异构操作系统环境的统一用户管理的研究

宋晓婵,刘连忠
(北京航空航天大学 电子政务研究所,北京 100083)

摘 要:随着政府、企业信息化建设的不断发展和基础设施的不断投入与升级,如何提供一种方便可行的方法,使用户能够更加迅速有效地访问和使用有着Windows,Unix,Linux操作系统的混合型网络资源,越来越受到人们的关注。因此,迫切需要实现统一的用户身份管理和认证。以统一身份管理系统的模型为研究对象,阐述了用户管理的基本概念和研究现状,并对现在主流操作系统的用户管理机制进行了分类总结。最后提出了一种基于目录服务的统一异构操作系统用户管理问题的解决方案。

关键词:异构操作系统;Active Directory;可插入认证模块;命名服务转换
中图分类号:TP311 **文献标识码**:A **文章编号**:1673-629X(2008)04-0144-03

Research of Unified User Management under Heterogeneous Operation System

SONG Xiao-chan, LIU Lian-zhong
(Institute of E-Government, Beihang University, Beijing 100083, China)

Abstract: With the development of information management systems in the government and enterprises, it is being paid more and more attention how supply an available and efficient method to help people access mixed-platform environments that include Windows, Unix, Linux, the resources in the Internet. So it becomes more and more important to achieve the goal of unified identity management and authentication. Put focus on the research of unified identity authentication, and did much study from the concept of user management to the status of present research, and also presents a summary of the current main operation system of these techniques. In this paper, propose the solution of the unified heterogeneous operation system user management based on the LDAP.

Key words: heterogeneous operation system; active directory; PAM; NSS

0 引 言

随着网络等基础设施的不断投入与升级,有很多用户在企业中都会遇到不同的网络,包括Windows NT,Windows 2000,Solaris,Linux和大型主机平台。由于历史发展的原因,各平台在用户管理上都有自己的管理工具,管理员要学习不同的方法去管理不同的平台,这样将给管理员带来很大的麻烦[1];另一方面,在这种混合环境中,用户通常需要单独的帐户来访问每个操作系统,由于身份和存取政策的不一致,可能会导致众多密码管理不善,以及多重使用者帐户必须以手动方式更新等问题[2],因此有必要建立一套身份管理系统来集中管理多个平台上的用户帐号。

收稿日期:2007-07-05
基金项目:国家863项目(2005AA113040)
作者简介:宋晓婵(1980-),女,江西景德镇人,硕士研究生,从事信息安全方面的研究;刘连忠,教授,主要从事计算机网络、数据库技术、网络信息安全等方面的研究。

1 用户身份管理研究现状

Windows NT/2000/2003中对用户账户的安全管理使用了SAM的机制,SAM提供的功能类似于Unix和Linux系统中PAM和NSS结合起来所提供的功能。在Windows Server 2003中,用户信息由SAM存储在本地计算机注册表中,域控制器用户信息则存储在Active Directory中。

较早Unix系统和Unix应用程序所使用的信息保存在简单的文本文件中。随着时间的推移,存储系统及应用程序信息的新方法被不断地开发出来并添加到Unix和Linux系统中。

国际上统一用户身份管理比较著名的产品有Vintela身份验证服务(VAS)和Novell Account Management(NAM)。VAS是设计用于将基于Unix和基于Linux的异类环境元素与基于Windows Server 2003的元素集成在一起的一套组件。将Unix和Linux与Windows平台集成在一起可以合并Active Directory中的所有用户和组帐户,并且可以提供用于身份验证、帐

户信息和安全策略的集中管理点。VAS扩展了 Active Directory 所触及的范围,不再受限于 Windows,这样就可以在 Active Directory 中使用 Microsoft 管理控制台(MMC)对所有用户和计算机帐户进行管理,无论操作系统平台是什么。NAM 将多个安全系统中正常储存的用户帐户整合到 eDirectory 中。使得用户能够透过单一的通用目录视图建立用户、更改密码、更改安全要素以及其他信息。

国内开发的能实现集中用户管理和单点登录的软件及相关研究应用大多数都是针对应用系统的统一用户管理和基于某种特定的机制实现身份认证,强调各种应用系统以统一的接口插入统一信息平台,但是并没有涉及到操作系统的集中用户管理和统一认证[3]。

2 Windows 用户管理机制

Windows NT 及 Windows2000/2003 中对用户帐户的安全管理使用了 security account manager (SAM)——安全帐号管理器的机制。Windows2000 是在 Windows NT 4.0 操作系统的域结构基础上改进而成的,并提供了一套为分布式网络环境设计的目录服务(Microsoft Active Directory)[4]。

2.1 Security Account Manager

安全帐号管理器对帐号的管理是通过安全标识进行的,安全标识在帐号创建时就同时创建,一旦帐号被删除,安全标识也同时被删除。安全标识是唯一的,即使是相同的用户名,在每次创建时获得的安全标识都是完全不同的。因此,一旦某个帐号被删除,它的安全标识就不再存在了,即使用相同的用户名重建帐号,也会被赋予不同的安全标识,不会保留原来的权限。

安全账号管理器的具体表现就是%SystemRoot%\\system32\\config\\sam 文件。SAM 文件是 Windows NT 的用户帐户数据库,所有 NT 用户的登录名及口令等相关信息都会保存在这个文件中。SAM 文件可以认为类似于 Unix 系统中的 Passwd 文件,不过没有这么直观明了。

大部分 SAM 操作都结构化为属性的读取和写入。对于工作站帐户,操作将从注册表读取并写入到注册表。域帐户操作是在 Active Directory 对象及其相应的属性上执行的,这些属性以列值的形式存储在目录数据库中。SAM 客户端调用公共 SAM 例程,这些例程再调用封装了 RPC 的内部例程。在服务器端,内部 SAM 例程执行成批的工作。

在 Windows NT 4.0 中,所有对帐户信息的访问都是通过内部 SAM 例程调用存储在注册表的帐户数据库来完成的。在 Windows Server 2003 中,SAM 服务器有效地将域控制器帐户信息从工作站帐户信息中分离出来,并将其放在 Active Directory 中而不是注册表中。SAM 是在动态链接库(DLL) samsrv.dll 中实现的。samsrv.dll 中的逻辑根据计算机的角色以不同方式管理安全主体数据库。在域控制器上,samsrv.dll 使用 Active Directory 进行安全主体存储。在所有其他 Windows Server 2003 计算机上,samsrv.dll 使用注册表中的 SAM 数据库进行存储。

2.2 Microsoft Active Directory

Active Directory 是网络体系结构的一个重要且不可分割的部分。Active Directory 使组织能够高效地共享和管理有关网络资源和用户的信息。此外,Active Directory 还充当保障网络安全的中心,使操作系统准备好验证用户的标识并控制用户对网络资源的访问。Active Directory 基于 Kerberos 5 和 LDAPv3 协议之上,可兼容所有平台上的 Kerberos 5 客户端和 LDAPv3 客户端。这使得 Active Directory 服务器能够在异类网络中提供安全和目录服务[5]。

Active Directory 提供了对基于 Windows 的用户账号、客户、服务器和应用程序进行管理的唯一点。同时,它也帮助组织机构通过使用基于 Windows 的应用程序和与 Windows 相兼容的设备对非 Windows 系统进行集成,从而实现巩固目录服务并简化对整个网络操作系统的管理。管理人员也可以使用 Active Directory 服务安全地将网络系统扩展到 Internet 上。

3 Unix/Linux 用户管理机制

3.1 Unix 和 Linux 的标识管理和目录服务

Unix 和 Linux 标识管理和目录服务已发展了许多年。随着时间的推移,存储系统及应用程序信息的新方法被不断地开发出来并添加到 Unix 和 Linux 系统中。包括:本地文件、DNS、NIS、NIS+、LDAP[4]。

3.1.1 基于本地的文件系统

Unix 和 Linux 操作系统过去使用文本文件来存储配置设置和其他系统信息。许多 Unix 和 Linux 配置文件都存储在 /etc 目录中。在此目录中存储的配置信息的主要例子是用户帐户和组帐户信息。用户配置的详细信息通常存储在两个文件中:/etc/passwd 和 /etc/shadow。

在文件中存储系统配置信息有许多缺点。最突出的缺点是文件通常对于特定计算机来说是本地的。每台计算机的管理都由编辑每台计算机自己的本地文件组成。例如,如果在网络中添加了一个用户,则此用户必须添加到每个他可能需要访问的 Unix 或 Linux 系统上的 passwd 文件中。在拥有上千台 Unix 和 Linux

服务器以及上千个用户的大型组织中,这种管理方法非常麻烦并且非常不实用。由于这个原因,所以发展出了集中管理 Unix 和 Linux 配置信息的方法。

3.1.2 Name Service Switch

为了简化提供 Unix 和 Linux 配置信息的不同方法的使用,人们开发了 Name Service Switch(NSS)——名称服务器交换体系结构。这种模块化的体系结构定义了标准 C 编程函数调用之间的接口,以及一个实现了将 Unix 信息存储在特定文件、数据库系统或目录中的服务模块。名称服务交换可以用于重新定义 Unix 和 Linux 从何处获得各种配置信息。NSS 是通过文件/etc/nsswitch.conf 配置的。

在 Unix 或 Linux 系统上通常可以找到的服务如表1所示。

表1 典型的 NSS 服务

服务名称	描述
compat	与 /etc/passwd、/etc/group 和 /etc/shadow 一起使用以支持旧式加号(+)和减号(-)表示法
db	使用以后缀 .db 作为结尾的本地数据库文件
dns	使用域名系统(DNS)
files	使用本地文本配置文件,通常在 /etc 下
hesiod	使用 hesiod 进行查找
nis	使用网络信息服务(NIS)进行查找
nisplus	使用 NIS+ 进行查找
ldap	用于 LDAP 查找

3.2 Unix 和 Linux 的身份认证和授权服务

Unix 和 Linux 身份验证和授权技术主要有:本地文件、NIS、NIS+、Kerberos。

3.2.1 基于文件的本地系统

过去,Unix 和 Linux 操作系统在文本文件中存储身份验证和授权信息。这些文件以及大量其他系统配置文件均位于 /etc 目录中。用户帐户信息的最终来源是/etc/passwd 文件。为了提高加密的 Unix 或 Linux 密码的安全性,人们开发了影子密码文件(/etc/shadow),只有系统超级用户可以读取 /etc/shadow 文件。

/etc/passwd 和 /etc/shadow 文件为系统提供身份验证信息。使用本地文件在 Unix 和 Linux 系统上的授权是以单个文件级别提供,权限是基于文件、目录和程序而设置的。组信息保存在 /etc/group 文件中,并且在 passwd 文件中通过 GID 字段引用。在 Unix 和 Linux 中,不可能使一个组成为另一个组的成员。

3.2.2 PAM——可插入式身份验证模块

为了使 Unix 和 Linux 系统能够使用其他身份验证方法,人们开发了可插入式身份验证模块(PAM)服务。PAM 为在 Unix 和 Linux 操作系统上配置身份验证系统提供了标准方法。可以使用不同的 PAM 模块提供用于验证用户身份和从标准本地帐户文件获取帐户信息的不同方法[6]。

PAM 中有四个独立的管理组。它们是:

1) 帐户。

该管理组提供检查帐户有效性的服务,例如,通过检查密码是否到期和确认是否允许用户访问此服务。

2) 身份验证。

该管理组使用选定的身份验证机制来验证用户的身份。这种机制可以是简单的质询/应答机制(比如:输入密码);也可以基于身份验证硬件(比如:视网膜扫描或智能卡读卡器)。

3) 密码。

该管理组提供使身份验证机制保持更新的方法。在最简单的情况下,这使用户可能更改其密码。在 Unix 和 Linux 上,更改密码是通过使用 passwd 命令来实施的。

4) 会话。

该管理组提供定义在授权服务之前和撤销服务授权之后需要执行的任务的功能。它可用于审核。

4 统一用户管理的设计方案

本节介绍一个基于目录服务的解决异构操作系统环境的统一用户管理问题的设计方案:

(1)使用基于标准的目录服务(基于 LDAPv3 的)。用户帐户保存在这个符合 LDAPv3 的目录中。

(2)为了实现 Windows NT 帐户与本系统的目录整合,用一个转向器替换 Windows NT 服务帐户管理器(SAM)。该转向器会要求 Windows NT 向本系统的目录服务查询用户信息,而不是 Sam。

(3)由于 Windows 2000 改变了用户管理和认证方式,就不再使用重新定向方法为 Windows 2000 提供帐户管理服务。而是实现 Windows Active Directory 与本系统目录服务间的同步。

(4)系统利用 Unix 和 Linux 提供的名称服务交换(NSS)模块使 UNIX 和 Linux 能够从系统目录中获得用户帐户的详细信息。

(5)系统利用 Unix 和 Linux 提供的可插拔认证模块(PAM)API,允许 Unix 和 Linux 通过系统目录服务进行用户认证。

5 结束语

用户管理是在企业、乃至更大范围内管理用户身份和用户权限的一个过程。它可帮助企业以最低的成本将恰当的资源提供给用户。当企业中网络环境越来

(下转第150页)

为了提高水印的安全性,在水印嵌入前,先对水印进行置乱处理,扰乱水印信息之间的相关性,即使攻击者提取了水印,也会因为其难以辨别而无法判断是否正确地提取了水印。

4 仿真实验

采用 384×384 的 lena 灰度图像,水印是 32×32 的二值图像,仿真软件为 matlab7.0,采用频域水印嵌入法将重要信息嵌入指纹图像中,为衡量算法的质量,引入两个评价指标:PSNR(峰值信噪比)和 NC(水印相似度),定义如下:

$$\mathrm{PSNR}=10*\log\left\{\frac{M*N*\max[C_0(i,j)]^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}[C_W(i,j)-C_0(i,j)]^2}\right\}$$

其中,M、N 代表图像的宽度和高度,$C_0(i,j)$、$C_W(i,j)$ 代表原始图像和嵌入水印图像的像素值。

$$\mathrm{NC}=\frac{M*N-\sum W(i,j)\otimes W'(i,j)}{M*N}$$

其中,M、N 代表图像的宽度和高度,$W(i,j)$、$W'(i,j)$ 表示原始水印和提取出来的水印的像素值。

本算法取嵌入强度 a 值为 0.08,阈值 T 为 0.3,得到嵌入水印图像 PSNR=46.02。在视觉上与原图没有什么区别,水印相似度 NC=0.9941。实验结果表明,利用指纹识别和数字水印进行身份认证,取得了很好的效果。仿真结果如图 3~6 所示。

5 结 论

基于人体生物特征和数字水印技术的网络双重身份认证,是利用生物特征的不变性和数字水印信号的非易失性,综合了数字水印和生物识别二者的优势,有着广阔的发展前景。仿真实验表明,指纹特征和数字水印可以成功地完成身份认证,提高了用户身份验证的效率,具有一定的鲁棒性。

图 3 原始图像

图 4 加入水印后的图像

图 5 原始水印

图 6 提取水印

参考文献:

[1] Schneirer B. The uses and abuses of biometrics[J]. Comm ACM,1999,42(8):136-139.

[2] 张毅刚,焦玉华,牛夏牧,等.基于指纹特征数字水印算法的身份认证技术研究[J].电子学报,2003,31(12A):2131-2134.

[3] 邵利平,覃 征,衡星辰.一种基于图像置乱变换的空域图像水印算法[J].计算机工程,2007,33(2):122-124.

[4] Yeung M, Pankanti S. Verification watermarks on fingerprint recognition and retrieval[C]// Proc. of SPIE Conference on Security and Watermarking of Multimedia Contents. San Jose: SPIE,1999.

[5] 谢 勋.基于数字水印与指纹识别的网络双重身份认证[J].计算机工程与科学,2006,28(6):27-29.

(上接第 146 页)

越复杂、应用系统的数量越来越多的时候,解决应用系统、操作系统、数据库系统等资源的统一用户管理问题就显得特别重要,有效的用户管理不但能够降低诸如密码保密性能不足之类的安全风险,并且最大程度地消除可能影响用户生产力的障碍。

参考文献:

[1] Altmann J, Sampath R. A User-Centric Framework for Network Identity Management[C]// Presented at Network Operations and Management Symposium. Vancouver, BC: [s. n.],2006:495-506.

[2] Gaedke M, Meinecks J, Nussbaumer M. A Modeling Approach to Federated Identity and Access Management[C]// Presented at Poster Proceedings of the 14th International World Wide Web Conference. Japan: [s. n.],2005:1156-1157.

[3] 孙丽萍,王 新,刘志俊,等.异构环境中统一用户管理的研究与规划[J].计算机工程与应用,2005,41(32):225-228.

[4] Microsoft TechNet. 针对 UNIX 的 Microsoft Windows 安全和目录服务解方案指南[EB/OL]. 2005. http://technet.microsoft.com.

[5] 赵保翠,刘 岗.基于 LDAP 的统一用户管理系统的设计和实现[J].微电子学与计算机,2005,22(11):59-62.

[6] Samur W. Unified Login with Pluggable Authentication Modules(PAM)[C]// Presented at the 3rd ACM Conference on Computer and Communication Security. India: [s. n.],1996:1-10.