Computers and Mathematics with Applications 65 (2013) 1234–1253

Contents lists available at SciVerse ScienceDirect

Computers and Mathematics with Applications

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

The configuration and detection strategies for information security systems

Hulisi Öğüt

Department of Business Administration, TOBB University of Economics and Technology, Söğütözü Cad, No:43 Ankara, Turkey

ARTICLE INFO

Keywords:
Intrusion detection system
Base rate fallacy
Configuration policy

ABSTRACT

Intrusion Detection Systems (IDSs) have become an important element of the Information Technology (IT) security architecture by identifying intrusions from both insiders and outsiders. However, security experts questioned the effectiveness of IDSs recently. The criticism known as Base Rate fallacy states that when IDS raises an alarm, the event is more likely to be benign rather than intrusive since the proportion of benign activity is significantly larger than that of intrusive activity in the user population. In response to too many false alarms, system security officers (SSO) either ignore alarm signals or turn off the IDS as the information provided by IDS is very skeptical. To alleviate this problem of IDSs, Ogut et al. (2008) [6] suggest that the firm may choose to wait to get additional signal and to make better decision about user type. One of the limitations of their model is that configuration point at which IDSs operate (the false negative and false positive rates) is exogenously given. However, the firm trying to minimize expected cost should also make a decision regarding the configuration level of IDSs since these probabilities are one of the determinants of future cost. Therefore, we extend Ogut et al. (2008) [6] by considering configuration and waiting time decisions jointly in this paper. We formulate the problem as dynamic programming model and illustrate the solution procedure for waiting time and configuration decision under optimal policy when cost of undetected hacker activity follows step wise function. As it is difficult to obtain waiting time and configuration decision under optimal policy, we illustrate the solution procedures for under myopic policy and focus on the characteristics of configuration decision under myopic policy. Our numerical analysis suggested that configuration decision is as important as waiting time decision to decrease the cost of operating IDS.

1. Introduction

Increasing use of the Internet for conducting business has made firms vulnerable to cyber attacks. Security breaches may compromise confidentiality, integrity and availability of critical information assets. Firms employ a variety of mechanisms to deal with information technology (IT) security breaches. Preventive technologies such as firewalls and anti-virus software are example of such IT security controls and they aim to stop intrusion from outsiders. Detection based systems complement the preventive technologies by detecting intrusions from both outsiders managing to break preventive technologies and malicious insiders who often create serious threat to organization (Secprodonline 2007). One of the most widely employed detective control mechanisms is the Intrusion Detection Systems (IDSs). IDSs try to detect intrusions when they occur by analyzing network packets and system log files. An IDS runs continually in the background and generates an alarm when it detects something that it considers as suspicious, anomalous, or illegal [1,2].

E-mail address: hogut@etu.edu.tr.

0898-1221/$ – see front matter © 2012 Elsevier Ltd. All rights reserved.
doi:10.1016/j.camwa.2012.05.015

The effectiveness of IDSs is measured using two parameters: the likelihood of (i) giving a signal upon an intrusion and (ii) being silent when there is no intrusion. Recently, some security experts evaluate the performance of the IDS in terms of these two measures and report that one of the biggest problems of the IDSs is to raise too many false alarms [3]. The criticism known as the base-rate fallacy states that when IDS raises an alarm, event is more likely to be benign rather than intrusive since the proportion of benign activity is significantly larger than that of intrusive activity in the user population [4]. Thus, the firm incurs high cost if it ignores the base rate (prior) and takes immediate action after every alarm. Base-rate fallacy stems from the well-known Bayes' theorem that shows the relationship among a posterior probability $P(A_i \mid B)$, a prior probability $P(A_i)$, and a conditional probability $P(B \mid A_i)$. Bayes' theorem is stated as the following well-known formula:

$$P(A_i \mid B) = \frac{P(A_i) \cdot P(B \mid A_i)}{\sum_{i=1}^{n} P(A_i) \cdot P(B \mid A_i)}.$$

The base-rate fallacy arises from the fact that when the probability distribution of A is highly skewed, $P(A_i \mid B)$ may become very low. For example, consider an intrusion detection scenario in which there are two types of users: benign and hackers. We assume that the probability that a user is a hacker, P (hacker), is equal to 1/1000. Let the following probabilities define the quality of the IDS: P (alarm signal|hacker) $=P$ (no-alarm signal|benign user) $=0.7$. Using the Bayes' theorem, we can compute P (hacker|alarm-signal) $\cong$ 0.002. In other words, when the IDS raises an alarm, the probability that the user is benign is 99.8%. These probabilities imply that IDS raises too many alarms for benign events. In response to too many false alarms, system security officers (SSO) either ignore alarm signals or turn off the IDS as the information provided by IDS is very skeptical. However, some researchers state that IDSs are the only available mechanism to deal with intrusions that have bypassed preventive technologies and should be used even with their current problems [5].

To alleviate base rate fallacy problem of IDSs, Ogut et al. [6] suggest that the firm may choose to wait to get additional signal and to make better decision about user type rather than terminating user session immediately after an alarm or ignoring all alarms from IDS. However, waiting is costly as hacker may cause more damage to the firm. Consequently, they address the problem of when to take an action following a signal from the IDS by considering the tradeoff between possibilities of more damage and making more informed decision. However, one of the limitations of their model is that the false negative and false positive rates of the IDS are exogenously given. Since configuration decision which is defined as the choice of false alarm probability affects the probability of future alarm and no-alarm signals, these probabilities are one of the determinants of future cost. Thus, the firm trying to minimize expected cost should take into account configuration decision. For this reason, we extend Ogut et al. [6] by considering configuration and waiting time decisions together. The polices developed in this paper can be implemented as a decision support system (DSS) that uses the IDS signals as input to make a recommendation about the optimal level of configuration which is the level of the false alarm probability and when to take action against a user.

We formulate the problem as dynamic programming model and illustrate the solution procedure for waiting time and configuration decisions under optimal policy when cost of undetected hacker activity follows step-wise function. As it is difficult to obtain waiting time and configuration decision under optimal policy, we illustrate the solution procedures for waiting time and configuration decision under myopic policy. We analyzed three cases using linear cost function. When the arrival rate of signal from hacker is greater than arrival rate of signal from benign user, we have found that myopic configuration level increases (decreases) when (i) cost of false alarm becomes lower (higher), (ii) prior probability that user being a hacker increases (decreases), (iii) cost of damage per time unit becomes higher (lower) and (iv) arrival rate of signal from hacker decreases (increases). Changes in the arrival rate of signal from a benign user do not affect the configuration level. When the arrival rate of a signal from a hacker is less than the arrival rate of a signal from a benign user and waiting times under myopic policy are greater than zero, we have found that the myopic configuration policy is not affected by the changes in the prior probability that user is hacker, the cost of false alarm and the damage cost per unit time. However, a more frequent signal from a hacker (benign user) decreases (increases) the configuration level under myopic policy. When the arrival rate of a signal from a hacker is less than the arrival rate of a signal from a benign user and one of the waiting times under myopic policy is equal to zero, configuration level under myopic policy increases (decreases) when (i) cost of false alarm decreases (increases), (ii) the prior probability that a user being a hacker increases (decreases) (iii) damage cost per unit time increases (decreases) and (iv & v) the arrival rate of a signal from a benign user and a hacker decreases (increases). In the simulation, we compare the cost performances of four policies: myopic policy with fixed configuration, optimal policy with fixed configuration, policy with myopic configuration (myopic configuration policy) and policy with optimal configuration (optimal configuration policy). As we expected, the cost incurred under the policy with optimal configuration is the lowest, while the cost incurred under myopic policy with fixed configuration is the highest. In addition, the myopic configuration policy performs better than optimal policy with fixed configuration. Our results from simulation analysis suggested that the behavior of optimal configuration policy is similar to the behavior of myopic configuration policy. For that reason, we believe that theoretical results obtained for myopic policy is likely to hold for optimal policy as well. Furthermore, we observe that the optimal configuration level is higher than the myopic configuration level in our analysis. Moreover, our simulation results show that the myopic configuration policy is nearly identical to the optimal configuration policy.

The organization of the rest of our paper is as follows. In the next section, we review the relevant literature. We describe our model of the intrusion detection problem in Section 3. In Section 4, we derive the optimal policy. In Section 5, we study