Journal of Southeast University (English Edition) Vol. 27, No. 2, pp. 144 – 147 June 2011 ISSN 1003—7985

Optimal configuration of firewall, IDS and vulnerability scan by game theory

Zhao Liurong Mei Shu'e Zhong Weijun

(School of Economics and Management, Southeast University, Nanjing 211189, China)

Abstract: The integrated linkage control problem based on attack detection is solved with the analyses of the security model including firewall, intrusion detection system (IDS) and vulnerability scan by game theory. The Nash equilibrium for two portfolios of only deploying IDS and vulnerability scan and deploying all the technologies is investigated by backward induction. The results show that when the detection rates of IDS and vulnerability scan are low, the firm will not only inspect every user who raises an alarm, but also a fraction of users that do not raise an alarm; when the detection rates of IDS and vulnerability scan are sufficiently high, the firm will not inspect any user who does not raise an alarm, but only inspect a fraction of users that raise an alarm. Adding firewall into the information system impacts on the benefits of firms and hackers, but does not change the optimal strategies of hackers, and the optimal investigation strategies of IDS are only changed in certain cases. Moreover, the interactions between IDS & vulnerability scan and firewall & IDS are discussed in detail.

Key words: economics of information systems; firewall; intrusion detection system (IDS); vulnerability scan; security portfolio strategy

doi: 10.3969/j.issn.1003 – 7985.2011.02.006

With the rapid development of microelectronics and the emergence of the information industry, an important feature of the information age is accessing information and exchanging information by networks. However, the diversification trends of information system security problems are getting evident. Mainstream security technologies include firewall, IDS and vulnerability scan, etc.

The traditional information security technology methods are mainly studied in a purely technical aspect[1-2]. The other methods are studied in economics and management aspects to conduct research on the IT configuration and strategy formulation[3-4]. However, there is little research on the use of IT portfolios[5-8].

1 Information Security Model

In a protected system, the protective measures are usually deployed to defend the security incidents by the system security policy[9]. The information security model is introduced as follows (see Fig. 1).

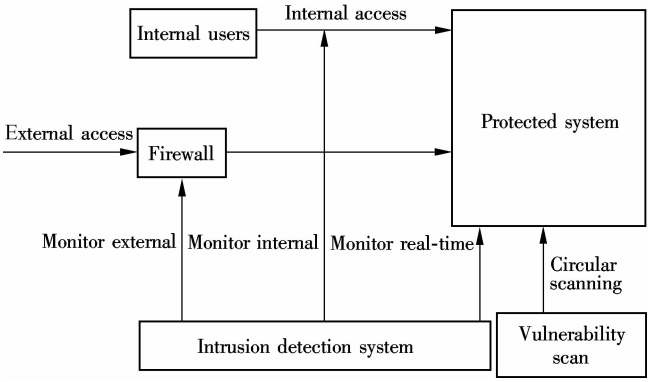

Fig. 1 Information security model

There are four reasonable technology portfolios: only deploying firewall and IDS, deploying none of the technologies, only deploying IDS and vulnerability scan, and deploying all the technologies. Cavusoglu et al.[8] discussed the first two portfolios, while our study focuses on the remaining portfolios. The parameters are defined as follows.

A hacker committing the intrusion derives a benefit of μ if the intrusion is undetected, and he/she incurs a penalty of β if the intrusion is detected, assuming $\mu \leqslant \beta$. Denote the probability that a user hacks by ψ, $\psi \in [0, 1]$.

The firm incurs a cost of c each time when it performs a manual investigation. The firm suffers a damage of d if an intrusion is undetected, and it prevents or recovers a fraction $\varphi(\varphi \leqslant 1)$ of d if an intrusion is detected, assuming that $c \leqslant d\varphi$.

Assume that the probability of firewall detection is $P_{\mathrm{D}}^{\mathrm{F}} = P(\text{classify as a hacker} \mid \text{user is a hacker})$, the probability of a firewall false negative is $1 - P_{\mathrm{D}}^{\mathrm{F}}$, and the probability of a firewall false positive is $P_{\mathrm{F}}^{\mathrm{F}} = P(\text{classify as a hacker} \mid \text{user is a normal user})$. And assume that the probability of IDS detection is $P_{\mathrm{D}}^{\mathrm{I}}$ (i.e. the probability that the IDS raises an alarm for an intrusion), then the probability of an IDS false negative is $1 - P_{\mathrm{D}}^{\mathrm{I}}$, and the probability of an IDS false positive is $P_{\mathrm{F}}^{\mathrm{I}}$ (i.e. the probability that the IDS raises an alarm when there is no intrusion), in which $P_{\mathrm{D}}^{\mathrm{F}} \geqslant P_{\mathrm{F}}^{\mathrm{F}}$, $P_{\mathrm{D}}^{\mathrm{I}} \geqslant P_{\mathrm{F}}^{\mathrm{I}}$[8, 10]. The configuration cost of the vulnerability scan is c_{S}, and the probability of scanner detection is $P_{\mathrm{D}}^{\mathrm{S}}$. As the relationship between IDS and vulnerability scan technologies can be summarized by saying that the vulnerability scan can significantly reduce the number of attackers that an IDS looks for. Simply define that $P_{\mathrm{D}}^{\mathrm{S}} = rP_{\mathrm{D}}^{\mathrm{I}}$, in which $r \in [0, (1 - P_{\mathrm{D}}^{\mathrm{I}})/P_{\mathrm{D}}^{\mathrm{I}}]$.

2 Model Analyses

Assume that all the parameters are common knowledge to all the players. A one-period game is considered in the model[11], which means that all the decisions and outcomes

Received 2010-12-07.

Biographies: Zhao Liurong (1986—), female, graduate; Mei Shue (corresponding author), female, doctor, professor, meishue@seu.edu.cn.

Foundation items: The National Natural Science Foundation of China (No. 71071033), the Innovation Project of Jiangsu Postgraduate Education (No. CX10B_058Z).

Citation: Zhao Liurong, Mei Shu'e, Zhong Weijun. Optimal configuration of firewall, IDS and vulnerability scan by game theory[J]. Journal of Southeast University (English Edition), 2011, 27(2): 144 – 147. [doi: 10.3969/j.issn.1003 – 7985.2011.02.006]

occur in a simultaneous instant. With backward induction, the following two portfolios are discussed in detail.

Portfolio 1 Only deploying IDS and vulnerability scan

Assume that a user's strategy is $S^{U} \in \{H, NH\}$, in which H is to hack, NH is not to hack; the 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 an alarm, while the second element is the firm's action when the 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 $\rho_1 \in [0, 1], \rho_2 \in [0, 1]$ and $\rho_2 \leqslant \rho_1$. The following probability computations are used in deriving the equilibrium.

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

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

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

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

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

The expected cost of the firm for the alarm F_A and the no-alarm F_N states respectively are

$$F_A(\rho_1, \psi) = \rho_1 c + \eta_1 (1 - \rho_1) d + \eta_1 \rho_1 (1 - \varphi) d + c_S \tag{6}$$

$$F_N(\rho_2, \psi) = \rho_2 c + \eta_2 (1 - \rho_2) d + \eta_2 \rho_2 (1 - \varphi) d + c_S \tag{7}$$

Then the firm's overall expected cost is

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

The hacker's expected benefit is

$$H(\rho_1, \rho_2, \psi) = \psi \mu - \psi \beta (\rho_1 (1 + r) P_D^I + \rho_2 (1 - P_D^I - rP_D^I)) \tag{9}$$

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

If $\mu/\beta > P_D^I (1 + r)$, then

$$\rho_1^* = 1, \ \rho_2^* = \frac{\mu - \beta (1 + r) P_D^I}{\beta (1 - P_D^I - rP_D^I)}$$

$$\psi^* = \frac{c (1 - P_F^I)}{d\varphi (1 - P_D^I - rP_D^I) - c (P_F^I - P_D^I - rP_D^I)}$$

If $\mu/\beta < P_D^I (1 + r)$, then

$$\rho_1^* = \frac{\mu}{\beta (1 + r) P_D^I}, \ \rho_2^* = 0$$

$$\psi^* = \frac{cP_F^I}{\varphi d (1 + r) P_D^I + cP_F^I - c (1 + r) P_D^I}$$

If $P_F^I = (1 + r) P_D^I = 1/2$, then

$$\rho_1^* + \rho_2^* = \frac{2\mu}{\beta}, \ \psi^* = \frac{c}{\varphi d}$$

Let the first derivatives of Eqs. (6), (7) and (9) equal 0, then the Nash equilibrium can be derived. Due to the limitation of space, the proof is omitted.

Low detection rates of IDS and vulnerability scan result in a high level of hacking, and, therefore, the firm will not only inspect every user who raises an alarm, but also a fraction of users that do not raise an alarm. On the other hand, sufficiently high detection rates of IDS and vulnerability scan reduce hacking. Therefore, the firm will not inspect any user who does not raise an alarm, and, in fact, it can inspect only a fraction of users that raise an alarm. Especially, when the interactive detection rate of IDS and vulnerability scan and false positive probability of IDS equal 1/2, the optimal strategy for hackers is to intrude the system with the probability of $c/\varphi d$, while $\rho_1^* + \rho_2^* = 2\mu/\beta$.

By substituting $r = 0$ in Proposition 1, the equilibrium is obtained when the firm only implements the IDS.

Proposition 2 The following mixed strategy profiles constitute the Nash equilibrium for the IDS.

If $\mu/\beta > P_D^I$, then

$$\rho_1^* = 1, \ \rho_2^* = \frac{\mu - \beta P_D^I}{\beta (1 - P_D^I)}$$

$$\psi^* = \frac{c (1 - P_F^I)}{d\varphi (1 - P_D^I) - c (P_F^I - P_D^I)}$$

If $\mu/\beta < P_D^I$, then

$$\rho_1^* = \frac{\mu}{\beta P_D^I}, \ \rho_2^* = 0, \ \psi^* = \frac{cP_F^I}{\varphi d P_D^I + cP_F^I - cP_D^I}$$

If $P_F^I = P_D^I = 1/2$, then

$$\rho_1^* + \rho_2^* = \frac{2\mu}{\beta}, \quad \psi^* = \frac{c}{\varphi d}$$

Compared with Proposition 1 and Proposition 2, when the detection probability of the IDS is lower, the intrusion probability of hackers will be increased after adding the vulnerability scan into the system with only IDS. The firm's investigation probability will be increased as well when the IDS does not raise an alarm. So in this case, only deploying the IDS is more efficient. Conversely, when the detection probability of the IDS is higher, the intrusion probability of hackers will be reduced when deploying both the IDS and the vulnerability scan. The firm's investigation probability will be reduced as well when the IDS raises an alarm, which means that, in this case, adding the vulnerability scan into the system is more reasonable. Especially, when $P_F^I = P_D^I = 1/2$, there is no difference for the hackers' optimal strate-

gies whether or not deploying the vulnerability scan into it the system (i.e., $\psi^* = c/\varphi d$ in both cases), so is it for $\rho_1^* + \rho_2^*$.

Portfolio 2 Deploying all the technologies, i.e., firewall, IDS and vulnerability scan

Assume that ε fraction of users is external users, and $1-\varepsilon$ fraction of users is internal users. The other assumptions are the same as Portfolio 1. From Fig. 1, internal users do not go through the firewall, which face the same deployment as Portfolio 1; external users access the system from outside the firewall, and hence are validated by the firewall. The parameters of external users are defined similarly as Eqs. (1) to (9). The proof is omitted.

Proposition 3 The following mixed strategy profiles constitute the Nash equilibrium for firewall, IDS and vulnerability scan.

If $\mu/\beta > P_D^I(1+r)$, $1-\varepsilon > P_D^F$, then

$$\rho_1^* = 1,\ \rho_2^* = \frac{\mu - \beta(1+r)P_D^I}{\beta(1 - P_D^I - rP_D^I)}$$

$$\psi^* = \frac{c(1-P_F^I)}{d\varphi(1-P_D^I - rP_D^I) - c(P_F^I - P_D^I - rP_D^I)}$$

and

$$P_D^F = \frac{[\mu - \beta(1+r)P_D^I](1-\varepsilon)}{\mu - \beta(1+r)P_D^I - (\mu-\beta)\varepsilon}$$

$$P_F^F = \frac{(2-P_F^I)[1-P_D^I - rP_D^I] - (1-P_F^I)(2-P_D^I - rP_D^I - P_D^F)}{1 - P_D^I - rP_D^I}$$

If $\mu/\beta < P_D^I(1+r)$, $1-\varepsilon < P_D^F$, then

$$\rho_1^* = \frac{\mu}{\beta(1+r)P_D^I},\ \rho_2^* = 0$$

$$\psi^* = \frac{cP_F^I}{\varphi d(1+r)P_D^I + cP_F^I - c(1+r)P_D^I}$$

where $P_D^F = 0$, or $\varepsilon = 0$; and $P_F^F = P_F^I P_D^F/((1+r)P_D^I)$.

If $P_F^I = (1+r)P_D^I = P_D^F = P_F^F = 1/2$, then

$$(2-\varepsilon)\rho_1^* + (1-\varepsilon)\rho_2^* = \frac{2\mu}{\beta},\ \psi^* = \frac{c}{\varphi d}$$

As the results show, adding the firewall into the system will impact on the benefits of hackers and firms. However, comparing Portfolio 1 and Portfolio 2, there is no difference for the optimal strategies of hackers. Without the case that $P_F^I = (1+r)P_D^I = P_D^F = P_F^F = 1/2$, investigation strategies of the IDS are not changed either. But it changes in the case $P_F^I = (1+r)P_D^I = P_D^F = P_F^F = 1/2$.

By substituting $r=0$ in Proposition 3, the interaction of firewall parameters and IDS parameters are derived as follows.

Proposition 4 The following mixed strategy profiles constitute the Nash equilibrium for the firewall and IDS.

If $\mu/\beta > P_D^I$, $1-\varepsilon > P_D^F$, then

$$P_D^F = \frac{(\mu - \beta P_D^I)(1-\varepsilon)}{\mu - \beta P_D^I - (\mu-\beta)\varepsilon},\ P_F^F = \frac{1-(1-P_F^I)(1-P_D^F)}{1-P_D^I}$$

If $\mu/\beta < P_D^I$, $1-\varepsilon < P_D^F$, then

$$P_D^F = P_F^F = 0 \text{ or } \varepsilon = 0$$

If $P_F^I = P_D^I = P_D^F = P_F^F = 1/2$, then

$$(2-\varepsilon)\rho_1^* + (1-\varepsilon)\rho_2^* = \frac{2\mu}{\beta},\ \psi^* = \frac{c}{\varphi d}$$

When the probability of IDS detection is lower, the probability of firewall detection will increase as the probability of IDS detection decreases and it will also increase as the external user's fraction decreases. When the probability of IDS detection is higher, the firm should not deploy the firewall (i.e., the probability of firewall detection is 0, or there are no external users, which means that it does not make sense to deploy the firewall). When the detection probability and false positive probability of firewall and IDS are 1/2, there are few external users (especially when $\varepsilon = 0$), and the firm should investigate with twice the probabilities when the IDS raises an alarm than when the IDS does not raise an alarm. Conversely, when there are large amounts of external users (especially when $\varepsilon = 1$), the firm does not have to investigate when the IDS does not raise an alarm, but should investigate with a probability of $2\mu/\beta$ when the IDS raises an alarm.

3 Conclusion

The security model including firewall, IDS and vulnerability scan is investigated by game theory. This paper mainly focuses only on two portfolios: only deploying IDS and vulnerability scan and deploying all the technologies. The Nash equilibrium strategy is derived by analyzing the security technologies selection, interaction and optimal configuration. Although the dynamic game model is not considered, which can enrich the analysis in practice, the effects of the model's parameters can be well reflected by the one-period model as well.

References

[1] Holden G. *Guide to firewalls and network security: with intrusion detection and VPNs* [M]. Boston: Course Technology, 2004.

[2] Gouda M G, Liu A X. Firewall design: consistency, completeness, and compactness [C]//*Proc of the 24th Int Conf on Distributed Computing Systems*. Tokyo, Japan, 2004: 320-327.

[3] Gal-Or E, Ghose A. The economic incentives for sharing security information [J]. *Information Systems Research*, 2005, **16** (2): 186-208.

[4] Lye K W, Wing J M. Game strategies in network security [J]. *International Journal of Information Security*, 2005, **4** (1): 71-86.

[5] Cavusoglu H, Raghunathan S. Configuration of detection software: a comparison of decision and game theory approaches [J]. *Decision Analysis*, 2004, **1** (3): 131-148.

[6] Piessens F. Taxonomy of causes of software vulnerabilities in internet software[C]//*Proc of the 13th Int Symp on Software Reliability Engineering*. Annapolis, ML, USA, 2002:

47 - 52.
[7] Zhu Jianming, Raghunathan S. Evaluation model of information security technologies based on game theoretic [J]. *Chinese Journal of Computers*, 2009, **32** (4): 828 - 834. (in Chinese)
[8] Cavusoglu H, Raghunathan S, Cavusoglu H. Configuration of and interaction between information security technologies: the case of firewalls and intrusion detection systems [J]. *Information Systems Research*, 2009, **20** (2): 198 - 217.
[9] Zhang Hongqi. *Information security technology* [M]. Beijing: Higher Education Press, 2008: 339 - 358. (in Chinese)
[10] Cavusoglu H, Mishra H, Raghunathan S. The value of intrusion detection systems (IDSs) in information technology security [J]. *Information Systems Research*, 2005, **16** (1): 28 - 46.
[11] Gordon L A, Loeb M P. The economics of information security investment [J]. *ACM Transactions on Information and System Security*, 2002, **5** (4): 438 - 457.

基于博弈论的防火墙、入侵检测系统和漏洞扫描技术的最优配置

赵柳榕　梅姝娥　仲伟俊

(东南大学经济管理学院,南京 211189)

摘要:为了解决基于攻击检测的综合联动控制问题,用博弈论方法对防火墙、入侵检测系统(IDS)和漏洞扫描技术的安全组合模型进行分析. 采用逆序归纳法研究了仅配置 IDS 和漏洞扫描技术组合、配置所有技术组合的 Nash 均衡. 结果表明,当 IDS 和漏洞扫描技术检测率较低时,公司不仅需要监测每个报警的用户,还需监测未报警的一部分用户;当 IDS 和漏洞扫描技术检测率足够高时,公司无需监测未报警用户,只需监测一部分报警的用户. 在信息系统中增加配置防火墙会影响公司和黑客的收益,但黑客的最优策略没有变化,IDS 的最优调查策略仅在一定情况下会改变. 此外,讨论了 IDS 与漏洞扫描、防火墙与 IDS 的配置交互问题.

关键词:信息安全经济学;防火墙;入侵检测系统;漏洞扫描;安全组合策略
中图分类号:C931