医院信息系统访问控制策略设计分析

赵 锋,曹文杰
(陕西师范大学 国际商学院,陕西 西安 710062)

摘 要:今天的医院信息系统(HIS)与先进的计算机、网络、通讯技术融合的速度越来越快,这虽然大大提升了医院各项业务信息化程度,但受传统信息安全策略固有缺陷的限制,同时也增大了越权行为、信息泄露信息安全事故的可能性。为解决这些问题,在信息系统安全目标和安全需求分析的基础上,提出了一种基于时间、空间环境制约因素的角色访问控制技术和一种在分布式环境下层次化的授权策略。本模型在角色访问控制模型的基础上,增加了时间和空间两个制约因素,能够使医院信息系统更加安全,降低访问控制事故的风险,为网络安全防护产生更大的技术效益。

关键词:医院信息系统;角色访问控制策略;授权策略;信息资源;信息安全
中图分类号:TP309 **文献标识码**:A **文章编号**:1673-629X(2010)06-0144-04

Design and Analysis of Access Control Strategy for Hospital Information System

ZHAO Feng, CAO Wen-jie
(School of International Business, Shaanxi Normal University, Xi'an 710062, China)

Abstract: Nowadays, advanced computer, network and communication technologies are greatly adopted in HIS, which enhanced information degree of hospital's business. But with inherent defects of traditional information safety strategy, it is easy for employees to overstep and give away information. To solve these safety problems, gives a role access control strategy based on time and location, based on research of safety targets and requirements of information system. Also, gives a hierarchical authorization strategy under distributed environment. Based on role access control strategy, this strategy adds time and space two constrains, so as to make HIS more safe, reduce role access control risks, and provide more technical benefit to network safety protection.

Key words: hospital information system; role access control strategy; authorization strategy; information resource; information safety

0 引 言

医院信息系统作为医院信息化业务的核心系统之一,已被广泛地应用和快速地改进,其自身功能和性能在不断发展的同时,对于医院各项日常业务所起的作用也越来越重要。随着对信息系统广泛而深入的应用,使用者对系统安全性的要求也越来越高[1]。

然而,在当前医院信息系统产品快速的发展过程中,传统的基于角色的访问控制策略[2]和静态授权模式已不能适应当前信息系统分布式和复杂化的发展趋势。

由于有意或无意地滥用用户角色权利,越权操作行为时有发生;用户角色消失,即用户不能再执行职责时,静态授权不能有效调整;用户不在工作地点、工作时间而登陆信息系统,传统访问控制策略不能有效限制[3];等等。这些访问控制策略的漏洞都增加了医院信息系统及其所承载的数据的安全性。因此,根据医院实际业务的特点,改进医院信息系统的访问控制策略,在现在显得尤其必要。

收稿日期:2009-07-16;**修回日期**:2009-11-23
作者简介:赵 锋(1971-),男,博士后,副教授,从事信息安全技术、信息安全管理、风险评估技术、电子政务、信用体系等研究。

1 医院信息系统安全目标及安全需求分析

1.1 医院信息系统电子业务识别与分析

1.1.1 医院信息系统机构分析

根据我国医院现行体系结构模式、管理模式和管理程序,医院信息系统包括门诊、急诊病人挂号子系统;医院门诊收费划价和门诊收费管理子系统;医院急诊病人管理子系统;医院门诊医生工作站子系统;检验信息子系统;医学影像子系统;医院住院医生工作站子系统;护士工作站子系统等在内的几十个子系统。根据实用性设计原则,医院可以根据其自身规模、财力、管理水平和管理需求来选择子系统,来完成不同的业务功能。

1.1.2　医院电子业务数据分析

一个医院信息系统所涉及的数据种类繁多,是各个业务部门所开展的电子业务的依据和结果,大体包括三大类:电子病历数据,可供病人查询和医疗统计;费用数据,包括病人收费数据和医院资源费用数据,可供医疗统计和经济核算;医院资源数据,包括医院各种设备、药品、消耗品、物资及工资数据,可供医院财务核算和审计。这些数据的规模程度、重要性、分布位置等各不相同,需要依据其自身特点,分析不同数据的安全需求。

1.1.3　医院电子业务的用户角色分析

医院信息系统中,参与电子业务的各类操作用户数量大、种类多,各用户所属的角色、参与的业务、进行业务操作的地点和时间、操作的信息资产类型及所设计到的业务数据各不相同[4]。仅以病人、门诊医师和信息管理员三种角色为例,各自特点见表1。

表1　医院信息系统三种角色属性表

角色	参与的业务	操作地点	操作时间	信息资产	业务数据
病人	查询	大厅	任意时间	自助信息查询终端	病人诊疗、费用等信息
门诊医师	写入、修改、查询	门诊部工作站	工作时间	工作站设备	病人信息、药房信息等
信息管理员	制定访问规则、审计访问记录、维护信息系统	信息管理部门	工作时间	信息管理部门的主机、服务器等	医院信息系统业务记录

1.2　医院信息系统访问控制安全目标分析

如果某类用户角色权利的使用超出了其特定的空间和时间限制条件,则为滥用或冒用。若擅自进行数据的查询或导处,会发生病人、医院数据泄漏,甚至造成相关法律问题;擅自导入,则可能会增加数据的存储空间,增加系统处理的复杂度,还有可能对已经开始的业务造成逻辑混乱。

因此,医院信息系统不同角色访问控制的安全目标可以描述为:所有用户在指定的专用终端上,在限定的时间条件下,通过特定的身份认证技术,行使其享有的权利,进行相应子系统的操作,处理相应的数据。

1.3　医院信息系统访问控制安全需求分析

根据角色级别,采用特定的身份认证技术、设置身份认证策略。身份认证策略要有具体的时间和空间条件限制,保证具有访问权限的用户,只有在职权范围内的时间、限定的设备上,才能通过身份认证并访问信息系统。所有用户在信息系统中的操作权限必须在限定的设备、网络接口和时间条件下行使。同时对用户的权限进行合理的分配,权限分配遵守最小权限原则、权限分离原则。授权机制要适应分布式环境的特点,采用动态授权[5]。

现阶段,医院信息系统的发展呈现出几个趋势:第一,信息系统覆盖的科室、职能部门增加,推动医院运营的信息化;第二,病人来院就诊的各个环节与医院信息系统关联程度加深,推动就诊流程网络化;第三,医院信息系统支持层的信息资产种类和数量快速增加,推动业务开展的无纸化和业务环境的复杂化。这三个发展趋势,都大大加强了医院各项业务对信息系统的依赖性。而一旦网络瘫痪或数据丢失,将会给医院和病人带来巨大的灾难和难以弥补的损失。因此,文中设计了一种基于时间、空间环境制约因素[6]的角色访问控制模型——TLRBAC (time - location - role - based access control)和一种在分布式环境下的层次化授权策略,以改进传统的基于角色的访问控制模型,使其更好地满足医院信息系统的安全性需求。

2　TLRBAC访问控制模型设计分析

该模型的基本思想:信息系统用户以一定的角色身份来访问信息系统,其访问行为须受到有时间和空间属性的访问控制规则的制约。这样,通过在访问规则中加入访问行为具体的时间和空间约束条件,可以对具体的访问行为实施有效控制。

2.1　模型制约因素分析

分析医院信息系统的访问控制安全目标和需求,我们认为时间和空间是对访问行为合法性影响较大的环境因素,将其作为访问控制规则中的环境制约因素。

2.1.1　时间因素分析

时间的范畴包括在职时间与离职时间、工作时间与非工作时间。下面具体分析一下各种类型。

在职时间是指医院信息系统的用户就职于医院的某个部门或科室的时间。从员工就职开始,医院信息系统管理部门就为其分配相应的权限及身份认证凭证,如口令、个人持证等,直至该用户离职为止。此后转入离职时间。届时收回其权限,取消其用户口令及密码、销毁其个人持证,使其不再具有任何原先的专用权限。

工作时间是指用户处于每个工作日可以行使其权限的时间。一般来说,从用户每天上班开始,直至下班,期间都可以行使其访问权限,因此可以将此作为工作时间。非工作时间即用户下班离岗的时间。

2.1.2　空间因素分析

空间针对的是用户接入医院信息系统、行使其访问权限的物理方位。一般对于其权限的行使仅限于各自的工作岗位。例如,医生和护士对应于各自的工作站,不允许在其他节点登陆;网管人员对应于信息部门的主机,对数据库和网络的管理不能在其他主机上操

作。

2.2 访问控制原理

TLRBAC模型的基本原理如图 1 所示[7]。

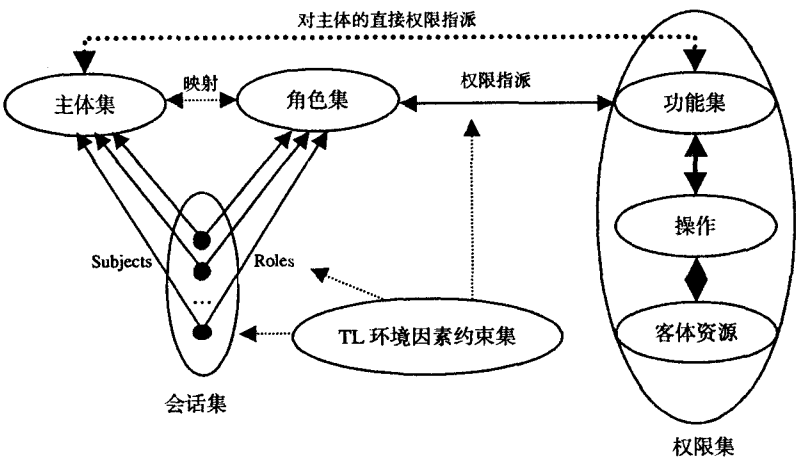

图 1 TLRBAC访问控制模型示意图

(1) 形成医院信息系统的各类表单,并建立相关的数据库文档。这包括以下工作:

a.在医院信息安全部门在主体用户分类和信息资产识别的基础上,创建主体用户表和客体资源表,描述两者特征;

b.依据主体用户的行政级别和职责范围,创建医院信息系统的角色表;

c.确立主体和角色的对应关系,形成会话集;

d.依据医院信息系统包含的功能模块,创建功能可实现的操作与客体资源对应的权限表。

(2) 根据会话集中包含的对应关系,实现主体到角色的用户指派。对角色表中各类角色进行权限指派,为其分配权限。当主体单位、客体对象和操作行为发生更改、增加、删除时,可以对主体临时直接指派权限,避免繁琐地调整角色授权方案。

这样就建立了主体用户与系统功能之间的间接联系,使得主体用户可以对客体资源进行访问和操作。同时,会话集中主体-角色对对应关系、角色集中角色以及角色与权限对的对应关系,又受 TL 环境约束集对限制。

2.3 访问控制策略的实现

这一模型所包含的访问控制策略,主要从身份认证、入网访问控制和操作权限控制三个方面来实现[8]。

2.3.1 身份认证策略

对于医院信息系统中各个用户,要根据其所属角色职责、权限的大小,采用适当的身份认证技术。包括用户名/密码方式、智能卡认证、动态口令、USB Key认证、生物识别技术等,这些身份认证技术的安全性等级逐渐增强,可适用于不同角色层次的用户。

2.3.2 入网访问控制策略

入网访问控制是网络访问的第 1 层安全机制。它控制哪些用户能够登录到服务器并获准使用网络资源,控制准许用户入网的时间和位置。用户的入网访问控制通常分为三步执行:用户名的识别与验证;用户口令的识别与验证;用户账户的默认权限检查。三道控制关卡中只要任何一关未过,该用户便不能进入网络。其中,默认权限检查须依据时间、空间环境因素的约束规则,使得网络能控制用户登录入网的位置、限制用户登录入网的时间、限制用户入网的主机数量,防止角色权限的冒用和滥用。

2.3.3 操作权限控制策略

操作权限控制是针对可能出现的网络非法操作而采取安全保护措施。用户和用户组被赋予一定的操作权限。网络管理员能够通过设置,指定用户和用户组可以访问网络中的哪些服务器和计算机,可以在服务器或计算机上操控哪些程序,访问哪些目录、子目录、文件和其他资源。同时,网络管理员的这种权限设置,要依据信息系统用户的自身职责,同时又要遵循用户进行业务操作的时间、空间方面的具体要求来开展,因而是一种动态的操作权限控制。

3 授权策略

随着医院信息系统的子应用系统不断增多,远程医疗快速发展以及社保、新合疗等接口的介入,系统中用户、资源的数量和种类不断增加,主体用户日益分散,集中式的授权方式已经不能完全满足当前医院信息系统的要求。因此可以采用分布式层次授权方式[9]。这种授权策略包含两个方面,即分布式和层次化授权策略。

(1)将原来的集中式授权改为分布式授权。这要求在医院信息系统所覆盖的各职能部门内部成立授权机构,将系统资源的访问控制权限分配给分布式环境下的各授权管理机构的管理者。由这些管理者对职能部门的各主体进行授权。这样,对全院各子系统的访问权限,就由单一的医院信息管理员统一分配,变为了由多个部门内部的授权机构分别分配。这样可以更灵活地适应各子系统主体的变动情况。

(2)采用层次化的授权方式。要设立最高授权管理机构,可由医院信息安全管理部门担任。信息安全管理部门将分布式环境下所有的信息资产进行识别,并制定最高的权限管理策略,然后将系统资源的访问

控制权限分配给分布式环境下的各授权管理机构的管理者;这些授权管理机构的管理者设置本层的授权策略,再依据其下属角色的层次结构授权。同时,较高层管理者制定的策略就构成了上层策略,各分布点管理者制定的策略就构成了下层策略。上层策略对下层策略具有约束作用。例如,可以由医院信息管理员给医院行政管理层和科室的主任医师或护士长进行授权,再由他们给下属的医师或护士授权。这样可以更好地适应各部门权限分配的需要,加强授权机制的合理性和可行性。

4　结束语

在分析医院信息系统安全目标及安全需求的基础上,提出访问控制策略中时间和空间两个必要的制约因素,进而设计并分析了基于时间和空间制约因素的角色访问控制模型——TLRBAC。时间、空间环境约束条件对访问控制的制约作用体现在对角色集中参与映射的角色进行约束、对角色获取的权限范围进行约束以及对会话集中主体和角色的对应关系进行约束。最后,提出了分布式层次化授权策略,在分布式环境下,对各个职能部门、科室的主体用户,依据其角色层级,逐级进行授权,从而避免对角色统一授权的繁重工作及由此可能出现的错误。

参考文献:

[1] 朱　莹,金凌紫,朱　鸿.医院信息系统安全性需求分析与总体设计初探[J].计算机系统应用,1998(8):2-5.

[2] Sandhu R S, Coyne E J, Feinstein H, et al. Role-based Access Control Models[J]. IEEE Computer, 1996,29(2):38-47.

[3] O'Neil M, Allam-Baker P, Cann S M, et al. Web Services Security[M]. [s.l.]:McGraw-Hill,2003.

[4] Ferraiolo D F. Proposed NIST Standard for Role-based Access Control[J]. ACM Transactions on Information and System Security,2001,4(3):224-250.

[5] Joshi J B D, Bertino E, Latif U, et al. A Generalized Temporal Role-based Access Control Model[J]. IEEE Transactions on Knowledge and Data Engineering, 2005,7(1):4-23.

[6] 董理君,余胜生,杜　敏,等.一种基于环境安全的角色访问控制模型研究[J].计算机科学,2009,36(1):51-59.

[7] 牛少彰,崔宝江,李　剑.信息安全概论[M].第2版.北京:北京邮电大学出版社,2007:121-123.

[8] Kandala S, Sandhu R. Secure Role-Based Workflow Models [C]//In: proceedings of the 15th IFIP WG 11.3Working Conference on Database Security. Niagara, Ontario, Canada: [s.n.],2002:45-58.

[9] 颜学雄,王清贤,马恒太.Web服务访问控制模型研究[J].计算机科学,2008,35(5):38-41.

(上接第 143 页)

功耗;同时解决了有线传输中的通信障碍问题。除此之外,还可以通过 Zigbee 模块进行定位。可以预测随着机器人技术和 Zigbee 技术的发展,在群体机器人中,Zigbee 将会得到广泛的应用。

参考文献:

[1] 原　羿,苏鸿根.基于 ZigBee 技术的无线网络应用研究[J].计算机应用与软件,2004,21(4): 89-91.

[2] 王吉富,刘梧林,郭建光.基于 ZigBee 技术的无线传感器网络应用研究[J].移动通信,2008(6):29-32.

[3] 白国亮.基于 zigbee 无线通信技术及其应用前景[J].林区教学,2009(6):79-80.

[4] Ruiz-Garcia L, Barreiro P, Robla J I. Performance of ZigBee-Based wireless sensor nodes for real-time monitoring of fruit logistics[J]. Journal of Food Engineering,2008,87(3): 405-415.

[5] 虞志飞,邬家炜.ZigBee 技术及其安全性研究[J].计算机技术与发展,2008,18(8):144-147.

[6] 李智军,周　晓,吕恬生.基于群体协作的分布式多机器人通信系统的设计与实现[J].机器人,2000,22(4):300-304.

[7] Kim H, Chung Jong-Moon, Chang Hyun Kim. Secured communication protocol for internetworking zigbee cluster networks[J]. Computer Communication,2009,32(13):1531-1540.

[8] Baronti P, Pillai P, Chook V W C, et al. Wireless Sensor networks: A survey on the state of the art and the 802.15.4 and ZigBee standards[J]. Computer Communication, 2007, 30(7):1665-1695.

[9] 潘　伟,黄　东.基于 Zigbee 技术的无线传感网络研究[J]. 计算机技术与发展,2008,18(9):244-247.

[10] 程　磊,王永骥,朱全民.基于通信的多移动机器人编队控制系统[J].华中科技大学学报,2005,33(11):67-70.

[11] 陈　飞.基于 ZigBee 的多机器人通信系统的设计[J]. 信息科学,2009(10):61-61.

[12] Abusaimeh H, Yang Shuang-Hua. Dynamic Cluster Head for Lifetime Efficiency in WSN[J]. International Journal of Automation and Computing,2009,6(1):48-54.

[13] 王艳秋,万钧力,邵旭昂,等.基于 ZigBee 的多机器人通信系统的设计[J].电子技术应用,2009(5):126-128.