MATEC Web of Conferences **44**, 01016 (2016)
DOI: 10.1051/matecconf/20164401016

A game-theory approach to manage decision errors

Chuan Xi Cai[1], Shu E Mei[1,a] and Wei Jun Zhong[1]

[1]*Department of School of Economics and Management, Southeast University, Nanjing, Jiangsu Province, China*

Abstract. With the fast development of modern computer and networks, information communication between firms and users becomes more complex. Recently, a game-theory approach has been widely used to investigate this issue. However, for firms and users, inaccuracies (defined as decision errors) persist in the gap between strategic decisions and actual actions. This paper, based on game theory, analyses the effects of decision errors on optimal equilibrium strategy of the firm and the user. Precisely speaking, we analysed how the firm and the user adjust their strategy accordingly to compensate for the mistakes caused by decision errors. Besides, we demonstrated that decision errors are not necessarily bad for the firm, and put forward the optimal methods of managing decision errors.
Keyword: Intrusion detection system (IDS); Game-theory; Decision Errors

1 Introduction

With the development of computers and networks, information security problems become increasing important in the key management area. Detection software (i.e., an intrusion detection system, IDS) provides effective supports for security management of information system, but fails to resolve the security problem of information system effectively by only relying on technology, since the environment of information system becomes more complex. Therefore, the economics of information security from the perspective of economics and management theory has developed rapidly in recent years. In the field of economics of information security, game theory has been used as a key research approach. For example, Cavusoglu & Raghunathan, Cavusoglu et al. and Levitin & Hausken give a game-theory analysis of the optimal configurations for security devices [1-3], Gao et al. and Hausken provide a game framework to discuss the investment of information security [4-5].

This paper attempts to discuss how to adjust the optimal strategy in the information system that has decision errors, and how to manage the decision errors. Decision errors are the inaccuracies between strategic decisions and actual actions, which is shown in Figure.1. Zhuang discusses the effect of decision errors by the agents on the social optimal investment in system security [6]. The work (Alpcan & Basar, Nguyen et al.) analyzes the decision errors of firms and users in the field of information security [7-8]. Our work is closely related to a seminal study [9], who analyzes the impact of the firms' and the users' decision errors on the equilibrium strategies and optimal configurations of the IDS.

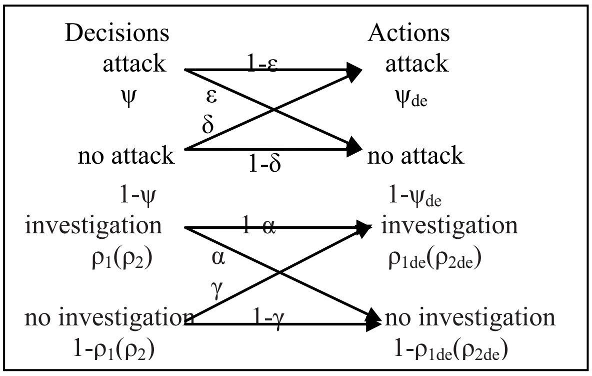

Figure.1. Decision errors of the firms and the users

In this paper, we developed a game-theory framework for the interaction between firms and users that include decision errors, analyzed the impact of decision error on equilibrium strategies and how the firm and the user adjust their strategy accordingly to compensate for the mistakes caused by decision errors. This paper proceeds as follow: section 2 provides a game model of the interaction between the firm and the user. Section 3 derives the equilibrium strategies, the adjustment strategies and the optimal methods of managing decision errors. Section 4 concludes this paper.

2 Model description

2.1 Strategies and notations

Probability of detection is P_D, probability of false negative is $1-P_D$; Probability of false positive is P_F.
$P_D = P$ (classified as attacker | attacking transaction);
$P_F = P$ (classified as attacker | normal transaction);

[a] Corresponding author: meishue@seu.edu.cn

$P_F = (P_D)^L$ (L>1) [10].

Because of the inaccuracy inherent in the IDS, manual investigations from a human security expert are necessary to verify the signal given by the IDS. It is assumed that manual investigations always succeed. We assume that a user's strategy is $S^U \in \{A, NA\}$, in which A is attacking transaction, NA is normal transaction; a firm's strategy is $S^F \in \{(I,I), (I,NI), (NI,I), (NI,NI)\}$, 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 the IDS raises a signal, while the second element is the firm's action when the IDS does not raise a signal. The mixed strategy pair of the firm is given by $(\rho_1, \rho_2) \in [0,1]\times[0,1]$, it is reasonable to assume $\rho_1 \geq \rho_2$, ρ_1 denotes the actual probability of a manual investigation in the presence of a signal, and ρ_2 denotes the actual probability of a manual investigation in the absence of a signal. Similarly, the mixed strategy of the user is given by the actual probability of attacking, $\psi \in [0,1]$.

Now, following [7-8], decision errors are introduced. Assume that parameter ε (parameter δ) denotes the probability that the user decides (not) to attack but ends up not attacking (attacking); and that parameter α (parameter γ) represents the probability that the firm intends (not) to implement manual investigation but ends up not implementing manual investigation (implementing manual investigation) regardless of whether the IDS generates a signal. ψ_{de} is the user's actual probability of attacking. ρ_{1de} (ρ_{2de}) denote the firm's actual probabilities of manual investigation when the IDS (dose not) generates a signal.

When the user attacks, it gains benefit of μ if not caught but receives a penalty of β if caught. The manual investigations incur a cost of c because the firm exerts some effort each time, and the necessary analysis software may be used. If an attack is undetected, the firm incurs a loss of d. If the firm successfully detects the attack, a fraction, $0 \leq \varphi \leq 1$, of d will be recovered. It is reasonable to assume that $c \leq d\varphi$, so that the firm's cost of investigation is not higher than its benefit if it detects an attack.

2.2 The model

The effect of decision errors can be described by the following equations:

$$\psi_{de} = (1-\varepsilon-\delta)\psi + \delta \qquad (1)$$

$$\rho_{1de} = (1-\alpha-\gamma)\rho_1 + \gamma \qquad (2)$$

$$\rho_{2de} = (1-\alpha-\gamma)\rho_2 + \gamma \qquad (3)$$

The following probability computations are used in deriving the equilibrium.

$$P(signal) = P_F + \psi_{de}(P_D - P_F) \qquad (4)$$

$$P(no\ signal) = 1 - P_F - \psi_{de}(P_D - P_F) \qquad (5)$$

$$\eta_1 = P(attack \mid signal) = \frac{\psi_{de} P_D}{P_F + \psi_{de}(P_D - P_F)} \qquad (6)$$

$$\eta_2 = P(attack \mid no\ signal) = \frac{\psi_{de}(1-P_D)}{1 - P_F - \psi_{de}(P_D - P_F)} \qquad (7)$$

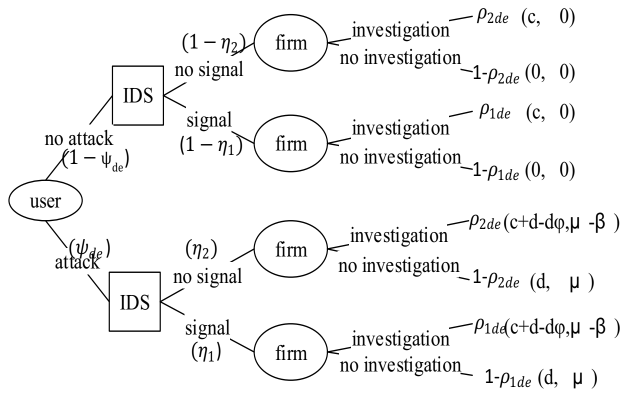

Figure 2. Game tree of our model

The game tree of our model is shown in Figure.2. The firm's expected costs when the IDS generate a signal and does not take the form:

$$M_s(\rho_1, \psi) = c\rho_{1de} + \eta_1(d - d\varphi\rho_{1de}) \qquad (8)$$

$$M_{ns}(\rho_2, \psi) = c\rho_{2de} + \eta_2(d - d\varphi\rho_{2de}) \qquad (9)$$

So, the firm's overall expected cost is

$$M(\rho_1, \rho_2, \psi) = M_s(\rho_1, \psi)P(signal) + M_{ns}(\rho_2, \psi)P(no\ signal) \quad (10)$$

Similarly, the user's expected benefits when the IDS generates a signal and does not take the form:

$$H_s(\rho_1, \psi) = \eta_1(\mu - \beta\rho_{1de}) \qquad (11)$$

$$H_{ns}(\rho_2, \psi) = \eta_2(\mu - \beta\rho_{2de}) \qquad (12)$$

Thus the overall expected benefits is

$$H(\rho_1, \rho_2, \psi) = H_s(\rho_1, \psi)P(signal) + H_{ns}(\rho_2, \psi)P(no\ signal) \quad (13)$$

3 Model analysis

3.1 The optimal strategies

In this section, assume that a simultaneous game is played between the firm and the user. The Nash equilibrium strategies of this game can be solved, in which neither the firm nor the user can improve its utility by unilaterally deviate its strategy.

Proposition 1**:** The following mixed strategy profiles constitute the Nash equilibrium in the presence of decision errors. Due to the limitation of space, the proof is omitted.

If $\mu > \gamma\beta + (1-\alpha-\gamma)\beta P_D$, then

$$\rho_1^* = 1, \rho_2^* = \frac{1}{1-\alpha-\gamma}\left[\frac{\mu - (1-\alpha)\beta P_D}{\beta(1-P_D)} - \gamma\right],$$

$$\psi^* = \frac{1}{1-\varepsilon-\delta}\left[\frac{c(1-P_F)}{c(P_D-P_F) + d\varphi(1-P_D)} - \delta\right];$$

If $\mu < \gamma\beta + (1-\alpha-\gamma)\beta P_D$, then

$$\rho_1^* = \frac{1}{1-\alpha-\gamma}\left[\frac{\mu - \beta\gamma}{\beta P_D}\right], \rho_2^* = 0,$$

$$\psi^* = \frac{1}{1-\varepsilon-\delta}\left[\frac{cP_F}{d\varphi P_D - c(P_D - P_F)} - \delta\right].$$

By substituting α=γ=ε=δ=0 in proposition 1, the equilibrium without decision errors is obtained.

Proposition 2: The following mixed strategy profiles constitute the Nash equilibrium without decision errors.

If $\mu > \beta P_D$, then

$$\rho_1^* = 1, \rho_2^* = \frac{\mu - \beta P_D}{\beta(1-P_D)}, \psi^* = \frac{c(1-P_F)}{c(P_D-P_F)+d\varphi(1-P_D)};$$

If $\mu < \beta P_D$, then

$$\rho_1^* = \frac{\mu}{\beta P_D}, \rho_2^* = 0, \psi^* = \frac{cP_F}{d\varphi P_D - c(P_D - P_F)}.$$

Low detection rates of IDS result in a high level of attacking, and therefore, the firm will not only inspect any users who raise a signal, but also a fraction of the users that do not raise a signal. On the other hand, sufficiently high detection rates of IDS reduce attacking. Therefore, the firm will not inspect any users who do not raise a signal, and, it can only inspect a fraction of the users that raise a signal.

3.2 The optimal configurations

Proposition 3: Decision errors have a great influence on the optimal strategies, and it is not necessary bad for the firm. With the change of decision errors, the firm and the user need to adjust their strategy accordingly to compensate for the mistake, which are illustrated by Table 1.

Table 1. The firm's and the user's adjustment to the strategy because of the decision errors

If	ρ_2^* ψ^*	$\frac{\mu}{\beta} > \frac{\gamma}{\alpha+\gamma}$	$\frac{\mu}{\beta} < \frac{\gamma}{\alpha+\gamma}$
Case1 $\rho_1^*=1$	$\frac{c(1-P_F)}{c(P_D-P_F)+d\varphi(1-P_D)} > \frac{\delta}{\varepsilon+\delta}$	A1 (↑, ↑)	B1 (↑, ↓)
	$\frac{c(1-P_F)}{c(P_D-P_F)+d\varphi(1-P_D)} < \frac{\delta}{\varepsilon+\delta}$	C1 (↓, ↑)	D1 (↓, ↓)
If	ρ_1^* ψ^*	$\frac{\mu}{\beta} > \frac{\gamma}{\alpha+\gamma}$	$\frac{\mu}{\beta} < \frac{\gamma}{\alpha+\gamma}$
Case2 $\rho_2^*=0$	$\frac{c(1-P_F)}{c(P_D-P_F)+d\varphi(1-P_D)} > \frac{\delta}{\varepsilon+\delta}$	A2 (↑, ↑)	B2 (↑, ↓)
	$\frac{c(1-P_F)}{c(P_D-P_F)+d\varphi(1-P_D)} < \frac{\delta}{\varepsilon+\delta}$	C2 (↓, ↑)	D2 (↓, ↓)

The proof is as follow:

Compare proposition 1 with proposition 2, we get:

Case1: If $\mu > \gamma\beta + (1-\alpha-\gamma)\beta P_D$, then $\rho_1^* = 1$,

$$\rho_2^*: \frac{1}{1-\alpha-\gamma}\left[\frac{\mu-(1-\alpha)\beta P_D}{\beta(1-P_D)} - \gamma\right] > \frac{\mu-\beta P_D}{\beta(1-P_D)} \Leftrightarrow \frac{\mu}{\beta} > \frac{\gamma}{\alpha+\gamma},$$

$$\psi^*: \frac{1}{1-\varepsilon-\delta}\left[\frac{c(1-P_F)}{c(P_D-P_F)+d\varphi(1-P_D)} - \delta\right] > \frac{c(1-P_F)}{c(P_D-P_F)+d\varphi(1-P_D)} \Leftrightarrow \frac{c(1-P_F)}{c(P_D-P_F)+d\varphi(1-P_D)} > \frac{\delta}{\varepsilon+\delta};$$

Case2: If $\mu < \gamma\beta + (1-\alpha-\gamma)\beta P_D$, then $\rho_2^* = 0$,

$$\rho_1^*: \frac{1}{1-\alpha-\gamma}\left[\frac{\mu-\beta\gamma}{\beta P_D}\right] > \frac{\mu}{\beta P_D} \Leftrightarrow \frac{\mu}{\beta} > \frac{\gamma}{\alpha+\gamma},$$

$$\psi^*: \frac{1}{1-\varepsilon-\delta}\left[\frac{cP_F}{d\varphi P_D - c(P_D-P_F)} - \delta\right] > \frac{cP_F}{d\varphi P_D - c(P_D-P_F)} \Leftrightarrow \frac{cP_F}{d\varphi P_D - c(P_D-P_F)} > \frac{\delta}{\varepsilon+\delta}.$$

According to Figure.1, when δ is low or ε is high ($\frac{c(1-P_F)}{c(P_D-P_F)+d\varphi(1-P_D)} > \frac{\delta}{\varepsilon+\delta}$, $\frac{cP_F}{d\varphi P_D - c(P_D-P_F)} > \frac{\delta}{\varepsilon+\delta}$), the user needs to increase his decision probability of attacking (ψ), because decision errors cause the user's actual probability of attacking (ψ_{de}) to be decreased. This is shown in section A1, B1, A2 and B2. When δ is high or ε is low ($\frac{c(1-P_F)}{c(P_D-P_F)+d\varphi(1-P_D)} < \frac{\delta}{\varepsilon+\delta}$, $\frac{cP_F}{d\varphi P_D - c(P_D-P_F)} < \frac{\delta}{\varepsilon+\delta}$), the user needs to decrease his decision probability of attacking (ψ), because decision errors cause user's actual probability of attacking (ψ_{de}) to be increased. This is shown in section C1, D1, C2 and D2.

When γ is low or α is high, that is, $\mu/\beta > \gamma/(\alpha+\gamma)$, the firm needs to increase his decision probability of manual investigation (ρ_1 or ρ_2), because decision errors cause the firm's actual probability of manual investigation ($\rho_{1\mathrm{de}}$ or $\rho_{2\mathrm{de}}$) to be decreased. This is shown in section A1, C1, A2 and C2. When γ is high or α is low that is, $\mu/\beta < \gamma/(\alpha+\gamma)$, the firm needs to decrease his decision investigation rate (ρ_1 or ρ_2), because decision errors cause the firm's actual investigation rate ($\rho_{1\mathrm{de}}$ or $\rho_{2\mathrm{de}}$) to be increased. This is shown in section B1, D1, B2 and D2.

To further understand the effect of decision errors on firm's strategies, we compare the firm's expected cost with decision errors and without decision errors. According to Proposition 1 and (10), we have:

If $P_D < (\mu-\gamma\beta)/((1-\alpha-\gamma)\beta)$, then

$$M(\rho_1^*, \rho_2^* \psi^*) = c - c\alpha + \frac{[d-(1-\alpha)d\varphi]c(1-P_F)}{c(P_D-P_F)+d\varphi(1-P_D)},$$

$$\frac{\partial \mathrm{M}}{\partial \alpha} = \frac{c(d\varphi-c)(P_D-P_F)}{c(P_D-P_F)+d\varphi(1-P_D)} > 0$$

If $P_D > (\mu-\gamma\beta)/((1-\alpha-\gamma)\beta)$, then

$$M(\rho_1^*, \rho_2^* \psi^*) = c\gamma + \frac{(d-\gamma d\varphi)cP_F}{d\varphi P_D - c(P_D-P_F)},$$

$$\frac{\partial \mathrm{M}}{\partial \gamma} = \frac{c(d\varphi-c)(P_D-P_F)}{(d\varphi-c)P_D + cP_F} > 0.$$

The firm's loss is composed of two components (investigation cost and expected damage). The investigation cost is increasing in the investigation rate, and the damage cost is increasing in the attacking probability. The value of IDS not only comes from improved detection of attackers, but also from increased deterrence of attackers [2]. With the increase of parameter α, decision errors cause the actual investigation rate to be decreased. It decreases the deterrence of attackers, so the attacking probability increases. Therefore, with the increase of parameter α, decision errors decrease investigation cost, but increase damage cost. Compared to parameter α, parameter γ has opposite effect. With the increase of parameter γ, decision errors decrease damage cost, but increase investigation cost.

When P_D is low, the firm not only inspect any users who raise a signal, but also a fraction of the users that do not raise a signal. Actual probability of manual investigation is changing with parameter α and γ. If P_D is low, when the firm inspect the users who do not raise a signal, with the change of actual investigation rate, the change of damage cost offset the change of investigation cost, causing the firm's total cost no change; when the firm inspect the users who raise a signal, with the decrease of actual investigation rate (with the increase of α), the increase of damage cost more than offset the saving realized in investigation cost, causing the firm's total cost to be increased.

When P_D is high enough, the firm will not inspect any users who do not raise a signal, and, it can only inspect a fraction of the users that raise a signal. If P_D is high, when the firm inspect the users who raise a signal, with the change of actual investigation rate, the change of damage cost offset the change of investigation cost, causing the firm's total cost no change; when the firm inspects the users who do not raise a signal, with the increase of actual investigation rate (with the increase of γ), the increase of investigation cost more than offset the damage cost, causing the firm's total cost to be increased.

Based on the above analysis, it is obvious that decision errors are not necessary bad for the firm except two cases. First is when P_D is low, decision errors cause the actual investigation rate to be decreased. Second is when P_D is high, decision errors cause the actual investigation rate to be increased. Decision errors are not neglected in practice, it will take firm a lot of money to decrease the decision errors. Therefore, the firm needs to decrease the decision errors only in the two cases above.

4 Conclusions

Decision errors should not be neglected in practice. In this paper, we investigate the effects of decision errors on the optimal strategies by developing a game theory framework between the firm and the users. We discuss the effect of decision errors on the optimal configurations and the firm's expected cost, and the adjustment strategy of both the firm and the user. That is how the firm and the user adjust their strategy accordingly to compensate for the mistakes caused by decision errors. Besides, we demonstrate that decision errors are not necessarily bad for the firm, and put forward the optimal methods of managing decision errors.

This paper assumes that both the firm and the user have complete knowledge about decision errors. But both firms and users have imperfect information about decision errors in practice. The optimal methods of managing decision errors is the problem that needs further research in this case.

References

1. H. Cavusoglu, S. Raghunathan. Configuration of detection software: A comparison of decision and game theory approaches. DATA ANAL *Decision Analysis,* **1(3):** 131-148(2004).
2. H. Cavusoglu, B. Mishra, S. Raghunathan. The value of intrusion detection systems (IDSs) in information technology security. INF SYSTEMS RES, **16(1):**28–46(2005)
3. G. Levitin, K. Hausken. Resource distribution in multiple attacks with imperfect detection of the attack outcome. RISK ANAL, **32(2):** 304-318(2012)
4. X. Gao, W. Zhong, S. Mei. Security investment and information sharing under an alternative security breach probability function. INF SYST FRONT, **17(2):** 423-438(2013)
5. K. Hausken. Information sharing among firms and cyber attacks. J ACCOUNT PUBLIC POL, **26(6):** 639-688(2007)
6. J. Zhuang. Impacts of subsidized security on stability and total social costs of equilibrium solutions in an n-player game with errors. ENG ECONOMIST, **55(2):**131–49(2010)
7. T. Alpcan, T. Başar. Network security: A decision and game-theoretic approach. CAMBRIDGE UNIV Press.(2010)
8. K. C. Nguyen, T. Alpcan, T. Basar. Security games with decision and observation errors. *ACC2010* (pp. 510-515). IEEE:(2010)
9. X. Gao, W. Zhong, S. Mei. A game-theory approach to configuration of detection software with decision errors. RELIAB ENG SYST SAFE, **119**, 35-43(2013)
10. H. Cavusoglu, S. Raghunathan. Configuration of and interaction between information security technologies: the case of firewalls and intrusion detection systems. INF SYSTEMS RES, **20(2):**198–217(2009)