第 34 卷 第 9 期 计 算 机 工 程 2008 年 5 月
Vol.34 No.9 Computer Engineering May 2008
·安全技术· 文章编号：1000—3428(2008)09—0180—03 文献标识码：A 中图分类号：TP309

异构环境下新型域的研究与设计

王文冰[1,2]，李晓勇[2]
(1. 郑州轻工业学院计算机与通信工程学院，郑州 450002；2. 上海交通大学信息安全工程学院，上海 200240)

摘 要：针对异构环境下账户管理无法统一的情况，提出一个基于跨平台新型域的解决方案。在异构环境下，该方案具有账户统一存储、统一认证和统一管理的功能，兼顾安全性和可实施性，实现一个完善的账户统一管理系统。实验结果证明了该方案的有效性。
关键词：异构环境；账户管理；轻量级访问协议

Research and Design of New-style Domain in Heterogeneous Environment

WANG Wen-bing[1,2], LI Xiao-yong[2]
(1. School of Computer and Communication Engineering, Zhengzhou University of Light Industry, Zhengzhou 450002;
2. School of Information Security Engineering, Shanghai Jiaotong University, Shanghai 200240)

【Abstract】 Aimming at separated accounts management in heterogeneous environment, this paper proposes a new solution which bases on a heterogeneous domain——Heterogeneous System Management Domain(HSMD). It solves the conflicts in account storing modes and authentication mechanism of different operating system. With attention to both security and practicability, a perfect unified heterogeneous accounts management platform is implemented. Experimental results show the method is effective.
【Key words】 heterogeneous environment; account management; Lightweight Directory Access Protocol(LDAP)

1 概述

目前，各种操作系统使用独立的账户存储和用户认证，为企业带来了管理负担和安全风险。Windows 系统使用 NT 域控制器或活动目录(AD)，统一管理认证网络中的 Windows 用户。其中，适用于 Windows 2000 系列服务器上的活动目录，基于 LDAP 目录来存储网络对象，采用经过扩展的 Kerberos 协议作为用户认证机制，统一管理 Windows 系统的账户存储、用户认证和资源管理。在 UNIX 领域中，用户信息通常保存在本地文件中，如/etc/passwd 文件。此外，UNIX 系统将网络信息服务、LDAP 目录等作为账户统一存储数据库。为简化应用程序、确定信息源，Solaris2.0 引入名称服务器交换(NSS)体系结构。通过标准接口和配置文件，NSS 使 UNIX 应用和信息保存机制不再静态绑定。类似 NSS 的实现机制，UNIX 系统使用可插式认证模块(PAM)作为应用程序和各种认证机制的中间层，毋需修改代码，即可在多种认证方式中切换。

Windows 系统和 UNIX 系统的账户信息格式和用户认证机制的不兼容，导致企业必须为异构系统部署多个单独的账户管理平台，从而使用户为登录不同平台而持有多个账户信息，不仅使用不方便，而且增加了管理员的工作和网络系统的安全风险。一些企业为解决这个问题，在多个账户数据库之间建立数据同步，如 Novell 公司的 NAM，这不仅没有解决账户管理和系统安全方面的问题，又带来软硬件资源浪费的新问题。

面对这种情况，企业急需一种能够统一管理异构系统账户的解决方案，不仅使网络部署更灵活，而且减轻企业的管理负担。基于 Samba 和 LDAP 目录，文献[1]提出一个异构环境下操作系统账户和网络服务账户统一保存的单点登录系统。虽然统一存储账户信息，却没有实现认证机制的统一化，尤其是它使 Windows 客户端不得不退回到安全性较差的 NTLM 认证方式。另一种解决方案是 PADL 公司的 NIS/LDAP 网关。它模拟 NIS 服务器，使账户信息从 LDAP 目录服务器而非本地文件读取，为信息在 UNIX 客户端和 Windows 域控制器之间的传输搭建桥梁。和文献[1]一样，NIS/LDAP 网关没有实现异构系统账户的统一认证，UNIX 客户端仍使用本地认证的方式完成对登录用户的认证工作，影响了账户信息的安全性和认证过程的高效性。

Samba 软件的最初目的是通过在非 Windows 平台上模拟 Windows 专属的 CIFS/SMB 协议来实现各种平台上文件和打印服务的无缝共享。自 2.8.8 版本开始，Samba 实现了 Windows NT 的域控制器功能，使 UNIX 服务器可以取代 Windows 域控制器管理一个 NT 域。本文基于 Samba 的域控制器功能，设计了一个新型的集成多种操作系统的 HSMD 域，不仅解决了不同操作系统的账户格式冲突问题，还实现了 MS Kerberos 协议和标准 Kerberos 协议之间的互操作，从而达到异构账户的统一管理认证。

2 HSMD 模型

通过 HSMD 域，本文提出一个易于扩展和部署的异构系统账户统一管理方案。HSMD 以 UNIX 域控制器为中心，管理由 Windows 和 UNIX 系统构成的异构分布环境。用户登录

作者简介：王文冰(1978－)，女，硕士研究生，主研方向：密码与网络安全；李晓勇，副教授、博士
收稿日期：2007-06-30 **E-mail：**wang_wb@sjtu.edu.cn

域中任何主机时，通过 Kerberos 协议向域控制器认证用户身份，认证通过后，用户可透明访问支持 Kerberos 协议的服务。

HSMD 域既不属于传统的 Windows 域也不属于传统的 NIS 域，而是集成管理 Windows 系统和 UNIX 系统的域。其中，接受域统一管理的用户、主机、服务统称为域成员。在 HSMD 域中，域控制器平等对待异构平台的域成员，并提供完善、一致的认证管理服务。图 1 为 HSMD 域的工作模型。

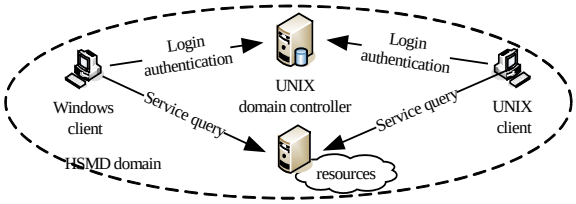

图 1　HSMD 域的工作模型

在 HSMD 域中，用户请求网络服务可概括为：

(1)登录认证，当用户从 Widows 或 UNIX 系统选择登录域时，首先向域控制器发送认证请求。域控制器根据认证请求所包含的用户信息和数据库中的授权信息，决定用户是否被允许登录。如果允许，域控制器返回一个标识认证通过的凭证。

(2)请求服务，当成功登录的用户请求域中任何平台上的服务时，向该服务器发送包括域控制器颁发凭证的认证请求。域控制器根据此凭证得知此用户合法，基于用户权限决定自己所能提供的服务。

从工作流程可以看出，HSMD 域统一保存账户信息，域中服务基于账户信息认证用户。所以，HSMD 域同时具备操作系统级别的单点登录功能。

3　系统设计

3.1　账户存储

轻量级访问协议(Lightweight Directory Access Protocol, LDAP)是目录服务访问协议的一种，它基于开销小且使用广泛的 TCP/IP 协议栈，只保留了使用频繁的功能，目前已发展到 LDAPv3 版本。基于 LDAP 目录的层次结构、存取访问控制机制和存储格式可定制等优势，HSMD 选择它作为域的账户统一存储数据库。

目录中所有条目按层次模型组织，是一个分级或类似树状的结构，被称为目录信息树。目录信息树中的对象被称为目录服务条目，由唯一标识名(DN)确保唯一性。每个条目是多个属性的集合，其类型由对象类确定。对象类分为 3 类：说明条目基本结构的结构对象类(Structural Object Class)，对条目结构进行辅助说明的辅助对象类(Auxiliary Object Class)，专门用来定义基本数据模型的抽象对象类(Abstract Object Class)。条目的对象类属性值决定了此条目中必须或可能包含的属性，必须包含的属性被称为强制属性；可能包含的属性被称为可选属性。

目录信息树的设计与系统所能提供给用户的服务紧密相关，对企业来说，它是部署 LDAP 目录服务的关键环节，包括确定唯一标识名、定义架构、搭建架构等工作。HSMD 域中的 LDAP 目录信息树所存储的内容分为 3 个部分：计算机账户，用户账户(服务账户和用户账户采用相同的形式，它的密码取决于服务安装者的密码)和组账户，分别存储在 DN 为 ou=Computers,dc=domain_name, ou=Users, dc=domain_name, ou=Groups, dc=domain_name 的组织单元中。账户与对象类之间的对应关系如表 1 所示。

LDAP 目录的组账户被分为两类，这与 Windows 系统和 UNIX 系统对用户和组的管理方法有关。在 Windows 系统中，用户是否隶属一个组是可选的；在 UNIX 系统中，每个用户必须隶属一个组。对于 HSMD 域来说，每个隶属于 Windows 组的域用户必然隶属于某个 UNIX 组，反之不成立。所以，除了集成 Windows 组信息和 UNIX 组信息的组账户外，还需要专门存储 UNIX 组信息的 UNIX 组账户。

表 1　目录信息树中的账户及其所属的对象类

账户	账户条目所属的对象类
计算机账户	Account, sambaSAMAccount, posixAccount, krb5KDCEntry
UNIX 组账户	PosixGroup
组账户	posixGroup, sambaGroupMapping
用户账户	inetOrgPerson, sambaSAMAccount, posixAccount, automount, krb5KDCEntry

UNIX使用UID和GID[2]分别标识用户和组。与Windows系统的安全标识符号(SID)相同，UNIX系统的用户名只是为了方便用户而设计的符号，真正用于操作系统识别用户信息的则是UID和GID。两者不同的是：由于UID和GID的分配与组成过于简单，导致不同主机的UID和GID极易重复，对系统安全造成严重威胁。为解决这个问题，HSMD把域中所有UNIX账户的UID和GID整合到一个命名空间，由域控制器进行统一分配。其中，0~500 的UID/GID预留给UNIX系统账户，比如 root, adm, tty 等账户；500~999 的UID/GID预留给Windows的系统账户，比如Administrator, Guests组等账户；其余的UID/GID按先来后到的顺序被统一分配给新添加的用户或组账户。

3.2　统一认证

用户认证是一个业务系统保证安全的重要元素，选择可靠的认证机制尤为重要。Kerberos协议的双向认证、集中存放账户条目等特性使它成为HSMD域实现用户统一认证的安全机制。从工作流程[3]可以看出，它具备了单点登录系统的“一次登录，全网漫游”的特征。

虽然 Kerberos 协议是个公开标准协议，但为了更好地服务于 Windows 客户端，微软对标准协议做了诸多扩展，比如自定义票据的授权数据域格式(标准 Kerberos 协议预留了授权数据域，但没有限定内容以及使用方法)、添加非标准加密算法和引入公钥加密体制等，这无疑为 HSMD 域实现基于 Kerberos 协议的异构系统统一认证带来困难。Heimdal Kerberos 为实现与 MS Kerberos 的互操作做了许多扩展，目前它支持公钥加密以及微软专有的 RC4-HMAC。

Heimdal Kerberos具有良好的稳定性、扩展性和兼容性，它使用一个抽象层HDB把账户数据库和Kerberos的其他实现模块隔离开来[4]。通过HDB和hdb-ldap插件，Kerberos可以选择LDAP目录做为账户数据库，并基于扩展性考虑，Heimdal Kerberos的hdb-ldap插件设计为可替换的，这为本文提供了扩展Heimdal Kerberos的可能。当Heimdal Kerberos选用LDAP目录做为后端数据库时，使用 krb5KDCEntry 对象类定义Kerberos的安全主体；而HSMD域中的LDAP目录使用自定义的目录信息树结构和目录条目属性。这为HSMD域整合Heimdal Kerberos带来新的问题：LDAP目录保存的账户属性不能被Heimdal Kerberos的KDC识别。为解决这个问题，本文设计一个新的hdb-ldap插件担任属性转换的角色。Heimdal Kerberos 使用 krb5KDCEntry 对象类表示安全主体条目，HSMD域使用posixAccount, sambaSamAccount等对象类表示用户和计算机账户。hdb-ldap需要在KDC存取账户数据库时完成这两类对象类之间的属性映射工作，映射关系如表 2 所示。

表 2　映射关系

Krb5KDCEntry 对象类属性	SambaSamAccount 对象类属性	描述
krb5PrincipalName	uid	用户名或者计算机名
krb5ValidEnd	sambaKickoffTime	用户自动注销的时间戳
krb5PasswordEnd	sambaPwdMustChange	密码到期的时间戳
krb5Key	sambaNTPassword	Unicode 格式的密码哈希值

4　系统安全性与可靠性分析

作为企业的集中认证管理平台，首先考虑的就是安全性。HSMD 域中用户的认证请求和响应以及服务请求和响应都使用对称密钥加密，客户端和服务器之间的每次会话使用不同的会话密钥加密数据，大大降低了所传输信息被窃听破译的可能性。本文基于 Samba 在 UNIX 服务器上构建域控制器，为网络资源搭建一个安全稳定的域环境奠定了基础。LDAP 目录存储域中用户、计算机、组和服务账户，是域控制器正常工作的基础和核心。HSMD 域利用 LDAP 目录的存取访问控制机制控制用户对目录对象的访问，减少了账户被非法篡改的可能性。

网络系统可靠性面对的最大威胁就是单点故障，也就是说，一个点不能正常工作带来的是整个系统的崩溃。在 HSMD 域中，域控制器负责域的管理、认证、账户存储工作，是整个域的核心，如果它发生故障，整个域将处于瘫痪状态。HSMD 域对域控制器多机备份来保障异构系统的可靠性。通过在域中设置多个域控制器，用户可以在一个域控制器没有响应时选择其他域控制器重新发送请求，从而避免由于一个域控制器的硬件或软件故障而导致整个域环境的瘫痪。同时，由于多个域控制器分流客户端请求，避免了单个域控制器负载过大，不仅满足大规模目录信息管理和快速对用户请求做出响应的要求，同时保证了 HSMD 域较高的运行可靠性。

总的来说，HSMD 域的设计过程遵照制定的原则，最终达到了预期功能，而且具有易实施、安全和可靠性高等优点。

5　结束语

针对异构环境下账户无法统一管理的问题，本文提出了一个对 Windows 系统和 UNIX 系统统一管理配置的 HSMD 域，该域通过修改对象类定义和设计合理的目录信息树。在 LDAP 目录中集中存储与平台无关的用户账户；解决异构系统中 Kerberos 协议互操作问题的前提下，设计了认证模块和账户存储模块的接口，使 Heimdal Kerberos 能够为域提供安全认证服务；最后分析了其性能特点。

在本文提出的 HSMD 域的基础上，企业可以实现异构系统统一管理平台、面向操作系统账户的单点登录系统等，为跨平台网络的账户数据整合和网络资源管理带来便利。

参考文献

[1] Futagawa J. Integrating Network Services of Windows and UNIX for Single Sign-on[C]//Proc. of International Conference on Cyberworlds. Tokyo, Japan: [s. n.], 2004: 324-328.

[2] 张相峰, 孙玉芳. 安全操作系统中用户账号的管理[J]. 中国科学院研究生院学报, 2004, 21(1): 95-100.

[3] IETF. The Kerberos Network Authentication Service (V5)[S]. RFC1510, 1993.

[4] Westerlund A. Heimdal and Windows 2000 Kerberos——How to Get Them to Play Together[C]//Proc. of USENIX Annual Technical Conference. Boston, USA: [s. n.], 2001: 267-272.

（上接第 158 页）

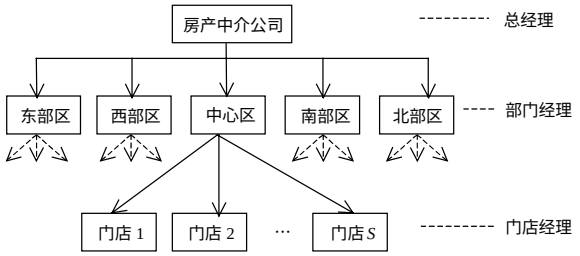

图 3　IBMPOffice 组织

如图 3 所示，该系统在纵向上存在多个管理层次，每个管理层能做各种业务查询工作，但看到的可视数据簇范围不同，这在标准的 RBAC 模型中无法得到控制。利用 ACBR3D 模型，通过分析各个级别各种查询功能的可视数据簇范围、各个可视数据簇之间的互斥、包容以及依赖关系，建立相应的可视数据簇集合，并通过岗位将它与角色进行关联，从而较好地控制各管理层的可视数据簇集合。设总经理的可视数据簇为 ds_{01}，部门经理的可视数据簇为 $ds_{1i}, 1 \le i \le n$，门店经理的可视数据簇为 $ds_{2j}, 1 \le j \le m$，且部门 k 下面有 g 个门店，于是容易得到如下关系：

$(ds_{1i}, ds_{1j}, DE), 1 \le i, j \le n, i \ne j$ ； $(ds_{2i}, ds_{2j}, DE), 1 \le i, j \le m, i \ne j$ ；

$(ds_{01}, ds_{1i}, DC), 1 \le i \le n$ ； $(ds_{01}, ds_{2j}, DC), 1 \le j \le m$ ；

$(ds_{1k}, ds_{2j}, DC), 1 \le k \le n, 1 \le j \le g$ 。

设 ds_1 为物业信息的可视数据簇， ds_2 为住宅信息的可视数据簇，由于查看住宅信息的前提是先能查看到物业信息，因此有 (ds_2, ds_1, DD) 。

6　结束语

本文针对 RBAC 模型描述能力的不足，提出了基于角色的三维空间访问控制模型——ACBR3D，该模型是 RBAC 模型的扩充，比 RBAC 模型更加具有通用性。通过时间维的扩充为授权委托提供了有效的方法；通过可视数据簇维上的扩充，解决了以往扩展的 RBAC 模型难以对访问数据可视范围进行控制的问题，因此该访问控制模型具有更加全面具体的描述能力。但由于可视数据簇的划分和具体系统的业务逻辑有密切关系，因此如何将它们解耦是下一步的研究方向。

参考文献

[1] Barka E, Sandhu R S. A Role-based Delegation Model and Some Extensions[C]//Proc. of National Information Systems Security Conference. New Orleans, USA: [s. n.], 2000.

[2] Bertino E, Bonatti P, Ferrari E. TRBAC: A Temporal Role-based Access Control Model[J]. ACM Transactions on Information and System Security, 2001, 4(3): 58-70.

[3] 黄　健, 卿斯汉. 带时间特性的角色访问控制[J]. 软件学报, 2003, 14(11): 1945-1954.

[4] 张少敏, 王保义. 一种具有时间约束的基于角色的授权管理模型[J]. 武汉大学学报: 理工版, 2006, 52(5): 578-581.

[5] Ahn G J. The RCL2000 Language for Specifying Role-based Authorization Constraints[D]. Fairfax, VA, USA: George Mason University, 1999.

[6] 董光宇, 卿斯汉. 带时间特性的角色授权约束[J]. 软件学报, 2002, 18(8): 1522-1527.