基于攻防博弈模型的网络安全测评和最优主动防御

姜 伟[1)] 方滨兴[1),2)] 田志宏[1),2)] 张宏莉[1)]

[1)](哈尔滨工业大学计算机网络信息安全研究中心 哈尔滨 150001)

[2)](中国科学院计算技术研究所 北京 100190)

摘 要 为了进行网络信息系统安全测评和主动防御,提出了网络防御图模型、攻防策略分类及其成本量化方法、网络攻防博弈模型和基于上述模型的最优主动防御选取算法. 最后通过一个典型的网络实例分析了上述模型和算法在网络安全测评和最优主动防御中的应用. 分析结果表明,提出的模型和方法是可行的、有效的.

关键词 网络安全;防御图;成本量化;攻防博弈;最优主动防御

中图法分类号 TP309 **DOI 号**: 10.3724/SP.J.1016.2009.00817

Evaluating Network Security and Optimal Active Defense Based on Attack-Defense Game Model

JIANG Wei[1)] FANG Bin-Xing[1),2)] TIAN Zhi-Hong[1),2)] ZHANG Hong-Li[1)]

[1)](*Computer Network and Information Security Research Center*, *Harbin Institute of Technology*, *Harbin* 150001)

[2)](*Institute of Computing Technology*, *Chinese Academy of Sciences*, *Beijing* 100190)

Abstract To evaluate the security of network information systems and perform active defense, this paper presents some models including defense graph model, attack-defense taxonomy and cost quantitative method, and Attack-Defense Game (ADG) model. Algorithms for selecting optimizing active defense strategy based on those models are proposed and analyzed in a representative network example. Results indicate that the models and methods are effective and efficient.

Keywords internet security; defense graph; quantitative cost analysis; attack-defense game model; optimal active defense

1 引 言

现有的网络安全技术依赖于防火墙、入侵检测和反病毒软件等,属于静态的、片面的被动安全防御,强调以攻击为中心,检测到攻击后才有所响应,此时已为时过晚,可能已经造成严重的损失,缺乏主动性和对攻击的预测能力. 为了保证网络系统的安全性和健壮性,世界各国政府、学术界和企业界都正在寻求新的防御技术. 在报告① 中作者提出:"主动实时防护模型与技术的战略目标是通过态势感知,风险评估、安全检测等手段对当前网络安全态势进

收稿日期:2008-12-08;最终修改稿收到日期:2009-02-12. 本课题得到国家"九七三"重点基础研究发展规划项目基金(2007CB311100)、国家"八六三"高技术研究发展计划项目基金(2007AA01Z442, 2007AA01Z406, 2009AA012437)资助. **姜 伟**,男,1979 年生,博士研究生,主要研究方向为网络与信息安全、网络攻防等. E-mail: jiangwei@pact518.hit.edu.cn. **方滨兴**,男,1960 年生,教授,博士生导师,中国工程院院士,主要研究领域为计算机体系结构、信息安全和计算机网络等. **田志宏**,男,1978 年生,博士,讲师,主要研究方向为计算机网络与信息安全等. **张宏莉**,女,1973 年生,教授,博士生导师,主要研究领域为网络信息安全、网络测量.

① 方滨兴. 解读信息安全创新突破点. http://www.cert.org.cn/articles/news/common/2007051823317.shtml, 2008

行判断,并依据判断结果实施网络主动防御的主动安全防护体系."

信息安全测评工作是保障网络和信息系统安全的基础.目前,基于网络安全测评的主动安全防御技术渐渐成为主流[1-2],这是因为与传统的被动防御技术相比,基于安全测评的主动防御技术能够帮助用户预先识别网络系统脆弱性以及所面临的潜在的安全威胁,根据安全需求来选取符合最优成本效应的主动安全防御措施和策略,从而提前避免危险事件的发生.

理想的防御系统应该对所有的弱点或攻击行为都做出防护,但是从组织资源限制等实际情况考虑,"不惜一切代价"的防御显然是不合理的,必须考虑"适度安全"的概念,即考虑信息安全的风险和投入之间寻求一种均衡,应当利用有限的资源做出最合理的决策.防御成本有效性是安全管理员考虑的重要因素.信息安全中攻防对抗的本质可以抽象为攻防双方的策略依存性,防御者所采取的防御策略是否有效,不应该只取决于其自身的行为,还应取决于攻击者和防御系统的策略.所以可以利用博弈论[3]来研究攻防矛盾及其最优防御决策等信息安全攻防对抗难题.Hamilton[4]指出,博弈论将在网络攻防对抗领域发挥重要作用,是未来信息安全很有前途的研究方向.

本文的主要贡献如下:(1)本文考虑了针对攻击的防御策略的成本有效性,对传统攻击图进行了改进和丰富,提出了用于网络系统安全评估的防御图模型,完整地给出了攻防策略分类及其成本/收益分析;(2)本文把网络攻防双方建模为二人非合作博弈模型,并详细地给出了攻防博弈模型的形式化描述.用此模型来研究网络攻防双方的矛盾冲突和最优决策;(3)本文提出基于上述模型的最优主动防御策略选取算法,帮助防御者采取最优防御策略进行主动防御.

本文首先介绍相关研究工作,然后给出用于网络系统安全评估的防御图模型和攻防策略分类及其代价量化模型.从而引出网络攻防博弈模型的形式化定义,接着描述基于上述模型的最优主动防御策略选取算法.以上几个部分是相互关联的整体,防御图模型用于帮助用户预先识别网络系统脆弱性以及所面临的安全威胁,从而可以确定攻防策略.攻防策略分类及其代价量化用于分析攻防双方的策略收益.攻防策略和攻防策略收益是攻防博弈模型的重要元素,是基于攻防博弈模型的最优防御策略选取算法的数据源.利用攻防博弈模型预先选取和实施最优的主动安全防御策略和措施,以避免危险和损失的发生,将被动防御变为主动防御.最后通过一个实例对模型和方法的有效性进行分析验证.

2 相关研究工作

目前,有关网络安全测评、防御代价定量分析和主动防御的研究工作还处于起步阶段,尚未形成系统化的理论方法.主要的研究工作可概括为以下几个方面.

(1)网络脆弱性测评分析方面

冯登国等人[5]分析了信息安全风险评估国内外现状、评估体系模型、评估标准、评估方法、评估过程等,探讨了国内外测评体系,指出了目前信息安全风险评估需要解决的问题,展望了信息安全风险评估的发展前景.林闯等人[6]介绍了网络安全性的随机模型与评价技术等方面的研究现状与进展,总结了网络安全性随机模型的若干研究方法和评价技术.在攻击树方面,Schneier[7]提出了利用攻击树形式化、系统化地描述系统安全的方法,用来对单个弱点威胁建模.Moore[8]详细地论述了以递归或渐进的方式来表达攻击变化的攻击树,能比较直观地反映攻击者实施攻击的步骤.在特权图方面,Dacier 等人[9]提出了特权图的概念,用来表达系统漏洞带来的攻击者对系统控制权限的变化,对系统的安全性进行评估.并且为弱点定义了一个度量来表达对此弱点进行攻击的成功可能性.Ortalo 等人[10]基于特权图思想提出了一种网络安全评估试验模型框架.在攻击图方面,Phillips 和 Swiler 提出基于图的网络弱点分析方法[11],这种方法可以检验一个成功攻击之后可能存在的所有结果,指出攻击者可以采取的那些具有较大成功概率的攻击路径,从而获得网络信息资产面临的不同风险.在模型检验方面,Ramakrishnan 等人[12]首先提出将模型检测的方法应用在主机弱点综合分析方面,并实现了一个 UNIX 系统下的弱点分析工具.Ritchey 和 Ammann[13]把模型检测这种评估方法的应用扩展到了网络系统的评估中.张永铮等人[1]提出了一个由风险网络和风险传播算法构成的风险传播模型,风险网络描述了网络系统的访问关系结构和风险态势,风险传播算法则给出了风险的运动规则.

(2)防御代价定量分析方面

信息安全经济学近年来逐渐成为研究热点,并取得了一些研究成果.Lee 在 2002 年首次提出了成本敏感模型作为响应决策的基础[14],根据响应成本

和攻击损失成本来决定是否响应.该响应决策思想比较简单.但其代价量化、代价分类和攻击分类的思想和方法对本文的研究内容有一定的借鉴意义.文献[15]中,给出了比较完整的攻防分类及其成本敏感模型,有效地应用于最优主动防御中.冯萍慧等人提出了脆弱性利用成本估算模型[16].通过对网络系统进行全面的脆弱性分析,并引入可靠性原理,从利用成本的角度对攻击代价进行估算,从而对网络系统的脆弱性进行量化评估,为管理员在权衡修复成本和效果时提供参考.

(3)博弈论在安全领域方面的应用

博弈论是一种基于事前的决策分析理论,由于在理解和建模冲突方面的价值,博弈论应用于安全相关问题的历史很久.开始于军事应用,1954 年 Haywood[17]通过分析二战中的军事运作证明了博弈论的应用与军事领域的有效性.后来应用于政治科学[18].近来应用于信息战和计算机网络安全,1997 年,Syverson[19]提出应用随机博弈来对网络中的正常节点和恶意节点进行理性分析的思想.1997 年 Burke[20]提出利用不完全信息的重复博弈对信息战中的攻击者和防御者行为建模.2002 年,Lye 和 Wing[21]利用随机博弈形式分析了防护者和攻击者双方纳什均衡和各自的最优策略.2003 年,Xu[22]基于完全信息的静态博弈设计和分析了 DDoS 防御系统,并使得该系统性能得到了优化.2003 年,Liu[23]提出了基于博弈理论的入侵意图、目标和策略推理模型,为这个领域的进一步发展做出了贡献.

本文借鉴了上述相关研究成果,但是也不同于上述研究工作.具体如下:首先,本文提出一种用于网络安全评估的防御图模型;其次,提出一种面向主动防御的攻防策略分类及其代价量化模型;最后,形式化定义攻防博弈模型并给出了基于上述模型的最优主动防御策略选取算法.

3 用于网络安全测评的防御图模型

网络攻击图(network attack graph)[11]是由攻击者在对目标网络进行攻击时可能采取的攻击路径组成的集合.攻击路径是攻击者进行攻击时所采取的攻击动作的序列.网络攻击图仅反映了攻击动作和系统状态变化情况,没有考虑各个攻击动作相应的防御策略及其攻防策略成本估计.为了评估网络信息系统安全和全面反映网络攻防策略及其代价情况,我们对攻击图模型进行了改进,并提出了网络防御(护)图(network defense graph)模型[24].

3.1　防御图定义

定义 1.　防御图(也称防护图,Defense Graph,简称 DG)是一个 6 元组,$DG=(S,\tau,S_0,S_s,S_a,S_d)$,其中 S 是图的节点集,每一个节点表示一种网络安全状态,$\tau\subseteq S\times S$,τ 是一种网络安全状态转换关系,$S_0\subseteq S$,S_0 是初始网络安全状态集合,$S_s\subseteq S$ 是攻击者目标状态集合,S_a 是攻击者策略集合,S_d 是防御者策略集合.

防御图是一个有向图,节点表示某种网络安全状态,表达了网络的资源属性和用户或攻击者对整个网络的访问能力.有向边表示攻击者利用各种原子攻击从一个网络安全状态到一个新的网络安全状态的转换关系和实现该转换的攻击成本/收益.这种状态变化可以表现为文件修改、系统配置改变、可执行程序运行、攻击者的特权提升等.S_a 是攻击者从初始节点到目标节点所有的攻击路径的集合,即攻击策略集合.每一个攻击路径是一个或多个原子攻击的序列.对于每一个原子攻击或攻击策略都对应一系列防御策略,所有的防御策略组成 S_d.如图 1 是某网络系统生成的防御图 $DG=(S,\tau,S_0,S_s,S_a,S_d)$,$S=\{A,B,C,D,E,F\}$,用标有字母的圆圈表示.$S_0=\{A\}$,$S_s=\{F\}$,用标有原子攻击名称和攻击收益的有向边表示状态转换关系,如 $a1:30$ 表示原子攻击 $a1$ 使得网络从状态 A 到状态 B,攻击收益是 30(单位是货币单位,可以用美元表示,下同),$S_a=\{1,2,3\}$.$S_d=\{s_1^d,s_2^d,s_3^d\}$用标有防御策略名称和收益的方框表示每条攻击路径的防御策略.

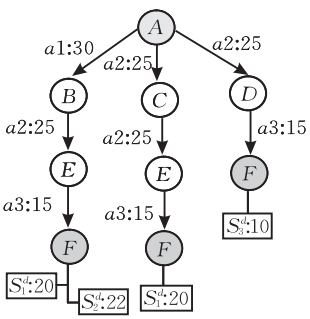

图 1　防御图实例

3.2　防御图的生成

防御图的建模和生成需要防火墙和路由器的配置文件、网络弱点扫描器、弱点数据库和攻防策略及其成本/收益量化模型等信息,具体模块图如图 2 所示.由于防御图的建模和生成不是本文讨论的重点,后续工作将重点讨论,这里不作详细介绍.

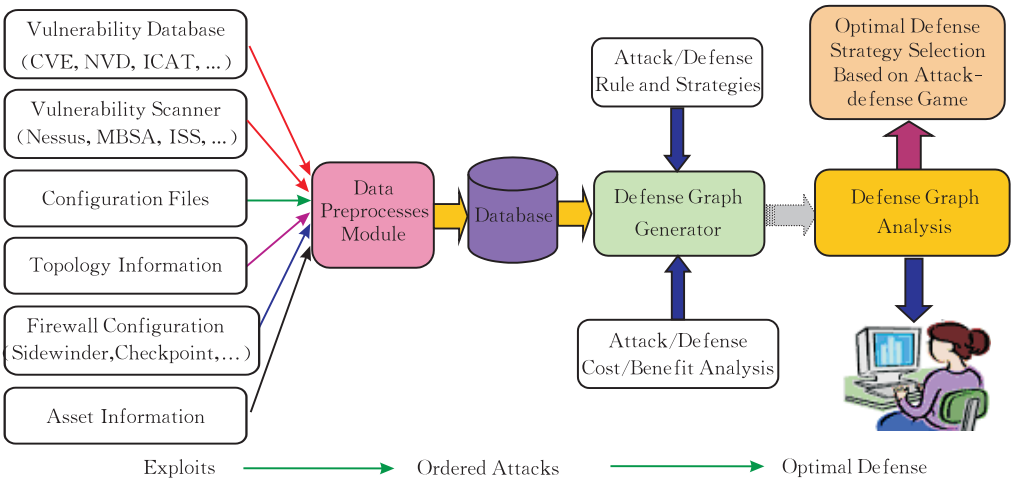

图 2 防御图生成模块图

3.3 攻防策略分类及其成本量化

网络攻防策略及其成本收益分析是防御图建模和最优网络安全防御的基础. 本节重点介绍网络攻防策略分类及其成本/收益模型. 由于目标资源的重要程度是随着网络环境的不同而变化,而且各类攻击的固有危害也是不尽相同. 所以攻击造成的损失不仅与攻击的类型有关,而且与攻击的目标有关. 为了能尽量精确地评估攻击损失代价,需要建立攻击分类模型和攻击对目标资源的损害模型,损失代价的量化可以结合攻击及其攻击目标进行计算.

攻防策略分类须考虑:(1)攻防策略分类空间大小直接影响后续攻防博弈模型分析复杂度;(2)攻防策略分类方法符合现有的防御系统. 参考 MIT 林肯实验室攻击分类[27],给出一种面向主动防御的攻击/防御分类方法. 攻击战略目的和攻击影响对主动防御系统评估决策具有重要意义. 所以攻击分类方法结合攻击战略目的和攻击影响作为分类依据,如表 1 所示. 我们在总结各种防御方法分类[24,26]基础之上,结合上述攻击分类和主动防御的时空特点,根据攻防博弈模型要求,将防御策略分为基于主机和基于网络的两大类,其中每一种防御分类包括若干个子类,具体如表 2 所示.

表 1 攻击分类

分类	描述	*AL*
Root	获取管理员权限	10
User	获取普通用户权限	5
Data	非授权访问或读写数据	3
DOS	拒绝服务攻击	2
Probe	扫描攻击	0.5
Other	其它	*

表 2 防御策略分类

分类	子类	描述	*Ocost*
基于主机防御	关闭进程	关闭可疑进程或者所有进程	OL1
	删除文件	删除被修改或者感染的文件	OL1
	删除用户账号	删除可疑用户账号	OL1
	关闭服务	关闭易受攻击的软件	OL2
	限制用户活动	限制可疑用户的权限和活动	OL2
	关闭主机	关闭被攻击主机	OL2
	重启主机	重新启动被攻击主机	OL2
	安装软件升级补丁	升级存在漏洞的软件到最新版本	OL2
	系统病毒扫描	利用杀毒软件扫描系统	OL3
	文件完整性检验	利用软件工具检验系统文件完整性	OL3
	安装系统升级补丁	升级系统到最新版本	OL3
	重新安装系统	安装被感染或者文件被修改的系统	OL3
	修改账号密码	修改系统的所有账号密码	OL2
	格式化硬盘	格式化硬盘去除所有恶意代码	OL3
	备份系统	备份系统数据	OL3
	其它	*	*

（续　表）

分类	子类	描述	*Ocost*
基于网络的防御	隔离主机	通过关闭 NIC 隔离受害主机	OL2
	丢弃可疑数据包	利用 IDS 或 Firewall 丢弃可疑数据包	OL2
	断开网络	断开信息系统与外部网络连接	OL2
	TCP 重置	发送重置包重置会话	OL2
	阻断端口	利用软件阻断端口	OL2
	阻断 IP 地址	利用软件阻断 IP 地址	OL2
	设置黑洞路由	利用 Firewall 修改路由表到不可达 IP	OL2
	其它	*	*

下面我们来分析攻防成本/收益，首先给出一些定义.

定义 2.　攻击回报 *AR*（Attack Reward）表示攻击者发动一次成功攻击所得到的好处，一般用该攻击对网络系统的损失来表示（用正值表示）. 事实上，攻击者收益一般少于网络系统损失[27]. 有时为了简便分析，可以把防御者的损失作为攻击者的所得.

定义 3.　攻击成本 *AC*（Attack Cost）表示攻击者发动一次攻击所需要的软硬件资源、专业知识和攻击被发现时相应的法律制裁（用负值表示）.

定义 4.　攻击致命度 *AL*（Attack Lethality）表示某类攻击所具有的固有危害程度. 表 1 中给出了各类攻击的致命度，用 0～10 之间的数值表示.

定义 5.　系统损失代价 *Dcost*（Damage cost）表示某类攻击对目标资源的损害程度.

攻击的目标资源损失可以用危险度（criticality）、安全属性损害来描述. Northcut[28] 提出用危险度和致命度来描述被攻击目标的重要性程度和攻击的固有危害，本文参考了他的量化思想. 在报告①中，作者提出了信息安全属性的可计算性的思想和模型. 在这里我们受该思想启发，将安全属性的损害可以分为完整性代价 *Icost*（Integrity cost）、机密性代价 *Ccost*（Confidentiality cost）和可用性代价 *Acost*（Availability cost）. 安全属性的损害对每一种安全属性代价具有一定偏重，用 (P_i, P_c, P_v) 来表示对完整性代价、机密性代价和可用性代价的偏重，且满足 $P_i+P_c+P_v=1$. 安全属性代价的值可以根据攻击将对目标资源产生的危害评估，可以用高、中、低来进行分类表示. 安全属性代价的偏重可以根据具体的网络环境来确定. 攻击 a 对网络系统的损失代价可以由式(1)来计算：

$$Dcost(a)=\sum_{1}^{m} AL\times criticality\times (Icost\times P_i+Ccost\times P_c+Acost\times P_a) \tag{1}$$

其中 m 是受攻击主机个数.

定义 6.　防御回报 *DR*（Defense Reward）表示针对某一攻击采取防御策略后，网络系统免受的损失. 一般用攻击对网络系统的损失来表示（用正值表示）.

定义 7.　操作代价 *Ocost*（Operation cost）表示防御者的防御操作消耗的时间和计算资源的数量. 根据防御操作的复杂程度分为以下 3 个级别[14]：

OL1：操作代价非常小，几乎可以忽略不计，如终止用户进程等.

OL2：防御操作在生效时间内持续占用系统资源，但占用资源较少，如配置防火墙规则.

OL3：防御操作在生效时间内持续占用较多的系统资源，如系统备份.

在表 2 中给出了各种防御策略的操作代价. 可以根据不同的网络情景用具体的代价值来表示各层次相对的操作代价，如 OL1 的操作代价可以设为 1～10，OL2 的操作代价可以设为 10～50，OL3 的操作代价可以设为 50～100.

定义 8.　负面代价 *Ncost*（Negative cost）表示防御策略导致系统无法正常工作或服务质量下降等带来的损失. 例如，关闭服务或系统可能无法正常用户提供相关服务. 可以用前面定义的系统可用性乘以一个负面系数 $r(a,d)$ 来表示：$Ncost=Acost\times r(a,d)$. 其中 $r(a,d)$ 表示用防御策略 d 来防御攻击 a 对系统可用性所具有的负面影响程度.

定义 9.　残余损失 *Rcost*（Remainder cost）表示防御系统执行防御策略后，攻击对系统带来的残余的未被消除的损失. 可以用以损失代价乘以残余系数来表示：$Rcost(a,d)=Dcost(a)\times\varepsilon(a,d)$. 其中 $\varepsilon(a,d)$ 表示用防御策略 d 来防御攻击 a 所具有的残余损失程度.

定义 10.　防御成本 *Decost*（Defense cost）是防

① 方滨兴. 关于信息安全属性的可计算性初探. 中国信息安全大会主题报告. http://www.51cto.com/art/200604/25703.htm

御策略的操作代价、负面代价和残余代价之和(用负值表示). 即

$$Decost(d)=Ocost+Ncost+Rcost$$
$$=Ocost(d)+Acost\times r(a,d)+Dcost(a)\times\varepsilon(a,d) \quad (2)$$

4 网络攻防博弈模型

理性的攻击者是考虑攻击成本的,在攻击所得利益相同而攻击成本不同的情况下,他会选择具有低成本的攻击方式的. 但是对于非理性的攻击者来说,他只考虑如何最大化攻击所得回报,不考虑攻击成本. 防御非理性攻击者只需要从攻击者角度来研究何种攻击策略能够使得攻击者具有最多的回报. 但是防御理性的攻击者具有一定的难度,本文只考虑理性的攻击者的防御研究.

假设 1. 攻击者是智能而理性的决策主体. 攻击者不会发动无利可图的攻击.

假设 2. 攻击者总是追求攻击收益最大化. 例如,攻击者偏向于对目标资源具有最大损害的攻击方式.

在攻防博弈过程中,攻击者和防御者都希望通过最优的策略来最大化他的收益,所以我们假定他们是理性的、合理的. 在以上两条合理假设的基础上,可以将攻击者与防御者(系统)的矛盾冲突关系描述为策略型攻防博弈模型,从而通过计算该博弈的纳什均衡获得攻击意图和最优的防御策略.

4.1 模型相关定义

定义 11. 攻防博弈模型 ADG(Attack-Defense Game)是一个三元组 $ADG=(N,S,U)$,其中

① $N=(P_1,P_2,\cdots,P_n)$是参加攻防博弈的局中人集合,局中人是博弈的决策主体和策略制定者. 在不同的博弈中局中人的含义是不同的,既可以是个人也可以是具有共同的目标和利益的团体或者集团,这里局中人是攻击者或防御系统. 若攻击者的数量≥2,则表示分布式协同攻击;若防御系统的数量≥2,则表示多个防御系统协同防御.

② $S=(S_1,S_2,\cdots,S_n)$是局中人的策略集合(strategy set), $\forall i\in n, S_i\neq\varnothing, S_i=(s_1^i,s_2^i,\cdots,s_m^i)$表示局中人 P_i的策略集合,是局中人 P_i进行博弈的工具和手段,每个策略集合至少应该有两个不同的策略,即 $m\geq 2$.

③ $U=(U_1,U_2,\cdots,U_n)$是局中人的效用函数集合(utility function). $\forall i\in n$, U_i是$\times_{i\in n}S_i\rightarrow R$ 的函数,表示局中人 P_i的效用函数,其中 R 是效用值. 效用函数表达了攻防双方从博弈中能够得到的收益水平,它是所有局中人策略的函数. 不同的策略可能得到不同收益,它是每个局中人真正关心的参数. 在上一节中我们已经对攻防双方的成本和收益进行了量化,这里攻防效用函数分别表示为攻防成本和回报之和.

图 3 给出了网络攻防博弈模型的图表示,该模型是网络攻防博弈模型的通用模型. 为了简化分析,我们只考虑 $n=2$ 的情况, $ADG=((P_a,P_d),(S_a,S_d),(U_a,U_d))$,其中 P_a表示攻击者, P_d表示防御者(系统). $S_a=(s_1^a,s_2^a,\cdots,s_m^a)$表示攻击者的攻击策略集合, $S_d=(s_1^d,s_2^d,\cdots,s_n^d)$是防御系统的防御策略集合. $\forall s_i^a\in S_a, s_j^d\in S_d, U_a(s_i^a,s_j^d), U_d(s_i^a,s_j^d)$分别表示防御系统对攻击者的攻击策略 s_i^a采取防御策略 s_j^d后攻击者和防御者的收益. 效用函数集合可以表示为一个矩阵 $\boldsymbol{U}$,攻击者可能选取的攻击策略用矩阵中每一行来表示,防御者选取矩阵中每一列作为其防御策略. 攻防双方的目标是最大化其收益,用矩阵中的数字表示攻防双方的收益. 图 4 给出了图 1 防御图实例对应的攻防博弈矩阵.

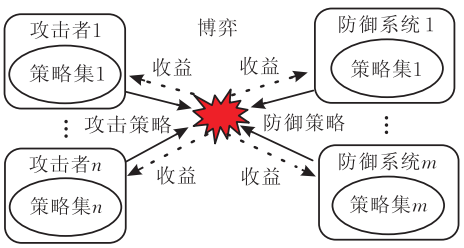

图 3 攻防博弈模型

在任何网络攻防环境中,攻击者和防御者之间的关系都是非合作的、对抗性的. 在攻防博弈的过程中,攻防双方不会事先将策略决策信息告知对方,攻击者总是希望通过破坏目标资源的功能或服务质量来获得最大化收益. 防御系统总是希望把系统的损伤降为最少. 所以我们的攻防博弈模型是一个非合作攻防博弈(Non-Cooperative ADG, NCADG).

$$\begin{array}{c|cccccc} & S_1^d & & S_2^d & & S_3^d & \\ \hline s_1^a & U_{a11} & U_{d11} & U_{a12} & U_{d12} & U_{a13} & U_{d13} \\ s_2^a & U_{a21} & U_{d21} & U_{a22} & U_{d22} & U_{a23} & U_{d23} \\ s_3^a & U_{a31} & U_{d31} & U_{a32} & U_{d32} & U_{a33} & U_{d33} \end{array}$$

图 4 攻防博弈收益矩阵

通常,在攻防博弈中,网络信息系统的损失即为攻击者的收益. 但是考虑到在一些特殊情况下,攻防双方的收益和损失并非总是相等. 所以攻防双方的

收益关系可分为零和(zero-sum)与非零和(nonzero-sum). 如果攻防双方的收益 U_a 和 U_d 满足 $U_a+U_d=0$，就称此为零和攻防博弈. $U_a+U_d\neq 0$，称为非零和攻防博弈. 根据不同的网络环境和攻防情景进行选择是否零和或非零和博弈模型.

下面给出几个重要定义，它们是后面主动防御策略选取算法的理论依据和求解方法.

定义 12.　纳什均衡(Nash Equilibrium[3]，NE). 在 $ADG=((P_a,P_d),(S_a,S_d),(U_a,U_d))$ 中，攻防策略对 (s_*^a,s_*^d) 是一个纳什均衡，当且仅当对每一个局中人 i，策略 s_*^i 是对付另一个局中人的最优对策：对于 $\forall s^a\in S_a, U_a(s_*^a,s_*^d)\geq U_a(s^a,s_*^d)$；对于 $\forall s^d\in S_d, U_d(s_*^a,s_*^d)\geq U_d(s_*^a,s^d)$.

在攻防双方都对对方具有完全信息的假设下，纳什均衡表示了攻防双方的最优对策. 利用定义 12 我们可以计算攻防博弈模型所有可能的纳什均衡. 但是考虑到攻防双方行为的不确定性，所以有时不可能存在一个纳什均衡，此时攻防各方必须考虑攻防混合策略.

定义 13.　混合策略(Mixed Strategy[29]，MS). 给定一个攻防博弈 $ADG=((P_a,P_d),(S_a,S_d),(U_a,U_d))$，攻防双方的混合策略分别是 $S_a=(s_1^a,s_2^a,\cdots,s_m^a)$ 和 $S_d=(s_1^d,s_2^d,\cdots,s_n^d)$ 的概率分布 $p_a=(p_{a1},p_{a2},\cdots,p_{am})$ 和 $p_d=(p_{d1},p_{d2},\cdots,p_{dn})$，且满足

$$0\leq p_{ai}\leq 1, 0\leq p_{di}\leq 1, \sum_{i=1}^{m}p_{ai}=1, \sum_{j=1}^{n}p_{dj}=1.$$

在网络攻防环境下，特别是防御者在处理单个攻击者的未知攻击策略时，利用先验知识(以前攻击者所采用的攻击策略的频率)来评估该攻击者可能使用的策略概率分布，从而可以采用混合防御策略.

定义 14.　混合策略纳什均衡(MSNE)[29]. 给定一个攻防博弈 $ADG=((P_a,P_d),(S_a,S_d),(U_a,U_d))$，攻防双方的混合策略分别是概率分布 $p_a=(p_{a1},p_{a2},\cdots,p_{am})$ 和 $p_d=(p_{d1},p_{d2},\cdots,p_{dn})$，那么攻防双方的期望收益分别用下式来计算

$$V_a(p_a,p_d)=\sum_{i}^{m}p_{ai}\left[\sum_{j}^{n}p_{dj}U_a(s_i^a,s_j^d)\right]=\sum_{i}^{m}\sum_{j}^{n}p_{ai}\cdot p_{dj}U_a(s_i^a,s_j^d) \tag{3}$$

$$V_d(p_a,p_d)=\sum_{j}^{n}p_{dj}\left[\sum_{i}^{m}p_{ai}U_d(s_i^a,s_j^d)\right]=\sum_{j}^{n}\sum_{i}^{m}p_{ai}\cdot p_{dj}U_d(s_i^a,s_j^d) \tag{4}$$

混合策略 (p_a^*,p_d^*) 是纳什均衡，当且仅当该混合策略是攻防双方的最优混合策略，即满足：对于 $\forall p_a, V_a(p_a^*,p_d^*)\geq V_a(p_a,p_d^*)$；对于 $\forall p_d, V_d(p_a^*,p_d^*)\geq V_a(p_a^*,p_d)$.

利用定义 14，我们可以计算攻防双方采用混合策略时的纳什均衡.

4.2　基于攻防博弈模型的主动防御策略选取算法

防御策略的选取十分复杂，因为针对单个攻击策略，防御决策只需要选择综合防御代价最小的策略. 而在多步攻击和多个攻击策略的情况下，有的防御策略可能对某类攻击有效，对其它攻击无效，同时要考虑到防御操作代价、负面代价和残余损失. 另外每个攻击策略的发生概率是未知的，如何保证该防御策略是最优的，即期望综合防御代价是最低的，是一个十分复杂的问题. 基于攻防博弈模型的主动防御策略选取可以很好地解决此类问题. 下面给出基于攻防博弈模型的主动防御策略选取算法，具体描述如下.

算法 1.　基于攻防博弈模型的主动防御策略选取算法.

输入：网络防御图 $DG=(S,\tau,S_0,S_s,S_a,S_d)$

输出：攻击意图和最优防御策略 S_{oa}

1. 初始化 $ADG=((P_a,P_d),(S_a,S_d),(U_a,U_d))$；
2. 构建攻击策略集合 $S_a=\{s_1^a,s_2^a,\cdots,s_m^a\}$；
3. 构建防御策略集合 $S_d=\{s_1^d,s_2^d,\cdots,s_n^d\}$；
4. If ADG 是零和攻防博弈模型($U_a=-U_d$) then
   //仅需计算 U_a 或 U_d，这里计算 U_d
5.　for all $s_i^a\in S_a$, do
6.　用式(1)计算 s_i^a 的所有原子攻击的攻击收益之和 $\sum_i Dcost(a_i)$；
7.　对每一个防御策略 $s_j^d\in S_d$，用式(2)计算 s_j^d 的 $Decost$，$U_{dij}=\sum_i Dcost(a_i)-Decost$；
8.　生成效用矩阵 $\boldsymbol{U}$；
9. else if ADG 是非零和攻防博弈模型($U_a\neq -U_d$) then
10.　对每一个攻击策略 $s_i^a\in S_a$，用式(1)计算 s_i^a 的所有原子攻击的攻击收益之和 $\sum_i Dcost(a_i)$，$U_{aij}=\sum_i Dcost(a_i)+AC$；
11.　对每一个防御策略 $s_j^d\in S_d$，用式(2)计算 s_j^d 的 $Decost$，$U_{dij}=\sum_i Dcost(a_i)+Decost$；
12.　生成效用矩阵 $\boldsymbol{U}$；
13. if 矩阵 $\boldsymbol{U}$ 存在鞍点　then
14.　调用纯策略求解子算法 Slove1(ADG)；
　　//求解 $ADG=((P_a,P_d),(S_a,S_d),(U_a,U_d))$
15. else if 矩阵 $\boldsymbol{U}$ 不存在鞍点　then
16.　调用混合策略求解子算法 Slove2(ADG)；

17. 对得到攻击意图和防御策略进行分析，确定最终的攻击意图和最优主动防御策略 S_{oa}；

18. return S_{oa}；

纯策略求解子算法具体如下.

算法 2. 纯策略求解子算法 Slove1(ADG).

输入：攻防博弈模型 ADG

输出：Nash Equilibrium

1. $M=\varnothing$；
2. for all $s_1 \in S_i$，
3. $\{S=\text{Solve1}(Sub(ADG,s_1))$
4. $S'=\underset{s\in S}{\text{argmax}}\, U_i(s_1,s)$；
5. //$\underset{s\in S}{\text{argmax}}\, U_i(s_1,s)$表示使$U_i(s_1,s)$取最大值的$s$集合
6. if $M=\varnothing$ or $U_i(s_1,S')=U_i(M)$
7. $M=M\cup Add(s_1,S')$；
8. //$Add(s_1,S')$表示添加策略 s_1 到 S'
9. if $U_i(s_1,S')>U_i(M)$；
10. $M=Add(s_1,S')$； $\}$

return M.

混合策略求解子算法具体如下.

算法 3. 线性规划求解混合策略子算法 Slove2(ADG).

输入：攻防博弈模型 ADG

输出：Nash Equilibrium

1. maximize v
2. subject to
3. for all $s_j \in S_j$；
4. $\sum_{i=1}^{m} p_i U(s_i,s_j) \geq v$；
5. $\sum_{i=1}^{m} p_i = 1$，$p_i \geq 0$.

4.3 算法复杂性分析

基于攻防博弈模型的主动防御策略选取算法的关键是攻防博弈模型 $ADG=((P_a,P_d),(S_a,S_d),(U_a,U_d))$的建立和求解，包括特定攻击策略的可行防御策略集合的建立，攻防策略成本量化和计算，最后就是攻防博弈模型的求解. 为了提高效率，攻防成本量化模型中许多参量可以预先配置在数据库中. 在防御策略选取模块初始化时，这些数据库信息加载入内存中. 例如攻击损失代价、资源描述、防御操作和负面代价系数表、残余损失系数表等防御代价模型参数. 整个算法的时间复杂度主要取决于两个子算法计算所有的纳什均衡. 给出以下两个关于子算法复杂度的定理. 由于篇幅限制，这里不给出定理的证明.

定理 1. 子算法 1 求解攻防博弈模型 $ADG=((P_a,P_d),(S_a,S_d),(U_a,U_d))$的最优纯策略集合的时间复杂度是线性时间的.

定理 2. 子算法 2 利用非线性规划求解攻防博弈模型 $ADG=((P_a,P_d),(S_a,S_d),(U_a,U_d))$的最优混合策略集合的时间复杂度是多项式时间的.

分析可见，整个算法的复杂度可以满足防御系统的需求.

5 应用实例与分析

为了验证前面所提出的攻防代价量化可计算模型和网络攻防博弈模型，本文采用如图 5 所示的网络拓扑结构来模拟攻防情景. 攻击主机位于外部网络，目标网络为交换网络，其中共有 3 台计算机，分别为公共 Web 服务器、文件服务器和内部数据库服务器. 防火墙将目标网络与外部网络分开，防火墙规则如表 3 所示. 利用弱点扫描软件对目标系统进行弱点分析，主机信息和得到的弱点信息如表 4 所示.

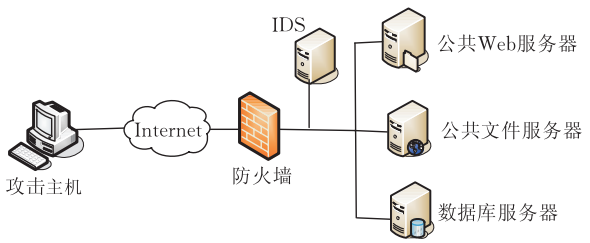

图 5 网络拓扑实例

表 3 防火墙规则信息

源主机	目的主机	服务	访问策略
All	Web server	http	Allow
All	Web server	ftp	Allow
All	File server	ftp	Allow
Web server	Database server	Oracle	Allow
File server	Database server	ftp	Allow

表 4 服务器弱点信息

主机	操作系统	弱点	Bugtraq 编号
Web server	Linux	Apache Chunked Enc.， Wu-Ftpd SockPrintf()	5033 8668
File server	Linux	Ftp .rhost overwrite	328
Database server	Linux	Oracle TNS Listener Local buffer overflow	4033 3886

假设攻击者在攻击主机上具有 Root 权限，并在此发起攻击，将获取数据库服务器的 Root 权限作为目标. 根据防火墙规则，攻击者在 Web 服务器、文件服务器上，仅仅具有最低的用户权限 Access，而无法访问数据库服务器. 但是服务器弱点的存在及其依赖关系，攻击者可以进行如表 5 所示的原子攻击，同时给出了攻击类别和致命度信息. 对服务器弱点、原子攻击及其关联关系进行评估分析，从防御策略库(参见表 2)选出可用的防御策略信息如表 6

所示，并考虑无防御措施的情况.

表 5　原子攻击描述

编号及名称	类别	AL
1. Apache chunk overflow	Root	10
2. Wu-Ftpd buffer overflow	Root	10
3. Ftp. rhosts	User	5
4. Remote buffer overflow	Root	10
5. Local buffer overflow	Root	10

表 6　防御策略描述

名称	$Ocost$	$Ncost$	$Rcost$ 中 ε 的取值
D_1：安装 Oracle 补丁	10	0	$\varepsilon_1=\varepsilon_2=\varepsilon_3=\varepsilon_5=1$，$\varepsilon_4=0$
D_2：安装 Apache 补丁	10	0	$\varepsilon_1=0$，$\varepsilon_2=\varepsilon_3=\varepsilon_4=\varepsilon_5=1$
D_3：取消“MAIL_ADMIN”	10	160	$\varepsilon_2=0$，$\varepsilon_1=\varepsilon_3=\varepsilon_4=\varepsilon_5=1$
D_4：关闭 FTP 服务	10	160	$\varepsilon_1=\varepsilon_2=\varepsilon_4=\varepsilon_5=1$，$\varepsilon_3==0$
D_5：取消 suid root	10	240	$\varepsilon_1=\varepsilon_2=\varepsilon_3=\varepsilon_4=1$，$\varepsilon_5=0$
D_6：不采取防御措施	0	0	$\varepsilon_1=\varepsilon_2=\varepsilon_3=\varepsilon_4=\varepsilon_5=1$

根据我们提出的网络防御图模型，对输入防火墙和路由器的配置文件、弱点数据库和防御策略等信息对该网络系统进行建模得到一个抽象的网络防御图，如图 6 所示. 通过对图 6 分析发现，虽然网络防火墙设置了静态的规则来保护网络中的数据库服务器，但由于弱点的依赖关系，还是存在 3 条可能的攻击路径到达攻击目标. 攻击者可能攻击策略为

$$A_1: A \xrightarrow{1} B \xrightarrow{4} E;$$

$$A_2: A \xrightarrow{2} C \xrightarrow{4} E;$$

$$A_3: A \xrightarrow{3} D \xrightarrow{3} F \xrightarrow{5} E.$$

其中 $A \xrightarrow{1} B \xrightarrow{4} E$ 表示攻击者从初始状态 A 利用原子攻击 1 到达 B，然后利用攻击 4 到达目标状态 E，即为一个攻击策略.

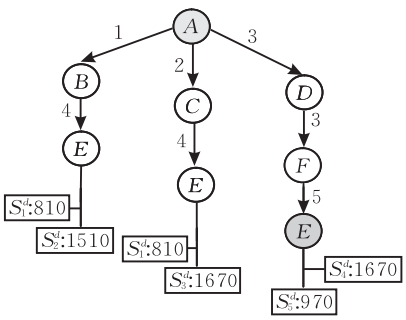

图 6　网络系统防御图

下面我们介绍利用上述算法来求解最优的防御策略的过程. 攻防策略集合确定完之后，需要计算攻防策略代价，为了简化分析，采用零和非合作攻防博弈模型来进行最优防御策略选取，从而仅需计算防御代价即可. 考虑到攻防代价的实际意义，防御者的防御代价取负值. 本文给出的具体代价数值都是以金融货币为单位的. 查询防御策略库得到各个防御策略的 $Ocost$，具体数值见表 4. 因为攻击都是针对某个服务器，可能造成该服务器的拒绝服务. 所以该攻击仅对目标资源的可用性产生危害，即 $P_i=P_c=0$，$P_v=1$. 若 $Ncost$ 很小时，我们可忽略不计，在表 4 中设为 0. 否则 $Ncost$ 的计算转换为对服务器 DOS 攻击的损失代价，因为防御策略的负面影响可以看作是对服务器的一次 DOS 攻击. Web 服务器和文件服务器的 $criticality$ 均为 4，Database 服务器的 $criticality$ 为 5. 安全属性代价的高、中、低分别用 30，20，10 来表示，Web 服务器和文件服务器的安全属性代价为 20，Database 服务器的安全属性代价为 30. 防御代价模型参数取值如表 6 所示，ε_i 表示防御策略防御编号为 i 的攻击所具有的残余损失程度. 然后，通过用式(1)和(2)来计算每一个攻击策略的防御代价，如图 7 攻防策略收益矩阵所示.

$$\begin{array}{c} \\ A_1 \\ A_2 \\ A_3 \end{array} \begin{array}{c} \begin{array}{cccccc} S_1^d & S_2^d & S_3^d & S_4^d & S_5^d & S_6^d \end{array} \\ \begin{pmatrix} 810 & 1510 & 1670 & 2470 & 2650 & 2300 \\ 810 & 2470 & 1670 & 2470 & 2470 & 2300 \\ 2310 & 2310 & 2470 & 1670 & 970 & 2300 \end{pmatrix} \end{array}$$

图 7　攻防博弈收益矩阵

Nash 根据 Brouwer 不动点定理给出了每一个有限博弈都有一个均衡点的证明[30]. 我们这里得到的攻防博弈是一个有限博弈，所以肯定存在均衡点. 最后，用定义 14 来求解上述建立的攻防双方采用混合策略时的纳什均衡. 利用基于攻防博弈模型的主动防御策略选取算法，得到一个纳什均衡：$p_a=\left(\frac{67}{159},0,\frac{92}{159}\right)$，$p_d=\left(\frac{28}{53},0,0,0,0,\frac{25}{53}\right)$. 即攻击者最优的攻击策略是以概率 $\frac{92}{159}$ 选择攻击策略 A_3 和以概率 $\frac{67}{159}$ 选择攻击策略 A_1；防御者最优的防御策略是以概率 $\frac{28}{53}$ 选择防御策略 D_1 和以概率 $\frac{25}{53}$ 选择防御策略 D_5. 所以对于防御者来说，最优的防御策略是 D_1 安装 Oracle 补丁，从而攻击者的目标将无法实现. 在实际应用中，可以根据网络环境和安全需求可以同时采取防御策略 D_1 和防御策略 D_5，这样网络信息系统安全性将大大加强.

6　结束语

为了进行网络信息系统安全测评和最优主动防御，提出了一个新的基于网络系统安全测评的主动

防御模型——网络攻防博弈模型，该模型包括网络防御图模型、攻防策略代价分类及其量化模型和基于上述模型的最优主动防御决策算法. 防御者以最优的防御代价进行网络安全加固和主动防御. 从而构建一套自动地风险评估、最优防御成本的主动防御模型，为及时有效地主动防御提供了有力保证.

最后通过一个典型的网络实例模拟和分析该模型和算法在网络安全测评和最优主动防御方面的应用.

参 考 文 献

[1] Zhang Yong-Zheng, Fang Bin-Xing, Chi Yue et al. Risk propagation model for assessing network information systems. Journal of Software, 2007, 18(1): 137-145(in Chinese)
(张永铮，方滨兴，迟悦等. 用于评估网络信息系统的风险传播模型. 软件学报，2007，18(1)：137-145)

[2] Nicol D M, Liljenstam M. Models and analysis of active worm defense//Lecture Notes in Computer Science, 2005, 3685: 38-53

[3] Nash John. Equilibrium points in n-person games. Proceedings of the National Academy of Sciences, 1950, (36): 48-49

[4] Hamilton S N, Miller W L, Ott A, Saydjari O S. The role of game theory in information warfare//Proceedings of the 4th Information Survivability Workshop. Vancouver, Canada, 2002: 45-46

[5] Feng Deng-Guo, Zhang Yang, Zhang Yu-Qing. Survey of information security risk assessment. Journal of China Institute of Communications, 2004, 25(7): 10-18(in Chinese)
(冯登国，张阳，张玉清. 信息安全风险评估综述. 通信学报，2004，25(7)：10-18)

[6] Lin Chuang, Wang Yang, Lin Quan-Lin. Stochastic modeling and evaluation for network security. Chinese Journal of Computers, 2005, 28(12): 1944-1956(in Chinese)
(林闯，汪洋，李泉林. 网络安全的随机模型方法与评价技术. 计算机学报，2005，28(12)：1944-1956)

[7] Schneier B. Attack trees. Dr. Dobb's Journal, 1999, 24(12): 21-29

[8] Moore Andrew P, Ellison Robert J, Linger Richard C. Attack modeling for information security and survivability. Technical Note: CMU/SEI-2001-TN-001, 2001

[9] Dacier M. Towards quantitative evaluation of computer security. Institut National Polytechnique de Toulouse, 1994

[10] Ortalo R, Deswartes Y, Kaaniche M. Experimenting with quantitative evaluation tools for monitoring operational security. IEEE Transactions on Software Engineering, 1999, 25(5): 633-650

[11] Phillips C A, Swiler L P. A graph-based system for network vulnerability analysis//Proceedings of the 1998 Workshop on New Security Paradigms. Charlottesville, Virginia, United States, 1998: 71-79

[12] Ramakrishnan C, Sekar R. Model-based vulnerability analysis of computer systems//Proceedings of the 2nd International Workshop on Verification, Model Checking and Abstract Interpretation. Pisa, Italy, 1998: 1-8

[13] Ritchey R W, Ammann P. Using model checking to analyze network vulnerabilities//Proceedings of the IEEE Symposium on Security and Privacy. Berkeley, CA, USA, 2000: 156-165

[14] Lee Wenke. Toward cost-sensitive modeling for intrusion detection and response. Journal of Computer Security, 2002, 10(1-2): 5-22

[15] Jiang Wei et al. A game theoretic method for decision and analysis of the optimal active defense strategy//Proceedings of the International Conference on Computational Intelligence and Security. Harbin, China, 2007: 819-823

[16] Feng Ping-Hui, Lian Yi-Feng, Dai Ying-Xia et al. An evaluation model of vulnerability exploitation cost for network system. Chinese Journal of Computers, 2006, 29(8): 1375-1382(in Chinese)
(冯萍慧，连一峰，戴英侠等. 面向网络系统的脆弱性利用成本估算模型. 计算机学报，2006，29(8)：1375-1382)

[17] Haywood O G. Military decision and game theory. Journal of the Operations Research Society of America, 1954, 2(4): 365-385

[18] Brams S J. Game Theory and Politics. New York: Free Press, 1975

[19] Syverson P F. A different look at secure distributed computation//Proceedings of the 1997 IEEE Computer Security Foundations Workshop. MA, USA, 1997: 109-115

[20] Burke D. Towards a game theory model of information warfare[M. S. dissertation]. Technical Report: AFIT/GSS/LAL/99D-1. Airforce Institute of Technology, 1999

[21] Lye K-W, Wing J. Game strategies in network security. School of Computer Science, Carnegie Mellon University, Pittsburgh: Technical Report CMU-CS-02-136, 2002

[22] Xu J, Lee W. Sustaining availability of Web services under distributed denial of service attacks. IEEE Transactions on Computers, 2003, 52(4): 195-208

[23] Liu P, Zang W. Incentive-based modeling and inference of attacker intent, objectives, and strategies//Proceedings of the 10th ACM Computer and Communications Security Conference(CCS'03). Washington, DC, 2003: 179-189

[24] Jiang Wei, Fang Bin-Xing et al. Optimal network security strengthening using attack-defense game model//Proceedings of the 6th International Conference on Information Technology: New Generations ITNG 2009. Las Vegas, Nevada, USA, 2009

[25] Lippmann R P, Fried D J, Graf I et al. Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation//Proceedings of the Information Surviv-

ability Conference and Exposition (DISCEX) 2000. Los Alamitos, CA: IEEE Computer Society Press, 2000, 2: 12-26

[26] Natalia Stakhanova, Samik Basu, Johnny Wong. A Taxonomy of Intrusion Response Systems. International Journal of Information and Computer Security, 2007, 1(1/2): 169-184

[27] Gordon L, Loeb M, Lucyshyn W, Richardson R. 2006 CSI/FBI computer crime and security survey//Proceedings of the Computer Security Institute. San Francisco, California, 2006: 1-29

[28] Northcutt S. Networking Intrusion Detection: An Analyst's Handbook. Indianapolis, Indiana, United States: New Riders Publishing, 1999

[29] Gibbons Robert. A Primer in Game Theory. New York: Pearson Higher Education, 1992

[30] Nash John. Non-cooperative games. The Annals of Mathematics, 2nd Ser., 1951, 54(2): 286-295

JIANG Wei, born in 1979, Ph. D. candidate. His research interests are network and information security, network attack and defense.

FANG Bin-Xing, born in 1960, professor, Ph. D. supervisor, member of Chinese Academy of Engineering. His current research interests include computer architecture, information security and computer network.

TIAN Zhi-Hong, born in 1978, Ph. D., lecturer. His research interests focus on network and information security.

ZHANG Hong-Li, born in 1973, professor, Ph. D. supervisor. Her research interests include network and information security, network measure.

Background

This research is partly supported by the National Basic Research Program (973 Program) of China under grant No. 2007CB311100, the National High Technology Research and Development Program (863 Program) of China under grant(Nos. 2007AA01Z442, 2007AA01Z406, 2009AA012437).

Traditional static protective measures are not sufficient to secure a complex networked system. Existing cyber security technologies can only passively prevent, detect, and react to cyber attacks. Intrusion detection (ID) architecture is a passive information processing paradigm. In many cases intrusion response is "too late" after very serious damage is caused. Attack prediction is very critical for cyber homeland security. It is a big challenge that making correct optimal proactive defense decisions during an earlier stage of the attack. In such a way we can transform passive to proactive cyber defense, and much less harm will be caused without consuming a lot of resources.

This paper views the interactions between an attacker and the defender as a two-player non-cooperative game and formulate an attack-defense game (ADG) model for the game. The defense graph model, attack-defense taxonomy and cost quantitative model are proposed. An algorithm for optimal active defense strategy selection based on those models is proposed. Optimal defense strategies with minimizing costs are used to defend the attack and harden the network in advance.