

基于博弈论的信息安全技术评价模型

朱建明¹⁾ Srinivasan Raghunathan²⁾

¹⁾(中央财经大学信息学院 北京 100081)

²⁾(德克萨斯大学达拉斯分校管理学院 德州 75083, 美国)

摘 要 信息安全在企业信息系统建设中越来越重要,如何评价信息安全技术成为当前的一个研究课题.文中基于博弈论,对由防火墙、入侵检测系统和容忍入侵技术构成的三层安全体系结构进行了分析,提出了对信息安全技术进行评价的模型.在对入侵检测系统分析评价的基础上,重点分析了防火墙、入侵检测与容忍入侵的相互影响和关系.研究表明,IDS的检测率、误报率与防火墙的性能有密切关系,系统安全配置直接影响信息安全机制的性能和成本效益,容忍入侵机制取决于入侵的损失评估、系统的成本和防火墙与IDS的性能.信息安全机制的优化配置对于信息安全的效应具有重要影响.

关键词 安全;入侵检测;评估;博弈论

中图法分类号 TP309

DOI号: 10.3724/SP.J.1016.2009.00828

Evaluation Model of Information Security Technologies Based on Game Theoretic

ZHU Jian-Ming¹⁾ Srinivasan Raghunathan²⁾

¹⁾(School of Information, Central University of Finance and Economics, Beijing 100081)

²⁾(School of Management, University of Texas at Dallas, Richardson, Texas 75083, USA)

Abstract Information security is more and more important in a firm's information systems. How to value the information security technologies is an important research issue recently. In this paper, the evaluation model of information security technologies is proposed based on game theory. And the information security technologies include firewall, intrusion detection system and intrusion tolerant which construct the three layers architecture. First, the value of intrusion detection system is presented. Then the relation between firewall, intrusion detection and intrusion tolerant is analyzed. It is found that the detection rate and false alarm rate are affected by the performance of the firewall. Research results show that the configuration of the information security technologies determines whether these technologies realized a positive or negative value. Intrusion tolerant is determined by the loss incurred by intrusion, the cost of the redundancy of the system, and performance of firewall and intrusion detection. It is important to a firm by optimal configuration for information security technologies.

Keywords information security; intrusion detection; evaluation; game theory

1 引 言

随着社会信息化水平的不断提高和电子政务与

电子商务的快速发展,信息系统与计算机网络的基础性、全局性作用日益增强.信息资源已经成为重要的生产要素、无形资产和社会财富,信息网络更加普及并日趋融合.信息系统受到入侵可能会给用户造

成巨大损失,特别是对于像军事、金融、电力等关键信息系统而言其安全性就更加重要。因此,政府和企事业单位都非常重视信息安全,在信息安全方面的投入持续增加,以期降低信息安全事件造成的损失,获得信息安全的保障^[1]。政府管理部门也强制或指导相关单位加强信息安全建设,如公安部制定了《计算机信息系统安全保护等级划分准则》,对信息安全提出了明确的要求。

通常,信息安全机制主要有两大类,即预防和检测。预防的信息安全技术代表是防火墙,其主要作用是过滤访问请求,阻止入侵发生;检测的技术主要有入侵检测系统(IDS),其主要作用是检测是否存在入侵事件^[2-3]。由于预防机制完全阻止入侵是不可能的,因此入侵检测就成为重要的信息安全技术。入侵检测作为动态安全技术中最核心的技术之一,能够实时地全面监控网络、主机和应用程序的运行状态,主动对计算机网络系统中的入侵行为进行识别和响应,提供了对内部攻击、外部攻击和误操作的实时检测,有效弥补了安全防御技术的不足。当一个潜在的入侵被检测到时,IDS会报警,表示有入侵存在。IDS报警后,系统自动响应,或由管理员检查事件并做出相应的响应。但是IDS的性能并不是完美的,存在误报和漏报的问题。这一现象可能会使管理员忽视IDS的报警,甚至认为IDS无用。2003年Gartner研究报告就曾指出IDS市场失败,建议企业将安全预算用在预防机制的建立上^①。2006年Gartner的报告再次强调新的技术会带来新的安全漏洞,什么时候采用什么技术对于企业来说是一个关键^②。因此,对信息安全技术的价值进行有效的评价就非常重要。

在信息安全技术应用方面,还有一个问题是信息安全机制的配置。同样的信息安全技术同样的应用环境采用不同的配置会产生不同的效果,这是一个安全管理的问题。对于防火墙来说,通过配置可以控制过滤的粒度。对于IDS来说,通过优化配置可以降低IDS的误报率和漏报率。但是在配置的过程中也会出现“顾此失彼”的问题,即减少了一种类型的错误,却会导致另一种类型错误的发生。对于企业信息系统而言,如何有效配置与管理企业的信息安全体系也是影响信息安全价值的重要因素。

当前,对信息安全技术的评价有许多种,但多数是从技术的角度,评价系统的安全性、可靠性和性能的。特别是对于IDS来说,主要是从技术的角度评价其检测率、误报率和漏报率。文献[4]对IDS的测

评内容包括有效性、实时性、可扩展性、易用性、容错性和处理性能等,其中有效性是IDS性能的重要衡量标准,主要体现在漏报率和误报率上。性能良好的IDS能将入侵事件的误报率和漏报率控制在一定范围内。本文基于博弈论对信息安全技术的价值进行评价,在文献[1]的基础上进行了扩展,特别是综合评价企业信息安全体系结构的成本与收益,为企业确定信息安全的最优策略提供依据。

本文第2节讨论有关信息安全技术评价方法的研究现状;第3节给出一个通用的信息安全体系结构模型,作为评价的参考模型;第4节运用博弈论对信息安全技术的价值进行分析和评价;第5节进行总结。

2 相关研究现状

安全是未来计算机体系结构研究中的最大挑战之一^③,其中对信息安全技术的评价是一个重要的研究内容。当前对信息安全技术的评价主要有两大类,一类是从技术的角度,评价信息安全技术的有效性和性能;另一类是应用经济学、管理学和统计学的方法对信息安全技术的价值进行评价^[1-8]。但是随着系统复杂度的不断增加,对信息安全的测试和评价越来越难。文献[9]提出了一套在恶意环境下评价信息安全体系结构的基准BASS(BASS1.0由7个基准组成)并开发了相应的程序。

当前从经济学和管理学的角度对信息安全技术的评价已经引起信息安全领域的重视^④。Ulvila和Gaffney提出了一个决策理论模型来判断IDS的最优运行点,并对IDS进行评价^[5]。文献[1]运用博弈论对IDS的价值进行了分析,文献[6]给出了在限定系统管理员检查率的条件下的IDS评价模型。文献[10]提出了一个评价IT安全投资的模型,为企业投资安全技术给出了若干参数。但是多数评价模型是建立在一种安全技术上的,对信息安全技术的

① Gartner. Hype cycle for information security. Gartner Research Report (May 30), Stamford, CT, 2003. <http://www.bus.umich.edu/KresgePublic/Journals/Gartner/research/115100/115119/115119.pdf>

② Gartner. Hype cycle for information security. Gartner Research Report (10 July), Stamford, CT, 2006. http://www.securitytechnet.com/resource/security/consulting/imperva_1914.pdf

③ Revitalizing Computer Architecture Research, CRA Conference on Grand Research Challenges, Dec. 2005, http://www.cra.org/Activities/grand_challenges/architecture/home.html

④ The Economics of Information Security. <http://infoseccon.net/workshop/bibliography.php>

综合评价还很少.

从博弈论的观点来看,信息安全实际上是信息保护者(如企业)与入侵者之间的博弈.将这一问题模型化,保护信息安全的一方希望最小化信息安全事件的损失,而入侵的一方希望进入信息系统,获得更大的利益.在博弈中,企业基于其价值决定是否使用信息安全技术,何时购买、安装和使用哪种信息安全技术.当企业决定使用一种信息安全技术时,如何使用才能获得最佳效果又是一个问题.一种情况是企业使用默认配置,另一种情况是根据企业运行环境进行配置优化.这些问题都会直接影响到信息安全技术的价值.以 IDS 为例,以往的研究表明,高的检测率与高的误报率是正相关的,而误报率会降低 IDS 的价值.当管理员不能够检查所有的报警时,只有在极端的环境中 IDS 才有用,这样的话还不如关掉 IDS 有效益^[6].

本文主要研究如何综合评价信息安全技术的价值,特别是信息安全技术的选择、使用与配置问题,通过将企业与入侵者作为一种博弈,对其博弈策略进行分析,指出影响信息安全技术价值的相关因素.

3 信息安全模型

为了便于分析,引入一个信息安全模型作为评价的参考模型(如图 1 所示).

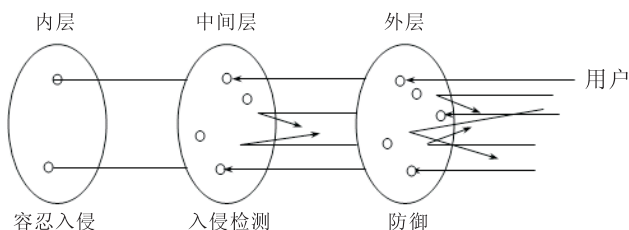


图 1 信息安全模型

信息安全体系结构是企业信息安全的基础,是保障企业信息资源机密性、完整性和可用性的综合方案.信息安全方案由风险评估、技术体系和安全策略构成.信息安全风险评估决定企业信息安全的级别、技术体系以及安全策略.总的来看,企业信息安全体系结构通常由 3 部分组成,即安全防御、入侵检测和容忍入侵.在这个模型中,IDS 对于企业信息安全的成本分析起着关键作用.

该模型建立在基于容忍入侵的三层安全结构上^[11],即外层抵御入侵、中间层检测入侵、内层容忍入侵.

(1) 外层——防御

这一层是对付入侵的第一层,外层防御的主要安全技术有认证、访问控制、防火墙等.客户访问企业信息系统时,要经过防火墙过滤,客户与服务器进行互相认证,运行访问控制策略进行访问控制.

(2) 中间层——入侵检测

对于经过外层进入系统的访问请求,由 IDS 进行监视. IDS 的主要功能是通过监视系统运行情况,分析系统日志文件和应用程序日志等系统和应用信息检测入侵,并对攻击进行识别和对攻击造成的破坏进行确定.

(3) 内层——容忍入侵

容忍入侵技术主要考虑在入侵存在的情况下系统的生存能力,其主要思想是用分布式系统中的硬件或者软件容错技术屏蔽任何入侵或者攻击对系统功能的影响,保证系统关键功能的安全性和健壮性.

4 信息安全技术的评价模型

简单来看,可以将企业信息系统的用户分成两类,即正常用户和入侵者.建立信息安全机制的目的就是保证正常用户按权限使用系统功能,同时及时发现入侵者,并将信息安全事件的影响降到最低.但是这一过程中可能会产生两类错误,即把入侵者当成正常用户、把正常用户当成入侵者.假设对 IDS 来说,检测率为 $P_D = P(\text{检测为入侵者} | \text{用户是入侵者})$,则漏报率为 $1 - P_D$,误报率为 $P_F = P(\text{检测为入侵者} | \text{用户为正常用户})$.对于完善的 IDS 来说, $P_D = 1$, $P_F = 0$.但事实上,由于用户行为的不断变化,当前的 IDS 技术 P_D 高的时候, P_F 也高^[1].

4.1 模型描述

假设模型由 3 部分组成,即用户、企业和信息安全技术.

用户 指企业信息系统的用户,包括外部用户和内部用户,外部用户分为合法用户和非法用户,内部用户分为按权限访问的正常用户和越权用户.入侵者指外部非法用户和内部越权用户.假设用户入侵的概率为 ψ ,入侵成功后入侵者可以获得的利益为 μ (泛指满足入侵者的需要),而入侵者被检测出来的代价是 β ,假设 $\mu - \beta \leq 0$.

企业 指企业信息系统的所有者,也是信息安全技术的使用者.使用信息安全技术后,管理员对 IDS 报警进行检查处理,同时对无报警信息的用户进行抽查.管理员检查报警用户的比例是 ρ_1 ,对没报警用户抽查的比例是 ρ_2 .假设每次检查的平均成

本是 c . 当一个入侵事件没有被检测出来时, 企业的损失是 d , 而如果检测出入侵, 企业可以减少损失的比例是 ϕ , 由于检查的成本不应当高于检测入侵的收益, 所以 $c \leq \phi d^{[1]}$.

信息安全技术 指三层安全体系结构, 外层使用防火墙进行过滤, 中间层使用 IDS 进行入侵检测, 对可疑事件报警和响应, 内层利用容忍入侵技术提高系统核心功能的可生存性. 容忍入侵技术以冗余为例, 系统采用 $m-n(m \leq n)$ 门限密码机制, 设置 n 个应用服务器, 每个应用服务器采用不同版本的系统, 只有同时入侵 m 个以上的服务器才能重构机密数据.

将信息安全看作企业与入侵者之间的一个博弈, 企业要保护信息系统安全, 而入侵者要侵入企业信息系统或越权对系统进行操作. 企业使用信息安全技术的目标是最小化入侵者带来的损失. 企业的信息安全投资收益依赖于入侵的程度, 而入侵者入侵的收益依赖于被发现的可能性, 入侵者被发现的可能性依赖于信息安全技术.

对于 IDS 来说, 用户策略 $S^U \in \{I, NI\}$, I 表示是入侵, 而 NI 表示非入侵. 企业策略 $S^F \in \{(R, R), (R, NR), (NR, R), (NR, NR)\}$, R 表示是管理员检查, 而 NR 表示管理员不检查. 其中将信息分成报警与不报警两类, 管理员检查与不检查, 从而有 4 种情况. 第 1 个元素表示当 IDS 报警时管理员作出响应, 第 2 个元素表示 IDS 没报警时管理员的响应.

假设入侵者的策略空间是 $\psi \in [0, 1]$, 企业的策略空间是 $(\rho_1, \rho_2) \in [0, 1] \times [0, 1]$, 则

$$\eta_1 = P(\text{入侵} | \text{报警}) = \frac{P_D \psi}{P_D \psi + P_F (1 - \psi)},$$

$$\eta_2 = P(\text{入侵} | \text{没报警}) = \frac{(1 - P_D) \psi}{(1 - P_D) \psi + (1 - P_F) (1 - \psi)},$$

$$P(\text{报警}) = P_F + \phi(P_D - P_F),$$

$$P(\text{没报警}) = 1 - P_F - \phi(P_D - P_F),$$

$$P(\text{入侵被检测到}) = \rho_1 P_D + \rho_2 (1 - P_D).$$

企业对报警的期望成本是

$$F_A(\rho_1, \psi) = \rho_1 c + \eta_1 (1 - \rho_1) d + \eta_1 \rho_1 (1 - \phi) d.$$

企业对没报警的期望成本是

$$F_N(\rho_2, \psi) = \rho_2 c + \eta_2 (1 - \rho_2) d + \eta_2 \rho_2 (1 - \phi) d.$$

企业总的期望成本是

$$F(\rho_1, \rho_2, \psi) = (P_F + \phi(P_D - P_F)) F_A(\rho_1, \psi) + (1 - P_F - \phi(P_D - P_F)) F_N(\rho_2, \psi).$$

入侵者的期望收益是

$$H(\rho_1, \rho_2, \psi) = \psi \mu - \phi \beta (\rho_1 P_D - \rho_2 (1 - P_D)),$$

其中 $\psi(P_D - P_F)$ 表示 IDS 的有效检测率. 企业期望成本最小, 而入侵者期望收益最大, 由此可以得出以下结论.

结论 1. 下列混合策略构成 IDS 的纳什均衡^[1]:

$$\text{如果 } \frac{\mu}{\beta} > P_D, \text{ 则 } \left(\rho_1 = 1, \rho_2 = \frac{\mu - P_D \beta}{(1 - P_D) \beta}, \psi = \frac{c(1 - P_F)}{c(P_D - P_F) + (1 - P_D) d \phi} \right);$$

$$\text{如果 } \frac{\mu}{\beta} \leq P_D, \text{ 则 } \left(\rho_1 = \frac{\mu}{P_D \beta}, \rho_2 = 0, \psi = \frac{c P_F}{P_D d \phi - c(P_D - P_F)} \right).$$

此外, 由企业总的期望成本与结论 1 可以得到, 企业对 IDS 的期望成本为

$$\begin{cases} \frac{c}{\phi} \frac{1 - ((\phi(1 - c/\phi d) P_D + (1 - \phi(1 - c/\phi d)) P_F)}{1 - ((c/\phi d) P_F + (1 - c/\phi d) P_D)}, & \text{当 } \mu/\beta > P_D; \\ \frac{c}{\phi} \frac{1}{c/\phi d + (1 - c/\phi d) P_D/P_F}, & \text{当 } \mu/\beta \leq P_D. \end{cases}$$

4.2 信息安全技术的价值分析

企业选择使用信息安全技术的目的是为了降低安全风险, 为企业带来正的收益. 但是同样的信息安全技术, 采用不同的配置, 信息安全技术的收益不同^[1]. 特别在同时采用多种信息安全技术的安全体系结构中, 企业信息安全的总收益并不是单项信息安全技术的收益总和, 不同信息安全技术可能会互相补充, 也可能会互相冲突, 甚至抵消. 本节重点分析三层安全体系结构中, 防火墙、IDS 和容忍入侵三者之间的相互关系.

综合考虑图 1 所示的信息安全模型, 博弈树如图 2 所示^[10], 图中的边上标注的是相应的概率, 如 ϵ 表示用户是外部用户的概率, q_1^F 表示外部非法用户被防火墙过滤掉的概率等.

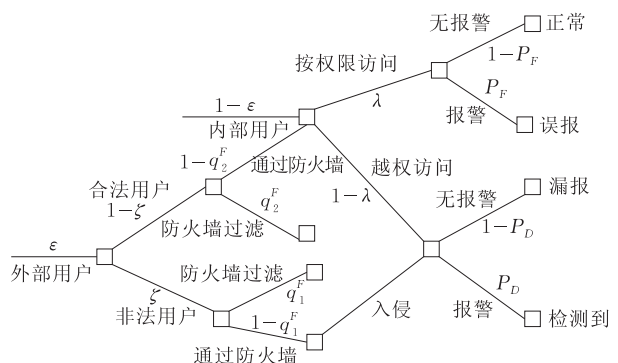


图 2 博弈树

(1) 防火墙与 IDS

作为外层防御的防火墙,主要通过对外部用户进行过滤.经过防火墙进入系统的外部用户有两类,其概率分别为:

外部合法用户进入系统的概率

$$P_{ea} = \epsilon(1 - \zeta)(1 - q_2^F);$$

外部非法用户进入系统的概率

$$P_{nea} = \epsilon\zeta(1 - q_1^F),$$

这部分用户即为入侵者;

外部合法用户与系统内部用户作为系统的合法用户的概率

$$P_{user} = 1 - \epsilon + \epsilon(1 - \zeta)(1 - q_2^F),$$

其中按权限进行操作的正常用户为

$$P_{user-i} = (1 - \epsilon + \epsilon(1 - \zeta)(1 - q_2^F))\lambda,$$

越权操作的用户为

$$P_{user-ni} = (1 - \epsilon + \epsilon(1 - \zeta)(1 - q_2^F))(1 - \lambda),$$

越权访问的用户也视为入侵者.因此,用户为入侵者的概率为

$$\begin{aligned} \psi &= P_{nea} + P_{user-ni} \\ &= \epsilon\zeta(1 - q_1^F) + (1 - \epsilon + \epsilon(1 - \zeta)(1 - q_2^F))(1 - \lambda). \end{aligned}$$

因此可以得出,入侵者被 IDS 检测并报警的概率为 $P_I = \psi P_D$,漏报的概率为 $P_{NI} = \psi(1 - P_D)$,被 IDS 误报的概率为 $P_N = P_{user-i} P_F$.

由此可见,IDS 的检测率、误报率与防火墙的性能有密切关系,而防火墙的性能主要是指对外部非法用户过滤的比率 q_1^F 和对合法用户过滤的比率 q_2^F .

(2) 配置对防火墙和 IDS 价值的影响

入侵者被 IDS 检测并报警的概率为 $P_I = \psi P_D$,管理员检查报警用户的比例是 ρ_1 ,漏报的概率为 $P_{NI} = \psi(1 - P_D)$,因此,最后成功的入侵者的概率为

$$\begin{aligned} P_{SI} &= P_I(1 - \rho_1) + P_{NI}(1 - \rho_2) \\ &= \psi P_D(1 - \rho_1) + \psi(1 - P_D)(1 - \rho_2). \end{aligned}$$

由此可以得出:提高对报警用户进行检查的比例 ρ_1 和对无报警用户的抽查 ρ_2 ,降低用户成功入侵的概率 ψ 能够降低成功入侵的概率.提高 ρ_1 和 ρ_2 会增加检查成本,优化防火墙的配置,提高防火墙的性能可以降低 ψ .

默认配置的 IDS 价值表如表 1 所示^[1],其中正值表示期望从信息安全技术中得到的价值.值得注

意的是,当 $\mu/\beta > P_D$,IDS 技术的使用反而会增加企业的成本.由此提醒企业使用信息安全机制的默认配置有时对企业是不利的.

4.1 节中的结论 1 表明 IDS 默认配置会出现两种情况,通过改变配置可以改变这种状态,使得 $\frac{\mu}{\beta} \leq P_D$,而使企业成本降低.提高检测率 P_D 是提高 IDS 收益的重要指标,一方面通过优化 IDS 配置,另一方面通过防火墙过滤外部非法用户,可以提高 P_D ,满足条件 $\frac{\mu}{\beta} \leq P_D$.

改变系统配置的方法取决于所使用的信息安全机制,比如设置 IDS 的检测率 P_D .因此企业信息安全成本可以视为 P_D 的函数,计算一级导数得到

$$\frac{\partial P_{SI}}{\partial P_D} = \psi(1 - \rho_1) - \psi = -\psi\rho_1 \leq 0.$$

因此,要降低企业信息安全成本,通过优化配置提高 IDS 的检测率 P_D 是关键.最优配置能够检测入侵,形成与完善的 IDS 相同的检查策略,说明信息安全机制的优化配置对于信息安全的效果具有重要的意义.

入侵率与检查率的影响:入侵率与检查率随着 $c/d\phi$ 和 μ/β 增加. $c/d\phi$ 越高表示企业人工检查效率降低,而 μ/β 越高表示入侵者的期望效益越大.二者的增加表示入侵增加,从而引起管理员检查更加频繁.

IDS 价值的影响:IDS 的价值随着 μ/β 下降.质量低的 IDS 必然价值会下降,然而 μ/β 增加,会刺激入侵者,反而会降低 IDS 的价值.这与直觉是不同的! μ/β 越高,企业会配置 IDS 设定高的检测率 P_D ,而导致高的误报率 P_F .由于管理员要检查所有报警的用户,误报率增加了企业的检查成本.

与入侵率和检查率不同,企业的参数 c 、 d 和 ϕ 对 IDS 的价值不依赖于 $c/d\phi$,而是依赖于单个参数的值. d 高,IDS 的价值就大; c 或 ϕ 增加,会引起 IDS 价值的增加或降低.

因此,威慑是 IDS 价值的关键.实施 IDS 的效益在于能够成功阻止多少入侵.

(3) IDS 与容忍入侵

对于 IDS 漏报的入侵和报警但没有响应的入侵,进入企业信息系统后,会给企业造成一定的损失 d .采用容忍入侵的体系结构,可以避免或减少损失.

例如系统的容忍入侵技术采用 $m - n (m \leq n)$ 门限密码机制,设置 n 个应用服务器,每个应用服务器采用不同版本的系统,只有同时入侵 m 个以上的服

表 1 信息安全的价值

条件	IDS 的价值	IDS 有收益吗?
$\mu/\beta > P_D$	$-\frac{c}{\phi} \frac{(P_D - P_F)(1 - \phi)(d\phi - c)}{d\phi - ((d\phi - c)P_D + cP_F)}$	否
$\mu/\beta \leq P_D$	$\frac{c}{\phi} \frac{(P_D - P_F)(d\phi - c)}{P_D d\phi - c(P_D - P_F)}$	是

务器才能重构机密数据. 假设设置一个应用服务器的成本为 S_c , 那么除主应用服务器外, 实现容忍入侵的成本为 $(n-1)S_c$.

假设在足够的时间 T_a 内, 入侵者可以攻陷一个服务器, 由于不同的应用服务器采用不同版本的系统, 可以假设入侵者攻陷不同服务器的时间是相同的, 那么管理员必须在时间 $T < mT_a$ 内发现入侵, 恢复系统, 保证系统正常运行.

企业信息系统是否采用这种基于门限密码的容忍入侵技术, 取决于 d 与 $(n-1)S_c$ 的比例关系, 各项参数的选择应该满足 $d > (n-1)S_c > d\psi(1-P_D)$. 其中与防火墙的性能和 IDS 的检测率密切相关.

最后需要指出的是容忍入侵反过来会进一步优化 IDS 的配置, IDS 会根据检测的情况为防火墙的配置提供依据.

5 结 论

信息安全管理是一项复杂的工作, 对信息安全技术的评价是对信息安全技术进行有效管理的基础. 本文基于博弈论, 对由防火墙、入侵检测和容忍入侵等信息安全技术构成的三层安全体系结构进行了分析, 提出了一个评价信息安全技术的综合模型, 分析了三者之间的相互影响. 研究表明, IDS 的检测率、误报率与防火墙的性能有密切关系, 而防火墙的性能主要通过对外部非法用户过滤的比率和对合法用户过滤的比率来描述. 系统安全配置直接影响信息安全机制的性能和成本效益, 信息安全机制的优化配置对于信息安全的具有重要的意义. 容忍入侵机制取决于入侵的损失评估、系统的成本和防火墙与 IDS 的性能. 因此, 在设置信息安全机制时, 要综合考虑不同信息安全技术之间的相互影响和相互关系, 通过优化配置, 提高信息安全技术的效益.

参 考 文 献

[1] Cavusoglu H, Mishra B, Raghunathan S. The value of intrusion detection systems in IT security. *Information Systems*

Research, 2005, 16(1): 28-46

- [2] Yue Bing, Fu Hong-Juan. The method of perfecting the audit information in intrusion detection system. *Chinese Journal of Computers*, 2002, 25(7): 772-777(in Chinese)
(岳兵, 傅红娟. 完善入侵检测系统审计信息的方法. *计算机学报*, 2002, 25(7): 772-777)
- [3] Qing Si-Han, Jiang Jian-Chun, Ma Heng-Tai, Wen Wei-Ping, Liu Xue-Fei. Research on intrusion detection techniques: A survey. *Journal of China Institute of Communications*, 2004, 25(7): 62-70(in Chinese)
(卿斯汉, 蒋建春, 马恒太, 文伟平, 刘雪飞. 入侵检测技术研究综述. *通信学报*, 2004, 25(7): 62-70)
- [4] Athanasiades N, Abler R, Levine J et al. Intrusion detection testing and benchmarking methodologies//*Proceedings of the 1st IEEE International Workshop on Information Assurance*. Darmstadt, Germany: IEEE Computer Society, 2003: 63-72
- [5] Ulvila J W, Gaffney J E. A decision analysis method for evaluating computer intrusion detection systems. *Decision Analysis*, 2004, 1(1): 39-54
- [6] Ryu Y U, Rhee H S. Evaluation of intrusion detection systems under a resource constraint. *ACM Transactions on Information and Systems Security*, 2008, 11(4): 20. 1-20. 24
- [7] Sabahi F, Movaghar A. Intrusion detection: A survey//*Proceedings of the 3rd International Conference on Systems and Networks Communications (ICSNC'08)*. Sliema, Malta, 2008: 23-26
- [8] Mu Cheng-Po, Huang Hou-Kuan, Tian Sheng-Feng. A survey of intrusion-detection alert aggregation and correlation techniques. *Journal of Computer Research and Development*, 2006, 43(1): 1-8(in Chinese)
(穆成坡, 黄厚宽, 田盛丰. 入侵检测系统报警信息聚合与关联技术研究综述. *计算机研究与发展*, 2006, 43(1): 1-8)
- [9] Poe James, Li Tao. BASS: A benchmark suit for evaluating architectural security systems. *ACM SIGARCH Computer Architecture News*, 2006, 34(4): 26-33
- [10] Cavusoglu Huseyin, Mishra Birendra, Raghunathan Srinivasan. A model for evaluating IT security investments. *Communications of the ACM*, 2004, 47(7): 87-91
- [11] Zhu Jian-Ming, Wang Chao, Ma Jian-Feng. Intrusion-tolerant based survivable model of database system. *Chinese Journal of Electronics*, 2006, 14(3): 481-484
- [12] Zhao W. A game theoretical view of byzantine fault tolerance design. *International Journal of Performability Engineering*, 2007, 3(4): 498-500



ZHU Jian-Ming, born in 1965, Ph. D., professor, Ph. D. supervisor. His research interests include information security and E-commerce.

Srinivasan Raghunathan, professor, Ph. D. supervisor. His research interests include information systems and information security.

Background

The increasing significance of information security to firms is evident from their growing IT security budgets. Firms rely on security technologies such as firewalls and intrusion detection systems (IDSs) to manage IT security risks. Although the literature on the technical aspects of IT security is proliferating, a debate exists in the IT security community about the value of these technologies. The research on these issues has become a new field, which called economics of information security. In this research, the professors in University of Texas at Dallas go ahead and they have published several important papers.

The primary goal of IT security is balancing the conflicting needs of information protection and information access. To achieve this goal, firms typically deploy several different information security technologies. The deployment of multiple technologies makes configuration challenging and how to

achieve the optimal benefit is a difficult problem. In this paper, the three layers architecture including firewall, intrusion detection and intrusion tolerant is discussed firstly.

Majority of the earlier literature is on intrusion detection. Game theory is a strong tools to provide the mathematical framework for analysis, modeling, decision, and control processes for information security and intrusion detection. So research on the evaluation model of information security technologies is based on game theoretic.

This research is supported by supported by the National Natural Science Foundation of China (grant Nos. 60573035, 60673162, 60743005) and Beijing Natural Science Foundation (grant No. 4082028). This paper presents the evaluation model of information security and they are a part of these projects.