“十二五”科学技术专著丛书

博弈论与信息安全

朱建明 田有亮 等著

BOYILUN YU
XINXI ANQUAN

北京邮电大学出版社
www.buptpress.com

“十二五”科学技术专著丛书

博弈论与信息安全

朱建明　田有亮　等著

北京邮电大学出版社
www. buptpress. com

内 容 简 介

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普及，网络犯罪、黑客攻击、泄露个人隐私等信息安全方面的问题对我们的工作、生活和学习的影响越来越大，提高全社会的信息安全意识和信息安全保障能力成为我们当前的一个重要任务。信息安全不仅是技术问题而且还是管理问题，信息安全是典型的攻击与防御的博弈，《博弈论与信息安全》汇集了近年来基于博弈论研究信息安全的最新成果。本书共10章，从博弈论基础开始，系统介绍了信息安全博弈模型、安全通信协议博弈机制、秘密共享体制的博弈论分析、信息安全的可用性与隐私保护的博弈分析以及社交网络的博弈分析等。本书从新的角度对信息安全理论与方法进行了研究，相关研究成果对于制定正确的信息安全策略，提高信息安全保障能力具有重要的参考价值。

本书适用于信息安全相关专业的本科生和研究生学习，也适用于从事信息安全相关工作的管理人员和技术人员学习和参考。

图书在版编目（CIP）数据

博弈论与信息安全 / 朱建明，田有亮等著 .-- 北京 ：北京邮电大学出版社，2015.7
ISBN 978-7-5635-4413-4
Ⅰ. ①博… Ⅱ. ①朱…②田… Ⅲ. ①博弈论－应用－信息安全－安全技术 Ⅳ. ①TP309
中国版本图书馆 CIP 数据核字（2015）第 155918 号

书　　名：博弈论与信息安全
著作责任者：朱建明　田有亮 等著
责 任 编 辑：刘　颖
出 版 发 行：北京邮电大学出版社
社　　址：北京市海淀区西土城路 10 号（邮编：100876）
发 行 部：电话：010-62282185　传真：010-62283578
E-mail：publish@bupt.edu.cn
经　　销：各地新华书店
印　　刷：北京九州迅驰传媒文化有限公司
开　　本：787 mm×1 092 mm　1/16
印　　张：14.5
字　　数：315 千字
版　　次：2015 年 7 月第 1 版　2015 年 7 月第 1 次印刷

ISBN 978-7-5635-4413-4　　定　价：36.00 元

序

随着社会信息化水平的提高和电子商务与电子政务的普及，计算机网络与信息系统的全局性和基础性日益加强，“互联网＋”行动计划将进一步推动互联网应用创新。与此同时，信息安全问题引起全世界的高度关注，“没有网络安全就没有国家安全，没有信息化就没有现代化”已经成为当前全社会的共识。2014 年中央网络安全与信息化领导小组的成立将信息安全的重要性提高到空前的战略高度。然而，当前的信息安全问题不容乐观，信息安全事件屡见不鲜，信息安全攻击手段日新月异，攻击方法层出不穷，信息安全威胁无处不在。如此严峻的信息安全现状正在给全球用户带来前所未有的挑战，成为当前世界性难题。尽管如此，无论是信息安全事件、攻击手段和方法，还是信息安全威胁，归根到底还是作为决策主体的“人”在其中起到至关重要和无可替代的作用。人作为决策主体，其自利行为和个体偏好将直接影响到各类信息安全事件的结局和安全威胁的程度。

博弈论是应用数学的一个分支，它是在对抗环境下做出有效决策的分析工具，特别是在具有多位参与者的复杂敌对环境下更加有效。博弈论已被广泛应用于经济学、政治学、军事科学、生物学、计算机科学等学科的各个研究领域。博弈理论和方法的应用扩展了这些学科的分析视野，拓展了其研究内容。信息安全是一门多学科交叉融合的学科领域，为实现信息的机密性、完整性、不可否认性、可用性等目标，研究内容涉及信息安全理论、安全技术、安全管理、安全标准、安全策略、安全测评、安全监控及用户隐私等。对这些信息安全问题的研究，归根到底可视为如何平衡信息安全领域其“安全性”和“效率”这个天平，如何有效解决在各种应用中的各类安全问题与其系统、算法的效率的平衡问题。博弈论为解决这类信息安全问题提供了新的思想和方法，我想这也可能是近几年来信息安全经济学作为一门新兴学科得到快速发展的主要原因之一。

本书作者长期研究信息安全，并将研究内容融入到信息安全与博弈论交叉科学问题的探索中。本书不仅在信息安全与博弈论交叉领域的理论方面有所突破，而且通过博弈理论和方法，对信息安全、安全通信协议、秘密共享、隐私保护、数据挖掘、信息安全投资、社交网络、网络舆情等方面进行一系列建模和实验验证。本书内容包含该领域国内外最新研究进展，系统阐述了信息安全与博弈论交叉领域理论及应用发展，将对我国信息安全交叉学科和信息安全经济学的研究起到积极的推动作用。

西安电子科技大学教授　马建峰

2015 年 5 月 26 日

前　言

当今世界，信息已经成为一种重要的战略资源，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。由于以开放式、分布式、异构性和移动计算等为主要特征的网络信息系统承载着巨大的数据和信息资源，提供着难以估量的网上信息服务、软件应用和业务处理，信息系统的一次故障或事故往往会造成巨大的影响，甚至是灾难。

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，日趋庞大的软件系统愈来愈脆弱。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。

在信息安全研究领域，普遍的观点认为，信息安全要靠信息安全技术，假设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的技术，那么信息安全问题就可以解决。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”。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。

博弈论(Game Theory)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引起了学术界的重视。信息安全是一种典型防御与攻击的博弈，而且属于不完全信息的非合作的动态博弈。

博弈论是在系统资源范围内实现安全最大化的一种方法，是研究决策者行为对他人影响的理论。一个博弈由参与方(player)、信息(information)、

行动(action)、效用(utilitie)等组成。参与方是博弈中做出决策和采取行动的个体。在安全博弈中,将网络中的计算机定义为结点,这些结点是安全博弈的参与方。信息是指参与方有关博弈的知识,其中包括可以采取什么行动和不能采取什么行动的约束。这些变量作为参与方效用函数的输入,是由参与方对可能采取行动的偏好决定的。偏好使参与方选择最佳值分配给博弈变量并在每一轮博弈中最大化其效用函数。行动的计划就是策略(strategy)。

本书系统介绍了博弈论在信息安全中的应用,重点研究了信息安全的博弈模型,设计了安全协议的博弈模型,可用性、可信性与隐私保护的博弈模型,并进行了隐私保护分布式数据挖掘的博弈分析、信息安全投资的博弈分析、社交网络用户隐私保护和网络舆情的博弈分析。本书所研究的理论与方法对于确定安全策略,更好地发挥安全技术的作用具有重要的理论意义和应用价值。

本书是作者在近年来研究成果的基础上完成的,朱建明和田有亮统筹全书,第1章由朱建明教授、王秦博士撰写,第2章、第4章、第5章由田有亮副教授撰写,第3章由高博博士撰写,第6章由高胜博士撰写,第7章由葛新景博士撰写,第8章由刘文臣博士撰写,第9章由黄启发博士撰写,第10章由宋彪博士撰写,王秦博士对全书进行了修订和校对。我国著名信息安全专家,西安电子科技大学马建峰教授为本书作序。

本书的出版得到国家自然科学基金项目(项目编号:61272398)和中央财经大学第一批青年科研创新团队支持计划资助。

在本书的出版过程中,著名经济学家、博弈论大师、诺贝尔奖得主约翰·纳什遇车祸去世。谨以本书的出版纪念这位大师!

目　录

第1章 概 述

本章学习要点：

- 信息安全现状；
- 信息安全与博弈论；
- 博弈论与密码学。

1.1 信息安全概述

近年来，计算机网络的发展为社会生活的各个方面带来了巨大的变化。互联网实现了计算机之间的互联，万维网(Web)实现了信息的互联，物联网则是物的互联，社会网络(Social Network)是人的互联，计算机网络将社会生活的各个方面更加紧密地联系在一起，我们正步入万物互联(Internet of Everything，IoE)的时代。当今世界，信息已经成为一种重要的战略资源，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。2015 年 2 月中国互联网络信息中心(CNNIC)发布的第 35 次《中国互联网络发展状况统计报告》显示，截至 2014 年 12 月，我国网民规模达 6.49 亿，互联网普及率为 47.9%。我国手机网民规模达 5.57 亿，比 2013 年年底增加了 5 672 万人。互联网发展从“广”到“深”，网民生活全面“网络化”。这些数据说明网络对社会的影响越来越大，与此同时，在日常工作和生活中，人们也越来越依赖计算机网络，越来越多地使用各种信息系统来处理敏感数据。IDC 在 2006 年估计全世界产生的数据量是 0.18 ZB，而 2011 年这个数字已经提升为 2006 年的 10 倍，达到 1.8 ZB，差不多对应全世界每个人一块一百多 GB 的硬盘，预计到 2020 年全球数据总量将超过 40 ZB(相当于 4 万亿 GB)，这一数据量是 2011 年的 22 倍。以开放式、分布式、异构性等为主要特征的网络信息系统承载着巨大的数据和信息资源，提供着难以估量的网上信息服务、软件应用和业务服务。因此，网络信息系统的一次故障或事故可能会造成巨大的影响，甚至是灾难。

从当前网络应用软件系统的发展趋势来看，应用需求越来越多，复杂度越来越高，可用性要求越来越强，日趋庞大的软件系统却越来越脆弱。与此同时，现代企业运行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(System of Systems，SoS)，造成信息系统的规模不断扩大，复杂性不断增加。另一

方面，现代信息技术使系统之间的连接更加容易，扩大了系统的边界，但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挑战。

1.1.1 信息安全问题的根源

信息安全是全世界都在关注的重要问题。在许多应用领域，有限的信息安全资源阻碍了安全机制对所有保护目标的全时段覆盖。因此，如何将有限的信息安全资源的保护作用发挥到最大成为一个值得研究的问题。

信息安全主要包括以下 4 个方面[1]：设备安全、数据安全、内容安全和行为安全。信息系统硬件结构的安全和操作系统的安全是信息系统安全的基础，密码、网络安全等技术是关键技术。只有从信息系统的硬件和软件的底层采取安全措施，从整体上采取措施，才能比较有效地确保信息系统的安全。

当前，信息安全问题的根源主要有 3 个方面：

第一，计算机与 Internet 相连，是当前信息安全问题的主要根源。Internet 具有国际化、社会化、开放化和个人化的特点。网络的发展把计算机变成网络中的一个组成部分，在连接上突破了机房的地理隔离，信息的交互扩大到了整个网络[1]。由于 Internet 网络缺少足够的安全设计，再加上网络技术的开放性和标准化，与 Internet 相连的计算机可能受到来自 Internet 上的任何一个机器的攻击。特别是全球信息化飞速发展，信息系统已经成为国家关键基础设施，社会对计算机网络的依赖日益增强。人类的生活越来越离不开互联网，人们可以自由地访问网络，自由地使用和发布各种类型的信息，但同时也面临着来自网络的安全威胁。

第二，微机的安全结构过于简单，操作系统存在安全缺陷。微机也称为个人计算机，是个人使用的计算机，而不是公用的计算机。与大型机、小型机相比，为了降低成本，个人计算机去掉了许多被认为是不必需的安全机制，如存储器的隔离保护机制、程序安全保护机制等。于是，在微机上执行程序可以不经过认证，程序可被随意修改，系统区域的数据可以随意修改，这样，病毒、蠕虫、木马等恶意程序就乘机泛滥了。另一方面，操作系统存在安全缺陷。操作系统是计算机最主要的系统软件，是信息安全的基础。由于操作系统越来越复杂，越来越庞大，致使操作系统不可能做到完全正确。操作系统的缺陷成为计算机的重要威胁。目前广泛使用的智能手机、平板电脑等设备的安全结构和操作系统更加简单，其安全威胁也更为突出。

第三，各种信息系统中所处理的信息越来越重要。由于信息是重要的战略资源，

各种计算机系统集中管理着国家和企业的政治、军事、经济等重要信息。特别是电子商务和电子政务的发展，在日常工作和生活中，人们越来越依赖信息系统，越来越多地通过信息系统管理企业的产、供、销、人、财、物，越来越多地使用计算机网络来传递敏感信息。因此计算机系统成为不法分子的主要攻击目标。

因此，信息安全问题的根源就是：**自身缺陷＋开放性＋黑客攻击**。

1.1.2 信息安全管理

近年来，信息安全理论与技术发展很快，从传统的加密解密、杀毒软件、防火墙、入侵检测发展到容忍入侵、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。

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的技术，信息安全问题就可以解决[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，明天攻击者可能又会找到一个新的漏洞。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依靠先进的技术，还需要从策略、管理、机制的角度提高信息安全的能力，而信息安全是包括技术、管理、法律在内的系统工程。

信息安全不仅仅是技术问题，也是管理问题。信息安全需要有专门的管理机构制定信息安全策略，要有法律法规做保障，要有经费的投入。另一方面信息安全机制会影响用户的方便性，会影响系统运行的性能，还需要投入经费成本和时间成本。所以信息安全是一个综合问题，需要从整体上进行规划和处理。

对于信息安全策略而言，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，甚至所付出的代价是得不偿失的，理性的欺诈者可能就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。

1.2 信息安全与博弈论

1944 年，冯·诺依曼和摩根斯坦所著的《对策论与经济行为》出版，标志着博弈论(Game Theory)诞生。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。在博弈论中，博弈是指利益存在冲突的决策主体在相互对抗(或合作)中，双方(或多方)相互依存的一系列策略和行动的过程集合。其中，对决策主体即人的基本假定是：人是理性的(rational)，理性的人是指他在具体策略选择时的目的是使自己的利益最大化，博弈论研究的正是理性的人之间是如何进行策略选择的。博弈论已经成为经济学的标准分析工具之一，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。在研究理性博弈参与人的行为策略方面，博弈论模型在许多领域都有成功应用。纳什均衡策略是理性博弈的最优策略，当防御者总是采取纳什均衡策略时，攻击者也只有采取相应的纳什均衡策略才能取得最大的攻击效用。网络攻防博弈模型将研究重点从具体攻击行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，从而更加有效地提高信息安全技术具有重要意义。

博弈论将实体间的相互操作看作是一个博弈，每个博弈参与者依据系统设计者事先定义好的规则选择策略并进行操作，在博弈结束时获得一定收益。博弈可以分为静态博弈和动态博弈，静态博弈指所有博弈者同时进行策略选择，动态博弈指博弈者的操作具有先后之分，重复博弈也是动态博弈的一种。博弈也可以分为完全信息博弈和非完全信息博弈，其中完全信息博弈指全体博弈者在进行策略选择时完全知道有关做出决定的所有信息，非完全信息博弈则相反，可能需要依凭一定的概率假设进行操作。博奕还可以分为非合作博弈与合作博弈，在非合作博弈中，实体用户之间没有签约协议或存在协作，在合作博弈中，实体间先协同获得最大的团体利益，再将团体利益分配到每个个体实体，在利益分配时会涉及公平性和团体稳定性等问题。当前研究中较多采用非合作博弈，从合作博弈的角度出发的研究并不太多。

在实体具有的信息和理性基础上，实体对博弈进行预测并实际选择策略，最终达到一种相互制约的结果均衡状态，该结果即博弈问题的解。博弈论研究的中心问题是寻找可能的解并研究其特性。对于非合作博弈论中的完全信息静态博弈，研究的最多的结果均衡态包括占优均衡和纳什均衡。占优均衡指每个人的选择策略都是占优策略而形成的一种均衡，占优策略是指不管他人选择何种策略，博弈者都有一个最大化自己收益的最佳策略，纳什均衡是指当其他博弈者的策略不变时，单方改变自己的策略时不能增加自己的收益。占优均衡一定是纳什均衡，反之则不一定。相对于最简单基础的完全信息静态博弈，其他类型博弈的解都在纳什均衡的基础上进行了改进，如完全信息动态博弈主要研究子博弈精炼纳什均衡，不完全信息静态博弈主要研究贝叶斯纳什均衡，不完全信息动态博弈研究精炼贝叶斯纳什均衡。对于合作博弈论而言，解指参与合作的博弈者最终分配得到的支付。合作博弈论从合作团体稳定性、公平性等角度提出不同的解，有稳定集(Stable Set)、核心(Core)、Shapley 值、核(Kernel)及核仁(Nucleolus)等。

近年来，有关博弈论与信息安全的研究越来越引起学术界的兴趣，越来越多的专著、期刊、会议论文使用了博弈论工具来研究网络安全问题。作为一类特殊的博弈，安全博弈研究攻击者和防御者间的博弈问题。安全博弈及其解决方案被作为正式的决策制定、算法研究以及攻击者行为预测的基础。所采用的博弈模型取决于决策者可获得的信息类型，及其行为空间和目标，安全博弈包含了从简单的确定性博弈到更加复杂的随机和有限信息博弈之间的很多种类，并且适用于一系列领域的安全问题，如入侵检测和无线网络中的密码学等。

物理层及 MAC 层、自组织网络、入侵检测系统、匿名与隐私、网络安全经济学、密码学中的安全问题是使用博弈论方法分析的网络安全问题的几个著名领域。实践中，所有这些问题包含了多个层面上的决策问题，例如高层的隐私和加密问题，物理层安全问题和信息安全管理问题。

1.2.1　物理层的安全问题

物理层的安全是通信网络中的一个重要的安全问题。物理层中的通信信道可能会遭受干扰和窃听攻击。虽然这些攻击对有线网络和无线网络都是威胁，但相对来说它们对无线网络的威胁更大。图 1.1 描述了无线网络中这样的攻击行为。

窃听是一种被动攻击，通常采用加密来预防这种攻击。而干扰是一种主动攻击，典型防御方案是扩频和跳频技术，或者是两者的组合。通过将攻击者与一个特定的效用函数相联系，可以对其恶意行为建模。效用函数代表了以防御者效用降低为代价的攻击者的收益。在物理层，合法用户和攻击者之间的交互经常使用零和博弈来建模，以刻画他们相互冲突的目标。