第一图书网, tushu007.com

# <<访问控制概论>>

## 图书基本信息

书名：<<访问控制概论>>

13位ISBN编号：9787560961392

10位ISBN编号：7560961398

出版时间：2010-8

出版时间：华中科技大学出版社

作者：洪帆 编

页数：208

版权说明：本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：http://www.tushu007.com

第一图书网, tushu007.com

# <<访问控制概论>>

## 前言

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。

第一图书网, tushu007.com

# <<访问控制概论>>

## 内容概要

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。

第一图书网, tushu007.com

# <<访问控制概论>>

## 书籍目录

第一图书网, tushu007.com


## 章节摘录

插图：计算机信息系统是由计算机及其相关和配套的设备、没施和网络构成的，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。

第一图书网, tushu007.com

# <<访问控制概论>>

## 编辑推荐

《访问控制概论》：高等学校教材·计算机信息安全专业

第一图书网, tushu007.com

# <<访问控制概论>>

## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问:http://www.tushu007.com