网络安全控制机制

林 闯 蒋屹新 尹 浩 著

清华大学出版社

国家科学技术学术著作出版基金资助出版

网络安全控制机制

林　闯　蒋屹新　尹　浩　著

清华大学出版社
北京

内 容 简 介

网络安全是计算机和通信领域很重要的研究方向，而网络安全控制机制是网络安全的基本保障，是网络安全中的重要研究内容。本书分为5章，第1章是访问控制机制，讲述了访问控制的最新进展，并讨论了移动通信和可信网络环境下的访问控制技术。第2章是认证机制，介绍AAA服务器的认证原理及其在无线网络中的应用，然后介绍多级安全域的认证模型，最后讨论了移动网络中的可以容忍DoS攻击的认证模型。第3章是数字签名机制，介绍数字签名中的公钥密码体制和椭圆曲线密码体制，并讨论了基于椭圆曲线的群体导向的签名方案。第4章是密钥管理机制，概述了基本的组密钥分发机制，讨论了自愈的组密钥分发协议和基于时限的组密钥分发机制，并阐述了无线传感器网络中的密钥管理。第5章是基于应用层组播的视频安全机制，介绍流媒体与应用层组播，数字水印技术以及视频加密技术，并详细描述了一个视频安全组播协议，讨论了视频流传输过程中的差错控制。

本书全面、系统地展示了网络安全控制机制的研究内容和最新成果，具有完整性、实用性和学术性。非常适合我国计算机网络和通信领域的教学、科研工作和工程应用参考。既可以供计算机、通信、电子、信息等相关专业的研究生和大学高年级学生作为教材或教学参考书，也可以供计算机网络研究开发人员、网络运营商等网络工程技术人员参考。

图书在版编目（CIP）数据

网络安全控制机制/林闯，蒋屹新，尹浩著．—北京：清华大学出版社，2008.12
ISBN 978-7-302-18673-1

Ⅰ．网…　Ⅱ．①林…　②蒋…　③尹…　Ⅲ．计算机网络－安全技术　Ⅳ．TP393.08

中国版本图书馆CIP数据核字(2008)第152079号

责任编辑：薛　慧
责任校对：赵丽敏
责任印制：王秀菊

出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　　编**：100084
社　总　机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质　量　反　馈：010-62772015，zhiliang@tup.tsinghua.edu.cn

印 刷 者：北京鑫丰华彩印有限公司
装 订 者：三河市溧源装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：20.25　　**字　数**：485千字
版　　次：2008年12月第1版　　**印　次**：2008年12月第1次印刷
印　　数：1～3000
定　　价：46.00元

本书如存在文字不清、漏印、缺页、倒页、脱页等印装质量问题，请与清华大学出版社出版部联系调换。
联系电话：010-62770177转3103　　产品编号：022523-01

FOREWORD

前言

背景

随着传感器、嵌入式设备、消费电子等设施的大量接入，互联网络在规模和应用领域上日益得到拓展，网络的规模仍在继续扩大，网络在国民经济生活中的基础性和全局性作用日益增强。尽管互联网已经转变并大大改善了人类社会的经济和生活方式，但同时也不得不面临大量的网络安全问题，如恶意攻击、垃圾邮件、计算机病毒、不健康资讯等。尽管信息网络的安全研究已经持续多年，但对网络攻击和破坏行为的对抗效果并不理想，仍然面临着严峻的挑战。

网络安全是计算机和通信领域重要的研究内容，而对网络安全控制机制的研究是保障网络安全的基本技术。国际标准化组织(ISO)在网络安全标准 ISO 7498—2 中定义了 5 种层次型安全服务：身份认证服务、访问控制服务、数据保密服务、数据完整性服务和不可否认服务。其中，访问控制是信息安全的一个重要组成部分，它作为系统安全的关键技术，既是一个老生常谈的内容又面临着新的挑战。随着网络技术的发展，访问控制技术也将作为网络安全的一个重要方面日益受到更多人的关注。授权和认证是访问控制的基础，正确的授权实际上依赖于认证。如何保证用户身份的真实性和合法性，如何正确授权用户的权限，是访问控制和认证机制中重要的研究内容。

虽然使用数据加密、访问控制等多项技术可以对数据通信时的保密性和完整性予以保证，然而仅仅有这些还是不够的，特别是近年来，随着电子商务的发展，人们通过通信网络进行迅速的、远距离的贸易，数字或电子签名也应运而生，并开始用于商业通信系统。这些都要求根据不同的情况设计出适合特定情况的安全而有效的数字签名，以适应飞速发展的网络环境下的安全需要。因此，数字签名也是网络安全机制中一项重要内容，其中基于椭圆曲线的数字签名方案成为热点研究内容。

此外，随着移动通信和数字服务的兴起，无论是 Internet、无线传感器网络，还是移动网络和流媒体服务，都对安全组通信协议的设计带来了颇多挑战，如开放设计的 Internet、易受入侵和非法攻击的移动网络、不可靠的无线传感器网络、流媒体系统的视频安全等因素。这使得组通信的应用将变得更加普遍，同时也对安全的组通信协议设计提出了许多新的并需亟待解决的课题。因此，有必要对组密钥管理进行研究，解决组通信中的安全问题。

作者在网络安全领域进行了一系列深入而系统的研究工作，本书主要对网络安全机制中的访问控制、身份认证、数字签名、密钥管理和视频安全技术进行全面、深入的阐述，书中绝大部分内容取材于我们近期在国际、国内一流学术期刊发表的论文，全面、系统地展示了很多新的研究成果和进展。

组织结构

本书主要对5种网络安全控制机制加以介绍，在结构上分为5章：

第1章是访问控制机制，首先概述了访问控制的发展过程，并对典型的访问控制模型进行了介绍，如自主访问控制、强制访问控制和基于角色的访问控制模型。然后基于Petri网对强制访问控制模型进行了安全性分析。针对移动网络的特点，提出了支持移动IPv6的访问控制模型，介绍方案的实现及其扩展。最后，对可信网络中的访问控制进行研究，根据可信网络中用户行为的可信模型，讨论了基于可信和信誉的访问控制机制。

第2章是认证机制，首先介绍RADIUS协议和AAA服务器的认证原理以及AAA在无线网络中的应用。然后针对大型、复杂的网络系统中存在着一系列相互信任或不相互信任的安全自治网络域，介绍多级安全域的认证模型，并用逻辑理论对安全域认证模型进行形式化描述。最后讨论了移动网络中的可以抵制DoS攻击的认证模型，通过性能和安全分析，证明该模型能够满足移动网络中安全性和可靠性的需求，并能抵制DoS攻击，极大地提高了认证协议的安全性。

第3章是数字签名机制，首先介绍公钥密码体制，对数字签名中的几个典型的机制进行阐述，如RSA，ElGamal，Schnorr和DSS数字签名机制。然后详细介绍椭圆曲线密钥体制，基于椭圆曲线提出了群体导向的数字签名方案，并对其进行安全分析和性能分析。

第4章是密钥管理机制，首先概述了组密钥分发机制研究现状，对集中式、分散式和分布式组通信密钥管理进行介绍。然后详细分析了基本的组密钥分发协议，并给出其安全性分析。提出了一个自愈的组密钥分发协议，并在此基础上讨论了基于时限用户撤销机制的自愈组密钥分发协议，给出了协议的具体应用和改进方案。最后，对无线传感器网络中的密钥管理进行了阐述和分析，介绍几个典型的密钥管理方案和协议，对其进行了综合分析，并给出了需要解决的研究问题。

第5章是基于应用层组播的视频安全机制，介绍流媒体与应用层组播、数字水印技术及视频加密技术，并提出了一个媒体相关的视频安全组播协议MSMP，详细介绍用户加入和退出机制，并对其可靠性和扩展性进行分析。最后讨论了视频流传输过程中的差错控制机制以及无线网络中多层非对等保护的动态优化组包策略。

本书特点与读者对象

本书具有以下鲜明特色。

(1) 完整性：内容丰富全面，结构合理，体系完整，将网络安全控制机制的5个方面，即访问控制、认证、数字签名、密钥管理和视频安全机制，进行全面和系统的介绍。

(2) 实用性：结合当前网络环境的特点，将网络安全控制机制应用于可信网络、移动网络和传感器网络，给出具体的应用实例，具有很强的实用性。

(3) 学术性：本书具有一定的理论高度和学术价值，书中绝大部分内容取材于作者近期在国际、国内一流学术期刊发表的论文，全面展示了大量网络安全方面最新的科研成果，具有很高的学术参考价值。

本书非常适合我国计算机网络和通信领域的教学、科研工作和工程应用参考。既可以供计算机、通信、电子、信息等相关专业的研究生和大学高年级学生作为教材或教学参考书，

也可以供计算机网络研究开发人员、网络运营商等网络工程技术人员参考。

致谢

作者的研究工作得到国家自然科学基金项目(Nos. 60673184, 60503052, 60429202, 60432030)、国家重点基础研究发展计划("973"计划)项目(No. 2006CB708301)和国家高技术研究发展计划("863"计划)项目(Nos. 2006AA01Z218, 2006AA01Z225)等的连续资助,在此表示深深的谢意!

西安第二炮兵工程学院的封富君博士(林闯的学生)在本书的写作过程中做了大量细致而辛苦的工作,在此对其表示衷心的感谢!

由于作者水平所限,加之计算机网络安全控制机制的研究仍处于不断的发展和变化之中,书中错误和不足之处在所难免,恳请专家、读者予以指正。

作 者
2008 年 5 月
北京 清华园

CONTENTS

目 录

Chapter

第1章 访问控制

访问控制技术起源于20世纪70年代，当时是为了满足管理大型主机系统上共享数据授权访问的需要。但随着计算机技术和应用的发展，特别是网络应用的发展，这一技术的思想和方法迅速应用于信息系统的各个领域。在30多年的发展过程中，先后出现了多种重要的访问控制技术，如自主访问控制（discretionary access control，DAC）、强制访问控制（mandatory access control，MAC）和基于角色的访问控制（role-based access control，RBAC），它们的基本目标都是防止非法用户进入系统和合法用户对系统资源的非法使用。访问控制技术作为实现安全操作系统的核心技术，是系统安全的一个解决方案，是保证信息机密性和完整性的关键技术，对访问控制的研究已成为计算机科学的研究热点之一。

本章对不同网络环境下的访问控制进行研究，给出了针对不同网络的访问控制模型。首先概述了访问控制的基本目标、发展过程、分类及其研究趋势，然后基于着色Petri网对强制访问控制进行形式化描述和安全分析。针对移动通信网络，给出了支持层次移动IPv6的访问控制方案。最后，研究下一代网络发展的必然趋势，即可信网络下的访问控制及其实现机制。

1.1 访问控制概述

国际标准化组织（ISO）在网络安全标准ISO 7498—2中定义了5种层次型安全服务：身份认证服务、访问控制服务、数据保密服务、数据完整性服务和不可否认服务。其中访问控制是信息安全的一个重要组成部分，作为系统安全的关键技术，访问控制是一个老生常谈的内容同时又面临着新的挑战。随着网络技术的发展，访问控制技术也将作为网络安全的一个重要方面日益受到更多人的关注。授权和认证是访问控制的基础，正确的授权实际上依赖于认证。认证是决定一个用户的身份是否合法的过程。授权决定一个用户是否有权访问系统资源。一个信息系统必须维护一些用户ID和系统资源之间的关系，建立一个授权用户被允许访问的资源列表。访问控制技术不仅包括授权和认证，还可以有很多其他形式，如智能卡、密钥锁、生物信息识别（如指纹、视网膜或人脸）等。

1.1.1 访问控制基本概念

任何访问控制模型都会用到用户(user)、主体(subject)、客体(object)、操作(operation)和权限(permission)的概念,下面对这几个概念进行简单的介绍。

用户:被授权使用计算机的人员。一个用户可能有多个 ID,而这些 ID 可能被同时激活。一个用户的会话实例称为会话(session)。

主体:可以被其他实体施加动作的主动实体。主体可以是用户或其他任何代理用户行为的实体(如进程、作业和程序)。一个用户可以有多个主体,即使该用户只有一个会话。

客体:接受其他实体动作的被动实体。客体可以是一个可识别的资源,一个客体可以包含另一个客体。一个实体可以在某一时刻是主体,而在另一时刻是客体,这取决于该实体的功能是动作的执行者还是被执行者。

操作:由主体激发的主动进程。每个访问控制模型都与信息流相关,但是基于角色的访问控制要求主体和操作区别开来。

权限:在受系统保护的客体上执行某一操作的许可。在客体上能够执行的操作通常与系统的类型有关,权限是客体和操作的联合。两个不同客体上的相同操作代表着两个不同的权限,单个客体上的两个不同操作代表着两个不同的权限。

此外,最小特权(least privilege)原则是系统安全中最基本的原则之一。所谓最小特权原则是指:用户所拥有的权力不能超过他执行工作时所需的权限,即每个主体(用户和进程)完成某种操作时必不可少的特权。只给予主体"必不可少"的特权,一方面保证所有的主体都能在所赋予的特权之下完成所需要完成的任务和操作;另一方面,限制了每个主体所能进行的操作。最小特权原则在保持完整性方面起着重要的作用,实现最小权限原则,需分清用户的工作内容,确定执行该项工作的最小权限集,然后将用户限制在这些权限范围之内。在基于角色的访问控制中,只有角色需要执行的操作才授权给角色。当一个主体要访问某个资源时,如果该操作不在主体当前活跃角色的授权操作之内,则该访问将被拒绝。

坚持最小特权原则要求用户在不同的时间拥有不同的权限级别,这依赖于所执行的任务或功能。在某些环境和权限下,不必要的权限有可能会增加用户的额外负担,因此必须限制权限。然而过多的权限有可能会泄露信息,因此为了保证系统的机密性和完整性,必须避免赋予多余的权限。

1.1.2 访问控制目标

访问控制只是系统安全的一个解决方案,为了更好地理解访问控制的目标,有必要了解信息系统的风险。信息系统的安全风险可分为 3 类:机密性、完整性和有效性,记为 CIA。

机密性(confidentiality):保持信息的安全和私有,防止信息泄露给未授权的用户;

完整性(integrity):防止信息被非法用户篡改或破坏;

可用性(availability):保障授权用户对系统信息的可访问性。

访问控制是保证信息机密性和完整性的关键技术。机密性要求只有授权的用户可以读取信息。一般来说，系统中的某些信息是非常重要的，如军事上的某些数据，公司的财务信息及个人的账户信息等，这些信息都对机密性要求较高。完整性要求只有授权的用户可以在授权的方式下修改信息，是为了维护系统资源处于一个有效的、预期的状态，防止资源被不正确、不适当地修改，或维护系统不同部分的数据一致性。访问控制并不能完全保证可用性，它的作用是，当一个非法的攻击者试图访问系统时，有可能会受到阻止。

1.1.3　访问控制发展过程

从 1960 年起安全问题就引起了人们的关注，最早由 Lampson[1] 提出了访问控制的形式化机制描述，引入了主体、客体和访问矩阵的概念。对访问控制模型的研究，从早期的 20 世纪六七十年代至今，大致经历了以下 4 个阶段：

1. 20 世纪六七十年代应用于大型主机系统中的访问控制模型，较典型的是 Bell-Lapadula 模型[2]（简称 BLP 模型）和 HRU 模型[3]。

(1) Bell-Lapadula 模型

Bell-Lapadula 模型，简称 BLP 模型，由 Bell 和 Lapadula 将军队访问控制规则融入数学模型，定义推理计算机系统的安全性。该模型指出，进程是整个计算机系统的一个主体，它需要通过一定的安全等级来对客体发生作用。进程在一定条件下可以对诸如文件、数据库等客体进行操作。其安全规则指出，用户仅能访问安全级等于或低于用户安全级的那些信息。这是一个简单的策略，容易被人理解，但是在计算机系统上实现这个策略则是很困难的。无法预料的系统漏洞和系统中不同组件的交互，使得计算机系统具有安全脆弱性。在该模型中，计算机系统中的实体被分成抽象的对象。安全状态得到了详细的说明，而且通过从一个安全状态转到另一个安全状态的方式来证明状态转移过程仍然是安全的，进而归纳证明了该系统是安全的。

BLP 模型有两个基本的规则：简单安全规则和 *-特性，通常称为“不上读”和“不下写”。简单安全规则指出：实体不能读取安全级别高于它的对象，即实体的安全级别必须大于等于对象的安全级别。 *-特性（星特性）指出：如果对对象执行写操作，实体的安全级别必须小于等于对象的安全级别。

$$\text{read: } SL(\text{Entity}) \geqslant SL(\text{Obj}) \quad \text{简单安全规则}$$

$$\text{write: } SL(\text{Entity}) \leqslant SL(\text{Obj}) \quad *\text{-特性}$$

其中，SL 表示实体或对象的安全级别。

BLP 模型的核心思想是在系统中设置多个安全等级（如普通、秘密、机密和绝密），并要求系统中的所有存取操作必须遵守模型给出的保护信息安全的规则，以此实现强制存取控制，防止具有高安全级别的信息流入低安全级别的客体。BLP 模型不能直接用于商业系统，主要应用于军事系统。虽然 BLP 模型为通用的计算机系统定义了安全属性，且这种模型比较容易实现，但“不上读”和“不下写”的规则忽略了完整性，而使非法越权篡改成为可能。

BLP 模型已成为计算机安全基础的研究对象，该模型的发展影响了许多其他模型的发展，甚至很大程度上影响了计算机安全技术的发展，并渗透到计算机安全建模的所有策略，

它是第一个将实际系统的属性转化为规则的属性模型。在 BLP 模型的基础上，形成了很多标准，其中包括美国国防部的可信计算机评估标准。尽管该模型存在很多争议，但是它促进了计算机安全基础领域的进一步研究。

虽然 BLP 安全模型控制了对信息的写操作，保护了系统的机密性，但是多级安全策略并没有阻止对信息的非法修改。因此在 BLP 安全模型之后，用户很快认识到需要这样一种模型：能够阻止高安全级的进程读取低安全级的信息，而且进程不被低安全级的信息所影响。

Biba 完整性模型[4]是 1977 年提出的，是 BLP 模型的副本。BLP 模型着重系统的机密性，而 Biba 完整性模型则着重保证对象的完整性。Biba 模型将主体和客体按照强制访问控制系统进行分类，这种分类方法一般应用于军事用途。数据和用户被划分为 5 个安全等级：公开(unclassified)、受限(restricted)、秘密(confidential)、机密(secret)和绝密(top secret)。Biba 完整性模型确保实体只能向安全级别比它低的对象写信息，避免了在 BLP 模块中易发生的一种情况：安全级别高的实体可能故意破坏安全级别低的对象，并且实体可以从安全级别比它高的对象中读取信息。因为该模块只需要保证完整性，它是从完整性等级的方面被描述的，而不是从安全性或敏感性等级方面。这些规则可以总结为：

$$\text{write}: IL(Entity) \geqslant IL(Obj) \quad \text{简单完整性规则}$$

$$\text{read}: IL(Entity) \leqslant IL(Obj) \quad *\text{-特性}$$

Biba 模型基于两种规则来保障数据的完整性和保密性：

下读(no-read-up)：主体不能读取安全级别低于它的数据；

上写(no-write-down)：主体不能写入安全级别高于它的数据。

Biba 模型并没有被用来设计安全操作系统，因为 Biba 模块中的所有模块可以读任意级别比它高的对象，可以发送信息给级别比它低的对象，这可能造成实体泄露高级别对象的内容，在一定程度上忽视了保密性。但大多数完整性保障机制都是基于 Biba 模型的两个基本属性构建的。

(2) HRU 模型

1976 年 Harrison，Ruzzo 和 Ullman 提出 HRU 模型[3]，提供了更改访问权限的策略和创建以及删除主题和对象的权限，并指出用传统的访问矩阵并不能保证系统的安全性，即安全需要是安全的并不能说明系统的配置是安全的。用户可以放弃访问权限，也可以授权给其他用户，其他用户又可以授权给另外的用户，因此当权限一级级地被传递时，系统无法保证非授权的用户不会非法得到访问权限。

2. 美国国防部在 1985 年公布的可信计算机安全评价标准(TCSEC)[5]中明确提出了访问控制在计算机安全系统中的重要作用，并指出一般的访问控制机制有两种：自主访问控制(DAC)和强制访问控制(MAC)。目前 DAC 和 MAC 被应用在很多领域，关于 DAC 和 MAC 的相关内容将在 1.1.4 节中介绍。

3. 从 1992 年最早的 RBAC 模型，即 Ferraiolo-Kuhn 模型[6]的提出，到 Sandhu 等人对 RBAC 模型的研究，先后提出了 RBAC96[7]，ARBAC97[8]，ARBAC99[9]模型，一直到 2001 年的 NIST RBAC 标准[10]。

Ferraiolo-Kuhn 模型将现有的面向应用的方法应用到 RBAC 模型中，是基于角色的访

问控制(RBAC)最初的形式化描述,它对主体-角色活动(subject-role activation)、主体-客体(subject-object)关系、用户-角色(user-role)关系和角色集活动(role-set activation)进行了描述。有以下 3 个基本规则:

规则 1　角色分配(role assignment):当一个主体被分配了一个角色时,该主体才能执行一个事务。身份认证过程并不是一个事务,而系统中用户的其他行为都是通过事务完成的,因此,活动用户需要有一些活动角色。

规则 2　角色授权(role authorization):一个主体的活动角色必须授予该主体。由规则 1,这条规则保证了用户只能执行被授权的角色。

规则 3　事务授权(transaction authorization):当一个事务被授予一个主体的活动角色时,该主体才能执行该事务。由规则 1 和规则 2,该规则保证了用户只能执行被授予的事务。

RBAC 模型的正式描述见表 1.1.1,其特点是所有访问都是通过角色来实现的。一个角色实质上是权限的集合,所有用户通过分配的角色来接受权限。角色是相对稳定的,而用户和权限则可能变化很快,通过角色对访问进行控制简化了管理。RBAC 关系图如图 1.1.1 所示。

表 1.1.1　Ferraiolo 对 RBAC 的形式化描述

RBAC 的形式化描述
活动角色:AR(s: subject)=｛主体 s 的当前活动角色｝
角色授权:RA(s: subject)=｛系统授给主体 s 的角色｝
事务授权:TA(r: role)=｛系统授给角色 r 的事务｝
exec(s: subject,t: tran)=true　当且仅当主体 s 有权执行事务 t,否则为 false 角色分配:$\forall s$: subject,t: tran · exec(s,t)⇒AR(s)≠∅ 角色授权:$\forall s$: subject · AR(s)⊆RA(s)

图 1.1.1　RBAC 关系图

多数计算机系统的访问控制是通过访问控制表(access control list, ACL)来实现的,所以系统资源,如文件、打印机和终端,都有一个授权用户列表,这样很容易回答“哪些用户可以访问客体 X”,但是却很难回答“用户 X 能够访问哪些客体”。后者的回答需要扫描系统中数以百万计的客体并记录访问控制列表,而这个过程在实际的系统中可能会需要一天的时间。这个机制的特点是:ACL 可以很容易地给客体增加权限,但很难激发一个用户的所有权限。

在一些系统中,用户被分为组,称为实体(entry)。RBAC 和组的概念有些相似,组是用户的集合而不是权限的集合,权限是与用户和用户所属的组相关联的,如图 1.1.2 所示。由于用户通过 UID(user ID)或 GID(group ID)来访问客体,因此,当组权限从客体上撤销时,一旦权限被激活,用户可能重新获得访问权限。RBAC 要求通过角色进行访问加强了系统的安全性。

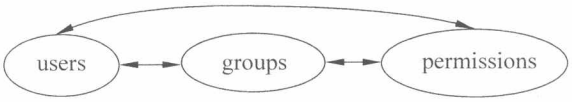

图 1.1.2 组访问控制关系图

Ferraiolo-Kuhn 模型的第 2 个重要特点是角色是分等级的：角色能够从其他角色中继承权限。此外，该模型包含了 Clark-Wilson 模型[11]。此后 NIST RBAC 参考模型对角色进行了详细的研究，在用户和访问权限之间引入了角色的概念，为 RBAC 模型提供了参考。关于 NIST RBAC 模型将在 1.1.4 节中加以介绍。

4. 此后，对访问控制模型的研究扩展到更多的领域，比较有代表性的有：应用于工作流系统或分布式系统中的基于任务的授权控制模型(TBAC)[12]，基于任务和角色的访问控制模型(T-RBAC)[13]，以及被称作下一代访问控制模型的使用控制(usage control，UCON)模型[14,15]，也称 ABC 模型[16]。UCON 模型不仅包含了 DAC，MAC 和 RBAC，而且还包含了数字版权管理(DRM)、信任管理等，涵盖了现代商务和信息系统需求中的安全和隐私这两个重要的问题，因此，UCON 模型为研究下一代访问控制提供了一种新方法，被称作下一代访问控制模型。

1.1.4 访问控制分类

访问控制策略是面向应用的，可以跨越多个计算平台，可以基于最小特权、权能、认证、责任或利益冲突。访问控制策略往往是动态变化的，是随着商业因素、政府规则和环境条件的变化而发生变化的，而策略需求在系统设计时是无法完全确定的，因此系统必须按照不断变化的策略加以设计。目前一般的访问控制策略有 3 种：自主访问控制(DAC)、强制访问控制(MAC)和基于角色的访问控制 (RBAC)。

1.1.4.1 自主访问控制

自主访问控制(DAC)是一种最普遍的访问控制安全策略，最早出现在 20 世纪 70 年代初期的分时系统中，基本思想伴随着访问矩阵被提出，在 UNIX 类操作系统中被广泛使用。DAC 主要是为多用户的数据库系统设计的，系统用户改变较少，并且所有的资源都由一个实体来控制，通过用户身份或用户所属的组对客体的访问进行限制，具有主动访问资源的用户和主体有能力将信息传递给另一个主体。DAC 的核心思想是主体的拥有者通常是它的建立者，可以主动授权给其他人访问该主体，故 DAC 又称为基于主体的访问控制。

1. DAC 实现

DAC 是目前计算机系统中实现最多的访问控制机制。它的实现方法一般是建立系统访问控制矩阵，矩阵的行对应系统的主体，列对应系统的客体，元素表示主体对客体的访问权限。为了提高系统性能，在实际应用中常常是建立基于行(主体)或列(客体)的访问控制方法。基于行的方法是在每个主体上都附加一个该主体可以访问的客体的明细表，有 3 种实现形式：权能表、前缀表和口令。基于列的自主访问控制是对每个客体附加一个可访问它的主体的明细表，有两种实现形式：访问控制表(ACL)和保护位，其中使用最多的是访问控制表。