Association for Information Systems
AIS Electronic Library (AISeL)

ICIS 2002 Proceedings

International Conference on Information Systems (ICIS)

December 2002

Optimal Design of Information Technology Security Architecture

Huseyin Cavusoglu
University of Texas at Dallas

Srinivasan Raghunathan
University of Texas at Dallas

Birendra Mishra
University of Texas at Dallas

OPTIMAL DESIGN OF INFORMATION TECHNOLOGY SECURITY ARCHITECTURE

Huseyin Cavusoglu
School of Management
The University of Texas at Dallas
Richardson, TX USA
huseyin@utdallas.edu

Srinivasan Raghunathan
School of Management
The University of Texas at Dallas
Richardson, TX USA
sraghu@utdallas.edu

Birendra Mishra
School of Management
The University of Texas at Dallas
Richardson, TX USA
bmishra@utdallas.edu

Abstract

Information technology (IT) security has emerged as an important issue in e-commerce. Firms typically employ multiple security technologies such as firewalls and intrusion detection systems (IDS) to secure their IT systems. An assessment of the value of these technologies is crucial for firms to design the optimal architecture. Such assessments are also useful to security technology developers in focusing their design efforts. We describe in this report our ongoing research in economic modeling of IT security management. Specifically we describe the technologies used in a typical IT security architecture, a game theoretical model of the significant aspects of the architecture, preliminary analysis of the model, and our current and future work. Our research, when completed, will yield guidelines that will help security technology deployment firms make their investment decisions and security technology developers make their design decisions.

1 INTRODUCTION

Increased interconnectivity among computers enabled by networking technologies, in particular the Internet, has boosted the scale and scope of information technology (IT) related crimes (Denning 2000). As electronic commerce continues to grow, so does cyber crime. IT security, which was once an overhead to a company's main operation, is now widely recognized as an important aspect of business operations (Cagnemi 2001) for all types of organizations.

IT security management seeks to manage the risks associated with IT assets such as loss, disruption, and unauthorized access of information and system resources. Firms employ several different mechanisms internally to secure their IT systems. Internal mechanisms fall into three major categories: *preventive*, *detective*, and *response*. Preventive mechanisms like firewalls allow only authorized traffic between the internal system and the external world. Preventive mechanisms aim to develop a defensive shield around IT systems to secure them. Detective mechanisms like intrusion detection systems (IDS) try to detect the intrusions when they occur by analyzing the log files to detect suspicious system use. Response mechanisms are the more detailed investigations, typically manual, of system use patterns to detect and confirm, as well as stop, illegal use of the system. A firm's internal mechanisms work in conjunction with external mechanisms, such as the laws and regulations enacted by governments, which act as a broad deterrent against IT-related crime.

Despite the importance of IT security to firms, researchers in the information systems area have not analyzed the issue from an economic perspective.[1] Research on IT security in engineering disciplines has focused on security technology, such as intrusion detection and firewall algorithms. An assessment of the economic value of IT security controls is critical to firms that deploy security technology as well as firms that develop the technology. Firms that deploy security technology require such assessments in order to make investment decisions. Firms that develop security technology require such assessments in order to focus their efforts on design parameters that offer the highest value to deploying firms.

Our ongoing research is aimed at deriving guidelines about and insights into the economic value of IT security mechanisms. Quantification of the value of IT security architecture requires an analytical model.[2] We seek a model that captures the essence of the IT security architecture and that is tractable. In order to develop the analytical model, we performed an extensive research of IT security technologies (Cavusoglu et al. 2001). A high level classification of the technologies based on only their function within the security architecture is insufficient to model the relevant parameters that affect their value. We studied processes underlying these technologies and abstracted the relevant parameters that measure their effectiveness.

In this research in progress report, we describe the problem, a model to analyze the problem, and preliminary analysis of the model. We consider a firm that deploys IT security to minimize its expected loss. We seek to answer the following specific research questions in this context. (1) What is the reduction in organizational loss, i.e., value, because of a security technology? (2) What is the optimal level of investment in each of these technologies? (3) What is the impact of cost and quality of technology on the optimal security architecture?

2 IT SECURITY ARCHITECTURE

Figure 1 shows a typical IT security architecture consisting of multiple layers of controls.[3] The technology deployed in each layer has different capabilities and characteristics. The outermost layer consists of firewalls as preventive controls to filter out unauthorized external traffic. The middle layer consists of intrusion detection mechanisms to detect unauthorized use of the system by both insiders and hackers who have successfully cracked the firewalls. The bottom layer consists of detailed investigations both to detect intrusions and in response to detection by the middle layer.

Firewalls are network access control devices that attempt to prevent intrusions from external hackers. They can be configured to allow traffic based on the service requested, the IP address of the source or destination, or the ID of the user requesting the service (Maiwald 2001). During firewall configuration, the security administrator defines traffic from outside that should be allowed by firewalls. Firewalls use two types of mechanisms. A *packet-filtering* mechanism performs filtering based on a set of rules encoded in an access control list. The rules may be based on source or destination address, protocol, port number, or other data found in the packet header. The filters read the Internet Protocol (IP) header of each packet received by the firewall. If header data satisfies the rules, the packet is allowed; otherwise it is dropped. A limitation of this mechanism is that criteria based solely on header information do not provide the precision of control that many organizations need (Krause and Tipton 1999). An *application layer* mechanism uses proxies. Each proxy checks not only the header information but also the service requested by the packet. Proxies allow the precision level of the control to be fine-tuned, but they have limitations. In the absence of a proxy, the user is denied access to that application. Typically firms use both of these mechanisms to control external traffic. The effectiveness of a firewall is measured by two parameters: the extent to which they (1) leak disallowed traffic and (2) stop valid traffic.

An IDS attempts to detect intrusions by analyzing audit trails that store event histories and network packets. An IDS runs continually in the background and generates an alarm when it detects something it considers suspicious, anomalous, or illegal. There are two primary mechanisms that an IDS uses to analyze events in order to detect attacks: Signature-based detection and anomaly detection (McHugh et al. 2000). Signature-based detection matches a predefined pattern of events, called a signature, associated with a known attack but fails when the attack pattern is new. Anomaly detection techniques use a *normal activity profile* for a system and flag all system states varying from the established profile in a statistically significant manner thus iden-

[1]Recently Gordon et al. (2002) argued the need for such research.

[2]See Cavusoglu et al. (2002) for an alternate approach based on the market valuation of firms.

[3]In this study, we are interested in only perimeter security. Therefore, we are modeling attacks against internal systems. Attacks occurring during transmission, for instance, are not addressed.

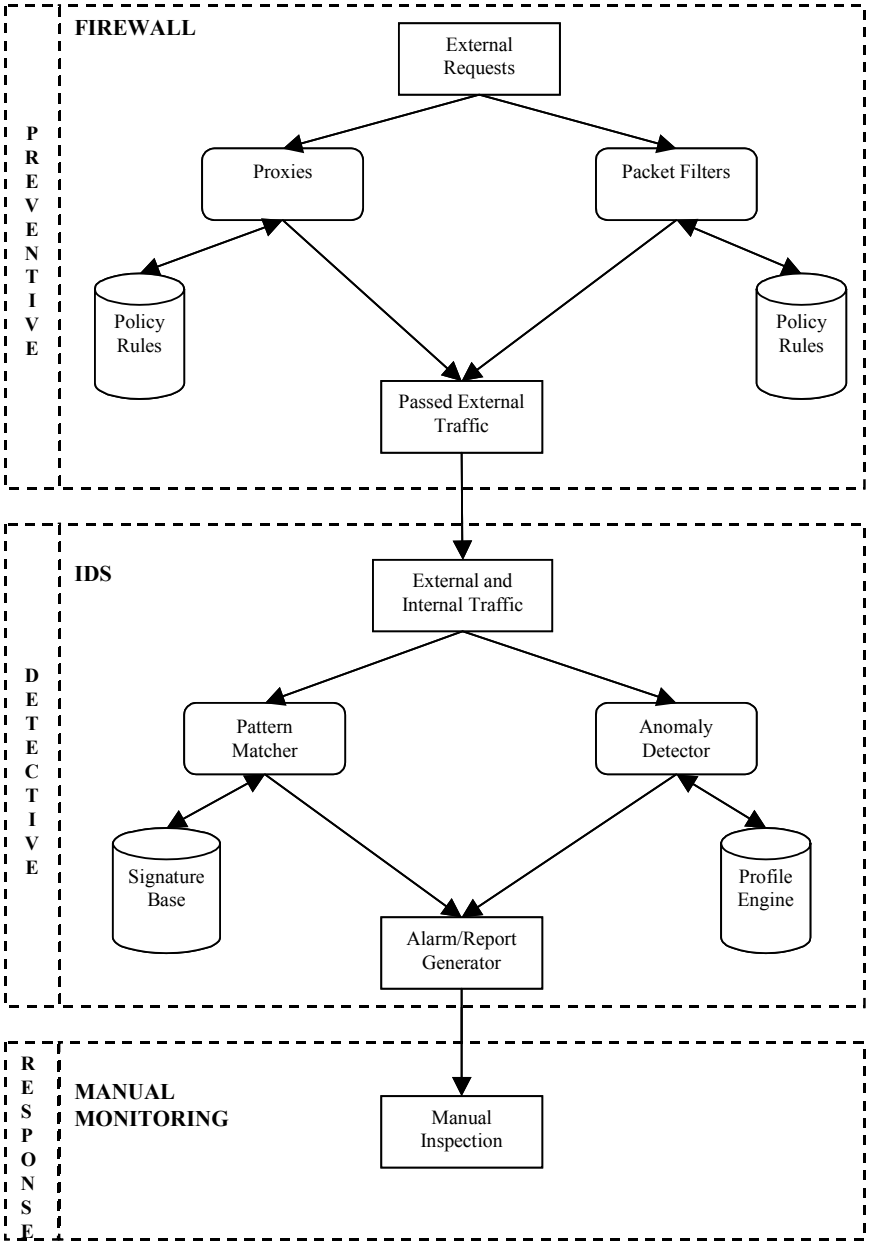

Figure 1. IT Security Architecture

tifying abnormal behavior. The normal activity profiles are constructed typically from historical data. Unfortunately, anomaly detection often produces a large number of false alarms, as normal patterns of users and system behavior can vary widely. However, unlike signature-based IDS, anomaly-based IDS are capable of detecting unseen attacks. Like firewalls, IDS are not perfect. The effectiveness of an IDS is measured using two parameters: the likelihoods of (1) giving a signal upon an intrusion and (2) being silent in case of no intrusion.

Following a signal from the IDS, a security analyst examines audit trails and log files of system resources to determine if there is a real intrusion and, if so, the type and the extent of the intrusion. If an intrusion is confirmed by the investigation, appropriate corrective measures are undertaken to limit further damage and recover, if possible, the damage already incurred.

It should be emphasized that the above security architecture works within the external legal framework of penalties and punishments that deters unauthorized use. The value of security control at any level depends critically on this legal framework as well as other controls surrounding it. Multiple layers of security are necessitated by the fact that many of the security controls

are imprecise. The costs associated with false positives and false negatives affect the value of a security control significantly. The security controls at different levels may also substitute and complement other controls. The cost structures associated with security mechanisms at different levels can be sharply different. These characteristics require that a firm simultaneously design all layers for optimal security.

The strategic nature of the problem is another dimension that needs to be considered when dealing with security. Soon after a new security technology is developed, hackers often figure out the loopholes and weaknesses of the technology and how it can be broken. Hackers do not select organizations randomly. They attack IT systems that are vulnerable and do not have appropriate controls. In essence, they strategically choose their victims and actions. A good illustration of the strategic game played by the security experts in a firm and the hackers is provided at http://www.msnbc.com/modules/hack_attack/hach.swf.

3 MODEL

Consider a firm interested in setting up its security architecture. The optimal design of security architecture depends on the extent of expected damage d that hackers can inflict on the firm and is known to both the firm and the intruder.[4] Most firms estimate possible damages along with their likelihoods in the IT security risk assessment phase (Peltier 2001). We assume that ε fraction of traffic comes from external users, and $(1 - \varepsilon)$ fraction originates from internal users. ζ fraction of external traffic comes from unauthorized users. These are supposed to be stopped at firewalls. Firewalls are not perfect. We model the effectiveness of the firewall through two parameters q_1^F and q_2^F. The parameter q_1^F denotes the probability that the firewall will stop an unauthorized external user. We assume that the firewall performs better than random guessing, so q_1^F lies between 0.5 and 1. q_2^F is the probability that legitimate external traffic passes through the firewall. The complement of q_2^F, $(1-q_2^F)$, reflects the fraction of legitimate external traffic stopped at the firewall. q_2^F is also assumed to be between 0.5 and 1 for the same reason as q_1^F.

All internal users are authorized users of the system. However, they as well as authorized external users can misuse the system by improperly accessing data or programs they are not authorized to use. A fraction λ of the authorized users is assumed to be dishonest. The second layer controls, IDS, are also not perfect. We model the effectiveness of the IDS through two parameters q_1^I and q_2^I. The parameter q_1^I denotes the probability that the IDS gives a warning signal whenever an intrusion occurs. We assume that q_1^I lies between 0.5 and 1. Sometimes the system classifies an action as anomalous when it is a legitimate action. q_2^I is the probability that there is no signal when there is no intrusion. q_2^I is also assumed to be between 0.5 and 1.

Following a signal from the IDS, an investigation is needed to determine the type and extent of the attack, if it is a true attack. The firm incurs a cost of c each time it monitors the audit trail of a user for a possible intrusion. Manual monitoring done by the firm may not detect intrusion with certainty. This imperfection of monitoring is captured by an effectiveness parameter α, the probability with which monitoring detects a true intrusion. If manual monitoring detects the intrusion, the firm recovers a fraction of the damage by the intruder without any additional cost. This fraction is captured by the parameter, ϕ.

Previous studies have shown that incentives for intruders are usually not related only to financial gains (Koerner 1999). We assume that when a hacker breaks into the system he gets a fixed utility of $\grave{\imath}$. If the intrusion is discovered, the hacker incurs a penalty. The penalty is composed of two components: A fixed penalty β and a variable penalty proportional to the expected amount of damage, γd (Nicholson et al. 2000). We assume that prices of security controls increase in their effectiveness. The price of the firewall is captured by $z_1(q_1^F - 0.5) + z_2(q_2^F - 0.5)$ whereas the price of the IDS is in the form of

[4] Although this assumption is necessary for mathematical tractability, it carries a great amount of uncertainty. However, sensitivity analysis with respect to d will give some implications even if the point estimate for damage is incorrect.

$w_1(q_1^I - 0.5) + w_2(q_2^I - 0.5)$. z_i and w_i characterize the relative costs of reducing type 1 and type 2 errors in the firewall and the IDS, respectively.[5]

4 MODEL ANALYSIS

Figure 2 depicts the game tree we use for analyzing firm and hacker strategies. The game starts with nature selecting the type of user, which can be external (node 1) with probability ε or internal (node 4) with probability $(1 - \varepsilon)$. Node 2 represents the unauthorized external user whereas node 3 symbolizes the authorized external user. Honest authorized users have a dominant strategy of not hacking. A dishonest authorized user can take two actions: *hack* or *do not hack*. If he decides to *hack*, the game moves to node 6, otherwise to node 7. In the next level, the IDS tries to detect intrusions which are captured by node 6. The firm makes decisions about whether to monitor or not based on the state (the signal or the no signal) it is in. The dashed curves in Figure 2 enclose the information sets of the firm. The game is made up of two parts: one in which there is a signal from the IDS (information set I1), and one in which there is no signal from the IDS (information set I2). The firm makes decisions without knowing exactly which node the game has reached within an information set.

The mixed strategy space for the dishonest user is a probability distribution ψ {*intrusion, no intrusion*} → [0,1] where ψ denotes the probability of intrusion. The strategy set of the firm is a vector $S^f \in$ {*monitor|no-signal, do-not monitor|no-signal, monitor|signal, do-not monitor|signal*}. We define $0 \le \rho_1 \le 1$ as the probability of monitoring given a signal from the IDS and $0 \le \rho_2 \le 1$ as the probability of monitoring given no signal.

The objective of the hacker is to maximize his expected payoff while the firm tries to minimize organizational loss. The payoff function for the firm is

$$F(\rho_1, \rho_2, \psi) = P(signal)F_S(\rho_1, \psi) + P(nosignal)F_N(\rho_2, \psi) + P(drop)Cost(drop) + Cost(controls)$$

where $F_S(\rho_1, \psi)$ and $F_N(\rho_2, \psi)$ are payoff functions for signal and no signal states, respectively. Each of these payoff functions consists of three parts: the loss from undetected intrusion, the loss from detected intrusion, i.e., the portion of the loss unrecovered even if the intrusion is detected, and the monitoring cost. *Cost(drop)* is the cost associated with dropping external authorized users at the firewall. *Cost(controls)* is the investment cost in firewalls and IDS.

The hacker's expected payoff is given below. The first part is the expected utility from the intrusion and the second part is the expected cost if the intrusion is detected.[6]

$$H(\rho_1, \rho_2, \psi) = \psi\mu - \psi(q_1^I\rho_1 + (1 - q_1^I)\rho_2)\alpha(\beta + \gamma d)$$

In order to determine optimal investment in security controls, we use backward induction. First we determine optimal response, i.e., frequency of manual monitoring, assuming that the firm has adopted the optimal security controls in both preventive and detective control layers. Then, using the optimal response in the last stage, we go to the first stage and decide on optimal effectiveness for both firewalls and IDS simultaneously.

We have analyzed the last stage of the game so far. The solution for this stage results in five Nash equilibria, two in mixed strategies and three in pure strategies. We summarize these equilibria in the following proposition.

---

[5]A type 1 error is incurred when the security control fails to detect the unauthorized activity: letting an unauthorized external user into the system in the case of a firewall and not giving a signal for hacking activity in the case of an IDS. On the other hand, a type 2 error is incurred when the security control detects something that it is not supposed to detect: not letting an authorized external user into the system in the case of a firewall and giving a signal for non-hacking activity in the case of an IDS.

[6]This model assumes that hackers do not select their victims randomly. The notion of strategic interaction requires the hacker to spend some time to determine which firms are vulnerable and worth attacking. The inclusion of such pre-hacking cost does not change the results and therefore omitted.

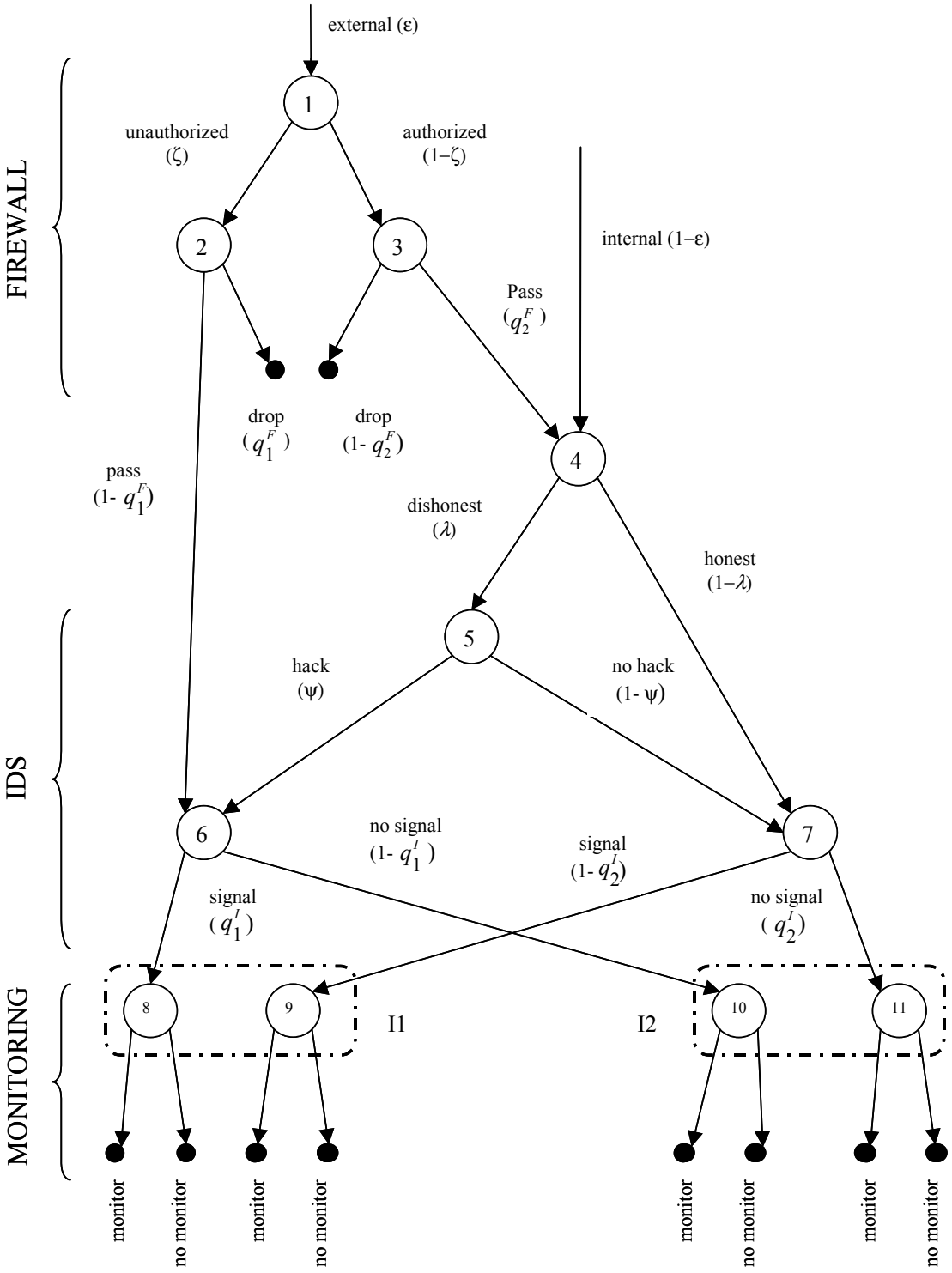

Figure 2. The Game Tree

Proposition 1: Optimal Monitoring Strategy for the Firm Along with Hacker's Strategy

Probability of Monitoring when there is a signal from IDS	Probability of Monitoring when there is no signal from IDS	Probability of Hacking
$\rho_1 = 1$	$\rho_2 = \frac{\mu - q_1^I \alpha(\beta + \gamma d)}{\alpha(\beta + \gamma d)(1 - q_1^I)}$	$\psi = \frac{cW_2 + (1 - q_1^I)\Gamma}{\Omega}$
$\rho_1 = \frac{\mu}{\alpha(\beta + \gamma d) q_1^I}$	$\rho_2 = 0$	$\psi = \frac{cW_1 - q_1^I \Gamma}{\Omega}$
$\rho_1 = 1$	$\rho_2 = 1$	$\psi = 0$
$\rho_1 = 0$	$\rho_2 = 0$	$\psi = 1$
$\rho_1 = 1$	$\rho_2 = 0$	$\psi = 1$

where

$$W_1 = (1-\varepsilon)(1-q_2^I) + q_2^F \varepsilon (1-q_2^I)(1-\zeta) + \zeta \varepsilon q_1^I (1-q_1^F)$$
$$W_2 = q_2^I \varepsilon (1-q_2^F) - \varepsilon (1-q_1^F)(1-q_1^I)\zeta + q_2^I q_2^F \zeta \varepsilon - q_2^I$$
$$\Gamma = d(1-q_1^F)\alpha \zeta \varepsilon \phi$$
$$\Omega = \lambda \left[\varepsilon (1 - q_2^F (1-\zeta)) - 1 \right] \left[c(q_1^I + q_2^I - 1) - q_1^I d \alpha \phi \right]$$

Preliminary analysis reveals that all equilibria can be succinctly characterized using the following two dimensions: (1) benefit to cost ratio of intrusion for the hacker and (2) cost to benefit ratio of monitoring for the firm. As the value of dimension (1) increases and/or the value of dimension (2) decreases, the firm increases its monitoring effort while the hacker reduces his probability of hacking. The firm always monitors a larger or equal fraction of cases that generate signals compared to those that did not generate a signal. These preliminary results are consistent with our intuitions.

5 FUTURE WORK

The equilibrium that will be reached will depend on the values of parameters. Currently we are identifying the conditions for different equilibrium. These conditions will provide insights into how the quality and cost of security architecture components affect the hacker and firm strategies. Further computing the organizational loss and minimizing it with respect to the quality parameters will provide the optimal quality levels for the security components.

We will also perform a sensitivity analysis of the optimal quality levels and organizational loss with respect to the cost parameters to derive insights into the impact of the cost structure on the optimal security configuration. We also plan on extending our analysis for the case when firms have a budget on IT security investment. In the future, we will extend the model using different types of hackers (internal and external) with different utility functions and the varying amounts of damage they can inflict on systems.

6 REFERENCES

Cagnemi, M .P. "Top Technology Issues," *Information Systems Control Journal* (4:6), 2001.

Cavusoglu, H., Mishra, B. K., and Raghunathan, S. "The Effect of Internet Security Breach Announcements on Shareholder Wealth," Working Paper, University of Texas, Dallas, 2002.

Cavusoglu, H., Mishra, B. K., and Raghunathan, S. "The Value of Intrusion Detection System in IT Security Architecture," Working Paper, University of Texas, Dallas, 2001.

Denning, D. "Reflections on Cyberweapons Controls," *Computer Security Journal* (16:4), 2000, pp. 43-53.

Gordon, L. A., Loeb, M. P., and Sohail, T. "A Framework for Using Insurance for Cyber Risk Management," *Communications of the ACM*, 2002 (forthcoming).

Koerner, B. I. "Who Are Hackers, Anyway?," *U.S News & World Report* (17:2), July 14, 1999, p. 53.

Krause, M., and Tipton, H. F. *Information Security Management Handbook*. Mission Viejo, CA: Auerbach Publications, 1999.

Maiwald, E. *Network Security: A Beginner's Guide*. Berkeley, CA: Osborne/McGrawHill, 2001.

McHugh, J., Christie A. C., and Allen J. "Defending Yourself: The Role of Intrusion Detection Systems," *IEEE Software*, September/October 2000.

Nicholson, L. J., Shebar, T. F., and Weinberg M. R. "Computer Crimes," *The American Criminal Law Review*, Spring 2000.

Peltier, T. R. *Information Security Risk Analysis*. Mission Viejo, CA: Auerbach Publications, 2001.