文章编号: 1001-0920(2008)05-0535-06

信息安全技术投资的自适应模型

董 红[1], 邱菀华[1], 吕俊杰[1], 张 雯[2]
(1. 北京航空航天大学 经济管理学院, 北京 100083; 2. 西北工业大学 计算机学院, 西安 710072)

摘 要: 根据攻防双方信息不对称现象,结合不完全信息博弈论及信息安全的有关理论,构建一个基于成本-收益的信息安全技术选择的投资博弈模型,得出在两种不同的安全技术配置下(仅使用防火墙或防火墙与入侵检测系统共用)博弈双方的最优策略. 通过对用户攻击率、系统响应率和入侵给系统带来的损失及系统的响应成本进行分析比较,探讨了安全技术的价值,从而给出能动态调整安全技术的自适应入侵响应策略. 最后通过实例进一步验证了相关结论.

关键词: 信息安全; 不完全信息博弈; 防火墙; 入侵检测系统; 成本效益
中图分类号: TP309 **文献标识码**: A

Adaptive model of information security technique investment

DONG Hong[1], *QIU Wan-hua*[1], *LV Jun-jie*[1], *ZHANG Wen*[2]
(1. School of Economics and Management, Beijing University of Aeronautics and Astronautics, Beijing 100083, China; 2. School of Computer Science, Northwestern Polytechnical University, Xi'an 710072, China. Correspondent: DONG Hong, E-mail: hudie1998@163.com)

Abstract: Focusing on the asymmetric information between attacker and defender, by applying the methodologies of game theory with incomplete information and network security, a game model of information security technique selections based on cost-benefit is constructed. The study shows the optimal strategies for the players in the deployment of two kinds of security techniques (only deploy firewall or both deploy firewall and intrusion detection systems(IDSs)). Then, by analyzing and comparing with hacking probability, investigation rate, the damage and response cost, the value of security techniques in an organization's IT security architecture is assessed, and thus an adaptive intrusion response strategy is made. Finally, the relative conclusion is illustrated further by an example.

Key words: Information security; Incomplete information game; Firewall; Intrusion detection systems; Cost-benefit

1 引 言

网络的普及和广泛应用,全球信息化水平的不断提高,使得国家和企业遇到的信息安全问题层出不穷,现已成为社会关注的热点问题. 人们不惜投入大量资金,使用各种安全技术和措施提高网络信息系统的安全性. 尽管如此,当前网络与信息安全的现状仍不容乐观. 国家虽然在网络安全方面持续投入,但发生安全事故的几率并未显著降低,各组织机构需在安全战略上重新思考,做出最适合的安全技术投资方案.

在以往信息安全的研究中,主要侧重于从技术角度(如加密、身份认证、访问控制等)保护信息资产,而很少强调信息安全的经济价值,如这些安全技术是否真正发挥了作用,它对一个组织的价值何在?是否安全技术和措施越全面,抵抗攻击的能力越大,期望损失越小?这些问题正是安全技术能否真正得到应用的关键. 因此,从这个角度来看,信息安全是一门以安全技术为基础,综合考虑管理和经济效益的系统工程学.

目前,从经济学角度进行信息安全投资的研究刚刚起步,但却发展迅速[1-4]. Gordon 等[5]构建了一种经济模型,帮助组织进行信息安全的最佳投资决策,但并未考虑负面经济因素对安全投资的影响,也没考虑攻击者的行为对投资策略的影响,即没有涉及博弈理论. Hoo[6]提出了一种决策分析的框架,用于评估各种 IT 安全方针和策略的合理性. 尽管该

收稿日期: 2007-01-16; **修回日期**: 2007-05-23.
基金项目: 国家自然科学基金项目(70372011); 高校博士点专项科研基金项目(20030006009).
作者简介: 董红(1984—),女,山西运城人,博士生,从事信息安全投资、风险决策等研究; 邱菀华(1946—),女,江西临川人,教授,博士生导师,从事管理决策分析、项目管理等研究.

方法很直观,但它将安全技术作为黑箱,无法说明安全技术是如何影响安全风险、期望损失及攻击发生的可能性. 文献[7-9]构建了基于成本的各类攻防博弈模型,对各参与方的成本进行了归纳和整理,但分类粗糙导致了估算精度较低. 文献[10,11]总结了成本效益分析对评估信息安全投资的优越性. 此外,文献[12,13]提出了一种评估信息安全投资的定性与定量相结合的方法,通过计算攻防双方的投资回报率,为决策者更有效地进行安全投资提供了依据,然而此方法仍停留在宏观层面,并未描述安全技术的效用.

现有文献没有提出实现安全效益和经济效益同时最优化的策略,各组织机构在信息安全投资方面仍具有盲目性. 没有任何一种安全技术或措施能为组织提供绝对的保护. 在信息安全体系中,企业通常会使用多种安全技术和防御措施,使入侵者面对多层控制,但这些安全技术是否真正发挥了作用? Cavusoglu 等[14,15]首次评估了 IT 安全技术对企业的价值,重点研究了不同性能配置的入侵检测系统(IDS)对企业和用户的效用模型. 研究表明,IDS 对企业的价值不仅取决于企业的成本参数,更依赖于攻击者的行为. 一个组织应合理配置其防御措施和检测控制措施,才可实现信息保护和信息可用之间的平衡.

文献[14,15]均假设信息是完全的,然而,现实中企业和用户的攻防行为都是在不完全信息条件下进行的. 本文以其研究为基础,通过假设防御方不知道用户攻击成功后的效用,但知道其先验概率引入不完全信息,提出了一个基于成本-效益的信息安全技术投资的综合博弈模型. 在两种不同的安全技术配置下(只使用防火墙或防火墙与 IDS 共用),首先对用户攻击率、系统响应率以及系统执行响应的成本进行评估;然后根据损失评估和响应成本分析调整响应策略,探讨了安全技术对组织的效用,从而达到自适应入侵响应的目的.

2 模型假设

将企业和系统用户作为博弈的双方,攻击者策略地选择攻击行动,企业也应策略地配置安全技术并调整响应策略,使其期望损失最小. 假设如下:

1) 企业:以现实中最常见的两种安全技术配置方式为例:仅使用一种安全技术——防火墙,或同时使用两种技术——防火墙和 IDS. 无论如何配置安全技术,系统管理员都要检查日志文件和分析审计踪迹,对入侵实施人工响应[16,17](后面提到的响应都指人工响应,不考虑自动响应). 然而,由于人工响应成本太高,无法实现实时响应,管理员只能以一定的概率执行响应. 设执行一次响应所需成本为 c,当系统未发现入侵时,企业将遭受 d 的损失;而发现入侵后将挽回损失 d 的一部分,记为 ϕd $(\phi \leq 1)$. 假定 $c \leq \phi d$,即响应成本不高于发现入侵后的收益.

2) 用户:只考虑外部用户(需经防火墙验证身份),其中合法用户为 u. 防火墙允许所有合法用户访问,阻止非法用户进入. 用户要实施入侵,必须首先进入系统. 设用户入侵的概率为 α,入侵未被发现时,用户将获得 μ 的正效用(不考虑入侵成本);否则将受到 κ 的惩罚,即净收益 $\mu - \kappa$. 此外,若合法用户被防火墙阻止,企业将损失 ω.

3) 防火墙和 IDS:防火墙主要用于控制外部用户的访问. 用两个参数衡量防火墙的性能:阻止非法用户访问的概率记为 P_D^F,阻止合法用户访问的概率记为 P_F^F. IDS 是一个以检测和控制为技术本质的主动防御系统,它在网络空间与网络攻击进行体系对体系的对抗. IDS 需对来自入侵探测器的实测结果发出警报以通知系统管理员,但由于现有的入侵检测手段存在不容忽视的虚警和漏警,其检测结果并不完全可信. 因此,设 P_D^I 为存在入侵时 IDS 报警的概率,P_F^I 为不存在入侵时 IDS 报警的概率. IDS 发现入侵后只是简单地报警,并不对可疑用户采取行动,只能通过系统管理员执行人工响应来证实和抵抗入侵.

企业对用户入侵成功后的效用 μ 没有准确了解,只能确定用户是高效用 μ_H 的概率为 ρ,低效用 μ_L 的概率为 $1-\rho$. 用户知道其入侵成功后的真实效用,而企业并不清楚 μ 的高低,只知道其先验概率 $\rho(\mu)$,即 ρ 是共同知识. 因此,本模型中参与人的信息是不完全的. 本文对不完全信息模型进行 Harsanyi 转换,引入"自然"作为虚拟局中人,将不完全信息转化为不完美信息的完全信息博弈,如图 1 所示,图中括号中为各参与方的支付函数.

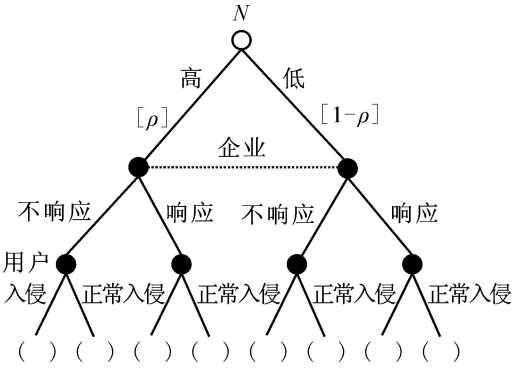

图 1 Harsanyi 转换后的攻防博弈

3 安全技术投资博弈模型

下面分别讨论在两种不同的安全技术配置下,

企业和用户各自的最优策略.

3.1　只有防火墙,没有 IDS 的情况

表 1 给出了对应不同策略组合的支付矩阵. 企业需决定执行人工响应的概率 $\beta,\beta\in[0,1]$,用成本表示企业的效用,收益代表用户的效用. 则企业的期望效用为:入侵给系统带来的损失以及合法用户被阻止的损失之和,即

$$\begin{aligned}C_{\text{firm}}(\alpha,\beta) &= C(\alpha,\beta)+P_F^E\omega=\\ &\beta\{\rho[\alpha(c+(1-\phi)d)+(1-\alpha)c]+\\ &(1-\rho)[\alpha(c+(1-\phi)d)+(1-\alpha)c]\}+\\ &(1-\beta)(\rho\alpha d+(1-\rho)\alpha d)+P_F^E\omega=\\ &\beta\alpha(1-\phi)d+\beta c+\alpha(1-\beta)d+P_F^E\omega. \end{aligned}\tag{1}$$

用户的期望效用为:入侵成功后的收益以及入侵被检测出后的惩罚之和,即

$$\begin{aligned}U_{\text{user}}(\alpha,\beta) &=\\ &\beta[\rho\alpha(\mu_H-\kappa)+(1-\rho)\alpha(\mu_L-\kappa)]+\\ &(1-\beta)(\rho\alpha\mu_H+(1-\rho)\alpha\mu_L)=\\ &\alpha(\rho\mu_H+(1-\rho)\mu_L)-\beta\alpha\kappa. \end{aligned}\tag{2}$$

表 1　企业和用户的期望效用(只存在防火墙)

	用户(高效用 μ_H)	
	入　侵	正　常
企业	响应 $(c+(1-\phi)d,\mu_H-\kappa)$	$(c,0)$
	不响应(d,μ_H)	$(0,0)$
	用户(低效用 μ_L)	
	入　侵	正　常
企业	响应 $(c+(1-\phi)d,\mu_L-\kappa)$	$(c,0)$
	不响应(d,μ_L)	$(0,0)$

对上述效用函数(1) 和(2) 求微分得

$$\alpha=\frac{c}{d\phi},\ \beta=\frac{\rho\mu_H+(1-\rho)\mu_L}{\kappa}.$$

将其带入式(1) 可得企业的期望效用为

$$C_{\text{firm}}(\alpha,\beta)=c/\phi+P_F^E\omega.$$

可见,无论企业是否执行人工响应,用户的最佳入侵策略是以 $\alpha=\frac{c}{d\phi}$ 的概率进行入侵. 同样,无论用户是否入侵,企业应以 $\beta=\frac{\rho\mu_H+(1-\rho)\mu_L}{\kappa}$ 的概率进行人工响应. 混合纳什均衡给出了一种现实解释. 企业对用户入侵成功后是高效用 μ_H 的期望越大,即 ρ 越大,执行响应的概率越大;而随着企业对用户入侵成功后是低效用 μ_L 的期望概率越小,或入侵被检测出来后惩罚 κ 的增大,用户将具有不实施入侵的激励,从而使企业倾向于不实施响应. 同样,随着企业响应成本的增大,或发现入侵后的收益减小,系统管理员将具有不实施响应的激励,从而使得用户倾向于实施入侵活动.

3.2　同时配置防火墙和 IDS 的情况

表 2 给出了 4 种情形下用户与企业的效用函数. 此时,企业需决定两个参数:IDS 报警时执行人工响应的概率 β_1 和 IDS 不报警时的人工响应率 β_2. 则企业的期望效用为:IDS 报警和不报警两种状态下的期望损失,及合法用户被阻止时的损失之和,即

$$C_{\text{firm}}(\alpha,\beta_1,\beta_2)=P_{\text{报警}}C(\alpha,\beta_1)+P_{\text{不报警}}C(\alpha,\beta_2)+P_F^E\omega.\tag{3}$$

其中

$$C(\alpha,\beta_1)=\beta_1 c+\eta_1(1-\beta_1)d+\eta_1\beta_1(1-\phi)d,$$
$$C(\alpha,\beta_2)=\beta_2 c+\eta_2(1-\beta_2)d+\eta_2\beta_2(1-\phi)d.$$

表 2　企业和用户的期望效用(防火墙和 IDS 共用)

		用户(高效用 μ_H)	
		入　侵	正　常
企业	报警	响应$\begin{pmatrix}P_D^I(c+(1-\phi)d),\\ P_D^I(\mu_H-\kappa)\end{pmatrix}$	$(P_F^I c,0)$
		不响应$(P_D^I d,P_D^I\mu_H)$	$(0,0)$
	不报警	响应$\begin{pmatrix}(1-P_D^I)(c+(1-\phi)d),\\ (1-P_D^I)(\mu_H-\kappa)\end{pmatrix}$	$((1-P_F^I)c,0)$
		不响应$\begin{pmatrix}(1-P_D^I)d,\\ (1-P_D^I)\mu_H\end{pmatrix}$	$(0,0)$
		用户(低效用 μ_L)	
		入　侵	正　常
企业	报警	响应$\begin{pmatrix}P_D^I(c+(1-\phi)d),\\ P_D^I(\mu_H-\kappa)\end{pmatrix}$	$(P_F^I c,0)$
		不响应$(P_D^I d,P_D^I\mu_L)$	$(0,0)$
	不报警	响应$\begin{pmatrix}(1-P_D^I)(c+(1-\phi)d),\\ (1-P_D^I)(\mu_L-\kappa)\end{pmatrix}$	$((1-P_F^I)c,0)$
		不响应$\begin{pmatrix}(1-P_D^I)d,\\ (1-P_D^I)\mu_L\end{pmatrix}$	$(0,0)$

给定IDS 报警或不报警的状态下,企业需作出是否执行人工响应的决策. 按照贝叶斯法则可得

$$P_{\text{报警}}=\alpha P_D^I+(1-\alpha)P_F^I,$$
$$P_{\text{不报警}}=\alpha(1-P_D^I)+(1-\alpha)(1-P_F^I),$$
$$\eta_1=P_{(\text{入侵}/\text{报警})}=\frac{\alpha P_D^I}{\alpha P_D^I+(1-\alpha)P_F^I},$$
$$\eta_2=P_{(\text{入侵}/\text{不报警})}=\frac{\alpha(1-P_D^I)}{\alpha(1-P_D^I)+(1-\alpha)(1-P_F^I)}.$$

用 户的期望效用为:入侵成功后的收益及入侵被检测出后的惩罚之和,即

$$U_{user}(\alpha,\beta_1,\beta_2) = \alpha\mu - \alpha\kappa(\beta_1 P_D^I + \beta_2(1 - P_D^I)). \quad (4)$$

命题 1 假定存在入侵时 IDS 报警的概率大于没有入侵时 IDS 报警的概率,即 $P_D^I > P_F^I$;IDS 报警时执行响应的概率大于不报警时响应的概率,即 $\beta_1 > \beta_2$.

比较企业在 IDS 报警和不报警时,执行人工响应的概率. 现实中,企业并不是根据掷硬币的结果选择自己的行动,所以分两种情况讨论,给出纳什均衡解(计算过程见 3.1 节).

当 $\mu = \rho\mu_H + (1-\rho)\mu_L > P_D^I k$ 时,有

$$\beta_1 = 1,\ \beta_2 = \frac{\mu - P_D^I\kappa}{(1 - P_D^I)\kappa},$$

$$\alpha = \frac{c(1 - P_F^I)}{c(P_D^I - P_F^I) + (1 - P_D^I)d\phi}. \quad (5)$$

只有当系统管理员以 1 的概率在 IDS 报警时执行响应,它才会以一定的概率在不报警时实施响应. 因为企业在报警时实施响应的期望效用要大于无报警时响应的效用,即报警时执行响应更有价值.

当 $\mu = \rho\mu_H + (1-\rho)\mu_L \le P_D^I k$ 时,有

$$\beta_1 = \frac{\mu}{P_D^I\kappa},\ \beta_2 = 0,$$

$$\alpha = \frac{cP_F^I}{P_D^I d\phi + c(P_F^I - P_D^I)}. \quad (6)$$

当 IDS 报警时,系统管理员执行响应的概率小于 1,那么在不报警时它不可能去实施响应.

将式(5) 和(6) 带入(3),可得企业的期望效用,即:

当 $\mu = \rho\mu_H + (1-\rho)\mu_L > P_D^I k$ 时,有

$$C_{firm}(\alpha,\beta_1,\beta_2) = \frac{c}{\phi}\frac{\phi d(1 - P_F^I) + \phi(\phi d - c)(P_F^I - P_D^I)}{\phi d(1 - P_D^I) + c(P_D^I - P_F^I)} + P_F^F\omega;$$

当 $\mu = \rho\mu_H + (1-\rho)\mu_L \le P_D^I k$ 时,有

$$C_{firm}(\alpha,\beta_1,\beta_2) = \frac{c}{\phi}\frac{P_F^I}{(1 - c/\phi d)P_D^I + (c/\phi d)P_F^I} + P_F^F\omega.$$

3.3 两种安全技术配置下的分析比较

为了帮助企业更合理地配置安全技术,评估它对组织的价值及效用,本文主要对以下参数进行比较分析.

1) 用户入侵的概率 α

无 IDS 时,$\alpha_{noids} = \frac{c}{d\phi}$.

存在 IDS,当 $\rho > \frac{P_D^I\kappa - \mu_L}{\mu_H - \mu_L}$ 时,有

$$\alpha_{ids} = \frac{c(1 - P_F^I)}{c(P_D^I - P_F^I) + (1 - P_D^I)d\phi} > \alpha_{noids};$$

当 $\rho \le \frac{P_D^I\kappa - \mu_L}{\mu_H - \mu_L}$ 时,有

$$\alpha_{ids} = \frac{cP_F^I}{P_D^I d\phi + c(P_F^I - P_D^I)} \le \alpha_{noids}.$$

企业使用 IDS 时,若

$$\rho > \frac{P_D^I\kappa - \mu_L}{\mu_H - \mu_L}\left(\text{或 } \rho \le \frac{P_D^I\kappa - \mu_L}{\mu_H - \mu_L}\right),$$

则用户入侵的概率比无 IDS 时大(小).

2) 执行人工响应的概率 β

同理可证:存在 IDS 时,企业执行人工响应的概率比不存在 IDS 时响应的概率小,即 $\beta_{ids} < \beta_{noids}$.

3) 总损失 LOSS

这是一个企业最为关心的问题. 它由两部分组成:入侵给组织带来的期望效用(这里指负效用,即期望损失) 和响应成本. 期望损失随着用户入侵次数的增加而增大,响应成本也随着响应次数的增多而增大.

当 $\mu = \rho\mu_H + (1-\rho)\mu_L \le P_D^I k$ 时,有

$$LOSS_{noids} = \text{期望效用} + \text{响应成本} = \frac{c}{\phi} + P_F^F\omega + \frac{\rho\mu_H + (1-\rho)\mu_L}{\kappa}c.$$

其中:$\frac{c}{\phi} + P_F^F\omega$ 为期望效用,包括入侵给系统带来的损失以及合法用户被阻止的损失;$\frac{\rho\mu_H + (1-\rho)\mu_L}{\kappa}c$ 为响应成本,由人工响应率 β 与单位响应成本 c 的乘积构成,$\beta = \frac{\rho\mu_H + (1-\rho)\mu_L}{\kappa}$(见 3.1 节).

$$LOSS_{ids} = \text{期望效用} + \text{响应成本} = \frac{c}{\phi}\frac{P_F^I}{(1 - c/\phi d)P_D^I + (c/\phi d)P_F^I} + P_F^F\omega + (\beta_1 P_{报警} + \beta_2 P_{不报警})c. \quad (7)$$

其中:$\frac{c}{\phi}\frac{P_F^I}{(1 - c/\phi d)P_D^I + (c/\phi d)P_F^I} + P_F^F\omega$ 为期望效用;$(\beta_1 P_{报警} + \beta_2 P_{不报警})c$ 为响应成本(见 3.2 节).

将 $\beta_1 = \frac{\mu}{P_D^I\kappa}, \beta_2 = 0$,

$$P_{报警} = \alpha P_D^I + (1 - \alpha)P_F^I,$$

$$P_{不报警} = \alpha(1 - P_D^I) + (1 - \alpha)(1 - P_F^I),$$

$$\alpha = \frac{cP_F^I}{P_D^I d\phi + c(P_F^I - P_D^I)},$$

$$\mu = \rho\mu_H + (1-\rho)\mu_L,$$

代入式(7) 可得

$$LOSS_{ids} = \frac{c}{\phi}\frac{P_F^I}{(1 - c/\phi d)P_D^I + (c/\phi d)P_F^I} + P_F^F\omega +$$

$$\left[\frac{\rho\mu_H + (1-\rho)\mu_L}{P_D^I\kappa} \quad \frac{P_F^I P_D^I d\phi}{P_D^I d\phi + c(P_F^I - P_D^I)}\right]c =$$

$$\frac{P_F^I}{(1-c/\phi d)P_D^I + (c/\phi d)P_F^I} \times$$

$$\left(\frac{c}{\phi} + \frac{\rho\mu_H + (1-\rho)\mu_L}{\kappa}c\right) + P_F^F\omega.$$

因为 $P_D^I > P_F^I, c \leq \phi d$,

所以 $P_F^I - ((1-c/\phi d)P_D^I + (c/\phi d)P_F^I) = (1-c/\phi d)(P_F - P_D) \leq 0$,

因为 $\frac{P_F^I}{(1-c/\phi d)P_D^I + (c/\phi d)P_F^I} \leq 1$,

所以 $\mathrm{LOSS}_{\mathrm{ids}} \leq \mathrm{LOSS}_{\mathrm{noids}}$.

当且仅当 $c = \phi d$ 时, $\mathrm{LOSS}_{\mathrm{ids}} = \mathrm{LOSS}_{\mathrm{noids}}$.

同理可证, 当 $\mu > P_D^I k$ 时, $\mathrm{LOSS}_{\mathrm{ids}} \geq \mathrm{LOSS}_{\mathrm{noids}}$.

可见, 只有当 $\mu \leq P_D^I\kappa$ 时, 使用 IDS 才可作为直接的威慑措施, 增加对攻击者被检测出的恐惧感. 因此, 入侵的概率要比没有 IDS 时小, 而且系统的响应成本也小于没有 IDS 时的成本, 从而使得 $\mathrm{LOSS}_{\mathrm{ids}} \leq \mathrm{LOSS}_{\mathrm{noids}}$, 此时使用 IDS 技术更有利. 而当 $\mu > P_D^I\kappa$ 时, IDS 系统并没有对攻击者构成威胁, 用户攻击的概率更大, 使期望损失远远大于响应成本的减少量, 直接导致 $\mathrm{LOSS}_{\mathrm{ids}} \geq \mathrm{LOSS}_{\mathrm{noids}}$. 故系统的 $P_D^I\kappa$ 值应尽可能大, 即提高发现入侵时的报警率 P_D^I, 同时增强惩罚力度 κ. 而在现实中, 由于误报和漏报是相互依存的, P_D^I 的提高势必导致没有入侵时报警的概率增大, 使得响应成本和系统费用增大; 此外, 对外部入侵者所能采用的惩罚力度 κ 偏小, 起不到威慑作用. 综上所述, 这正是很多机构不太愿意使用 IDS 等安全技术的原因, 也是黑客活动愈演愈烈的原因之一.

另外, 考虑是否配置 IDS 技术, 还依赖于企业对攻击者入侵成功后的效用属于 μ_H 的预期概率 ρ. ρ 越小, 企业越倾向于使用入侵检测系统. 因此, 企业应综合权衡各因素, 正确评估技术的真正效用, 将资金投入到更有利的安全技术和措施上, 同时实现经济效益和安全效益最大化.

4　算例分析

假设 $\mu_H = 800, \mu_L = 100, P_D^I = 0.7, P_F^I = 0.6, P_F^F = 0.3, \omega = 100, \kappa = 1\,000, \phi = 0.7, c = 50, d = 10\,000$, 如何配置安全技术可使总损失最小.

1) 当 $\rho > \frac{P_D^I\kappa - \mu_L}{\mu_H - \mu_L} = 6/7$ 时, 只使用防火墙.

设 $\rho = 1$, 则

$\alpha_{\mathrm{noids}} = 7.14‰, \alpha_{\mathrm{ids}} = 9.52‰, \alpha_{\mathrm{ids}} > \alpha_{\mathrm{noids}}$,

$\beta_1 = 1, \beta_2 = 0.33, \beta_{\mathrm{noids}} = 0.8$,

$P_{\text{报警}} = \alpha P_D^I + (1-\alpha)P_F^I = 60.1\%$,

$P_{\text{不报警}} = \alpha(1-P_D^I) + (1-\alpha)(1-P_F^I) = 39.9\%$,

$\beta_{\mathrm{ids}} = 0.732\,7 < \beta_{\mathrm{noids}}, \mathrm{LOSS}_{\mathrm{noids}} = 141.43, \mathrm{LOSS}_{\mathrm{ids}} = 146.27, \mathrm{LOSS}_{\mathrm{ids}} > \mathrm{LOSS}_{\mathrm{noids}}$.

2) 当 $\rho \leq \frac{P_D^I\kappa - \mu_L}{\mu_H - \mu_L} = 6/7$ 时, 应同时使用防火墙和 IDS. 设 $\rho = 1/2$, 则

$\alpha_{\mathrm{noids}} = 7.14‰, \alpha_{\mathrm{ids}} = 6.12‰, \alpha_{\mathrm{ids}} \leq \alpha_{\mathrm{noids}}$,

$\beta_1 = 0.64, \beta_2 = 0, \beta_{\mathrm{noids}} = 0.45$,

$P_{\text{报警}} = \alpha P_D^I + (1-\alpha)P_F^I = 60\%$,

$P_{\text{不报警}} = \alpha(1-P_D^I) + (1-\alpha)(1-P_F^I) = 40\%$,

$\beta_{\mathrm{ids}} = 0.384 < \beta_{\mathrm{noids}}, \mathrm{LOSS}_{\mathrm{noids}} = 123.93, \mathrm{LOSS}_{\mathrm{ids}} = 110.59, \mathrm{LOSS}_{\mathrm{ids}} < \mathrm{LOSS}_{\mathrm{noids}}$.

5　结　　论

本文从博弈论的角度, 导出了在不完全信息条件下的自适应安全技术配置及入侵响应的最优策略, 并探讨了安全技术对组织的真正价值. 评估入侵的损失及分析响应成本, 是信息安全技术投资的自适应模型研究的目的之一. 本文采用逆向归纳法, 首先评估出在两种既定的安全技术配置下, 攻击给系统带来的潜在损失及响应成本; 然后根据损失评估和响应成本重新配置安全技术, 并调整响应策略, 达到快速响应. 研究表明, 安全技术的配置与存在入侵时 IDS 的报警率、对入侵者的惩罚力度及对用户效用高低的先验概率等因素有关. 当 $\rho > \frac{P_D^I\kappa - \mu_L}{\mu_H - \mu_L}$ 时, 使用防火墙技术更有效; 而当 $\rho \leq \frac{P_D^I\kappa - \mu_L}{\mu_H - \mu_L}$ 时, 同时使用防火墙和 IDS 对组织更有价值. 此模型的构建和分析适用于各种组织, 尤其对政府、航空航天等涉及国家重要机密的机构尤为重要. 决策者应选用最具投资效益的安全技术, 动态调整入侵响应策略, 以提高信息系统的安全性及抵抗攻击的能力.

不同组织机构应根据自身情况对安全提出明确需求, 选用合理的安全技术, 避免盲目投资, 同时实现安全效益和经济效益的最大化. 这也是下一步研究工作的内容之一, 即不同性质企业的安全投资问题. 此外, 安全技术配置方案及响应策略不是一成不变的, 它随着攻击行为的变化而变化, 所以, 多阶段的动态攻防博弈及随机博弈是将来的研究热点.

参考文献(References)

[1] Anderson R. Why information security is hard — An economic perspective [C]. Proc of the 17th Annual Computer Security Applications Conf. New Orleans, 2001: 358-361.

[2] Campbell K, Gordon L, Loeb M, et al. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market[J].

J of Computer Security, 2003, 11(3): 431-448.
[3] Gordon L, Loeb M, Lucyshyn W. Information security expendituresand real options: A wait-and-see approach [J]. Computer Security, 2003, 19(2): 1-7.
[4] Gordon L, Loeb M, Lucyshyn W. Sharing information on computer systems security: An economic analysis [J]. J of Accounting Public Policy, 2003, 22(6): 461-485.
[5] Gordon L, Loeb M. The economics of information security investment[J]. ACM Trans IS Security, 2002, 5(4): 438-457.
[6] Hoo K J S. How much is enough? A risk management approach to computer security [D]. San Franciso: Stanford University, 2000.
[7] Lee W, Fan W, Miller M, et al. Toward cost-sensitive modeling for intrusion detection and response[J]. J of Computer Security, 2001, 10(1): 5-22.
[8] Meadows C. A cost-based framework for analysis of denial of service in networks [J]. J of Computer Security, 2001, 9(1/2): 143-164.
[9] Wei H, Frinke D, Carter O, et al. Cost-benefit analysis for network intrusion detection system[C]. CSI 28th Annual Computer Security Conf. Washingten, 2001: 29-31.
[10] Gordon L A, Loeb M P. Budgeting process for information security expenditures[J]. Communication of the ACM, 2006, 49(1): 121-125.
[11] RT Mercuri. Security watch: Analyzing security costs [J]. Communications of the ACM, 2003, 46(6): 15-18.
[12] Bistarelli S, Fioravanti F, Peretti P. Defense trees for economic evaluation of security investments[C]. Proc of the 1st Int Conf on Availability, Reliability and Security. Vienna, 2006: 416-423.
[13] Cremonini M, Martini P. Evaluating information security investments from attackers perspective: The return-on-attack (ROA) [C]. Proc of the 4th Workshop on the Economics of Information Security. Cambrige: Massachusetts, 2005.
[14] Cavusoglu H, Mishra B, Raghunathan S. The value of IDS in IT security architecture [J]. Information Systems Research, 2005, 19(1): 28-46.
[15] Cavusoglu H, Mishra B, Raghunathan S. A model for evaluating IT security investments [J]. Communications of the ACM, 2004, 47(7): 87-92.
[16] Mc Hugh J, Christie A C, Allen J. Defending yourself: The role of intrusion detection systems [J]. IEEE Software, 2000, 17(5): 42-51.
[17] NIST Publication 800-12, An introduction to computer security[S].

(上接第 534 页)

参考文献(References)

[1] Crassidis J L, Markley F L. Sliding mode control using modified rodrigues parameters [J]. J of Guidance, Control and Dynamics, 1996, 19(6): 1381-1383.
[2] Zeng Y, Araujo A D, Singh S N. Output feedback variable structure adaptive control of a flexible spacecraft[J]. Acta Astronautica, 1999, 44(1): 11-22.
[3] Hu Q L, Ma G F. Vibration suppression of flexible spacecraft during attitude maneuvers[J]. J of Guidance, Control and Dynamics, 2005, 28(2): 377-380.
[4] Hu Q L, Ma G F. Variable structure control and active vibration suppression of flexible spacecraft during attitude maneuver [J]. Aerospace Science and Technology, 2005, 9(1): 307-317.
[5] Hu Q L, Ma G F. Control of three-axis stabilized flexible spacecrafts using variable structure strategies subject to input nonlinearities[J]. SAGE J of Vibration and Control, 2006, 12(6): 659-681.
[6] Hu Q L, Ma G F. Spacecraft vibration suppression using variable structure output feedback control and smart Materials [J]. ASME J of Vibration and Acoustics, 2006, 128(2): 221-230.
[7] Iyer A, Singh S N. Variable structure slewing control and vibration damping of flexible spacecraft [J]. Acta Astronautica, 1991, 25(1): 1-9.
[8] Song G, Kotejoshyer B. Vibration reduction of flexible structures during slew operations[J]. Int J of Acoustics and Vibration, 2002, 7(2): 105-109.
[9] Di Gennaro S. Output stabilization of flexible spacecraft with active vibration suppression[J]. IEEE Trans on Aerospace and Electronic Systems, 2003, 39(3): 747-759.
[10] Krstic M, Kanellakopoulos I, Kokotovic P. Nonlinear and adaptive control design[M]. New York: Wiley, 1995.