of alternative targets plays an extremely important role in attackers' decisions. Regarding investments in security technology, our model shows that results of analysis that takes the attacker's alternative opportunities into account can be considerably different from results obtained with such common decision theory techniques as the Annual Loss Expectancy (ALE)

[1] We prefer the expression "economic behavior" to "profit-driven" as the more accurate and less restrictive one.

approach (Soo Hoo, 2000) that do not take into account the strategic nature of the problem. We then use our findings to discuss various approaches to investments in security technology and make recommendations regarding security practices of individual firms as well as policy recommendations.

Our results suggest that traditional non-strategic approaches that continue to be widely used in current information security practices can severely underestimate positive effects of security investments, therefore leading to underinvestment in information security or misallocation of resources. The comparison of results from two alternative specifications of our model suggests that lack of information attackers have about the security characteristics of each potential target benefits systems with low security level, hurts system with high security level, and reduces the incentives for individual firms to invest in security.

2. Related Work

Our research belongs to the field of economics of information security. Of all the issues within that broadly defined area, we are focusing on what economic research has to say about the best strategies for investing in security technologies. The advantage of the economic approach over the more traditional ones is that it recognizes and accounts for the presence of a strategic interaction between different parties involved in a particular issue.

The literature combining economic approach with information technology issues is vast. Clemons (1991) discusses the reasons why businesses have difficulty evaluating when to use information technology. In particular, relevant for our research is his observation that some investments should be made to limit the possibility of future losses, which is the case of security technology investments, rather than to obtain long-term additional value. When companies face relevant environmental changes, again one common scenario for information security, needed investments in information technology may be diverted if such changes are not foreseen, the effect which Clemons called the "trap of the vanishing status quo".

A lot of work has been done since then. Unfortunately, despite the number of works making a case for wider use of economic approach to information security (Anderson, 2001, Gordon and Loeb, 2002a, Gordon et al., 2003, Rodewald, 2005, Schechter, 2005), little attention has been paid to those findings by security practitioners, and more traditional approaches that often overlook important aspects of information security continue to prevail. One of many examples in that regard is Gordon and Richardson (2004) which provides a comparative analysis of two traditional investment evaluation techniques, Return on Investment (ROI) and Net Present Value (NPV). They show that in spite of the better applicability of NPV to computer security relative to ROI, ROI is still by far the most popular metric used, as documented by the 2005CSI/FBI Computer Crime and Security Survey (Gordon et al., 2005). That point is similar to one we make in our work, where we show how traditional investment evaluation techniques can greatly underestimate the effectiveness of a security solution by not considering the strategic nature of the problem and the interdependency between attackers' and defenders' actions.

Among other attempts to develop better techniques for evaluation investment in security, Geer (2005) introduces an alternative to traditional ROI formula suggesting to perform a cost-effective analysis, rather than a cost-benefit analysis, when costs and benefits are not commensurate. Purser (2005) proposes a modification to the ROI approach that would assign a monetary value to an increase or decrease in the risk resulting from an investment. According to that approach, a risk increase results in a lower ROI and vice versa. While the idea of considering a secondary effect of security investments resulting from a modified operational environment is similar to the one explored in our paper, our approach, based on game theory, is better suited to model such an interdependent behavior.

Other work in the game theory field that is related to ours includes Cavusoglu and Raghunathan (2004), which compares decision theory and game theory approaches in the context of the configuration of detection software. Although the subject of their paper is different from ours, the approach they follow is close to what we have done in terms of contrasting the results obtained by each of the two approaches. Cavusoglu et al. (2004) and Cavusoglu et al. (2005) also propose game-theoretic models for evaluating security investments. However, their work focuses on specific security technologies, whereas we consider the more general problem of evaluating investments in computer security solutions.

Since the main purpose of investing in security is to defend against malicious attackers, acquiring proper understanding of attackers' behavior is a necessary step towards best security practices. Jonsson and Olovsson (1997) contributed to such understanding by performing an empirical study of attackers' behavior in a laboratory environment. While their work is descriptive in nature, we are able to use some aspects of their analysis as a starting point in setting up our model. In particular, they provide empirical evidence of several distinctive phases of an attack and hypothesize the presence of "behavioral" and "preventive" effects of security measures, which is supported by our analysis.

Bier et al. (2005) is perhaps the closest to our work. It models the behavior of a defender that must allocate defensive resources to a collection of locations and the behavior of an attacker that must choose a location to attack. Key to their approach is to recognize that a defender can influence the attacker's choice of a target by selecting which resources to protect better and which let be an easier target. Such strategic decision is the ground for the defender's policy. While the starting premise of our analysis is very similar, the context of our problem is different. Besides, our model analyzes the case of multiple attacks and the endogenous choice of effort put into each attack. We also vary the informational structure of the model, which allows us to discuss the benefit of complete information about the security level of the defended system.

Enders and Sandler (2004) discuss the strategic interaction between defenders and attackers in the context of anti-terrorism policies. They identify two separate mechanisms, the income effect and the substitution effect, through which a defensive measure may mitigate a specific security threat. While their approach is conceptually similar to ours, our results are more directly applicable to information security.

Other works directly related to the issues we are interested in include Kuhnreuther and Heal (2003) and Kearns and Ortiz (2004), which introduce the concept of an interdependent security game and show that the ultimate safety of each participant may depend in a complex way on the actions of the entire population. Although in the present work we have used some elements of interdependent security models by discussing the effect of a security measure on the strategic behavior of attackers, we plan to extend our work in that direction.

3. The model

The model consists of a certain number of systems that serve as targets for malicious attacks and an unspecified number of attackers all of whom are identical. An attacker targets one system at a time and puts a certain amount of effort, x, into attacks.

The cost, C, of attacks consists of two parts. One component, represented by the opportunity cost of effort, is assumed to be a linear function of x.[2] The second component is target specific. The more effort an attacker spends on one target, the more evidence he leaves behind and the higher are the chances he will be detected, which we assume to be costly for him (because of a potential punishment or for some other reasons). Therefore the marginal cost of effort is increasing in the amount of effort spent on a given target, $\frac{\partial C(x)}{\partial x} > 0$, $\frac{\partial^2 C(x)}{\partial x^2} > 0$.

If successful, an attack results in an intrusion. The expected benefit from an attack is $E(B(x)) = \pi(x) \cdot G$, where $\pi(x)$ is the probability of success given the amount of effort put into attacking a given target and G is the one-time payoff the attacker receives in the case of a successful intrusion. The size of that payoff is assumed to be the same for all targets.

Attackers are maximizing their expected net payoff from attacks. They do so by deciding how much effort to spend on each target. The rule for optimally choosing the amount of that effort, further referred to as the optimal stopping rule, can be expressed in at least two alternative ways. It is in an attacker's best interest to stop attack attempts when the expected net benefit of his continued effort is no longer positive,

[2] Following the approach of Jonsson and Olovsson (1997), we make no distinction between effort and time. Thus the intensity of effort, or how much effort is exerted in a unit of time, in our model is assumed to be exogenous and constant. A more complex setup is saved for later work.

$ENB(x) \le 0$, or when the marginal benefit of effort no longer exceeds its marginal cost, $MB \le MC$. Naturally, both decisions are equivalent.[3]

If we denote $\hat{x}$ the amount of effort that solves $MB = MC$, then the attacker's expected net payoff after he expended x units of effort but achieved no success is

$$ENB(x) = \int_x^{\hat{x}} \rho(\tau)(G - C(\tau) + C(x))d\tau - (1 - \pi(\hat{x} - x))(C(\hat{x}) - C(x)), \tag{1}$$

where $\pi(\hat{x}) = \int_0^{\hat{x}} \rho(\tau)d\tau$ and $1 - \pi(\hat{x}) = \int_{\hat{x}}^{\infty} \rho(\tau)d\tau$.

Here, $\rho(x)$ denotes the conditional probability distribution function given no success upon spending effort x.

We start our analysis by choosing specific functional forms for benefit and cost. The marginal cost of effort is assumed to be given by $MC = \alpha_0 + \alpha_1 x_i$. Following the approach commonly used in the literature (Littlewood et al, 1993, Jonsson&Olovsson, 1997, Cavusoglu&Raghunathan, 2004), we model the amount of effort that needs to be spent before an attack results in an intrusion as an exponential random variable with rate parameter λ. The probability of success of each attack is therefore a function of effort given by $\pi(x) = 1 - e^{-\lambda x}$. We find it more convenient to characterize the aforementioned exponential distribution by the scale parameter $\mu = \lambda^{-1}$. Since $\frac{d\pi}{d\mu} < 0$, one can think of μ as the security level of the system subject to attacks, with greater values of μ corresponding to better protected systems.

Due to the memorylessness property of the exponential distribution, $\rho(x)$ in the expressions above equals $1/\mu$ for any x.

3.1 Scenario 1 – One target

We start with the simplest case in which there is only one specific target the attacker is interested in. Its security level, λ, is common knowledge. The attacker's expected net benefit from attacking that target is

$$ENB(x) = G - \mu\alpha_0 - \mu\alpha_1 x - \mu^2\alpha_1(1 - e^{x/\mu}e^{-(G/\mu - \alpha_0)/\mu\alpha_1}) \text{ for any } x \ge 0. \tag{2}$$

It is easy to show that $ENB(x) = 0$ is solved by $\hat{x} = \dfrac{G - \mu\alpha_0}{\mu\alpha_1}$. Thus, we have the following proposition:

[3] The literature on optimal search (Cozzolino, 1972) confirms that fact.

Proposition 1. The amount of effort an attacker optimally puts into breaching a system, $\hat{x}$, increases in the size of the payoff he receives in the case of intrusion, ($\frac{\partial \hat{x}}{\partial G} > 0$), decreases in the target's security level ($\frac{\partial \hat{x}}{\partial \mu} < 0$), and decreases in the cost of performing an attack ($\frac{\partial \hat{x}}{\partial \alpha_0} < 0$, $\frac{\partial \hat{x}}{\partial \alpha_1} < 0$).

Here is a numerical example to help illustrate attacker's decisions in this case:

Let G=1000, $\mu = 50$, so that $\pi(x) = 1 - e^{-0.02x}$, and $\alpha_0 = 10, \alpha_1 = 2$.

From either $ENB(x) = 0$ or $MB = MC$, $\hat{x} = \dfrac{G - \mu\alpha_0}{\mu\alpha_1} = 5$.

The following graphs may clarify the decision making process and the equivalence of the two approaches to solving the optimal stopping problem. Figure 1 is trivial and shows the marginal benefit and marginal cost of effort. Clearly, stopping at $\hat{x} = 5$ is in the attacker's best interest.

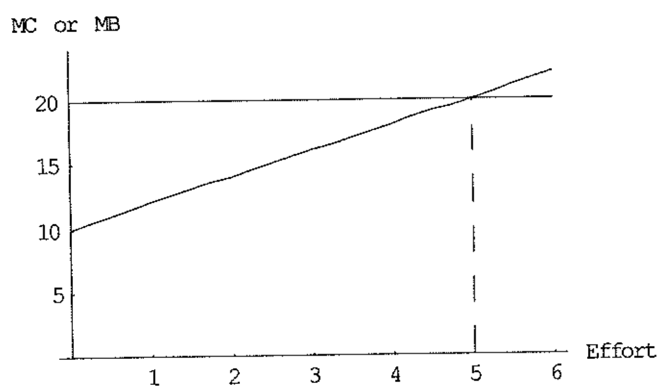

Figure 1. Marginal cost and marginal benefit of attacker's effort.

Figure 2 shows the overall expected net benefit that can be received from attacking the target as a function of effort that will be put in (as viewed before the start of attack attempts). Given the knowledge about the target's security parameter, μ, the attacker knows that the maximum value of the total expected net benefit is going to reach its maximum at $\hat{x} = 5$ ($ENB(\hat{x}) = 24.19$) and decrease afterwards. In other words, the attacker can make an advance commitment to putting in 5 units of effort (or less if he happens to succeed sooner).

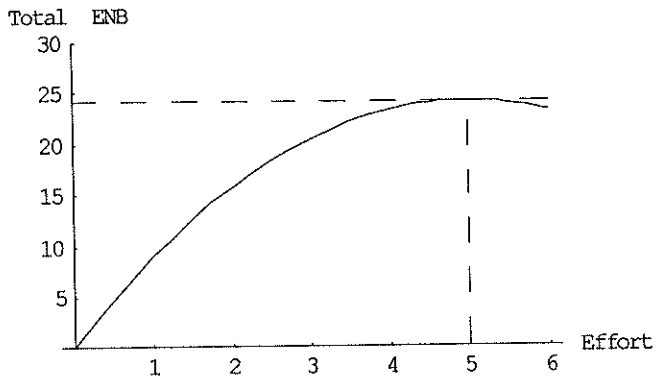

Figure 2. Expected net benefit from attacks as a function from future effort spent, as viewed before attacks start.

Still another way to present the stopping decision is through the remaining expected net benefit from attacks after some effort has been already spent. See Figure 3. Naturally, the more effort has been spent already, the greater is the marginal cost of effort and the smaller is the net benefit the attacker still expects to derive from future effort. In this version of the model the attacker keeps trying until $ENB(x) = 0$. We find this representation the most insightful of the three and will utilize it in the analysis of more advanced versions of the model.

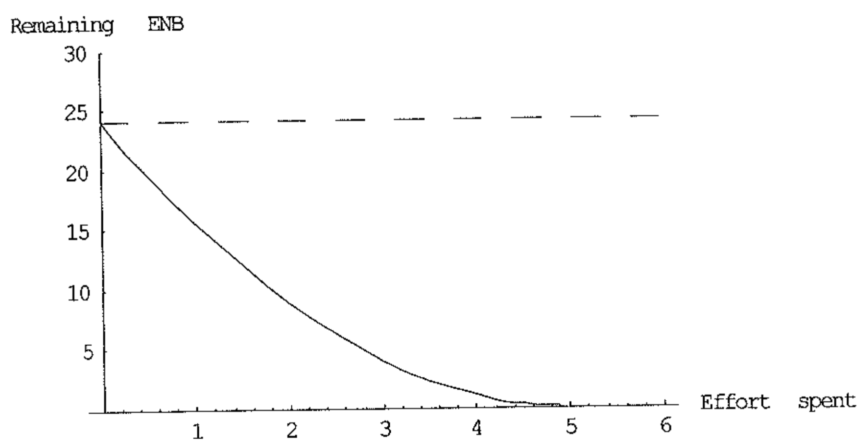

Figure 3. Expected net benefit of future effort as a function of effort spent.

3.2 Scenario 2 – Multiple identical targets

There are N systems (potential targets) with the same security level, μ, which is common knowledge. Attackers are now able to switch from one target to another. Switching to a different target involves some cost, which we interpret as the cost of effort put into the "learning phase" of an attack [4] in the context of the aforementioned Jonsson and Olovsson (1997).The size of the switching cost, C_S, is assumed to be the same for each target.

One major difference between this setup and the one discussed above is that there is now an outside opportunity present that has a certain value to an attacker. Therefore the attacker will make the decision to stop attacking one target and switch to another, randomly picked, target once his remaining expected net benefit from the current target gets smaller than the net benefit he expects to get if he switches. The optimal stopping rule for this case is therefore

$$ENB(x) = ENB(0) - C_S. \tag{3}$$

Proposition 2. The maximum amount of effort an attacker puts into attacking a target increases in the size of the switching cost, C_S. ($\frac{\partial \hat{x}}{\partial C_S} > 0$).

For $C_S = 5$ and the parameter values used above, (2) is solved by $\hat{x} = 0.5548$. See Figure 4 below.

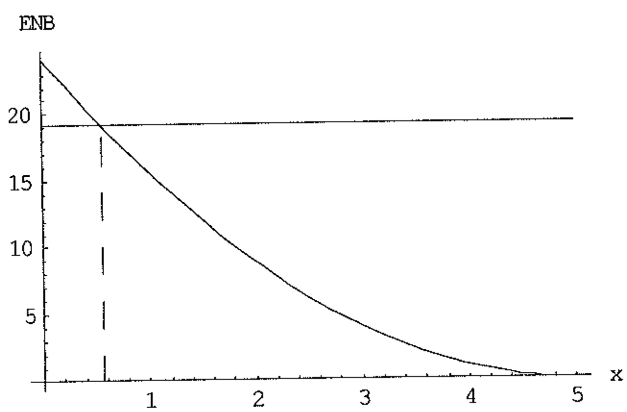

Figure 4. Optimal stopping decision in the presence of multiple targets and switching cost.

The downward sloping line on the graph above shows the expected net benefit from continuing attacks on the present target, $ENB(x)$. As discussed above, it decreases in the amount of effort already spent, $\frac{\partial ENB(x)}{\partial x} < 0$. The horizontal line represents $ENB(0) - C_S$. Once $ENB(x) \le ENB(0) - C_S$, the attacker is better off paying the one-time switching cost, C_S and switching to a different target.

[4] For example we may think of usual reconnaissance operations performed to gather information on potential targets like port scanning, OS and application fingerprinting, and so forth.

Note that if $C_S = 0$, then $\hat{x} = 0$ trivially. Therefore in the absence of switching costs and presence of multiple identical targets attackers would be switching all the time.

The analysis done insofar did not discuss decisions made by defenders. Those decisions are endogenized in the next modification of the model.

3.3 Scenario 3 – Heterogeneous targets

There are (H+L) systems (targets) present, H of which have a high security level and L have a low security level. We will further refer to such targets as being of *H-type* or *L-type*, respectively, where $\lambda_H < \lambda_L$. The type a target belongs to becomes known to attackers with certainty after the reconnaissance stage (hence upon paying the switching cost, C_S).

The expected net benefit received from a target of a known type is a modification of (2) obtained earlier:

$$ENB_i(x) = G - \mu_i\alpha_0 - \mu_i\alpha_1 x - \mu_i{}^2\alpha_1(1 - e^{x/\mu_i} e^{-(G/\mu_i - \alpha_0)/\mu_i\alpha_1}) \text{ for any } x \geq 0. \tag{4}$$

where $i = H, L$. Switching to a different, randomly chosen target involves cost C_S and gives the attacker an expected net benefit

$$\begin{aligned} &ENB_{random} = \eta ENB_H(0) + (1-\eta)ENB_L(0) = \\ &G - \eta\mu_H\alpha_0 - \eta\mu_H^2\alpha_1(1 - e^{-(G/\mu_H - \alpha_0)/\mu_H\alpha_1}) - (1-\eta)\mu_L\alpha_0 - (1-\eta)\mu_L^2\alpha_1(1 - e^{-(G/\mu_l - \alpha_0)/\mu_l\alpha_1}), \end{aligned} \tag{5}$$

where $\eta = \dfrac{H}{H+L}$ is the proportion of H-type systems in the population.

Applying the optimal stopping rule to this version of the model suggests that the attacker should continue putting effort into one target as long as $ENB_{random}(0) - ENB_i(x) \leq C_S$ and switch to a different randomly chosen target when $ENB_{random}(0) - ENB_i(x) \geq C_S$, where $i = H, L$ is the type of his present target. Thus, the effort after which it is optimal to switch/change targets is given by the solution to

$$ENB_{random}(0) - ENB_i(x) = C_S. \tag{6}$$

No explicit solution for (6) exists. However, using differentiating an implicit function we are able to get the result stated in the following proposition.

Proposition 3. Given the presence of targets of different security types and attackers' ability to determine the target type, the amount of effort optimally put by an attacker into a target decreases in its security level μ, $\dfrac{d\hat{x}}{d\mu} < 0$.

This important fact drives many results of our paper and has important implications for security practices. It suggests that every security solution affects the state of security through two distinct mechanisms. One is what we call the *direct* or *technical effect*, represented by the increased ability of a system to withstand intrusion attempts given the intensity of those attempts. The direct effect is commonly recognized by security practitioners. It can be shown that, when the probability of attack success is small, the direct effect is approximately proportional to the increase in the security parameter μ:

$$\frac{\partial \pi}{\partial \mu} \cdot \frac{\mu}{\pi} = \frac{x e^{-x/\mu}}{\mu(1-e^{-x/\mu})} \approx 1.$$

Thus, according to the direct effect, a 10% increase in security level results in an approximately 10% reduction in the probability that each attack will result in a successful intrusion.

There is, however, another effect as well, which we call *indirect* or *behavioral effect*. Ceteris paribus, a more secure system is less appealing to attackers than a less secure one. Thus, a security enhancement performed at one system diverts attackers' effort away from it, and, since $\pi(\mu, x) = 1 - e^{-x/\mu}$, less effort on attackers' part translates into a lower probability of a security incident.

This fact deserves to be summarized in another proposition.

Proposition 4. Given the heterogeneity of target types and the presence of economizing attackers able to determine a target's type, any security improvement causes more than proportional reduction in the probability of success of each individual attack.

The result in Proposition 4 can be confirmed by differentiation by the chain rule:

$$\frac{d\pi}{d\lambda} = \underset{(+)}{\frac{\partial \pi}{\partial \lambda}} + \underset{(+)}{\frac{\partial \pi}{\partial \hat{x}}} \, \underset{(+)}{\frac{\partial \hat{x}}{\partial \lambda}} > \frac{\partial \pi}{\partial \lambda} > 0 \qquad (7)$$

While the probability with which an individual attack results in an intrusion is qualitatively important, it is not directly observed by defenders. Instead, defenders are primarily concerned with the frequency with which security incidents ("intrusions" according to our terminology) occur. Moreover, the loss incurred by defenders per unit of time (Annual Loss Estimate, ALE, is one example) is directly related to the number of security incidents per unit of time. Therefore we chose to discuss security enhancement solutions in the context of their effect on the frequency of intrusions.

The frequency of intrusions is the product of the probability that an attack results in an intrusion, $\pi_i(x_i) = 1 - e^{-\hat{x}_i/\mu_i}$, and the rate of attackers' arrival at a target. The arrival rate is the same across targets. It is proportional to the overall number of attackers, N_A, and inversely proportional to the number of potential targets, N_T and the average length of an attacker's stay on each target, τ . To determine τ , one needs to realize that an attacker leaves one target and starts looking for another if he either has successfully breached the system or feels the current target is no longer worth his continued effort. Once we know the solution to the optimal stopping condition for each type of system, $\hat{x}_i$, $i = H, L$, we can determine the average, or "expected", length of stay of an attacker at a system:

$$\tau_i = \int_0^{\hat{x}_i} x f(x) dx + \hat{x}_i e^{-\hat{x}_i/\mu_i} = \mu(1 - e^{-\hat{x}_i/\mu_i}). \tag{8}$$

Keep in mind that if switching cost is interpreted as the opportunity cost of the reconnaissance effort, then it has to be included in the calculation of the length of stay as τ_S . A sufficiently close approximation for it is $\tau_S = C_S / \alpha_0$. Thus, an attacker spends an average of $(\tau_S + \tau_H)$ units of effort on an H-type system and $(\tau_S + \tau_L)$ units of effort on an L-type system. Since effort in our model is equivalent to time, attackers return to the pool and start probing another target at $\tau = (\tau_S + \eta\tau_H + (1-\eta)\tau_L)$ intervals. Finally, the frequency of intrusions equals

$$v_i = \frac{N_A \cdot \pi(\mu_i, \hat{x}_i)}{N_T(\tau_S + \eta\tau_H + (1-\eta)\tau_L)} = \frac{N_A(1 - e^{-\hat{x}_i/\mu_i})}{N_T\left(\tau_S + \eta\mu_H(1 - e^{-\hat{x}_H/\mu_H}) + (1-\eta)\mu_L(1 - e^{-\hat{x}_L/\mu_L})\right)}, \tag{9}$$

where $i = H, L$.

We are now able to state the effect of a security enhancing solution on the frequency of intrusions and therefore on the annual loss expectancy.

Proposition 5. Given the heterogeneity of target types and presence of economizing attackers who are able to determine a target's type, any security enhancement causes more than proportional reduction in the frequency of security incidents and in the expected annual loss from attacks (ALE). The extent of that reduction, $\xi = \left| \frac{v_L - v_H}{\mu_H - \mu_L} \right|$, *is inversely related to the size of the switching cost,* $\frac{d\xi}{dC_S} < 0$.

The specifics of the indirect, or behavioral effect may become clearer from the numerical simulation results. For simulations, we use the same parameters as before, $G = 1000$, $\alpha_0 = 10, \alpha_1 = 2$, $C_S = 5$. The security parameters of the two target types are $\mu_H = 55$ and $\mu_L = 50$. There is an equal proportion of systems of each type, $\eta = 0.5$. The number of attackers and the total number of targets are both normalized to 1.

Initially, an L-type defender with $\mu_L = 50$ suffers intrusions with frequency $\nu_L = 0.0197$. They result from attackers arriving at his system at the rate of 0.916 per unit of time, staying no more than $\hat{x}_L = 1.089$, and each attack leads to a success with probability $\pi_L = 0.0215$.

Next, a security enhancement is considered that would change the system security parameter to $\mu_H = 55$. If the rate of attackers' arrival and individual attacker's effort were assumed to remain the same, then it would be reasonable to expect the frequency of breaches to decrease to $\nu_{H/L} = 0.0178$. In reality, however, due to the amount of effort being substantially reduced (from $\hat{x}_L = 1.089$ to $\hat{x}_H = 0.094$), the frequency of intrusions also sees a significant drop to $\nu_H = 0.0017$.

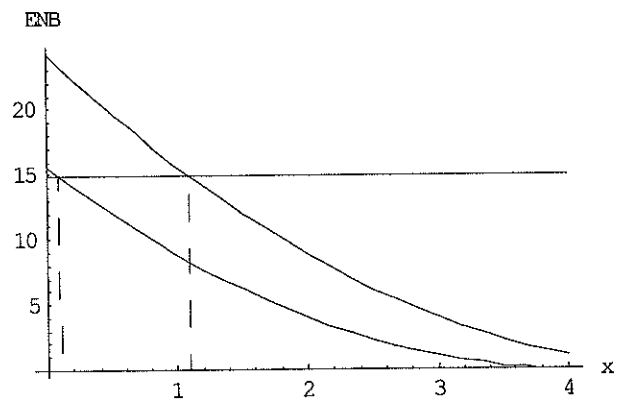

Figure 5. Difference in the optimal attacker's effort across target types.

Naturally, the outcome of a security enhancing measure depends on the distribution of target types and the size of the switching cost. Both effects are illustrated by the diagrams below.

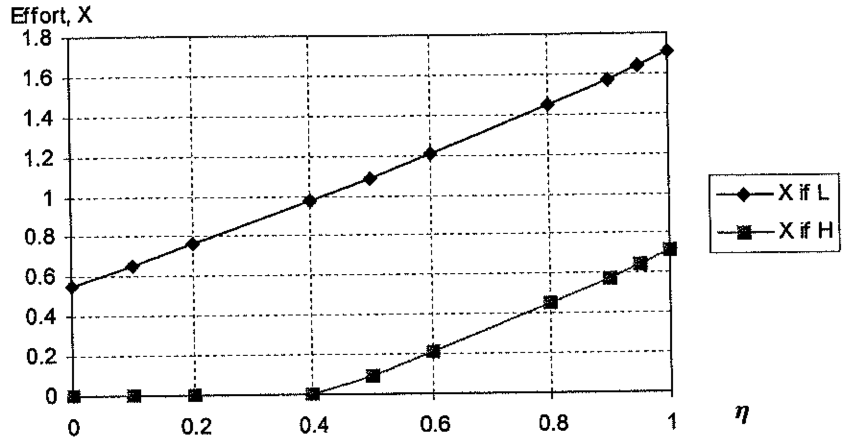

Figure 6. Optimal attacker's effort as a function of the type of the system and the composition of the population. Parameter η denotes the proportion of H-type systems.

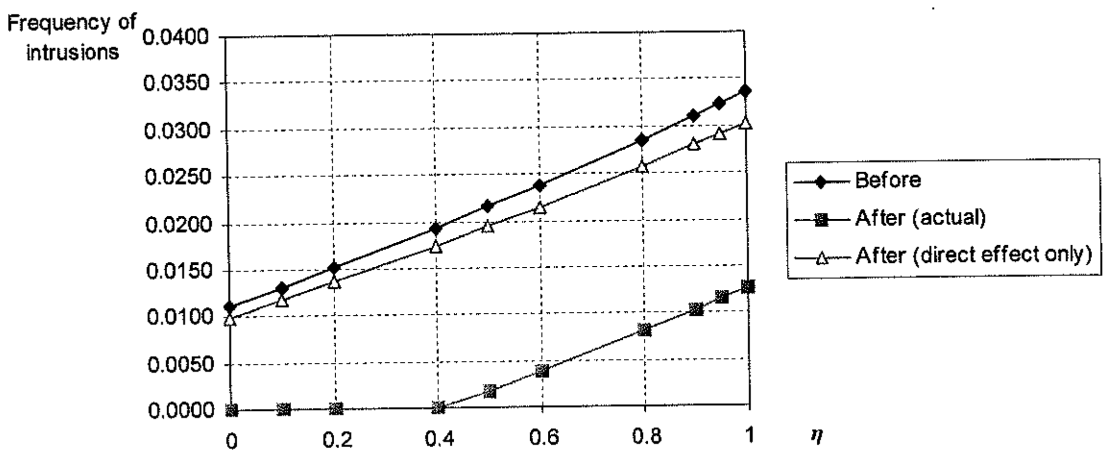

Figure 7. Direct only and overall effects of a security enhancement on the frequency of breaches, plotted against the proportion of H-type systems. The top curve, "Before", represents an L-type system before security enhancement. The middle one, "After (direct effect only)", shows the expected effect of upgrading to H-type, taking only the direct effect into account. The bottom line, "After (actual)", shows the frequency of intrusions that will actually occur as a result of an upgrade. It includes both the direct and the behavioral effect.

The size of direct and indirect effects of increased security on the frequency of intrusions and therefore the ALE can be seen from Figure 7. There, the top line represents the frequency of intrusion occurrences for an L-type system (before investment in security is made). The middle line shows the rate that is expected after its security level is raised from L to H if only the direct effect is accounted for. The bottom line is the intrusion rate after the security is raised, given the presence of both direct and behavioral effects. As the diagram indicates, the indirect effect a security enhancement may have on the frequency of breaches can substantially exceed the direct effect. It is also possible that an attacker will not find it worthwhile to spend any effort at all on an H-type target and will prefer to leave an H-type target immediately and look for an L-type target instead.

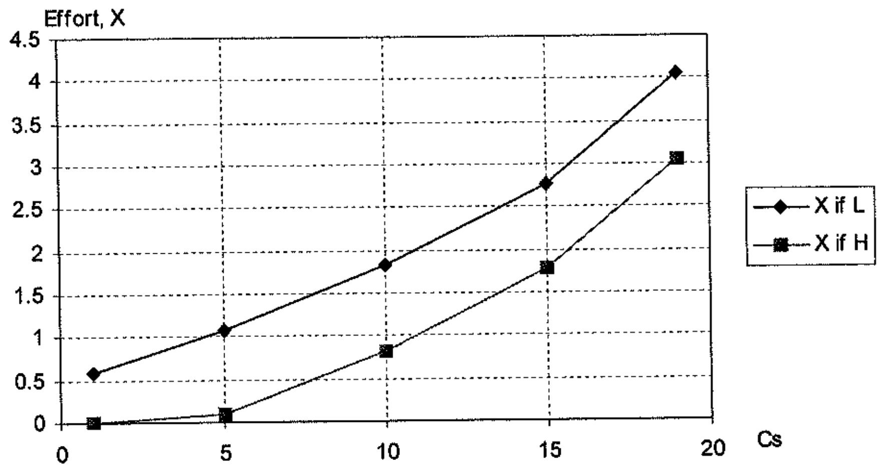

Figure 8. The effect of the switching cost C_s on the effort put by attackers into systems of each type.

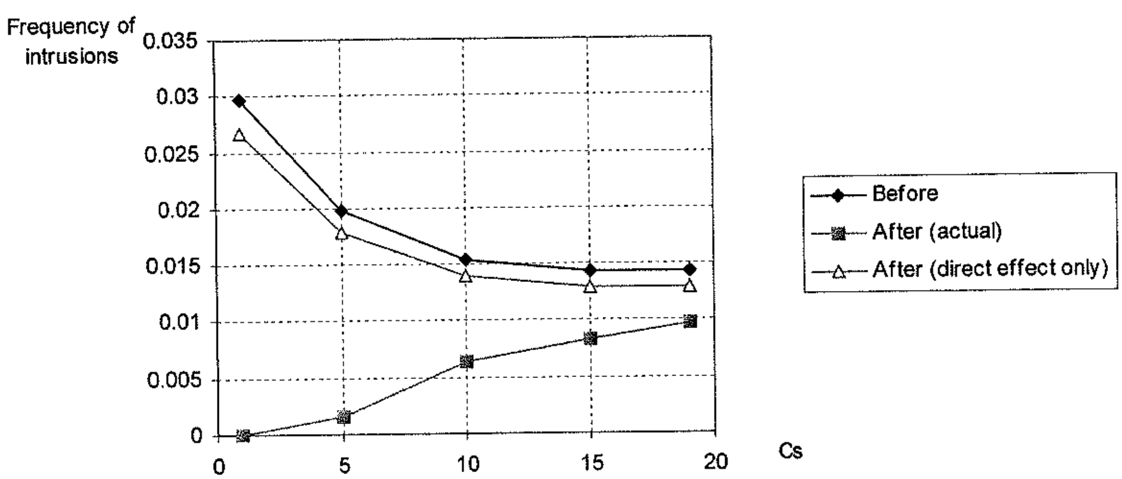

Figure 9. Frequency of intrusions before and after a security enhancement, plotted against the switching cost. The top curve, "Before", represents an L-type system before security enhancement. The middle one, "After (direct effect only)", shows the expected effect of upgrading to H-type, taking only the direct effect into account. The bottom line, "After (actual)", shows the frequency of intrusions that will actually occur as a result of an upgrade. It includes both the direct and the behavioral effect.

Figure 8 confirms the second result of Proposition 5, namely the positive correlation between the size of the switching cost and the amount of effort put into each attack on L-type and H-type systems, respectively.

Figure 9 allows us to elaborate on some specifics of the layered security approach and compartmentalized security architectures (Wells&Thrower, 2002). Those approaches have gained popularity in the last several years and have proven to be superior to more traditional approaches to information security that rely on a security perimeter only. However, existing security guidelines rarely make a distinction between investments into different security layers. If anything, there still seems to exist a tendency toward the "secure the perimeter" philosophy, according to which security investments should focus more on preventing intrusion attempts at early stages and therefore be concentrated on system areas that are closest to the external network. That means more attention is given to exterior layers of security than to interior ones. No clear consensus on the issue exists, however.

In the context of our model, the switching cost can represent the security of the exterior layer whereas the security parameter μ is a characteristic of the interior layer. As Figure 9 clearly indicates, strengthening outer echelons of defense may be less effective in reducing the frequency of intrusions than a combination of enhancing the security of the interior layer at the same time making that enhancement evident to attackers. It also shows that the higher the security level of a system, the more reason it has to signal its security level to attackers. As discussed above, such a signal may induce attackers to switch to other targets instead of continuing the intrusion attempts. This means that, at least for well-protected systems, it may be beneficial to have some means of implicit communication with attackers that would make them able to assess the target's security level. That is strikingly different from the aforementioned "secure the perimeter" approach and the traditional preference for opacity of protected networks that limit the amount of available information about deployed security measures.

Figure 9, however, has to be interpreted with care since the switching cost there is assumed to be the same across all systems. In reality, a security professional in charge of a specific system can control only the cost to an attacker of switching to his system but not to other systems. Second, as we try to translate this theoretical result into real world security practices, it is not completely clear what can serve as a credible signal of strong inner security and not undermine that security at the same time. Therefore, we are not ready to make any recommendations for security practices an individual firm may follow based on this result. (A further exploration of this issue is among our priorities for future research.)

That result presents an interesting policy issue, however. It suggests that the same change in μ causes a bigger change in the frequency of intrusions when switching costs are smaller, that is, when it is easier for attackers to determine what type of a target they are dealing with. Therefore, incentives to invest in security are stronger when switching costs for all systems are small.

3.4 Scenario 4 – Targets with unknown security level

Finally, we consider the case when the defender knows its security type but attackers do not. Thus, in this case we are dealing with incomplete asymmetric information. In this case, attackers base their behavior on their beliefs about the security level of a particular target.

The attacker's belief that he is dealing with an L-type target after effort x has not resulted in a break-in, $P(i = L \mid x)$, can be determined from the Bayes' theorem,

$$P(i = L \mid x) = \frac{P(x \mid i = L) \cdot P(i = L)}{P(x)} = \frac{(1-\eta)e^{-x/\mu_L}}{(1-\eta)e^{-x/\mu_L} + \eta e^{-x/\mu_H}} \qquad (10)$$

Here, $P(x \mid i = L)$ is the probability that an L-type target will remain intact after effort x has been spent on it. $P(i = L)$ is derived from the known prior distribution of systems within the population, and $P(x)$ is the probability that an attack on a randomly chosen target will not lead to success after effort x has been spent. It equals the weighted sum of corresponding probabilities for the two types.

It is easy to show that $\frac{\partial P(i = L|x)}{\partial x} < 0$, which implies that the more effort a target is able to withstand, the less likely the target is of the L-type. It also means that, unlike all the cases discussed so far, the marginal benefit of effort in this case is decreasing in effort. To see this is so, recall that in the deterministic cases discussed above $MB(x \mid i) = e^{-x/\mu_i} \cdot G / \mu_i$, where i is the system type. Given the Bayesian mechanism of forming beliefs, the marginal benefit of effort is given by

$$MB_{Bayes}(x) = P(i = L \mid x)MB(x \mid L) + P(i = H \mid x)MB(x \mid H) = \frac{G\left((1-\eta)\mu_H e^{-2x/\mu_L} + \eta\mu_L e^{-2x/\mu_H}\right)}{\mu_H \mu_L ((1-\eta)e^{-x/\mu_L} + \eta e^{-x/\mu_H})} \qquad (11)$$

and $\frac{\partial MB_{Bayes}(x)}{\partial x} < 0$. Even though the attacker's perception of his marginal benefit is constantly evolving, the optimal stopping rule can still be applied. Clearly, $MB_H(x) \leq MB_{Bayes}(x) \leq MB_L(x)$, which in turn implies $\hat{x}_H \leq \hat{x}_{Bayes} \leq \hat{x}_L$. See the graph below.

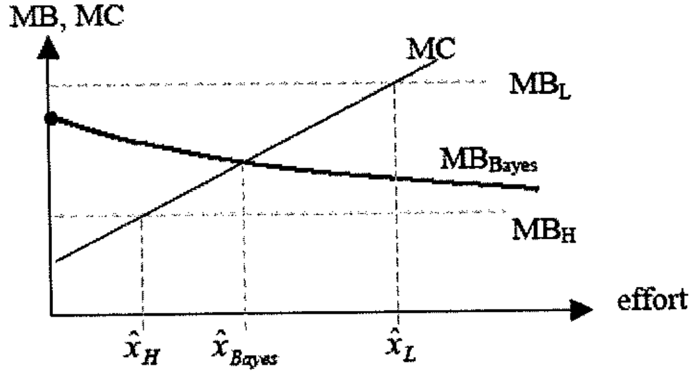

Figure 10. Marginal benefit and the solution to the attacker's optimal stopping problem for the complete information and the incomplete asymmetric information cases. The dot represents the prior probability of success from a randomly selected target. The expected marginal benefit of attacker's effort decreases because the more effort the attacker spends on a target with no success, the more he believes he is dealing with an H-type system.

In order to preserve consistency with the preceding analysis, the optimal stopping rule can also be approached using the expected net benefit from future effort, which in this case equals

$$ENB_{Bayes}(x) = P(i = H \mid x)ENB_H(x) + P(i = L \mid x)ENB_L(x) = \frac{\mu_H^2\alpha_1(z_H(x) - 1 + e^{-z_H(x)})\eta e^{-x/\mu_H} + \mu_L^2\alpha_1(z_L(x) - 1 + e^{-z_L(x)})(1-\eta)e^{-x/\mu_L}}{(1-\eta)e^{-x/\mu_L} + \eta e^{-x/\mu_H}} \quad (12)$$

where $z_i(x) = \dfrac{G/\mu_i - \alpha_0 - \alpha_1 x}{\mu_i\alpha_1}$, $i = H, L$. Once again, $ENB_H(x) \le ENB_{Bayes}(x) \le ENB_L(x)$ for any x and $\hat{x}_H \le \hat{x}_{Bayes} \le \hat{x}_L$.

The following two propositions summarize the results of our analysis of this case.

Proposition 6. When targets are heterogeneous and their type cannot be determined by attackers, the optimal amount of effort put forth by an attacker does not depend on the type of the system. For L-type targets, that amount is smaller than in the case when the target type is known to attackers (the complete information case) whereas for H-type targets it is greater than in the complete information case.

The expression for the frequency of intrusions at a given system in the presence of uncertainty about the target type is modified accordingly:

$$v_{i,uncert} = \frac{N_A(1 - e^{-\hat{x}_{Bayesi}/\mu_i})}{N_T\left(\tau_S + \eta\mu_H(1 - e^{-\hat{x}_{Bayesi}/\mu_H}) + (1-\eta)\mu_L(1 - e^{-\hat{x}_{Bayesi}/\mu_L})\right)}. \quad (13)$$

It can be shown that $v_H < v_{i,uncert} < v_L$, where v_H and v_L are the frequencies of intrusions in the complete information case given by (9). As was pointed out earlier, the ALE at each system is directly related with the frequency with which intrusions occur. Therefore, we have the following proposition.

Proposition 7. Attackers' uncertainty about target types increases the annual loss expectancy of H-type systems and decreases it for L-type systems. The overall effect of the attackers' uncertainty about target types on the aggregate welfare is negative when the proportion of H-type systems in the population, η, is large and it is positive when η is small.

Numerical simulations were performed for the same parameters as before, $G = 1000$, $\alpha_0 = 10$, $\alpha_1 = 2$, $C_S = 5$, $\mu_H = 55$, and $\mu_L = 50$. Figure 11 confirms $\hat{x}_H \leq \hat{x}_{Bayes} \leq \hat{x}_L$.

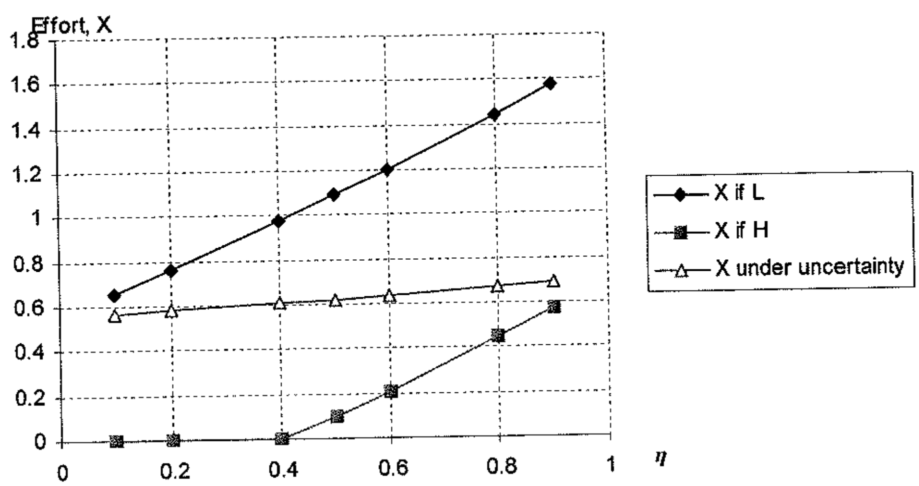

Figure 11. Effort optimally put by attackers into each system under different scenarios (as a function of the composition of the population). The top and the bottom lines represent $\hat{x}_L$ and $\hat{x}_H$, respectively, from the complete information case, as shown earlier in Figure 6.

Figure 12 shows the frequencies of intrusion in the incomplete asymmetric information case as a function of the relative proportion of H-type and L-type systems in the population. Since attackers now put the same amount of effort into attacking each system, the only difference in the frequency of intrusions across the two types (shown by the two lines in the middle) is attributed solely to the direct effect and is therefore proportional to the increase in the security parameter. This suggests that under incomplete asymmetric information the incentives to invest in security are substantially reduced.

Frequency of intrusions for each type in the certainty case is also provided for comparison. Clearly, attackers' uncertainty about target types benefits L-type systems and hurts H-type systems. The size of each type's welfare gain or loss from information asymmetry depends on the composition of the population. The fewer H-type systems there are, the more important it is for them to distinguish themselves from the rest of the population, therefore the loss in their welfare resulting from informational asymmetry will be greater, and vice versa.

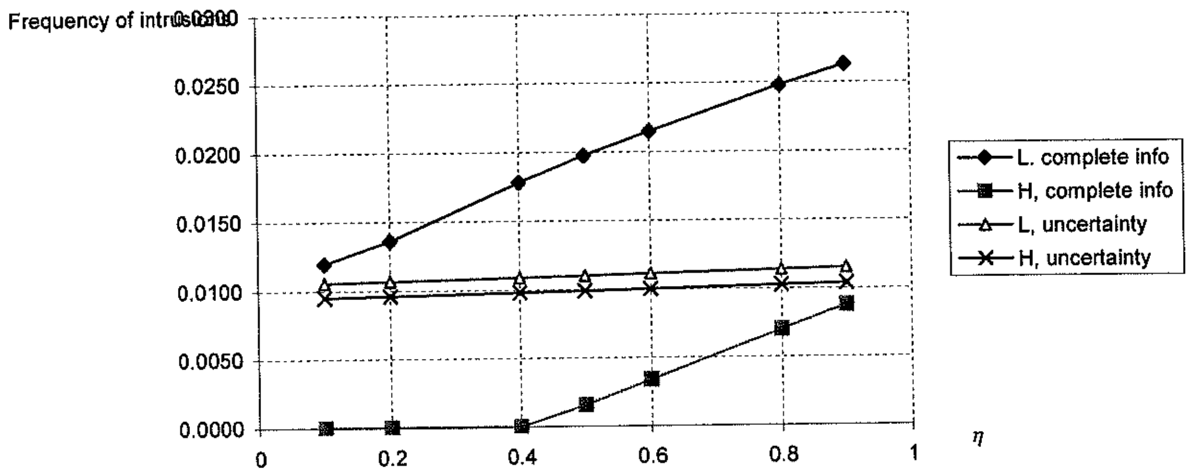

Figure 12. Frequency of intrusions under different scenarios (as a function of the composition of the population). The top and the bottom lines represent intrusion frequencies for L-type and H-type systems, respectively, from the complete information case, provided earlier in Figure 7. The two lines in the middle represent intrusion frequencies for the two types in the uncertain information case.

4. Discussion and Conclusion

Two cases were considered, one in which attackers were able to obtain information about each target's security level and the other in which the security level was known only to defenders. In both cases, attackers could choose from among multiple alternative targets. In the first, complete information case, attackers' optimal strategy is to put more effort into attacking systems with low security level than into systems with high security level. As a result, any increase in the defender's security level has two effects on the frequency of security incidents. One is the direct effect that is attributed to technical characteristics of a system and decreases the probability of success for a given attack effort. The second, indirect, or behavioral effect decreases the amount of effort an attacker puts into intrusion attempts, thus further decreasing the frequency of security incidents and the ALE.

Traditional approaches to security practices tend to focus only on the direct effect of security solutions and overlook the behavioral one. However, as our results show, the magnitude of the behavioral effect can greatly exceed that of the direct one. As a result, the benefit an individual system may get from a security enhancement may be severely underestimated if the behavioral effect is not taken into consideration. That would mean that some security investments that are in fact worth making will not be made, which leads to either underinvestment in security at the individual system level or, at the very least, to substantial misallocation of resources.

The magnitude of the behavioral effect depends on the distribution of target security levels, or types, and attackers' costs of switching between alternative targets. The smaller the switching costs, the greater the overall reduction in successful intrusions suffered by the system. If switching costs are a representation of the amount of effort an attacker needs to spend to find out the target type, then the above result means that the efficacy of security investment depends on the characteristic of the environment which we call "opacity". The greater the switching costs, the more "opaque" the environment is in the sense that it gets harder for attackers to determine the type of a target, which weakens the behavioral effect. If, on the contrary, the environment is "transparent" and determining the type is relatively easy, then the behavioral and the overall effects of a security investment will be stronger. From the practical perspective, this means that a given security solution will be more efficient if potential attackers are aware of extra tools being deployed.

Since greater transparency makes a security investment translate into a greater reduction in the frequency of intrusions and therefore losses, incentives for firms to invest in security in that case will also be greater. To summarize, if the characteristic of the environment (transparent vs. opaque) is treated as exogenous, then greater transparency increases the incentive to improve security whereas opacity weakens them.

In reality, environment is not exogenously given. It is an outcome of ongoing security practices and individual firms' decisions about the best way to spend security budgets. In that context, it is also interesting to discuss the effect of changes in the environment on systems of each type. That issue can also be discussed in the context of switching costs but is best done by considering the second modification of our model, namely that of incomplete asymmetric information, in which attackers never know the target type with certainty. As a result, they treat every target the same, and the behavioral effect is not present.

As the results of the analysis of that case clearly indicate, opacity penalizes better protected systems and favors those with weaker protection. As a result, systems whose security level is consistently low relative to the rest of the population will have preference for opacity over transparency since it gives them a better chance to disguise themselves as well-protected systems, thus reducing the amount of effort attackers put into attacking them. Well-protected systems, on the contrary, are better off in a transparent environment than in an opaque one and therefore have an incentive to signal their high security level to the attackers in order to separate themselves from L-type systems. This is consistent with existing theoretical research on economics of incomplete asymmetric information (Akerlof 1970) that suggests that the ability to signal one's type (more transparency in the context of our model) benefit "high quality products" (H-type systems) and penalize "low quality products" (L-type systems).

This result has interesting practical implications for the case of layered security architecture. Poorly protected systems may have more reason to invest in the exterior security layer, thus increasing opacity, whereas for well protected systems investment in the security of interior layers may be more beneficial, assuming they intend to maintain their advantage in protection level over the rest of the population.

The incomplete asymmetric information version of the model also allowed us to address the effect of informational issues and the distribution of system types on the expected welfare losses from attacks. When the proportion of H-type systems in the population is small, then the benefit each of them gets from transparency (thus from identifying themselves as H-type systems) is substantial while L-type systems do not lose much since there are so many of them. When the proportion of H-type systems is large, the opposite is true. Interestingly, we did not find any effect of informational assumptions on the aggregate welfare since any benefit H-type systems as a group get from increased transparency was offset by a reduction in L-type systems welfare.

To a certain extent, the above discussion of opacity versus transparency is related to the debate surrounding the "security through obscurity" approach (Perens, 1998; Beale, 2000, Schneier, 2002, Swire, 2004). "Security through obscurity" is the term coined to denote technical security solutions the effectiveness of which is based on the secrecy of processes, protocols, or algorithms, which contrasts the basic rule of cryptography, the principles of the open source movement, and the open public disclosure of security vulnerabilities. In our model, a similar trade-off between disclosing information about the security level and keeping them secret exists. On both occasions, the resulting conclusions are controversial, although overall evidence seems to favor the rejection of the "security through obscurity" (or "security through opacity" in our case) approach. Today, when it comes to the information related to the security level of a corporate network, the practice is to keep it secret because its disclosure might favor attackers. The results of our study suggest, however, that a certain degree of transparency in handling such information may also have its virtues.

As always, our analysis has some limitations. Most importantly, our model is static in the sense that it only analyses the instantaneous effect of security enhancement assuming the distribution of system types and the rate of attackers' arrival at each target stayed the same. The interrelationship between the decisions of individual defenders and what we called the environment can be fully and properly understood only in a dynamic game-theoretic model. Besides, another aspect of security as a dynamic process is the fact that the outcome of any individual decision will also depend on what other systems are doing at the same time. Therefore incorporating tools used in the analysis of interdependent security games is going to greatly enrich our analysis.

5. References

Akerlof, G.A. (1970). The Market for 'Lemons': Quality Uncertainty and Market Mechanism. *Quarterly Journal of Economics*, 84(3):488-500.

Anderson, R.J. (2001). Why Information Security is Hard – an Economic Perspective. In *Proc. of the 17th Annual Computer Security Application Conference*, New Orleans, LA.

Avizienis, A., Laprie, J., and Randell, B. (2000). Fundamental Concepts of Dependability. In *Proc. of the Third Information Survivability Workshop*, Boston, MA.

Avizienis, A., Laprie, J., Randell, B., and Landwehr, C. (2004). Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Transactions on Dependable and Secure Computing, 1(1):11-33.

Beale, J. (2000). "Security Through Obscurity" Ain't What They Think It Is. *Bastille Linux*. Available at http://www.bastille-linux.org/jay/obscurity-revisited.html.

Bier, V., Oliveros, S., and Samuelson, L. (2005). Choosing what to Protect: Strategic Defensive Allocation against an Unknown Attacker. *Journal of Public Economic Theory*, forthcoming.

Cavusoglu, H. and Raghunathan, S. (2004). Configuration of Detection Software: A Comparison of Decision and Game Theory Approaches. *Decision Analysis*, 1(3):131–148.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). A Model for Evaluating IT Security Investments. *Communications of the ACM*, 47(7):87-92.

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2005). The Value of Intrusion Detection Systems in Information Technology Security Architecture. *Information Systems Research*, 16(1):28-46.

Clemons, E. K. (1991). Evaluation of Strategic Investments in Information Technology. *Communications of the ACM*, 34(l):22-36.

Cozzolino, J. M. (1972). Sequential search for an unknown number of objects of nonuniform size. *Operations research*. 20:293-308.

Curry, S. (2002). Bug Watch: Hacker Motivation. *Vnunet.com*. Available at http://www.vnunet.com/vnunet/news/2117147/bug-watch-hacker-motivation?vnu_lt=vnu_art_related_articles

Denning, D. E. (1990). Concerning Hackers Who Break into Computer Systems. *Phrack*, 3(32). Available at http://www.phrack.org/show.php?p=32&a=3.

Enders, W. and Sandler, T. (2004). What Do We Know About the Substitution Effect in Transnational Terrorism?. In Andrew Silke and G. Ilardi(eds.) *Researching Terrorism Trends, Achievments, Failures* (Frank Cass).

Geer, D. E. (2005). Making Choices to Show ROI. *Secure Business Quarterly*, 1(2). Available at http://sbq.com/sbq/rosi/sbq_rosi_making_choices.pdf.

Gordon, L. A. and Loeb, M. P. (2002a). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*, 5(4):438-457.

Gordon, L. A., Loeb, M., and Lucyshyn, W. (2003). Information Security Expenditures and Real Options: A Wait-and-See Approach. *Computer Security Journal*, 19(2).

Gordon, L. A. and Loeb, M. (2005). *Managing Cybersecurity Resources: A Cost-Benefit Analysis*. McGraw-Hill.

Gordon, L. A., Loeb, M., Lucyshyn, W., and Richardson, R. (2005). *2005 CSI/FBI Computer Crime and Security Survey*. Computer Security Institute.

Gordon, L. A. and Richardson, R. (2004). The New Economics of Information Security. *Information Week*, 53-56. Available at http://www.banktech.com/aml/showArticle.jhtml?articleID=18901266.

Jajodia, S., J. Miller. (1993). Editor's preface. *Journal of Computer Security*. 16(4):43–53.

Jonsson, E. and Olovsson, T. (1997). A Quantitative Model of the Security Intrusion Process Based on Attacker Behavior. *IEEE Transactions on Software Engineering*, 23(4).

Kearns, M. and Ortiz, L. E. (2004). *Algorithms for Interdependent Security Games*. In S. Thrun, L. Saul, and B. Scholkopf, editors, *Advances in Neural Information Processing Systems* 16. MIT Press.

Kuhnreuther, H. and Heal, G. (2003). Interdependent Security. *The Journal of Risk and Uncertainty*, 26(2/3):231-249.

Littlewood, B., Brocklehurst, S., Fenton, N., Mellor, P., Page, S., Wright, D., Dobson, J., McDermid, J., and Gollmann, D. (1993). Towards Operational Measures of Computer Security. *Journal of Computer Security*, 2:211-229.

Leeson P.T. and Coyne , C. J. (2006). The Economics of Computer Hacking. *Journal of Law, Economics and Policy.*

Liu, P., Zang, W. and Yu, M. (2005). Incentive-Based Modeling and Inference of Attacker Intent, Objectives, and Strategies. *ACM Transactions on Information and System Security* , 8(1):78-118.

McDermott, J. (2005). Attack-Potential-Based Survivability Modeling for High-Consequence Systems. In *Proc. of the Third IEEE Int. Information Assurance Workshop*, Washington, DC.

Nicol, D. M., Sanders, W. H., and Trivedi, K. S. (2004). Model-Based Evaluation: From Dependability to Security. IEEE Transactions on Dependable and Secure Computing, 1(1):48-65.

NIST 800-30. (2002). Risk management guide for information technology systems. National Institute of Standards and Technology Special Publication, Gaithersburg, MD.

Ortalo, R., Deswarte, Y., and Kaâniche, M. (1999). Experiments with Quantitative Evaluation Tools for Monitoring Operational Security. *IEEE Transactions on Software Engineering*, 25(5):633-650.

Perens, B. (1998). Why Security-Through-Obscurity Won't Work. Slashdot. Available at http://slashdot.org/features/980720/0819202.shtml.

Purser, S. (2004). Improving the ROI of the Security Management Process. *Journal of Computers & Security*, 23 (7):542-546.

Rodewald, G. (2005). Aligning Information Security Investments with a Firm's Risk Tolerance. In *Proc. of the Information Security Curriculum Development (InfoSecCD) Conference '05*, Kennesaw, GA.

Schechter, S. E. (2004). *Computer Security Strength and Risk: A Quantitative Approach*. PhD thesis, Harvard University DEAS.

Schechter, S. E. (2005). Toward Econometric Models of the Security Risk from Remote Attack. *IEEE Security&Privacy*, 3(1):40-44.

Schneier, B. (2002). Secrecy, Security, and Obscurity. *Crypto-Gram*, Available at http://www.schneier.com/crypto-gram-0205.html#1.

Sieberg, D. (2005). Hackers shift focus to financial gain. CNN. Available at http://www.cnn.com/2005/TECH/internet/09/26/identity.hacker/

Soo Hoo, K. J. (2000). *How Much Is Enough? A Risk-Management Approach to Computer Security*. Doctoral dissertation, Stanford University School of Engineering.

Swire, P. P., (2004). A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?. *Journal on Telecommunications and High Technology Law*, 2.

Wells, M., and Thrower, W. (2002). The Importance of Layered Security. *Symantec Corporation.* Available at http://enterprisesecurity.symantec.com/article.cfm?articleid=769&EID=0