

基于博弈论的网络空间安全若干问题分析

朱建明, 王秦

(中央财经大学 信息学院, 北京 100081)

摘要: 信息安全经济学是信息安全的一个重要研究领域, 博弈论是研究信息安全经济学的主要基础理论和工具之一。基于博弈论对网络空间安全的主要问题进行了分析, 其中包括网络攻防、密码协议设计和安全技术配置。对于网络安全攻防, 重点分析了攻防双方的对抗状况和防守方之间的互相依赖; 对于密码协议设计, 重点分析了博弈论在秘密共享和安全多方计算当中的应用; 对于安全技术配置, 重点分析了博弈论在入侵检测系统和防火墙技术中的应用。最后指出了当前研究存在的不足和信息安全经济学未来的研究方向。

关键词: 网络空间安全; 博弈论; 密码学

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2015.00006

Analysis of cyberspace security based on game theory

ZHU Jian-ming, WANG Qin

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

Abstract: Information security economics is an important research area and game theory is one of the main basic theories and tools of cyberspace security. Based on game theory, the main problems of cyberspace securing were analyzed which including network attack and defense, cryptographic protocol design, and security technology configuration. The conflicts between attackers and defenders as well as the dependence among defenders were mainly analyzed on network and defense. Game theory's applications in secret sharing and secure multi-party computation were emphasized on cryptographic protocol design. The game theory's applications in intrusion detection system and firewall technology were analyzed on security technology configuration. Finally, the limitations of current researches and carries on the forecast to the future research directions were pointed out.

Key words: cyberspace security; game theory; cryptography

1 引言

近年来, 互联网的发展为社会生活的各个方面带来了巨大的变化。特别是“互联网+”战略将互联网应用推向一个新的阶段, 传统产业在互联网平台上焕发了新活力。与此同时, 信息作为一种重要的战略资源引起了世界范围内的广泛关注, 信息的获取、处理和安全保障能力成为一个

国家综合国力的重要组成部分。随着互联网的快速发展, 网络空间安全问题正变得日益严峻。国家互联网应急中心(CNCERT/CC)最新发布的《网络安全信息与动态周报》显示, 在2015年11月2日至11月8日的一周内, 境内感染网络病毒的主机数量达99.9万台, 较前一周环比增加37.8%; 境内被篡改网站数量为2 616个; 境内被植入后门的网站数量为2 535个; 针对境内网站的仿冒

收稿日期: 2015-09-09; 修回日期: 2015-09-30。通信作者: 王秦, wwwqqq8688@163.com

基金项目: 国家自然科学基金资助项目(61272398)

Foundation Item: The National Natural Science Foundation of China(61272398)

页面数量为3 295个。由此可见,当前网络空间安全问题已经深入到社会生活的各个方面,其所面临的形势非常严峻!

面对安全威胁,无论是国家,还是企业和个人都面临如何保障信息安全的问题。传统的手段主要是研究各类信息安全技术以提高抵御攻击的能力。然而,仅仅依靠信息安全技术在日益复杂的互联网环境下越来越难以满足安全要求。首先,安全信息通常是高度不对称的,一般是攻击者占有优势。其次,攻击者可以选取任意一个漏洞发起攻击,而用户则需要对所有漏洞进行防范。此外,攻击者可以选择许多攻击方法甚至是非法手段,某些最新的信息技术通常也首先被攻击者所使用,而用户一般只能在一些有限的得到认可的方法中做选择。随着接入网络设备的不断增多以及攻击技术的不断增强,攻击者越来越能够从更大范围更有效地发动攻击。尽管用户都有自己的安全需求,各类安全技术也层出不穷,多数主体依然无法实现充分的安全。

因此,在重视发展信息安全技术的同时,越来越多的学者关注战略的角度,尝试使用经济学方法来解决信息安全问题。博弈论作为其中一种重要的方法,在网络空间安全中的应用也得到了越来越多学者的重视。本文试图分别通过对博弈论在网络安全攻防、密码学和安全技术配置中的应用进行综述,展示目前使用博弈论工具研究网络空间安全问题的基本现状和信息安全经济学的主要内容。

2 信息安全问题的思考

从当前网络应用软件系统的发展趋势来看,应用需求愈来愈多,复杂度愈来愈高,可用性要求愈来愈强,而日趋庞大的软件系统却愈来愈脆弱。与此同时,现代企业运营会涉及不同组织的多个信息系统,系统之间的联系日益密切,形成系统的系统(SoS, system of systems),造成信息系统的规模不断扩大,复杂性不断增加。另一方面,现代信息技术(如Web技术)使系统之间的连接更加容易,系统的边界不容易确定,不同系统的连接会造成系统运行的不确定性和不可预见性,从而增加系统的风险。而且随着网络集成度和开放性的日益提高,信息系统的一次安全事件所造成的影响更大,涉及的

面更宽。信息系统自身的脆弱性和来自内、外部的各种威胁及攻击,使得信息安全问题十分突出。特别是近年来,随着网格计算、对等计算、云计算、社会计算等互联网计算模式的发展,共享的网络计算环境已经演化成为边界模糊、系统开放的公用化计算环境,这对信息安全理论与技术提出了新的要求和新的挑战。

近年来,信息安全理论与技术发展很快,从传统的对加密解密、杀毒软件、防火墙、入侵检测的研究到对容忍入侵、可生存性、可信计算、信息保障等的研究,从关注信息的保密性发展到关注信息的可用性和服务的可持续性,从关注单个安全问题的解决发展到研究网络的整体安全状况及变化趋势。信息安全领域进入了以立体防御、深度防御为核心思想的信息安全保障时代,形成了以预警、攻击防护、响应、恢复为主要特征的全生命周期安全管理,出现了大规模网络攻击与防护、互联网安全监管等许多新的研究内容。安全管理也由信息安全产品测评发展到大规模信息系统的整体风险评估与等级保护等^[1]。

对于信息安全来说,信息安全技术无疑是最重要的。甚至很多人认为,只要有足够好的访问控制机制、形式化证明了的密码协议、有效的防火墙、更好的检测入侵和恶意代码技术,那么信息安全问题就可以得到解决^[2]。事实上,任何技术都是一把“双刃剑”,既可以用来防护,也可以用来攻击,即所谓“道高一尺,魔高一丈”。今天刚刚修复了一个安全漏洞,明天攻击者又找到了另一个新的漏洞。另一方面,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”,即考虑在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^[3]。因此,解决信息安全问题不仅要靠先进的技术,还需要从策略、管理、机制的角度提高信息安全的能力,信息安全是包括技术、管理、法律在内的系统工程。

在传统的基于密码技术的安全通信中,都假定其参与方要么是诚实的要么是恶意的。诚实的参与方在通信过程中总是遵照通信协议的要求执行,不存在欺诈行为,而恶意的参与方总是以任

意的方式欺诈其他参与方以达到其某种不可告人的目的。但是，无论参与方如何“聪明”，当他达到其欺骗目的时都要付出一定的代价，在某些情况下，甚至是得不偿失的，理性的欺诈者可能会反思其欺诈行为是否值得的问题。那么在参与者是理性的情形下，怎样权衡各参与方的最大化收益，是非常值得研究的问题。

博弈论是研究决策主体的行为发生直接相互作用时的决策以及这种决策的均衡问题，是研究竞争中参与者为争取最大利益应当如何做出决策的数学方法，是研究多决策主体之间行为相互作用及其相互平衡，以使收益或效用最大化的一种对策理论。近年来，博弈论与信息安全的研究也引起了学术界的重视^[4]。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。

网络攻防博弈模型将研究重点从具体攻击行为为转移到研究攻击者与防御者组成的对抗系统，包含了网络攻防对抗双方关系的主要属性，如攻击目标属性、攻击策略相关属性等，抓住了网络攻防对抗过程的关键因素，如激励、效用、代价、风险、约束、策略、安全机制、安全度量、安全漏洞、攻击手段、防护手段、系统状态等。利用网络攻防博弈模型可以推断网络攻防双方的均衡策略。因此，信息安全是一种典型防御与攻击的博弈，网络攻防博弈模型对于研究信息安全攻防策略，更加有效地提高信息安全技术的作用具有重要意义。

3 网络安全的攻防博弈

对于网络用户攻防博弈的研究通常需要假定用户是自私的。攻击者通过利用安全漏洞、损害其他用户利益来提升自身效用。这些攻击者的动机可能包括谋取金钱利益、得到同行认可或满足自己好奇心等。攻击者可能选择整个网络进行攻击，也可能就某几个终端节点发动攻击。总之，用户无法做到信任其他网络参与者。

一般而言，网络安全攻防博弈可以表示成类似 $(S, A^1, A^2, Q, R^1, R^2, \beta)$ 的形式^[5]。其中， S 为状态集， A^1 和 A^2 分别表示攻击者和防御者的行动集合， Q 为状态转移函数， R_1 和 R_2 分别为攻击者和

防御者的支付， β 为支付的折扣率。

目前，使用博弈论来刻画网络安全攻防交互已经得到了许多学者的重视。Manshaei 等^[6]就 6 个方面对网络安全与隐私中的博弈论应用进行了综述，即物理层和 MAC 层的安全、移动网络应用层安全、入侵检测系统、匿名与隐私、网络安全经济学以及密码学。Grossklags 等^[8]研究了几种重要的博弈类型，分别讨论了在何种情况下应该采用保护或保险手段。这几种安全博弈类型的比较如表 1 所示。

表 1 安全博弈类型比较

博弈类型	描述	参考文献
共同努力安全博弈	系统的防御水平取决于个体贡献之和	[7-11]
最弱环安全博弈	系统的防御水平取决于防御水平最低的个体	[7-10]
最佳防御安全博弈	系统的防御水平取决于防御水平最高的个体	[7-9,11]
最弱目标安全博弈	攻击者只对防御水平最低的个体进行攻击	[8]

Neyyan 等^[12]通过使用纳什均衡的概念研究了针对泛洪攻击的防御策略。Carroll 和 Grosu^[13]使用信号博弈来建模攻击者和防御者之间的欺诈现象，并讨论了采用欺诈策略给防御者带来的好处。孙薇等^[14]分析了信息安全攻防博弈和防守博弈，得出了促使企业进行信息安全投资的策略，并给出了一些具体建议。刘建波^[15]从成本差异最大化的角度来评价最佳防御策略的选取，有着很强的现实意义。

网络安全问题是典型的 IDS (interdependent security) 问题^[16]，即存在多个自私的参与者，他们可以选择投资于安全或维持现状。这些个体都想在一定风险水平下投资最少，而风险不仅取决于自己的投资情况，也取决于其他参与者的投资情况。当包含两个参与者时，博弈可以表示为表 2 的形式。

表 2 相互依赖的安全博弈

	参与者 2 投资	参与者 2 不投资
参与者 1 投资	$(Y-c, Y-c)$	$(Y-c-qL, Y-pL)$
参与者 1 不投资	$(Y-pL, Y-c-qL)$	$\{Y-[pL+(1-p)qL], Y-[pL+(1-p)qL]\}$

在表 2 中， Y 表示参与者的原有收益， c 表示安全投资成本， p 表示安全威胁发生的概率， q 表示威胁传播的概率， L 表示威胁发生后的损失。

可以证明, 包含两个直至多个参与者的情况下, 所有个体间只存在两种纳什均衡: 全部投资或全部不投资。因而必须采用相应手段来消除这种外部性。Laszka 等^[17]对信息安全投资间的相互依赖问题进行了全面的分析。IDS 中可能存在不确定性问题: 网络配置各不相同, 用户可能对攻击概率以及风险传播的概率并不了解。Johnsona 等^[18]使用基于风险参数的概率分布研究了这一问题, 并根据假定的分布得出了贝叶斯纳什均衡。吕俊杰等^[19, 20]研究了企业间病毒传染的外部性问题, 定量刻画了企业间的相互依赖程度, 得出了相应均衡解, 并把问题扩展到了风险内生的条件下。

演化博弈论是博弈论一个新的发展方向。它假设博弈主体是有限理性的, 将关注点放在长期形成的演化稳定策略。近年来也有学者使用演化博弈论分析信息安全攻防问题。孙薇等^[21]分析了企业和攻击者的复制动态和演化稳定策略, 指出投资成本是促使所有企业投资信息安全的关键策略。

4 密码协议的博弈论分析

传统的密码协议都假定参与方或者诚实, 或者恶意。其中诚实的参与方在通信过程中总是遵守协议, 而邪恶的参与方总是使用各种手段欺诈其他参与方而违背协议。博弈论的观点认为所有参与方都是理性的, 即保证自身利益最大化。与此相反, 密码学中并不排斥非理性行为。

博弈论在密码协议中的应用主要体现在秘密共享和安全多方计算问题上。典型的秘密共享问题是指秘密份额被分发给参与者, 只有一定数量以上的参与者才能重构出秘密。安全多方计算问题中参与者只能接受自己的私密输入, 并不能从他人的输入中获得任何额外信息。安全多方计算与博弈论的比较如表 3 所示。

表 3 安全多方计算与博弈论的比较

	安全多方计算	博弈论
动机	在模型之外	博弈支付
参与方	完全诚实或恶意	理性
解决方案	安全协议	均衡
隐私	目标	工具
提前结束	可能	不会

使用博弈论分析安全多方计算问题需要引入理性参与者。在这一博弈形式中, 参与者的类型是其输入, 每个参与者试图猜测输出。他们都想得到正确的输出, 而不希望其他参与者得到正确输出。另外, 参与者也希望尽可能少地泄露自己的输入, 尽可能多地得到其他参与者的输入。这里要考虑两方面的问题^[22]。首先, 参与者依据自身利益报告真实输入, 需要描述这类非合作计算函数。其次, 需要考察在何等程度上现有的安全多方计算协议可以形成该扩展博弈的适当均衡。

国外文献方面, Dodis 和 Rabin^[22]对密码学和博弈论的区别及相互影响进行了详细的阐述。Katz^[23]就密码学在博弈论中的应用和博弈论在密码学中的应用分别进行了综述。Kol 和 Naor^[24]考虑了秘密共享和安全多方计算的公平协议问题, 其设计的协议可以进行任意轮迭代。Gossner 和 Tomala^[25]研究了非完美监控重复博弈下的秘密关联问题。Caballero-Gil 和 Hernandez-Goya^[26]使用博弈论设计了一个包含两个参与人的秘密协议, 以达到最大化保证诚实参与人利益的目的。国内文献方面, 田有亮等^[27]基于扩展式博弈建立安全协议模型, 通过分析博弈过程, 可以很好地预测各方的策略选择及其原因。在文献[28]中, 田有亮等分析了博弈论环境下的秘密分发机制和秘密重构机制, 但对局中人效用的刻画仍需要进一步研究。张国荣等^[29]改变传统安全求和方法中参与方行为良好的假定, 假定参与方可以自己选择诚实或共谋, 结果表明算法可以很好地保护隐私。罗喜召等^[30]尝试在理性密码学与传统博弈论之间建立联系, 证明了防范秘密攻击的两方安全计算是计算博弈中可忽略的调解人的通用实现。

5 基于博弈论的信息安全技术配置

企业使用信息安全技术抵御攻击者攻击, 而攻击者试图入侵企业获得资源或造成破坏。在这一相互作用的过程中, 如何选择安全技术的响应策略, 不同安全技术的配置之间如何相互影响, 可以使用博弈论进行评价。

目前这一方面的研究主要围绕入侵检测系统展开。关于入侵检测系统的博弈论分析可以归纳为图 1 的形式。

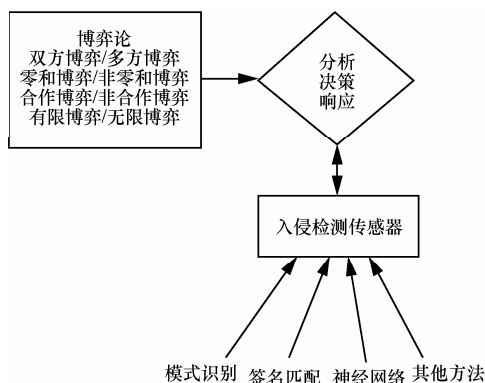


图1 入侵检测系统的博弈论分析

Alpcan 和 Bacsar 在文献[31]中给出了入侵检测博弈模型的一般形式。此模型为包含 N 个参与者的非合作非零和重复博弈，采用隐马尔可夫模型描述。定义参与者 i 的行动空间为 $A^i := \{a_1^i, a_2^i, \dots, a_{A_{\max}}^i\}$ 。 N 个参与者的行动状态为 $S^a := \{A^1 \times A^2 \times \dots \times A^N\}$ ，行动概率为 $X^a := [x_1^a, x_2^a, \dots, x_{A_{\max} \times N}^a]$ ，其中 $0 \leq x_i^a \leq 1$ ，并且 $\sum_{i=1}^{A_{\max} \times N} x_i^a = 1$ 。系统的状态为 $S = S^a \times S^e$ 。 S^e 为系统原来的状态，有 $S^e := \{s_1^e, s_2^e, \dots, s_{E_{\max}}^e\}$ ，在各个状态下的概率为 $X^e := [x_1^e, x_2^e, \dots, x_{E_{\max}}^e]$ 。因此系统状态的概率为 $X := [x^e, x^a]$ 。系统的状态转移方程为 $X(n+1) = MX(n)$ ，其中 M 为分块对角矩阵，有 $M := \text{diag}[M(x_1), M(x_2), \dots, M(x_{A_{\max} \times N})]$ 。每个参与者的成本不仅与其他参与者的行动有关，也与系统状态有关。定义参与者 i 的成本为 $c^i(s_j)$ ，其中 $s_j \in S$ 。假设参与者在博弈每一阶段都知道自己的成本但对系统状态 x^e 只有有限观测。假设参与者 i 的观测为 $y^i = O^i M(s_j^a)$ ，其中 O^i 为参与者 i 的观测矩阵， $s_j^a \in S^a$ 。

国外文献方面，Alpcan 等^[32]使用博弈论工具研究了带有传感器网络的分布式入侵检测系统。Zhu 等^[33]讨论了面对多重攻击下分布式入侵检测系统的配置问题。Agah 等^[34]使用二人零和非合作博弈和马尔可夫决策方法来研究传感器网络中的

入侵检测问题，实验证明该博弈框架能显著提高防御效率。Chen 等^[35]研究了异质网络下入侵检测系统中攻击者和防御者的最佳策略。国内文献方面，朱建明等^[36]对由防火墙、入侵检测系统、容忍入侵技术组成的安全体系结构进行了评价，重点分析了入侵检测系统的配置策略。夏子超等^[37]使用演化博弈论分析了入侵检测系统响应策略随时间的变化趋势，重点关注了用户和入侵检测系统策略的动态调整和状态的稳定性，但其实用性尚需要实验验证。赵柳榕等^[38]研究了虚拟专用网和入侵检测系统的信息安全技术组合与黑客的博弈均衡，结果表明配置 VPN 对降低 IDS 的误报率并不总是正相关。

也有学者对其他信息安全技术进行研究。比如，Liao 等^[39]研究了防火墙规则是否应该保持私密的问题。文中建立了如表 4 所示的模型。

管理员有 3 个策略，即不公开防火墙规则、公开真实规则和公开虚假规则。攻击者有两个策略，即攻击和不攻击。通过对纳什均衡的分析，文中指出在当今的互联网环境下保持防火墙规则私密已经不再适宜，提出带有虚假信息的公开防火墙规则优于私密的防火墙规则，并能在多重网络的情况下达到更大的社会最优。此外，在文献[40]中，周华等分析了攻击者和容忍入侵系统构成的二人零和博弈，全面分析了各个状态下的纳什均衡。但文中假设博弈主体是完全理性的，存在一定的主观性。

6 结束语

本文在充分总结现有文献的基础上，分别从网络安全攻防、密码协议设计、安全技术配置 3 个方面对网络空间安全的博弈论分析进行了综述。当前研究仍存在一些不足。总体来说，基于博弈论的网络空间安全问题研究起步较晚，目前的研究方法仍然不够系统。此外，现有文献普遍存在着一定的主观性。现实的安全环境极其复杂，

表 4

防火墙规则选取博弈模型

		管理员		
		不公开规则 (S_d^o)	真实规则 (S_d^T)	虚假规则 (S_d^F)
攻击者	攻击 (S_a^f)	$[\mu(S_a^f, S_d^o), \mu(S_a^f, S_d^o)]$	$[\mu(S_a^f, S_d^T), \mu(S_a^f, S_d^T)]$	$[\mu(S_a^f, S_d^F), \mu(S_a^f, S_d^F)]$
	不攻击 (S_a^o)	$[\mu(S_a^o, S_d^o), \mu(S_a^o, S_d^o)]$	$[\mu(S_a^o, S_d^T), \mu(S_a^o, S_d^T)]$	$[\mu(S_a^o, S_d^F), \mu(S_a^o, S_d^F)]$

攻击概率、风险损失等参数通常难以估计,加上当前形势下攻击手段越来越多样化,更给建模带来了难度。未来可以考虑以下几个研究方向:第一,将博弈论方法与其他方法结合,如马尔可夫决策方法等;第二,研究信息安全投资的网络拓扑影响,现实中企业之间可能存在复杂的网络拓扑关系,需要将这种影响考虑在内;第三,目前博弈论在密码学中的应用多数带来了更加复杂的网络协议,可以研究如何使用博弈论简化密码协议。

参考文献:

- [1] 冯登国,张敏,张妍,等. 云计算安全研究[J]. 软件学报, 2011,22(1):71-83.
FENG D G, ZHANG M, ZHANG Y, et al. Study of cloud computing security[J]. Journal of Software, 2011, 22(1): 71-83.
- [2] ANDERSON R. Why information security is hard-an economic perspective[EB/OL]. <http://www.acsac.org/2001/papers/110.pdf>.
- [3] 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): 817-827.
JIANG W, FANG B X, TIAN Z H, et al. The testing of network security and the optimal active defense based on offensive and defensive game model[J]. Chinese Journal of Computers, 2009, 32(4): 817-827.
- [4] HARRINGTON P D. Using noncooperative potential games to improve network security[D]. Stillwater: Oklahoma State University, 2010.
- [5] JEANNETTE K W, WING J. Game strategies in network security[J]. International Journal of Information Security, 2005, 4(1-2): 71-86.
- [6] MANSHAEI M H, ZHU Q, ALPCAN T, et al. Game theory meets network security and privacy[J]. ACM Computing Surveys, 2012, 45(3):533-545.
- [7] VARIAN H. System reliability and free riding[J]. Economics of Information Security Kluwer -, 2004, 2(5799):1-15.
- [8] GROSSKLAGS J, CHRISTIN N, CHUANG J. Secure or insecure?: a game-theoretic analysis of information security games[C]//Proceedings of the 17th International Conference on World Wide Web, Beijing, 2008:209-218.
- [9] GROSSKLAGS J, JOHNSON B, CHRISTIN N. The price of uncertainty in security games[M]//Economics of Information Security & Privacy. Berlin Heidelberg: Springer, 2010: 9-32.
- [10] GROSSKLAGS J, RADOSAVAC S, CARDENAS A A, et al. Nudge: intermediaries' role in interdependent network security[J]. Lecture Notes in Computer Science, 2010, 6101: 323-336.
- [11] PAL R, HUI P. Modeling internet security investments: tackling topological information uncertainty[M]//Decision and Game Theory for Security. Berlin Heidelberg: Springer, 2011: 239-257.
- [12] NEYYAN R, PAUL A, DESHWAL M, et al. Game theory based defense mechanism against flooding attack using puzzle[J]. Emerging Trends in Computer Science & Information Technology Etcit, 2012 (2): 35-40.
- [13] CARROLL T E, GROSU D. A game theoretic investigation of deception in network security[C]//Proceedings of 18th International Conference on Computer Communications and Networks. 2009: 1-6.
- [14] 孙薇,何德全,孔祥维,等. 运用博弈论探讨信息安全问题[J]. 科技管理研究, 2009, 29(1):233-235.
SUN W, HE D Q, KONG X W, et al. Discussing the information security problems by using game theory[J]. Science and Technology Management Research, 2009, 29(1): 233-235.
- [15] 刘建波. 一种基于攻防成本博弈的防御策略评价模型[J]. 计算机技术与发展, 2011, 21(10):229-232.
LIU J B. A evaluation model of defending strategies based on attack-defense cost game[J]. Computer Technology and Development, 2011, 21(10): 229-232.
- [16] KUNREUTHER H, HEAL G. Interdependent security[J]. Journal of Risk & Uncertainty, 2003, 26(2-3):231-249.
- [17] LASZKA A, FELEGYHAZI M, BUTTYAN L. A survey of interdependent information security games[J]. ACM Computing Surveys, 2014, 47(2).
- [18] JOHNSON B, GROSSKLAGS J, CHRISTINA N, et al. Uncertainty in interdependent security games[J]. Decision Game Theory for Security, 2010, 6442: 234-244.
- [19] 吕俊杰,邱苑华,王元卓. 基于相互依赖性的信息安全投资博弈[J]. 中国管理科学, 2006, 14(3):7-12.
LV J J, QIU W H, WANG Y Z. The information security investment games based on interdependency[J]. Chinese Journal of Management Science, 2006, 14(3):7-12.
- [20] 吕俊杰,邱苑华,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.
LV J J, QIU W H, WANG Y Z. Network security investment externality and game strategies[J]. Journal of Beijing University of Aeronautics and Astronautics, 2006, 32(12): 1499-1502.
- [21] 孙薇,孔祥维,何德全,等. 基于演化博弈论的信息安全攻防问题研究[J]. 情报科学, 2008 (9):1408-1412.
SUN W, KONG X W, HE D Q, et al. Study of information security attack and defend based on evolutionary game theory[J]. Information Science, 2008 (9): 1408-1412.
- [22] DODIS Y, RABIN T. Cryptography and game theory[J]. Algorithmic Game Theory, 2007(1).
- [23] KATZ J. Bridging game theory and cryptography: recent results and future directions[M]//Theory of Cryptography. Berlin Heidelberg: Springer, 2008: 251-272.
- [24] KOL G, NAOR M. Cryptography and game theory: designing protocols for exchanging information[M]//Theory of Cryptography. Berlin Heidelberg: Springer, 2008: 320-339.
- [25] GOSSNER O, TOMALA T. Secret correlation in repeated games with imperfect monitoring[J]. Mathematics of Operations Research, 2007, 32(2):413-424.
- [26] CABALLERO G P, HERNANDEZ G C, BRUNO C C. A game-theoretic model for two-party cryptographic protocols[C]//International Conference on Information Technology: Coding & Computing. 2004: 773-777.
- [27] 田有亮,彭长根,马建峰,等. 安全协议的博弈论机制[J]. 计算机研究与发展, 2014, 51(2):344-352.
TIAN Y L, PENG C G, MA J F, et al. The game mechanism of security protocol[J]. Computer Research and Development, 2014,

- 51(2): 344-352.
- [28] 田有亮, 马建峰, 彭长根, 等. 秘密共享体制的博弈论分析[J]. 电子学报, 2011, 39(12): 2790-2795.
TIAN Y L, MA J F, PENG C G, et al. The game theory analysis of secret sharing schemes[J]. Acta Electronic Silica, 2011, 39(12): 2790-2795.
- [29] 张国荣, 印鉴. 基于博弈论的安全多方求和方法[J]. 计算机应用研究, 2009, 26(4):1497-1499.
ZHANG G R, YIN J. The methods of secure sum based on game theory[J]. Application Research of Computers, 2009, 26(4): 1497-1499.
- [30] 罗喜召, 钱陪德, 朱艳琴, 等. 防范秘密攻击的安全计算的博弈论实现[J]. 南京航空航天大学学报, 2012, 44(1):70-74.
LUO X Z, QIAN P D, ZHU Y Q, et al. The game theory realization of security computing in prevent secret attacks [J]. Journal of Nanjing University of Aeronautics and Astronautics, 2012, 41(1): 70-74.
- [31] ALPCAN T, BACSAR T. An intrusion detection game with limited observations[J]. Proceedings of Int.symp.on Dynamic Games & Applications Sophia Antipolis, 2006, 8137:222-232.
- [32] ALPCAN T, BASAR, TAMER. A game theoretic approach to decision and analysis in network intrusion detection[C]//Proceedings of the 42nd IEEE Conference on Decision and Control, Maui, HI. 2003:2595-2600.
- [33] ZHU Q, TEMBINE H, BASAR T. Network security configurations: A nonzero-sum stochastic game approach[C]//Proceedings of the American Control Conference. 2010: 1059-1064.
- [34] AGAH A, DAS S K, BASU K, et al. Intrusion detection in sensor networks: a non-cooperative game approach[C]//The 3rd IEEE International Symposium on Network Computing and Applications. 2004:343-346.
- [35] CHEN L, LENEUTRE J. A Game theoretical framework on intrusion detection in heterogeneous networks[J]. IEEE Transactions on Information Forensics & Security, 2009, 4(2):165-178.
- [36] 朱建明, RAGHUNATHAN S. 基于博弈论的信息安全技术评价模型[J]. 计算机学报, 2009, 32(4):828-834.
ZHU J M, RAGHUNATHAN S. The evaluation model of information security based on game theory[J]. Chinese Journal of Computers, 2009, 32(4): 828-834.
- [37] 夏子超, 银鹰, 陈晓桦. 入侵检测系统响应策略的进化博弈论分析[J]. 微计算机信息, 2009 (33):60-61.
XIA Z C, YIN Y, CHEN X H. The evolutionary game theory analysis of intrusion detection system response strategy[J]. Microcomputer Information, 2009 (33): 60-61.
- [38] 赵柳榕, 梅姝娥, 仲伟俊. 虚拟专用网和入侵检测系统最优配置策略的博弈分析[J]. 管理工程学报, 2014, 28(4).
ZHAO L R, MEI S E, ZHONG W J. The game theory analysis of virtual private network and the optimal allocation of intrusion detection system[J]. Journal of Industrial Engineering and Engineering Management, 2014, 28(4).
- [39] LIAO Q, LI Z, STRIEGEL A. Could firewall rules be public-a game theoretical perspective[J]. Security & Communication Networks, 2012, 5(2):197-210.
- [40] 周华, 周海军, 马建峰. 基于博弈论的入侵容忍系统安全性分析模型[J]. 电子与信息学报, 2013(8):1933-1939.
ZHOU H, ZHOU H J, MA J F. Safety analysis model of intrusion tolerance system based on game theory[J]. Journal of Electronics Information Technology, 2013(8): 1933-1939.

作者简介:



朱建明 (1965-), 男, 山西太原人, 博士, 中央财经大学教授, 博士生导师, 主要研究方向为信息安全、信息系统安全。



王秦 (1990-), 男, 甘肃天水人, 中央财经大学博士生, 主要研究方向为信息安全经济学。