Assistant Professor Liu-Rong ZHAO, PhD
E-mail: zhaoliurong@hotmail.com
Nanjing Technology University
Professor Shu-E MEI, PhD
Southeast University
Professor Wei-Jun ZHONG, PhD
Southeast University

AN ECONOMIC ANALYSIS OF THE INTERACTION BETWEEN FIREWALL, IDS AND VULNERABILITY SCAN

Abstract. *In the field of information security, it is worth mentioning that a single security technology cannot resist myriad kinds of risks at all times. Therefore, how to create multi-technology security architecture has become a hot issue. In this paper we study the configuration of and interaction between firewall, IDS and vulnerability scan. It shows that different configuration parameters affect hackers' decision on intrusion. Then we get the complementary condition and conflicting condition of the three technologies by solving the mixed strategy Nash equilibrium, thus guiding the configuration strategy for the firm. In particular, although the vulnerability scan does not prevent the invasion for information security system, based on the interaction analysis of technology combinations, it can also bring positive effects in certain condition if information security system configures the vulnerability scan.*

Key words: *economics of information systems, firewall, IDS, vulnerability scan, technology interaction*

JEL Classification: C72, L86.

1. Introduction:

In the era of a ubiquitously networked world, organizations must avoid costly information security breaches. Unfortunately, they cannot make all of their information 100% secure every minute. The information system security technologies are only as good as their weaknesses or vulnerabilities. With the increasing exposure to cyber attacks, hackers can not only target such computer systems, but also use them to launch attacks against other systems connected to the Internet. Several empirical and theoretical studies support the notion that hackers rationally make their decisions based on the amount of efforts that will be required to succeed in hacking and the rewards from a successful hack, which is partly dependent on how secure the system is [**Schechter S.E., Smith M.D., 2003**]. Thus

there is growing awareness of the need to properly configure the IT technologies that are capable of dealing with the complex and multifaceted decision situations encountered in different attacks.

Any given security technology addresses only specific vulnerabilities, and could possibly create additional vulnerabilities. It is worth mentioning that a single security technology cannot resist myriad kinds of risks at all times. For instance, firewall can control external access at the perimeter, which may prevent the damage that illegal external users inflict on the firm; but it cannot stop the attacks perpetrated by internal users of the system. Distinct form firewall, IDS monitors events occurring in a computer system, which responds to the suspected invasion and process in time. However, its feature database upgrades too slow to catch up with the development of Internet. In the same vein, although vulnerability scan can evaluate the security configuration of the system by scanning the network weaknesses, it cannot prevent the invasion either. In order to ensure dynamic security of network systems, various integrated information technologies are often used to achieve the security goals. There into, the deployment of firewall, IDS and vulnerability scan is a common combination, which can solve the integrated linkage control problem based on attack detection. We expect that configured technologies can make up defects for each other, but they play different roles in different environments, leading to different security strategies for the firm.

In the race to secure data and systems, research conducted by practitioners and academics has primarily focused on technical aspects of information security; rigorous analyses based on economic principles are rare [**Huang C.D., Hu Q., Behara R.S., 2008**]. Clearly，exclusive reliance on either the technical or managerial controls is inadequate. Reviewing the literature, the research methods of information security technology are different from the perspectives of economics and management. The analytic hierarchy process（AHP）was used to address two information security issues: how to spend this limited information security budget most effectively, and how to make the case to the organization’s chief financial officer for an increase in funds of information technologies to further enhance the organization’s information security [**Bodin L.D., Gordon L.A., Loeb M.P., 2005**]. A Genetic Algorithm was presented and evaluated based approach enabling organizations to choose the minimal-cost security profile providing the maximal vulnerability coverage [**Mukul G., Jackie R., Alok C., Jie C., 2006**]. The Technology Acceptance Model was developed to investigate the factors that affect the use of security protection strategies by home computer users in relation to a specific, but crucial security technology for home — a software firewall coverage [**Nanda K., Kannan M., Richard H., 2008**]. In recent years, game theory is considered as a mainstream method to solve the information security technology problems. Game theory was proposed for determining IT security investment levels and compare game theory and decision theory approaches on several dimensions such as the investment levels, vulnerability and payoff from investments [**Cavusoglu H., Raghunathan S., Yue**

W.T., 2008a]. They found that decision theory is inadequate to address decisions about security investment. Modeling the interaction between a firm and hacker's decisions requires game theory. An analytical framework was developed to investigate the competitive implications of sharing security information and investments in security technologies [**Gal-Or E., Ghose A., 2005**]. A novel approach was introduced to extend the basic ideas of applying game theory in stochastic modelling, and presented a framework for evaluation of the impacts of hackers' diversity [**Moayedi B.Z., Azgomi M.A., 2012**].

There are mounts of literatures on problems of information security investment and information security behavior. Most of these studies do not explicitly consider information security technology, and researches in this stream mainly focus on a single technology, thus interaction between security technologies is absent in these models. Two models were established to assist firms in the configuration process of detection software based on the decision and game theory [**Cavusoglu H., Raghunathan S., 2004**]. The strategic interaction between a vendor and a firm was studied in balancing the costs and benefits of patch management [**Cavusoglu H., Cavusoglu H., Zhang J., 2008b**]. The management and configuration of intrusion prevention system were analyzed by inspection game theory [**Li T.M., Zhong W.J., Mei S.E., 2008**]. There are more achievements on the configuration and decision-making on IDS. Cavusoglu et al. represented by detection and false alarm rates in IDS, which determined whether a firm realized a positive or negative value from the IDS [**Cavusoglu H., Mishra B., Raghunathan S., 2005**]. Li et al. analyzed the sequential game model of intrusion detection and real-time response in the network [**Li T.M., Zhong W.J., Mei S.E., 2007**]. Various waiting time policies were examined to deal with the problem of false alarms in IDS [**Ogut H., Cavusoglu H., Raghunathan S., 2008**]. Then the author extended his paper by considering configuration and waiting time decisions jointly [**Ogut H., 2013**]. Tansun and Tamer investigated IDS configuration in network intrusion detection and accessed control systems separately, modeling the interaction between the attackers and IDS [**Tansun A., Tamer B., 2003**], [**Tansun A., Tamer B., 2004**]. The intrusion detection and intrusion response were studied based on incomplete information dynamic game [**Wang W.P., Zhu W.W., 2007**]. Wei and Metin separately showed that a firm can use a mixture of reactive and proactive responses to the alarms generated by IDS, and can analyze cost-based IDS configuration under active or passive responses [**Wei Y.T., Metin C., 2007**], [**Wei Y.T., Metin C., 2010**]. However, few of the above mentioned papers consider the configuration when multiple technologies are deployed as part of layered security architecture. Configuration of and interaction between a firewall and IDS were studied on, and showed 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

environments [**Cavusoglu H., Raghunathan S., Cavusoglu H., 2009**]. The interaction with firewall and IDS was analyzed based on an evolutionary game [**Yin Y., Xia Z.C., 2009**]. The evaluation model of information security technologies was proposed on game theory, which included firewall, intrusion detection system and intrusion tolerant [**Zhu J.M., Raghunathan S., 2009**]. From the discussion above, we get a conclusion that most of the literatures are based on one or two information security technologies, but there are few on more than two technology combinations, rather do they address interaction between security technologies. Based on Zhao et al. [**Zhao L.R., Mei S.E., Zhong W.J., 2011**], our paper explicitly incorporates the discussion of interaction between firewall, IDS and vulnerability scan, which provides the theory guide for firm when deploying these three technologies. This paper aims to analyze the feature of technologies as an optimal information systems strategy by game theory in the context of different invasions. We also present the results using the numerical experiments.

The paper will proceed as follows. Section 2 establishes the security model, in which the information technologies are firewall, IDS and vulnerability scan. We derive that the firm and hackers separately get different mixed strategy Nash equilibriums of IT configuration. And we endogenously discuss the interaction between information technology combinations, especially on conflicting condition and complementary condition. In section 3 we verify our theory by the numerical analysis. Section 4 provides a practical illustration for our analytical results. Section 5 summarizes our conclusions and future research directions.

2. The model

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 firm pursues to minimize its expected loss from intrusions; on the other hand, the hacker pursues to maximize his expected benefit. If the game achieves the balance, a reasonable strategy and proper technical parameter configurations will be the key factors. Davies presented the way that firewalls, IDS and vulnerability assessment are packaged commercially (i.e. in his paper, he defined vulnerability assessment the same as the tool of vulnerability scanner) [**Davies R.M., 2002**]. He considered how these three key technologies interact and attempted to answer the question: “Is this simply a case of more technologies and cost, or does a combination of these technologies provide real advantages?” Four practice advices were qualitatively provided in the end of his paper. In reality, Dragon soft company is one of the most famous security software companies in Taiwan. It proposed the developing design conception of Golden Triangle for information security (Fig. 1), which emphasized

that deploying IDS and vulnerability scan remedy the firewall rules, so that the firewall can block more invasions and increase the reliability of network protection. In practice, according to the network topology 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, and scan the system at regular intervals to find the vulnerabilities of configuration changes and fix them in time. In Cavusoglu's paper, the rational deployment of firewall will always reduce the firm's expected loss [**Cavusoglu H., Raghunathan S., Cavusoglu H., 2009**]. Therefore, we summarize the security technology strategy for the firm, denoted by $S^F \in \{(\text{firewall}, \text{vulnerability scan}), (\text{firewall}, \text{IDS}), (\text{firewall}, \text{IDS}, \text{vulnerability scan})\}$. On the other hand, we denote the hacker's strategy by $S^H \in \{\text{intrusion}, \text{not intrusion}\}$. The game process between the firm and hacker is discussed as follows.

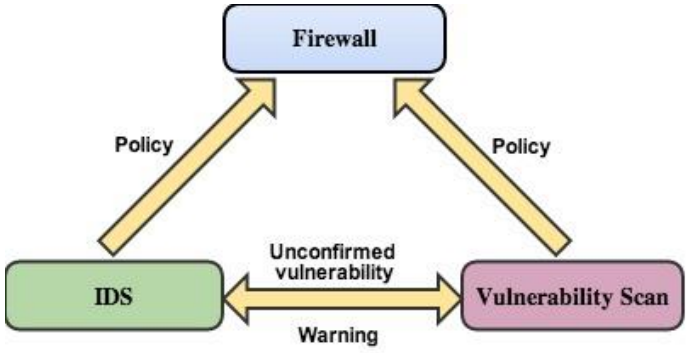

Figure 1. Golden Triangle for information security

Assuming that all participants can access each other's information, the key parameters of the model are defined as follows:

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. The deployment cost of firewall is c_F. When preventing the intrusion by firewall, the benefit of the firm is a, in which $a > c_F, P_D^F \le 1$.
2. Similarly, define probability of IDS detection P_D^I, i.e. P_D^I is the probability that the IDS raises an alarm for an intrusion.

Probability of IDS false negative is $1- P_D^I$ i.e. $1- P_D^I$ is the probability that the IDS does not raise an alarm for an intrusion. The deployment cost of IDS is c_I. When preventing the intrusion by IDS, the benefit of the firm is g, in which $g > c_I, P_D^I \le 1$.

3. The scan frequency of vulnerability scan is P_S, and the deployment cost of vulnerability scan is c_S. When remedying the information security system by vulnerability scan, the benefit of the firm is w, in which $P_S w > c_S, P_S \ge 1$.
4. If the hacker attacks successfully, the loss of firm is d.
5. The probability of deployment of technology combinations is q_i $(i = 1,2,3)$ for the firm, in which q_1 is the probability of combination (firewall, vulnerability scan); q_2 is the probability of combination (firewall, IDS); q_3 is the probability of combination (firewall, IDS, vulnerability scan).
6. The cost of hacker for intrusion is c; if he attacks successfully, the benefit of the hacker is m; but if he is detected, then the punishment of the hacker is b.
7. Denote the probability that a user hacks by y ($y \in [0,1]$).

Lemma 1: When the strategy profile is {(strategy of firm), (strategy of hacker)} = {((firewall, vulnerability scan), only firewall), (hack, not to hack)}, the mixed strategy Nash equilibrium is $y^* = \frac{c_S}{P_S w}$, q_1^* may take any value.

Proof. The game process between the firm and hacker is showed as follows.

Hacker		Hack	Not to hack
Firm	Deploy (firewall, vulnerability scan)	$P_D^F a - c_F - (1- P_D^F)d + P_S w - c_S$, $(1- P_D^F)m - c - P_D^F b$	$a - c_F - c_S$, 0
	Only deploy firewall	$P_D^F a - c_F - (1- P_D^F)d$, $(1- P_D^F)m - c - P_D^F b$	$a - c_F$, 0

When the probability of combination (firewall, vulnerability scan) is $q_1 = 1$, the probability of only deploying firewall is $1 - q_1 = 0$. Denote the benefit of firm by $p_G(1, y)$ or $p_G(0, y)$ in each situation.

We have

$$\pi_G(1,y)=[P_D^F a - c_F - (1- P_D^F)d + P_S w - c_S]y + (a - c_F - c_S)(1- y) \quad (1)$$
$$= (P_D^F - 1)(a + d)y + P_S wy + a - c_F - c_S$$
$$\pi_G(0,y)=[P_D^F a - c_F - (1- P_D^F)d]y + (a - c_F)(1- y) = (P_D^F - 1)(a + d)y + a - c_F \quad (2)$$

From $\pi_G(1,y)=\pi_G(0,y)$, we have $y^* = \frac{c_S}{P_S w}$;

When the probability that a user hacks is $y = 1$, then the probability that a user does not hack is $1-y = 0$. Denote the benefit of the hacker by $\pi_H(q_1,1)$ or $\pi_H(q_1,0)$ in each situation. We have

$$\pi_H(q_1,1)=[(1- P_D^F)m - c - P_D^F b]q_1 + [(1- P_D^F)m - c - P_D^F b](1- q_1) \quad (3)$$
$$\pi_H(q_1,0) = 0 \quad (4)$$

From $\pi_H(q_1,1)=\pi_H(q_1,0)$, we have $P_D^{F*} = \frac{m - c}{m + b}$.

Lemma 2: When the strategy profile is {(strategy of firm), (strategy of hacker)} = {((firewall, IDS), only firewall), (hack, not to hack)}, the mixed strategy Nash equilibrium is $(q_2^*, y^*) = (\frac{(m + b)P_D^F + c - m}{P_D^F P_D^I (m + b) - P_D^I m - P_D^I b}, \frac{c_I}{P_D^I d + P_D^I g - d})$.

Proof. The game process between the firm and hacker is showed as follows.

Hacker		Hack	Not to hack
Firm	Deploy (firewall, IDS)	$P_D^F a - c_F - \lambda(1- P_D^F)d$, $+P_D^I g - c_I$; $(1- P_D^F)(1- P_D^I)m + c$ $- P_D^F P_D^I b - P_D^F(1- P_D^I)b$ $- P_D^I(1- P_D^F)b$	$a - c_F - c_I$, 0
	Only deploy firewall	$P_D^F a - c_F$ $- (1- P_D^F)d$; $(1- P_D^F)m + c$ $- P_D^F b$	$a - c_F$, 0

When the probability of combination as (firewall, IDS) is $q_2 = 1$, the probability of only deploying firewall is $1- q_2 = 0$. Denote the benefit of firm by $\pi_G(1,y)$ or $\pi_G(0,y)$ in each situation. We have

$$\pi_G(1,y)=(P_D^F - 1)(a + d)y + (P_D^I d + P_D^I g - d)y + a - c_F - c_I \quad (5)$$
$$\pi_G(0,y)=(P_D^F - 1)(a + d)y + a - c_F \quad (6)$$

From $\pi_G(1,y)=\pi_G(0,y)$, we have $y^* = \frac{c_I}{P_D^I d + P_D^I g - d}$;

When the probability that a user hacks is $y = 1$, then the probability that a user does not hack is $1-y = 0$. Denote the benefit of the hacker by $p_H^{\text{¢}}(q_2,1)$ or $p_H^{\text{¢}}(q_2,0)$ in each situation. We have

$$p_H^{\text{¢}}(q_2,1)=[(1- P_D^F)(1- P_D^I)m+ c- P_D^F P_D^I b- P_D^F(1- P_D^I)b- P_D^I(1- P_D^F)b]q_2+[(1- P_D^F)m+ c- P_D^F b](1- q_2) \quad (7)$$

$$p_H^{\text{¢}}(q_2,0) = 0 \quad (8)$$

From $p_H^{\text{¢}}(q_2,1)=p_H^{\text{¢}}(q_2,0)$, we have $q_2^* = \dfrac{(m+b)P_D^F + c - m}{P_D^F P_D^I(m+b) - P_D^I m - P_D^I b}$.

Lemma 3： When the strategy profile is {(strategy of firm), (strategy of hacker)} = {((firewall, IDS, vulnerability scan), only firewall), (hack, not to hack)}, the mixed strategy Nash equilibrium is $(q_3^*, y^*) = (\dfrac{(m+b)P_D^F + c - m}{P_D^F P_D^I(m+b) - P_D^I m - P_D^I b}, \dfrac{c_S + c_I}{P_D^I d + P_D^I g - d + P_S w})$.

Proof. The game process between the firm and hacker is showed as follows.

Hacker		Hack		Not to hack
Firm	Deploy (firewall, IDS, vulnerability scan)	$P_D^F a - c_F - 2(1- P_D^F)d$, $+P_D^I g - c_I + P_S w - c_S$	$(1- P_D^F)(1- P_D^I)m+ c$ $- P_D^F P_D^I b - P_D^F(1- P_D^I)b$ $- P_D^I(1- P_D^F)b$	$a - c_F - c_I - c_S$, 0
	Only deploy firewall	$P_D^F a - c_F$, $- (1- P_D^F)d$	$(1- P_D^F)m+ c$ $- P_D^F b$	$a - c_F$, 0

When the probability of combination as (firewall, IDS, vulnerability scan) is $q_3 = 1$, the probability of only deploying firewall is $1- q_3 = 0$. Denote the benefit of firm by $p_G^{\text{¢}}(1,y)$ or $p_G^{\text{¢}}(0,y)$ in each situation. We have

$$p_G^{\text{¢}}(1,y)=(P_D^F - 1)(a+d)y+(P_D^I d + P_D^I g - d)y + P_S w y + a - c_F - c_S - c_I \quad (9)$$

$$p_G^{\text{¢}}(0,y)=(P_D^F - 1)(a+d)y + a - c_F \quad (10)$$

From $p_G^{\text{¢}}(1,y)=p_G^{\text{¢}}(0,y)$, we have $y^* = \dfrac{c_S + c_I}{P_D^I d + P_D^I g - d + P_S w}$;

When the probability that a user hacks is $y = 1$, then the probability that a user does not hack is $1-y = 0$. Denote the benefit of the hacker by $p_H^{\text{¢}}(q_3,1)$ or $p_H^{\text{¢}}(q_3,0)$ in each situation. We have

$$p_H^{\text{¢}}(q_3,1)=[(1- P_D^F)(1- P_D^I)m+ c- P_D^F P_D^I b- P_D^F(1- P_D^I)b- P_D^I(1- P_D^F)b]q_3+[(1- P_D^F)m+ c- P_D^F b](1- q_3) \quad (11)$$

$p_H^{\Phi}(q_3,0) = 0$ （12)

From $p_H^{\Phi}(q_3,1)=p_H^{\Phi}(q_3,0)$, we have $q_3^* = \frac{(m+b)P_D^F + c - m}{P_D^F P_D^I (m+b) - P_D^I m + P_D^I b}$.□

Before we discuss the interaction between technologies by three theorems, the conflicting condition and complementary condition are defined as follows.

Definition 1: When deploying the technology combination (A, B), the benefit of the firm is higher than the situation of deploying only A, then we call technology A is complementary with technology B.

Definition 2: When deploying the technology combination (A, B), the benefit of the firm is less than the situation of deploying only A, then we call technology A is conflicting with technology B.

Theorem 1: When $y < \frac{c_S}{P_S w}$, firewall is conflicting with vulnerability scan; and when $y > \frac{c_S}{P_S w}$, firewall is complementary with vulnerability scan.

Compared the technology combination ((firewall, vulnerability scan), only firewall) by Lemma 1, the mixed strategy Nash equilibrium is $y^* = \frac{c_S}{P_S w}$. So when $y < \frac{c_S}{P_S w}$, the benefit of the firm with deploying the technology combination (firewall, vulnerability scan) is less than deploying only firewall. By the definition 2, firewall is conflicting with vulnerability scan in this condition. Similarly, when $y > \frac{c_S}{P_S w}$, firewall is complementary with vulnerability scan. In addition, q_1^* may take any value, which shows that the vulnerability scan can just estimate the information security system but cannot prevent the intrusion. On the other hand, the firewall's parameter P_D^F does play a role in hacker's strategy. Based on lemma 1, we have $P_D^{F^*} = \frac{m - c}{m + b}$, so when $P_D^F < \frac{m - c}{m + b}$, hacker will intrude the system; while $P_D^F > \frac{m - c}{m + b}$, hacker will not intrude the system. Those facts illustrate that the firm should configure the firewall's parameters according to this condition. Therefore, in order to maximize the safety level and economic benefits, when the firm has enough resources to configure firewall and vulnerability scan technology, it is necessary to assess the information security risks and information security technologies firstly, then the firm needs to estimate the hacker's intrusion by

honeypots and user logs etc. (i.e. discriminating the probability and ways of intrusion). If the intrusion probability is lower (i.e. $y < \frac{c_S}{P_S w}$), the firewall is conflicting with vulnerability scan. In this situation the firm does not need to configure both technologies, which will lead to an economic waste. Only configuring the firewall may resist the invasion from the hacker. However, if the intrusion probability is higher (i.e. $y > \frac{c_S}{P_S w}$), the firm needs to configure both technologies to ensure a certain security level and achieve maximum benefits.

On the other hand, if the firm intends to deter the hacker's intrusion, it critically depends on the configuration parameters of firewall (i.e. P_D^F is greater or less than $\frac{m - c}{m + b}$). After assessing hacker's intrusion, the firm may allow hackers to know its capabilities for defense intrusion by information disclosure, so that the hackers will dispel the intension of hacking. Similarly, based on lemma2 and lemma 3, we have theorem 2 and theorem 3.

Theorem 2: When $y < \frac{c_I}{P_D^I d + P_D^I g - d}$, firewall is conflicting with IDS; and when $y > \frac{c_I}{P_D^I d + P_D^I g - d}$, firewall is complementary with IDS.

Theorem 2 shows that although the interaction between firewall and IDS technology can provide proactive warning of vulnerabilities and reactive detection of exploitation, the IDS still remains a certain probability of false negative. The firm should assess the environment in which it is operating and look out for threats from unexpected directions, then make a tradeoff between the benefits and costs whether deploying IDS. When the intrusion probability is lower, the deployment benefits of IDS are less than its defects (such as manual investigation cost, etc.). In this situation, the optimal strategy of the firm is only to configure the firewall. When the intrusion probability is higher, the defense effect of IDS and interaction with firewall are highlighted comparing the value of information and technology costs while configuring both technologies. In this situation, the optimal strategy of the firm is to simultaneously configure both technologies. Similarly, we can explain the optimal strategy of the firm from Theorem 3.

Theorem 3: When $y < \frac{c_S + c_I}{P_D^I d + P_D^I g - d + P_S w}$, firewall is conflicting with IDS and vulnerability scan; and when $y > \frac{c_S + c_I}{P_D^I d + P_D^I g - d + P_S w}$, firewall is complementary with IDS and vulnerability scan.

Compared lemma 2 with lemma 3 and theorem 2 with theorem 3 respectively, we conclude that the optimal deployment probability of combination

(firewall, IDS) q_2^* is the same as the optimal deployment probability of combination (firewall, IDS, vulnerability scan) q_3^* even with different intrusion probability y . However, additionally deploying vulnerability scan will have different effect on intrusion probability. When the probability of (firewall, IDS) is q_2^*, we have $y^* = \frac{c_I}{P_D^I d + P_D^I g - d}$, denoted by $y = y|_{q_2^*}$; when the probability of (firewall, IDS, vulnerability scan) is q_3^*, we have $y^* = \frac{c_I + c_S}{P_D^I d + P_D^I g - d + P_S w}$, denoted by $y = y|_{q_3^*}$. In the next step, we will compare $y|_{q_2^*}$ with $y|_{q_3^*}$, which is the same process as comparing $y|_{q_3^*} - y|_{q_2^*}$ with 0. With some proofs, we can derive that:

When $c_S(P_D^I d + P_D^I g - d) = c_I P_S w$, we have $y|_{q_3^*} = y|_{q_2^*}$, which shows that there is no difference between deploying (firewall, IDS) and (firewall, IDS, vulnerability scan) for intrusion probability of the hacker. At present, it is difficult to identify any great advantage from running all three technologies.

When $c_S(P_D^I d + P_D^I g - d) > c_I P_S w$, we have $y|_{q_3^*} > y|_{q_2^*}$, which shows that deploying (firewall, IDS, vulnerability scan) for hacker's optimal intrusion probability is higher than deploying (firewall, IDS). Vulnerability scan will bring negative effect on information security system.

When $c_S(P_D^I d + P_D^I g - d) < c_I P_S w$, we have $y|_{q_3^*} < y|_{q_2^*}$, which shows that the firm's strategy of additionally deploying vulnerability scan is superior to the combination (firewall, IDS). The reason is that there is the advantage of strength in depth with each technology providing additional coverage and monitoring the operation of the other technologies, thereby increasing confidence in the security of the overall environment.

Analyzing the theorem1, 2, and 3 in different condition, the optimal game strategy between firm and hacker is different as well. If the firm wants to maximize his benefits, estimation of hacker's strategy parameters is firstly needed with the past empirical data. Afterwards the firm should decide to deploy the proper technology combinations to resist the hacker's attacks. Although vulnerability scan can not prevent the intrusion, from the study of technologies interaction, in particular, additionally deploying vulnerability scan in the information security system may bring the positive effect to the system as well. In the end, these theorems verify the conclusion that deploying more technologies will not contribute to the system in certain situation [**Zhao L.R., Mei S.E., Zhong W.J., 2011**]

. Improper deployment will bring the negative effect to the system, which affects the firm's benefits.

3. Numerical analysis

With numerical analysis we research on the deployment of information security technology combinations of (firewall, vulnerability scan), (firewall, IDS) and (firewall, IDS, vulnerability scan), then the conflicting condition and complementary condition are subsequently discussed.

Case 1: Compare the deployment strategy of (firewall, vulnerability) with only firewall.

Let $P_D^F = 0.6, c_F = 5, a = 40, P_S = 2, c_S = 5, w = 4, d = 30, c = 15, m = 25, b = 30, y_i = \frac{i}{10}, (i = 1,...,10)$, the relationship between the firm's benefits and intrusion probability is shown as Figure 2.

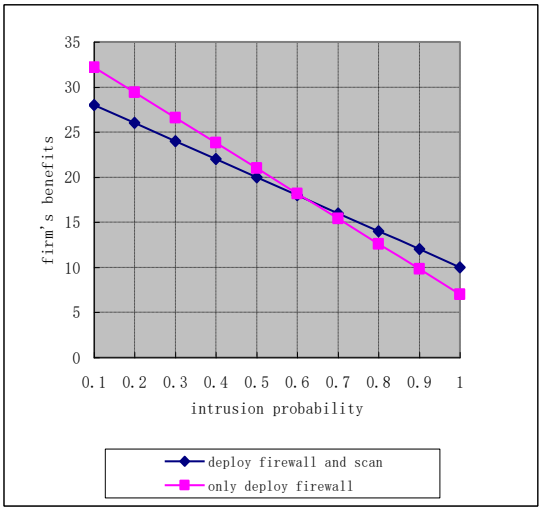

Figure 2. Relationship between the firm's benefits and intrusion probability compared with (firewall, vulnerability scan) and firewall

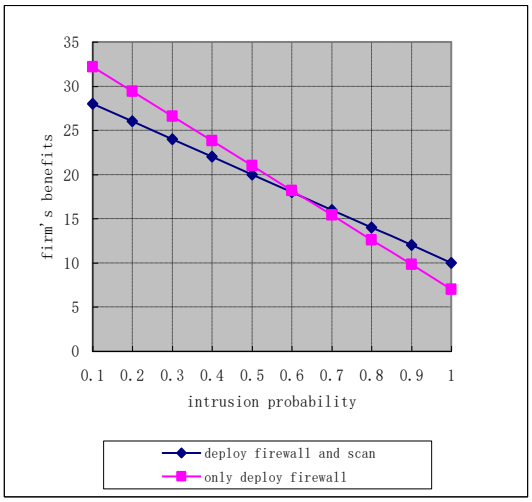

Figure 3. Relationship between the firm's benefits and intrusion probability compared with (firewall, IDS) and firewall

By Lemma 1, we have $y^* = \frac{c_S}{P_S w} = \frac{5}{8}$. By theorem 1, when $y^* < \frac{5}{8}$, the firewall is conflicting with vulnerability scan. As shown in fig. 2, the firm's yield curve of combination (firewall, vulnerability scan) is lower than the curve of only deploying firewall. While $y^* > \frac{5}{8}$, the firewall is complementary with vulnerability scan. Then the firm's yield curve of combination (firewall, vulnerability scan) is higher than the curve of only deploying firewall. We can prove that the curvilinear trend is consistent with theorem 1. Similarly we can explain the curve in case 2 and case 3.

Case 2: Compare the deployment strategy of (firewall, IDS) with only firewall.

Let $P_D^I = 0.4, g = 80, c_I = 5$, while the other parameters keep the same with case 1, then the relationship between the firm's benefits and intrusion probability is shown as Fig.3. By Lemma 2, we have $y^* = \frac{c_I}{P_D^I d + P_D^I g - d} = \frac{5}{14}$. The curvilinear trend is consistent with theorem 2.

Case 3: Compare the deployment strategy of (firewall, IDS, vulnerability scan) with only firewall.

The parameters are the same as case 1 and case 2, then the relationship between the firm's benefits and intrusion probability is shown as Fig.4. By Lemma

3, we have $y^* = \frac{c_S + c_I}{P_D^I d + P_D^I g - d + P_S w} = \frac{5}{11}$. The curvilinear trend is consistent with theorem 3.

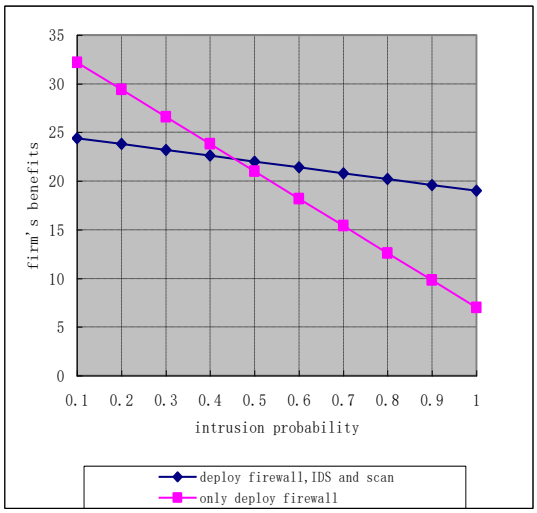

Figure 4. Relationship between the firm's benefits and intrusion probability compared with (firewall, IDS, vulnerability scan) and firewall

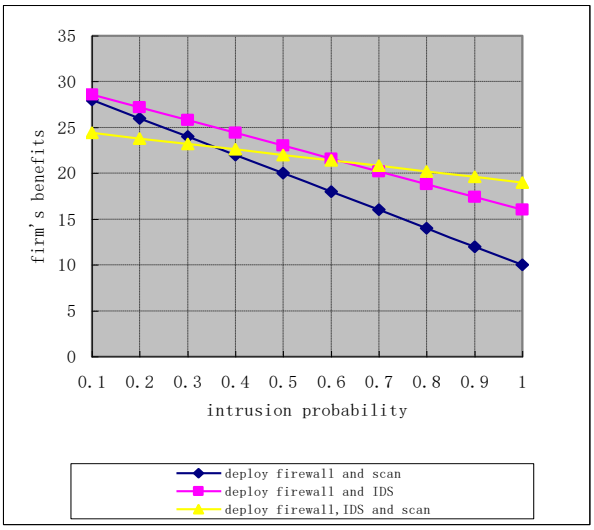

Figure 5. Relationship between the firm's benefits and intrusion probability when deploying three technology portfolios separately

4. A practical illustration

The illustration of the Theorems' results is provided in the next example. An organization is decided to buy information security technologies to reduce the

security risks (i.e. units of all the costs and benefits are thousand dollars). The organization aims to maximize its benefit and minimize its cost face to different threats, or reduce the intrusion probability from the hacker given a benefit goal.

First, the organization engaged security Audit Company to estimate the potential loss from security breach, which would cost the organization 30 in this case. The user log and honeypots technology can record the hacker's behavior and frequency of attacks, thus evaluate the cost of hacker for intrusion is 15. If the hacker attacks successfully, he may have the benefit of 25; if the hacker were caught, his punishment would be 30. In the security software market, the features of firewall, IDS and vulnerability scan are as follows: (1) the probability of firewall detection is 0.6. If the organization deploys the firewall, it would cost 5; and the benefit from preventing the intrusion is 40. (2) The probability of IDS detection is 0.4. If the organization deploys the IDS, it would cost 5; and the benefit from preventing the intrusion is 80. (3) The scan frequency of vulnerability scan is 2. If the organization deploys the vulnerability scan, it would cost 5; and benefit from remedying the information security system is 4. So far it looks like deploying three technologies is the favourite, but as was shown in Fig. 5, more IT combination will not always bring more benefits. The optimal deployment strategy depends on the intrusion probability of the hacker.

If the organization aims to maximize its benefit and minimize its cost face to different threats, the best decision for the organization is to deploy firewall and IDS when intrusion probability is lower than 0.625,because in this situation, the benefit of deploying firewall and IDS will always be higher than those of other technology combinations. On the other hand, when intrusion probability is higher than 0.625, the best decision for the organization is to deploy firewall, IDS and vulnerability scan.

If the organization aims to reduce the intrusion probability from the hacker given a benefit goal, for example, the organization needs to achieve the benefit of 20, then the best decision for the organization is to deploy firewall and vulnerability scan. Because in this situation, the intrusion probability of deploying firewall and vulnerability scan is lower than those of deploying other technology combinations. If the organization needs to achieve the benefit of 24, then the best decision for the organization is to deploy firewall, IDS and vulnerability scan. However, if the organization needs to achieve the benefit of 28.6, the best decision for the organization is to deploy firewall and IDS. Because only deploying firewall and IDS can receive the benefit goal of 28.6 rather than the other technology combinations.

Form the above discussion, the presented example has some limitation, but it can provide an approximate quantitative estimation.

5. Conclusions

This paper studied three technologies interaction based on Golden Triangle for information security, which contributes to the emerging literatures of information security economics in multiple aspects. First, the existed researches mainly focus on the technology of firewall and IDS, but more than three technologies are rarely studied in this field. Also, there are few researches on the vulnerability scan technology in view of economics and management, either on the strategy and deployment of combination with firewall, IDS and vulnerability scan. Our findings offer insights into these three technologies in conflicting and complementary condition based on game theory. By solving the mixed strategy Nash equilibriums, we analyzed the game process between the firm and hacker, which provides the theory guidance for the policymaker when making the security strategy. Finally, the numerical simulations prove our theorems. We figured out that more IT combinations would not bring more benefits. In particular, theorem 1 and theorem 3 show that improper deployments of vulnerability scan will bring the negative effect to the information security system. The vulnerability scan cannot prevent the intrusion; however, it does reduce the hacker's intrusion probability in certain condition. The reason is that vulnerability scan can remedy the firewall and IDS improving their detective effectiveness, which plays a role in preventing the intrusion indirectly.

As with all researches, this study is not without limitations. First, we studies on complete information static game between the firm and hacker. This requires that the players have complete information by the formerly empirical data. For all practical purposes, the change of new technology and firm's structure will lead to an opaque fact in which the players cannot get the complete information each other. Besides, the game is a dynamic and repeated process. However, as its process is fairly complex, it still has practical significance for discussing the deployment of three technologies with complete information static game. Likewise, every information security technology has a large mount of deployment parameters; we just analyze the key parameters such as the probability of firewall detection, the probability of IDS detection and the scan frequency of vulnerability scan etc., whereas the other parameters are not discussed in details.

Our study points to several future directions for research. The first stream would be the interaction between firewall, IDS and vulnerability scan with incomplete information static game. Another extension is to add other parameters of three technologies, which aims to get better information technology strategies. Additionally, we can explore the other information security technology combinations based on game models, such as the combination with firewall, IDS and anti-virus technology; the combination with firewall, IDS and VPN technology, and so on. Furthermore, investigating a real firm as a research object is another direction in the future.

Acknowledgements

The authors would like to acknowledge the financial support of the National Nature Science Foundation of China (No: 71071033) and the Innovation Project of Jiangsu Postgraduate Education (No: CX10B_058Z).

REFERENCES

[1] Bodin, L.D., Gordon, L.A., Loeb, M.P. (2005), ***Evaluating Information Security Investments Using the Analytic Hierarchy Process.*** *Communications of the ACM*, The Association for Computing Machinery;

[2] Cavusoglu, H., Cavusoglu, H., Zhang, J. (2008b), ***Security Patch Management: Share the Burden or Share the Damage?*** *Management Science*, INFORMS;

[3] Cavusoglu, H., Mishra, B., Raghunathan, S. (2005), ***The Value of Intrusion Detection Systems in Information Technology Security Architecture.*** *Information Systems Research*, INFORMS;

[4] Cavusoglu, H., Raghunathan, S. (2004), ***Configuration of Detection Software: A Comparison of Decision and Game Theory Approaches.*** *Decision Analysis*, INFORMS;

[5] Cavusoglu, H., Raghunathan, S., Cavusoglu, H. (2009), ***Configuration of and Interaction between Information Security Technologies: the Case of Firewalls and Intrusion Detection Systems.*** *Information Systems Research*, INFORMS;

[6] Cavusoglu, H., Raghunathan, S., Yue, W.T. (2008a), ***Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment.*** *Journal of Management Information Systems*, M.E. Sharpe;

[7] Davies, R.M. (2002), ***Firewalls, Intrusion Detection Systems and Vulnerability Assessment: A Superior Conjunction?*** *Network Security*, ELSEVIER;

[8] Gal-Or, E., Ghose, A. (2005), ***The Economic Incentives for Sharing Security Information.*** *Information Systems Research*, INFORMS;

[9] Huang, C.D., Hu, Q., Behara, R.S. (2008), ***An Economic Analysis of the Optimal Information Security Investment in the Case of a Risk-Averse Firm.*** *International Journal of Production Economics*, ELSEVIER;

[10] Li, T.M., Zhong, W.J., Mei, S.E. (2007), ***A Sequential Game Analysis of Intrusion Detection and Timeliness Response.*** *Systems Engineering (in Chinese)*, The Association for Systems Engineering of Hunan Province;

[11] Li, T.M., Zhong, W.J., Mei, S.E. (2008), ***Inspection Game Analysis of Intrusion Prevention System Management and Configuration.*** *Journal of Systems Engineering (in Chinese)*, The Association for Systems Engineering of China;

[12] Moayedi, B.Z., Azgomi, M.A. (2012), ***A Game Theoretic Framework for Evaluation of the Impacts of Hackers Diversity on Security Measures.*** *Reliability Engineering and System Safety*, ELSEVIER;
[13] Mukul, G., Jackie, R., Alok, C., Jie, C. (2006), ***Matching Information Security Vulnerabilities to Organizational Security Profiles: A Genetic Algorithm Approach.*** *Decision Support Systems*, ELSEVIER;
[14] Nanda, K., Kannan, M., Richard, H. (2008), ***Locking the Door but Leaving the Computer Vulnerable: Factors Inhibiting Home User's Adoption of Software Firewalls.*** *Decision Support Systems*, ELSEVIER;
[15] Ogut, H., Cavusoglu, H., Raghunathan, S. (2008), ***Intrusion-Detection Policies for IT Security Breaches.*** *Journal on Computing*, INFORMS;
[16] Ogut, H. (2013), ***The Configuration and Detection Strategies for Information Security Systems.*** *Computers and Mathematics with Applications*, ELSEVIER;
[17] Schechter, S.E., Smith, M.D. (2003), ***How Much Security is Enough to Stop a Thief?*** *Springer-Verlag*, New York, ISBN: 3-540-40663-8;
[18] Tansun, A., Tamer, B. (2003), ***A Game Theoretic Approach to Decision and Analysis in Network Intrusion Detection.*** 42nd IEEE Conference on Decision and Control;
[19] Tansun, A., Tamer, B. (2004), ***A Game Theoretic Analysis of Intrusion Detection in Access Control Systems.*** 43rd IEEE Conference on Decision and Control;
[20] Wang, W.P., Zhu, W.W. (2007), ***Network Security Behaviour Model Based on Dynamic Non-Cooperative Game Model with Incomplete Information.*** *Mini-Micro Systems*, Chinese Academy of Sciences;
[21] Wei, Y.T., Metin, C. (2007), ***Intrusion Prevention in Information Systems: Reactive and Proactive Responses.*** *Journal of Management Information Systems*, M.E. Sharpe;
[22] Wei, Y.T., Metin, C. (2010), ***A Cost-Based Analysis of Intrusion Detection System Configuration Under Active or Passive Responses.*** *Decision Support Systems*, ELSEVIER;
[23] Yin, Y., Xia, Z.C. (2009), ***An Evolutionary Game Analysis of the Interaction with Firewall and Intrusion Detection System.*** Proceedings of the Eighth International Conference on Machine Learning and Cybernetics;
[24] Zhao, L.R., Mei, S.E., Zhong, W.J. (2011), ***Optimal Configuration of Firewall, IDS and Vulnerability Scan by Game Theory.*** *Journal of Southeast University*, Southeast University;
[25] Zhu, J.M., Raghunathan, S. (2009), ***Evaluation Model of Information Security Technologies Based on Game Theoretic.*** *Chinese Journal of Computers*, China Computer Federation.