

普适环境中基于角色的隐私保护系统设计

刘 恒, 王铁军, 周明天, 余 堃

(电子科技大学 计算机科学与工程学院, 四川 成都 610054)

摘 要: 对普适环境下的服务隐私保护进行研究, 提出了基于角色的隐私保护系统, 在该系统中采用角色机制在实现服务隐私的同时完善了用户隐私保护. 同时针对服务隐私保护过程中出现的关键问题(过量比对、服务信任迁移、信息过滤等)做出了详细的分析, 提出了一套全面的解决方案.

关键词: 普适计算; 隐私保护; 基于角色; 智能空间; 无线网络

中图分类号: TP393

文献标识码: A

文章编号: 1000-7180(2010)12-0042-05

Design of a Role-based Privacy Protect System for Pervasive Computing

LIU Heng, WANG Tie-jun, ZHOU Ming-tian, SHE Kun

(College of Computing Science and Engineering, UESTC, Chengdu 610054, China)

Abstract: By the study on service privacy protect for pervasive computing, this paper presents a Role-Based privacy protect system to protect the privacy of both user and service. Meanwhile, a comprehensive solution has been presented by the detailed analysis on some key programs(excess comparison, trust transfer, information filter etc).

Key words: pervasive computing; privacy protect; role-based; smart space; wireless network

1 引言

随着普适计算(Pervasive Computing)技术的发展,用户在获得便捷服务的同时,也面临了更大的隐私泄露危险^[1]. 随着对普适计算环境下服务的研究,隐私保护的相关技术也日益显现出其重要性.

在普适计算环境中,用户(乙方, β)为了获取个性化服务,需要向服务提供方(甲方, α)发送包括用户身份、用户位置、个人设置等各类隐私数据. 在获取到用户隐私后,由于服务间的信息共享^[2]或恶意的应用服务方对用户数据进行的数据挖掘^[3-4],都会导致用户的大量隐私信息暴露于危险环境下. 目前对普适计算环境中的隐私保护研究主要侧重于对用户隐私的保护,在用户获得个性化服务的同时减少用户隐私的泄露.

随着研究深入,我们发现作为普适计算环境中的重要组成部分,应用服务也存在隐私保护的需求. 应用服务分布在普适计算环境中,可以被用户动态发现和使用. 用户在使用服务的同时,可能会查询应用服务的相关信息,如服务位置、服务状态、服务的访问策略等. 然而,并非所有用户都有需要或有权限查询服务信息,过于透明的服务信息查询机制将对服务的安全和稳定带来危害. 因此,如何在为用户提供服务的同时,屏蔽无权用户对服务资源的隐私信息的窥视就成为了普适计算环境下隐私保护的一个重要内容.

2 普适环境下的隐私保护

普适计算环境是一个典型的分布式环境. 应用服务分散在环境的各个角落,用户和应用服务之间

通过定位信息进行关联发现. 当用户进入应用服务提供方的有效服务范围时,用户被告知服务的存在. 通过双方约定的机制进行信息交换,从而获取服务的相关属性和状态进行服务使用.

鉴于用户对隐私概念的界定的不同,用户隐私保护(即乙方隐私保护)主要侧重于采用隐私策略实现. 用户通过策略机制编写隐私需求,在获取服务时,对服务所要求用户提供的数据进行隐私策略过滤,只有满足隐私策略的数据才会进入应用服务环境(即甲方). 在早期研究中,我们对乙方隐私保护的方法进行了分析研究,提出了通过安全中间件对用户隐私进行保护^[5-6],在本文中我们将不再讨论乙方隐私保护而将重点放在甲方隐私保护研究上.

对于甲方的隐私保护,在现有研究中,尚无具体研究成果. 随着用户和服务的增多,应用服务提供方的隐私需求渐渐增强. 通过分析发现,甲方隐私主要体现在以下方面.

(1) 信息隐私保护. 应用服务自身包含了大量隐私数据,如:服务位置、服务状态、管理员信息、服务属性等. 某些应用服务并不希望服务自身或服务属性被用户发现,例如:楼道监控摄像头的位置信息不希望被用户获知;教室的投影设备只能由教师用户访问管理,其余身份的用户将无权使用设备,甚至无法发现设备.

(2) 策略隐私保护. 服务的安全策略在与用户策略进行比对的同时,不能泄露服务策略设置信息. 若服务策略泄露,恶意用户将通过对策略的猜测和反复尝试,从而突破策略的约束,访问到其不允许访问的服务.

(3) 信任迁移与角色迁移. 在一个普适环境中通常有多个彼此独立的信任域,每个信任域中又包含多个服务域,如何实现用户对不同信任域间的信任的自动迁移,以及不同服务域间的角色迁移,减少服务与用户的策略过量比对.

针对服务的上述隐私需求,我们在原有的安全中间件平台的研究基础之上,提出了一种基于角色的隐私保护模型,利用 RBAC, PRBAC, PKI/PMI 技术,同时实现了用户隐私保护和服务隐私保护.

3 设计思想

在本设计中,我们将甲方(α)和乙方(β)的隐私

需求进行了明确分割. 鉴于隐私保护需求自身的用户定制性,我们将隐私需求设计作为可定制的模块进行独立开发,通过安全中间件实现整合. 在本设计中,主要关注甲方隐私保护模块.

通过观察,我们发现普适计算环境中的应用服务的位置信息、服务属性、服务权限都相对稳定,因而我们采用轻量目录访问协议(Lightweight Directory Access Protocol, LDAP),利用目录数据库(Service Tree, ST)存储服务属性信息、角色信息及隐私级别描述信息.

3.1 信息隐私保护

如何界定服务隐私以及如何确定服务隐私的级别是服务信息隐私保护的一个重要基础. 服务信息隐私的界定因素主要包括以下方面. ①服务的类型,不同类型的服务对信息的隐私界定不同. 如,监控设备服务认为设备位置是一个高隐私的数据,而打印机服务则认为设备位置属于低隐私数据. ②用户的身份. 服务隐私是一个相对概念,相对于不同用户身份,隐私界定不同. 我们采用隐私矩阵的方式描述服务隐私(表 1),对于管理员用户而言,所有的服务信息均属于低隐私级别,对于普通用户而言,系统审计信息属于高隐私级别,对于受限用户而言,系统状态也属于高隐私级别.

表 1 服务隐私矩阵

ATTRIBUTE						ATTRIBUTE
STATE POSITION NAME OWNER POLICY						ROLE
USER						
USER1	R/W/E	R/W/E	R/W/E	R/W/E	R/W/E	ADMIN
USER2	R	R	R	R		USER
USER3	R		R	R		LIMITED
USER4			R	R		GUEST
.....						

从统计数据可以发现,服务隐私级别随用户身份的不同而产生差异. 然而在普适环境中,用户流动量大,用户身份具有不可预期性,从而使信息隐私级别的划分存在很大困难. 针对这一问题,我们提出安全中间件与 RBAC(Role Based Access Control)相结合的解决方法. 通过角色信息区分用户身份,对服务信息的实施不同级别和权限的管理,从而完成对服务的信息隐私保护.

3.2 策略隐私保护

在服务模型中,用户提出服务访问请求,通过双方的隐私策略信息比对,确定用户的角色,从而赋予用户相应的权限. 在用户权限确定的过程中,策略比

对是角色确定的关键,是否允许用户查看策略信息是角色确定的一个关键问题。

在模型中,我们以 P3P^[7] 规范为标准,采用统一的策略描述语言 XML,进行策略描述.通过安全中间件平台,对用户策略和服务策略进行自动比对.中间件平台作为信任域的管理平台,独立于用户和服务提供方.利用独立的中间件平台来完成策略比对,可以有效地实现用户策略隐私和服务策略隐私的双向保护。

3.3 信任迁移与角色迁移

在普适环境中,不同的应用服务具有不同的服务响应范围,称之为服务域.不同环境提供的服务有着不同的安全等级要求(称之为信任域),用户根据不同安全等级建立对环境的不同信任程度.为了保障用户隐私,当用户在不同的服务域中切换,用户的角色信息也同时发生变化.不同的信任域的切换,将导致用户重新进行双向信任验证。

随着用户路径的变化,这种切换频繁出现,随之带来的过度比对和重复确认令用户操作变得繁琐.针对这一现状,如何使用用户的角色和信任实现平滑迁移,成为了隐私保护中增强用户使用体验的一个关键问题。

(1) 跨服务域的隐私角色迁移。

当用户跨服务域运动时,由于服务的变化,用户的角色信息产生变化.该角色变化主要取决于用户的属性和服务的安全隐私要求.在用户角色上,利用 BASE ROLE(BR)形成了一套通用角色信息,该角色信息包含 B_ADMIN, B_USER, B_LIMITED_USER (B_L_USER), B_GUEST 四种基础角色定义。

服务域可以直接使用 BASE ROLE 角色,也可以针对 BASE ROLE 进行二次开发,做属性和功能的扩展或限制.用户进行跨服务域移动时,通过对服务方和用户的策略比对,确定用户所属角色.如图 1 所示。

用户 Tom 在服务域 A 和服务域 B 之间发生迁移,系统会自动对用户当前持有角色信息进行判断, TOM 在服务域 A 上具有 BR 角色是 (B_GUEST),当 TOM 进入服务域 B 时,系统触发 POLICY MATCH 子模块实现用户的隐私信任角色迁移,避免了繁杂的策略匹配.若用户角色隶属于服务域 A 的自定义角色,则进入新服务域 B 时,通

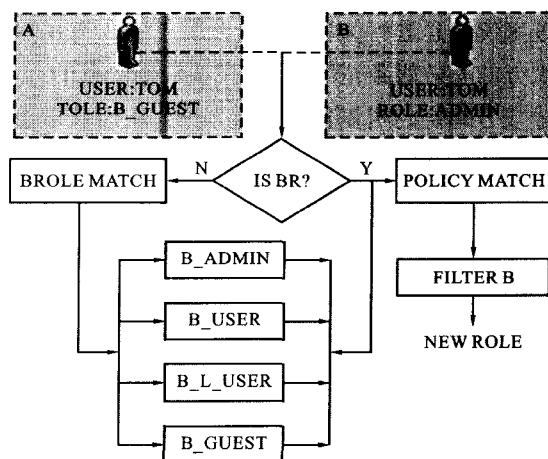


图 1 用户角色判断流程

过 BROLE MATCH 子模块完成服务自定义角色和系统角色之间的映射,经 POLICY MATCH 子模块完成用户属性、隐私策略和服务策略之间的比对,获取对应的服务角色.角色迁移过程中无需用户干预,实现了用户角色的无缝转换。

(2) 不同信任域中的隐私信任迁移

通常不同的信任域隶属于不同的组织机构管理,故而在角色定义上,采用不同的策略.想要实现角色的平滑过渡存在很大的困难,目前常见的做法是通过统一可信任的 CA 组织实现.通过不同隐私等级的划分,各信任域之间建立一个彼此的信任程度链接,利用 PKI 技术和 CA 证书,当用户跨信任域移动时实现基于 CA 证书的信任迁移.在本课题的另一个文献中着重对此问题进行了讨论^[8]。

4 平台架构和设计实现

4.1 平台架构

图 2 是普适计算环境下的基于角色的隐私保护模型的平台架构,在此架构中,主要功能模块可以独立部署,支持灵活配置或替换.该平台采用安全中间件技术,对用户、服务和策略进行了统一存储,减少了用户和服务之间的消息通信量,有效地增强了用户的使用体验。

该隐私保护系统构架在定位服务系统之上,通过底层的定位服务系统获取用户和服务的位置信息.在定位服务系统发现用户进入到信任域的有效范围时,隐私保护平台向用户发出告知信息。

在系统中,鉴于服务数据的固定性和用户数据的同步要求,统一采用 LDAP 数据库进行存储。

4.2 用户管理模块

用户管理模块作为隐私保护平台的用户接口模块为用户的个人信息管理提供了图形化的访问接口.其主要功能包括用户注册、信息管理、用户匿名、用户隐私策略管理等一系列操作.其中,用户信息将保存在用户信息目录(USERS TREE)中.

进入信任域的用户按来源不同分为用户创建和

用户同步两种管理模式.用户创建模式,当用户从非服务区进入服务区,此时用户将作为全新用户进行用户条目的生成.当用户从服务区的一个信任域进入另一个信任域,或者从一个服务区进入另一个服务区,此时,用户数据通过 LDIF 数据交换协议实现同步,用户无需重新注册,系统通过用户同步模式从相邻信任域中通过同步驱动实现用户信息同步.

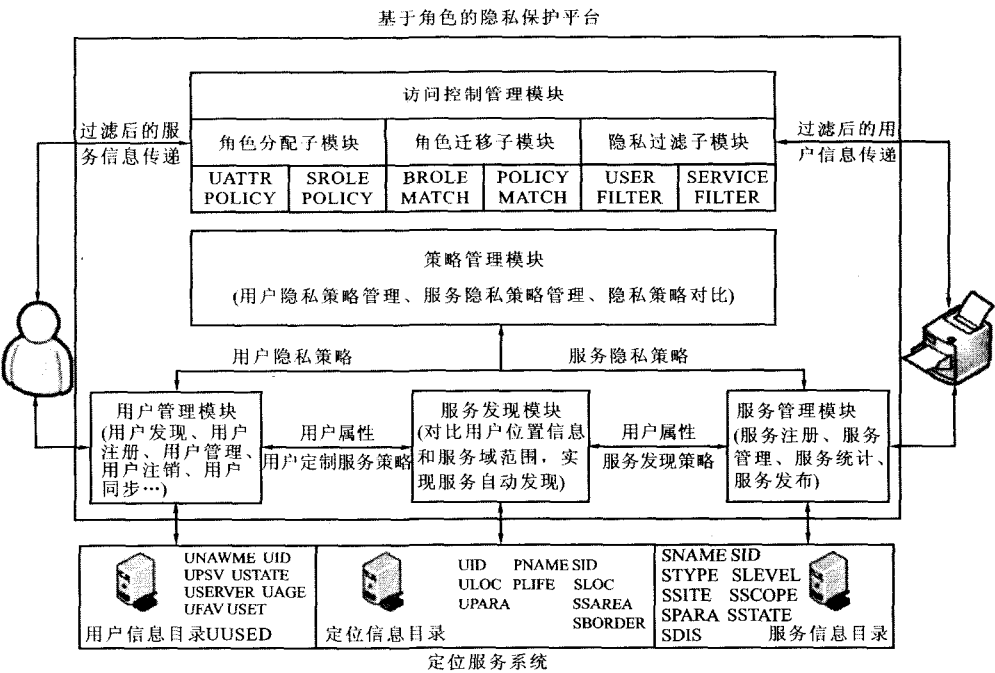


图 2 基于角色的隐私保护模型平台框架

4.3 服务管理模块

该模块负责普适环境中的服务管理.实现服务的注册、变更、发布.应用服务管理员通过该模块对信任域内的服务进行管理维护,包括服务注册、服务属性修改、服务审计信息管理、服务域维护、服务故障汇报等.服务信息通过服务信息目录 (APPS TREE)进行维护.

4.4 服务发现模块

在普适计算中,服务发现是一个重要环节,该模块决定用户的服务获取和服务使用.服务发现模块根据用户位置、用户定制服务信息提示用户可使用的服务位置,并将用户定制服务列表保存至用户数据库中.若用户定制了服务发现策略,该模块将调用用户服务发现策略自动为用户提示相关服务.服务发现模块根据用户服务定制可以提供个性化的服务发现和联想服务关联等增值服务.

同时通过服务方定制的服务发现策略,可以对

部分特殊服务进行服务隐藏.当用户身份或其他属性不符合服务发现策略,用户将无法获知其周围环境的服务,从而改变传统服务发现模式中服务的被动暴露状态.如:酒店顾客在酒店范围能发现灭火设备、自助餐饮服务,而对于酒店服务人员,在相同位置可以发现灭火设备,酒店考勤设备,清洁设备、打印机服务等服务.

4.5 策略管理模块

该模块主要实现用户策略和服务策略自动比对.在平台中,用户策略和服务策略通过 XML 语言基于标准的 P3P 隐私策略规范进行设计,实现机器比对.

模块通过对用户隐私策略设置的正则表达式与服务隐私策略的正则表达式的映射比对,得出比对结果(匹配权值, T),若用户和服务方均采用标准 P3P 策略模式, T 为布尔值.若用户方采用非标准 P3P 策略机制,则 $T \in [0, 1]$,通过用户设定不同信任级别完成匹配判定.采用权值范围模糊匹配模式

可以有效兼容非标准 P3P 策略客户端。

4.6 访问控制管理模块

访问控制管理模块作为平台的关键模块主要负责用户角色的生成、角色用户对服务的访问,用户跨服务域的角色迁移。通过访问控制平台,可以有效地实现对服务的保护。它包括以下子模块。

角色分配子模块:根据用户的隐私策略从用户数据库中取出用户可用属性,同时结合服务方隐私策略对服务方可分配角色进行比对,为用户自动划分角色并形成用户角色对(user, role, permission, object)。

角色迁移子模块:实现用户跨服务域迁移时的角色迁移。角色迁移子模块会提取用户在前一个服务域的角色信息通过服务策略比对和角色映射完成跨服务域的角色迁移(如图 1 所示)。

隐私过滤子模块:该模块是一个双向过滤替换模块

用户到服务,在将用户信息提交给相应服务之前实现用户信息过滤,将服务不需要的用户信息进行过滤或替换,如 tom 被分配了 guest 角色,则 tom 的姓名、年龄等数据将可以采用低精度替换原则进行保护。

服务到用户,将服务信息提交给用户移动终端之前,根据用户角色进行服务信息过滤,如对于 guest 用户 TOM 而言,自助售货机的工作时间属性、货物更新数据均属于无用信息可以实现过滤。

同时,当用户跨信任域移动时,策略管理模块将两个信任域的不同隐私策略要求进行比对,当用户从高隐私策略环境进入低隐私策略环境时,向用户发出提示信息。

5 结束语

就目前缺乏研究的服务隐私领域进行分析,提出基于角色的服务隐私管理模式,在提供服务的同时保障了服务的隐私,实现了服务的信任传递。同时,在该系统中,通过对角色的级别设定,实现了服务信任的自动迁移,有效地降低了用户信任的比对,在实现隐私保护的同时,降低了用户使用的复杂性。

本研究的后续研究包括:①隐私级别的界定和

隐私信息内容的范围和筛选;②隐私的描述;③友好且完善的用户隐私策略制定界面。

参考文献:

- [1] Rezgui A, Ouzzani M, Bouguettaya A, et al. Preserving privacy in web services [C]// Proceedings of the 4th international workshop on Web information and data management. McLean, Virginia, USA; ACM Press, 2002: 56—62.
- [2] Louise Barkhuus A D. Location-based services for mobile telephony: a study of users' privacy concerns[C]// Proceedings of the 9th IFIP TC13 International Conference on Human-Computer Interaction. Zurich, Switzerland; ACM Press, 2003: 709—712.
- [3] Agrawal PR, Srikant R. Privacy-preserving data mining [C]// Proceedings of the ACM SIGMOD Conference on Management of Data. Dallas, Texas, USA; ACM Press, 2000: 439—450.
- [4] 桂琼,程小辉.一种隐私保护的分布式关联规则挖掘方法[J]. 微电子学与计算机, 2009, 26(9): 57—60.
- [5] 刘恒,王铁军,余堃,等.一个普适计算环境中的定位隐私保护模型[J]. 计算机应用研究, 2009(6): 2110—2113.
- [6] 周华,孟相如,张立.基于中间件的入侵容忍体系结构研究[J]. 微电子学与计算机, 2008, 25(12): 67—69.
- [7] Marchiori M, Cranor L, Langheinrich M, et al. The platform for privacy preferences 1.0 (P3P1.0) specification[EB/OL]. (2002-11-12)[2009-03-13]. [http://www.w3.org/TR/P3P/\(2002\)](http://www.w3.org/TR/P3P/(2002)).
- [8] 谢鸿波,周明天.基于概率和条件逻辑的 PKI 信任模型推理[J]. 小型微型计算机系统, 2006, 27(1): 69—71.

作者简介:

刘恒女,(1980—),博士生.研究方向为无线网络、普适计算、智能空间。

王铁军男,(1979—),博士生.研究方向为无线网络、网格计算。

周明天男,(1939—),教授,博士生导师.研究方向为网络计算、分布式计算与信息安全。

余堃男,(1967—),教授,博士生导师.研究方向为无线网络、中间件、并行计算。