基于C/S和B/S模式的应用系统安全机制的设计

周　庆　甘仞初　李洪磊（北京理工大学经济与管理学院 100081）

摘要：随着电子商务的兴起，Internet技术的广泛应用，基于C/S和B/S混合模式的应用系统安全问题受到人们更多的关注。本文结合应用系统的功能设计、数据库表结构设计和界面设计，探讨了基于C/S和B/S模式的应用系统的安全机制问题。采用PowerBuilder7.0和ASP技术，开发了相应的安全控制功能模块，并将其运用在实际的系统开发中。

关键词：Client/Server　Browser/Server　应用系统安全中图分类号

1　系统安全层次结构

清华大学胡道元教授提出了网络安全分层理论，根据ISO七层网络协议，将网络系统安全划分成两个层次：网络层安全和应用层安全，包括物理层信息安全，链路层的网络数据安全，网络层的路由安全和访问控制，操作系统访问控制的安全和对应用服务的审计，以及应用层的应用平台的安全和应用系统的安全等内容。

应用层安全是建立在网络层安全基础之上的，主要是管理和控制用户对信息资源和服务资源的使用。其中应用平台安全是指：建立在网络系统之上的应用软件服务的安全，如数据库服务器、电子邮件服务器、Web服务器等的安全。其安全性主要表现在用户和服务器间的双向身份认证以及信息和服务资源的访问控制，一般可采用SSL等技术来增强应用平台的安全性。而应用系统的安全是指：为用户提供业务处理服务的应用软件系统的安全，包括对使用应用系统资源的用户的身份认证，用户的访问权限控制，以及应用系统功能使用情况审计等。[1]

2　应用系统安全设计

随着网络信息技术的发展，电子商务的兴起，Internet技术的广泛运用，将浏览器/服务器(Browser/Server)模式和客户机/服务器(Client/Server)技术结合起来，充分利用B/S模式的跨平台优势和C/S技术强大的企业级业务处理能力，为企业提供及时、准确的信息支持，成为当前应用系统开发的必然趋势。因此，基于C/S和B/S混合模式的应用系统安全成为一个十分重要的问题。

2.1 功能设计

应用系统的安全机制包括授权访问控制，统一的身份验证机制，对用户访问对象操作的审计和记录机制，数据通信的安全机制等。应用系统的安全与系统设计和系统实施密切相关，特别是在B/S模式下，应用系统需调用相互关联的各个Web网页来实现业务处理过程，而每一个Web网页是作为独立的文件存放在服务器上的，如何保证授权用户对指定Web页面的访问控制，以及保证业务处理过程中所需调用的Web页面的连续性，是基于Web的信息系统设计所必需考虑的问题。为实现基于C/S和B/S模式的安全控制，需设计以下相关功能模块：用户信息管理，用户授权管理，应用系统日志管理，基于C/S模式的用户登录验证、用户修改密码功能和用户操

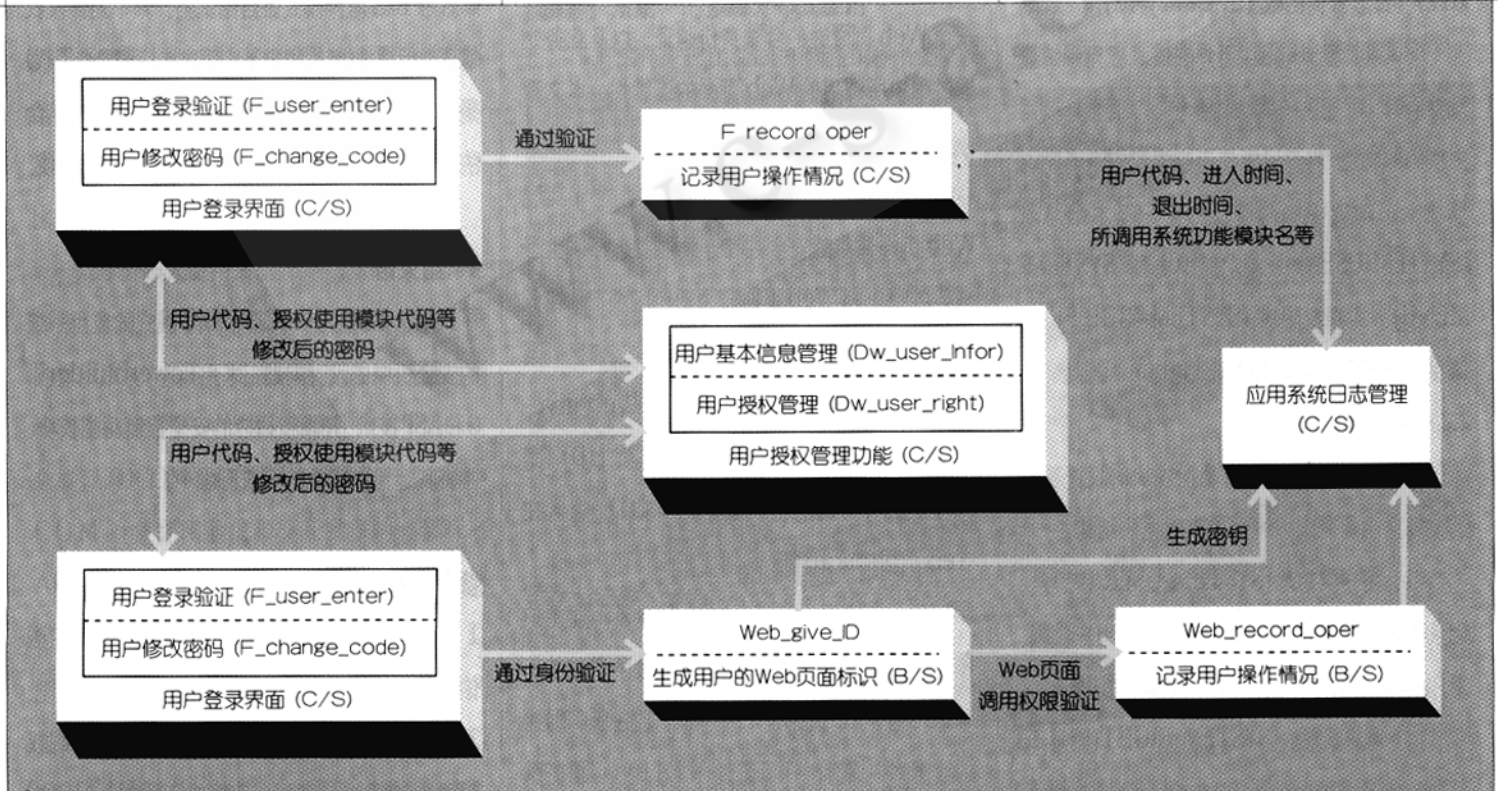

图1 功能关联图

作情况记录功能，以及基于B/S模式的用户登录验证、用户修改密码功能和用户操作情况记录功能、Web网页业务处理连续性控制功能等。各功能模块之间的联系如图1所示：

(1) 用户信息及授权管理：对系统用户的基本情况（用户名、用户密码、隶属单位、权限级别等）进行维护；并对每个用户名进行授权，使各用户只能使用对其授权的某些系统功能。该功能模块需涉及到用户基本信息表（SYSTEM-USER）、系统功能模块表（SYSTEM-MENU）、用户权限表（SYSTEM-RIGHT）；需调用用户信息数据窗口（dw-yhxx）、用户授权控件（tv-give-right）等。

(2) 系统日志管理：跟踪记录各用户对应用系统所进行的操作，记录其使用过的系统功能模块、进入时间、退出时间等。该功能模块需涉及到用户基本信息表（SYSTEM-USER）、系统功能模块表（SYSTEM-MENU）、系统日志表（SYSTEM-LOG）；需调用系统日志函数（uf-xtrz）、日志查询函数（uf-query-rz）。

(3) 用户登录验证：用户在进入应用系统登录界面时，可在系统确认其身份后，拥有修改用户密码的功能；用户只能使用被授权的系统功能模块。该功能模块需涉及到用户基本信息表（SYSTEM-USER）、系统功能模块表（SYSTEM-MENU）、用户权限表（SYSTEM-RIGHT）；需调用用户权限验证函数（uf-right）。

2.2 数据表结构设计

在完成应用系统安全功能模块的设计基础上，根据功能需求，设计如下数据表结构：

(1) 用户信息表[SYSTEM-USER（略）]：记录系统授权用户的基本信息，包括用户代码、用户名称、用户单位、用户权限级别等。

(2) 用户权限表[SYSTEM-RIGHT(略)]：记录授权用户所能调用的系统功能模块代码及名称等。

(3) 系统功能模块表[SYSTEM-MENU(略)]：记录应用系统各功能模块的基本信息，包括功能模块编号、子系统代码、功能模块名称、Web环境中的链接地址等。

字段名称	中文含义	类　型
MY	密钥	Varchar(256)
YHDM	用户代码	char(7)
DWBH	单位代码	char(10)
RQ	日期	Date
YHXM	用户姓名	char(20)

表1　SYSTEM-KEY密钥表

(4) 子系统代码表[SYSTEM-SUB-SYSTEM(略)]。

(5) 日志表[SYSTEM-LOG(略)]：记录用户对系统功能的使用情况，包括用户代码、进入时间、退出时间、系统功能名称等。

(6) 密钥表[SYSTEM-KEY(表1)]。

2.3 界面设计

应用系统的界面设计应考虑到具体的业务处理过程，考虑到授权用户调用系统对象的连续性和安全性，特别是B/S模式下，授权用户调用每一个Web页面时的合法身份验证，以及业务处理过程中所调用的Web页面的连续性。本文着重探讨B/S模式下的界面设计。

在B/S模式的Web页面设计上，为了实现Web页面调用的安全性和连续性，选择采用了框架技术，将Web页面分为四个区域：系统标识、菜单栏、按扭功能区、业务处理工作区。当授权用户通过身份验证后，即调用Web-give-ID功能函数产生一个256位的随机值（ID），同时存入服务器端的密钥表中，并将ID隐含在Web页面的菜单栏区里。

每一个授权用户每一次登录，以及不同用户登录时，由Web-give-ID功能函数所产生的一个256位的ID值都是不一样的，且在服务器端的数据库中保存时间不超过一个小时（可根据系统用户要求调整ID值保存时间的长短）。当用户调用不同Web页面进行业务处理工作时，系统会根据表明用户身份的用户代码和密码值（利用Session对象在不同网页中进行传递），菜单栏中的ID值，以及数据库中的用户代码和ID值进行三方验证，从而保证了授权用户对Web页面调用的合法性、有效性、安全性和连续性。

3　应用实例

陕西东盛医药销售有限责任公司是一家大型医药销售及新药的开发企业，公司为了实现对客户和销售业务的有效管理，对远程销售信息进行实时控制，提出开发远程销售信息管理系统，希望通过Internet将销售合同、客户信息、发货信息、回款信息等及时准确地汇总到公司总部，从而达到优化流程、降低销售成本、提高工作效率的目的。该系统基于Client/Server和Browser/Server两种计算模式，采用ASP技术和PowerBuilder7.0开发相应的业务处理功能模块，以及应用系统安全控制功能模块，充分发挥C/S和B/S两种模式各自的优势。其中用户授权管理功能模块(包括用户基本信息维护和用户授权)是基于C/S模式，采用基于角色和基于功能相结合的授权机制，使得授权操作简单易行、灵活方便。

4　结束语

本文探讨了基于C/S和B/S模式的应用系统的安全机制的设计问题，采用Powerbuilder7.0和ASP技术，开发了相应的安全控制功能模块，并将其运用在实际的系统开发中。

参考文献

1 胡道元，信息网络安全模型与安全平台，中国信息导报[J]，2000　No.8。

2 陈锦刚、顾利珉、谢剑英，管理信息系统权限管理的探讨与实现，计算机工程[J]，2000 NO.3。