第38卷第2期 四川大学学报(工程科学版) Vol.38 No.2
2006年3月 JOURNAL OF SICHUAN UNIVERSITY (ENGINEERING SCIENCE EDITION) Mar. 2006

文章编号:1009-3087(2006)02-0132-05

B/S架构的单点登录系统模型

李旭伟,汤丽萍,朱 宏,李香菊
(四川大学 计算机学院,四川 成都 610065)

摘 要:为了满足企业的具体应用集成需求,提出了一种B/S架构的单点登录模型,并讨论了密码同步的解决方案。该模型采用活动目录、ActiveX插件和Kerberos认证,将传统的C/S遗留应用(包括标准Windows应用、FTP和Telnet等)和Web应用集成到B/S模式下,用户通过IE浏览器调用具体的应用,提高了企业应用的可用性和可管理性,增强了用户访问的安全性.

关键词:活动目录;活动目录服务接口;Kerberos;密码同步;单点登录
中图分类号:TP393.09 **文献标识码**:A

A Single Sign On Model Based on B/S Architecture

LI Xu-wei, TANG Li-ping, ZHU Hong, LI Xiang-ju
(School of Computer, Sichuan Univ., Chengdu 610065, China)

Abstract: A Single Sign On (SSO) model based on B/S architecture was proposed for integrating the enterprise's applications, and the solution to keep the passwords synchronized was discussed also. The SSO model integrates the enterprise's legacy applications based on C/S into B/S structure, adopting AD, ActiveX and Kerberos authentication. So the users are able to invoke the C/S applications in the IE as well as the Web applications, and it strengthens the security of user access by Kerberos authentication.

Key words: AD; ADSI; Kerberos; password synchronized; SSO

随着信息技术和网络技术在政府和企业中的广泛应用,各种各样的应用系统得到了大规模的普及。各种应用按照应用特征可以分为以下的几大类:1)传统的Windows应用,例如各种可以单机运行的Windows应用程序、Client/Server模式的数据库应用程序等,这些应用的特性是具有特定的登录界面或窗口,要求用户输入登录参数(用户、口令及参数);2)基于浏览器的Web应用,如电子邮件服务、企业Web应用、OA,这些应用一般通过浏览器访问Web服务器,服务器以页面方式(实际是一个表单)要求用户输入登录参数,用户输入并确认后由Web服务器上的脚本程序进行验证;3)基于命令行方式的各种网络应用,如FTP服务、Telnet应用(如对远程服务器的配置管理、对交换机、路由器等网络设备的配置管理)等,Telnet的使用范围更广,系统和网络管理员频繁使用该程序来管理各种Unix主机和网络设备,管理员需要记忆大量的主机名或IP地址、用户名、口令以及端口等信息。企业用户所使用的应用系统越多,用户需要记忆越多的登录参数(用户名、口令和参数),登录时出错的可能性就会越大,使用不方便,受到非法截获和破坏的可能性也会大大增加,系统的安全性就会相应降低;而如果用户忘记了口令,不能正确的登录系统,就需要请求管理员的帮助,而且只能在重新获得口令之前等待,造成了系统和安全管理资源的不必要的开销。

收稿日期:2005-07-21
作者简介:李旭伟(1963-),男,副教授.研究方向:计算机网络与信息化.

单点登录(Single Sign On,SSO),是企业信息化不断深化以及网络应用不断推广的必然结果。所谓单点登录,简单地说,就是用户通过一次身份验证,可以透明登录所有授权应用。使用单点登录的意义如下:

1)自动完成登录:用户通过一次登录,便可自动访问所有已授权的企业级应用和系统,不需要用户手动输入对应的登录名和密码,提高了用户的工作效率;

2)利用强认证机制对用户进行基本身份验证,提供了单点登录的安全性;

3)提高用户工作效率:用户不至于再陷入多次登录的麻烦,也不用再为访问网络资源要记住多个密码。同时,帮助中心的人员也会从中受益,因为他们不用再去应付那么多因忘记密码而造成的帮助请求了;

4)更有效的管理:用户的帐号数据统一保存、集中管理,减少了出错的机率,同时也减轻了网络管理员维护时的负担。

目前许多大型软件公司都研发了自己的单点登录软件产品,例如 CA 公司的 eTrust SSO、NOVELL 公司的 SecureLogin 等,但这些产品都是基于 C/S 架构的。本单点登录系统模型把传统的 C/S 应用集成到 B/S 模式下,简化了系统维护量;用户登录 SSO 系统采用 Kerberos 认证的方式,提高了系统的安全性;同时部分提供了密码同步机制,主动提供修改密码的入口,系统自动跟踪用户修改密码过程,并维护 SSO 中存储的密码和具体应用系统的密码一致性。

1　模型的技术简介

将简要介绍与单点登录模型有关的技术背景,包括活动目录、ADSI 接口、ActiveX 启动本地应用及 Kerberos 认证等技术。

1.1　活动目录

活动目录[1]是 Windows 2000/2003 Server 整体环境的一部分,是存储用户信息、打印机、服务和定制数据的目录服务。从某种程度上说,活动目录就是存储代表网络用户及资源的基于对象的数据库。每个对象中都存储着与特定用户和网络资源有关的信息。对象可以在目录的树状结构中分层存储。

活动目录具有以下特点:

1)兼容性。活动目录(Active Directory,AD)支持开放标准,轻量目录访问协议(Lightweight Directory Access Protocol,LDAP)是用于访问 AD 中数据的一个标准。而 LDAP 是一个 Internet 标准,可以用于访问不同的目录服务。

2)安全性。活动目录支持多种安全认证协议,包括 Kerberos、SSL、分布式口令验证(Distributed Password Authentication,DPA)、Windows NT NTLM。安全性与活动目录完全集成在一起。不仅可以针对目录中的每个对象定义访问控制,也可以对其每个属性进行操作。可以指定哪些组、用户具有查看或使用对象的权限,可以针对对象进行何种操作。

3)扩展性。活动目录是可扩展的,这意味着管理员可以将对象的新类添加到架构(Schema)中,而且还可以将新属性添加到现有的对象类中。

1.2　ADSI 接口

ADSI[1]是微软推出的基于活动目录但又不与特定目录相关的网络目录接口。就像 ODBC 作为统一的数据库访问接口一样,ADSI 屏蔽了具体目录服务系统的不同,它统一了许多底层服务的编程接口,程序员可以使用一致的对象技术来访问这些底层服务。ADSI 接口包括两个方面,实现 ADSI 目录服务的提供者和使用 ADSI 的客户。每一个当前被支持的目录服务必须有一个 ADSI 提供者,它是一个能访问目录集或某个特定目录的 COM 组件集。安装 ADSI 时,它会附带一些 Microsoft 写的标准提供者,一般包括:1)LDAP 提供者,能访问任何符合 LDAP 标准的目录;2)WinNT 提供者,能访问 NT 4 控制的域中的机器上的信息;3)IIS 提供者,能访问 IIS 元数据库;4)NWCompat 和 NDS 提供者,能访问 Novell 目录。ADSI 客户与普通的 COM 客户程序类似,它调用 ADSI 接口访问目录服务所提供的各种功能,包括查找目录、读取目录对象的属性,如果允许的话,还可以修改对象的属性。

另外 ADSI 还具有以下特点:1)支持多种编程语言,因为 ADSI 基于 COM 机制,所以可以通过任何一种支持 COM 的语言来使用 ADSI,包括 Visual Basic、Java、C、C++ 以及 VBScript 等,另外,一些基于 Perl 和 Python 的实现也能支持访问 ADSI。2)支持双接口,对于支持自动化的客户,它可以通过 ADSI 自动化接口调用目录服务提供者的属性和方法;对于性能要求比较高的客户,它可以通过 COM 接口访问目录服务提供者。

1.3　ActiveX 启动本地 Windows 应用

IE 全面支持 ActiveX。ActiveX 是基于构建对象模型(COM)的,它与具体的编程语言无关。作为针对 Internet 应用开发的技术,ActiveX 被广泛应用与

WEB 服务器以及客户端的各个方面。在客户端或服务器端利用 VBScript、JavaScript 等脚本语言操作 ActiveX 控件,传递数据,协调它们之间的操作。以下代码是用 JavaScript 调用记事本程序:

```
< script language = javascript >
    var wsh = new ActiveXObject("wscript. shell")
    wsh. run("notepad. exe")
< / script >
```

1.4 Kerberos 认证

Kerberos 是为 TCP/ IP 网络设计的可信的第三方鉴别协议。该协议允许用户通过网络向服务器证明其身份,并且也可要求服务器证明身份。Kerberos[2] 的运行环境由以下三大部分组成:1) 密钥分配中心(Key Distribution Center, KDC),它是整个系统的核心部分,其中维护了所有用户的帐户信息,每个 KDC 都提供了两种服务,认证服务(AS) 和会话授权服务(Ticket Granting Service,TGS),AS 的工作是对用户的身份进行初始认证,若认证通过便发放给用户一个称为 TGT(ticket granting ticket) 的票据,凭借该票据用户可访问 TGS,从而获得访问应用服务器时所需的服务票据(ST) ;2) Kerberos 的应用服务器,它的功能在于接受用户服务请求,从票据中提取会话密钥,解开加密信息来验证用户,并提供给合法用户所要求的服务;3) Kerberos 的客户端,它的主要功能是在用户登录时将登录密码转换为该用户的长期密钥,发送各种请求信息,并接收从 KDC 返回的信息。

2 模型的设计

详细介绍了单点登录的模型结构,并对模型的安全性和密码同步问题进行了讨论。

2.1 模型结构

图 1 为三层 B/ S 架构的单点登录模型。该模型主要包括客户端插件(Web SSO Assistant、WinApp SSO Assistant、FTP SSO Assistant 和 Telnet SSO Assistant)、KDC 密钥发布中心、权限分配中心、Web 服务器(Web 服务模块、单点身份验证模块、AD 通讯模块、审计模块,SMS 短消息模块及 Web 开发接口) 和 AD 服务器(用户凭证库、二级登录凭证库)。

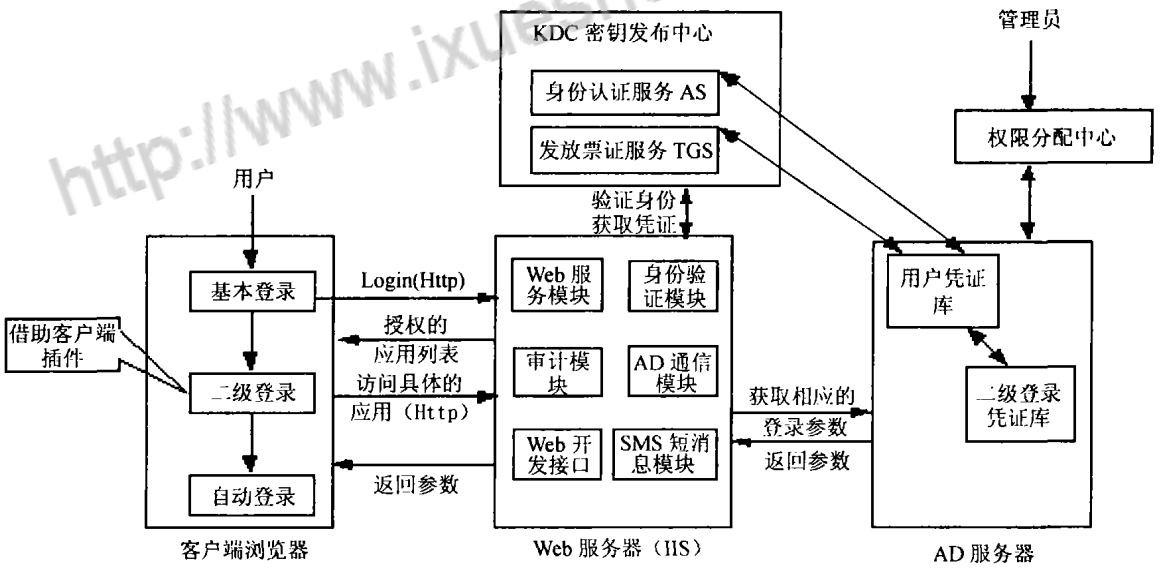

图 1 三层 B/ S 单点登录模型

Fig. 1 SSO model based on three tier B/ S architecture

其各部分的功能简介如下:客户端插件,当授权用户访问被许可的具体资源时,经 Web 服务器的 AD 通信模块,向 LDAP 目录服务器发出查询相应资源的登录名和密码等参数,并将查询结果自动填入登录对话框,完成登录过程。(如果用户是第一次访问授权某一类资源时,则相应的插件自动安装);KDC 密钥发布中心,负责对用户的单点身份进行 Kerberos 验证;权限分配中心,是基于 Windows 图形界面的客户端程序,用来简化单点登录系统管理员对用户、用户组、可访问资源(包括 Web 资源,Windows 应用程序,Ftp,Telnet 等) 等的管理,包括应用特征获取与设置、应用管理、应用许可管理(分配应用管理者、使用权限分配与管理等) 等功能;Web 服务器,是单点登录的核心之一,需要配置一些模块来完成客户与 AD 服务器及 KDC 密钥发布中心之间的数据传输和处理,另外提供审计模块跟踪用户的操作,

如登录和退出系统、应用资源的使用、登录参数的修改等;SMS 短消息模块,需要在 Web 服务器上安装 GSM 或 CDMA 的 modem,为用户提供短消息方式查询用户登录参数提供接口;Web 开发接口,为今后的应用软件或系统的开发提供接口规范,可以方便的将新系统或应用的开发直接集成到 SSO 中,由 SSO 直接进行管理和认证;AD 服务器,用来存储用户凭证库和二级登录凭证库,用户凭证库用来保存用户的数字证书、证书注销列表以及用户的信息等,二级登录凭证库,用来存储用户的权限相关信息,包括用户身份信息、数据资源信息和角色信息,通过角色建立用户和资源间的联系,真正实现了基于角色的权限管理模型,保证了权限分配的简单性和合理性,另外还存储密码修改入口的特征信息,当用户修改具体的用户密码时,SSO 借助密码修改入口的特征信息,主动提供密码修改的入口,并跟踪用户的修改操作,将修改后的密码信息存入二级登录凭证库中,达到密码同步。

客户登录具体应用的流程如下:

1)用户通过浏览器输入登录请求信息,浏览器通过 HTTP 协议向 Web 服务器发出带有该信息的请求,该请求与 Web 服务器的 Web 服务模块交互;

2)经由身份验证模块与 KDC 密钥发布中心交互,用户与身份认证服务器相互认证,获取凭证;

3)身份认证服务器利用该用户证书的主题名在 AD 目录中查找该用户的二级登录凭证库数据,并通过 Web 服务器,向用户返回授权的应用控制列表;

4)用户通过浏览器,向 Web 服务器发出具体的应用请求;

5)Web 服务器,通过 AD 通信模块,与 AD 服务器交互,获取相应的登录参数,然后通过 Web 服务模块,向用户返回相应的登录参数;

6)客户端借助相应的插件,将返回的登录参数自动填入相应的登录框,完整登录过程。

2.2　安全性方面的讨论

由于 ActiveX 本身的不安全性,为了在客户端安全借助 ActiveX 来启动本地应用,对 ActiveX 控件必须采取安全措施,如数字签名、浏览器的安全级别的设定等。数字签名向用户提供一个电子形式的包装,以帮助他们确认软件是否被非发行者以外的人篡改过,这需要微软向软件开发商授权。通过设定浏览器的安全级别让用户知道在什么环境下可以安全地使用此控件,实质是客户端对下载的 AciveX 控件的一种信任机制。

使用数字证书对控件进行签名有以下步骤[3]:

1)向数字证书提供商购买数字证书;

2)下载 Microsoft 公司的数字签名工具包 codesign.exe;

3)利用 codesign.exe 包中的工具进行签名。

数字签名时可以写入公司的基本信息,或者给用户以适当的提示。

2.3　密码同步

密码同步就是保持二级登录凭证库中的密码和对应的应用的密码的一致性。密码同步是单点登录难点,也是关键点。现有的单点登录产品,如 CA 公司的 eTrust SSO、NOVELL 公司的 Securelogin 等,都没有解决密码同步的问题。用户修改了具体应用的密码时,在 SSO 系统的二级登录凭证库中对应的密码信息并没有得到同步更新,当用户随后 SSO 系统访问这一具体应用时,自动登录失败,并提示用户输入新的登录密码,通过用户手动输入的方式达到密码的一致更新。

本模型提出密码同步的解决方案,可以部分解决密码同步的问题,包括标准的 Windows 应用和 Web 应用的密码同步(限制条件:要求用户在 SSO 环境下修改用户密码,SSO 系统中有修改密码这一功能菜单)。在 Web 应用中,修改用户密码的表单中一般包括三个域,旧密码、新密码和确认密码。而对企业来说,所要访问的 Web 应用一般都是明确的,可以把每个授权用户修改 Web 应用的特征信息,如 url,用户名等保存在二级登录凭证库中。当用户修改某一 Web 密码时,就根据二级登录凭证库中修改 Web 应用的特征信息,主动进入修改密码的入口(change password 页面,如 http://reg.163.com/ChangePasswd.jsp?username=**),并跟踪用户的操作过程,如果修改用户密码成功,就提取新的用户密码,更新二级登录凭证库中对应的密码信息。对应标准的 Windows 应用,采用相同的方法,只是提取的 Windows 应用的特征信息有所不同。

3　模型实现

模型的具体实现是以中石油吐哈油田分公司的单点登录需求为背景,将传统的需要独立的用户认证策略的应用(如标准 Windows 应用、Web 应用及基于命令行方式的 FTP 服务、Telnet 应用等)集成到基于 B/S 架构模式的单点登录系统中,实现了“一次登录,多次访问”。模型采用 Visual Studio.Net 集成环境中的 C# 语言开发,目录服务器采用微软的活

动目录(AD)。为了实现 B/S 架构的单点登录模型,编写了一个 ActiveX 控件(SSo.dll),实现登录参数的自动填写、自动提交和自动完成登录的过程。该控件主要包括 4 个主要的函数:public void LoginWindow()、public void LoginWeb()、public void LoginFtp()和 public void LoginTelnet(),分别实现 Windows 应用、Web 应用、FTP 和 Telnet 等应用的自动登录功能。

以自动登录 Windows 应用程序片断为例,简要说明用 ActiveX 控件协助完成自动登录的大致过程:

```
public void LoginWindow(string exec Path,
string win Class Name,string win Text,
string input Name Order,string input Pwd Order,
string btn Order,string win User Name,
string win Pwd)
  {
    .../ /启动应用程序
    Process Win = new Process();
    Win.StartInfo.FileName = exec Path;
    Win.StartInfo.UseShellExecute = false;
    / /查找主窗口
    parent Hwnd = FindWindow(win Class Name,
    win Text);
        …
    / /找到主窗口,并处理
    EnumChildWindowsProc child Windows Proc =
    new EnumChildWindowsProc(EumWinChiPro);
      try
      {
        / /遍历主窗口
        EnumChildWindows(parent Hwnd,
        child Windows Proc,null);
      }
      catch
      {
        hwnd List.Clear();
        return;
      }
    ?/自动填入用户名,自动填入密码,自动登录
    SendMessage(hwnd Name,WM SETTEXT,0,
      win User Name);
/ /函数中调用的 WinAPI
    [DllImport("User32.dll",CharSet = CharSet.Auto,
    EntryPoint = "FindWindow")]
    public static extern IntPtr FindWindow(
    string lpClassName,string lpWindowName);
    [DllImport("User32.dll",CharSet = CharSet.Auto,
    EntryPoint = "SendMessage")]
    public static extern int SendMessage(IntPtr hWnd,
      int Msg,int wParam,string Lparam);
    [DllImport("User32.dll",CharSet =
    CharSet.Auto)]
    public static extern bool EnumChildWindows(
    IntPtr hWndParent,EnumChildWindowsProc
    lpEnumFunc,string lPam)
```

4 结束语

与现有的单点登录系统相比,该模型主要有以下优点:1)通过 ActiveX 启动本地应用的方式,将 C/S 应用集成到 B/S 模式下,客户端只需要自动安装少量的 AcitveX 插件,简化了系统的维护更新工作;2)采用 Kerberos 认证机制,增强的单点的安全性;3)部分解决了密码同步问题。另外对于 FTP、Telnet 应用中如何进行密码同步是一个值得进一步研究解决的问题。

参考文献:

[1]Robert R King. Windows Server 2003 活动目录从入门到精通[M]. 薛菲,王曼珠,译. 北京:电子工业出版社.

[2]Bruce Schneier. 应用密码学——协议、算法与 C 源程序[M]. 吴世忠,祝世雄,张文政,译. 北京:机械工业出版社,2000.

[3]Li Xin, Liu Lianchen, Wu Cheng. ActiveX based remote software deployment[J]. Computer Applications, 2002,22(12):44-47. [李昕,刘连臣,吴澄. 基于 ActiveX 技术的软件远程发布[J]. 计算机应用,2002,22(12):44-47.]

(编辑 杨 蓓)

阅读此文的还阅读了：

26. 基于Documentum系统的单点登录的实现

27. 单点登录系统方案研究

28. 基于PKI/PMI的单点登录系统

29. 基于校园网的单点登录认证系统研究

30. 基于Web服务的单点登录系统

31. 构筑LDAP+Samba域单点登录系统:单点登录实现集中管理

32. 单点登录原理及实现

33. 建立企业单点登录系统

34. 单点登录系统建设方案

35. 单点登录系统在特检行业中的设计与实现

36. 构建稳固的单点登录系统

37. 单点登录浅析

38. 电子政务中单点登录应用模型研究

39. 基于混沌一次一密认证的单点登录系统的研究

40. 单点登录系统(SSO)技术实现剖析

41. 云计算环境下单点登录模型研究

42. 单点登录技术专利分析

43. 基于OAuth2.0的单点登录系统

44. 与应用无关的单点登录系统

45. 单点登录系统方案研究

46. 基于CAS的单点登录系统的实现

47. 改进模型的单点登录系统的设计

48. 基于PKI的多域单点政务网登录模型

49. 浅析单点登录系统设计与实现

50. 基于SSO实现承钢多系统单点登录