Information Systems Research
Vol. 20, No. 2, June 2009, pp. 198–217
ISSN 1047-7047 | EISSN 1526-5536 | 09 | 2002 | 0198

DOI 10.1287/isre.1080.0180

Configuration of and Interaction Between Information Security Technologies: The Case of Firewalls and Intrusion Detection Systems

Huseyin Cavusoglu, Srinivasan Raghunathan
School of Management, University of Texas at Dallas, Richardson, Texas 75083
{huseyin@utdallas.edu, sraghu@utdallas.edu}

Hasan Cavusoglu
Sauder School of Business, University of British Columbia, Vancouver, British Columbia, V6T 1Z2 Canada,
cavusoglu@sauder.ubc.ca

Proper configuration of security technologies is critical to balance the needs for access and protection of information. The common practice of using a layered security architecture that has multiple technologies amplifies the need for proper configuration because the configuration decision about one security technology has ramifications for the configuration decisions about others. Furthermore, security technologies rely on each other for their operations, thereby affecting each other's contribution. In this paper we study configuration of and interaction between a firewall and intrusion detection systems (IDS). We show that deploying a technology, whether it is the firewall or the IDS, could hurt the firm if the configuration is not optimized for the firm's environment. A more serious consequence of deploying the two technologies with suboptimal configurations is that even if the firm could benefit when each is deployed alone, the firm could be hurt by deploying both. Configuring the IDS and the firewall optimally eliminates the conflict between them, ensuring that if the firm benefits from deploying each of these technologies when deployed alone, it will always benefit from deploying both. When optimally configured, we find that these technologies complement or substitute each other. Furthermore, we find that while the optimal configuration of an IDS does not change whether it is deployed alone or together with a firewall, the optimal configuration of a firewall has a lower detection rate (i.e., allowing more access) when it is deployed with an IDS than when deployed alone. Our results highlight the complex interactions between firewall and IDS technologies when they are used together in a security architecture, and, hence, the need for proper configuration to benefit from these technologies.

Key words: information security; software configuration; information security technologies; firewalls; intrusion detection systems; economics of information systems; analytical modeling
History: Paulo Goes, Senior Editor; Debabrata Dey, Associate Editor. This paper was received on September 26, 2006, and was with the authors $5\frac{3}{4}$ months for 2 revisions. Published online in *Articles in Advance* February 26, 2009.

1. Introduction

Software configuration refers to the process of setting software quality parameters to meet specific user requirements. Proper configuration is particularly critical for information technology (IT) security software, as evidenced by frequent warnings by security experts about risks from using default ("out-of-the-box") settings (McCarthy 1998). The commonly cited risk is that default configurations are insecure and using them allows hackers to more easily exploit known software vulnerabilities (Piessens 2002). Configuration is also important from an operational economics perspective. For instance, Software Engineering Institute (SEI) guidelines (Allen et al. 1998) for installing security software recommend that firms adjust configuration to balance their own security and operational requirements.[1] Furthermore, configuration assumes more significance in an IT security context because firms frequently deploy a layered security architecture comprised of diverse security technologies (Cavusoglu 2003).

The primary goal of IT security is balancing the conflicting needs of information protection and infor-

[1] Similar observations have been made for explosives detection systems used by airports (NMAB 1998).

mation access. To achieve this goal, firms typically deploy technologies such as firewalls and intrusion detection systems (IDS), along with other security measures such as manual investigations and physical access controls. The deployment of multiple technologies makes configuration challenging because the configuration decision about one technology has ramifications on the configuration decisions of others, and, consequently, configuration decisions have to be coordinated to achieve the optimal overall performance. Industry reports highlight the problem associated with excessive false alarms generated by IDS that are not configured properly (Gartner 2003). Apart from the configuration issue, there exists a debate within the IT security community about whether a firewall obviates the need for or complements an IDS (Magalhaes 2004, NSS 2004), illustrating the mixed experiences about the performance of these technologies when deployed together. Axelsson (2000, p. 189) summarized the debate as follows.

> The best effort [security] is often achieved when several security measures are brought to bear together. How should intrusion detection collaborate with other security mechanisms to this synergy effect? How do we ensure that the combination of security measures provides at least the same level of security as each applied singly would provide, or that the combination does in fact lower the overall security of the protected system?

He continued, noting that "...they [these questions] remain largely un-addressed by the research community. This is perhaps not surprising since many of these questions are difficult to formulate and answer." The research described in this paper seeks to shed light on the above questions raised by the security community regarding the configuration of and interaction between security technologies.

Our major goal is to understand the strategic interaction between a firewall and an IDS in managing security risks to provide normative guidelines to firms on security technology deployment decisions. Firewalls and IDS are historically considered to address distinct IT security objectives, however, because firewalls are typically implemented to prevent intrusions and IDS to detect intrusions, these two controls are not independent of each other in their operations. Controlling external access via a firewall at the perimeter may prevent the damage that illegal external users can inflict on the firm. But the firewall cannot stop the attacks perpetrated by internal users of the system. In addition, the firewall reduces the traffic into the system, thereby affecting the potential value that an IDS can provide. On the other hand, deploying an IDS may discourage both internal and external users from committing an unauthorized act because they face the risk of being detected. The IDS may also lessen the importance of controlling access at the perimeter, therefore limiting the potential role that a firewall can play in security. This trade-off gets even more complicated given that the firm can configure these security technologies within their quality profiles. One may expect that IDS and firewall substitute (i.e., diminish the value of) each other. However, it is not clear whether this intuition is always valid, and whether there are cases in which the two technologies complement (i.e., enhance the value of) or conflict with (i.e., eliminate the value of) each other. Furthermore, it is not obvious whether configuration can alter the interaction effect between the two security technologies. Hence, the firm is faced with very complex decisions when it considers using a firewall and an IDS in its security architecture: *which security technologies to deploy* and *how to configure them*.

Cavusoglu et al. (2005) analyze the value of deploying an IDS for IT security management. In their model, they assume that the firm implements only an IDS and consider only internal users that do not have to pass through a firewall.[2] They do not address the question of how a firewall and an IDS interact with each other. Furthermore, they do not analyze how the deployment of an IDS affects the firm's decision about allowing access to external users. Finally, their analysis does not offer any answer to the crucial question of whether more controls result in better security risks. To address these questions, we build on the model of Cavusoglu et al. (2005) by adding a firewall to the firm's security architecture. We distinguish between internal and external users of the system. We also endogenize the firm's external access control policy when there is no firewall in the security architecture. The implications of this general model go well beyond the implications of prior models that considered security technologies individually. With these

[2] Alternatively, the lack of a firewall in their model can be interpreted that the firm allows all external users to access the system without any screening at the perimeter.

new elements, we explore (i) the optimal configuration decisions for a firewall and an IDS, (ii) the interaction effect between the firewall and the IDS, and (iii) the impact of configuration on the firm's access control policy and on the type of interaction between the firewall and the IDS.

Our analysis provides new significant insights into IT security technology deployment decisions that consider the interaction between security technologies and their configurations. We show that deploying a technology, whether it is a firewall or an IDS, could hurt the firm if its configuration is not optimized for the firm's environment. A more serious consequence of deploying the two technologies with suboptimal configurations is that even if the firm could benefit when each is deployed alone, contrary to what one may expect, the firm could be hurt if it deploys both. Configuring the IDS and the firewall optimally eliminates the conflict between them, ensuring that if the firm benefits from deploying each of these technologies when deployed alone, it will also benefit from deploying both. When optimally configured, while the deployment of an IDS diminishes the value of a firewall and vice versa (that is, the IDS and the firewall substitute each other) under some conditions, a surprising result is that an IDS and a firewall complement each other under other conditions. The complementarity effect can occur provided it is optimal for the firm to prohibit external access in the absence of a firewall. We find that an optimally configured IDS, in addition to serving as a detection control, serves as an access control also. Because it functions as a deterrent to attackers, an optimally configured IDS may enable the firm to allow external access that the firm prohibits otherwise. While the optimal configuration of an IDS does not change whether a firewall is deployed, a firewall should be configured to operate at a lower detection rate (i.e., allowing more access) when it is used with an IDS than without.

Our findings offer important insights into the debate mentioned earlier about how intrusion detection and other security mechanisms should collaborate to achieve the best security risk management. While the conventional wisdom is that the best security is achieved only when several technologies are brought together, we find that this is not always the case. Instead of a synergy effect, a firewall and an IDS, if suboptimally configured, could have a conflicting effect, leading to a deterioration of security. One way to ensure a synergistic effect is to configure the two technologies jointly prior to deployment.

The remainder of the article is organized as follows. We review the relevant literature in §2. We discuss the configuration problem and our model in §3. We derive the equilibrium hacking and investigation strategies in §4. In §5, we analyze the value of security technologies and subsequently the interaction effect between them when they are deployed at their default configurations. In §6, we analyze optimal configuration decisions and the resulting impact on the interaction effect. In §7, we show the robustness of our results by analyzing alternative model specifications. In §8, we discuss the implications of our results and future research directions.

2. Related Literature

Research on information security technologies has analyzed both the technical and the economic aspects of the design and implementation of security controls. The technical research has focused largely on the design of algorithms related to firewalls, IDS, and others, such as encryption. Various approaches to firewall design are discussed in Holden (2004) and Gouda and Liu (2004). IDS design uses two broad approaches. The significant developments in signature-based IDS are highlighted in Garvey and Lunt (1991), Porras and Kemmerer (1992), Ilgun (1992), Lunt (1993), Kumar and Spafford (1996), and Monrose and Rubin (1997). The algorithms used in anomaly-based IDS are presented in Lunt and Jagannathan (1988), Lunt (1990), Lunt (1993), D'haeseleer et al. (1996), Porras and Neumann (1997), Neumann and Porras (1999), and Zamboni and Spafford (1999). Because firewalls and IDS are deployed in a variety of environments with different security-related cost structures, these technologies are designed so that their behavior can be tuned by individual firms through the process of configuration to fit their operating environments. We focus on configuration issues faced by firms that deploy these technologies; consequently, we assume that their technical design is exogenous to our problem.

Research on the economics of security technologies is based on the notion that security technologies are imperfect, and, therefore, policies based on the cost-benefit trade-off are required to support these technology implementations. The imperfections of security technologies are typically captured using false-positive and false-negative error rates. Because different firms may have different tolerance levels for error rates and different acceptable levels for detection rates, researchers have begun to investigate how to configure a given security technology to fit a specific deployment environment. Cavusoglu et al. (2005) analyze the value of IDS and show that IDS offer a positive value only when they deter hackers. Ulvila and Gaffney (2004) propose a decision analysis approach to configure IDS. Cavusoglu and Raghunathan (2004) compare decision analysis and game theoretic approaches to configure IDS and show that the game theoretic approach is superior. Ogut et al. (2008) examine various waiting time policies to deal with the problem of false alarms in IDS. Yue and Baghci (2003) consider how to tune the quality parameters of a firewall to maximize its benefit. Every study in this stream of research focuses on a single technology. None considers configuration when multiple technologies are deployed as part of a layered security architecture. Therefore, they do not address interaction between security technologies.

Our study contributes to the growing literature on the economics of information security. Researchers have considered the economic incentives of parties involved in information security to address various issues, such as security vulnerability discovery and disclosure (Schechter 2002, Ozment 2004, Cavusoglu et al. 2007, Nizovtsev and Thursby 2005), security information sharing (Gordon et al. 2003, Gal-Or and Ghose 2005), patch management (Cavusoglu et al. 2008; August and Tunca 2006, 2008), and security investments and risk management (Ogut et al. 2005). However, this stream of research does not model specific security technologies, and, therefore does not provide insights into how these technologies should be configured to minimize the cost of security.

3. The Model

We model an environment in which a firm is evaluating the adoption of security technologies to extend its enterprise by providing access to outside vendors and partners. The common practice in such contexts is to implement a "defense-in-depth" IT security architecture (Whitman and Mattord 2003). In this architecture, three layers—the firewall at the network (periphery) layer, the IDS at the host (middle) layer, and manual investigation at the data (interior) layer—are used to provide security. Firewalls are implemented to control the traffic between a trusted network ("Internal") and untrusted ("External") networks. The internal network is trusted because the firm can exercise its own security policies over the network, but the firm does not have such a control over external networks. Even though external networks are untrusted, the firm may still want to allow communications from them. In this setup, a firewall controls the traffic between internal and external networks using an Access Control List (ACL), and an IDS monitors events occurring in host and internal systems and warns human experts about suspected intrusions. A key difference between firewall and IDS technologies is that while a firewall takes actions against a suspected intrusion by blocking the traffic, an IDS sends only an alarm to the security administrator, who may terminate the user's session.[3] Another difference is that although an IDS can detect intrusions originating from both internal and external networks, a firewall can prevent intrusions coming from external networks only.

Both a firewall and an IDS are configurable within their design profiles. The design profile of a firewall or an IDS is depicted by a receiver operating characteristic (ROC) curve. The ROC curve relates the probability of true detection (stopping an illegal external user in the case of a firewall, and raising an alarm for an unauthorized activity of a user in the case of an IDS) and the probability of false detection (stopping a legal external user in the case of a firewall and raising an alarm for a normal activity of a user in the case of an IDS). The shape of the ROC curve depends on the algorithm used by the technology. In a typical ROC curve, the probability of true detection is higher than the probability of false detection, and the probability of true detection is an increasing concave function of the probability of false detection (Trees 2001). We discuss the derivation of an ROC curve in §3.2. Security

[3] There are also active IDS that take action against suspected intrusions on their own. Because of high false positives, many commercial IDS do not support active response. Therefore, we assume that the firm uses a passive IDS.

administrators can configure an IDS or a firewall to operate at a specific point on the ROC curve by tuning certain parameters in an IDS or by modifying the ACL in a firewall.

3.1. Model Description

We consider two types of users. All internal users have access to the system from inside the firewall, i.e., they do not go through the firewall. External users access the system from outside the firewall, and, hence, are validated by the firewall, if one exists, before accessing the system. We assume that ε fraction of users is external users. We also classify users into two groups: legal and illegal. Legal users are those that offer a positive payoff to the firm if they do not abuse their privileges whereas illegal users do not offer a positive payoff to the firm under any circumstance. While all internal users are legal users of the system, only a proportion ζ of external users are legal users. The reason for this difference between internal and external users is that, as explained previously, the firm can control its internal users by deploying its own authentication and other access control mechanisms, but the firm does not have a similar control over external users.[4] Clearly, an ideal firewall will allow all legal external users and stop all illegal external users. After gaining access to the system, a user (internal or external) may choose to abuse (intrude) the system by executing unauthorized actions. The objective of an IDS is to detect these intrusions by internal as well as external users.

A user (internal or external) that abuses the system, whom we refer to as a hacker, derives a benefit of μ, if the intrusion is undetected. If the intrusion is detected, the hacker incurs a penalty of β for a net benefit of $(\mu - \beta)$. We assume that $\mu \leq \beta$; that is, a hacker that is detected does not enjoy a positive benefit. Users that gain access to the system choose to hack depending on factors such as μ, β, and the likelihood that they will get caught. We denote the probability of hacking for a user as ψ. An illegal external user could also derive an additional utility solely from cracking the firewall; that is, even if the illegal external user does not abuse the system after gaining access, he/she may enjoy some utility. Because this additional utility does not change our results, we have normalized it to zero.

We assume that the benefit to the firm under normal use by a legal user is ω. When a user hacks the system and the hacking is undetected, the firm incurs a damage of d. However, the firm can detect hacking by manually investigating user log files. Firms can confirm or rule out hacking only through manual investigation. In general, manual investigation is too costly to be done all the time. When the firm does not deploy an IDS, the firm may manually investigate a proportion of users. When the firm deploys an IDS, the firm may investigate a proportion of users that generate alarms from the IDS and a possibly different proportion of users that do not generate alarms. The firm incurs a cost of c each time it performs a manual investigation. We assume that manual investigations confirm or rule out intrusions with certainty.[5] If the firm detects hacking, the firm prevents or recovers a fraction, $\phi \leq 1$, of d. It is reasonable to assume that $c \leq \phi d$ so that the firm's cost of investigation is not higher than the benefit it gets if it detects an intrusion. The payoffs to the firm under different scenarios of system usage are given in Table 1.

The firm may deploy only a firewall, only an IDS, both a firewall and an IDS, or neither in its security architecture. We measure the effectiveness of a firewall through two parameters: P_D^F and P_F^F. P_D^F is the probability that the firewall stops an illegal external user. P_F^F is the probability that the firewall stops a legal external user. In practice, the value of P_F^F is likely to be low, and P_D^F is likely to be high. However, for a given firewall, these parameters are not independent. The security stance of the firm, reflected by its configuration decision, determines the combination of P_D^F and P_F^F for the firewall deployed. While the paranoid approach in configuration leads to a high P_D^F and P_F^F, the open approach results in a low P_D^F and P_F^F (Holden 2004). For a given firewall, we capture the relationship between P_D^F and P_F^F as $P_D^F = (P_F^F)^{r_F}$, where r_F captures the technology profile of the firewall. We derive this functional form for the ROC curve in §3.2.

[4] Although all internal users are assumed to be legal, they can still misuse their privileges, and our model captures this aspect. Our model can also be easily extended to the case where a proportion of internal users is assumed to be illegal. The results do not change qualitatively.

[5] Our results do not change qualitatively when manual investigation is imperfect.

Table 1 The Payoffs to the Firm

	Normal use	Undetected intrusion	Detected intrusion
Internal user	ω	$-d$	$-(1-\phi)d$
Legal external user	ω	$-d$	$-(1-\phi)d$
Illegal external user	0	$-d$	$-(1-\phi)d$

The model for the IDS is similar to that of a firewall and is identical to that in Cavusoglu et al. (2005). Specifically, P_D^I is the probability that the IDS raises an alarm for an intrusion, P_F^I is the probability that the IDS raises an alarm when there is no intrusion, and $P_D^I = (P_F^I)^{r_I}$, where r_I captures the technology profile of the IDS.

3.2. Derivation of ROC Curve

The ROC curve for a security technology can be derived analytically or experimentally (Durst et al. 1999, Lippmann et al. 2000, Yue and Bagchi 2003). In the following paragraph, we illustrate the analytical derivation of the ROC curve for a firewall. A similar approach is also used to derive the ROC curve for an IDS, and is discussed in Cavusoglu et al. (2005). Consider a firm that is configuring the ACL for a firewall. The firm has decided to put an external site (say an IP address) in the "deny" or "permit" list of a firewall based on the level of threat ("threat index") associated with the traffic coming from that site. The threat index represents the estimated probability that a user from that site is an illegal user. The firm includes a site in the "permit" list only when the threat index for that site is below a threshold value. For instance, Cisco PIX firewall relies on this type of index values to deny or permit traffic. Similarly, IDS classify a user as a hacker or not based on whether a numerical score computed from the transaction history (i.e., anomaly index) exceeds a threshold value.

Let the estimated threat index for a site be x, and the threshold value that determines whether to put the site in the "permit" or "deny" list be t. Let a site for which $x > t$ be put in the "deny" list. We assume that $f_T(x)$ and$f_U(x)$ are the probability density functions of x for "trusted" sites and "untrusted" sites, respectively. We further assume that $f_U(x)$ stochastically dominates $f_T(x)$, i.e., $F_T(x) \geq F_U(x)$, $\forall x$. This assumption implies that trusted sites are less of a threat than untrusted sites. It then follows that

$$P_D^F = \int_t^\infty f_U(x)\,dx \quad \text{and} \quad P_F^F = \int_t^\infty f_T(x)\,dx.$$

We can easily show that $P_D^F > P_F^F$. Furthermore, P_D^F is an increasing concave function of P_F^F for many probability distributions. The exact shape of the ROC curve depends on the probability density function of x. We assume that x follows an exponential distribution. Exponential distributions, besides being analytically tractable, capture the skewed nature of the threat index of trusted and untrusted sites very well.[6] If x for trusted and untrusted sites follow exponential distributions with parameters θ_T and θ_U, $\theta_U > \theta_T$, respectively, then we get

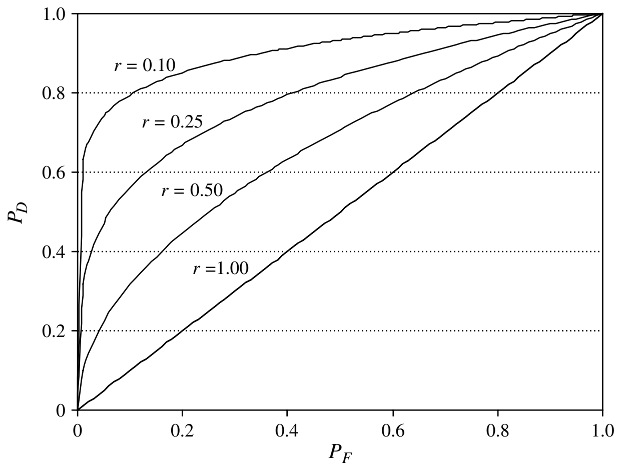
$$\begin{aligned} P_D^F &= \int_t^\infty \theta_U e^{-(\theta_U x)}\,dx = e^{-\theta_U t}, \\ P_F^F &= \int_t^\infty \theta_T e^{-(\theta_T x)}\,dx = e^{-\theta_T t}, \\ &\Rightarrow\ P_D^F = (P_F^F)^{r_F}, \end{aligned}$$

where $r_F = \theta_T/\theta_U$ is between zero and one. The parameter r_F represents the technology profile of the firewall. The lower the value of r_F, the better the quality of the firewall. Figure 1 shows sample ROC curves for various values of r. For both the firewall and the IDS, we use this power function for the ROC curve in our analysis.

We make two observations about our modeling of the system access and protection problem. First, a user is penalized only when the firm detects abuse of the system. If an illegal external user attempts to gain access and is stopped by the firewall, he/she does not incur any penalty. This assumption is reasonable because we know that firewalls routinely stop numerous hacking attempts by users, and these users are not (and cannot be) penalized. Second, in our model, we normalize the payoffs such that cracking a firewall alone does not cause any damage to the firm. The firm incurs damage only when the user abuses the system after gaining access. This assumption is reasonable because a significant proportion of intruders, known as sport hackers, are not interested in doing anything

[6] Cavusoglu and Raghunathan (2004) also use exponential distributions in deriving the ROC curve for an IDS.

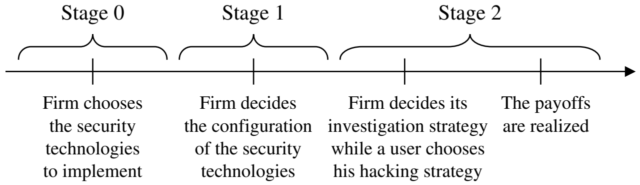
Figure 1 ROC Curves for Various Values of *r*



more than penetrating the firm's firewall mechanism to "take a look around" (Campbell et al. 2003, p. 242). Though the firm does not incur any direct damage when an illegal user gains access, there is an indirect cost in that an illegal user can never benefit the firm, whereas a legal user can. Note also that even if the firm is assumed to incur a fixed cost when an illegal user cracks the firewall, the equilibrium that we derive and our qualitative results about the value of firewall and IDS and interactions between a firewall and an IDS do not change.

We model the security problem as a multistage game with observed actions between the firm and system users. Figure 2 shows the timeline. First, the firm determines its security architecture, i.e., it decides whether to implement only a firewall, only an IDS, both a firewall and an IDS, or neither a firewall nor an IDS. Then, in stage 1, the firm chooses the configuration of technologies it decided to implement in stage 0. Then, given the configuration, the firm sets its manual investigation strategy while users set their hacking strategies. Finally, the payoffs are realized. We assume that the firm and users are risk neutral.

Figure 2 The Timeline for the Game


Stage 0
Stage 1
Stage 2
Firm chooses the security technologies to implement
Firm decides the configuration of the security technologies
Firm decides its investigation strategy while a user chooses his hacking strategy
The payoffs are realized

The rationale for the timeline is that configuration decisions are more strategic (long-term) and are more difficult to change compared to manual investigation strategies because changes to software configurations often require extensive testing prior to implementation.[7] We assume that all parameters are common knowledge to all players. Thus, in stage 1 of the game, the firm makes its configuration decision by rationally anticipating its and users' best responses in stage 2 of the game. In stage 2, both the firm and users observe the configuration decisions of stage 1, and simultaneously choose their strategies. Thus, we assume that in stage 2, users know whether the firm has implemented one, both, or, none of the technologies, and their configurations. This assumption is reasonable because it is well known that attackers, both internal and external, acquire knowledge about hosts and networks and their vulnerabilities using a variety of techniques including social engineering, probing, and IP fingerprinting before launching their attacks (Whitman and Mattord 2003). Furthermore, it is possible that internal users may have better information about the firm's decisions in stage 1 than external users. We capture this difference by assuming that internal users have perfect knowledge about the firm's decisions in stage 1, but external users are uncertain about configuration decisions. An external user's belief about the firewall configuration has a probability density function $g^F(p_D^F)$ with mean equal to the true firewall configuration P_D^F and support $[\underline{P}_D^F, \bar{P}_D^F]$. Similarly, an external user's belief about the IDS configuration has a probability density function $g^I(p_D^I)$ with mean equal to the true IDS configuration P_D^I and support $[\underline{P}_D^I, \bar{P}_D^I]$. These probability functions imply that users' beliefs about configurations are unbiased.

4. Model Analysis: Equilibrium in Stage 2

We perform the analysis using backward induction. That is, we first derive the equilibrium for the firm's

[7] For instance, in a firewall, the sequence of rules is critical in implementing a security policy; adding, deleting, or modifying a rule could mask (contradict) other rules in a firewall. Therefore, potential contradictions have to be carefully analyzed before making a change to the firewall rule set. Such issues do not arise in the case of manual investigation strategies.

investigation strategy and a user's hacking strategy given the firm's implementation and configuration strategies. Note that the firm can choose to implement and configure one, both, or none of the security technologies in stage 1 of the game. Subsequently, we determine the firm's optimal implementation and configuration strategy. The cases when the firm implements only a firewall, only an IDS, or neither a firewall nor an IDS are special cases of the more general case where the firm implements both a firewall and an IDS. Consequently, we derive the equilibrium strategies for the firewall plus IDS case and then specialize them to other cases.

When the firm implements a firewall and an IDS, the strategy of a user who has gained access to the system, S^U, is to hack, H, or not hack, NH, i.e., $S^U \in \{H, NH\}$. The firm's strategy, S^F, is to investigate, I, or not investigate, NI, the user in each of the two states: alarm and no-alarm. That is, $S^F \in \{(I, I), (I, NI), (NI, I), (NI, NI)\}$, where the first element in each pair specifies the firm's action when the firm observes an alarm from the IDS, and the second element is the firm's action when it does not observe an alarm from the IDS. For example, (I, NI) implies that the firm investigates the user if it receives an alarm from the IDS for that user and does not investigate if it does not receive an alarm.

We derive the subgame perfect Nash equilibrium for the game between the firm and users. To do that, we first obtain the Nash equilibrium of the simultaneous game in stage 2. Let ρ_1 and ρ_2 denote the firm's investigation probabilities when the IDS raises an alarm and when the IDS does not raise an alarm, respectively. Table A.1 in the appendix provides the list of all probability expressions required to compute the expected payoff for the firm.

The firm's expected payoffs per user in the alarm and no-alarm states given that the user gains access are given by the following:

$$\begin{aligned}F_A(\rho_1, \psi) &= \omega(P_{I,\,\text{no-hack}\,|\,\text{Alarm}} + P_{E,\,\text{legal, no-hack}\,|\,\text{Alarm}}) - \rho_1 c\\ &\quad - P_{\text{hack}\,|\,\text{Alarm}}(1-\rho_1)d - P_{\text{hack}\,|\,\text{Alarm}}\rho_1(1-\phi)d\\ F_{NA}(\rho_2, \psi) &= \omega(P_{I,\,\text{no-hack}\,|\,\text{No-alarm}} + P_{E,\,\text{legal, no-hack}\,|\,\text{No-alarm}})\\ &\quad - \rho_2 c - P_{\text{hack}\,|\,\text{No-alarm}}(1-\rho_2)d\\ &\quad - P_{\text{hack}\,|\,\text{No-alarm}}\rho_2(1-\phi)d.\end{aligned}$$

The firm's overall expected payoff per user is

$$\begin{aligned}F(\rho_1, \rho_2, \psi) &= P_{\text{Access}}(P_{\text{alarm}\,|\,\text{Access}}F_A(\rho_1, \psi)\\ &\quad + P_{\text{no-alarm}\,|\,\text{Access}}F_{NA}(\rho_2, \psi)).\end{aligned}$$

An internal user's expected payoff from hacking is given by

$$H_I(\rho_1, \rho_2, \psi) = \mu\psi - \beta(\rho_1 P_D^I + \rho_2(1-P_D^I))\psi.$$

An external user's expected payoff from hacking, after gaining access, is given by

$$\begin{aligned}&H_E(\rho_1, \rho_2, \psi)\\ &\quad = \mu\psi - \beta\psi\int_{\underline{P}_D^I}^{\bar{P}_D^I}(\rho_1 p_D^I + \rho_2(1-p_D^I))\cdot g^I(p_D^I)\,dp_D^I\\ &\quad = \mu\psi - \beta(\rho_1 P_D^I + \rho_2(1-P_D^I))\psi.\end{aligned}$$

The firm maximizes $F_A(\rho_1, \psi)$ when it gets an alarm from the IDS, and $F_{NA}(\rho_2, \psi)$ when it does not get an alarm. A user maximizes his/her payoff.

The following proposition shows the Nash equilibrium strategies for the firm and a user.

Proposition 1. *The equilibrium for stage* 2 *of the game when the firm implements a firewall and an IDS is given by the following*:

$$\begin{cases}\psi^* = \dfrac{cP_F^I}{d\phi P_D^I - c(P_D^I - P_F^I)}, \quad \rho_1^* = \dfrac{\mu}{P_D^I\beta}, \quad \rho_2^* = 0\\ \quad \textit{if } \dfrac{\mu}{\beta} \le P_D^I,\\ \psi^* = \dfrac{c(1-P_F^I)}{c(P_D^I - P_F^I) + (1-P_D^I)d\phi}, \quad \rho_1^* = 1, \quad \rho_2^* = \dfrac{\mu - P_D^I\beta}{(1-P_D^I)\beta}\\ \quad \textit{otherwise}. \qquad \square\end{cases}$$

{The proofs for all our main results are available in Part A of the online supplement to this paper.[8]}

Proposition 1 is intuitive. A sufficiently high detection rate for the IDS reduces hacking. Therefore, the firm will not inspect any user who does not raise an alarm, and in fact, it may inspect only a fraction of users that raise an alarm. On the other hand, a low detection rate results in a high level of hacking, and

[8] All proofs are contained in an online supplement to this paper that is available on the *Information Systems Research* website (http://isr.pubs.informs.org/ecompanion.html).

therefore, the firm will not only investigate every user who raises an alarm, but also a fraction of users that do not raise an alarm. The equilibrium when the firm implements only a firewall, only an IDS, or neither an IDS nor a firewall can be derived from Proposition 1 by making appropriate substitutions to the firewall and IDS quality parameters. By substituting $P_D^I = P_F^I = 0$ in Proposition 1, we get the equilibrium when the firm implements only a firewall. The substitutions imply that no alarm is generated, and, by implication, no false alarm is generated. Notice that in the firewall only case, ρ_1^* is not meaningful because it represents the probability of investigation when there is an alarm. The case when the firm implements only an IDS is more complex because two possibilities arise when there is no firewall. In the first possibility, which we refer to as the *no-external-access* (NEA) scenario, the firm does not allow external access and restricts access to internal users only. In the second possibility, which we refer to as the *full-external-access* (FEA) scenario, the firm allows external access despite the absence of a firewall. The former scenario can be analyzed by setting $P_D^F = P_F^F = 1$ in our model, and the latter scenario is equivalent to substituting $P_D^F = P_F^F = 0$. For the case when the firm implements neither a firewall nor an IDS, we substitute $P_D^I = P_F^I = 0$, $\rho_1 = 0$, $\rho_2 = \rho$, and, depending on whether we model the FEA or the NEA scenario, either $P_D^F = P_F^F = 0$ (FEA) or $P_D^F = P_F^F = 1$ (NEA). Based on these substitutions, we obtain the following result.

Corollary 1. *For stage* 2 *of the game*, (a) *the equilibrium when the firm implements only the IDS, for both NEA and FEA scenarios, is identical to the equilibrium in the firewall plus IDS case given in Proposition* 1, (b) *the equilibria for the firewall only case and the no technology case, for both NEA and FEA scenarios, are identical and are given by the strategy profile* ($\rho^* = \mu/\beta$, $\psi^* = c/d\phi$). □

The firm's expected equilibrium payoffs under various security architectures are given in Table 2.

It is clear from expected payoff expressions for the no-technology case that the firm will allow external access even when it implements neither a firewall nor an IDS, iff $\Lambda = (c/\phi)/(\omega\zeta(1-(c/d\phi))) \leq 1$. The numerator and the denominator are, respectively, the expected cost and the expected benefit from allowing access to an external user. Hence we denote the quantity Λ as the *cost-to-benefit-ratio-for-external-access*.

5. The Value of a Firewall and an IDS Under Default Configurations

We first analyze the value of a firewall and an IDS to the firm if the firm uses default configurations. That is, parameters P_D^F (hence, P_F^F) and P_D^I (hence, P_F^I) are exogenously specified and may not be optimal for the firm. Then, we consider the case in which the firm chooses optimal values for these parameters to assess the value with configuration. We compute the value of a specific technology (or both technologies) as the firm's expected payoff when it implements a specific technology (or both technologies) minus the firm's expected payoff when it does not implement any technology.[9] Even though the ROC curve for a technology relates its two quality parameters, we show them as though they are independent for clearer exposition.

5.1. The Value of Implementing Only a Firewall

Using the payoff expressions given in Table 2, we can compute the value of firewall to be

$$\varepsilon\left((1-\zeta)P_D^F\left(\frac{c}{\phi}\right) - P_F^F\zeta\left(\omega\left(1-\frac{c}{d\phi}\right)-\frac{c}{\phi}\right)\right)$$

for the FEA scenario, and

$$\varepsilon\left((1-P_F^F)\omega\zeta\left(1-\frac{c}{d\phi}\right)-\left(\frac{c}{\phi}\right)(1-\zeta P_F^F-(1-\zeta)P_D^F)\right)$$

for the NEA scenario. Thus, we have the following result for the firewall.

Proposition 2. *For the default configuration scenario, the value of implementing only a firewall is positive iff*

$$\frac{P_F^F}{\zeta P_F^F+(1-\zeta)P_D^F} < \Lambda < \frac{(1-P_F^F)}{\zeta(1-P_F^F)+(1-\zeta)(1-P_D^F)}. \quad \square$$

A high cost-to-benefit-ratio-for-external-access will make prohibiting external access superior to providing external access even with the help of a firewall. On the other hand, a low value for this ratio

[9] Our value analysis assumes that the cost of implementing a control is normalized to zero. This is a typical assumption in information economics (Christensen and Feltham 2005). The idea is that a security control will not be implemented unless it is valuable.

Table 2 **Firm's Equilibrium "Payoff" Under Various Security Architectures**

Security architecture	Firm's payoff
No technology	
NEA	$\dfrac{(1-\varepsilon)(\omega(d\phi-c)-cd)}{d\phi}$
FEA	$\dfrac{\omega(d\phi-c)(1-\varepsilon(1-\zeta))-cd}{d\phi}$
Firewall only	$\dfrac{\omega(d\phi-c)(1-\varepsilon+(1-P_F^F)\varepsilon\zeta)-cd(1-P_D^F\varepsilon+(P_D^F-P_F^F)\varepsilon\zeta)}{d\phi}$
IDS only	
NEA	$\dfrac{(1-\varepsilon)(\omega(c-d\phi)P_D^I+cdP_F^I)}{(c-d\phi)P_D^I-cP_F^I}, \quad \text{if } \dfrac{\mu}{\beta}\le P_D^I$
	$\dfrac{(1-\varepsilon)((d\phi-c)(\omega(1-P_D^I)+c(P_D^I-P_F^I))-cd(1-P_F^I))}{c(P_D^I-P_F^I)+d\phi(1-P_D^I)}, \quad \text{if } \dfrac{\mu}{\beta}>P_D^I$
FEA	$\dfrac{\omega(c-d\phi)(1-\varepsilon(1-\zeta))P_D^I+cdP_F^I}{(c-d\phi)P_D^I-cP_F^I}, \quad \text{if } \dfrac{\mu}{\beta}\le P_D^I$
	$\dfrac{(d\phi-c)(c(P_D^I-P_F^I)+\omega(1-\varepsilon(1-\zeta))(1-P_D^I))-cd(1-P_F^I)}{c(P_D^I-P_F^I)+d\phi(1-P_F^I)}, \quad \text{if } \dfrac{\mu}{\beta}>P_D^I$
IDS and firewall	$\dfrac{\omega(c-d\phi)(1-\varepsilon+(1-P_F^F)\varepsilon\zeta)P_D^I+cd(1-\varepsilon P_D^F+\varepsilon\zeta(P_D^F-P_F^F))P_F^I}{(c-d\phi)P_D^I-cP_F^I}, \quad \text{if } \dfrac{\mu}{\beta}\le P_D^I$
	$\dfrac{(c(P_D^I-P_F^I)(c-d\phi)+cd(1-P_F^F))((1-P_D^F\varepsilon)+(P_D^F-P_F^F)\varepsilon\zeta)}{-c(P_D^I-P_F^I)-d(1-P_D^I)}+\dfrac{(c-d\phi)(1-P_D^I)w(1-\varepsilon+(1-P_F^F)\varepsilon\zeta)}{-c(P_D^I-P_F^I)-d(1-P_D^I)}, \quad \text{if } \dfrac{\mu}{\beta}>P_D^I$

will make unrestricted external access superior to restricted external access using a firewall. Thus, a firewall is valuable only for the intermediate range of values for cost-to-benefit-ratio-for-external-access. Of course, this range depends on the firewall quality. A higher (lower) P_D^F (P_F^F) for the same P_F^F (P_D^F) increases the firewall quality and the range in which the firewall offers a positive value. The upper limit of the region specified in Proposition 2 represents the accuracy of the firewall in allowing external traffic, measured as the ratio of the likelihood that a legal user is allowed by the firewall to the likelihood that any external user is allowed by the firewall. The lower limit of the region represents the inaccuracy of the firewall in dropping external traffic, measured as the ratio of the likelihood of a legal external user being dropped by the firewall to the likelihood of any external user being dropped by the firewall. Clearly, the upper limit is greater than 1 while the lower limit is less than 1, which implies that a firewall can be beneficial to some firms that allow external traffic, as well as to some other firms that do not allow external traffic, when they do not deploy any technology.

5.2. The Value of Implementing Only an IDS

The value of IDS is given in Table 3. We highlight the significant finding as Proposition 3.

Proposition 3. *For the default configuration scenario, the value of implementing only an IDS is positive iff* $(\mu/\beta)\le P_D^I$. □

The value of IDS can be further explained by isolating the two effects it has on a firm. First, it alters the firm's probability of manual investigations by allowing more targeted investigations. Second, it changes the users' hacking probability by altering the probability of a hacker getting caught. We can write the value of IDS as the following:

$$\begin{aligned}
&F_{\text{IDS}}^*(\rho_1^*,\rho_2^*,\psi_{\text{IDS}}^*)-F_{\text{No-IDS}}^*(\rho^*,\psi_{\text{No-IDS}}^*)\\
&\quad=[F_{\text{IDS}}^*(\rho_1^*,\rho_2^*,\psi_{\text{No-IDS}}^*)-F_{\text{No-IDS}}^*(\rho^*,\psi_{\text{No-IDS}}^*)]\\
&\qquad+[F_{\text{IDS}}^*(\rho_1^*,\rho_2^*,\psi_{\text{IDS}}^*)-F_{\text{IDS}}^*(\rho_1^*,\rho_2^*,\psi_{\text{No-IDS}}^*)].
\end{aligned}$$

The first term on the right-hand side of the above equation represents the increase in the firm's payoff if the firm alters its investigation strategy but users

Table 3 The Value of IDS

Region	Condition(s)	The value of IDS	Is IDS beneficial?
$\frac{\mu}{\beta} > P_D^I$	$\Lambda < \frac{\omega\zeta(1-P_D^I)+c(P_D^I-P_F^I)}{\omega\zeta(1-P_F^I)}$	$-\frac{c(P_D^I-P_F^I)(d\phi-c)(d(1-\phi)+\omega(1-\varepsilon(1-\zeta)))}{d\phi(c(P_D^I-P_F^I)+d\phi(1-P_D^I))}$	No
	$\frac{\omega\zeta(1-P_D^I)+c(P_D^I-P_F^I)}{\omega\zeta(1-P_F^I)} < \Lambda < 1$	$-\frac{c(P_D^I-P_F^I)(d\phi-c)(1-\varepsilon)(d(1-\phi)+\omega)}{d\phi(c(P_D^I-P_F^I)+d\phi(1-P_D^I))} - \frac{\varepsilon((d\phi-c)\omega\zeta-cd)}{d\phi}$	No
	$\Lambda > 1$	$-\frac{c(P_D^I-P_F^I)(d\phi-c)(1-\varepsilon)(d(1-\phi)+\omega)}{d\phi(c(P_D^I-P_F^I)+d\phi(1-P_D^I))}$	No
$\frac{\mu}{\beta} \leq P_D^I$	$\Lambda < 1$	$\frac{c(P_D^I-P_F^I)(d+\omega(1-\varepsilon(1-\zeta)))(d\phi-c)}{d\phi((d\phi-c)P_D^I+cP_F^I)}$	Yes
	$1 < \Lambda < \left(\frac{P_D^I}{P_F^I}\right)$	$\frac{c(P_D^I-P_F^I)(d+\omega)(1-\varepsilon)(d\phi-c)}{d\phi((d\phi-c)P_D^I+cP_F^I)} + \frac{\varepsilon((d\phi-c)P_D^I\omega\zeta-cdP_F^I)}{(d\phi-c)P_D^I+cP_F^I}$	Yes
	$\Lambda > \left(\frac{P_D^I}{P_F^I}\right)$	$\frac{c(P_D^I-P_F^I)(d+\omega)(1-\varepsilon)(d\phi-c)}{d\phi((d\phi-c)P_D^I+cP_F^I)}$	Yes

do not alter their hacking strategy after implementing the IDS. The second term represents the increase in the firm's payoff when users alter their hacking strategy in response to the change in firm's investigation strategy. Clearly, the first term incorporates the impact of the direct effect arising from targeted investigations, which we denote as the *detection effect* of the IDS. The second term incorporates the impact of the indirect (or strategic) effect arising from the change in hacking probability, which we denote as the *deterrence effect* of IDS. An analysis of these two effects on the value of IDS shows that the detection effect is positive for all parameter values, which implies that targeted investigations enabled by the IDS always help the firm. However, the deterrence effect is positive, i.e., the IDS reduces the probability of hacking only when $\mu/\beta \leq P_D^I$. When $\mu/\beta > P_D^I$, the deployment of an IDS increases the probability of hacking, and the loss from the higher level of hacking offsets the benefit from improved detection, which, in turn, hurts the firm.

Another important question is whether implementation of an IDS has any impact on the firm's decision to allow or deny external access. The following result answers this question.

Corollary 2. *When the firm implements only an IDS, it will allow external access iff* $\Lambda < P_D^I/P_F^I$. □

We noted in §4 that when the firm implements neither a firewall nor an IDS, it will allow external access when $\Lambda < 1$. Because $P_F^I < P_D^I$, in the region $1 < \Lambda < P_D^I/P_F^I$, the firm switches its policy from disallowing external access to one of allowing external access because of the IDS. The reason for this result is that the improved detection enabled by IDS deters hackers, which, in turn, decreases the cost of allowing external access.

5.3. The Interaction Effect Between a Firewall and an IDS

The expression for the value of firewall and IDS combination is complex. Therefore, we include it in Part A of the online supplement. However, an analysis of the expression reveals several insights into the interaction between an IDS and a firewall. The key research question that we address here is how the presence of one technology affects the value obtained from the other. We let $V_x =$ Value of technology x when deployed alone, and $V_{x+y} =$ Value of technologies x and y when deployed together. Then, the interaction between technologies x and y can be categorized into three types, as defined below.

Complementary: Technologies x and y are *complementary* if $V_{x+y} > \max(V_x, V_y)$ and $V_{x+y} > \max(0, V_x) + \max(0, V_y)$.

Substitutes: Technologies x and y are *substitutes* if $V_{x+y} \geq \max(V_x, V_y)$ and $V_{x+y} \leq \max(0, V_x) + \max(0, V_y)$.

Conflicting: Technologies x and y are *conflicting* if $V_{x+y} < \max(V_x, V_y)$.

The definition of complementary technologies implies that deploying both technologies results in a higher value than deploying only one and, further, that the incremental value offered by a technology is greater when the firm deploys the other technology than when it does not. In the case of substitutes, while deploying both technologies still results in a higher value than deploying only one, the incremental value obtained from a technology is less when the firm deploys the other technology as well. Finally, when the technologies are conflicting, deployment of both technologies hurts the firm, i.e., the firm realizes the greatest value by deploying only one of the technologies. Now, we present one of the most significant results of this study, which describes the interaction between the values of firewall and IDS technologies with default configurations.

Proposition 4.

(1) *When* $\mu/\beta \leq P_D^I$

- *If*

$$\left(\frac{P_F^F}{\zeta P_F^F + (1-\zeta)P_D^F}\right)\left(\frac{P_D^I}{P_F^I}\right) < \Lambda < \min\left\{\frac{P_D^I}{P_F^I}, \max\left\{\left(\frac{P_F^F}{\zeta P_F^F + (1-\zeta)P_D^F}\right)\left(\frac{P_D^I}{P_F^I}\right), \frac{1-P_F^F}{\zeta(1-P_F^F) + (1-\zeta)(1-P_D^F)}\right\}\right\},$$

then IDS and firewall substitute *each other.*

- *If*

$$\min\left\{\frac{P_D^I}{P_F^I}, \max\left\{\left(\frac{P_F^F}{\zeta P_F^F + (1-\zeta)P_D^F}\right)\left(\frac{P_D^I}{P_F^I}\right), \frac{1-P_F^F}{\zeta(1-P_F^F) + (1-\zeta)(1-P_D^F)}\right\}\right\} < \Lambda < \left(\frac{1-P_F^F}{\zeta(1-P_F^F) + (1-\zeta)(1-P_D^F)}\right)\left(\frac{P_D^I}{P_F^I}\right),$$

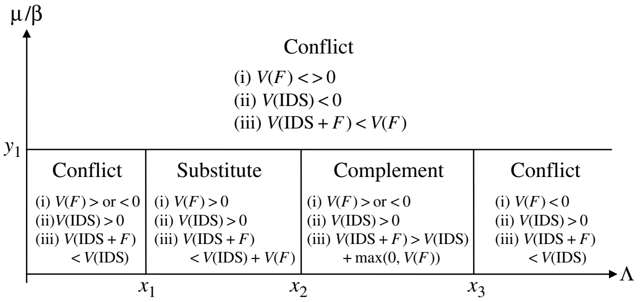
then IDS and firewall complement *each other.*

- *Otherwise, IDS and firewall* conflict *with each other.*

(2) *When* $\mu/\beta > P_D^I$: *IDS and firewall* conflict *with each other.* □

Proposition 4 can be shown graphically as Figure 3. First, the very significant and unexpected result in Proposition 4 is that deploying both a firewall and an IDS can be *worse* for a firm than deploying only one of them. The conflict effect occurs when one technology has a negative value, which is not completely surprising because the technology that has the negative value diminishes the value of the other technology when both are deployed together. However, a surprising finding is that the IDS and the firewall may conflict with each other even when each has a positive value individually. This scenario occurs in the region where $\mu/\beta \leq P_D^I$ and $(P_F^F/(\zeta P_F^F + (1-\zeta)P_D^F)) < \Lambda < (P_F^F/(\zeta P_F^F + (1-\zeta)P_D^F))(P_D^I/P_F^I)$. The explanation for the conflict between the firewall and the IDS in this region is as follows. If the firm does not deploy an IDS, then the firm finds that controlling the external access with the help of a firewall is valuable. However, when the firm deploys an IDS, the deterrence effect of the IDS reduces hacking probability, which, in turn, makes allowing unfettered external access more desirable than controlled access using a firewall. In this scenario, controlling external access with the help of a firewall conflicts with the IDS. In essence, an IDS, which is traditionally viewed as a detective control, serves as an access control because of its strategic effect on hackers. When the access control function of an IDS conflicts with that of a firewall, the firm will find it optimal to use only one of them.

Figure 3 **Interaction Between a Firewall and an IDS**



Second, firms that enjoy the complementary effect have a *higher* cost-to-benefit-ratio-for-external-access than firms that enjoy the substitution effect. The question of interest to security managers is why complementarity requires a higher cost-to-benefit-ratio-for-external-access. A firm that has a higher cost-to-benefit-ratio-for-external-access is less likely to allow external access if a firewall is absent. Suppose the firm does not allow external access if a firewall is absent so that the IDS receives traffic only from internal users. If the firm implements a firewall on top of the IDS, which necessarily means that the firm allows external access, the same IDS receives a higher traffic because now it also gets traffic from external users that have been allowed by the firewall. Because the value of an IDS is directly proportional to the number of users it receives and because users do not change their strategies when a firewall is added to the security architecture, the value of IDS can only be higher in the presence of a firewall than in the absence, which indicates the complementary effect. Now consider the case in which the firm allows external access even without a firewall, which is likely to occur when the cost-to-benefit-ratio-for-external-access is sufficiently low. In this scenario, if the IDS is augmented with a firewall, the traffic to the IDS decreases because the firewall will block some of the external users. Consequently, the incremental value of the IDS is lower in the presence of a firewall than in the absence. In essence, for a firewall and an IDS to complement each other, each technology should perform its intended function: An IDS should act solely as a detective control and should not allow the firm to open up external access, and a firewall should act solely as an access control mechanism.

$$y_1 = P_D^I, \quad x_1 = \left(\frac{P_F^F}{\zeta P_F^F + (1-\zeta)P_D^F}\right)\frac{P_D^I}{P_F^I},$$

$$x_3 = \left(\frac{1-P_F^F}{\zeta(1-P_F^F)+(1-\zeta)(1-P_D^F)}\right)\frac{P_D^I}{P_F^I}$$

$$x_2 = \min\left\{\frac{P_D^I}{P_F^I}, \max\left\{\left(\frac{P_F^F}{\zeta P_F^F + (1-\zeta)P_D^F}\right)\frac{P_D^I}{P_F^I}, \frac{1-P_F^F}{\zeta(1-P_F^F)+(1-\zeta)(1-P_D^F)}\right\}\right\}.$$

Third, we find that in the NEA scenario, a firewall that hurts the firm when deployed alone may become *beneficial* when deployed along with an IDS. A firewall hurts the firm only if the expected gain from external users is less than the expected loss from hacking. An IDS with a positive value reduces the probability of hacking. This enhances the expected benefit from external users and reduces the loss from hacking. Consequently, a firewall may become beneficial when used with an IDS even if it is not beneficial when used alone.

The results about the value of IDS and firewall technologies and, more important, on the interaction between the two, have significant implications for managers. Given our finding that a firewall and an IDS may conflict with each other, one of the most important questions of managerial significance is how to avoid the conflict. A deeper analysis of our results provides possible answers to this question. First, if the quality of the firewall is high (i.e., r_F is low), then as the false positive rate of firewall approaches zero, the conflict effect disappears; however, the conflict effect does not vanish if the quality of the firewall is low. Hence, firms should consider augmenting the IDS with a high-quality firewall that has a low false positive error. If the firm cannot deploy a high quality firewall with a low false positive rate, allowing complete external access to reap the maximum benefit from the IDS is better than restricting external access. Second, irrespective of the firewall quality, the detection rate of IDS is a critical determinant of the interaction effect. An IDS that has a low detection rate will always conflict with any firewall. So, a firm should choose an IDS that has a high detection rate to avoid the conflict effect. Furthermore, if an IDS is also not good at detecting attacks, then the firm should not use any technology.

The above implications assume that the firm does not or cannot use optimal configurations for the firewall and the IDS. An interesting question is whether configuring them optimally will eliminate the adverse effects and lead to new implications. We answer this question in the next section.

6. Analysis of Optimal Configurations for Firewall and IDS in Stage 1

In our analysis so far, we had assumed that the firewall and IDS are not optimally configured. Now, we derive the firm's optimal configurations for these technologies. For both IDS and firewall, we use their respective ROC curves to identify the optimal configuration point and then compute the value of each technology at the optimal configuration point. Recall that $P_D^F = (P_F^F)^{r_F}$ and $P_D^I = (P_F^I)^{r_I}$, where $0 < r_F$, $r_I < 1$.

6.1. Optimally Configured Firewall

We show the following result regarding the optimal configuration when the firm implements only a firewall.

Proposition 5.

(i) *When the firm finds it optimal to allow external users in the no technology case, it is optimal to deploy a firewall configured at* $P_F^{F*} = (cdr_F(1-\zeta)/(d\phi\omega\zeta - c(d+\omega)\zeta))^{1/(1-r_F)}$. *The firewall offers a nonnegative value at the optimal configuration point.*

(ii) *When the firm finds it optimal to disallow external users in the no technology case,*

- *if* $\Lambda < 1/(r_F + (1-r_F)\zeta)$, *it is optimal to deploy a firewall configured at* $P_F^{F*} = (cdr_F(1-\zeta)/(d\phi\omega\zeta - c(d+\omega)\zeta))^{1/(1-r_F)}$. *The firewall offers a nonnegative value at the optimal configuration point.*
- *Otherwise, it is optimal not to deploy a firewall and continue to disallow external users.* □

Proposition 5 shows that if the firm allows external access in the absence of a firewall, then it always benefits by deploying an optimally configured firewall to control the external traffic. However, if the firm does not allow external access in the absence of a firewall, then it benefits from allowing external access and controlling the external traffic using a firewall only when cost-to-benefit-ratio-for-external-access is lower than a threshold (i.e., $1/(r_F + (1-r_F)\zeta)$). Because the threshold increases with firewall quality, deploying an optimally configured firewall benefits more firms if the quality is sufficiently high.

6.2. Optimally Configured IDS

We know that when $\mu/\beta > P_D^I$, the value of IDS is negative, and when $\mu/\beta \le P_D^I$, the value of IDS is positive. Therefore, the firm will always configure the IDS such that the detection rate is higher than or equal to μ/β, i.e., $\mu/\beta \le P_D^I$. We summarize the results regarding the optimal configuration of the IDS below.

Proposition 6. *When the firm implements only an IDS, the optimal configuration is given by* $P_D^{I*} = \mu/\beta$, *and the firm realizes a nonnegative value at the optimal configuration point.* □

It is interesting to note that the firm configures the IDS at the same point irrespective of how the firm handles the external traffic (i.e, no external access versus full external access). This result also generalizes the finding of Cavusoglu et al. (2005) who found identical optimal configuration for the IDS.

6.3. Optimally Configured Firewall and IDS Combination

We know that when $(\mu/\beta) > P_D^I$, IDS and firewall conflict with each other. So, the firm configures the IDS such that $(\mu/\beta) \le P_D^I$ when the IDS is deployed together with a firewall. The optimal configuration for the firewall and IDS combination is given in the following result.

Proposition 7. *If* $\Lambda < (1/(r_F + (1-r_F)\zeta)) \cdot (\mu/\beta)^{(r_I-1)/r_I}$, *the firm implements both firewall and IDS and configures them at*

$$P_D^{I*} = \frac{\mu}{\beta} \quad \textit{and}$$

$$P_D^{F*} = \left(\frac{cdr_F(1-\zeta)}{(d\phi - c)\omega\zeta(\mu/\beta)^{(r_I-1)/r_I} - cd\zeta}\right)^{r_F/1-r_F}.$$

Otherwise, the firm only implements the IDS, configures it at $P_D^{I*} = \mu/\beta$, *and disallows external access.* □

The most interesting insights from Propositions 5–7 relate to (a) how the configurations of the firewall and the IDS change when they are deployed together, compared to when they are deployed alone and (b) how optimal configuration affects the interaction between the two. We find that (i) the configuration point of the IDS does not change whether it is used alone or together with a firewall, and (ii) the firewall is configured to operate at a lower detection rate when it is used with an IDS than without, i.e., P_D^{F*} (when used alone) > P_D^{F*} (when used with an IDS). For example, suppose $r_F = 0.3$, $r_I = 0.5$, $\omega = 50$, $\zeta = 0.1$, $c = 2$, $d = 100$, $\phi = 0.5$, $\varepsilon = 0.5$, $\mu = 8$, and $\beta = 10$. We find that the optimal configuration points for the firewall when used together with an IDS and when used alone are $P_D^{F*} = 0.494$, $P_F^{F*} = 0.095$, and $P_D^{F*} = 0.548$, $P_F^{F*} = 0.134$, respectively. Knowing that there is a detective control after the firewall, the firm chooses to be less strict in allowing access because the IDS acts as a deterrent to users that gain access. Such deterrence is absent when there is no IDS, causing the firm to be stricter in allowing access. Surprisingly, the implementation of a firewall does not change the configuration of the IDS. The reason for this result is two-fold: (i) The firewall is not a control against internal hackers, and (ii) the firewall is not a deterrent against external hackers. Unlike IDS, external hackers are not penalized when they are stopped by a firewall, therefore they do not change their attack strategies based on the existence of a firewall. In the same vein, the strategy of internal hackers is unaffected by the firewall because they do not have to pass through the firewall. Because users' (both internal and external) hacking strategies are unaffected by the firewall configuration, and all users are identical from the IDS's perspective, the configuration of an IDS is unaffected by the firewall.

Another interesting observation from Propositions 5–7 is that an optimally configured firewall is valuable in a larger region when it is deployed with an optimally configured IDS. So, a firm that prefers to block external access even with an optimally configured firewall may prefer to deploy the firewall instead of blocking external access when it deploys an optimally configured IDS also. The intuition is that the IDS makes the firewall more valuable because of the complementarity effect between them, as explained before.

The following result shows how the firewall and the IDS interact with each other when they are configured optimally.

Corollary 3. *Optimally configured firewall and IDS* substitute *each other when*

$$\Lambda < \min\left(\left(\frac{\mu}{\beta}\right)^{(r_I-1)/r_I}, \left(\frac{1-P_F^{F*}}{1-(\zeta P_F^{F*}+(1-\zeta)P_D^{F*})}\right)\right),$$

and complement *each other when*

$$\min\left(\left(\frac{\mu}{\beta}\right)^{(r_I-1)/r_I}, \left(\frac{1-P_F^{F*}}{1-(\zeta P_F^{F*}+(1-\zeta)P_D^{F*})}\right)\right) < \Lambda < \left(\frac{1}{r_F+(1-r_F)\zeta}\right)\left(\frac{\mu}{\beta}\right)^{(r_I-1)/r_I}. \quad \square$$

The above result shows that optimally configured IDS and firewall *never* conflict with each other. However, even with the optimal configuration, firewall and IDS do not necessarily complement each other. An analysis of the regions in which an optimally configured firewall and an optimally configured IDS complement or substitute each other shows that an optimally configured firewall and an optimally configured IDS can complement each other only if the firm does not allow external access in the no-technology case. If the firm allows external access in the no-technology case, optimally configured IDS and firewall only substitute each other. In summary, we find that by optimally configuring an IDS and a firewall, the firm eliminates the negative effect from joint implementation of these technologies. That is, optimally-configured IDS and firewall always offer a nonnegative value and never conflict with each other.

One of the significant implications of the results in this section is that even if security managers optimally configure the firewall and the IDS, implementing both is not always the best option. Whereas managers need to take into account the quality and false positive and false negative rates of these technologies if they are not optimally configured because of potential adverse interaction, managers do not have to worry about such adverse interaction if the technologies are optimally configured. Contrary to what one may expect, when optimally configured, as the quality profile of either technology goes up (either r_F or r_I decreases), IDS and firewall are more likely to substitute than to complement each other.

Optimal configuration has implications even when only one of the technologies is implemented. If the firm is operating in an open environment where the benefit of external access outweighs the potential cost of it (like an e-commerce environment), the firm can never be worse by implementing an optimally configured firewall irrespective of its quality. On the other hand, if the firm is operating in a closed environment where the benefit of external access falls short of the potential cost (like a military environment), the firm can be better off without an optimally configured firewall. Finally, whereas not using any technology may be the best choice when optimal configuration is not considered, firms will always find it better to use one or both technologies when they are optimally configured.

7. Robustness of Our Results: Alternative Model Specifications

In previous sections, we analyzed a model in which all users were homogenous with respect to their utility from hacking and penalty for hacking when caught. While users were classified into different types such as external versus internal and legal versus illegal, they differed only with respect to the benefit they offered to the firm. A case could be made that external hackers may incur a lower expected penalty than internal hackers because external hackers are more difficult to catch. Similarly, there could be differences in their utilities because the motivations of internal and external hackers are often different (Ciampa 2005). In this section, we analyze whether our results are robust to changes in our assumption about the homogeneity of users' utility and penalty parameters.

7.1. Alternative 1: Heterogeneity in Incentives to Hack Between Legal and Illegal Users[10]

In our base model, we assumed that, under normal use, the firm realizes a positive payoff only when the user is legal. The base model did not consider the payoff to a user under normal use. In many situations, a legal user conducts normal business with a firm because she has some economic payoff, and an illegal user realizes a positive economic payoff only by hacking. On the other hand, if a legal user is caught hacking, she is likely to lose her current and future payoff from the normal business in addition to any other penalty, but an illegal user who is caught hacking suffers only the penalty. Consequently, a legal user is likely to have less (or no) incentive to hack compared to an illegal user. We model such heterogeneity in incentives to hack between legal and illegal users by analyzing a model in which legal users do not have incentives to hack whereas illegal users decide to hack depending on their utility from hacking and the penalty if caught hacking. The rest of the model remains the same as the base model.

The detailed analysis of this new model is given in Part B of the online supplement. We show that all our results (Propositions 1–7 and Corollaries 1–3) hold qualitatively in the new model. The only difference between a result in our base model and the corresponding result in the new model relates to the expressions for the cut-off values that separate different regions. For example, the result corresponding to the interaction between a firewall and an IDS from the first alternative model is given below.

Proposition 4B.

(1) *When* $\mu/\beta \le P_D^I$

- *If*

$$\frac{P_F^F[(d\phi-c)P_D^I+cP_F^I]}{\varepsilon[(1-\zeta)P_D^F+\zeta P_F^F]d\phi P_F^I} < \Lambda < \min\left\{\frac{(d\phi-c)P_D^I+cP_F^I}{d\phi P_F^I}, \max\left\{\frac{P_F^F[(d\phi-c)P_D^I+cP_F^I]}{\varepsilon[(1-\zeta)P_D^F+\zeta P_F^F]d\phi P_F^I}, \frac{1-P_F^F}{1-\varepsilon P_D^F+\varepsilon\zeta(P_D^F-P_F^F)}\right\}\right\},$$

then IDS and firewall substitute *each other.*

- *If*

$$\min\left\{\frac{(d\phi-c)P_D^I+cP_F^I}{d\phi P_F^I}, \max\left\{\frac{P_F^F[(d\phi-c)P_D^I+cP_F^I]}{\varepsilon[(1-\zeta)P_D^F+\zeta P_F^F]d\phi P_F^I}, \frac{1-P_F^F}{1-\varepsilon P_D^F+\varepsilon\zeta(P_D^F-P_F^F)}\right\}\right\} < \Lambda < \frac{(1-P_F^F)[(d\phi-c)P_D^I+cP_F^I]}{[1-\varepsilon P_D^F+\varepsilon\zeta(P_D^F-P_F^F)]d\phi P_F^I},$$

then IDS and firewall complement *each other.*

- *Otherwise, IDS and firewall* conflict *with each other.*

(2) *When* $\mu/\beta > P_D^I$: *IDS and firewall* conflict *with each other.*

A comparison of Proposition 4 and Proposition 4B shows that they are qualitatively identical. Furthermore, we confirmed that the intuition for a result in the base model and that of the corresponding result in the new model were also identical. Hence, we conclude that homogeneity in incentives of legal and illegal users does not drive our results.

7.2. Alternative 2: Heterogeneity in Incentives to Hack Between Internal and External Users

We analyzed the case in which internal and external users are heterogeneous with respect to the penalty if caught hacking. We also broadened the definition of hacking to include breaking of the firewall by an illegal external user. The primary difference between the two alternative models considered in this section is the following. In alternative 1, the hacking probability is different for legal and illegal users, but is independent of whether the user is internal or external. However, in alternative 2, the hacking probability

[10] We thank the anonymous reviewers for suggesting this model specification.

is different for internal and external users, but is independent of whether the user is legal or illegal.

In alternative 2, the net penalty was assumed to be β and $\Delta\beta$ for an internal and an external hacker, respectively, where $0 < \Delta < 1$. The algebraic expressions were significantly more complex than those in the base model because hacking rates were different for external and internal users. The detailed analysis of this new model is given in Part C of the online supplement. Again, we found that while equilibrium strategies were different from those for the base model, our results on the value of firewall, the value of IDS, the value of firewall and IDS combination, and the nature of interaction between a firewall and an IDS in terms of complementary, substitution, and conflict effects were qualitatively similar to those reported in our base model. Hence, we conclude that homogeneity in incentives of internal and external users does not drive our results. The result corresponding to the interaction between a firewall and an IDS from the second alternative model is given below.

Proposition 4C.

(1) *When* $\Delta < \mu/\beta \leq P_D^I$

- *If*

$$\bar{\Lambda} < \frac{(1-P_D^I)(1-P_D^F)\varepsilon\zeta}{(1-P_D^I)(1-P_D^F)\varepsilon\zeta+(1-P_F^I)(1-\varepsilon+(1-P_F^F)\varepsilon-(1-P_F^F)\varepsilon\zeta)},$$

then IDS and firewall substitute *each other.*

- *If*

$$\frac{(1-P_D^I)(1-P_D^F)\varepsilon\zeta}{(1-P_D^I)(1-P_D^F)\varepsilon\zeta+(1-P_F^I)(1-\varepsilon+(1-P_F^F)\varepsilon-(1-P_F^F)\varepsilon\zeta)}$$

$$< \bar{\Lambda} < \frac{(1-P_D^F)\varepsilon\zeta}{(1-P_D^F)\varepsilon\zeta+(1-\varepsilon+(1-P_F^F)\varepsilon-(1-P_F^F)\varepsilon\zeta)},$$

then IDS and firewall complement *each other.*

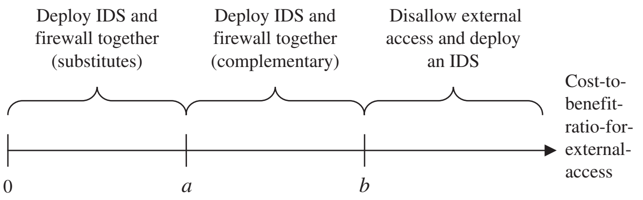
(2) *When* $\Delta > \mu/\beta > P_D^I\Delta$ *and*

$$\bar{\Lambda} < \frac{(1-P_D^I)(1-P_D^F)\varepsilon\zeta}{(1-P_D^I)(1-P_D^F)\varepsilon\zeta+(1-P_F^I)(1-\varepsilon+(1-P_F^F)\varepsilon-(1-P_F^F)\varepsilon\zeta)},$$

IDS and firewall conflict *with each other, where* $\bar{\Lambda} = c/d$.

In summary, the analysis of alternative model specifications shows that all our results about the value of firewall and IDS technologies are robust and are not driven by specific assumptions about user behavior. Thus, we conclude that our explanations in terms of the deterrence and detection effects of an IDS and the access control function of a firewall and an IDS are the drivers for the results we obtained in this paper.

Figure 4 Design of the Optimal Security Architecture, $\{a = \min((\mu/\beta)^{(r_I-1)/r_I}, (1/(r_F + (1-r_F)\zeta)))$ **and** $b = (1/(r_F + (1-r_F)\zeta))(\mu/\beta)^{(r_I-1)/r_I}\}$


Deploy IDS and firewall together (substitutes)
Deploy IDS and firewall together (complementary)
Disallow external access and deploy an IDS
Cost-to-benefit-ratio-for-external-access
0
a
b

8. Discussion and Conclusions

The analysis presented in previous sections offered important theoretical insights into the role played by configuration in the value of IDS and firewall technologies. From a manager's perspective, important implications of our analysis pertain also to insights into the optimal firewall and IDS deployment policies. The optimal deployment policy offers guidance on when the firm should implement both a firewall and an IDS, when it should implement only an IDS, only a firewall, or neither, and whether the firm should allow external access when the firm does not use a firewall. These policies can be derived directly from the results stated in previous sections. We depict the optimal deployment policy graphically, as shown in Figure 4. The figure assumes that the firm that deploys the security technologies optimally configures them. The figure reveals that the firm should implement both a firewall and an IDS when the cost-to-benefit-ratio-for-external-access is low. If this ratio is very low, even though the firm should implement both, the technologies substitute (imperfectly) each other. If the ratio is moderately low, then the technologies complement each other. When cost-to-benefit-ratio-for-external-access is sufficiently high, the firm should restrict the access to insiders only and deal with hacking from insiders with the help of an IDS. This result runs counter to the recommendation by some in the IT security community to rely only on firewalls for balancing access and protection needs (Gartner 2003).[11] We also find that optimal security architectures require implementation of both a

[11] This result assumes that the firm configures its controls optimally before implementing them. If the firm is to deploy its security controls with default configurations, then the optimal security architecture may require the firm to implement only a firewall (see Cavusoglu et al. 2005).

firewall and IDS, except in a case in which the cost-to-benefit-ratio-of-external-access is sufficiently high. An example of this could be military and defense systems in which the benefit from external access is very small because the proportion of external users who are legal is very low (even though damage cost can be higher compared to other systems).

We used a stylized model for our analysis, and the model can be extended in several directions. Our model does not capture the fact that hackers may shift their resources to target different firms depending on the security controls deployed by firms. This issue was recently addressed by Cremonini and Nizovtsev (2006), who model the behavior of attackers when attackers are able to obtain complete information about the security characteristics of their targets and when such information is unavailable. They find that when attackers can distinguish targets by their security characteristics and switch between multiple alternative targets, the effect of a given security measure is stronger. That is because attackers rationally put more effort into attacking systems with low security levels. Ignoring that effect would result in underinvestment in security or misallocation of security resources. Future research should investigate how attackers' shifts in hacking strategy affect firms' configuration decisions. Furthermore, we considered a one-shot game in our analysis. In reality, the game between a firm and hackers is a repeated one, with each party trying to maximize its current and future periods' payoffs by observing the past. We leave this analysis to future research. Other extensions such as the impact of firm's risk profile on configuration decisions and an analysis of other functional forms for the ROC curve are also left for future research.

Acknowledgments

The authors thank the seminar participants at the University of Texas at Dallas, Carnegie Mellon University, Tulane University, Baruch College, University of Alberta (Canada), Koç University (Turkey), and ESADE (Spain). They also thank the senior editor, Paulo Goes; the associate editor, Debabrata Dey; and three anonymous referees as well as the participants at the International Conference on Information Systems (2002), Workshop on the Economics of Information Security (2003), and Workshop on Information Systems and Economics (2005) for their comments and suggestions. This research was partially supported by a summer 2007 grant from the Network, Electronic Commerce, and Telecommunications (NET) Institute.

Appendix

Table A.1 Probability Computations

Event	Probability expression
A user gains access to the system	$P_{\text{Access}} = (1-\varepsilon) + (\varepsilon[(1-\zeta)(1-P_D^F) + \zeta(1-P_F^F)])$
A user who has gained access is an internal user	$P_{I\,\vert\,\text{Access}} = (1-\varepsilon)/P_{\text{Access}}$
A user who has gained access is an external legal user	$P_{E,\,\text{legal}\,\vert\,\text{Access}} = \varepsilon\zeta(1-P_F^F)/P_{\text{Access}}$
A user who has gained access is an external illegal user	$P_{E,\,\text{illegal}\,\vert\,\text{Access}} = \varepsilon(1-\zeta)(1-P_D^F)/P_{\text{Access}}$
A user who has gained access generates an alarm from the IDS	$P_{\text{alarm}\,\vert\,\text{Access}} = P_D^I\psi + P_F^I(1-\psi)$
Hack by an internal user given that IDS has generated an alarm	$P_{I,\,\text{hack}\,\vert\,\text{Alarm}} = \dfrac{P_D^I\psi P_{I\,\vert\,\text{Access}}}{(P_D^I\psi + P_F^I(1-\psi))}$
Normal use by an internal user given that IDS has generated an alarm	$P_{I,\,\text{no-hack}\,\vert\,\text{Alarm}} = \dfrac{P_F^I(1-\psi)P_{I\,\vert\,\text{Access}}}{(P_D^I\psi + P_F^I(1-\psi))}$
Hack by an external legal user given that IDS has generated an alarm	$P_{E,\,\text{legal, hack}\,\vert\,\text{Alarm}} = \dfrac{P_D^I\psi P_{E,\,\text{legal}\,\vert\,\text{Access}}}{(P_D^I\psi + P_F^I(1-\psi))}$
Normal use by an external user given that IDS has generated an alarm	$P_{E,\,\text{legal, no-hack}\,\vert\,\text{Alarm}} = \dfrac{P_F^I(1-\psi)P_{E,\,\text{legal}\,\vert\,\text{Access}}}{(P_D^I\psi + P_F^I(1-\psi))}$
Hack by an external illegal user given that IDS has generated an alarm	$P_{E,\,\text{illegal, hack}\,\vert\,\text{Alarm}} = \dfrac{P_D^I\psi P_{E,\,\text{illegal}\,\vert\,\text{Access}}}{(P_D^I\psi + P_F^I(1-\psi))}$

Table A.1 (Cont'd.)

Event	Probability expression
Normal use by an external illegal user given that IDS has generated an alarm	$P_{E,\,\text{illegal, no-hack}\,\vert\,\text{Alarm}} = \dfrac{P_F^I(1-\psi)P_{E,\,\text{illegal}\,\vert\,\text{Access}}}{(P_D^I\psi + P_F^I(1-\psi))}$
Hack by an internal user given that IDS has not generated an alarm	$P_{I,\,\text{hack}\,\vert\,\text{No-alarm}} = \dfrac{(1-P_D^I)\psi P_{I\,\vert\,\text{Access}}}{(1-P_D^I\psi - P_F^I(1-\psi))}$
Normal use by an internal user given that IDS has not generated an alarm	$P_{I,\,\text{no-hack}\,\vert\,\text{No-alarm}} = \dfrac{(1-P_F^I)(1-\psi)P_{I\,\vert\,\text{Access}}}{(1-P_D^I\psi - P_F^I(1-\psi))}$
Hack by an external legal user given that IDS has not generated an alarm	$P_{E,\,\text{legal, hack}\,\vert\,\text{No-alarm}} = \dfrac{(1-P_D^I)\psi P_{E,\,\text{legal}\,\vert\,\text{Access}}}{(1-P_D^I\psi - P_F^I(1-\psi))}$
Normal use by an external legal user given that IDS has not generated an alarm	$P_{E,\,\text{legal, no-hack}\,\vert\,\text{No-alarm}} = \dfrac{(1-P_F^I)(1-\psi)P_{E,\,\text{legal}\,\vert\,\text{Access}}}{(1-P_D^I\psi - P_F^I(1-\psi))}$
Hack by an external illegal user given that IDS has not generated an alarm	$P_{E,\,\text{illegal, hack}\,\vert\,\text{No-alarm}} = \dfrac{(1-P_D^I)\psi P_{E,\,\text{illegal}\,\vert\,\text{Access}}}{(1-P_D^I\psi - P_F^I(1-\psi))}$
Normal use by an external illegal user given that IDS has not generated an alarm	$P_{E,\,\text{illegal, no-hack}\,\vert\,\text{No-alarm}} = \dfrac{(1-P_F^I)(1-\psi)P_{E,\,\text{illegal}\,\vert\,\text{Access}}}{(1-P_D^I\psi - P_F^I(1-\psi))}$
Hack given that IDS has generated an alarm	$P_{\text{hack}\,\vert\,\text{Alarm}} = P_D^I\psi/(P_D^I\psi + P_F^I(1-\psi))$
Hack given that IDS has not generated an alarm	$P_{\text{hack}\,\vert\,\text{No-alarm}} = (1-P_D^I)\psi/(1-P_D^I\psi - P_F^I(1-\psi))$

References

Allen, J., G. Ford, B. Fraser, J. Kochmar, S. Konda, D. Simmel, L. Cunningham. 1998. Security for Information Technology Service contracts. SEI Security Improvement Modules CMU/SEI-SIM-003, Software Engineering Institute, Pittsburgh.

August, T., T. I. Tunca. 2006. Network software security and user incentives. *Management Sci.* **52**(11) 1703–1720.

August, T., T. I. Tunca. 2008. Let the pirates patch? An economic analysis of network software security patch restrictions. *Inform. Systems Res.* **19**(1) 48–70.

Axelsson, S. 2000. The base-rate fallacy and the difficulty of intrusion detection. *ACM Trans. Inform. System Security* **3**(3) 186–205.

Campbell, P., B. Calvert, S. Boswell. 2003. *Security+Guide to Network Security Fundamentals*. Course Technology, Boston.

Cavusoglu, H. 2003. The economics of IT security. Ph.D. thesis, University of Texas at Dallas, Richardson.

Cavusoglu, H., S. Raghunathan. 2004. Configuration of detection software: A comparison of decision and game theory approaches. *INFORMS Decision Anal.* **1**(3) 131–148.

Cavusoglu, H., H. Cavusoglu, S. Raghunathan. 2007. Efficiency of vulnerability disclosure mechanisms to disseminate vulnerability knowledge. *IEEE Trans. Software Engrg.* **33**(3) 171–185.

Cavusoglu, H., H. Cavusoglu, J. Zhang. 2008. Security patch management: Share the burden or share the damage? *Management Sci.* **54**(4) 657–670.

Cavusoglu, H., B. Mishra, S. Raghunathan. 2005. The value of intrusion detection systems (IDSs) in information technology security. *Inform. Systems Res.* **16**(1) 28–46.

Cavusoglu, H., S. Raghunathan, H. Cavusoglu. 2005. How do security technologies interact with each other to create value? The analysis of firewall and intrusion detection system. Workshop on Information Systems and Economics. Irvine, CA.

Christensen, P. O., G. Feltham. 2005. *Economics of Accounting—Performance Evaluation. Springer Series in Accounting Scholarship*, Vol. 2. Springer, New York.

Ciampa, M. 2005. *Security+Guide to Network Security Fundamentals*. Course Technology, Boston.

Cremonini, M., D. Nizovtsev. 2006. Understanding and influencing attackers' decisions: Implications for security investment strategies. Workshop on the Economics of Information Security, Cambridge, UK.

D'haeseleer, P., S. Forrest, P. Helman. 1996. An immunological approach to change detection: Algorithms, analysis, and implications. *Proc. IEEE Sympos. Security Privacy*, Oakland, CA, 110–119.

Durst, R., T. Champion, B. Witten, E. Miller, L. Spannuolo. 1999. Testing and evaluating computer intrusion detection systems. *Comm. ACM* **42**(7) 53–61.

Gal-Or, E., A. Ghose. 2005. The economic incentives for sharing security information. *Inform. Systems Res.* **16**(2) 186–208.

Gartner. 2003. *Hype Cycle for Information Security*. Gartner Research Report (May 30).

Garvey, T., T. Lunt. 1991. Model-based intrusion detection. *Proc. 14th National Comput. Security Conf.*, Washington, DC, 372–385.

Gordon, L., M. Loeb, W. Lucyshyn. 2003. Sharing information on computer systems security: An economic analysis. *J. Acc. Public Policy* **22**(6) 461–485.

Gouda, M. G., X.-Y. A. Liu. 2004. Firewall design: Consistency, completeness, and compactness. *24th Internat. Conf. Distributed Comput. Systems*, Tokyo, 320–327.

Holden, G. 2004. *Guide to Firewalls and Network Security*. Course Technology, Boston.

Ilgun, K. 1992. Ustat: A real-time intrusion detection system for Unix. Master's thesis, Computer Science Department, University of California at Santa Barbara.

Kumar, S., E. Spafford. 1996. A pattern matching model for misuse intrusion detection. *The COAST Project*. Purdue University, West Lafayette, IN.

Lippmann, R. P., J. W. Haines, D. J. Fried, I. Graf, J. Kobra, K. Das. 2000. The 1999 DARPA off-line intrusion detection evaluation. *Comput. Networks* **34**(2) 579–595.

Lunt, T. 1990. Ides: An intelligent system for detecting intruders. *Proc. Sympos.: Comput. Security, Threat Countermeasures*, Rome, 110–121.

Lunt, T. 1993. A survey of intrusion detection techniques. *Comput. Security* **12**(4) 405–418.

Lunt, T., R. Jagannathan. 1988. A prototype real-time intrusion detection expert system. *Proc. 1988 IEEE Sympos. Security Privacy*, Oakland, CA, 59–66.

Magalhaes, R. 2004. *Network Security Recommendations That Will Enhance Your Windows Network*, WindowsSecurity.com.

McCarthy, L. 1998. *Intranet Security*. Sun Microsystems Press, Santa Clara, CA.

Monrose, F., A. Rubin. 1997. Authentication via keystroke dynamics. *4th ACM Conf. Comput. Comm. Security*, Zurich, 48–56.

Neumann, P., P. Porras. 1999. Experience with emerald to date. *Proc. 1st USENIX Workshop Intrusion Detection Network Monitoring*, Santa Clara, CA, 73–80.

Nizovtsev, D., M. Thursby. 2005. Economic analysis of incentives to disclose software vulnerabilities. Workshop on the Economics of Information Security. Boston.

NMAB. 1998. *Configuration Management and Performance Verification of Explosives-Detection Systems*. Publication NMAB-482-3, National Academy Press, Washington, DC.

NSS. 2004. Gigabit intrusion detection systems. White paper, The NSS Group, Carlsbad, CA.

Ogut, H., H. Cavusoglu, S. Raghunathan, 2008. Intrusion-detection policies for IT security breaches. *INFORMS J. Comput.* **20**(1) 112–123.

Ogut, H., N. Menon, S. Raghunathan. 2005. Cyber insurance and IT security investment: Impact of interdependent risk. Workshop on the Economics of Information Security, Boston.

Ozment, A. 2004. Bug auctions: Vulnerability markets reconsidered. Workshop on the Economics of Information Security, Minneapolis.

Piessens, F. 2002. A taxonomy of causes of software vulnerabilities in Internet software. *13th Internat. Sympos. Software Reliability Engrg.*, Annapolis, MD, 47–52.

Porras, P., R. Kemmerer. 1992. Penetration state transition analysis: A rule-based intrusion detection approach. *IEEE 8th Annual Comput. Security Appl. Conf.*, San Antonio, TX, 220–229.

Porras, P., P. Neumann. 1997. Emerald: Event monitoring enabling responses to anomalous live disturbances. *Proc. 20th Nat. Inform. Systems Security Conf.*, Baltimore, 353–365.

Schechter, S. 2002. How to buy better testing: Using competition to get the most security and robustness for your dollar. *Infrastructure Security Conf.*, Bristol, UK, 73–87.

Trees, H. V. 2001. *Detection, Estimation and Modulation Theory-Part I*. John Wiley, New York.

Ulvila, J. W., J. E. Gaffney. 2004. A decision analysis method for evaluating computer intrusion detection systems. *INFORMS Decision Anal.* **1**(1) 35–50

Whitman, M., H. Mattord. 2003. *Principles of Information Security*. Course Technology, Boston.

Yue, W. T., A. Bagchi. 2003. Tuning the quality parameters of a firewall to maximize net benefit. *Lecture Notes in Comput. Sci.*, Distributed Computing—IWDC 2003, Springer, Berlin/Heidelberg, 321–329.

Zamboni, D., E. Spafford. 1999. New directions for the AAPHID architecture. *Workshop Recent Adv. Intrusion Detection*. West Lafayette, IN.