Association for Information Systems

AIS Electronic Library (AISeL)

ICEB 2010 Proceedings

International Conference on Electronic Business (ICEB)

Winter 12-1-2010

The Optimal Configuration and Their Strategic Analysis of Information System Security Technology Portfolios

Liurong Zhao

Shu’e Mei

Weijun Zhong

Follow this and additional works at: https://aisel.aisnet.org/iceb2010

This material is brought to you by the International Conference on Electronic Business (ICEB) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICEB 2010 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

THE OPTIMAL CONFIGURATION AND THEIR STRATEGIC ANALYSIS OF INFORMATION SYSTEM SECURITY TECHNOLOGY PORTFOLIOS

Liurong Zhao, Shu-e Mei, Weijun Zhong, School of Economics and Management, Southeast University, Nanjing, Jiangsu, China

E-mail: springzlr@163.com, meishue@seu.edu.cn, zhongweijun@seu.edu.cn

Abstract

Confronted with the increasingly severe information security problems, proper configuration of security technologies is critical to enhance the information systems performance. To solve the integrated linkage control problem based on attack detection, the security model including firewall, intrusion detection system (IDS) and vulnerability scan is analyzed by game theory. The analyses show that more IT portfolio will not bring better benefits, and more fixed vulnerabilities are not the better choice for the firm either. However, reasonable configuration of firewall will always reduce the firm’s expected loss. According to the Nash equilibrium of the model, technical parameters are configured to minimize the firm’s expected loss.

Key words: economics of information systems; firewall; IDS; vulnerability scan; security portfolio strategy

1 Introduction

With the rapid development of microelectronics and emergence of information industry, the tide of informatization is billowy. An important feature of information age is accessing to information and exchanging information by network [1], e-commerce has developed rapidly, and online transaction of enterprises has carried on actively [2]. But science and technology is two sides sword. When the whole society popularizes information technology, the diversification trends of information systems security problems are getting evident: hackers spread, privacy issues, computer network crime, confidence crisis, variety purposes of system invasion, etc., especially the increasingly severe e-commerce security problems. In view of rigorous information security trend, all kinds of IT security measures were successively found. Mainstream security technologies include firewall, IDS and vulnerability scan, etc. [3]. Nevertheless each IT has its own advantages and limitations, and only the proper configuration of IT can achieve the information system dynamic security, which is the key to balance the information protection and information access as well.

Different information system security problems can be solved by different IT portfolios. In general, according to the different security threats and protection focuses, information system security should generate the following five strategies: the integrated linkage control problem based on attack detection; the border security control problem based on active defense; the unified access management problem based on source control; the integrated threat management problem based on security fusion; the closed-loop strategy management problem based on asset protection. Our findings offer solutions to the integrated linkage control problem based on attack detection, it mainly needs to deploy vulnerability scan, intrusion detection, firewall, etc., and to achieve a linkage control between firewall, IDS, routers and switches. In this problem, all the security threats are reflected in the attacker's malicious behavior. The attacks are effectively recognized by detecting their behavior characteristics. As a result, the linkage between security equipment and network equipment executes an effective control to prevent the attacks.

At present, there are two significant trends to address the information system security. One transition is from the traditional IT security to the integration of IT and security management; the other transition is from the traditional use of a single IT to the use of IT portfolios. The traditional information security technology methods are mainly studied in a purely technical aspect, whose research has focused on the design of algorithms related to firewalls, IDS and others, such as encryption. For example, various approaches to firewall design are discussed in Holden and Gouda and Liu [4], [5]. The algorithms used in anomaly-based IDS are presented in Neumann and Porras, and Zamboni and Spafford [6], [7]. The other methods are studied in an economics and management aspect to study on the IT configuration and strategy formulation, which integrate IT and security management. Therefore, in the last few years, a new research filed has arisen in information management system—Economics of Information Security. Gal-Or and Ghose have analyzed the relationship between the security technology investments and information sharing by game theory, and show that the higher substitutability among the enterprises product, the more valuable the security information sharing, i.e. the more intense competition industry will benefit more when it establishes the sharing alliances[8]. Lye and Wing have established a random game model, which obtains the Nash equilibrium and the best strategy selection between the managers and the attackers [9]. Hu, Hart and Cooke have analyzed the role of external and internal influences on information systems security in a neo-institutional perspective [10]. There are more abundant achievements on the traditional use of a single IT. For instance, Li etc. have analyzed the intrusion prevention system management and configuration by inspection game theory [11].Alpcan has established the model of nonzero-sum and non-cooperative dynamic game between two players [12]. Cavusoglu and Raghunathan have respectively analyzed the IDS configuration based on decision theory and game theory, when it defends the attacks [13]. However, there is little research on the use of IT portfolios. Piessens has proposed that if the IT selection and portfolios are used inappropriately, the hackers may attack successfully by the weakness in the installation of software, which means the more use of IT may not be able to improve the security [14]. Zhu and Raghunathan have proposed the evaluation model of information security technologies on game theory, which include firewall, intrusion diction system and intrusion tolerant [15]. Cavusoglu etc. have studied configuration of and interaction between a firewall and IDS, and 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 [16].

Thus for the information security problems are very important, there are a large number of relevant domestic and international achievements in the recent years, although the economics of information security is a new field. But most of the achievements are based on one security IT, and there are few on the security IT portfolios, especially on more than three IT portfolios. The development of information network is a game process between information protection technology and information attack technology. In this game, we assume that the player using information protection technology is the firm, and the other player using information attack technology is the hacker, then the game transfers into the game between the firm and the hacker. The objective of the firm is to minimize its expected loss from intrusions; on the other hand, the hacker is to maximize his expected benefit. If the game is to achieve the balance, a reasonable strategy and proper technical parameter configuration will be the key factors. In this paper, the security model including firewall, intrusion detection system (IDS) and vulnerability scan has been analyzed by game theory, and the problem of IT selection and optimal configuration has been studied. Moreover, the game strategy has been analyzed, and the impact on the access control policy for the firm has been proposed subsequently. In the end, it concludes the paper with a discussion of the implications of our results and future research directions.

2 Information Security Model

In a protected system, the protective measures are usually deployed to defense the security incidents by the system security policy [17]. For sake of analysis, an information security model is introduced here (Figure 1).

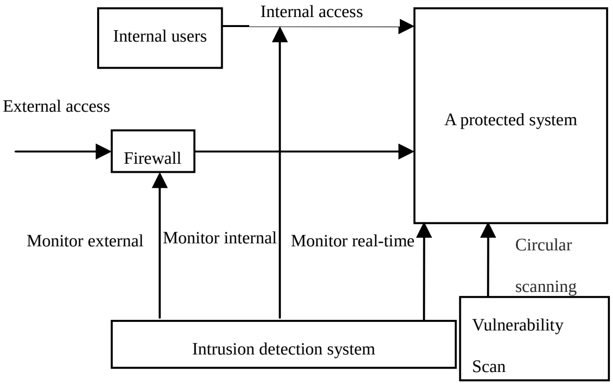

Figure 1 Information Security Model

Although each IT security has different objectives, they are not independent of each other in control. Firewall can generally prevent intrusion, IDS can detect intrusion, and vulnerability scan can identify the security risks and the vulnerabilities exploited by hackers. In practice, according to the network topology, applications and safety requirements, we deploy the proper firewall; monitor the key points of the network in real-time by IDS, adjust the system automatically by the system administrator or security strategy after discovering the intrusion; scan the system at regular intervals to find the vulnerabilities of configuration changes and fix them in time. Generally there are four reasonable technology portfolios: only deploy firewall and IDS; only deploy IDS and vulnerability scan; deploy all the technologies; deploy none of the technologies. Therein, the principle of firewall and IDS portfolio is that, IDS is able to detect the intrusion outside the firewall, and firewall is able to further adjust the security strategy by the feedback information of IDS, which can prevent the intrusion behavior from the beginning, and that can greatly improve the entire defense system performance. In addition, the principle of IDS and vulnerability scan portfolio is that, IDS acquires the anomaly cases of attacks, whereas scanner acquires the security risks of the objective system. The exist vulnerabilities in the system is able to be derived reversely by the attack information from IDS; on the other side, the system risks are able to effectively connect with the attack states to estimate and forecast the trend of attacks.

Cavusoglu etc. [10] have discussed the portfolio: only deploy firewall and IDS; and deploy none of the technologies, which have researched on the configuration of and interaction between firewall and IDS. The result is that default setting usually brings the risk, and the vulnerabilities of software could be easy found by the hacker in this case. When firewall and IDS are in the same security system, only the proper configuration can benefit the firm from both the security and economy. Based on paper [10], our study focuses on the portfolio: only deploy IDS and vulnerability scan; and deploy all the technologies.

3 Model Analyses

We consider two types of users, the internal users and external users. 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. No matter the portfolio (ⅰ) only deploy IDS and vulnerability scan, or the portfolio (ⅱ) deploy all the technologies, all users have to go through the scanner at regular intervals. However, the principle of the scanner is regularly testing the network risks, not as the same effect as firewall and IDS which can defense or prevent the invasion. So the effect of scanner is ahead of risk control initiatively for the firm, but for the hacker, it has raised the potential cost of invasion. We discuss the three broad components of our model—hacker, firm, and technology, and define the parameters as follows.

（Ⅰ） Hacker

(1) A hacker committing the intrusion derives a benefit of μ if the intrusion in undetected.

(2) If the intrusion is detected, the hacker incurs a penalty of β for a net benefit of $(\mu\text{-}\beta)$. We assume that $\mu \le \beta$; that is, a hacker that is detected does not enjoy a positive utility.

(3) Denote the probability that a user hacks by ψ ($\psi \in [0,1]$).

（Ⅱ） Firm

(1) The firm incurs a cost of c each time it performs a manual investigation.

(2) When an intrusion is undetected, the firm incurs a damage of d .

(3) If the firm detects an intrusion, the firm prevents or recovers a fraction, $(\phi \le 1)$ of d . It is reasonable to assume that $c \le d\phi$, so that the firm's cost of investigation is not higher than the benefit it gets if it detects an intrusion.

（Ⅲ）Technology

(1) Probability of firewall detection $P_D^F = P(\text{classify as a hacker} \mid \text{user is a hacker})$, i.e. firewall stops an illegal external user. Probability of firewall false negative is $1 - P_D^F$, i.e. firewall does not stop an illegal external user. Probability of firewall false positive $P_F^F = P(\text{classify as a hacker} \mid \text{user is a normal user})$, i.e. firewall stops a legal external user.

(2) Similarly, define probability of IDS detection $\mathrm{P_D}^{\mathrm{I}}$, i.e. $\mathrm{P_D}^{\mathrm{I}}$ is the probability that the IDS raises an alarm for an intrusion. Probability of IDS false negative is $1 - \mathrm{P_D}^{\mathrm{I}}$ i.e. $1 - \mathrm{P_D}^{\mathrm{I}}$ is the probability that the IDS does not raise an alarm for an intrusion. Probability of IDS false positive $\mathrm{P_F}^{\mathrm{I}}$ i.e. $\mathrm{P_F}^{\mathrm{I}}$ is the probability that the IDS raises an alarm when there is no intrusion.

(3) The configuration cost of vulnerability scan is c_S ; the firm performs a manual investigation when detects the intrusion, the potential benefit of scanner for the firm is $d\phi_S$ $(\phi_S \le 1)$, the potential cost of scanner for the hacker is β_S .

The objective of the firm is to minimize its expected loss from intrusions; on the other hand, the hacker is to maximize his expected benefit. We perform the analysis using backward induction. That is, we first derive the equilibrium for the firm's investigation strategy and a user's hacking strategy given the firm's implementation and configuration strategies, then figure out the equilibrium point. Subsequently, we determine the firm's optimal implementation and configuration strategy. Consequently, we derive the equilibrium strategies. In the following paragraphs, we separately analyze the portfolio (ⅰ) only deploy IDS and vulnerability scan, and the portfolio (ⅱ) deploy all the technologies.

Portfolio (ⅰ): only deploy IDS and vulnerability scan

Assume a user's strategy S^U∈ ｛H,NH｝, in which H is to hack, NH is not to hack.; the firm's strategy S^F∈ ｛（I,I）（I,NI）,(NI,I),(NI,NI)｝, in which I is to investigate, NI is not to investigate, and the first element in each ordered pair is the firm's action when IDS raises an alarm, while the second element is the firm's action when IDS does not raise an alarm. Let ρ_1 and ρ_2 respectively denote the firm's investigation probabilities when the IDS raises an alarm and when the IDS does not raise an alarm, in which （$\rho_1 \in [0,1]$） , and （$\rho_2 \in [0,1]$） . In general, $\rho_2 \le \rho_1$. The following probability computations are used in deriving the equilibrium.

$$\eta_1 = P(\text{intrusion}|\text{alarm}) = \frac{P_D^I\psi}{P_D^I\psi + P_F^I(1\text{-}\psi)} \qquad (1)$$

$$\eta_2 = P(\text{intrusion}|\text{no-alarm}) = \frac{(1-P_D^I)\psi}{(1-P_D^I)\psi + (1\text{-}P_F^I)(1\text{-}\psi)} \qquad (2)$$

$$P(\text{alarm}) = P_D^I\psi + P_F^I(1-\psi) = P_F^I + \psi(P_D^I - P_F^I) \qquad (3)$$

$$P(\text{no-alarm}) = 1 - P_F^I - \psi(P_D^I - P_F^I) \qquad (4)$$

$$P(\text{hacker is detected}) = \rho_1 P_D^I + \rho_2(1-P_D^I) \qquad (5)$$

The firm's expected cost for the alarm F_A and the no-alarm F_N states respectively are:

$$F_A(\rho_1,\psi) = \rho_1 c + \eta_1(1-\rho_1)d + \eta_1\rho_1(1-\phi)d + c_S - \eta_1\rho_1 d\phi_S \qquad (6)$$

$$F_N(\rho_2,\psi) = \rho_2 c + \eta_2(1-\rho_2)d + \eta_2\rho_2(1-\phi)d + c_S - \eta_2\rho_2 d\phi_S \qquad (7)$$

Then the firm's overall expected cost is:

$$F(\rho_1,\rho_2,\psi) = \qquad (8)$$
$$(P_F^I + \psi(P_D^I - P_F^I))F_A(\rho_1,\psi) + (1-P_F^I - \psi(P_D^I - P_F^I))F_N(\rho_2,\psi)$$

The hacker's expected benefit is:

$$H(\rho_1,\rho_2,\psi) = \psi\mu - \psi(\beta+\beta_S)(\rho_1 P_D^I + \rho_2(1-P_D^I)) \qquad (9)$$

Proposition 1: The following mixed strategy profiles constitute the Nash equilibrium for the IDS and vulnerability scan.

If $\frac{\mu}{\beta+\beta_S} > P_D^I$,

then

$$((\rho_1^* = 1, \rho_2^* = \frac{\mu-(\beta+\beta_S)P_D^I}{(1-P_D^I)(\beta+\beta_S)}), \psi^* = \frac{c(1-P_F^I)}{d(\phi-\phi_S)(1-P_D^I) - cP_F^I + cP_D^I});$$

If $\frac{\mu}{\beta+\beta_S} \le P_D^I$,

then

$$((\rho_1^* = \frac{\mu}{(\beta+\beta_S)P_D^I}, \rho_2^* = 0), \psi^* = \frac{cP_F^I}{P_D^I(\phi+\phi_S)d - cP_F^I - cP_D^I}).$$

Proof: The first derivatives of (6), (7) and (9) are:

$$\frac{\partial H}{\partial \psi} = \mu - (\beta+\beta_S)(\rho_1 P_D^I + \rho_2(1-P_D^I)) \qquad (10)$$

$$\frac{\partial F_A}{\partial \rho_1} = c - \eta_1 d + \eta_1(1-\phi-\phi_S)d \qquad (11)$$

$$\frac{\partial F_N}{\partial \rho_2} = c - \eta_2 d + \eta_2(1-\phi-\phi_S)d \qquad (12)$$

We can verify that, $\frac{\partial F_A}{\partial \rho_1} = 0, \frac{\partial F_N}{\partial \rho_2} = 0$ cannot be satisfied simultaneously, and $\frac{\partial F_A}{\partial \rho_1} \ge \frac{\partial F_N}{\partial \rho_2}$. Consequently, in the equilibrium, $\frac{\partial F_A}{\partial \rho_1} > 0, \frac{\partial F_N}{\partial \rho_2} = 0,$ or $\frac{\partial F_A}{\partial \rho_1} = 0, \frac{\partial F_N}{\partial \rho_2} < 0$.

Therefore we have two possible equilibrium scenarios: $\rho_1 = 1, 0 < \rho_2 < 1$ and $0 < \rho_1 < 1, \rho_2 = 0$.

When $\rho_1 = 1, 0 < \rho_2 < 1$,

In this scenario, (10) and (12) must equal to zero, and (11)>0.Sloving (10) and (12) for ρ_2 and ψ respectively, we get

$$\rho_2^* = \frac{\mu-(\beta+\beta_S)P_D^I}{(1-P_D^I)(\beta+\beta_S)}, \qquad (13)$$

$$\psi^* = \frac{c(1-P_F^I)}{d(\phi-\phi_S)(1-P_D^I) - cP_F^I + cP_D^I}, \qquad (14)$$

$\because$(13) is substituted into $0 < \rho_2 < 1, \therefore P_D^I < \frac{\mu}{\beta+\beta_S}$

$\therefore$ When $\frac{\mu}{\beta+\beta_S} > P_D^I$, the strategy profiles of Nash equilibrium is:

$$((\rho_1^*, \ \rho_2^*), \ \psi^*) =$$
$$((1, \frac{\mu-(\beta+\beta_S)P_D^I}{(1-P_D^I)(\beta+\beta_S)}), \frac{c(1-P_F^I)}{d(\phi-\phi_S)(1-P_D^I) - cP_F^I + cP_D^I}).$$

Similarly, $0 < \rho_1 < 1, \rho_2 = 0$

When $\frac{\mu}{\beta+\beta_S} \le P_D^I$,the strategy profiles of Nash equilibrium is:

$$((\rho_1^*, \ \rho_2^*), \ \psi^*) =$$
$$((\frac{\mu}{(\beta+\beta_S)P_D^I}, 0), \frac{cP_F^I}{P_D^I(\phi+\phi_S)d - cP_F^I - cP_D^I}).□$$

Conclusion 1: when $\frac{\mu}{\beta+\beta_S} > P_D^I$, the profitable probability of hack invasion is higher than the detected probability of hack invasion. That means the portfolio of only deploy IDS and scanner cannot benefit the firm, but hurt the firm. One of the reasons is that, the manual investigation will be conducted as soon as IDS has raised an alarm, which is very expensive and inefficient. The other reason is that, hacker prefers to intrude system in this case. Assume the probability of neutral for hacker's intruding is 0.5, then in this case, the probability that a user hacks $\psi^* > 0.5$, we have $c - d(\phi - \phi_S) \geq 0$, i.e. $c \geq d(\phi - \phi_S)$, which means the investigation cost is higher than the firm's benefit, so it cannot create efficiency for the firm.

Conclusion 2: From the expression of equilibrium strategy, whether $\frac{\mu}{\beta + \beta_S} > P_D^I$ or $\frac{\mu}{\beta + \beta_S} \leq P_D^I$, the defense strategy of the firm is relevant to the parameters $\mu, \beta, \beta_S, P_D^I$, and μ, β, β_S reflect the requirements of the firm's security environment; the intrusion strategy of the hacker is relevant to the parameters $c, d, \phi, \phi_S, P_F^I, P_D^I$,and c, d, ϕ, ϕ_S reflect the characters of the hacker's intrusion

Portfolio（ⅱ）deploy all the technologies, i.e. Firewall, IDS and Vulnerability scan

We assume that ε fraction of users is external users, and only a proportion ζ of external users are legal users. The benefit to the firm under normal use by a legal user is ω, the other assumptions are the same as portfolio (ⅰ), then:

P(A user gains access to the system)=

$$(1\text{-}\varepsilon)+（\varepsilon[(1-\zeta)(1-P_D^F)+\zeta(1-P_F^F)]）=\mathrm{P_e} \qquad (15)$$

P(A user is an internal user)=

$$\frac{1\text{-}\varepsilon}{(1\text{-}\varepsilon)+（\varepsilon[(1-\zeta)(1-P_D^F)+\zeta(1-P_F^F)]）}=\mathrm{P}_{in} \qquad (16)$$

P(A user is an external legal user)=

$$\frac{\varepsilon\zeta(1\text{-}\mathrm{P}_F^F)}{(1\text{-}\varepsilon)+（\varepsilon[(1-\zeta)(1-P_D^F)+\zeta(1-P_F^F)]）}=\mathrm{P_{eout}} \qquad (17)$$

The firm's expected cost for the alarm F_A^F and the no-alarm F_N^F with firewall states respectively are:

$$F_A^F=\omega(\frac{P_F^I(1-\psi)P_{\mathrm{in}}}{P_D^I\psi+P_F^I(1-\psi)}+\frac{P_F^I(1-\psi)P_{\mathrm{eout}}}{P_D^I\psi+P_F^I(1-\psi)}) \qquad (18)$$

$$F_N^F=\omega(\frac{(1\text{-}P_F^I)(1-\psi)P_{\mathrm{in}}}{1\text{-}P_D^I\psi\text{-}P_F^I(1-\psi)}+\frac{(1\text{-}P_F^I)(1-\psi)P_{\mathrm{eout}}}{1\text{-}P_D^I\psi\text{-}P_F^I(1-\psi)}) \qquad (19)$$

Then the firm's expected cost for the alarm F_A' and the no-alarm F_N' states respectively are:

$$\begin{aligned}&F_A'(\rho_1,\psi)=\rho_1 c+\eta_1(1-\rho_1)d+\eta_1\rho_1(1-\phi)d+c_S\\&-\eta_1\rho_1 d\phi_S\text{-}\omega(\frac{P_F^I(1-\psi)P_{\mathrm{in}}}{P_D^I\psi+P_F^I(1-\psi)}+\frac{P_F^I(1-\psi)P_{\mathrm{eout}}}{P_D^I\psi+P_F^I(1-\psi)})\end{aligned} \qquad (20)$$

$$\begin{aligned}&F_N'(\rho_2,\psi)=\rho_2 c+\eta_2(1-\rho_2)d+\eta_2\rho_2(1-\phi)d+c_S\\&-\eta_2\rho_2 d\phi_S\text{-}\omega(\frac{(1\text{-}P_F^I)(1-\psi)P_{\mathrm{in}}}{1\text{-}P_D^I\psi\text{-}P_F^I(1-\psi)}+\frac{(1\text{-}P_F^I)(1-\psi)P_{\mathrm{eout}}}{1\text{-}P_D^I\psi\text{-}P_F^I(1-\psi)})\end{aligned} \qquad (21)$$

Then the firm's overall expected cost is:

$$\begin{aligned}&F'(\rho_1,\rho_2,\psi)=P_{\mathrm{e}}[(P_F^I+\psi(P_D^I-P_F^I))F_A'(\rho_1,\psi)\\&+(1-P_F^I-\psi(P_D^I-P_F^I))F_N'(\rho_2,\psi)]\end{aligned} \qquad (22)$$

The hacker's expected benefit is:

$$H(\rho_1,\rho_2,\psi)=\psi\mu-\psi(\beta+\beta_S)(\rho_1 P_D^I+\rho_2(1-P_D^I)) \qquad (23)$$

Proposition 2: The equilibrium when the firm implements the firewall, IDS and vulnerability scan is identical to the equilibrium in proposition 1.

Proof: To have the equilibrium point, evaluate

$$\frac{\partial H}{\partial \psi}=0, \frac{\partial F_A{}'}{\partial \rho_1}=0, \frac{\partial F_N{}'}{\partial \rho_2}=0$$

Through the observation, there are no ρ_1, ρ_2 in (18) and (19), so if derivation, i.e. $\frac{\partial F_A{}'}{\partial \rho_1}=\frac{\partial F_A}{\partial \rho_1}, \frac{\partial F_N{}'}{\partial \rho_2}=\frac{\partial F_N}{\partial \rho_2}$, then the equilibrium in portfolio (i) is identical to the equilibrium in portfolio (ii).□

Conclusion 3: Although the equilibrium in portfolio (i) is identical to the equilibrium in portfolio (ii), as $F_A^F \geq 0, F_N^F \geq 0$, a proper configuration of firewall will reduce the firm's overall expected loss. If give the expected firm's loss, the reduce parts by firewall can be used to deploy the other technologies or upgrades, which will improve the firm's information security environment.

Conclusion 4: No matter the portfolio (i) or (ii), $d\phi_S$ in vulnerability scan does have impact on the hacker's intrusion strategy. The higher $d\phi_S$, the lower the probability of hack's intrusion, and the stronger the system protection is. So the scanner should be upgraded its database in time, and set scanning period rationally to help the firm reduce the probability of hacking. However, it does not mean the higher the better. In non-Nash equilibrium, the firm's expected loss is not the minimum loss, i.e. repairing all the vulnerabilities is not the best strategy for the scanner. It should reasonably repair the system vulnerabilities in terms of security level requirements. Otherwise the improper repair will cause the blue screen of death to the system, which is inconvenience to the firm.

4 conclusions

Firewall, IDS and vulnerability scan are mainstream security technologies. To solve the integrated linkage control problem based on attack detection, we establish the security model including these three technologies. The Nash equilibrium strategy is derived by analyzing the security technologies selection and optimal configuration. We show that deploying all the technologies is not the best choice for the firm. Conversely, it will hurt the firm. However, reasonable configuration of firewall will always reduce the firm's expected loss. It is significant for the optimal configuration of information security policy. The technical parameters in vulnerability scan do have impact on the hacker's intrusion strategy, but not imply that the more the repair the better the system performance.

We make a tentative research on the information security technology portfolios. Future research should investigate as follows: (1) Study on the interaction between firewall, IDS and vulnerability scan, for instance, how does the vulnerabilities in scanner impact on the configuration of firewall and IDS; (2) Consider a real firm as a research object, then the optimal information security strategy is proposed by configuring proper technical parameters. (3) Solve the optimal configuration problems of the other four network security strategies in the introduction part.

Acknowledge

This research is supported by the National Nature Science Foundation of China (No: 71071033) and the Innovation Project of Jiangsu Postgraduate Education (No: CX10B_058Z).

References

[1] Sushil K. Sharma and Joshua Sefchek., Teaching Information systems security courses: A hands-on approach, Computers & Security, 26, 2007, pp.290-299.

[2] Shen Changxiang., Introduction to Information Security, PHEI, Beijing, 2009.

[3] Stamp M., Crypto Basics, In Information Security: Principles and Practice, CA: John Wiley & Sons, San Francisco, 2006, pp. 11-31.

[4] Holden G., Guide to Firewalls and Network Security, Course Technology, Boston, 2004.

[5] Gouda M.G. and X-Y A. Liu., Firewall design: Consistency, Completeness, and Compactness, 24th Internat. Conf, Distributed Comput. Systems, Tokyo, 2004, pp.320-327.

[6] Neumann P. and P. Porras., Experience with Emerald to Date, Proc. 1st USENIX Workshop Intrusion Detection Network Monitoring, Santa Clara, CA ,1999, pp.73-80.

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

[8] Gal-Or E and Ghose A., The Economic Incentives

for Sharing Security Information, Information Systems Research, 16, February 2005, pp.186-208.

[9] Lye K W and Wing J M., Game Strategies in Network Security, International Journal of Information Security, 4, 2005, pp.71-86.

[10] Qing Hu, Paul Hart and Donna Cooke., The Role of External and Internal influences on information systems security— a neo-institutional perspective, Journal of Strategic Information Systems, 16, 2007,pp.153-172.

[11] Li Tianmu, Zhong Weijun and Mei shu-e., Inspection Game Analysis of Intrusion Prevention System Management and Configuration, Journal of Systems Engineering, 23, May 2008,pp.589-595.

[12] Alpcan T. and Basar T., A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection[C], Decision and Control 42nd IEEE Conference 3, 2003,pp. 2595- 2600.

[13] Huseyin Cavusoglu and Srinivasan Raghunathan., Configuration of Detection Software: a Comparison of Decision and Game Theory Approach, Decision Analysis, 9, 2004, pp.131-148.

[14] Piessens F., Taxonomy of Causes of Software Vulnerabilities in Internet Software, The 13th International Symposium on Software Reliability Engineering Location, Annapolis, Maryland,2002, pp.47-52.

[15] Zhu Jianming and Srinivasan Raghunathan., Evaluation Model of Information Security Technologies Based on Game Theoretic, Chinese Journal of Computers, 32, April ,2009,pp.828-834.

[16] Cavusoglu H., Raghunathan S and Cavusoglu H., Configuration of and Interaction between Information Security Technologies, Information Systems Research, 20, 2009, pp.198-217.

[17] Zhang Hongqi., Information Security Technology, HEP, Beijing, 2008, pp.339-358.