一种基于攻防成本博弈的防御策略评价模型

刘建波
(山东财政学院 计算机网络中心,山东 济南 250014)

摘 要:为了探求信息系统的最佳防御等级策略,从经济博弈论的全新角度研究信息安全攻防策略问题,提出一种基于"诱导迂回"的信息安全系统架构,建立基于攻防成本差异博弈的评价体系,以成本差异最大化为基点建立一种边界数学模型,刻画网络安全攻防矛盾,从而解决最佳防御策略的选取。通过仿真实验数据分析上述信息结构与模型。结果证明,提出的模型和系统结构是可行有效的,对于减少信息安全投资的盲目性、指导建设防御体系具有重要的实践意义。

关键词:信息安全;攻防博弈;成本;收益;诱导迂回;防御策略
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2011)10-0229-04

A Evaluation Model of Defensive Strategy Based on Attack-Defense Game Cost

LIU Jian-bo
(Network Center, Shandong University of Finance, Jinan 250014, China)

Abstract: In order to explore the optimal strategy of defense level of information system, it researches the problem of information safety from the view of economy game, and proposes an system structure of information security based on "inducible and circuitous tactics", and then establishes a evaluation system based on the game of the difference of attack-defense game, in which proposes a boundary mathematical model based on the difference of cost to depict the contradiction of attacker and defender. At last, it analyzes above structure and model through the typical experimental data. Results indicate that the structure and model is feasible and effective, and also has important practical significance to reduce the blindness of the investment and to direct the building of defense system.

Key words: information security; attack-defense game; cost; profit; inducible and circuitous tactics; defensive strategy

0 引 言

随着信息技术与互联网的不断发展,网络信息安全已经成为信息社会所面临的最重要问题,其关系到国家的政治、经济、社会等各个领域。其实,"不惜一切代价"的防御是不理性的,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的一种均衡[1]。从信息安全经济学博弈理论角度看,与实现系统防御产生一定的成本相同,对于网络的任何攻击手段都要付出一定的代价,因此可以利用博弈论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[2]。为了更好地实现系统防御以及综合的"性价比",笔者认为应该同时对攻防两种角色成本进行综合评价,所以提出一种基于攻防成本博弈的防御策略评价模型,以攻防成本差异最大化为基点评价防御策略。

1 相关研究工作

从信息安全经济学角度分析信息安全成为近年来研究的重点方向。相关研究也取得了值得借鉴的成果,Lee在2002年首次提出了成本敏感模型作为响应决策的基础[3],根据响应成本和攻击损失成本来决定是否响应;文献[4]中,给出了比较完整的攻防分类及其成本敏感模型,有效地应用于最优防御策略的制定。而将博弈论应用于信息安全分析的应用研究并不是很多:1997年Burke[5]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[6]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。文中借鉴了上述研究成果,但与之不同,具体如下:建立基于攻防成本博弈的数学模型;定义攻防经济参数,利用攻防博弈模型检验实验数据,并提出不同信息结构的最佳防御等级设定策略。

2 基于"诱导迂回"的信息安全系统架构

信息安全架构主要由蜜罐系统和真实系统两个部

收稿日期:2011-03-24;**修回日期**:2011-06-27
基金项目:山东省社科规划项目(09DJGZ18)
作者简介:刘建波(1978-),男,硕士,工程师,研究方向为计算机网络安全与数据挖掘。

分组成，其基本原理如下：对于所有外部访问，需要基于目的端口由防火墙和路由器分析过滤，正常访问直接访问真实系统中服务器，而可疑访问被转发到蜜罐系统。

为了便于量化研究，架构中按照安全等级和重要性将信息抽象成三种集合：普通信息、蜜罐信息和权威信息[7]，参见图 1 。

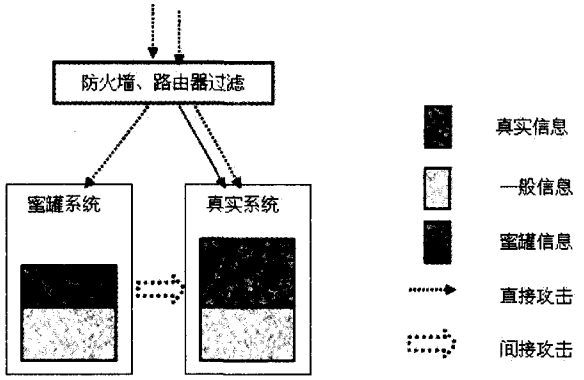

图 1 系统架构

为了诱导潜在入侵者，系统架构中将两个系统中设置完全相同的普通信息，当然该类信息比例并不是越高越好，要限制其信息量和完整性，从而保证即便入侵者进入蜜罐系统进行非法操作，也不会影响真实系统的正常运行。除了设置普通信息之外，还需在设置一定的“权威信息”，这里的权威信息不同于真实系统中的权威信息，该类信息的破解及其获取难度加大，其目的在于诱导真实系统的潜在入侵者，成功入侵者获取该类信息会得到更大的成就感，自然就会降低入侵真实系统的可能。至此，在文中提出的评价模型中，就可以针对以上两种系统中的几类信息内容设置不同的安全等级并进行相关评价。

3 系统防御等级评价模型

基于以上提出的信息安全架构，文中提出一种基于攻防成本博弈的防御等级评价模型。

3.1 条件假设

为了更好地利用信息安全经济学理论研究该问题，提出以下假设：

假设 1：信息安全设计人员基于信息内容分别设置信息的保护等级。

假设 2：按照潜在入侵者最终行为将入侵行为分成两类，即入侵蜜罐系统和真实系统。

假设 3：潜在入侵者与系统保护管理行为都有各自的“成本”与“收益”，成本可能是资金投入也可能是脑力投入，入侵者的收益可能是物质的，也可能为心理上的满足或者愉悦感，信息安全管理行为的收益可能为系统的安全稳定运行带来的社会价值或者管理者的成功感，为了便于研究，模型中将以上提及的成本和收益都抽象成经济成本和收益[8,9]。

假设 4：攻击者和防御者都追求利益最大化[10]。

3.2 变量定义与分析

基于信息安全经济学中提出的博弈理论，文中基于入侵者与防御者成本差异最大化为切入点，提出对应环境变量及其评价模型。

变量定义参见表 1。

表 1 变量定义表

变量	含义表述	变量	含义表述
T	攻击事件时间点	C_D	保护蜜罐系统权威信息的单位成本
NDT	时间 T 进入蜜罐系统的入侵者数	C_G	保护真实系统权威信息的单位成本
N_{GT}	时间 T 进入真实系统的入侵者数	C_M	保护普通信息的单位成本
P_{DT}	时间 T 蜜罐系统中权威信息的安全级别	E_D	进入蜜罐系统获得权威信息的单位成本
P_{GT}	时间 T 真实系统中权威信息的安全级别	E_G	进入真实系统获得权威信息的单位成本
P_{MT}	时间 T 普通信息的安全级别	E_M	进入蜜罐系统获得普通信息的单位成本
Q_D	蜜罐系统中的权威信息	V_D	进入蜜罐系统获得权威信息的单位收益
Q_G	真实系统中的权威信息	V_G	进入真实系统获得权威信息的单位收益
Q_M	普通信息	λ	防御者收益贴现率

一般情况下，随着信息安全级别的增加，正如图 2 所示，防御者基于信息安全级别的变化的成本投入总量变化率远大于入侵者总投入变化率[11]，图 2 真实反映了两种成本与信息安全级别之间的关系：与入侵者借助某些技术手段发现系统漏洞进行攻击相比，系统安全设计维护人员的付出相当高，比如安全设备资金投入、优化过滤算法、定期系统补丁、进行入侵检测报告等。

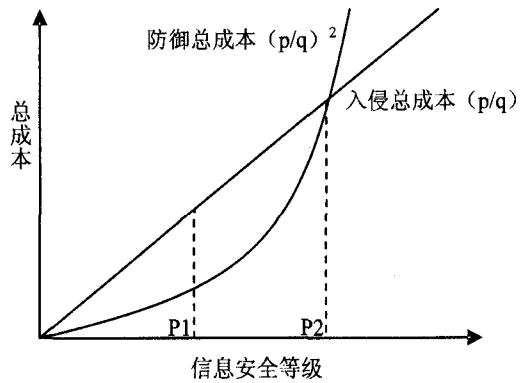

图 2 成本与安全级别关系

虽然两种总成本与信息安全级别都呈现正比关系，但是存在一定的差异：如果信息安全级别小于 P2，防御者总成本小于入侵者总成本，反之，防御者总成本变化率远大于入侵者。因此，从信息安全经济学博弈

论角度分析，信息安全级别的设定要充分权衡两种总成本的差异，并不是安全级别越大越好，在兼顾入侵者成本的基础上，要充分考虑其“性价比”。因此可以从入侵者与防御者投入成本差异最大化为入手点，建立系统防御等级评价模型。

3.3 模型建立

基于以上变量定义与分析，建立如下基于攻防博弈的数学评价模型。

$$\text{Maocirvinaze } \overline{w} = n_{D1} \cdot (e_D \cdot P_{D1}/q_D + e_{M1}/q_M) - (c_D \cdot (p_{D1}/q_D)^2 + c_M \cdot (p_{M1}/q_M)^2) + n_{G1} \cdot e_G \cdot (p_{G1}/q_G + p_{M1}/q_M) - (c_G \cdot (p_{G1}/q_G)^2 + c_M \cdot (p_{M1}/q_M)^2) + \lambda \cdot \sum_{n-2}^{t} (n_{Dn} \cdot (e_D \cdot p_{Dn}/q_D + e_M \cdot p^{M2}/q_M) - (c_D \cdot (p_{Dn}/q_D)^2 + C_M \cdot (p_{M2}/q_M)^2) + n_{Gn} \cdot e_G \cdot (p_{Gn}/q_G + p_{Mn}/q_M) - (c_G \cdot (p^{Gn}/q_G)^2 + c_M \cdot (p_{Mn}/q_M)^2))$$

约束条件：

$$p_{Di}, p_{Gi}, p_{Mi} \geqslant 0$$

$$v_D \cdot (q_D + q_M) \geqslant e_D \cdot (p_{Di}/q_D + p_{Mi}/q_M)$$

$$v_G \cdot (q_G + q_M) \geqslant e_D \cdot (p_{Gi}/q_G + p_{Gi}/q_G)$$

为了从经济学角度更好地进行数字实验仿真，模型中引入了贴现率，其目的为了充分体现不同时间点的利率差异。为了归一化检验，假设入侵时间点 $t = 2$，即在两个时间点发生入侵行为，基于评价模型求出变量 $P_{D1}, P_{D2}, P_{G1}, P_{G2}, P_{M1}$ 和 P_{M2} 的一重积分：

$$P_{D1} = \frac{n_{D1} \cdot e_D \cdot q_D}{2 \cdot C_D}$$

$$P_{D2} = \frac{\lambda \cdot n_{D2} \cdot e_D \cdot q_D}{2 \cdot C_D}$$

$$P_{G1} = \frac{n_{G1} \cdot e_G \cdot q_G}{2 \cdot C_G}$$

$$P_{G2} = \frac{\lambda \cdot n_{G2} \cdot e_G \cdot q_G}{2 \cdot C_G}$$

$$P_{M1} = \frac{(n_{D1} \cdot e_D + n_{G1} \cdot e_G) \cdot q_M}{4 \cdot C_M}$$

$$P_{M2} = \frac{\lambda \cdot (n_{D2} \cdot e_D + n_{G2} \cdot e_G) \cdot q_M}{4 \cdot C_M}$$

从计算结果可以看出，系统架构中的蜜罐系统和真实系统的防御等级策略取决于入侵者数、单位信息入侵成本、信息量和单位信息保护成本。与单位信息保护成本呈现一种反比关系，与其他三个变量呈现正比关系。

4 实验结果分析

为了更进一步分析文中提出的评价模型，根据提出的假设，实验环境中模拟了若干组数据（见表 2）。进行归一化检验信息安全等级设定与相关参数的关系，得到详细分析结果。

表 2　实验变量数据

$n_{D1}=95$	$e_D=4$	$c_M=50$	$v_D=7$
$n_{D2}=75$	$e_G=7$	$q_D=5$	$v_G=10$
$n_{G1}=55$	$c_D=35$	$q_G=8$	$\lambda=0.06$
$n_{G2}=35$	$c_G=70$	$q_M=4$	

从图 3 看出，蜜罐系统和真实系统中的防御等级随着贴现率的增加而减低，而且从攻击事件发生的时间点来看，先前发生的攻击事件的安全等级变化率小于后续事件，比如 p_{D1} 的变化率效率 P_{D2}，P_{G1} 变化率小于 P_{G2}。因此，如果银行贴现率比较高，在保证净利润的前提下，防御者在系统运行前期设置高等级安全级别获得的利润要远大于后期[12]。从信息安全经济学博弈论角度分析，由于防御者和入侵者之间存在着相互竞争，其中一方的高利润必定以对方的高成本为代价，因此，为了便于分析问题，可以将设计者贴现率与入侵者成本贴现率同等看待。基于这一原理，若攻击系统成本贴现率比较高，入侵者更倾向在前期进行入侵攻击活动。基于以上分析，可以得出重要结论：在高贴现率背景下，为了更好地实现信息安全，防御者在前期设计的信息防御等级应该明显高于后期。

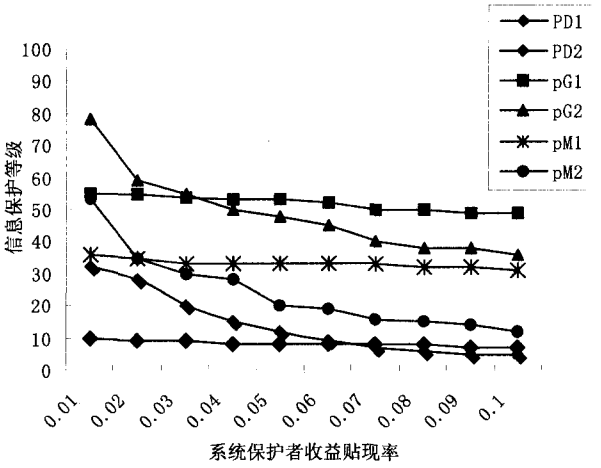

图 3　贴现率与安全等级

图 4 呈现出蜜罐系统和真实系统中共有的普通信息 q_M 与信息安全防御等级关系分布图，在两个攻击时间点，系统安全防御等级都随着普通信息量的增加而增加。由于普通信息在两个系统中都有一定比重，信息量越大，对攻击者的诱惑力越大；同时，考虑成本贴现率，入侵者采用的策略可能选择较早的时间点进行攻击，以获得更大的收益。基于以上分析，可以得出重要结论：如果两个系统中的普通信息比重比较大，为了降低入侵者的成功率，应该在前期设置比较高的系统防御等级为宜。

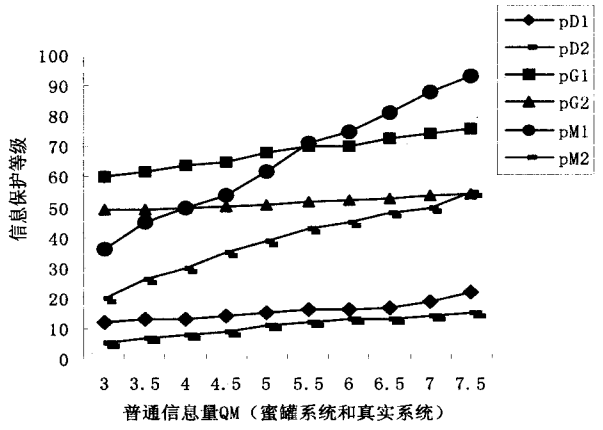

图 4 普通信息与安全等级

5 结束语

为了评价最优信息防御等级，文中提出基于攻防博弈的系统防御等级评价模型，实验数据分析结果表明，其研究方法能针对各自不同的信息结构制定最佳防御等级。

需要指出，按照信息安全经济学成本效益博弈分析方法决策，实现起来比讨论要难很多，文中模型提及的若干假设是基于常态环境的假设，现实中存在诸多不可控因素。比如，信息系统正常运行过程中并不能准确把握入侵者的具体人数以及入侵时间；另外，入侵者可能不以某种经济利益为目的攻击信息系统。因此，要从信息安全经济学角度全面分析系统攻防体系，还需要针对类似这些问题进行深入研究，也是今后值得研究的重点。

参考文献：

[1] 孙剑颖. 企业信息安全投资的经济学决策模型浅析[J]. 东北财经大学报，2005(3)：67-68.

[2] 姜 伟，方滨兴，田志宏，等. 基于攻防博弈模型的网络安全测评和最优主动防御[J]. 计算机学报，2009，32(4)：818-819.

[3] Lee Wenke. Toward cost-sensitive modeling for intrusion detection and response[J]. Journal of Computer Security，2002，10(1-2)：10-20.

[4] Jiang Wei. A game theoretic method for decision and analysis of the optimal active defense strategy[C]//Proceedings of the International Conference on Computational Intelligence and Security. Harbin，China：[s. n.]，2007：819-820.

[5] Burke D. Towards a game theory model of information warfare [R]. [s. l.]：Airforce Institute of Technology，1999.

[6] Lye K W，Wing J. Game strategies in network security[R]. Pittsburgh：School of Computer Science，Carnegie Mellon University，2002.

[7] 孟祥宏. 信息安全攻防博弈研究[J]. 计算机技术与发展，2010，20(4)：160-162.

[8] 吉鸿珠，顾乃杰. 基于博弈论的网络安全量化评估算法[J]. 计算机应用与软件，2009，26(9)：4-6.

[9] 孙 薇. 组织信息安全投资中的博弈问题研究[D]. 大连：大连理工大学，2008.

[10] 吕俊杰，邱菀华，王元卓. 网络安全投资外部性及博弈策略[J]. 北京航空航天大学学报，2006，32(12)：1499-1502.

[11] 石 进，陆 音，谢 立. 基于博弈理论的动态入侵响应[J]. 计算机研究与发展，2008，45(5)：750-755.

[12] 王 军. 信息安全的经济学分析及管理策略研究[D]. 哈尔滨：哈尔滨工业大学，2007.

（上接第 139 页）

[5] Tsai Cheng-fa，Tsai Chun-wei，Tseng Ching-chang. A new hybrid heuristic approach for solving large traveling salesman problem[J]. Information Sciences，2004，166(1)：67-81.

[6] 邹 鹏，周 智，陈国良，等. 求解 TSP 问题的多级归约算法[J]. 软件学报，2003，14(1)：35-42.

[7] 许丽佳，蒲海波，蒋宏健. 改进遗传算法的路径规划研究[J]. 微计算机信息，2006，22(2)：251-253.

[8] Helsgaun K. An effective implementation of the Lin-Kernighan traveling salesman heristic[J]. European Journal of Operational Research，2000，126(1)：106-130.

[9] Warlimont R. On the iterates of Euler's function[J]. Arch-Math，2001，76：345-349.

[10] Ong H L. Worst-Case Analysis of Two Traveling Salesman Heuristics[J]. Operations Res，1984，86(3)：273-277. [11] 宋世杰，刘高峰，周忠友，等. 基于改进蚁群算法求解最短路径和 TSP 问题[J]. 计算机技术与发展，2010，20(4)：144-147.

[12] 谢胜利，唐 敏，董金祥. 求解 TSP 问题的一种改进的遗传算法[J]. 计算机工程与应用，2002，38(8)：58-62.

2011 CCF 中国计算机大会

第八届 CCF 中国计算机大会(2011 CCF China National Computer Conference，CCF CNCC2011)将于 2011 年 11 月 24-26 日在深圳市会展中心举行。欢迎全国各界人士踊跃参加。会议网站：http://sewm2011.hbu.cn

会议咨询：张明，袁方(sewm2011@hbu.cn，13933221661)