高等学校教材·计算机信息安全专业

访问控制概论

洪帆◉主编

Access Control

華中科技大學出版社
http://www.hustp.com

高等学校教材 · 计算机信息安全专业

访问控制概论

◉ 洪　帆　主编

◉ 汤学明　崔永泉　龙　涛　编著

华中科技大学出版社
http://www.hustp.com
中国 · 武汉

图书在版编目(CIP)数据

访问控制概论/洪　帆　主编. —武汉：华中科技大学出版社，2010.8
ISBN 978-7-5609-6139-2

Ⅰ. 访…　Ⅱ. 洪…　Ⅲ. 电子计算机-安全技术-高等学校-教材　Ⅳ. TP309

中国版本图书馆 CIP 数据核字(2010)第 064841 号

访问控制概论　　洪　帆　主编

策划编辑：沈旭日
责任编辑：沈旭日
封面设计：刘　卉
责任校对：刘　竣
责任监印：熊庆玉
出版发行：华中科技大学出版社(中国·武汉)
　　武昌喻家山　　邮编：430074　　电话：(027)87557437
印　　刷：湖北新华印务有限公司
开　　本：710mm×1000mm　1/16
印　　张：13.75
字　　数：275 千字
版　　次：2010 年 8 月第 1 版第 1 次印刷
定　　价：23.80 元

内容提要 Abstract

本书系统地论述了访问控制的基本概念、方法和技术，以及访问控制技术的应用，主要内容包括身份认证，自主访问控制与访问矩阵模型，强制访问控制与 BLP 模型，基于角色的访问控制与 RBAC96 模型簇，各种访问控制技术在操作系统、数据库系统及应用系统中的应用实例。在多域访问控制方面，介绍了基于角色映射的多域安全互操作、动态结盟环境下基于角色的访问控制、安全虚拟组织结盟的访问控制、基于信任管理的访问控制技术，以及权限管理基础设施 PMI。

本书可作为高等院校计算机、信息安全、通信等专业的本科生或研究生的教材，也可供从事与信息安全相关的专业教师、科研和开发人员参考。

前言 Preface

信息是社会发展的重要战略资源，在全球信息化高速发展的同时，信息安全事件也日益增加，日趋严重，信息安全保障已成为维护国家安全和社会稳定的极其重要的因素。信息安全研究内容广泛，包括密码学和访问控制等基础理论研究、操作系统和数据库管理系统等基础支撑软件安全研究、病毒和黑客入侵等攻防技术研究、安全技术框架和安全基础设施研究，以及应用系统运行安全的研究，涉及电子政务、电子商务等众多应用领域。近年来，随着信息安全保密工作的广泛开展和不断深入，信息安全研究的重点逐渐从运行环境、基础设施的安全转向应用系统、信息内容本身的安全保护和访问控制。

随着信息技术的飞速发展及广泛深入的应用，现实社会的政治、军事、经济、金融、商业，以至人们的日常生活等活动已主要以电子化的方式进行和完成，信息系统中的电子文档大量代替了原来的纸质文件。敌对分子和犯罪分子也逐渐将常规的作案手段转变为运用计算机及通信领域中的高科技手段来进行。这样一来，原有的一套社会管理模式(如各个组织、团体的进出门卫制度，对员工的权利、义务及行为规范等)，在信息系统中，都必须转化为对主体(程序或用户)行为的考察和控制。据有关资料统计，对于计算机信息系统的安全威胁 80%来自于系统内部，即来自于系统内合法用户对资源的越权访问和非法使用。访问控制的任务就是要解决这一问题，系统必须根据用户的身份信息，给不同的用户授予不同的权限，并控制这些用户在系统允许的授权范围内活动。国际标准化组织(ISO)在网络安全标准(ISO7498-2)中定义了 5 个层次的安全服务(身份认证服务、访问控制服务、数据保密服务、数据完整性服务、不可否认服务)，访问控制是其中的一个重要组成部分。由此可见，访问控制对信息系统的安全起到至关重要的作用，它是保证信息系统安全的关键技术之一。

从广义上来说，访问控制包括对主体的身份认证、对主体的授权，以及当主体访问系统资源时，系统根据主体的身份信息及所授予的权限对主体的行为进行控制，即访问控制决定哪些主体能够访问系统、能访问系统的哪些资源，以及以怎样的方式来

访问这些资源。在系统中通过访问控制可阻止非法用户进入系统，并规范和限制合法用户的行为，防止合法用户越权操作，从而保证系统资源安全、受控地被使用。

由于信息系统的规模越来越大、环境越来越复杂、信息交换越来越频繁，使得身份认证的机制变得更为重要和复杂，它已成为安全研究的一个重要专题。因此，当前在谈到访问控制时，往往主要是指对主体的授权和根据其授权对主体访问资源行为的控制。也有的人将其分得更细，访问控制仅指后者。不论如何界定，在信息系统中，这三者之间必须紧密配合，才能确保系统中的敏感信息不被非法窃取和破坏。

根据不同的系统背景和应用环境，访问控制的策略和技术有着不同的特点。无论是操作系统、数据库管理系统，还是应用系统(如电子政务、电子商务系统)，都需要对系统中的数据、程序及设备等资源的访问制定相应的访问控制策略，并按照制定的策略实施具体的控制技术，因此，访问控制涉及的范围极其广泛。访问控制和密码学一样，是信息安全专业的核心基础，它们是信息安全的两大支撑技术。作为信息安全专业的大学生，不可不具备这方面的知识。

目前，适合各个层次的、密码学方面的教材已经较为普遍，但国内目前尚未见到系统地讲述访问控制理论和技术的教材。一般仅在操作系统、数据库或者网络安全等教材中，有选择性地对所涉及的访问控制技术进行简要的描述，因此，学生很难全面了解访问控制的基本原理、实现技术和发展状况。本书从访问控制的基本概念、原理、模型和具体实现技术等方面，系统地阐述了访问控制的基础理论知识，并结合访问控制在操作系统、数据库管理系统及网络和应用系统等领域的应用，以实例的形式进行了深入剖析，旨在帮助读者在原理和实践上对访问控制都有一个全面和清晰的了解与把握。

本书在写作的过程中特别注重对访问控制的不同方法和模型进行对比性研究，详细分析了每一种访问控制技术所期望达到的安全目标，以及在不同应用环境下的具体体现形式。通过这种循序渐进的方式，使读者理解对访问控制方法和模型的选择，最终是由信息系统的安全目标所决定的，因而能做到举一反三，将所学的访问控制理论知识灵活运用在系统安全设计之中。

本书第 1 章至第 3 章主要讲述信息安全、身份认证和访问控制的基础知识，介绍访问控制的基本概念、原理和几种常见的访问控制方法；第 4 章讲述访问控制模型，包括访问矩阵模型、BLP 模型和基于角色的访问控制模型；第 5 章从操作系统、数据库管理系统和应用系统三个方面，通过具体的实例来讲述访问控制的实现方法；第 6 章至第 8 章主要讲述复杂、分布式环境下访问控制的理论和实现技术，包括多域环境

下的访问控制技术、分布式环境下的信任管理技术，以及基于 PKI /PMI 权限管理基础设施的访问控制原理与技术。网络和分布式系统的普及应用，特别是动态结盟的应用环境，使得多管理域之间的互访互操作逐渐频繁，并已成为一种发展的必然趋势，于是，域间的访问控制也将逐渐成为研究的热点。

本书适合作为信息安全及相关专业本科和硕士研究生的专业性教材，也可作为电子政务、电子商务和信息系统安全设计等课程的辅助参考教材。建议按课内 56 学时进行讲授，也可根据需要对内容进行增删。教师在教学过程中，针对第 5 章的内容，还可结合课后的习题，配以适当的上机实验课。希望本书能对信息安全工作者有所裨益。

本书是作者多年来在华中科技大学计算机学院信息安全专业讲授访问控制概论课程，以及长期从事信息安全的研究和产品开发的基础上编写而成。本书由洪帆主编，第 1、3、4 章由洪帆编写，第 2 章由肖海军、张昭理编写，第 5 章由汤学明、龙涛编写，第 6、7 章由崔永泉编写，第 8 章由龙涛编写。

付才参加了文稿的修改并编写了部分章节，肖海军参加了修改和统稿，胡福林参加了部分的编写工作。本书在编写过程中参考了国内外许多相关的文献和书籍，在此一并表示衷心的感谢。

感谢华中科技大学计算机学院为作者提供了良好的研究和教学环境，感谢华中科技大学出版社为本书的出版所做的大量工作。

由于时间和水平所限，书中错漏之处在所难免，恳请读者和同行专家对本书提出宝贵意见。

作　者

2010 年 1 月

目录 Content

第1章 概 述

计算机的出现，特别是开放式的计算机因特网的普及与发展，使得信息的载体和传播方式发生了根本性的变化，极大地方便了信息的处理与传递，也极大地方便了信息的获取与共享。在信息时代的今天，随着计算机网络广泛应用到社会的各个领域，任何一个国家的政治、军事、经济、外交、商业和金融都离不开信息，科学的发展和技术的进步也离不开信息，信息已成为社会发展的重要战略资源。信息的地位与作用随着信息技术的快速发展，越来越显示出它的重要性。因此，对信息的开发、控制和利用，已成为国家利益之间、竞争对手之间争夺的重要内容。相应地，信息安全已成为各国、社会各界关注的焦点，与国家安危、经济发展、社会稳定和战争胜负息息相关。信息安全已成为一个重要的研究领域。

对信息安全的维护需要综合运用管理、法律、技术等多种手段。在技术层面上又需要综合运用身份认证、访问控制、密码、数字签名、防火墙、安全审计、灾难恢复、防病毒和黑客入侵等多种安全技术，并进一步建立信息安全基础设施和构建信息安全的保障体系。

身份认证相当于信息系统的门卫，它识别要求进入系统的每一个用户是否是该系统的合法用户，拒绝非法用户进入系统。访问控制则是对进入系统的合法用户对系统资源的访问权进行限制，使用户对资源的使用只能在允许的范围之内。从广义上讲，身份认证也可以看作是一种访问控制。

1.1 信息安全

从人类有信息交流开始，信息安全的问题就存在，但在不同的时期由于信息存储和传输的设备、方式不同，维护信息安全的手段也就不同。早期，计算机诞生之前，人们较多关注的是信息在传递过程中的保密性，使用的也是一些简单的手工加密变换。随着数学、计算机和通信技术的发展，信息的处理和传输能力大大提高，信息安全的含义更为丰富，仅靠传统的密码变换已不能满足信息安全的要求。因此，必须研究计算机和通信安全的新理论和新技术。

计算机信息系统是由计算机及其相关和配套的设备、设施和网络构成的，是按照一定的应用目标和规则对信息进行采集、加工、存储、传输和检索等处理的复杂的人机系统。信息系统可能遭受到各种各样的攻击和威胁，而这些攻击和威胁所造成的损失主要体现在系统中信息的安全性和可用性受到了破坏，它往往使得系统中存放的信息被窃取、篡改、破坏、删除或无法传递，甚至整个系统崩溃。20 世纪 80 年代末期，一场计算机病毒危机席卷全球，人们在震惊之余，第一次意识到精心构建的计算机系统是如此不堪一击。随着数据库和网络技术的广泛应用，计算机及其网络系统的这种脆弱性暴露得更加充分。计算机犯罪案件迅猛增加，已成为一种社会隐患。

1.1.1 信息系统面临的主要威胁

威胁信息系统安全的因素来自于多个方面，总的来说，可分为人为的恶意攻击和软硬件故障、用户操作失误两类。其中，有预谋的人为攻击的威胁程度和防范难度远大于第二类，是系统防范的重点。

据美国联邦调查局的报告，计算机犯罪是商业犯罪中最大的犯罪类型之一，每年计算机犯罪造成的经济损失高达数十亿美元。加之国际互联网络的广域性和可扩展性，计算机犯罪已成为具有普遍性的国际问题。

从总体来看，威胁信息系统安全的方式主要有以下几种。

1. 窃取

合法用户，甚至非法用户（冒充合法用户，进入了系统）未经许可却直接或间接获得了对系统某项资源的访问权，从中窃取了有用的数据或骗取了某种服务，但不对信息作任何修改。这种攻击方式通常被称为被动攻击。

用程序或病毒截获信息是这一类攻击的常见手段。在通信设备或主机中预留程序代码或施放病毒程序，这些程序通过对信息流量进行分析，或通过对信息的破译以获得机密信息，并将有用的信息通过某种方式发送出去。

搭线窃听也是常见的手段，将导线搭到无人监守的网络传输线上进行监听，如果所搭的监听设备不影响网络的负载平衡，网络站点是无法发现的。

对难于搭线监听的可以用无线截获的方式得到信息，通过高灵敏接收装置接收网络站点辐射的电磁波或网络连接设备辐射的电磁波，通过对电磁信号的分析恢复原数据信号从而获得网络信息。

被动攻击不易被发现，原因是它不会导致系统中信息的任何改动，系统的操作和状态也不被改变，留下的痕迹很少，甚至不留痕迹。对付这种攻击的方法主要是采用加密技术，形成加密通道。

2. 篡改

未经授权的用户成功地获得了对某项资源的访问权后，对信息的全部或部分进行肆意地修改、删除、添加，改变其中内容的次序或形式，改变信息的流向，或者修改程序的功能，改变系统的状态和操作等，破坏信息的完整性、真实性和有效性。某些情形的更改可以用简单的措施检测出来，但有一些更精妙的更改却很难发现或检测。

在金融犯罪的案件中，大多是通过修改程序或修改数据达到贪污和欺诈钱财的目的。

3. 伪造

威胁源在未经许可的情形下，在系统中产生出虚伪的数据或服务。例如，电子商务中，不法分子可能希望在网络通信系统中加上假的交易，或者在现有的数据库中增加记录。

伪造信息在网络通信中往往可以使对方落入陷阱。

4. 拒绝服务

威胁源使系统的资源受到破坏或不能使用，从而使数据的流动或所提供的服务终止。

用户的误操作，软硬件出现故障均可能引起系统内的数据或软件的破坏，因而使得计算机不得不停止工作。隐藏在计算机中具有破坏性的病毒程序被激活后，可能会毁掉系统中某些重要的数据，甚至可能删除系统中的所有数据且使其无法恢复，更严重的可能导致整个系统的瘫痪。又例如，一些不法分子通过断电设置障碍，采用纵火、爆炸、盗窃通信设备等手段导致计算机系统的硬件遭到破坏，使计算机及通信系统无法正常工作。

拒绝服务攻击还可能使网站服务器充斥大量要求回复的信息，消耗网络带宽或系统资源，导致网络或系统不胜负荷以至瘫痪而停止提供正常的网络服务。

5. 重放

在网络通信中重放以前截获到的过时信息，欺骗收方。

6. 冒充

一个实体假冒另一个实体的身份是一种常见的网络攻击手段。

黑客闯入系统的主要途径之一是破译用户的口令，从技术的角度看，防止口令被破译并不困难，但具体执行却较麻烦。经常有些 Web 主管，更不用说用户，同样的口

令连续使用好几个月。工作组的成员辞职了，工作组的口令却不改变。甚至，有的用户将自己的口令告诉自己的朋友，这其中就可能有黑客。

7. 抵赖

在网络通信中，用户可能为了自己的利益，在事后否认曾经对信息进行过的生成、签发、接收等行为。

1.1.2 信息系统的脆弱性

以计算机为核心的信息系统面临如此之多的威胁，反映出信息系统本身存在一些固有的弱点和脆弱性。它的脆弱性主要表现在以下方面。

1. 硬件设施的脆弱性

除难以抗拒的自然灾害，如雷击、地震、水灾等外，温度、湿度、尘埃、电磁干扰和人为破坏等均可以影响计算机系统各种设备的正常工作。保证计算机信息系统各种设备的物理安全是计算机信息系统安全的前提。

通过电磁辐射使计算机系统信息被截获而失密的案例已有很多，在理论和技术支持下的验证工作也证实了这种截取距离在几百米，甚至可达千米的复原显示给计算机系统信息的保密工作带来了极大的危害。为了防止系统中的信息在空间中的扩散，通常是在物理上采取一定的防护措施，以减少或干扰扩散出去的空间信号。这对重要的政府部门、军事和金融机构在构建信息中心时都将成为首要设置的条件。

在一块小小的磁盘上或光碟上，可以存储大量的数据信息，而它们很容易放在口袋里带出办公室，数据存储的高密度为入侵者窃取信息带来了便利。

另外，这些存储介质也很容易受到损坏(有意或无意)，造成大量信息的丢失。

保存在存储介质上的数据可能会将存储介质永久地磁化，因此存储介质上的信息有时擦除不净或不能完全擦除掉，使得介质上留下可读的痕迹，这些信息一旦被利用就可能产生泄密。

另外，大多数计算机操作系统中，删除文件时仅仅只将文件名删除，并将相应的存储空间释放，而文件的内容还原封不动地保留在存储介质上，利用这一现象，入侵者也可以窃取机密信息。

单个、孤立信息的价值往往不大，但如果将大量相关的信息聚集在一起，经过筛选和分析，则可显出这些信息的重要性。计算机的特点之一就是能收集大量的信息并对其进行自动、高效的处理，这种聚生性可被入侵者利用来窃取他感兴趣的机密信息。

2. 软件的脆弱性

计算机信息系统的软件可分为三类:操作平台软件、应用平台软件和应用业务软件。它们以层次结构组成信息系统的软件体系。操作平台软件处于最底层,支持着上层软件的运行。因此,操作平台软件的安全是整个信息系统安全的基础,它的任何风险将直接危及到应用平台软件和应用业务软件的安全。应用平台软件在维护自身安全的同时,必须为应用软件提供必要的安全服务。应用业务软件处于顶层,直接与用户打交道。对系统的许多攻击都是通过应用业务层来实施的,它的风险直接反映了系统的安全风险。

在软件的设计与开发过程中往往存在许多错误、缺陷和遗漏,从而形成系统的安全隐患,而且系统越大、越复杂,这种安全隐患就越多。据有关资料估计,微软开发的操作系统 Windows 的各种版本,平均每 100 行代码大约要出现 0.5～1 个错误或缺陷。这些缺陷和漏洞恰恰是黑客进行攻击的首选目标。

导致黑客频频攻入系统内部的主要原因是,相应系统和应用软件本身的脆弱性和安全措施不完善。另外,信息系统中的"后门"是普遍存在的,它可能是生产厂家或程序员在生产过程中为了自便而设置的,也可能是黑客入侵后在其中设置的。黑客利用后门可以在程序中建立隐蔽通道,植入一些隐蔽的恶意程序,进行非法访问,达到窃取、篡改和破坏信息的目的。

目前市场上尚无任何一个大型操作系统或数据库管理系统可以做到完全正确无误、没有缺陷,所以这些系统的厂商都要定期地推出新的版本,其中包括数以千计修改过的语句和代码。这些改动大多数是为了纠正系统中的错误或弥补其缺陷。这些系统的设计者永远无法充满自信地宣布已经找到了系统中的所有漏洞。另一方面,入侵者们多数不会公布他们的发现,因此,当你将重要的敏感信息委托给一个大型操作系统或网络中的一台计算机时,你没有理由不为你的信息的安全担忧,尤其是当这些信息对入侵者有足够的价值时。

虽然任何操作系统和数据库管理系统都有缺陷,但绝大多数系统是可用的,可以基本完成其设计功能。这就如一个墙上有洞的房间,虽能居住,却无法将盗贼拒之门外。

3. 网络通信的脆弱性

网络系统中,通信线路很容易遭到物理破坏,也可能被搭线窃听,甚至于插入、删除信息。无线信道的安全性更加脆弱,因此通过未受保护的外部线路可以从外部访问到系统内部的数据。

资源共享是建立计算机网络的基本目标之一,但这也为系统安全的攻击者利用

共享的资源进行破坏活动提供了机会，也为攻击者利用资源共享的访问路径对其他非共享资源进行攻击提供了机会。

计算机网络是一个复杂的系统，网络的可扩展性使得网络的边界具有不确定性，这使得网络的管理变得十分困难，构成了对网络安全的严重威胁。

信息传输时，一个节点到另一个节点可能存在多条路径，一份报文在从发送节点到达目标节点之间可能要经过若干个中间节点，这种路径的不确定性和中间节点的不确定性，使得仅有起始节点和目标节点的安全保密性还不足以保证信息的安全。

数据库技术和网络，特别是 Internet 网技术的兴起、发展和广泛应用极大地促进了社会信息化的进程，它使得信息可以超越时间和空间的界线达到最大程度的共享。现在，无论在地球上的什么地方，也无论什么时候，只要轻点一下计算机鼠标，就可以获得许许多多来自不同地方和部门的信息。人们在享受技术进步为工作、生活带来的这种方便和效率的同时，也感受到了它所带来的对系统中信息安全的威胁。当前，信息系统的多平台、充分集成的分布式模式成为最流行的处理模式，而集中分布相结合的处理方式也很受欢迎。21 世纪的信息系统将建立在庞大、集成的网络基础上，而在新的信息系统环境中，由于移动计算的普及，存取点将大大增加，从而信息系统的薄弱环节将分布更广。事实上，现代计算机领域中的任何一个大的技术进步都可能对计算机系统自身的安全构成一种新的威胁，所有这些威胁都需要研究出新的方法和技术来予以消除。

1.1.3 信息安全的目标

现代信息技术的飞速发展为社会带来了巨大的效益，高速计算机和高速网络的逐步政用化、商用化、军用化和民用化反映了当今社会对信息及信息技术的巨大依赖性。信息已成为人类宝贵的资源，它关系到国家的机密和企业的发展，甚至关系国家和企业的生死存亡。正因为信息在人类社会活动、经济活动中起着越来越重要的作用，因此信息的安全日益受到社会越来越广泛和高度的重视。

所谓信息系统的安全，是指对于信息系统中的硬件、软件及数据进行保护，防止它们因偶然或恶意的原因而遭到破坏、更改或泄露。为此，信息系统在获取、存储、处理、传输和控制信息的过程中，要建立和采取一些技术上和管理上的安全保护措施。

信息系统安全从需要保护的对象考虑，可分为外部安全和内部安全。外部安全是指构成信息系统的计算机硬件、外部设备以及网络通信设备的安全，使其不会丢失或受到毁坏，能为系统提供正常的服务。内部安全是指信息系统中程序、数据和服务的安全，使其不被破坏，更改和泄露。无论是内部安全还是外部安全，信息系统安全的最终目标是要使得信息在系统内的任何地方、任何时间和任何状态下保持其安全