复杂网络环境下访问控制技术

李凤华 熊金波◎著

Access Control Technology for Complex Network Environment

中国工信出版集团
人民邮电出版社
POSTS & TELECOM PRESS

复杂网络环境下访问控制技术

李凤华 熊金波◎著

Access Control Technology for Complex Network Environment

人民邮电出版社
北京

图书在版编目（CIP）数据

复杂网络环境下访问控制技术 / 李凤华，熊金波著
. -- 北京 : 人民邮电出版社，2015.12
ISBN 978-7-115-39475-0

Ⅰ. ①复… Ⅱ. ①李… ②熊… Ⅲ. ①访问控制－研究 Ⅳ. ①TP309

中国版本图书馆CIP数据核字(2015)第117612号

内 容 提 要

随着通信技术、网络技术和信息技术的快速发展与广泛应用，形成了包含移动互联网、云计算、物联网和大数据等具有开放性、移动性、异构性、多安全域并存等诸多特性的复杂网络环境。在该环境中，通过“网络之网络”访问“系统之系统”已经成为信息化发展的必然趋势，并持续不断地孕育和催生出诸多新型信息传播方式和信息服务模式，将人类生活带进“万物互联、智慧互通”的新时代。本书在梳理信息技术发展历程的基础上，以访问控制技术为核心，系统地阐述了复杂网络环境下访问控制的模型、技术及应用实例。全书共分为 7 章，主要内容包括：信息技术发展历程与信息传播、访问控制模型研究进展、基于行为的访问控制、面向云计算的访问控制、权限可伸缩的访问控制、访问控制应用研究、面向网络空间的访问控制技术发展趋势。

本书适合复杂信息系统的研发人员学习，也可作为网络空间安全、信息安全、计算机科学与技术等相关专业研究生指导用书，还可作为相关学科研究人员的参考用书。

◆ 著　　李凤华　熊金波
责任编辑　邢建春
执行编辑　肇　丽
责任印制　彭志环

◆ 人民邮电出版社出版发行　　北京市丰台区成寿寺路 11 号
邮编　100164　　电子邮件　315@ptpress.com.cn
网址　http://www.ptpress.com.cn
固安县铭成印刷有限公司印刷

◆ 开本：700×1000　1/16
印张：17.5　　2015 年 12 月第 1 版
字数：284 千字　　2015 年 12 月河北第 1 次印刷

定价：76.00 元

读者服务热线：(010)81055488　印装质量热线：(010)81055316
反盗版热线：(010)81055315

序

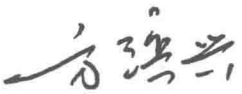
伴随着信息技术的飞速发展，访问控制模型与技术自 20 世纪 70 年代至今已走过近半个世纪，经历了从无到有、由简到繁、从理论到实践的巨大变革。访问控制是信息安全的核心技术之一，通过制定有效的访问控制策略，使合法用户在限定时间内获得有效的系统访问权限，对系统的资源进行授权访问。

早期的访问控制技术旨在实现大型主机上共享数据的授权访问，先后出现了自主访问控制模型和强制访问控制模型。随着信息技术的进一步发展，以及互联网、移动互联网等技术的崛起，访问控制模型与技术也在不断演进。面对爆炸式增长的各类信息系统，形成了一系列具有代表性的访问控制模型，包括基于角色的访问控制模型、基于任务的访问控制模型、面向分布式和跨域的访问控制模型、时空关联的访问控制模型、基于安全属性的访问控制模型、基于行为的访问控制模型等。然而，上述模型存在信任域单一、信息资源的所有权与管理权集中控制、对不同应用的自适应能力较差等诸多问题。云计算技术的出现使得上述问题更加突显，传统基于策略管理的访问控制模型不能适应各种随机、跨单位、跨安全域、跨信息系统的信息访问模式。为此，基于密码算法的访问控制模型应运而生，先后出现了基于时间、身份、属性等加密算法的访问控制模型。

近年来，移动互联网、物联网、云计算、大数据等技术相互融合与交织发展，使社交网络、搜索等新型信息传播方式不断打破传统有界系统和网络的边界，将无穷多个有界系统和网络随机动态组合，为人们呈现出了一个“无界”的泛在网络，“信息跨网行，交互跨域间”的时代已经来临。本书作者针对泛在网络中数据所有权与管理权分离、时空特性与访问授权具有高度动态性且均与数据的流动紧密关联等问题，致力于研究并实现以访问授权高度动态性和访问策略自适应性为主要特征的新型访问控制模型和技术，对推进访问控制模型及其相关技术的同步发展，具有很强的理论研究和实际应用价值。

本书作者长期从事访问控制方面的理论研究与应用开发，针对不同信息服务模式

和应用场景提出了一系列新型访问控制模型，已运用于数据库等相关产品中，取得了良好的效果，并获得了相关科研奖项。本书对访问控制模型及相关技术做了系统的梳理与论述，对访问控制模型与技术的发展趋势进行了展望，并指出了未来演化发展方向，对访问控制研究工作具有指导意义。

中国工程院院士 

前言

随着通信技术、网络技术和信息技术的持续快速发展和应用的广泛普及，形成了包含移动互联网、云计算和物联网等具有开放性、异构性、移动性、动态性、多安全域并存等诸多特性的复杂网络环境。在复杂网络环境中，通过“网络之网络（NoN，network of network）”访问“系统之系统（SoS，system of system）”已经成为信息化发展的必然趋势，并持续不断地孕育和催生出新的信息传播方式和信息服务模式，将人类生活带进“万物互联、智慧互通”的新时代，信息的获取和利用已经或者即将达到“信息随心行、交互在指间”的理想境界。在这种新的信息传播方式和服务模式下，信息资源、服务等面临着新的安全需求和挑战，网络空间安全被提升到国家安全战略层面。

访问控制作为一种核心的信息安全技术，能够保证复杂网络环境下的资源和服务被合法用户使用，同时防止被非法用户窃取和滥用。本书以复杂网络环境下的应用需求、访问控制模型、访问控制相关技术、应用实例等研究为主线，结合作者多年的科研实践经验，从理论模型到实际应用，系统阐述了面向复杂网络环境的访问控制相关理论与技术。在复杂网络环境中访问信息资源时，人们所处的环境状态与时间状态、采用的终端设备、从何处接入、经由的网络、要访问的信息资源及其安全属性等因素对访问权限所产生的影响是传统的访问控制模型无法处理的，需要新的访问控制模型，自适应调节“谁、何时、使用何设备、从何处接入网络、经由何网络、访问何资源、对资源做何处理、数据保存多长时间”8 个维度的相关因素，实现随时随地安全访问无处不在的信息资源，真正达到“信息随心行、交互在指间”的理想境界。

全书共 7 章，主要内容如下。

第 1 章为绪论，站在信息技术与信息传播的角度，系统总结了计算机硬件、操作系统、数据库系统和计算机网络等技术的演化发展历程，并对计算机网络发展的不同阶段进行了详细分析，归纳了不同阶段的特征，揭示了不同阶段信息传播的本质。

第 2 章概述了访问控制模型研究进展，包括面向主机的访问控制、面向组织形态确定的访问控制、面向分布式协同的访问控制、权限可伸缩的访问控制、面向社交网

络的访问控制、面向云计算的访问控制等模型及相关技术的研究现状与发展趋势。

第 3 章论述了基于行为的访问控制，在综合考虑环境、时态、角色的基础上定义行为的概念，阐述了基于行为的访问控制模型及其管理模型，并引入多级安全模型，结合基于行为的访问控制模型，论述了基于行为的多级安全访问控制模型，为后续研究提供了理论基础和方法。

第 4 章阐述了面向云计算的访问控制，包括云计算环境下访问控制应用场景分析、相关密码学基础，系统阐述了基于密码算法的数据安全创建、轻量级访问控制与可信删除等访问控制方案，包括系统模型、安全模型、系统描述、算法描述、综合分析与相关安全性证明等部分。

第 5 章论述了权限可伸缩的访问控制，包括面向多维数字媒体的访问控制与面向结构化文档的访问控制，从系统模型及权限描述、模型构建与形式化、结构化文档多级安全描述方法、基于行为的结构化文档访问控制、原型系统设计与实现机制等方面进行了系统阐述。

第 6 章阐述了访问控制应用研究，针对协作信息系统、Web 服务、数据库管理系统等典型应用中访问控制所面临的挑战，结合基于行为的访问控制技术，系统介绍了面向协作信息系统、Web 服务与数据库管理系统等的访问控制模型与相关机制的具体实施方法。

第 7 章以信息传播方式的演化为主线，总结了访问控制技术的发展进程，剖析了网络空间中信息传播方式与信息服务模式的演进规律，论述了现有访问控制模型的不足，从 8 个维度展望了面向网络空间的访问控制技术发展趋势。

本书内容系统且新颖，从计算机网络与信息传播方式的发展，到新的信息传播方式与信息服务模式对访问控制提出的新需求和新挑战，再到各种访问控制模型及其实施，并从理论方法到关键技术再到实用系统，全面阐述了复杂网络环境的访问控制内涵。本书所介绍的部分内容超越当前技术，具有新颖性。例如，面向网络空间的新型访问控制模型已综合考虑访问请求实体、广义时态、接入点、资源、访问设备、网络、网络交互图、网络传播链、资源传播链、场景约束等因素，能够灵活地包含传统的 DAC、MAC、RBAC、ABAC 等模型，可实现网络空间中细粒度、多层次、灵活的数据共享的访问控制，具有灵活性和可扩展性，可进一步完善以适应未来信息传播方式与信息服务模式的新发展。

本书主要由李凤华研究员、熊金波副教授完成，是李凤华研究员团队多年来在访问控制方面的研究成果。除封面署名作者以外，还包括苏铓博士，王彦超、谢绒娜、单芳芳博士研究生。在编写过程中得到团队牛犇、张恩等博士，何媛媛、华佳烽、孙哲、王新宇等博士研究生，李宁、李勇俊、李子孚、熊芳欣等硕士研究生的协助，他们做了大量的细致工作，在此表示衷心感谢！感谢人民邮电出版社的大力支持，对为本书出版的所有相关人员的辛勤工作表示感谢！

本书的出版得到国家自然科学基金项目（61170251）、国家高技术研究发展计划（863 计划）项目（2012AA013102）、教育部科学技术研究重点项目（209156）、北京市自然科学基金项目（4102056）的支持和资助。

本书代表作者对于复杂网络环境下访问控制技术的观点，由于作者水平有限，书中难免有不妥之处，敬请各位读者赐教与指正！

李凤华

中国 · 北京

2015 年 12 月

目录

第6章 访问控制应用研究

第7章 面向网络空间的访问控制技术发展趋势

第1章 绪 论

信息技术的演进与社会进步相互促进。计算机科学与技术是信息技术的核心，计算机硬件、操作系统、数据库等技术的快速发展推动信息技术不断变革、螺旋式发展，先后经历了单机时代、局域网/广域网时代、互联网/云计算时代等发展阶段，并正进入到物联网/万物互联时代。在此过程中，信息传播方式和信息服务模式发生了巨大的变革，智慧互通成为未来不可阻挡的趋势，并已演进为通过“网络之网络”访问“系统之系统”，信息的获取和利用已经或者即将达到“信息随心行、交互在指间”的理想境界。

本章通过对信息技术的发展历程进行概要、全面的归纳总结，将信息技术的发展分为单机、局域网/广域网、互联网/云计算、物联网/万物互联等 4 个阶段，并系统梳理了各个阶段信息传播的特点。

1.1 引言

自 20 世纪 70 年代至今，信息传播方式先后经历了单机、局域网/广域网、互联网/云计算、物联网/万物互联等发展阶段，如图 1-1 所示。

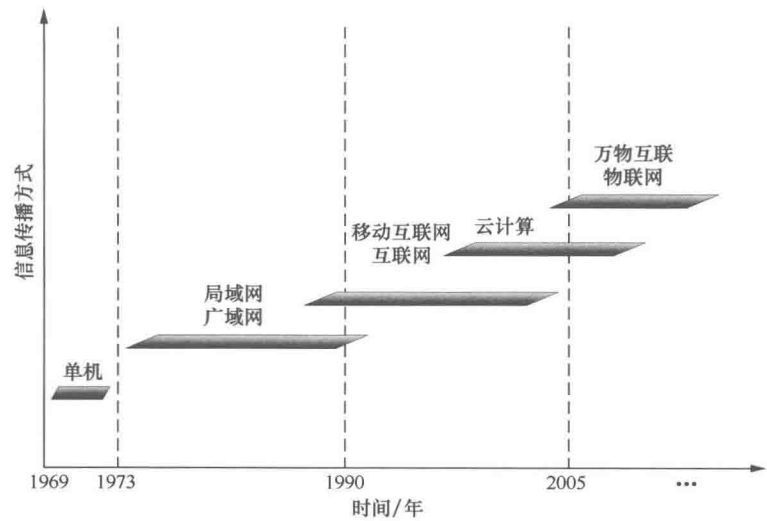


图 1-1　信息传播方式的演进

1.1.1 单机时代

计算机是20世纪最伟大的科学技术发明之一，普惠到人类社会的各个领域，已成为人们日常生活中不可缺少的工具。计算机科学与技术也随之发展成为一门重要的学科，改变了人们的生产、生活方式。

（1）计算机硬件发展

1946年，美国奥伯丁武器试验场生产了第一台全自动电子数字计算机“埃尼阿克”（ENIAC，electronic numerical integrator and calculator），旨在满足计算弹道需要。电子计算机ENIAC采用电子管作为基本元件，每秒可进行5 000次加减运算。随后，经过半个多世纪的飞速发展，计算机已成为具有强大信息处理功能的现代化电子设备。在人类科技史上还没有任何技术可以与电子计算机的发展速度相提并论。计算机硬件的发展迄今为止已经历了4个时代[1,2]。

① 第一代（1946年～1958年）：电子管数字计算机。计算机的基本结构包括运算器、控制器、存储器和输入输出装置。运算器和控制器采用电子管；主存储器采用汞延迟线、磁鼓、磁芯，外存储器采用磁鼓和磁带；输入输出装置主要使用穿孔卡。电子管数字计算机奠定了计算机技术的基础，但是其缺点明显，例如，体积大、耗电大、可靠性差、价格昂贵、维修复杂等。

② 第二代（1958年～1964年）：晶体管数字计算机。晶体管在计算机中的应用标志着第二代计算机的诞生。相比于电子管数字计算机，晶体管数字计算机具有体积小、重量轻、耗电少、可靠性高、计算能力强、寿命长等优势。主存储器采用磁芯，外存储器逐渐采用更为先进的磁盘。伴随出现了操作系统、打印机、内存以及高级程序设计语言等软件、设备和工具，软件产业也由此产生，主要应用于科学计算和各种事务处理，并逐步应用于工业控制。

③ 第三代（1964年～1971年）：集成电路数字计算机。第三代计算机的主要特征是集成电路（IC，integrated circuit），计算机的逻辑元件采用小规模集成电路（SSI，small-scale integration）、中规模集成电路（MSI，medium-scale integration）。相比于晶体管，集成电路体积更小、耗电更少、可靠性更高、计算能力更强、寿命更长，使第三代计算机的性能比第二代计算机又有了很大的提高，应用领域日

益扩大。主存储器采用半导体，软件逐渐完善，高级程序设计语言、分时操作系统得到了进一步的发展。

④ 第四代（1971 年至今）：大规模集成电路数字计算机。计算机的逻辑元件和主存储器都采用了大规模集成电路（LSI，large-scale integration)。大规模集成电路数字计算机开始使用鼠标进行可视化操作，其体积越来越小、价格越来越低、计算能力越来越强。第四代计算机在运算速度、存储容量、可靠性及性价比等诸多方面都取得了长足发展，其软件配置更加丰富，操作系统日益成熟，数据管理系统被普遍使用，呈现出多极化、多媒体、智能化等发展趋势。

（2）操作系统发展

操作系统是管理计算机硬件的程序，为应用程序提供支撑，但并不与计算机硬件一起出现。它是为了满足提高资源利用率、增强计算机系统性能等现实需求，伴随着计算机技术本身及其应用的日益发展而逐步地形成和完善起来的。计算机操作系统的发展归纳如下 8 类[3~10]。

① 手工操作（无操作系统）（1946 年～20 世纪 50 年代中期）。1946 年诞生的第一台计算机中尚未出现操作系统，此时的计算机操作主要通过人工直接操作计算机硬件的方式实现。然而，手工操作方式存在用户独占全机、运算器等待手工操作等局限性，严重降低了计算机资源的利用率。

② 单道批处理系统（20 世纪 50 年代后期～20 世纪 60 年代中期）。20 世纪 50 年代后期，由于手工操作速度和计算机处理速度差异较大，人机矛盾逐渐凸显，需要减少手工操作，逐渐实现作业的自动过渡，单道批处理系统应运而生。单道批处理系统可对作业进行批量处理，具有自动性、顺序性、单道性等特点。

③ 多道批处理系统（20 世纪 60 年代中期）。为解决单道批处理系统无法充分利用系统中的所有资源所导致系统性能较差的问题，在批处理系统中引入多道程序设计技术。该技术可以提高 CPU 利用率、提高内存和 I/O 设备利用率、增加系统吞吐量，使系统具有调度性、无序性、多道性等特点。这一阶段，最为典型的多道批处理系统是运行在 IBM S/360 上的 OS/360 MVT，该操作系统可同时支持 15 个程序，通过将中央存储器分区，并在各分区中运行各程序的方式来提高资源利用率和管理效率。

④ 分时系统（20 世纪 60 年代中期）。作为多道程序设计的自然延伸，分时