Reliability Engineering and System Safety 119 (2013) 35–43

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

A game-theory approach to configuration of detection software with decision errors

Xing Gao*, Weijun Zhong, Shue Mei

School of Economics and Management, Southeast University, Nanjing, Jiangsu, China

ARTICLE INFO

Article history:
Received 19 July 2011
Received in revised form
3 May 2013
Accepted 3 May 2013
Available online 17 May 2013

Keywords:
Detection software
Intrusion detection systems
Game-theory
Decision errors

ABSTRACT

The modern computer and communication networks that firms rely on have become more complex due to their dynamic, distributed and heterogeneous features; it is therefore increasingly important to characterize the interaction between a firm and a user to ensure information security. Recently, a game-theory approach has been widely employed to investigate this issue, including the optimal configurations of the detection software. However, for both the firm and the user, inaccuracies may persist in the gap between strategic decisions and actual actions, due to the effects of irrationality and the error-prone nature of the devices that carry their commands. This paper analyzes the effects of decision errors on the optimal strategies of both the firm and the user and, in particular, on the optimal configurations of the detection software. We finally demonstrate that decision errors can promote several pure equilibrium strategies and that fine-tuning these configurations quickly becomes difficult. Furthermore, we find that decision errors can drastically influence the optimal configurations and expected costs for a firm.

1. Introduction

An increase in the electronic collaboration between various organizations and economic entities has led to sophisticated computer and communication networks. Cyber-attacks frequently take advantage of the propagation of vulnerabilities among these networks. Consequently, information security has recently become a crucial and challenging issue. Detection software (i.e., an intrusion detection system, IDS) can enhance the security level of a firm by monitoring events in network systems, analyzing security problems and alerting security experts [1]. Due to inaccuracies in the IDS, there exist a false-negative failure probability that the IDS will classify a fraudulent transaction as normal and a false-positive failure probability that the IDS will classify a normal transaction as fraudulent. Consequently, further measures, such as manual investigations, are typically undertaken to detect fraudulent transactions more efficiently [8–10].

Earlier contributions regarding information security mainly involved security schemes and technology principles. With the development of information systems, these traditional solutions cannot guarantee a completely secure environment. The economics of information security has developed rapidly in recent years, emphasizing how to address security problems from the perspectives of economic and management theories. In the field of information security economics, game theory has been used as a key research approach. For example, Refs. [8–10] give a game-theory analysis of the optimal configurations for security devices, whereas Refs. [12,14,15] provide a game framework to discuss the investment of information security. Furthermore, there have been many game-theory applications in the security literature [4–7,16–23,27–30].

This paper attempts to further discuss the optimal configurations for detection software in the presence of decision errors. Our work is closely related to a seminal study by Cavusoglu and Raghunathan [8], who compare decision and game-theory approaches toward the optimal strategies of firms and users, as well as the optimal configurations of detection software. The study [8], as well as the subsequent research [9,10], assumes that the strategic decisions of the firm and the user remain fully consistent with their actual actions, implying that these strategic decisions must be implemented accurately. However, decision errors may be inevitable in practice. Decision errors of both the firm and the user occur because of irrationality and because the channels carrying their commands are error-prone [3,24]. In some scenarios, the actual actions of the firm and the user may deviate from their strategic decisions by misjudging their preferences or acting emotionally. Meanwhile, technology devices might lead to errors when these decisions reach imperfect implementation systems. Zhuang [31] discusses the effect of decision errors by the agents on the social optimal investment in system security. The work [3,24] analyzes the decision errors of a firm and a user in the field of information security. Decision errors are also closely associated with certain theoretical analyses, such as the expected profit [2] and static evaluation in a selective game tree search [11]. In

* Corresponding author.
E-mail address: gxingstar@163.com (X. Gao).

0951-8320/$ - see front matter © 2013 Elsevier Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ress.2013.05.004

addition to decision errors, observation errors may occur due to bounded rationality, which causes the players to observe the outcomes of their actions imperfectly [3,22,24]. This paper excludes observation errors and focuses on decision errors. In the context of decision errors, two important questions arise in information security. What are the optimal strategies of the firm and the user? What are the optimal configurations of the IDS?

In this paper, we answer these two questions by developing a game-theory framework for the interaction between the firm and the user that includes decision errors, analyzing the impact of decision errors on the equilibrium strategies and optimal configurations of the IDS. This paper proceeds as follows: Section 2 provides a game model of the interaction between the firm and the user. Section 3 derives the equilibrium strategies and the optimal configurations. Section 4 concludes this paper.

2. The model framework

2.1. ROC curve

There are typically two types of transactions between a firm and a user: a large percentage of legal transactions and a small percentage of illegal transactions. Because illegal transactions may incur a serious monetary loss, the firm usually equips an IDS to classify whether a transaction is normal or fraudulent using pattern recognition. The efficiency (accuracy) of the IDS is characterized by two types of classification rates: a false-positive failure probability that the IDS will classify a normal transaction as fraudulent and a false-negative failure probability that the IDS will classify a fraudulent transaction as normal. Let P_D represent the probability of classifying a fraudulent transaction as fraudulent and P_F represent the probability of classifying a normal transaction as fraudulent, then false-negative and false-positive failure probabilities are given by $1-P_D$ and P_F, respectively. In general, the IDS is expected to have a large P_D and small P_F. However, an increase in one of P_D and P_F is unfortunately tied to an increase in the other. Here, following [8–10], the ROC (receiving operating characteristics) curve that describes the relationship between P_D and P_F is explained in detail.

Statistical analysis serves as an important method for the IDS to judge whether transactions (events) are normal or fraudulent. A statistical description should be created in advance to obtain a threshold value$t$, which characterizes normal transactions. The threshold value may be access times, operation failure times, data flow and time delay. Given an IDS that obtains a numerical score$x$ from transaction data, the IDS classifies a transaction as fraudulent if x exceeds t . Assume that the probability density functions of x for normal and fraudulent transactions are $f_N(x)$ and $f_F(x)$, respectively. It is straightforward that

$$P_D = \int_t^\infty f_F(x)dx \tag{1}$$

$$P_F = \int_t^\infty f_N(x)dx. \tag{2}$$

Assume that the numerical scores for normal and fraudulent transactions follow exponential distributions with parameters λ_N and λ_F, respectively, $\lambda_N > \lambda_F$, which ensures analytical tractability and simultaneously can capture the skewed nature of transaction data well[1]. Then one can explicitly solve P_D and P_F as follows:

$$P_D = \int_t^\infty \lambda_F e^{-\lambda_F x}\, dx = e^{-\lambda_F t} \tag{3}$$

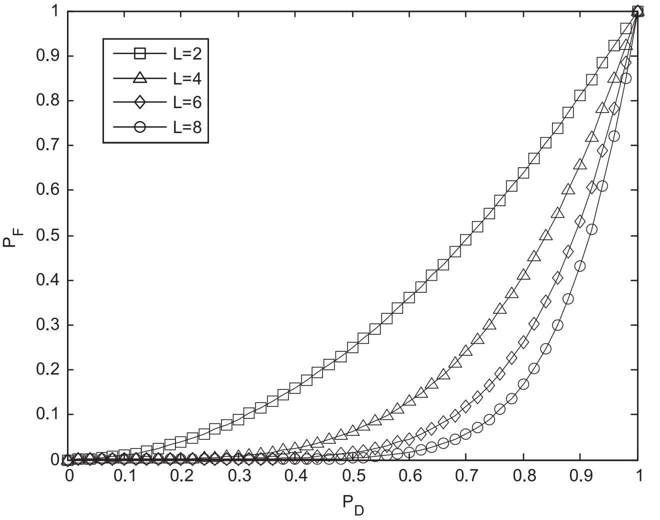

Fig. 1. ROC curve.

$$P_F = \int_t^\infty \lambda_N e^{-\lambda_N x}\, dx = e^{-\lambda_N t}. \tag{4}$$

hence, $P_F = (e^{-\lambda_F t})^{\lambda_N/\lambda_F} = {P_D}^{\lambda_N/\lambda_F} = {P_D}^L$, with $L = \lambda_N/\lambda_F > 1$, as shown in Fig. 1.

2.2. Strategies and notations

Because of the inaccuracy inherent in the IDS, manual investigations from a human security expert are necessary to verify not only the transactions classified as fraudulent by the IDS but also the transactions classified as normal. It is assumed that manual investigations always succeed. The IDS generates a signal when it classifies a transaction as fraudulent. Therefore, the pure strategies of the firm are whether to manually investigate the transaction both when the IDS generates a signal and when it does not generate a signal. That is, the pure strategies consist of (Investigation, Investigation), (Investigation, No investigation), (No investigation, Investigation), and (No investigation, No investigation), where the first element in each strategy pair denotes the decision to be made when the firm observes a signal and the second element represents the decision when the firm fails to observe a signal. However, the pure strategies of the user are to commit fraud and not to commit fraud; that is, (Fraud) and (No fraud). In addition to the pure strategies, the strategies of the firm can be mixed, meaning that the firm manually investigates transactions at certain probabilities (frequencies) in the presence or absence of a signal. The mixed strategy pair of the firm is given by $(\rho_1, \rho_2) \in [0,1] \times [0,1]$, where the first element denotes the probability of a manual investigation in the presence of a signal, and the second denotes the probability of a manual investigation in the absence of a signal. Similarly, the mixed strategy of the user is given by the probability of committing fraud, $\psi \in [0,1]$. Obviously, these mixed strategies reduce to the pure strategies described above when the probabilities reach the boundaries of the related strategy spaces.

Now, following [3,24], decision errors are introduced. For example, the human security expert hired by the firm or the user may be irrational and emotional, implying that they may not take actual actions in accordance with their strategic decisions. In addition, both the devices that help the user commit fraud and

[1] The skewed nature of transaction data is crucial to choose an appropriate probability density function. This nature can be captured very well by exponential distributions. That is why exponential distributions can be readily applied in reliability engineering and complex systems. In particular, literature [25,26] provides some actual transaction data to validate the reasonability.