电子政务资源安全管理的研究与应用

张球河,李也白,王宇鸽,尹天明
(北方工业大学 信息工程学院,北京 100041)

摘 要:随着计算机和网络技术的发展,电子政务已经成为时代的必然,电子政务安全也随之成为人们关注的焦点。电子政务安全应该从物理层、网络层、系统层、应用层上总体考虑。文中从应用系统角度出发对电子政务资源安全管理进行了研究和探讨,主要分析、研究了身份认证和访问控制这两层安全服务,并给出了相应的基于J2EE的系统平台设计方案。该方案应用到了某工业局电子政务系统当中,达到了用户的安全需求,整个系统实现了较为灵活的安全配置和控制。

关键词:电子政务;安全;身份认证;访问控制
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2006)09-0222-02

Research and Application of E-Government Resource Security Management

ZHANG Qiu-he, LI Ye-bai, WANG Yu-ge, YIN Tian-ming
(College of Information Engineering, North China University of Technology, Beijing 100041, China)

Abstract: With the development of computer and network technology, E-government becomes necessity of the epoch, and its security is becoming focus of people. The E-government security should be researched from 4 ties, the physical, network, system and application. The paper studies the E-government resource security management from the applied system, mainly about the user authentication and access control. It gives the corresponding solution project based-on J2EE. The solution had been applied in an E-government system of an industrial bureau, it meets to the user's requirement, and implements the flexible secure configuration and control.

Key words: E-government; security; user authentication; access control

0 引 言

电子政务(E-Government)是一个将政府工作标准化、政府工作服务化、政府工作信息化、政府工作网络化、政府工作公开化的系统工程。

目前,关于电子政务安全性的研究已有很多,但很多都集中在网络安全、主机安全、数据安全和备份,以及病毒防治等方面,关于电子政务应用层的安全则没有很好的论述和解决方案。应用层安全是在应用程序内部执行访问控制原则,以阻止和侦测未授权的访问,确保应用程序只用于预定的目的,只被适当的用户使用。因此,在一定的安全基础设置具备的条件下,进行电子政务应用层安全的研究与应用是很有必要的。

1 应用系统安全服务模型

安全体系从整体上定义信息系统所提供的安全服务和安全机制以及系统元素间的关系和交互。以下主要从安全服务上入手考虑电子政务应用系统安全。

安全服务是一个系统各功能部件所提供的安全功能的总和,从协议分层的角度看,底层实体为上层实体提供服务,而对外屏蔽安全服务的具体实现。开放系统互联参考模型(OSI/RM)中提出了一个概念性安全体系结构框架,定义了5组安全服务:认证服务、保密服务、数据完整性服务、访问控制服务、抗抵赖服务。

应用系统安全体系的安全服务包括通信双方的身份的标识与认证;主体的授权与访问控制;数据存储与传输的完整性;数据存储与传输的保密性以及抗抵赖服务。各种安全服务之间存在相互依赖的关系,单独采用其中的一种安全服务是无法满足需要的。这些安全服务之间的关系可以看成是一种层次关系,如图1所示[1]。在应用系统中,所有安全服务的实现都依赖主体与客体的身份标示和认证,所以身份认证处于安全服务模型的最低层;访问控制是整个安全系统的核心,其目标是防止对任何资源进行非授权的访问,它在身份认证的基础之上为完整性服务、保密性服务和抗抵赖性服务提供安全保障;数据的完整性和保密性确保数据在流通中不被窜改和窃取,它们是认证和访问控制有效性的重要保证;抗抵赖是在其它安全服务的保障下,在接收方收到完整、保密的数据信息之后才会

收稿日期:2005-11-15
作者简介:张球河(1981-),男,浙江台州人,硕士研究生,研究方向为电子政务、WEB信息系统、数据库;李也白,硕士生导师,研究方向为电子政务、电子商务、数据库技术。

涉及到的,所以抗抵赖性服务处于整个安全服务模型的最顶层。

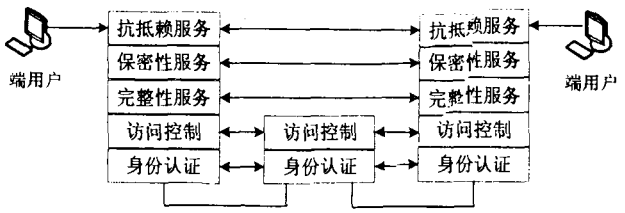

图 1　安全服务层次模型

2　基于 J2EE 的电子政务资源安全管理设计方案

2.1　设计目标

本研究针对某工业局电子政务系统的具体应用。该工业局电子政务系统分为内网、外网和公网 3 部分,每部分的安全性都不同,如图 2 所示。内网处于最内层,公网处于最外层,随着图中箭头所示方向,安全性要求越来越低。内网主要为工业局的内部办公系统,安全性要求最高;外网为工业局和其他政府部门之间的协同办公,以及同企业之间的业务系统,安全性要求次之;公网主要是针对公众提供各类信息服务,安全性最低。

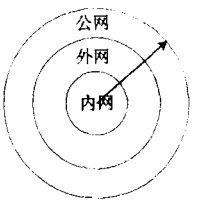

图 2　三网安全层次示意图

根据图 1 安全服务模型和实际的系统应用,电子政务资源安全管理平台必须提供安全服务模型中提出的各种服务,才能保证电子政务系统的安全运行。结合系统应用的实际情况,具体对身份认证、访问控制、权限管理、安全审计、数据加密等方面进行研究和设计实现。其中权限管理包括了用户管理、角色管理、资源管理、角色分配和资源权限分配等。

2.2　总体设计

根据系统的需求及实际的条件,采用 Windows2000 Server + Bea Weblogic + Oracle 9i 作为整个系统的开发、运行环境,结合 J2EE 架构的优势和系统的功能需求,提出了如图 3 所示的基于 J2EE 架构的系统软件结构图。

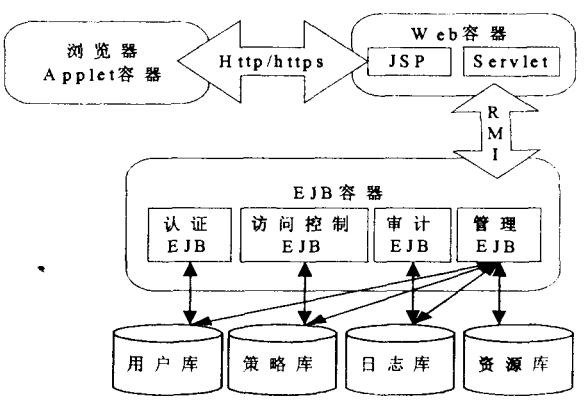

图 3　系统软件结构图

从图 3 可以看出,J2EE 提供了从客户端到应用服务器、EJB 和数据库端的解决方案的技术支持。整个应用安全系统主要基于 JSP 和 EJB 技术实现,通过实体 EJB 来封装对数据库的访问操作。认证 EJB 主要实现对用户身份的认证,确认和获取用户身份信息;访问控制 EJB 根据策略库控制用户对系统资源的访问,采用基于角色的访问控制 RBAC 模型;审计 EJB 实现对用户访问操作的跟踪记录,并用于分析系统是否存在信息泄漏等安全问题;管理 EJB 实现用户身份管理、资源管理、授权管理、日志管理等,对身份认证、访问控制及安全审计提供支持。

2.3　详细设计

根据电子政务资源安全管理的设计目标和总体设计,提出了如图 4 所示的功能模块结构图。

由图 4 可以看出,身份认证模块、访问控制模块和安全设计模块在用户访问系统期间是实时运行的,用于验证用户身份、防止用户执行非法操作,保证系统的运行安全。授权管理模块主要实现后台的安全管理,对身份认证模块、访问控制模块和安全设计模块提供支持。加/减密模块对整个系统运行过程中数据信息的传输和存储提供保密性安全服务,保障信息的完整性和保密性。

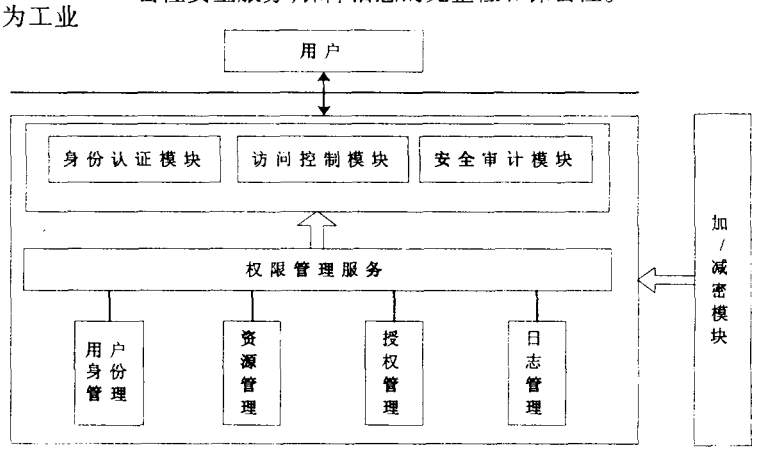

图 4　模块结构图

功能模块的详细信息如下:

(1) 身份认证模块。

在用户的登录系统时,确认用户身份,验证用户身份的合法性,防止非法用户的访问,然后才能实现对于不同用户的访问控制和记录。在本系统中采用了一次性口令技术实现用户的身份认证,具体应用一次性口令中的挑战/应答机制来实现一次性口令认证[2]。

(2) 访问控制模块。

访问控制实质上是对资源使用的限制,决定访问用户是否被授权对某资源的执行某种操作。文件、数据库、应用程序等都是资源,本系统主要是针对 B/S 系统的功能资源,采用基于角色的访问控制模型来实现对用户的访问控制[3]。在实际应用中,用户身份认证通过后,访问控制模块获取用户的当前角色、资源及访问所需的操作权限,根据授权管理设定的访问控制策略来判定用户的访问是

(下转第 226 页)

2.2 拉式模型分析

与推式模型相比,该拉式模型有明显的优点:

(1)在推式模型中,CAS服务器是单一的、集中式的服务器,一旦出现故障将导致整个社区内的所有资源因用户无法获取包含CAS服务器权限签署的代理证书而拒绝提供服务;而在拉式模型中增加多个从属分布式的缓存服务器,大大提高了CAS服务的可靠性,同时也可以将对虚拟组织权限管理与权限查询应答分离开来,大大提高了CAS服务器的运行效率和性能。

(2)在拉式模型中由资源提供者向CAS缓存服务器来获取用户的权限声明,可以节约资源相对紧张的用户的带宽开销和运行负荷,充分利用网格资源。

(3)CAS缓存服务器、CAS服务器没有被暴露在社区信任域以外,而是与资源提供者处于同一信任域中,被攻击的可能性降低,从而大大提高了CAS服务的安全性和可靠性。

(4)在推式模型中需要对X.509证书格式进行非标准的扩展,以在代理证书中嵌入权限声明;而在拉式模型中则可以直接使用X.509的标准证书格式,提高了其适用范围和通用性。

(5)在推式模型中用户需要向资源提供者提出服务请求时,总是要先登录CAS服务器获取权限声明;而拉式模型中,资源提供者先认证用户的服务请求,如果认证失败则不需要向服务器获取权限声明,大大降低了集中式CAS服务器的运行负荷,也间接提高了其运行效率和可靠性。

3 结 论

文中所提出的拉式模型很好地解决了推式模型中所存在的问题,极大地提高了使用CAS服务器进行社区授权管理的网格应用的安全性和可靠性,是一个较为优越的模型。

参考文献:

[1] Foster I, Kesselman C. The Grid 2: Blueprint for a Future Computing Infrastructure[M]. 金 海,袁平鹏,等译. 北京:电子工业出版社,2004.

[2] 徐志伟,冯百鸣,李 伟. 网格计算技术[M]. 北京:电子工业出版社,2004.

[3] The Globus Toolkit[EB/OL]. http://www.globus.org/toolkit,2005.

[4] Foster I, Kesselman C, Tsudik G, et al. A Security Architecure for Computational Grids[A]. The 5th ACM conference on Computer and Communication Security[C]. San Francisco, CA:[s.n.],1998.

[5] 都志辉,陈 渝,刘 鹏. 网格计算[M]. 北京:清华大学出版社,2002.

[6] Sotomayor B. The Globus Toolkit 3 Programmer's Tutorial [EB/OL]. http://www.chinagrid.net/grid/download/prog-tutorial-0.4.3,2003.

[7] GT 4.0: Security: Community Authorization Service[EB/OL]. http://www.globus.org/toolkit/docs/4.0/security/cas/,2005.

(上接第223页)

否合法,从而达到访问控制的目的。在系统的访问控制上实现分级访问控制策略,文献[4]提出了基于多粒度权限的访问控制。

(3) 安全审计模块。

主要用于事后的日志分析。当发生安全问题时,可以根据日志记录,分析问题并可追查事故责任人,同时可以根据访问记录和设置的规则进行安全审计分析,判断系统是否受到安全威胁。

(4) 授权管理服务。

为身份认证模块、访问控制模块和安全设计模块提供支持,包括用户身份管理、资源管理、授权管理、日志管理。用户身份管理包括用户信息管理、角色信息管理及用户角色的分配;资源管理包括系统功能模块、数据库资源、其它数据资源等信息的管理;授权管理实现将不同资源的访问权限授给不同的访问角色,间接实现对用户的授权;日志管理就是对应用系统的日常访问记录进行管理、维护和分析。

(5) 加/减密模块。

加/减密模块为系统中的重要数据提供保密服务,保证数据的传输和存储安全,采用MD5、AES等算法实现数据的加密[5]。

3 总 结

从应用系统角度出发对电子政务安全管理进行了研究和探讨,并给出了相应的基于J2EE的系统平台设计方案。该方案应用到了某工业局电子政务系统当中,取得了一定的效果,达到了用户的安全需求,整个系统实现了较为灵活的安全配置和控制。同时该方案具有一定的普适性,也能应用到其它的电子政务系统当中。

参考文献:

[1] 宋宇波,胡爱群. 电子政务安全体系结构的探析[J]. 计算机工程,2003,29(10):12-13.

[2] 张 宏 陈志刚. 一种新型一次性口令身份认证方案的设计与分析[J]. 计算机工程,2004,30(17):112-113.

[3] 黄 凯,陈 云,阎如忠,等. 基于角色的B/S系统访问控制的研究与应用[J]. 计算机工程与应用,2003(20):228-229.

[4] 叶春晓,符云清,吴中福,等. 基于多粒度权限的访问控制[J]. 计算机应用研究,2004(10):87-88.

[5] 李海燕,徐汀荣. 基于BS的电子政务系统中信息加密技术的设计与实现[J]. 苏州大学学报,2004,24(6):46-47.