

一种普适计算下的访问控制策略

朱益霞,孙道清,沈 展

(安徽师范大学 数学与计算机科学学院,安徽 芜湖 241003)

摘 要:计算技术的发展是以人类服务为目标的,需要一种“以人为本”的计算模式,而普适计算正是这样的一种革新性的计算模式。访问控制作为一种重要的安全措施在系统安全中得到了广泛应用,而普适计算模式下的系统安全也需要一种合适的访问控制策略。为此,比较了现有访问控制模型的各自特点和适用范围,分析了普适计算环境下访问控制策略的特殊要求,在此基础上详细描述了普适计算模式下动态访问控制策略实现方法。并在 ARM7 嵌入式实验箱现有资源基础上模拟了普适环境下考虑上下文信息的访问控制中的部分机制。

关键词:普适计算;访问控制;上下文相关;基于角色

中图分类号:TP301

文献标识码:A

文章编号:1673-629X(2010)08-0091-05

An Access Control Scheme for Pervasive Computing

ZHU Yi-xia, SUN Dao-qing, SHEN Zhan

(Mathematics and Computer Science College, Anhui Normal University, Wuhu 241003, China)

Abstract: The development of computing science is to serve human, so it needs a people centered computing paradigm, and ubiquitous computing breeds as such an innovatory computing model. Access control is widely applied to system security as an important safety precaution, and system security in pervasive computing likewise needs an appropriate strategy. For that purpose, compare the characteristics and application scope of the existing access control models, analyze the special access control policy requirements in pervasive environments. On these bases, give a minute description on implementation method of dynamic access of pervasive computing. And simulated part of the dynamic access control mechanism in pervasive computing using available resources of ARM7 embedded experimental box.

Key words: pervasive computing; access control; context-aware; role-based

0 引言

随着计算科学和通信技术的发展,普适计算^[1]作为一种新的计算模式孕育而生。普适计算是物理空间和信息空间的融合,在这个融合的空间中,人们可以随时随地、透明地获得数字化服务^[2],它将给人类带来极大的便利。这种新的计算模式力图真正全面实现计算技术的“以人为本”,把技术渗透到人们生活当中以致人们无须关注技术本身就能自然地享受服务。普适计算是计算、通信等技术极大发展的结果,也对计算机科学的各个层次研究都提出了新的要求和技术挑战。比如:在硬件或接入层次,要研究嵌入环境的和便于携带的计算设备、传感设备和显示设备;在网络层次,要把

无线网络作为基础研究;在系统软件层次,要研究如何实现数据的交互、任务的协作、用户隐私保护等;在人机交互层次,要实现透明的蕴涵式交互,新的交互模式和感知接口。

访问控制策略作为系统安全的一部分,牵涉到上述多种层次的技术。基于上述各层次技术的改变,普适计算下的访问控制也必然会有新的特点,同样也就有着新的要求。

在桌面计算模式下,人们在访问控制的研究领域取得了丰硕的成果,提出了许多访问控制模型,比较经典的有早期的自主访问控制模型和强制访问控制模型,比较热门的有基于任务的访问控制模型和基于角色的访问控制。

文中将简单地对这几种模型进行介绍和比较,会发现它们从系统角度出发对资源进行安全保护,其原理可以简单描述为:如果主体对某客体发出访问请求并有访问权限,那么提供访问操作,是一种被动安全模型。这几种模型并没有将执行操作的环境考虑在内,不适合普适环境的访问,因为普适环境中的安全策略

收稿日期:2009-12-09;修回日期:2010-02-26

基金项目:安徽省自然科学基金(070412043);安徽高校省级自然科学研究重点项目(2006KJ024A)

作者简介:朱益霞(1983-),女,硕士研究生,研究方向为普适计算及其安全;孙道清,副教授,硕士生导师,研究方向为普适计算与网络安全。

与用户和系统的上下文息息相关。

1 桌面模式下几种访问控制模型的比较

1.1 自主访问控制(DAC)

DAC(Discretionary Access Control)的基本思想是先确认访问主体的身份以及它所属的分组,再根据其身份和授权来决定其访问模式权限。“自主”主要体现在,主体(用户或用户进程)能够自己决定是否将其拥有的访问控制权限或访问权限的某个子集授予其他的主体,并有权收回^[3]。

DAC一般采用建立系统访问控制矩阵的方法,来实现主体对客体资源的有限制的访问。在访问控制矩阵中,行对应系统的主体,列表示客体,元素表示相应主体对某个客体的访问授权。主体(用户或用户进程)对任一客体资源发出访问请求,系统都要先检查这个访问控制矩阵。如果矩阵中该主体(行)和该客体(列)对应的元素记录有这个访问类型,那么允许主体访问,否则就拒绝访问。

1.2 强制访问控制(MAC)

MAC(Mandatory Access Control)依据主体和客体安全级别的比较来决定主体对客体是否有访问权限。在 MAC 系统中,安全管理员给每一个主体和客体分配固定的安全属性,利用这个安全属性决定一个主体是否可以访问某个客体^[4]。安全属性是强制的,由安全管理员向主体和客体分配安全标签即安全级,普通用户不能任意更改。

MAC 利用下读/上写来保证数据的保密性,并且通过这种梯度安全标签来实现信息的单向流通。主体对客体进行访问时遵循“向下读,向上写”的原则,即:如果主体需要读客体的数据,则其必要条件是主体的密级不小于客体的密级;如果主体要向客体中写入数据,则其必要条件是主体的密级不大于客体的密级。

1.3 基于角色的访问控制模型(RBAC)

RBAC(Role - Based Access Control)是在 1992 年由 Ferraiolo 和 Kuhn 提出的。它的提出引人注目,很快成为访问控制研究的热点。RBAC 的突出特点是在用户和访问权限之间创新性地引入了角色这一概念,使得用户和权限不直接发生联系,而是通过角色联系起来。系统赋予用户以某角色,于是用户即拥有属于该角色的所有权限,从而对资源进行访问。

在 RBAC 中,角色可以理解为访问权限的集合,系统通过对用户授予角色以及对角色授予权限来实现访问控制(见图 1)。RBAC 中的一个用户可拥有多个不同角色,而一个角色可以授权给多个不同用户。系统根据用户的具体访问请求产生相应的会话,用户会话

决定启用某一角色子集作为该用户的当前活跃角色。在 RBAC 中,一个角色可包含多个不同权限,而一个权限可被多个不同角色包含。角色之间也可存在继承关系,从而形成了角色层次结构。用户会话激活了当前活跃角色子集,也即使得用户拥有了该角色子集所包含和继承的所有权限。

RBAC 模型对传统直接授权模型是个突破性的改进,其功能相当强大,也具有很强的实用性^[5,6],因此学术界和工业界都对 RBAC 给予了广泛关注,NIST 还专门成立了研究机构对其进行深入和系统的研究。在充分深入研究的基础上,美国乔治梅森大学信息系统和系统工程系的 R. Sandhu 等人于 1996 年提出了著名的 RBAC96 模型。RBAC96 模型实际上是一个模型簇,用 4 个不同层次的模型系统而全面地描述了基于角色的访问控制策略在多方面、多层次的应用意义。它们分别是 RBAC0(基础模型)、RBAC1(层次模型)、RBAC2(约束模型)、RBAC3(层次约束模型)^[7]。

1.4 基于任务的访问控制模型(TBAC)

TBAC(Task - Based Access Control)是一种基于任务、动态授权的主动安全模型^[8~10]。它从企业应用的实际安全需求出发,突出“面向任务”,从基于任务(活动)的角度来进行访问控制,进而完成安全模型的建立和安全机制的实现。由于任务的执行是动态的,所以 TBAC 提供的访问控制安全管理也必然是动态实时的。

TBAC 系统对每个任务赋予一定的访问权限,因此一个任务的执行就是主体使用所拥有的访问权限对客体进行访问的过程。任务所拥有的访问权限是有限的,随着任务的执行,权限逐渐消耗。直至任务完成时,权限也消耗完,主体就不能继续访问客体了。系统对用户授予访问权限,不仅要考虑主体、客体本身,还要考虑当前要执行的任务以及任务的状态。用户对客体资源的访问权限也不是固定不变的,随着执行任务的变化而动态改变。在 TBAC 中,角色和任务的概念不太清晰,且其角色也不支持层次等级,需要与 RBAC 结合起来应用。

TBAC 和各种各样的业务或任务紧密相关,其统一化系统的设计非常复杂。

1.5 上述访问控制模型的比较

综上所述,每种访问控制模型都有其产生的特定背景和要求,也各有优缺点。DAC 较弱,MAC 太强,TBAC 统一化访问控制难以实现,RBAC 较为灵活有效。但以上几种访问控制模型都是针对桌面计算模式而研究和设计的,DAC、MAC、RBAC 中主客体权限固定,不能根据系统上下文的改变而动态地修改;TBAC

虽然考虑到上下文因素,但是它没有将角色和任务区分开来,导致控制上的混乱。这几种访问控制模型在桌面模式下都是经典且优秀的,也有着各自适用的领域,但它们都不适合普适计算模式下高度自主化人性化的交互方式。普适计算环境下,主体、客体的状态和上下文信息是授权访问必须考虑的问题,其访问控制也有特定的要求。文中介绍了一种适合普适计算要求的上下文相关的动态访问控制模型。

2 DRBAC

针对普适计算下特定的需求,DRBAC^[11](Context-Aware Dynamic Role-Based Access Control)根据收集到的环境上下文信息^[12],动态改变主体所激活以及角色所激活的权限,提出了基于环境上下文信息的DRBAC模型。

2.1 普适计算下的访问控制特点和需求

普适计算是随时随地有效访问计算资源的一种新型计算模式,嵌入式环境、传感设备、无线网络等技术普遍使用,人们与计算设备的交互自发而蕴涵地产生。普适计算系统一旦开启就不会死机或需要重启,这就要求在设计的时候必须保证系统的稳定性、安全性^[14],比如防止系统访问量超过系统的承受力、杜绝特权用户在不合适的时间访问资源等;另外,系统资源中有涉及用户自身隐私的部分,这就要求对应特定的资源,不同的用户有不同的访问权限。

比如在一个大学的智能建筑里,有很多不同的智能空间,如管理者办公室、会议室、教室、实验室等,里面有很多不同的资源设备。对于这个智能系统,访问者也会有不同的身份,如管理者、教授、普通教师、普通员工、学生等。在这个普适环境中,要求系统能在用户进入的时候自动识别其身份,并根据其身份和所处空间、时间的不同分配不同的角色,使其具有相应的访问权限;当访问者离开特定的空间或者超过时间限制时,系统要能自动改变访问者的角色。另外,当系统自身环境状态(如系统中饮用水或咖啡等资源不足、某设备当前访问量过大等等)不适合继续访问某资源的时候,系统也要能自适应地改变用户的访问权限。

DRBAC在RBAC的基础上,运用上下文机制动态地改变访问许可,它能满足两个普适计算模式下的访问要求:(1)当用户的上下文改变时,其当前活跃角色相应改变。(2)当环境的上下文改变时,资源对不同用户的角色权限设定相应地改变。

2.2 DRBAC模型

DRBAC继承了RBAC的授权机制,其模型也是在RBAC基础上添加了上下文监测机制,如图1和图2

所示。图1的RBAC模型体现了用户、角色、权限之间的关系,因为有了角色的纽带作用,使得授权管理得以简化,管理开销也相应减少。但图1中角色指派和权限指派是需要管理人员人为预设的,不能根据环境上下文自适应地动态改变。而图2的DRBAC模型正是针对这一点增加了上下文监测代理,随时监测主体(用户)和客体(资源)的状态,并相应地、动态地改变用户的活跃角色和资源授权。

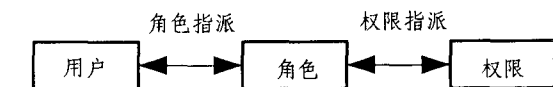


图1 RBAC模型结构图

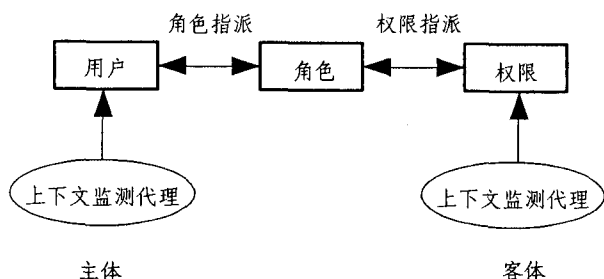


图2 DRBAC模型结构图

2.3 DRBAC访问控制策略描述

在DRBAC中,每个用户都有自己的一个角色子集,每个资源针对不同的用户也设定了不同的角色,每个角色拥有一个权限子集。角色之间是有继承关系的,高一级的角色拥有低角色的访问权限,如图3所示,R21(教授)拥有R31(普通教员)和R32(讲师)的访问权限;权限之间也具有继承关系,如图4所示,P1包含P21和P22的所有权限。中央权威机构CA(Central Authority)控制着整个访问机制。

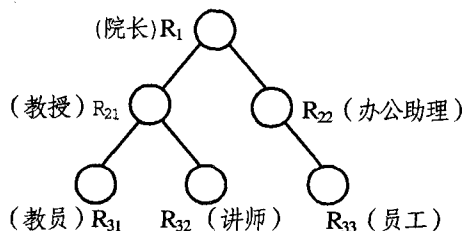


图3 角色层次图

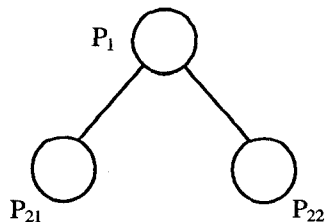


图4 权限层次图

当某用户进入特定空间时,CA根据用户特性为其分配角色子集,并为用户设定上下文监测代理(context agent)。上下文监测代理随时监测用户的上下文环境

(位置、时间等),根据会话(session)的不同,通过角色状态机(role state machine)来改变当前活跃角色(active role)。比如,当张教授带着 PDA 到某办公室后,CA 根据其身份信任状为其分配一个角色子集{教授,讲师,教员},假设代理根据其操作的不同确定“教授”为当前活跃角色,于是张教授就拥有了“教授”的所有访问权限。当张教授离开该办公室时,智能代理监测到用户位置状态发生了变化,于是通过状态机改变其角色,如把张教授的角色改为“教员”。这样,离开了该办公室的张教授就只能拥有普通教员的访问权限。

同时,每个资源也拥有一个上下文监测代理,该代理监控环境状态,并动态地通过权限状态机(permission state machine)改变每个 role 的权限。例如,假设系统设定当某办公室饮用水等足量时,“教授”这个角色拥有 P1 权限(假设为系统根据个人喜好为其冲泡咖啡、奶茶等)。智能代理会始终监测系统环境变量,当发现饮用水用完时,安全策略会自动调整“教授”角色的权限为 P21(假设为不可随意饮用饮料)。当工作人员添加了饮用水后,安全策略应能自动调整“教授”角色的权限为 P1。这样就能实现当环境的上下文改变时,资源对不同角色的权限设定相应地改变,从而保证系统不会因为访问过量而出错或者崩溃。

3 实现设计

3.1 实验环境

运用 ARM7 嵌入式实验箱模拟普适环境下考虑上下文信息的访问控制中的部分机制,即系统根据上下文信息的变化而相应改变用户角色或角色权限。在本实验中表现为,当系统中按键值发生变化时,系统能检测到其变化并通过 LED 灯和 LCD 数据来做出反映。

实验在 x86 Linux 平台(Intel x86 体系结构和 Linux for x86 操作系统)下,交叉编译可以在嵌入式平台(μ clinux 操作系统 + ARM7 体系)下运行的模拟程序,利用实验箱已知资源模拟文中所述 DRBAC 策略的部分实现。

3.2 设计思路

用 8 个带锁的按键来模拟环境变量,其中 d0、d1、d2、d3 模拟用户的上下文状态,d4、d5、d6、d7 模拟资源的上下文状态。按键在按下和未按下状态之间的变换表示环境变量即上下文的改变。系统会从数据总线上检测到数据变化,通过 8 个 LED 灯亮和灭以及 LCD 上的数据值来反映。

3.3 设计框架

使用一片缓冲芯片 74LS244 来把 CPU 外面的输

入数据写入 CPU 的并行总线上,之后,并行总线上的数据被一片数据锁存芯片 74LS273 保留,CPU 通过选中锁存芯片,并读取预先设给锁存器地址内的内容,就可以把数据读出,来确定外面的数据的高低。本实验用 8 个带锁的按键的按下和未按下两种工作状态来表示输入接口的高低状态,然后,再通过 8 个 LED 灯亮和灭两种工作状态,以及 LCD 上用数据值来清楚地反映各状态的输出显示,从而完成模拟的系统检测环境信息变化的实现。

在 C 程序中的实现,如下程序所示:

```
while(1)
{
    urole( ) // 检测 d0~d3 位用户上下文信息变化
    {
        r = (* (volatile unsigned int *)0x8200008); //从缓冲芯片
        74LS244 地址处读取数据
        d0 = r>>7&1; // 提取 d0~d3 位的状态数据
        d1 = r>>6&1;
        d2 = r>>5&1;
        d3 = r>>4&1;
    }

    rpermission( ) // 检测 d4~d7 位环境上下文信息变化
    {
        r = (* (volatile unsigned int *)0x8200008); //从缓冲芯片
        74LS244 地址处读取数据
        d4 = r>>3&1; // 提取 d4~d7 位的状态数据
        d5 = r>>2&1;
        d6 = r>>1&1;
        d7 = r>>0&1;
    }

    data = (d7<<7|d6<<6|d5<<5|d4<<4|d3<<3|d2<<2|d1<<1|d0);
    (* (volatile unsigned *)0x8400000) = data; // 向 74LS273
    写入数据

    if (data != data_pre) // 判断用户上下文和环境上下文有
    没有变化,并通过 LED 或 LCD 显示
    {
        Set_Color(GUI_YELLOW);
        Set_Font(&GUI_Font8x16);
        GUI_DispBinAt(data,170,120,8); // 显示二进制数据
        GUI_DispHexAt(data,170,140,4); // 显示十六进制数据
        GUI_DispDecAt(data,170,160,3); // 显示十进制数据
        data_pre = data;
    }
}
```

在上面的程序中,data_pre = d7d6d5d4d3d2d1d0,其中 d3d2d1d0 表示用户上下文信息,d7d6d5d4 表示环境上下文信息。对 data_pre 可以设置初始值,假设 da-

ta_pre=11111111,用d3=1来描述用户没有进入普适环境,用d7=1来描述教授角色拥有享受个性化饮品服务。当d3所对应的按键按下时(模拟系统检测到某用户进入普适环境系统,即用户位置信息发生变化),系统检测到这个变化后,会相应地改变data的值(模拟给用户赋某个角色,比如给某个用户赋教授角色),并在LED上显示。当d7所对应的按键按下时(模拟环境中水资源不足,即环境上下文信息发生变化),系统检测到这个变化后,会相应地改变data的值(模拟改变角色的权限,这里为data中d7位变为0,假设为教授角色没有权限享受个性化饮品服务),并在LED上显示;同样,当工作人员添加足够的水资源后(用d7按键不按下来表示),系统检测到这个变化,会相应改变data值的d7为1来体现教授角色拥有享受个性化饮品服务的权限。

本实验的上下文信息的变化检测,在普适环境中可以用各种传感器来实现,比如位置传感器可以用来检测用户是否进入环境中等等。

4 结束语

访问控制是安全访问数据必要的环节,在普适计算的智能化环境中尤其重要。文中在介绍桌面计算模式下的典型访问控制策略基础上,提出在普适环境下访问控制的特殊需求,并对普适环境下上下文相关的动态访问控制策略(DRBAC)作详细描述。文中也通过实验模拟了系统检测上下文环境变化并做出反应的过程。最后,提出了DRBAC相关的数据描述设计。

(上接第90页)

参考文献:

- [1] 丁玉美,高西全.数字信号处理[M].第2版.西安:西安电子科技大学出版社,2000.
- [2] 钱文明,刘新宁,张艳丽.基于Cyclone系列FPGA的1024点FFT算法的实现[J].电子工程师,2007,33(2):12-14.
- [3] Chu Chao,Zhang Qin,XIE Yingke,et al.Design of a high performance FFT processor based on FPGA[C]//Proceedings of Design Automation Conference, Asia and South Pacific. Shanghai,China:[s. n.],2005:920-923.
- [4] Sung C H,Lee K B,Jen C W.Design and implementation of a scalable fast Fourier transform core[C]//Proceedings of 2002 IEEE ASIA-Pacific Conference on ASIC, Aug 2-8,2002, Taipei,China. Piscataway,NJ,USA:IEEE,2002:295-298.
- [5] 梁曦捷,肖璋.一种基于FPGA的顺序迭代FFT设计[J].微计算机信息,2005,21(12):135-137.

参考文献:

- [1] Weiser M. The Computer for the 21st Century[J]. Scientific American,1991,265(3):94-104.
- [2] 徐光佑,史元春,谢伟凯.普适计算[J].计算机学报,2003,26(9):1042-1050.
- [3] Sandhu R,Samarati P. Access Control: Principles and Practice[J]. IEEE Communications,1994,32(9):40-48.
- [4] Snyder L. Formal Models of Capability-Based Protection Systems[J]. IEEE Transactions on Computers, 1981,30(3): 172-181.
- [5] 孙尚辉,曹宝象,王廷蔚.扩展RBAC模型在文档管理中的应用[J].计算机技术与发展,2007,17(3):210-213.
- [6] 孟庆荣.协同编辑中访问控制模型的设计与实现[J].计算机技术与发展,2007,17(2):72-74.
- [7] Feinstein H,Sandhu R,Coyne E,et al. Role-based access control models[J]. IEEE Computer,1996,29(2):38-47.
- [8] 邓集波,洪帆.基于任务的访问控制模型[J].软件学报,2003,14(1):76-81.
- [9] 郭慧,李阳明,王丽芬.基于角色和任务的访问控制模型的设计与研究[J].计算机工程,2006,32(16):143-145.
- [10] 景栋盛,杨季文.一种基于任务和角色的访问控制模型及其应用[J].计算机技术与发展,2006,16(2):212-214.
- [11] Zhang G,Parashar M. Context-Aware Dynamic Access Control for Pervasive Applications[C]//Proceedings of the Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS). [s. l.]:[s. n.],2004:219-221.
- [12] 李蕊.上下文感知计算若干关键技术研究[D].长沙:湖南大学,2007.

- [6] 褚振勇,齐亮,田红心,等.FPGA设计及应用[M].第2版.西安:西安电子科技大学出版社,2006.
- [7] 李磊,赵建明.高速可重组 16×16 乘法器的设计[J].微电子学与计算机,2007,24(6):120-122.
- [8] 王定,余宁梅,张玉伦.改进型booth华莱士树的低功耗高速并行乘法器的设计[J].电子器件,2007,30(1):252-255.
- [9] Hsiao S-F,Jiang M-R. Efficient Synthesiser for Generation of Fast Parallel Multiplier[J]. Computers and Digital Technology, IEEE Proceedings,2000,147(1):49-52.
- [10] 贾玉臣,吴嗣亮.快速傅里叶变换的误差分析[J].北京理工大学学报,2005,25(8):739-742.
- [11] 段小东,顾立志.高性能基4快速傅里叶变换处理器的设计[J].计算机工程,2008,34(24):238-240.
- [12] 张傲华,张正鸿,尧德中.一种基于FPGA的高性能FFT处理器设计[J].电子对抗技术,2005,20(4):44-47.