基于分级保护的 OA 系统应用层访问控制

张天白　王　晶*
(北京化工大学 信息科学与技术学院, 北京　100029)

摘　要: 本文着眼于一个涉密信息系统的建设角度,在应用层访问控制上深化分级保护的思想,并提出了合理的解决方案。系统采用 C/S 与 B/S 相结合的结构,引入主客体分级保护和部门属性,来改进基于角色的访问控制以实现用户和权限的分离、并采用管理员角色分权制衡、系统数据库的综合审计和对审计日志的分布式存储等技术手段,实现了应用层上的分级保护访问控制。这些方法充分体现了将系统访问控制环节的对象差异化,对重点对象进行重点防护和特殊对待的分级保护思想。该方法能够使目前涉密信息系统的安全性得到有效提升,充分保护其系统的安全。

关键词: 分级保护; 涉密 OA 系统; 基于角色的访问控制; 访问审计
中图分类号: TP393

引　言

随着计算机技术和通信技术的快速发展,计算机及其网络成为泄密的重要渠道和被攻击的目标。涉密 OA 系统的建设过程中,《涉及国家秘密的信息系统分级保护技术要求》和《涉及国家秘密的信息系统分级保护管理规范》是主要遵循的标准[1]。访问控制作为信息系统保护框架中的核心措施之一,在标准和法规中始终贯穿了分级保护思想,如对物理层和网络层边界环境的访问,应按安全域等级或风险分析得到的安全需求,选择不同力度的措施进行保护。在系统应用层的层面,现有系统多是针对具体的某个薄弱点,从软件技术上组织局部安全策略,控制措施无法形成系统化的合力以保证控制的粒度。

本文以工作中涉及国家秘密的 OA 系统为研究对象,探讨在应用层访问控制设计过程中分级保护思想的应用,并给出了一个以 Oracle 9i 和 IBM Domino/Notes 为数据库工具构建的典型 OA 系统的应用层访问控制的模型。模型涉及具体设计措施包括:采用 C/S 和 B/S 二元体系结构来适应复杂的网络环境;采用改进的基于角色的访问控制策略(RBAC)使用户与权限的关系清晰灵活,并结合对主客体的分级设置克服了传统 RBAC 的一些缺陷;管理员三权分立与审计有效解决了其权限过大对系统的威胁;数据库的综合审计及对审计日志的分级存储处理,为包括管理员在内的所有用户的操作问责提供了有效依据。

1　系统体系结构

从系统的整体结构上来看,涉密系统采用数据层、逻辑层和表现层的三层软件体系架构,同时根据管理员和普通用户的不同需求,将逻辑层放在客户端或服务器端,即采用 Client/Server 和 Browser/Server 混合的架构,简化了网络应用的开发与运行维护,如图 1 所示。

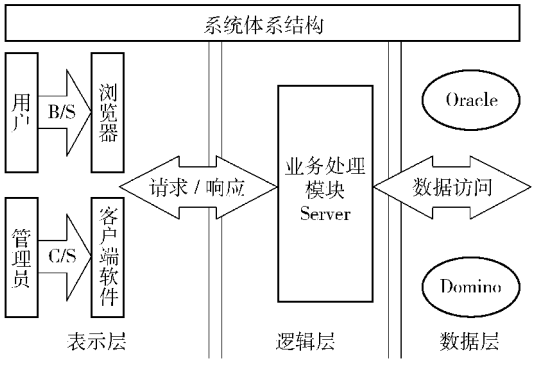

图 1　系统体系结构

Fig. 1　Architecture of the system

以往的信息系统包括涉密系统多采用单纯的 C/S 或 B/S 系统,使程序难以适应复杂的网络环境,网络配置和应用模式死板,不可避免地会因网络功

收稿日期: 2010-07-12
第一作者: 男,1984 年生,硕士生
* 通讯联系人
E-mail: jwang@ mail. buct. edu. cn

能与安全策略冲突而产生漏洞。系统开发技术人员多争执于两种架构的优劣比较,对某一系统具体安全需求的分析却不足。相比于一般信息系统,涉密办公类信息系统又有其特殊的情况和需求。涉密系统多在一个封闭的环境中,为固定群体提供服务,具有对权限多层次校验,处理用户面固定且对用户要求高、安全需求层次高等特点,迎合了 C/S 结构的专长,因而 C/S 结构可被系统中数据维护人员、专业分析人员等管理员类角色使用;而另一方面,对系统中其他的一般工作人员,Browser/Server 又可以灵活建立在广域网的基础上,降低对客户端操作人员和操作环境的要求,简化网络开发与运行维护的成本。因而在系统开发中,可以采用一种基于 C/S 与 B/S 混合的架构,再依据系统的具体需求加以细节变化。

2 应用层访问控制策略

安全访问控制策略提供了分配用户访问权限的依据,从而截断破坏系统与泄密数据的途径。按照安全访问控制策略授予的用户权限,应是用户能完成其工作的最小权限集合。访问控制模型应能够准确表达和分析系统访问控制策略,有效监控资源访问活动,仅授权用户在合法的时间内才能获得有效的访问权限,从而防止非法入侵和泄密数据。系统中访问控制主要集中于物理层,网络层和应用层三个层次,本访问控制模型定位于应用层,改进了基于角色的访问控制机制,实现用户与访问权限的分离,构建可靠、安全的访问构架。

2.1 改进基于角色的访问控制

在涉密信息系统中,安全管理工作较为复杂,一般包括大量不同敏感程度的信息和各种访问需求的用户。系统采用基于角色的访问控制模型(RBAC),并引入信息主客体分级加以改进,防止越权。

RBAC 包括以下几种对象:(1)用户,一个可以独立访问计算机系统中的数据或者用数据表示的其它资源的主体;(2)角色,系统中具有某一种或多种权限的对象,权限和角色本身都可以增加和删除;(3)权限,对计算机系统中的数据或者用数据表示的其它资源进行访问的许可。RBAC 的方法是安全管理人员根据需要定义各种角色,并设置合适的访问权限,而用户根据其责任和资历再被指派为不同的角色。这样,整个访问控制过程被分成两个部分:即访问权限和角色相关联。角色再与用户关联,从而实现了用户与访问权限的逻辑分离[2],并通过分配和取消角色来完成用户权限变化,给出静态与动态授权约束。

但基本的 RBAC 方法也存在着两个常见问题:(1)较大主客体系统运行时的控制粒度;(2)系统中客体交换缺少限制。

本模型从系统建设的角度出发,对第一个问题的解决方法为:用户除关联带有固定权限级别的角色外,再附加部门参数(或系统应用单位依据实际情况,自定一个相同组织结构意义的参数)。

除了非密公告性信息,一个部门内信息即使其密级低于外部门一个业务不相关人员的密级,该消息也不能为此人所访问;对需要部门间协同的工作中的信息流转,应在对应的部门内建立专门的人员传递通道。人员无法访问的信息,不仅包括“由于密级不够而不能访问”的信息,也包括“由于业务无关而不必访问”的信息。这样既有力地规范了信息的流向,减小了人员的可能知悉范围,反过来又在人员的工作中增加了其所接触信息的有效性,减小了人员的工作负担和差错率。为适应单位内偶尔的部门成立、撤销和整合,系统提供专门的模块用来设置组织部门。在新设定的部门内对角色进行增减,从权限表为其赋予合适的权限。

RBAC 系统实现了用户与访问权限的逻辑分离,清晰描述了角色层次关系,而部门参数的引入减小了信息控制的粒度,提高了系统的效率。该系统易于进行多用户多级别的权限管理,保护工作流中的应用数据不被非法浏览或修改。在主客体分级保护的轮廓内,每个用户只能访问和操作其所在部门内、不高于自己密级的信息,只能在与本身工作直接相关的主体范围内接受和流转信息。实现了最少权限原则——这也是涉密系统工作的基本原则之一。结合用户登录鉴别和审计机制,构成了可靠的安全访问框架,如图 2 所示。

而 RBAC 存在的另一个问题,可以通过客体的存储分级保护来解决。

国家法规规定,按照主体类别、客体类别进行涉密信息和重要信息的访问控制[3]。本模型设计了主客体分级结构,做到主体控制到具体用户,客体控制到信息类别,如图 3 所示。

每个主体和每个客体都必须明确其对应的分级项,作为其必要的标记属性。系统从“密级”和“职

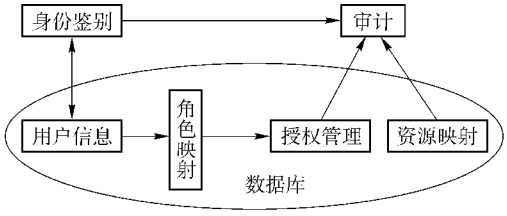

图 2　信息访问框架

Fig. 2　The information access framework

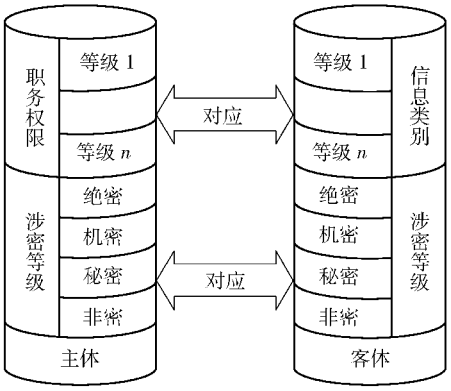

图 3　主客体分级对应

Fig. 3　Subject-object correlation

务—类别”两个角度控制重要信息的访问，限定哪些信息可以为哪些用户使用。系统中信息客体按密级从低向高分为非密、秘密、机密、绝密，对应的信息主体也分为非密、秘密、机密、绝密。引入传统强制访问控制的思想，确保密级信息的知悉范围，杜绝高密信息流向低密人员的现象和工作流中低密级用户收发高密级文件。每个用户只接触自己被授权范围内的信息。

系统同时采用对信息客体按密级不同存放在不同数据库服务器节点的措施，对各密级服务器采取专门的不同强度的保护，降低数据存储的风险。信息分布式分级存储还将应用于审计日志，后文中将讲述。同时阻止不同密级服务器节点间的数据交换，缓解了 RBAC 中“访问过程中产生的客体间信息流可能因为不明确的信息流控制方法导致用户获得非法数据”的结构缺陷问题[4]。

2.2　管理员角色管理

访问主体中的管理员是个特殊的用户群体，拥有特殊的操作权限，可能造成大规模的破坏和泄密。针对管理员问题，本模型设计了专门的集中管理与分散管理相结合的措施。设立 3 种管理员角色：即系统管理员，保密员和审计员，控制系统安全的不同方面。具体的管理员角色划分及职能描述见表 1。对于初始化系统，增加、修改和删除管理员等特殊环节，设置“超级管理员”角色，平时将其严格控制为关闭状态。超级管理员密码分为 3 部分，交 3 种管理员角色分别保存，需要该角色启动时，要 3 部分角色在场同时应用密码。

表 1　管理员角色划分

Table 1　Division of administrator roles

名称	职责及工作描述
系统管理员	1. 负责新流程开发，配置、维护，管理业务流程； 2. 负责用户的注册、删除，生成用户标识符，保证用户标识符在 OA 系统生命周期的唯一性； 3. 负责组织机构的变动调整，负责与用户权限相关的各类角色的设置
保密员	1. 负责人员涉密等级和职务等信息调整和用户权限的分配； 2. 负责保管所有除系统管理员以外的所有用户的 ID 标志符文件。安全保密管理员不能以其他用户身份登录系统； 3. 不能查看和修改任何业务数据库中的信息
审计员	1. 负责监督查看系统审计日志，但不能增删改日志内容； 2. 负责监督查看系统管理员、安全保密管理员和安全审计管理员的操作日志，但不能增删改日志内容； 3. 负责查看用户的审计记录，不能修改和增加、删除审计日志内容； 4. 负责定期备份、维护和导出日志

由于管理员身份的特殊性，应用系统的安全在很大程度上取决于管理员系统的优劣。本系统采取的“三权分立”既避免了片面的集中管理方式的缺乏监督和不可控性，也避免了单独的分散管理方式的分权漏洞和协调一致问题。

3　访问审计机制

为了能够追踪用户对系统操作的历史，模型广泛引入了审计机制。除了用户登录时记录计算机 IP 地址，MAC 和用户名外，该模型还强化了资源映射即数据库应用的审计，将对数据库做的全部修改记录在日志文件中。审计记录包括事件时间，类型、主体、客体和操作等，供审计管理员定期审计。数据库审计策略保证了对数据库的操作始终在有监控的条件下进行，当出现了重大的涉密业务办理失误或蓄意的失泄密事件，需要进行责任追查认定时，数据库审计可以提供有力的审计证据。

3.1　数据库访问审计

由于数据库直接保存了系统的数据信息，更容

易受到外部非法入侵,修改和破坏,其造成的后果也更直接更严重,系统其他的一些审计功能也需要数据库审计来辅助实现,所以信息系统开发首选成熟的数据库产品。模型以关系型数据库 Oracle 9i 和文档型数据库 Domino/Notes 为例进行说明,具有较高可靠性,可控性和可追踪性。

3.1.1 Oracle 审计日志

Oracle 的物理数据库结构包括数据文件,日志文件,控制文件。其中日志文件组用于收集数据库日志。该系统开启了 Oracle 9i 的 Auditing 审计特性,通过三种措施实现对数据库系统的操作的记录和对特定业务数据表(如日志)的控制,见表 2。

表 2 Oracle 审计措施

Table 2 Audit of Oracle

审计措施	说明
语句级	审计某种类型的 SQL 语句,记录创建、丢弃等表操作
权限级	审计某一系统权限的使用状况,包含大部分的对数据库对象的数据定义语言操作
实体级	监视所有用户对某一指定用户表的存取和更新状况

语句级、权限级和实体级审计记录保存在系统视图里,控制普通用户对审计记录的访问权限,禁止其在该表中进行操作。通过日志代理程序将日志文件按其审计内容的不同分开存放,由审计员进行定期对日志导出归档。利用 Oracle 的审计功能监视和记录数据活动,可以方便的收集数据库操作信息和用户信息,以备查用。

3.1.2 Domino 审计日志

Domino/Notes 是当今比较流行的协同群件系统,在网络管理和服务器管理方面具有公认的高安全性,是建立 OA 系统可靠的选择。办公网络中协作是靠工作流技术来实现的,即工作群组中为达成某一个共同目的,而需要多人协力,以循序或平行工作的形式来共同完成的任务[5]。

本模型的 Domino 安全性管理中,协作网络的各种工作流都加入了记录审计信息功能,系统自动将用户的登录,操作,管理等状态记录到审计模块中。将生成的审计日志存为特定表单,日志只有管理员可读,且对日志的修改和删除按照对管理员角色的细分来严格控制,这样以审计日志的形式加强了系统的安全。操作日志审计内容如表 3。

表 3 Domino 审计项

Table 3 Audit of Domino

中文名称	域名	说明
日志序号	logNo	记录当天访问次序
时间	Logtime	登录日期及时间
人员	Loguser	访问人员 ID
操作类型	Logtype	新建、删除、修改、查看、办理、检索、统计
访问的数据库	Logdatabase	数据库名称
访问 IP 或 MAC	LogIPorMAC	访问者的 IP 地址或者计算机的 MAC
访问信息	Logbz	备注信息(文档 ID)

3.2 审计日志存储

为加强审计日志特别是高密级数据操作日志的安全,模型对日志采用分布式安全管理方法。该方法采用日志代理、管理网关和多服务器节点,对日志记录进行完整性验证、级别检测和分布式存储。日志代理采用实时抽取方式将日志发送到管理网关。管理网关主要完成日志的暂时接收存储,按设备管理日志对应的安全域级别、Oracle 和 Domino 审计日志对应的被审计数据表和公文的密级进行检测,在服务器节点进行日志的存储和审计员分析,如图 4 所示。这样,不同级别的审计日志,连同不同级别的工作数据(公文),被存到了不同级别的数据库服务器节点中,也有利于按级别对数据库服务器采用不同的外部保护措施。

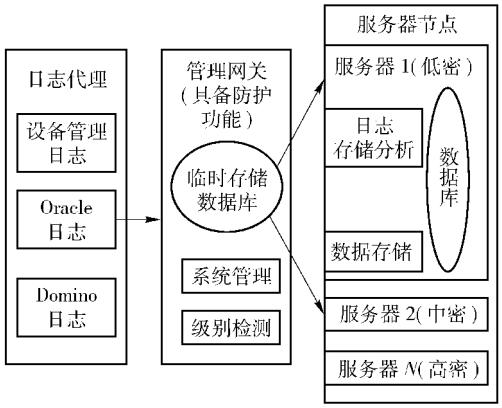

图 4 用户日志存储

Fig. 4 Storage of user logs

针对 3 种管理员角色的用户,系统管理员和保密员在系统内的任何操作都有审计日志,日志存入较高级别的服务器。他们可以查看普通用户的审计记录,但不能修改、增加和删除审计日志内容。审计员负责监督查看系统管理日志、其他两种管理员的操作日志和普通用户的操作日志,但不能对这些日

志修改和删除。系统提供审计信息导出工具，由审计员导出审计日志文件，并存储在其他位置。对于已导出的审计信息，审计管理员可以进行清除来节省服务器成本。审计信息的导出和清除操作也产生审计日志，存入较高级别服务器，特别的，该审计信息不允许修改删除。

4　结论

本文针对信息系统应用层访问控制中的一些问题提出了解决方法，这些方法相互渗透构成了新的分级保护模型。新模型将系统环节差异化，依照对象重要程度给予差异化而高效的保护。应用层相关对象的分级保护延伸了分级保护的概念，与物理层和网络层的访问控制措施共同作用，高效率而又较低成本地实现了国家相关法规中，对安全访问控制“严禁高密低传”、“最少权限”和“既不过保护又不欠保护”的要求。

参考文献：

[1] 刘玉林，王建新，谢永志. 涉密信息系统风险评估与安全测评实施[J]. 信息安全与通信保密，2007(1)：142-144.
Liu Y L, Wang J X, Xie Y Z. A study about secret-involved information system risk evaluation and security testing evaluation[J]. China Information Security, 2007(1): 142-144. (in Chinese)

[2] Ferraiolo D F, Cugini J A, Kuhn D R. Role-based access control: Features and motivation[C]// Proc of the 11th annual computer security application conf. Washington: IEEE Computer Society Press, 1995: 241-248.

[3] 国家保密局. BMB17—2006 涉及国家秘密的信息系统分级保护技术要求[S]. 北京：中国标准出版社，2006.
Administration for the Protection of State Secret. BMB17—2006 Gradational security protection technology requirements for classified information system[S]. Beijing: Standards Press of China, 2006. (in Chinese)

[4] 于泠，陈波，肖军模. 多策略的工作流管理系统访问控制模型[J]. 系统过程理论与实践，2009，29(2)：151-158.
Yu L, Chen B, Xiao J M. Multi-policy access control model for workflow management system[J]. Systems Engineering-Theory & Practice, 2009, 29(2): 151-158. (in Chinese)

[5] 马亮，顾明. 基于角色的工作流系统访问控制模型[J]. 小型微型计算机系统，2006，27(1)：136-140.
Ma L, Gu M. Role-based access control model for workflow systems[J]. Mini-Micro Systems, 2006, 27(1): 136-140. (in Chinese)

An application layer access control model based on gradational security protection in an office automation system

ZHANG TianBai　WANG Jing

(College of Information Science and Technology, Beijing University of Chemical Technology, Beijing 100029, China)

Abstract: Nowadays the access control in a security office automation (OA) system focus on three layers of the International Standards Organization (ISO) seven-layer architecture, namely the physical layer, the network layer and the application layer. Here new methods are adopted in a model where the system architecture is composed of Client/Server (C/S) and Browser/Server (B/S), such as the improved role-based access control (RBAC) method with a correlation between the subjects and objects of the access course, the subdivision and restriction of administrator users, an integrated audit to database, as well as the distributed storage of the audit logs. Discriminating between the objects in the access control process in this way affords gradational security protection to national standards, and offers operational benefits.

Key words: gradational security protection; security OA system; role-based access control; access audit