基于Notes的OA系统的安全机制

高发桂
(湖北民族学院 信息工程学院,湖北 恩施 445000)

摘 要:设计了基于Notes的C/S与B/S相结合的混合模式办公自动化系统。充分利用网络安全技术和Lotus Domino/Notes本身所具有的身份验证、存取控制、字段级加密和电子签名等安全措施,对系统按物理层、网络层、服务器层、数据库层、设计元素和标识符等层次分别进行安全性设计,从而设计出一个能充分保证办公自动化安全的控制机制。

关键词:Notes;混合模式;办公自动化;安全机制
中图分类号:TP309;TP317.1 **文献标识码**:A **文章编号**:1673-629X(2006)09-0236-04

Security Mechanism of OA System Based on Notes

GAO Fa-gui
(School of Information Engineering, Hubei Institute for Nationalities, Enshi 445000, China)

Abstract: Mainly studies the OA system based on the Lotus Domino/Notes. The system uses the mixed model uniting C/S with B/S. It makes full use of the secure technology of the network and safety measure which Lotus Domino/Notes itself has, such as identity recognition, access control, field encryption and electronic signature. The security is developed according to the physical layer, network layer, service layer, database layer, project element and identifiers into which the system is separated. Thereby the control mechanism designed in the paper can ensure the OA system security fully.

Key words: Notes; mixed model; OA; security mechanism

0 引 言

办公自动化(Office Automation,OA)是将现代化办公和计算机网络功能结合起来的一种新型的办公方式,是当前新技术革命中一个非常活跃和具有很强生命力的技术应用领域,是信息化社会的产物。通过网络,组织机构内部的人员可跨越时间、地点协同工作。通过OA系统所实施的交换式网络应用,使信息的传递更加快捷方便,从而实现了办公的高效率。作为政府或企业的办公承载体,OA系统上的各种文件都在不同程度上涉及国家各行业的秘密,安全保密控制历来很严的政务管理系统中存储和运行着邮件、公文及大量的重要数据,因此数据库及网络的安全性是极其重要的。Lotus Domino/Notes本身具有优秀的安全机制,它提供了身份验证、存取控制、字段级加密和电子签名等安全措施,可采用身份验证来保证用户和服务器、服务器和服务器之间连接的可靠性,即使闯过防火墙也无法进入Notes系统。

1 基于Lotus Notes/Domino OA系统的设计

1.1 系统体系结构设计

传统的C/S结构的优点是网络负载均衡,传输量小,安全性好,缺点是应用程序分布在众多的客户方而引起维护的工作量大;而在B/S结构下,数据库和应用程序集中在服务器方,客户方只需安装一个简单的浏览器,这可以大大降低维护工作量,而安全性略差。本系统采用C/S与B/S模式相结合的模式。对于安全性要求较高的系统模块采用C/S结构,如公文管理、会议管理、日常办公系统、电子邮件系统等;而对安全性要求相对较低的系统模块采用B/S结构,如公共信息系统。固定的办公用户安装Notes客户端,通过客户端使用Domino资源,构成C/S结构,以便充分利用Notes的安全技术,保障办公信息的安全。

利用Noets Web Publish能力,校园网上的非办公用户可以通过浏览器浏览发布的办公信息。对这类用户一般只有浏览公开办公信息的权限。这种混合模型,既有C/S机构的严谨又不乏B/S结构的灵活性。基于上述设计思想,可以得到OA系统体系结构,如图1所示[1]。

1.2 系统主要功能设计

本系统包括公用信息、公文管理、日常事务、个人办公、会议管理、系统管理等子系统,并和教务系统做好接口。每一子系统既可独立完成某一单项办公事务,相互间又可有机结合,真正实现了无纸化的协作OA。各系统功能模块如图2所示。

收稿日期:2006-01-09
作者简介:高发桂(1964-),女,湖北宜昌人,硕士,副教授,研究方向为计算机网络安全和信息安全。

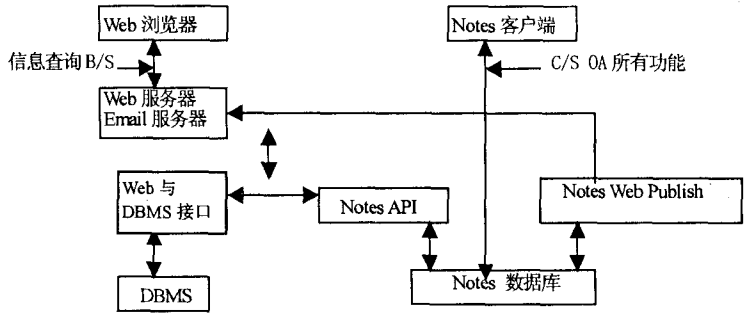

图 1　OA 系统体系结构图

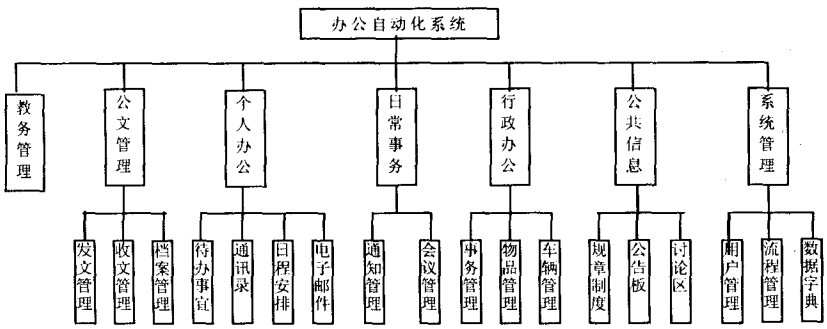

图 2　系统功能模型图

2　OA 系统安全机制的设计

2.1　系统安全设计原则

根据高校 OA 系统现实存在的安全问题,在系统总体设计中,为了满足学校办公的可靠、机密等要求,内部办公系统采用 C/S 结构,充分利用 Notes 自身的安全机制(可靠而且编程负担轻);在面向全校远程访问的信息化方面(如各类查询系统等)采用基于 Web 的 B/S 结构。本 OA 系统安全策略主要遵循适应性、动态性、简单性、系统性和最小授权等原则。

2.2　系统安全控制机制设计

为了保证系统信息安全以及文档数据库的安全,可以把安全性看作由几层[2,3]组成:用户或服务器一旦通过安全性的一层后,就执行安全性的下一层。本 OA 系统分为物理层、网络层、服务器层、数据库层、设计元素层和标识符层。根据用户的不同应用需求,制定不同的安全策略。根据这些安全策略,在不同层次上建立和设置了一套完整的安全控制机制模型(如图 3 所示)。

安全控制机制	标识符	口令、访问权限	
	设计元素	域:加密、折叠区域、印章隐藏	打印文件控制 禁止屏幕拷贝
		文档:读者和作者权限控制、匿名控制	
		表单、视图:使用存取列表、视图存取列表、特定域	
	数据库	目录链接存取、数据库存取控制列表、加密、签名	
	服务器	服务器存取控制权限、授权、匿名存取、公钥比较、口令检查、交叉验证	
	网络	双网卡、防火墙、VPN(网络隧道)、操作系统平台安全	
	物理	环境安全、设备安全、介质安全	

图 3　系统安全控制机制

2.3　系统安全控制模型

2.3.1　物理层安全性

在物理上保护服务器和数据库的安全性与禁止未授权的用户和服务器访问一样重要。因此,所有 Donimo 服务器放在通风、安全的区域,例如:一个上锁的房间。如果服务器不安全,则未授权用户可能绕开安全性功能(如存取控制列表设置)并访问服务器上的应用程序、使用操作系统拷贝或删除文件、或物理损坏服务器硬件本身。

2.3.2　网络层安全性

网络安全性防止未授权用户闯入网络并假扮 Notes 授权用户,以及防止他们偷听 Domino 系统所在的网络。通常使用网络硬件和软件或通过加密控制网络访问。偷听仅在事务未被加密时发生。因此要防止偷听,应加密所有 Domino 和 Notes 事务。加密网络端口,防止未授权的用户使用网络协议分析器读取数据。使用 Notes 端口加密功能加密网络传输,如果使用 Internet 协议,则通过 SSL 进行加密。具体采用如下措施:

1)划分若干子网,办公用机器全部分配内部 IP 地址,Web 服务器安装双网卡,运行不同协议,实现办公网络和现有校园网络隔离[4];

2)利用防火墙技术,防止办公系统与外部网络相连后的信息泄露;

3)充分利用操作系统提供的安全措施;

4)利用虚拟专用网(VPN)隧道技术[5]。

对于本地注册用户,只需在他们的客户端上安装 Notes 客户端软件,就可以通过校园网访问本系统。远程注册用户可通过 Modem 或无线网卡与 Internet 网络连接,但要想进入校园网必须穿过防火墙,在这里采用了虚拟专用网隧道技术。因此,对于这样的用户,在客户端上只要安装 IE 和 VPN 隧道技术相关的 VPN 软件。这样的远程用户必须先在 VPN 上注册,然后进行用户身份验证,只有合法的 VPN 用户才能穿过防火墙进入校园网,从而访问本系统。

2.3.3　服务器层安全性

本系统的所有用户和服务器都建立了相应的标识符文件。在任何用户或服务器访问一个数据库之前,数据库所驻留的服务器都要检查此用户或服务器标识符中的验证字,以确认是否为合法身份。当系统经过身份验证并确认为是合法的用户后,服务器还要检查公共通讯录中的"允许访问列表"和"拒绝访问列表",以确定用户或服务器是否具有访问权限。如果为 Internet/Intranet 访问服务器,则应设置 SSL、名称和口令验证,来保护在网络上传输的网络数据,并验证服务器和客户机。此外,可设置防火

墙服务器,防止 Internet 服务器受到来自企业网络外部的未经授权的访问。

2.3.4 数据库层安全性

本系统中的每个数据库都有一个存取控制列表来限制访问数据库的对象。一个数据库对用户而言,有7项访问级别,权限由大到小依次为:管理者、设计者、编辑者、作者、读者、存取者、不能存取者。对不同层次的用户设定了不同的访问权限。

2.3.5 设计元素安全性

(1)在视图层、表单层上。

视图就是根据所选择的条件对数据库中的文档信息进行列表显示。在这一层上设计为只有具有数据库管理者权限的用户,才能设定某些指定的视图或文档,而且只能供具有相同访问级别的用户群组中的指定用户进行访问或修改,其他用户无权对视图进行改动。在表单层上,为了保证公文的严肃性和保密性,在发文管理时,只是发送链接部分,原文只有一份,储存在校办服务器上,当合法的具有读者权限的一般用户访问文件时,虽然能看到公文全文,但看不到具有法律效应的公章,并且禁止这些用户对公文进行拷屏操作。在发文管理子系统中,对不同身份的用户显示不同的视图,如秘书身份的用户只能看到公文流转的情况,可根据这些信息对公文进行催办。

(2)在文档级层上。

文档就是文档数据库中的单个记录。每个数据库中的任何一个文档都在文档中定义和实现了执行读操作的读者域以及执行写操作的作者域。每个文档根据发送对象的不同进行程序自动设置,非读者域的成员无法获得任何文档信息。

(3)在域级层上。

在通知通告子系统中,设计了一个特殊域:Content域。该域支持系统对特定通知在流转过程中进行加密、电子签名、防止拷贝、反馈回执、邮递报告等功能定义,保证传输过程的安全可靠,通知邮递选项主要有 Importance(重要性)、Mood Stamp(语气标记)、Delivery Priority(发送优先级)、Delivery Report(发送报告)以及 Sign(* * *)(电子签名)、Encrypt(加密)、Return Receipt(要求回执)、Prevent Copying(防止复制)8个选项。电子签名使读者确信作者的身份和信息没有被改动过。签名后系统将该域的数据和作者的用户标识符和个人密钥结合起来,创建一个惟一的电子签名。签名和作者的公用密钥、用户标识符里的验证字或验证者列表一起存储在文档里,用于密级通知的下发。

除上述安全控制机制之外,加密和解密技术贯穿于数据库、视图、文档、域级的安全控制当中。加密和解密技术主要采用的是特殊编码方式,解密信息存为密钥,密钥可以发送,只有拥有密钥的用户才能解密已加密的信息。这可以防止在传送信息时,信息在网上被截获,或者在网上进行破译数据库的拷贝。另外,还可以防止当信息转发时,转发人不能阅读的现象发生。

2.3.6 标识符安全性

Notes 或 Domino 标识符惟一标识一个用户或服务器。Domino 使用标识符中的信息控制用户和服务器对其他服务器和应用程序的存取。管理员的职责之一是保护标识符并确保未授权用户不能使用它们。

在获得对验证者和服务器标识符文件的访问权限前,一些站点可能要求多个管理员输入口令,这样可以防止由某个人控制标识符。在这种情况下,为防止未经授权存取标识符文件,每个管理员应确保每条口令都是安全的。

2.4 系统安全控制关键技术

2.4.1 文件发送与文件接收的安全性控制

在文件发送上,除了具有管理员身份的用户以外,本系统的其他用户都设计为"读者"。为了便于对读者的管理,并与服务器公用地址薄中其他系统的用户区别开来,又建立了另外一个数据库,该数据库与公文数据库一起存储在服务器上。该数据库按照各个用户工作职能的不同,分为院领导、二级学院(系或处、室)领导、下属科级单位等三个用户组。"学校办公用户"作为用户视图,通过数据库对用户视图的调用,就可以根据不同的发送公文,有选择性地以群组或个人形式选择不同的发送对象。

在文件接收上,对每一个"读者"用户都建立了相应的文件,并设定了相应的密码。用户进入本系统时,必须与服务器之间进行身份验证和电子签名,只有验证为合法的用户,才能进入本系统。具有读者权限的用户接收公文时,为了进一步验证是否为本系统所承认的用户,还必须完成签收人签名,因为院办秘书室对各个单位的收文管理人员都做了备案,非法用户不能擅自进入本系统,否则院办秘书会进行责任追究。当收文管理人员完成上述安全性验证之后,方可阅读标准公文内容,但由于对电子公章域的隐藏,这些用户看到的是没有电子印章的标准公文。

2.4.2 电子印章安全性技术

对于高校的公文,公章是使公文起到法律效应的必要条件。本系统采用的是电子公章形式,采用指纹进行盖章的权限验证,并将指纹特征值和日期信息转化成图形噪声,嵌入印章图像[6],借助于扫描仪设计电子公章,具有法律效应。

电子印章以 Word 图片形式存放在数据库管理员的客户端本地,即有权发送公文的秘书的计算机上。因此,设计电子印章域用来存放公章,该域只对具有特殊身份,即必须拥有管理员权限并具有"秘书"角色的用户开放。

对于具有其他存取权限的用户,公章域的安全性主要是通过环境变量"permitprint"来控制的,也就是通过公式(@Environment("permitprint"))是否为"true"来屏蔽。Permitprint 初始值是"false"。用户最初进入系统时,permitprint=!"true",即公章域是隐藏的,而且还禁止其他用户对此域进行预览读、预览编辑、拷贝到剪贴板的操作。具有读者存取权限的用户在 Notes 的客户端接收文件管

理时,环境变量 permitprint = "false",因此,在计算机屏幕上是看不到电子公章的。但当打印文件时,permitprint = "true",这样,具有读者存取权限的用户只有通过打印机才能够打印出带有电子公章的标准红头文件。

同时,对院办秘书这样的用户还设计了与其他用户不同的功能,其中包括公文打印预览、发送公文、进入起草状态、查阅公文签收状态、公文打印等。通过这些安全性控制,进一步加强了电子公章的安全性保护,从而也保证了文件传输安全、可靠。

2.4.3　打印控制及打印状态监视系统

本系统对公文的合法打印以及打印份数进行了设计,并实现了一些安全控制机制。设计各单位打印份数的初始值为"2",即变量 typenum = 2。如果打印份数大于2份,则有再申请打印份数的提示。在设计中,设置环境变量"permitprint"初始值为"false ",打印签名变量 printname 为"",当用户打印文件并签名后,环境变量"permitprint"为"true ",打印签名变量 printname 不为空,打印份数加1,即 Printnumber + 1。这时方可打印带有电子印章的公文正文。但对一般用户,由于电子公章域有禁止预览读的控制,"读者"用户在计算机屏幕上仍始终看不到电子印章。

另外还设计了一个打印状态监视库 print。打印状态监视库的管理员设为"院办秘书",其为打开 print 库、查询各个文件的打印结果、修改打印份数的权限。在该数据库中,同时还设计了打印控制视图和打印查询视图。打印控制视图主要是发文时间,打印查询视图主要是创建时间。两个视图均可以对各单位的秘书收文状况进行动态监视。

3　结　论

OA系统的网络层和数据库应用层的安全性建设决定整个系统的安全等级,而高安全性和高可用性一直是文中研究的重点。设计了基于C/S和B/S混合模式的OA系统,提出了综合利用 Lotus Domino/Notes 本身具有的安全机制、网络的安全技术和操作系统本身的安全特性,建立OA系统安全控制机制的模型。本模型经实验证明具有高安全性、高可用性。但高安全性必然是效率的损失。如何在OA系统里满足高安全性、高可用性要求的同时,提高文件处理的效率,将是下一步将要讨论的问题。

参考文献:

[1] 邴志刚,郑　君,储　健,等. 基于 Domino/Notes 的高校OAS解决方案[J]. 天津职业技术师范学院学报,2003(1):19-22.

[2] 张秋余,袁占亭,冯　涛. 办公自动化系统的设计与安全策略研究[J]. 兰州理工大学学报,2004(2):82-85.

[3] 余冬梅,刘密霞,冯　涛. 网络安全系统设计的研究[J]. 微机发展,2004,14(2):125-127.

[4] 李文印,吴　迪,叶润国. OA系统安全性设计及实现[J]. 吉林大学学报(信息科学版), 2003(4): 21-26.

[5] 郭雪梅,陈家晖,张江洋. OA系统安全防范的几点方法[J]. 广东自动化与信息工程,2004(4):43-45.

[6] 马康玉,刘　超,陈剑波. 生物识别技术在法院办公自动化中的应用-电子印章系统开发[J]. 微机发展,2003,13(5):52-54.

(上接第235页)

以使 DSS 签名的复杂度增加,主要是大数的长度增加。最大可以产生1024位的有效签名。不过解密加密时系统所付出的代价将会比较大。

3　总　结

介绍了密码体系中数字签名标准 DSS,主要阐述了它的快速实现方法和主要步骤,包括 DSS 的主要算法:大素数测试米勒-勒宾算法,高次幂的模指数剩余计算,模逆的计算。给出了 DSS 在计算机中的模拟过程,并对其安全性进行了分析和说明。通过 DSS 加解密系统程序的测试和运行,证明了 DSS 算法在防窜改、防抵赖等的功能,从中得到其在电子商务、保密传输方面的广泛应用。随着当今世界信息化的发展,数字签名技术作为网络信息安全的重要方面,必将得到进一步的发展。

参考文献:

[1] Harn L, Mehta M, Wen-Jung Hsin. Integrating Diffie-Hellman key exchange into the digital signature algorithm (DSA) [J]. Communications Letters, IEEE, 2004, 8(3): 198-200.

[2] Nel J J, Kuhn G J. Generation of keys for use with the digital signature standard (DSS), Communications and Signal Processing[A]. Proceedings of the 1993 IEEE South African Symposium[C]. Jan Smuts Airport: Institute of Electrical and Electronics Engineers, Rand Afrikaans University, 1993.6-11.

[3] Arazi B. Integrating a key distribution procedure into the digital signature standard[J]. Electronics Letters, 1993, 29(11): 966-967.

[4] 陈少真,李大兴. 基于变形 DSA 的有效群签名[J]. 计算机工程与设计,2004,25(3):323-326.

[5] Schneier B. 应用密码学——协议、算法和C源程序[Z]. 吴世忠等译. 成都:国防保密重点实验室,1996.

[6] 陈鲁生,沈世镒. 现代密码学[M]. 北京:科学出版社,2002.

[7] 卡茨安 H. 标准数据加密算法[M]. 陈太一,屠世桢译. 北京:人民邮电出版社,1983.

[8] 杨义先,林须端. 编码密码学[M]. 北京:人民邮电出版社,1992.

[9] 卢铁成. 信息加密技术[M]. 成都:四川科学技术出版社,1989.