普适计算环境中的访问安全性研究

徐金芳，张永胜
（山东师范大学 信息科学与工程学院，山东 济南 250014）

摘 要：对具有开放性特点的普适计算环境来说，用户的多样性是不可避免的，而用户的多样性带来了安全威胁，为此把用户分为固定用户和流动用户，在使用角色访问控制的普适环境中运用单点登录技术，提高了管理的效率，简便了固定用户的使用，并且对实现上的细节做了概述。又针对不同类型用户进行了访问时间的限制，主要是限制了流动用户的权限，限制其分配角色的使用时间，降低其潜在的破坏性和风险，从而提高了相对开放的普适环境的安全性。

关键词：普适计算；角色访问控制；单点登录；时间限制
中图分类号：TP393.03 **文献标识码**：A **文章编号**：1673-629X(2009)03-0161-03

Study the Security of Access Control in Pervasive Computing Environment

XU Jin-fang, ZHANG Yong-sheng
(School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China)

Abstract: The diversity of users has brought security threats to the open pervasive computing environment. Thus the user is divided into fixed users and unfixed users. It employs a single sign-on technology in pervasive environment which used RBAC model, the management efficiency was improved, and the realization of the details were outlined. And different types of users executed a time restriction, the permissions of the unfixed users were restricted, raising the security to the relatively open environment.

Key words: pervasive computing; RBAC; single sign-on; time restrictions

0 引 言

在普适计算模式下，计算设备和传感器节点等设备与环境无缝集成，提供随时随地的智能服务。因为普适计算涉及到商业领域、基础设施和个人利益，相关的安全攻击可能利用网络、协议和密码算法等的漏洞形成威胁，所以普适计算环境中的安全研究至关重要。

根据著名的熵增原理，实际有意义的是受外界影响下熵的变化[1]，即它与环境不能割裂，而环境与资源都是低熵资源，具有同等的地位。文献[1]中指出把人、机、环境看作是一个系统的三大要素，要从系统总体出发研究相互关联的复杂系统，所以要研究普适计算的安全问题，包括人在内的环境因素不容忽视。在角色访问控制(RBAC)中通过引入角色概念，实现了用户与权限的逻辑分离，屏蔽用户的多样性，但并不代表引入角色后用户多样性问题就彻底解决[2]。

收稿日期：2008-07-07
基金项目：国家自然科学基金(90612003)
作者简介：徐金芳(1982-)，女，山东东营人，硕士研究生，研究方向为信息安全、访问控制及普适计算研究；张永胜，副教授，研究方向为 Internet 信息处理、XML 应用研究。

文中的主要工作：提出研究普适环境的安全性必须考虑其最大特点——开放性，着重研究普适环境中的角色访问控制用户(主体)的不同。在开放的普适环境中将用户分为固定用户和流动用户，并使用了单点登录技术，并对流动用户进行了访问时间的限制。

1 相关技术

由于用户在访问不同业务系统时需要独立访问该业务系统；同时，用户需要在各系统间频繁地切换，操作较复杂，无法快速地获得相关业务信息并加以分析利用，此外，用户在进行业务操作时，需要分别登录到不同的应用系统中，由于系统较多，用户账号或密码遗忘现象时有发生，或者一套简单用户名和密码多系统使用，造成保密强度降低等问题；而在安全性和系统管理方面，企业需要大量的 IT 技术管理人员，分别管理和维护不同系统(如：ERP、统计分析、OA、财务、Notes 系统等)的用户信息。需要建立可靠、安全、保密的业务系统网络环境，保证企业业务不受破坏和干扰。

针对这种状况，企业希望通过实施建立企业级的单点登录系统和安全防护系统，为企业用户提供统一

的信息资源认证访问入口，建立统一的、基于角色的和个性化的信息访问、集成平台。以下对文中用到的相关技术进行简要说明。

(1)普适计算：就是当使用者与普适环境交互时，充分利用分布在环境中的传感器和计算设备来识别使用者，并向使用者提供智能服务，如传感器，计算设备和通讯设备需要主动感知使用者的行为，并根据使用者的行为和喜好以及周围的环境变化进行调整，以提供灵活方便的服务[3]。

(2)单点登录(SSO)：在门户项目中，经常会遇到如何实现单点登录的问题。用户只需登录一次，即可通过单点登录系统访问后台的多个应用系统，无需重新登录后台的各个应用系统。后台应用系统的用户名和口令可以各不相同，并且实现单点登录时，后台应用系统无需任何修改。

(3)基于角色访问控制：即 RBAC，作为对传统访问控制的最佳替代技术，目前受到越来越多的关注。在 RBAC 中权限(许可)与角色相联系，用户按其职责和资格被分配到相应的角色中，从而获得角色中的权限。

2 普适计算中的单点登录

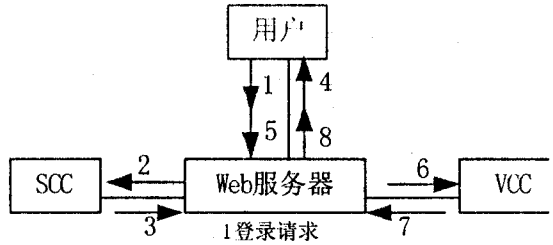
2.1 固定用户单点登录的实现

由于固定用户的访问频率高，对系统使用单点登录技术无疑会大大方便用户。HTTP 协议的无连接性不能保证用户访问的连续性，故用 Cookie 来保存相关的信息，以便用户在下次访问服务器时不再提供相同的信息[4]。

用户在首次访问服务器时向服务器发出登录请求，提供自己的用户 ID 和密码(PSW)，Web 服务器把从用户接收到信息包括用户 IP 传递给 SSC(Set - Cookie Component)，以生成安全 Cookie，然后把安全 Cookie 传回 Web 服务器，再由 Web 服务器把安全 Cookie 返回用户浏览器保存。当用户再次向服务器发出服务请求时，用户浏览器会自动把安全 Cookie 发送给 Web 服务器。Web 服务器把接收到的安全 Cookie 提交给用于验证的组件 VCC(Verify - Cookie Component)。VCC 在完成验证后向 Web 服务器返回该用户有效的角色集。然后，Web 服务器根据返回的角色信息来为用户提供相应的服务或拒绝用户的服务请求。如图 1 所示。

整个过程中用户只登录一次，在以后的访问中，安全 Cookie 将为用户提供身份认证，并向服务器提供用户所属角色信息，从而实现一次登录，全网漫游。在普适环境中角色访问控制前提下相对固定用户使用单点登录过程为：

用 Roles - Cookie 表示用户所属的角色集。它是用户在系统中所属的所有角色的集合，服务器可以直接根据这些角色来控制用户的访问。由于角色在系统中相对稳定，因此可将用户角色信息保存在 Cookie 中，这样 Web 服务器就可直接根据 Cookie 中的角色信息来控制用户的访问，从而提高了访问效率。



1登录请求
2用户信息
3，4，6安全Cookie
5服务请求
7Roles
8服务结果

图 1 单点登录过程图

首先验证用户身份，得到证实后 SCC 从角色服务器上取回用户所属的角色集(Roles)，再送至签名组件进行签名，签名后的 SCC 生成安全 Cookie，传至 Web 服务器。VCC 对安全 Cookie 的签名进行验证，并验证其有效期，之后验证其是否被人盗用，上述检验全部通过后，调用相关函数验证 Roles - Cookie 中的角色信息是否有效，因为在生成 Cookie 后，服务器中的角色可能发生改变。管理员通过浏览器进行安全管理，Web 服务器记录角色发生的改变。在验证时把用户不再拥有的角色从角色集中删除，并将用户新增角色加入角色集，最终得到有效的角色集，Web 服务器根据有效角色集为用户提供服务。

2.2 单点登录分析及实现

根据对用户的大体分类，并考虑单点登录具体的实现方案。在普适环境中使用 ActiveX 插件这种方式，这种方式优点在于 B/S、C/S 结构中都适用。每个加入到 SSO 的系统都需要一个配置文件，这个配置文件是放在 SSO 服务器上的。用户到其他系统的认证，是通过这个配置文件来完成的。SSO 在配置完成后，有一个 URL 连接，专门用于管理其他应用系统的密码。每个用户登录到 SSO 服务器后，首次访问某个应用系统时，如果该系统的用户名和口令信息在 SSO 服务器上没有保存，会自动重定向到密码配置页面，让用户配置密码。密码配置完成后，以后用户再访问应用系统时，就直接进入相应的应用系统了。

通过组合简单的访问控制和 SSO 功能，为客户提供一个即插即用的 SSO 解决方案。用户无须修改应

用系统(包括Web应用系统和C/S结构应用系统),自由选择前置代理和后置代理或组合使用方式。只需简单的配置,即可使用SSO应用功能。既可通过ActiveX插件这种方式,也可通过客户端的方式。在系统配置中需存储专门的用户认证信息列表。如表1所示。

表1　用户认证信息

用户	系统	用户名	密码
001	系统甲	A	6616
001	系统乙	B	8818
001	系统丙	C	44A1

另外多个应用系统,可能不在同一个域下,虽然会话本身是保存在服务器端,但是会话id是需要Cookie来传递的,而Cookie不允许跨域访问,而且考虑到各个系统的开发工具也各不相同,即使在同一个域下,不同的开发工具所开发的应用程序之间也很难共享会话,因此要用共享会话的方式来实现单点登录也不现实。因此通过在客户端浏览器、单点登录系统和Web应用系统之间传递临时会话,并让Web应用系统直接到单点登录系统中获取认证信息来实现单点登录。为保证不同开发工具都能够到单点登录系统获取认证信息,采用xml-rpc在Web应用系统和单点登录系统之间进行通讯。用户登录单点登录系统时,通过单点登录系统用户表中的字段来验证用户身份。登录以后,用户可以设置各个系统到该系统用户的映射关系。设置好以后,当通过该系统进入其他某个Web应用系统时,该系统会为该用户和该系统生成一个临时会话编号(hash),并转到Web应用系统中的登录检测页面,登录检测页面通过获取到的临时会话编号,来调用单点登录系统的获取用户名和密码的xml-rpc API,如果用户名密码正确,则转到正常登录后的页面,如果不正确,则转到登录错误的页面。这里,xml-rpc API在返回用户名和密码后,将删除单点登录系统数据库中相应的临时会话,并且临时会话存在的时间也是尽可能的短,因此只要保证服务器之间的对话不能被监听,即可保证安全性。

3　流动用户访问时间的限制

按照熵增原理,低熵物质具有在适当的空间"扩散"能力,正是这种扩散能力显示了其本身的潜力。因为在相对开放的普适环境中,用户是相对流动的,所以不仅将其看作服务的接受者,还要将其看作安全的破坏者。鉴于此,将时间限制信息加入到XML文档之中[5],对流动性较大的用户,限制其分配角色的使用时间,降低其潜在的破坏性和风险。

根据XML的特点,在XML文档[6]之中加入时间限制信息有两种。其一是通过增加标签增加时间限制信息,另外一种就是为XML文档中增加属性:ValidTime(True/False)表示系统有效时间,TransactionTime表示事务的开始时间和结束时间。在有效时间为True时,才能继续用TransactionTime属性进行时间限制。如表2所示。

表2　对用户角色时间限制举例

角色	ValidTime	TransactionTime
Administator	T	2008-1-1~2009-2-1
visitor	T	2008-1-1~2008-1-2

```
<Role
TransactionTime="[2008-01-01~2009-02-01]" ValidTime
="T">
Administator
</Role>
<Role
TransactionTime="[2008-01-01~2008-01-02]" ValidTime
="T">
Visitor
</Role>
```

通过上面时间限制属性的添加,不仅可以及时地限制用户增强安全性,也可更方便地获得某段时间内的文档,以便进行查询。但要按时间实现XML文档的有效查询,还需对XML的查询语言进行扩展。这样建立起一套可行的安全、易用的网络环境[7],最大限度地降低突发性灾难对关键业务环境的影响。

4　结束语

网格技术、计算机技术和传感器技术的发展,推动了普适计算研究的发展。文中是从普适计算环境的特点和安全需求出发,分析了用户对安全的威胁并将其分类[8],在安全机制应该根据用户需求的原则且使用RBAC的前提下研究了单点登录技术及实现,具有必要的灵活性和安全性。最后对用户进行时间限制,增强系统安全性。

参考文献:

[1] 屈柳玲,李正良.从熵和火用的视角论人-机-环境关系[J].科学技术与哲学,2008(4):55-58.

[2] LI Pei-wu,LU Zheng-ding. Encapsulation and Distributed Management of the Role Ranges in RBAC[J]. Mini-microSystems,2005,26(2):252-255.

[3] 李世群,陈克非.普适计算中的安全问题研究[D].上海:上

(下转第167页)

若想让系统每次启动时都能自动地加载静态ARP,则可将这个批处理软件拖到“windows——开始——程序——启动”中。使用静态ARP缓存增大了网络维护量,在较大或经常移动主机的网络中这样做更为困难。使用静态ARP缓存只能防止ARP欺骗,对IP地址冲突、Flood攻击仍然没有办法阻止。

2)对病毒源头的机器进行处理,杀毒或重装系统。此操作非常重要,因为解决了ARP欺骗的源头PC机的问题,就可以保证内网免受攻击。

3)用可防ARP攻击的交换机(彻底防治)[6]。使用三层交换机,绑定“端口-MAC-IP”,限制ARP流量,及时发现并自动阻断ARP攻击端口,合理划分VLAN,彻底阻止盗用IP、MAC地址,杜绝ARP的攻击,这也是目前防止ARP攻击的最有效方法之一。

5　结束语

网络欺骗攻击作为一种非常专业化的攻击手段,给网络安全管理者带来了严峻的考验。ARP欺骗是一种典型的欺骗攻击类型,它利用了ARP协议存在的安全漏洞,并使用一些专门的攻击工具,使得这种攻击变得普及并有较高的成功率。文中通过分析ARP协议的工作原理,探讨了ARP协议从IP地址到MAC地址解析过程中的安全性,给出了网段内ARP欺骗的实现过程,提出了一种有效的检测系统和几种可行的解决方案,以最大限度地杜绝ARP欺骗攻击的出现。总之,对于ARP欺骗的网络攻击,不仅需要用户自身做好防范工作之外,更需要网络管理员应该时刻保持高度警惕,并不断跟踪防范欺骗类攻击的最新技术,做到防范于未然。

参考文献:

[1] Plummer D C. An Ethernet Address Resolution Protocol[M]. 北京:机械工业出版社,1982.

[2] 谢希仁. 计算机网络[M]. 第4版. 北京:电子工业出版社,2003.

[3] Nachreiner C. Anatomy of an ARP Poisoning Attack[EB/OL]. 1999-07-11. http://www.watchgu-ard.com.

[4] Liruixue. ARP协议的缺陷及ARP欺骗的防范[M]. 北京:机械工业出版社,2007.

[5] 任　侠,吕述望. ARP协议欺骗原理分析与抵御方法[J]. 计算机工程,2003,29(9):127-128.

[6] 宋　志. 一种基于PVLAN的反ARP欺骗的技术实现方法[J]. 计算机安全,2007(10):55-59.

(上接第160页)

跟踪和发现客户的流失趋势,及早采取预防措施,最大限度地降低客户流失率。

4　结束语

研究和实现了决策树分类算法ID3,通过该算法作用于银行数据,得出一个银行客户流失的模型,通过提取模型中的规则,对于银行预测客户流失特征具有一定的辅助作用。

参考文献:

[1] Han Jiawei, Kamber M. Data mining: Concepts and Technique [M]. Beijing: China Machine Press, 2006.

[2] 盛昭瀚,柳炳祥. 客户流失危机分析的决策树方法[J]. 管理科学学报,2005,8(2):20-25.

[3] Tan Pang-Ning, Steinbach M, Kumar V. 数据挖掘导论[M]. 北京:人民邮电出版社,2006:89-193.

[4] Rud O P. 数据挖掘实践[M]. 北京:机械工业出版社,2003:225-264

[5] 王黎明. 决策树学习及其剪枝算法研究[D]. 武汉:武汉理工大学,2007.

[6] 任　伟,丁荣涛. 改进的ID3算法在学习模型的研究与应用[J]. 福建电脑,2007(8):109-110.

[7] 杨　明,张载鸿. 决策树学习算法ID3的研究[J]. 微机发展(现更名:计算机技术与发展),2002,12(5):6-8.

(上接第163页)

海交通大学,2007.

[4] 任　栋,刘连忠. 一种Web应用环境下安全单点登录模型的设计[J]. 计算机工程与应用,2002,38(24):174-176.

[5] 黄　建,倪惜珍. 引入时间特性的角色访问控制[D]. 北京:中国科学院研究生院,2003.

[6] Matheus A. How to declare access control policies for XML structured information objects using OASIS' eXtensible Access Control Markup Language (XACML) [C]//. proceedings of the 38th Hwaii Conference on System Sciences. [s. l.]: [s. n.], 2005.

[7] Chou Shih-Chien. LRBAC: A Multiple-Levelled Role Based Access Control Model for Protecting Privacy in Object-Oriented Systems[J]. Journal of Object Technology, 2004, 3(3): 91-120.

[8] 许　谦,雷咏梅. 一种增强访问控制的服务发现机制[J]. 计算机技术与发展,2007,17(5):99-100.