基于 Notes 的 OA 系统的安全性研究

陆剑江
(苏州大学 计算机科学与技术学院, 江苏 苏州 215006)

摘　要: 从 Notes 系统的自身特点出发,并且结合 OA 系统的逻辑层次结构提出了 OA 系统的安全结构模型,通过设计一系列切实有效的安全策略,从而对基于 Notes 的 OA 系统的安全性作了比较深入的研究。

关键词: Notes; OA; 层次结构; 安全性
中图法分类号: TP317.1　　**文献标识码**: A　　**文章编号**: 1001-3695(2005)01-0117-03

Research on Security of OA System Based on Notes

LU Jian-jiang
(School of Computer Science & Technology, Suzhou University, Suzhou Jiangsu 215006, China)

Abstract: First gives out a safe architecture model of OA system from the point of the characteristic of Notes system itself and the logic hierarchy architecture of OA system. It studies the security of the OA system based on Notes through designing a series of practical and effective strategies.

Key words: Notes; OA; Hierarchy Architecture; Security

随着电子化、信息化的普及,人们对信息安全的需求也逐步扩展到社会生活的各个领域。人们希望信息在计算机的存储、处理以及网上传递过程中不被非法用户访问,同时必须确保对合法用户提供各种服务,以及阻止非法授权用户的非法入侵等。目前,在大多数的政府,企业和学校里都在各自局域网络的基础上构建了基于自身 Intranet 范围的办公自动化系统,从原有的依赖于人的传统办公模式转移到以计算机和网络数据交换为核心的网络办公自动化系统,由于系统中储存了办公过程中的所有流转信息、公文档案信息以及各种保密的人事信息等内容,所以安全性就显得尤为重要,一旦系统存在安全漏洞或者遭到恶意破坏将会给系统带来无法弥补的损失。应该说,安全性对于任何一个部门的办公自动化系统都是至关重要的,没有安全保障的系统对于信息工作的发展可以说是一种潜在的威胁。由于目前许多大中型企业和事业机关的办公自动化应用系统都是架构在 Lotus Notes 平台之上的,所以本文将重点对基于 Notes 平台的 OA 系统中的安全性作比较深入的研究。本文将从 OA 系统层次结构和安全结构模型入手,设计出切实有效的安全策略,从而解决 OA 系统的安全性问题。

1　OA 系统的层次结构模型

无论是建立在何种平台之上的 OA 系统,从系统本身的功能角度看,系统总是要包含发文流转模块、发文检索模块、发文发布模块以及系统管理模块等;从系统的数据交换上来讲,主要负责完成在不同用户或者不同服务器之间的数据传递,模仿计算机网络的 OSI 参考模型,我们可以设计出 OA 系统所遵循的逻辑层次结构模型,如图 1 所示。系统一般由处于最底层的物理交换层,处于最上层的实际应用层以及处于中间的操作系统层、数据分析层、功能模块层、业务逻辑层等层次组成。其中,物理交换层主要负责办公系统的各种底层数据交换,一般由于操作系统层的不同其数据处理的方式也会有所区别。数据分析层主要负责系统中的各种数据分析、统计与汇总的功能;而功能模块层以及业务逻辑层等分别负责系统功能模块的划分以及确定系统的实际办公应用的业务逻辑等。从系统实施的组织结构以及分工角度看,一般而言,系统最终办公用户在第一层工作,系统设计人员在第二、三层工作,系统分析员在第四、五层工作,硬件安装与维护人员在第六层工作,而系统管理员则可以在任意层工作。各层次结构之间由下而上是系统的实现过程,由上而下是系统分析过程。它们之间的相互关系是: 下一层是上一层的基础,而上一层是下一层的实现目标。

上　　下

实际应用层	业务逻辑层	功能模块层	数据分析层	操作系统层	物理交换层

图 1　OA 系统逻辑层次结构模型

2　OA 系统的安全结构模型

从图 1 所示的 OA 系统逻辑层次结构模型中可以看出,在 OA 系统的每一个逻辑结构层次上,系统的安全性都可能受到攻击,所以系统必须在一个或者多个层次上提供诸如身份鉴别、访问控制、数据保密性等相应的安全服务来保障系统的安全,而各种安全服务又可以由权限控制、数据加密和防火墙等安全策略来提供。基于这种思想,可以提出 OA 系统的安全结构模型如图 2 所示。该模型是由系统层次机构、安全服务、安全策略三者构成的状态图。图 2 中,分别体现了 OA 系统中的逻辑层次结构模型,以及针对该层次结构模型,系统应该提供的安全策略和安全服务。在该安全结构模型中,体现了三者之间的相互关系,由于安全策略及安全服务都由多个策略及多项服务组成,而且 OA 系统的层次结构模型也对应了许多不同的

收稿日期: 2003-10-22; 修返日期: 2004-03-04

层次,所以可以认为一种安全服务可以通过一种或者几种安全策略提供,一种安全对策可以用来提供一种或多种安全服务,各种安全对策提供安全服务可以在 OA 系统的一个或多个层次上进行,相互之间是相辅相成的关系。

图 2 OA 系统的安全结构模型

3 Notes 系统中安全控制的主要策略

具有完善安全机制的 Lotus Notes 在许多对信息安全问题极为敏感的机构中担任着至关重要的消息传递平台,Notes 系统的一个重要特性就是其强大可靠的安全机制。但是在设计基于 Notes 的 OA 系统的实际实现方案时,仍然必须考虑系统中可能会出现安全性方面的问题。从物理交换层次或者操作系统层次上来考虑,如保证物理服务器的安全以及网络数据传递的安全性等。针对系统内信息的安全性而言,则应该设计相应的安全策略,并作为系统的一部分来进行设计和考虑,必须控制诸如下列事件的发生:未经授权的黑客访问、未经授权的数据复制、不规范操作引起的灾难、硬件设施的损坏引起的数据丢失、邮件被截取、通过邮件的附件传播病毒和外部用户透过 Domino/Notes 服务器侵入内部系统等。针对诸多可能发生的安全隐患,系统安全保障的实现方法主要可以分为两大类:①是建立在数据加密、用户授权确认机制上的开放型方法;②是以“防火墙”技术为代表的被动防卫型网络安全保障系统。在设计基于 Notes 系统 OA 系统的安全策略时,我们可以从 Notes 自身提供的安全策略出发,并结合上述两种安全保障的实现方法来构筑系统的总的安全策略。在设计具体的系统安全保障策略时,可以针对实际 OA 系统的硬件和软件设计的特点,采用诸如防火墙技术、用户身份安全验证、权限控制、备份及恢复机制、计算机病毒的防治、加密措施以及数字签名等措施中的一种或几种,从而整合出一套符合自身特点的安全策略。

3.1 应用防火墙技术

对于一个运行在网络环境上的 OA 系统,为了维护内部 Intranet 网络的安全,防止来自外部网络的侵害和破坏,有效的防范非法入侵人员窃取系统内的重要信息,可以在内部网和外部网之间建立防火墙。该防火墙可以安装在路由器上,也可以安装在一台主机上。防火墙的功能设置则根据用户的防火墙策略来确定,即系统中哪些信息允许通过防火墙,哪些信息不允许通过防火墙。另外,使用防火墙既可以起到数据包过滤的功能,同时又能起到应用代理服务器的功能,其中数据包过滤防火墙可以监控 IP 数据包的流向和它所包含的信息,通过对数据包进行过滤操作,删除所有的未经授权的数据包;而应用代理服务器防火墙可以控制内部和外部的客户机之间的信息流,使用代理服务器,则每个经 Domino 授权的计算机不再拥有一个实际的 IP 地址,而是一个虚拟的 IP。这样,可以保障每个经 Domino 授权的计算机不可被外部的计算机访问,从而确保信息的安全。

3.2 用户身份安全验证

系统的安全性是从客户/服务器的验证开始的,它是一种双向的问答过程,为的是保证用户/服务器的互相识别。标志符文件的口令使怀有恶意的用户即使在物理上获得了用户的标志符文件,其未授权的访问仍将遭到拒绝。而且一般用户选择兼有字母和数字字符的长口令,该口令对付穷举破译(Dictionary Attacks)非常有效。系统对保密信息采用分级安全验证手段,而对公共信息则允许使用匿名访问以及不经过验证的服务器访问,即使无法完成合法的验证也可进行服务器访问。

3.3 权限控制

OA 系统的权限控制应该与系统的管理层次相适应。在 OA 系统中,不同用户的层次不同,因而能使用的系统资源和能访问的系统功能也应该是不同的。通过访问权限可以限定用户可以使用的系统资源和系统功能。

一般情况下,用户的类型有个人、服务器、混合组、个人组、服务器组等。在 Notes 系统中,每个用户具有七种存取级别,权限从大到小分别是:管理者、设计者、编辑者、作者、读者、存放者和不能存放者。在此基础上,通过对存取控制列表(ACL)和执行控制列表的(ECL)的设置可以真正作到对系统内各个层次用户的权限控制。

采用权限控制列表(ACL)提供授权或拒绝存取共享数据库、文档、视图、文件夹、表单和域的能力。通过允许或拒绝对本系统内的指定的服务器的存取,可以限制单个用户对服务器的存取权限。如所有服务器上都可以设置一个拒绝访问服务器的列表,该表中列出不允许访问相应服务器的有关人员或组的名单。

采用执行控制列表(ECL)可以让用户来控制 Notes 在他们的工作站上所能执行的操作,如访问文件系统、存取工作站上的文档和数据库、存取 NOTES.INI 变量、存取工作站以外的数据库、访问外部程序、发送邮件,以及修改工作站 ECL 等。通过这些控制手段可以阻止信息盗窃或者自激活的病毒毁坏数据和工作站操作系统。

3.4 备份及恢复机制

系统所运行的 Domino 平台上已经提供了丰富的日志功能,日志虽能记录任何非法操作,但要真正使系统从灾难中恢复出来,还需要一套完善的备份及恢复机制。备份是防止 OA 系统意外事故的最基本也是最有效的手段。备份就是当 OA 系统遭到非法用户的破坏,或是受到病毒的攻击,导致系统的数据损坏,通过事先备份的系统数据来进行恢复,保证系统的可用性。在具体选择备份时,可以选择硬件备份、双机热备份、磁盘双工与镜像、系统备份、应用系统备份和数据备份等方式。

通常,办公系统一旦投入使用,就必须不间断地运行,为了保证做到系统始终如一地正常运行,必须防止诸如存储设备的异常损坏等不可预料的故障发生,所以系统中可采用上述提及的一些备份和恢复措施。比如,可以在系统内配置两台相同的服务器,其中一台为主服务器,另一台为备份服务器。在这两台服务器上安装高速镜像卡,两台服务器通过高速链路连接。在系统运行时,数据存入主服务器的同时,也存入备份服务器,这就是双机热备份的措施。具体实施时,可采用热插拔的 SCSI 硬盘组成磁盘容错阵列,以 RAID 1 的镜像方式进行系统的实时热备份,以确保系统始终运行在正常负荷下,并将重要的数据作定时的备份。如果确实在系统运行期间发生了无法预

料的错误或者故障,无法从现场将数据恢复,那么,在系统中使用的双机备份运行方式就发挥作用了。配置的两个服务器中,由于一台是主服务器,另一台是备份服务器,这样保证即使主服务器出现故障,其备份服务器也可以继续完成正常的公文处理,以便给技术人员充足的时间对出现的问题进行处理。

3.5　公文流转信息的跟踪

对于没有条件采取双机备份的用户来说,可以采取对公文流转信息的跟踪来弥补无法备份的不足,同时通过对流转进行跟踪可以详细地记录公文在每个流转时刻的实际位置和办公人员,为系统的监控提供详实而可靠的依据。这需要在进行系统设计时将该信息跟踪模块嵌入到系统的流转实现逻辑中。Notes 是基于电子邮件的群件办公平台,所以信息在系统内的流转主要靠系统的电子邮件服务来提供的,即当用户 A 给用户 B 发送了一个公文,则在系统内则表现为用户 A 发送了一个电子邮件,而用户 B 则收到了相应的电子邮件,只是在系统内对于这类公文邮件不是按照普通邮件来处理罢了。鉴于此实现模式,我们可以在用户的发送模块中嵌入系统信息的监控模块,将用户当前的公文信息同时发往某个用于跟踪管理的数据库,这样,在该数据库中就记录了所有公文发送的状态信息,包括公文的发送人、接收人、发送时间、公文内容和当前流转序列等监控内容,由于记录了一个公文在系统内流转所经历的每个步骤,所以一旦由于不规范操作或其他原因破坏了用户的公文数据库,则可以依据此跟踪数据库中的相应记录对用户的公文数据库进行恢复。经过实际的应用证明,该方法是行之有效的,可以对任何用户的任何公文流转过程进行恢复。

3.6　计算机病毒的防治

有效地防治计算机病毒对保障 OA 系统的安全性非常重要。对于单机模式运行的 OA 系统,计算机病毒的防治比较简单,只要计算机用户掌握了计算机病毒的基本知识和使用成熟、能可靠防治计算机病毒的产品的使用方法,经常进行查病毒和杀病毒工作,一般是能有效地防止病毒的侵害。但是对于网络环境下的 OA 系统,对病毒的防治比较复杂一些,具体可采取如下一些措施:恰当地设置网络服务器上系统资源的访问权限和存取权限,可以在一定程度上防止病毒攻击;用可防病毒的硬件产品,如防病毒卡、主板等;选用计算机的防病毒软件产品,如基于服务器的防病毒软件,诸如一些病毒防火墙,有实时扫描病毒能力,并能自动跟踪病毒的来源。

3.7　加密措施

在 OA 系统中,为了防止非法用户窃取机密信息和非授权用户越权操作数据,必须对 OA 系统中的重要数据进行加密。在基于 Notes 的办公自动化系统中可以采取数据库加密、字段加密、文档加密、信道加密和网络端口加密等手段。其中,数据库加密可以通过使用本地安全性选项,并利用一个用户或服务器 ID 来进行加密,这样,只有在用户的专用密钥能够解密附加的密钥时,用户才能本地访问加密的数据库。字段加密可以由数据库的设计者通过创建和分发的特殊密钥来进行,这样可以限制那些授权用户可以访问的字段。为了弥补管理或物理安全性上的漏洞,可以在数据库设计中使用文档密钥。这样,即使可以得到文档,但是却得不到文档的内容;同时,在发送电子邮件时也应使用这一特性,前提是用户必须能够存取个人通信录或公用通信录中的收件人的公用密钥。文档加密可以使用公钥或者私钥来进行,并且可通过将密钥添加到某个表单,这样通过该表单所创建的任何文档都被自动加密。另外,也可以让用户使用自己的密钥来对文档进行管理。由于通过网络发送数据时,任何能够截取网络报文的人,通过跟踪或电子偷窃技术,都可以读取没有加密的数据。为了避免此情况的发生,可以采取网络端口加密,它允许那些未加密的数据在端口级别进行加密,以能够通过网络安全传输。此外,由于 OA 系统以 Intranet 作为传输网络,所以可在 Intranet 可访问到的服务器上实行信道加密,这样各种侦听手段就将无用武之地。

3.8　数字签名

采用数字签名(电子签名)不但能使得电子邮件或者文档具有法律效力,可以完全确认消息是谁发送,文档是谁建立的;而且能够证明电子邮件或者文档是否传输过程中被其他人修改过,即可以保证电子邮件和文档的完整性。数据库设计者还可以控制某个数据库的字段和部分是否需要进行数字签名,单个用户可以选择对邮件消息进行签名。数字签名使用与确认和身份验证过程使用的都是相同的 RSA 密钥对。使用公钥进行加密的过程必须包括以下三个步骤:①发送者用自己的密钥对文档中的特定内容进行加密并且建立数字签名;②在发出该文档之前,用接收者的公钥对整个文档进行加密,这样已经加密的信息现在被嵌入到新的加密文档中;③文档发送给接收者后,接收者用自己的密钥解密即可。

4　结束语

构建一个安全可靠的系统,仅考虑基于网络物理设备的安全性或者单独采用某种安全策略都是不够的,也是不可取的。虽然实际应用中的办公系统在各自表现形式和功能划分上会有比较大的差别,但是从系统的本质上来看,一般都是建立在文中提到的 OA 系统的逻辑层次结构模型之上的,同时结合 OA 系统的安全结构模型,总可以从诸多安全策略中整合出一整套符合自身的安全控制策略。从 OA 系统的发展角度来看,将来很可能与 ERP 系统、物流管理系统等结合,所以必须同时考虑各个系统自身的安全性以及各个系统整合之后的总体安全性;同时,从系统的一些实现细节上来讲,必须尽量避免由于误操作所引起的信息不安全问题,这些可以通过在设计过程中增加用户的确认或者建立各种操作的跟踪恢复机制来弥补。

参考文献:

[1]　omino Developer's Reference 开发人员手册[M]. 北京:北京希望电子出版社,2000.

[2]　Domino Application Solution for Enterprise 企业应用解决方案[M]. 北京:北京希望电子出版社,2000.

[3]　陈传波,金旭军,刘广宇.群件安全结构分析与设计[J].计算机应用研究,2000,17(1):50-52.

[4]　Lotus Notes/Domino R 5.1 Complete Reference 使用大全[M]. 北京:北京希望电子出版社,2000.

[5]　Domino Developer's Guide 应用开发指南[M]. 北京:北京希望电子出版社,2000.

作者简介:

陆剑江(1976-),男,江苏常州人,博士研究生,主要研究方向为协同工作、分布式计算、中文信息处理。