文章编号:1001 - 9081(2006)05 - 1146 - 02

支持单点登录的统一资源管理体系研究

董亮卫,汪文勇,黄鹂声
(电子科技大学 计算机科学与工程学院,四川 成都 610054)
(lsh@uestc.edu.cn)

摘 要:对几种单点登录模型进行了分析与比较,提出了一种基于经纪人和代理模型的 Kerberos 单点登录与统一资源管理框架,以简化网络登录和资源访问过程中的用户身份认证和管理环节。介绍了该系统的体系结构以及系统中关键部分的工作原理。

关键词:单点登录;Kerberos;密钥分发中心
中图分类号: TP393 **文献标识码**:A

Study on unified resource management architecture supporting SSO

DONG Liang-wei, WANG Wen-yong, HUANG Li-sheng
(*College of Computer Science and Engineering, University of Electronic Science & Technology of China, Chengdu Sichuan* 610054, *China*)

Abstract: Several single sign-on models were analyzed and compared. A broker and agent-based Kerberos single sign-on and unified resource management frame was proposed, which helps to simplify the user authentication and management process of network sign on and resource access. The structure and its implementation of the frame were also introduced.

Key words: SSO(Single Sign-On); Kerberos; KDC(Key Distribution Center)

0 引言

传统的认证机制是基于用户名和密码的,每一个系统都建立有自己的用户信息数据库,用以验证用户的身份。

从技术上分析,传统的认证机制有着严重的安全问题。首先,用户名和密码信息会在网络上传送,且常常为明文传送,这就很容易被攻击者截取到,假扮合法用户来攻击系统。另外,在一般的系统中,用户为了方便记忆往往会选用一些较为简便的密码形式,这很容易遭受到密码猜测的攻击,尤其是基于字典方式的攻击往往非常有效。

对网络管理员来说,这样的系统会使他们的工作量大大增加。因为每个系统都保存有自己的用户信息数据库,在复杂的管理过程中存在安全隐患,容易引起信息泄密、数据篡改、数据欺骗等安全问题,造成严重后果。

本文针对上述问题,提出了基于单点登录(Single Sign-On,SSO)的统一资源管理体系,以实现一种支持跨系统单点登录的统一资源管理体系。

1 系统目标

系统设计的目标是:采用统一认证架构和管理方式,使用户只通过一次身份认证,就能够进入不同的应用系统,对不同的资源进行统一访问。系统总体目标如图 1 所示。

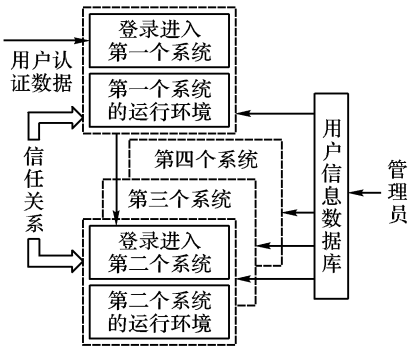

图 1 单点登录系统的目标

为了使系统更具有实用性,选择了两种操作系统(Windows2000 和 Linux)、一种数据库(Oracle 8)作为目标对象,完成单点登录和统一资源管理平台的开发和试验。

2 单点登录模型的比较与选择

实现单点登录系统有不同的模型,包括:

(1) 基于网关的模型

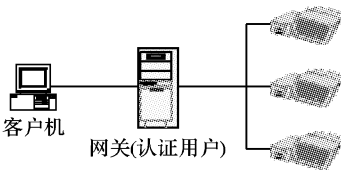

图 2 基于网关的模型

如图 2 所示,在基于网关的模型中,网关是通往所有服务资源必须经过的一道“门”,这些服务资源处在可被信赖的网络中。网关可以是一台防火墙,也可能是一个精心设计的加/解密服务器。所有的客户机都与网关相连接,网关再与各种应用服务器进行连接,网关把外界客户机与内部的服务资源隔离开来。该模型的优点是简单,缺点是安全强度低。因此,该模型一般应用于互联网上的普通应用服务,而很少用于企业或机构等对安全性要求高的环境。

(2) 基于经纪人的模型

如图 3 示,该模型由三个部分组成:支持认证服务的客户端,认证服务器和支持认证服务的应用服务器。其中认证服务器扮演经纪人的角色,因为所有的认证都是通过它来完成的。其工作流程是:所有的客户机在访问系统资源之前首先向认证服务器进行身份验证(当然,为提高

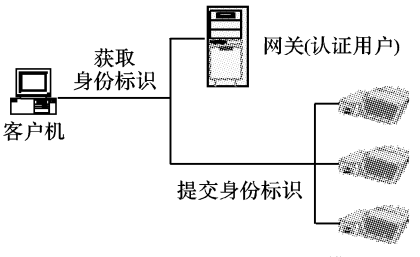

图 3 基于经纪人的模型

收稿日期:2005 - 10 - 19;**修订日期**:2006 - 02 - 27

作者简介:董亮卫(1979 -),男,河北人,硕士研究生,主要研究方向:计算机软件; 汪文勇(1967 -),男,四川简阳人,副教授,博士,主要研究方向:计算机网络与软件; 黄鹂声(1975 -),男,重庆人,讲师,硕士,主要研究方向:计算机网络与软件.

系统的安全性可以采用相互认证方式);当用户通过身份验证后,认证服务器返回给用户一个电子身份标识,用户通过该电子身份标识去访问其他的应用服务器,从而实现单点登录。如果电子身份非法或者过期,则应用服务器会拒绝提供服务。

该模型的最大优点是数据的集中管理,缺点是实施难度大。

(3) 基于代理的模型

如图 4 所示,在基于代理的解决方案中,有一个自动地为不同的应用程序进行用户身份认证的代理程序,这个代理程序可以用不同的方式来工作。比如,它可以使用口令或加密密钥来自动进行认证工作,从而将认证的负担从用户移开。代理也能被放在服务器上面,在服务器的认证系统和客户端认证方法之间充当"翻译"。

该模型的优点是可移植性好、使用方便,缺点是管理难度大,尤其是用户数据库依然是分散管理。

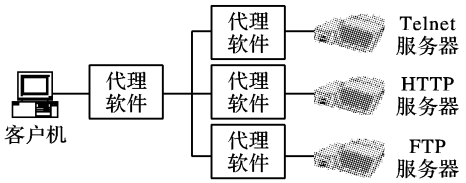

图 4　基于代理的模型

经过以上比较,我们结合采用基于经纪人的模型和基于代理的模型来实现系统,以吸纳两种模型的优点:经纪人模型可以方便地进行用户的集中管理,使系统具有较大的可扩展性和安全性;代理模型易于部署和移植,而且一旦部署完成,对用户完全透明。

实现支持单点登录的统一资源管理系统,其最大的工作量在于要对原有的系统(如操作系统和数据库系统)加以改动或增加外壳,使它们能支持新的认证方式和认证协议。

因此,该体系一个重要的工作就是开发客户端及应用服务器端为实现单点登录所需的各程应用程序包,以提供给它们一个统一的调用接口,方便地实现单点登录。由于篇幅所限,本文对这一部分工作不做赘述。

3　构架设计

整个系统由 KDC 服务器、Console 和 Agent 三个部分组成,体系结构如图 5 所示。

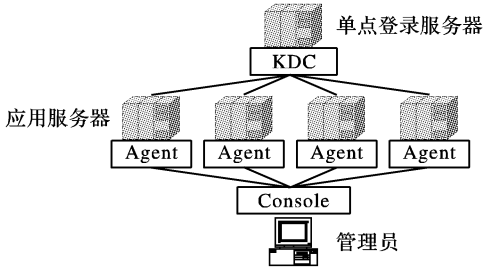

图 5　支持 SSO 的资源管理体系框架

各个部分功能分配如下:

KDC 服务器运行于 Linux 操作系统,作为一个 Kerberos 服务器和安全数据管理中心,由一个服务软件和多个工具软件组成,具有安全数据库管理和维护、票据发放、用户和服务认证三个基本功能。也就是说,它由 Authentication Service (AS,认证服务)、Ticket Granting Service (TGS,票据发放服务)、安全数据库服务三部分组成。它能够对本地磁盘上的安全数据库进行管理和维护,如用户管理、服务器管理和密码管理;能够对数据库服务器端的 Agent 进行合法性验证,也能够对 Console 操作用户进行单次登录验证;能够根据用户的访问请求,向用户发放各种服务器和 Agent 的访问票据。

Agent 工具运行于 Linux 和 Windows 操作系统,作为一个守护服务进程,具有四个基本的功能:向 KDC 服务器验证自身的合法性;验证 Console 提交的访问票据的合法性;接受并响应 Console 端的命令和请求;对被管对象(宿主数据库系统)进行管理操作。

Console 工具运行于 Windows 操作系统,由一个管理控制台软件和若干工具模块组成,具有五个基本功能:向 KDC 服务器登录;向 KDC 服务器注销;从 KDC 服务器获取票据;将票据提交给 Agent 并接受其验证;向 Agent 发出数据库管理命令并接收其反馈结果。

4　KDC 服务器

系统的体系结构如图 6 所示。

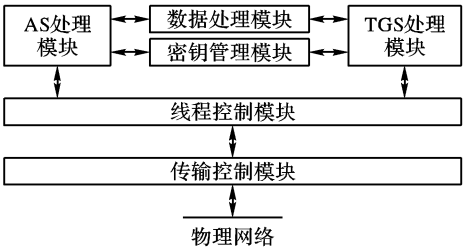

图 6　KDC 服务器结构

认证服务器主要分为以下多个模块:

(1) 传输控制模块

传输控制模块分为两大功能部分。接收部分用来接收传递给服务器的各种数据,并且要判断数据传送是否结束,以便启动相应的线程来处理接收到的数据;发送部分则是将处理后的数据,根据用户的地址信息,传递到对应的用户去。在传输控制部分也会有超时控制等机制,以确保系统的正常运行和及时处理各种异常情况。

传输控制模块中另一个重要功能就是根据用户的连接请求启动线程来进行处理,提高系统的响应速度。

(2) 线程控制模块

线程控制模块是整个系统设计的关键环节,对系统的工作性能起着至关重要的作用。我们设计有一个线程控制列表,对所有的线程进行统一的管理,负责线程的启动、停止、增加及删除操作。

每一个用户的新建连接都会产生一个新的线程来进行处理,以提供给用户一个较为快速的任务响应。通过线程控制模块,可以动态调整系统最多允许同时运行的线程数和对线程进行适当的调度,以适应各种不同的实际需求。

(3) 数据处理模块

对各种数据信息进行解包或封装操作,包括有加密/解密函数,针对于票据、authenticator 等数据结构的解析与封装函数等。

(4) 密钥管理模块

负责随机生成会话密钥与将用户输入的用户名及密码转换成用户的长期密钥。

(5) TGS 处理模块

对用户申请具体的应用服务票据的请求进行处理。如果通过了用户的身份认证,并且用户所提交的请求也是合法的,便会返回给用户相应的票据和会话密钥。

(6) AS 处理模块

接收并处理用户的登录和注销请求,检查用户提供的登录名称和密码是否合法,验证用户身份及权限,完成单点登录过程,并记录用户的登录和注销状态。 (下转第 1189 页)

```
ADDRESS64 highInstr = ((ADDRESS64) endhigh) < <32; \
instr = highInstr + (ADDRESS64) lowAddrInstr;
```

附录 2　switch_sparse. c 的源程序

```
#include <stdio. h >
int main( )
{ int n;
  printf( "Input a number, please: ");
  scanf( "%d", &n);
  switch( n) {
    case 2: printf( "2! \n"); break;
    case 20: printf( "20! \n"); break;
    case 200: printf( "200! \n"); break;
    case 2000: printf( "2000! \n"); break;
    case 20000: printf( "20000! \n"); break;
    case 200000: printf( "200000! \n"); break;
    case 2000000: printf( "2000000! \n"); break;
    case 20000000: printf( "20000000! \n"); break;
    case 200000000: printf( "200000000! \n"); break;
    case 2000000000: printf( "2000000000! \n"); break;
    default: printf( "Other! \n");
    }
  return 0;
}
```


参考文献:

[1] 文延华, 漆锋滨, 黄传信. 二进制翻译技术初探[J]. 高性能计算技术, 2003, (1): 49 - 52.

[2] CIFUENTES C, VAN EMMERIK M, RAMSEY N, *et al.* The University of Queensland Binary Translator(UQBT) Framework[EB/OL]. http: //www. itee. uq. edu. au/ ~ cristina/, 2001.

[3] Intel IA-64 Architecture Software Developer's Manual — Overview of Volume 3: Instruction Set Reference[EB/OL]. ftp: //download. intel. com/design/Itanium/manuals/245319. pdf/, 2000.

[4] GEVA R, MORRIS D. IA-64 Architecture Disclosures White Paper [EB/OL]. http: //www. cs. nmsu. edu/rvinyard/itanium/docs/IA-64_arch_wp. pdf.

(上接第 1147 页)

5　Agent 代理模块

按照系统各个功能模块的划分,Agent 部分的体系结构如图 7 所示。

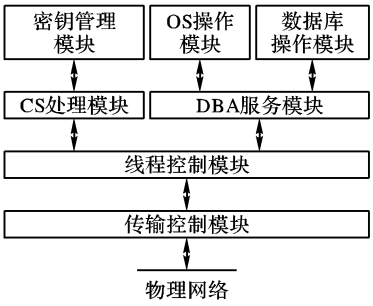

图 7　Agent 体系结构

Agent 部分包括了传输控制模块、线程控制模块、CS 处理模块、密钥管理模块、DBA 服务模块、数据库操作模块、OS 操作模块等。

其中,数据库操作模块和 OS 操作模块分别作为数据库系统、操作系统的代理外壳,接收并分析 Console 发来的管理和监控请求,通过查找知识库,转换为实际的操作语义,调用相关数据库和操作系统控制函数,并根据返回结果,再次查找知识库,形成执行结果,反馈给 Console 用户。

6　Console 管理平台

系统的体系结构如图 8 所示。

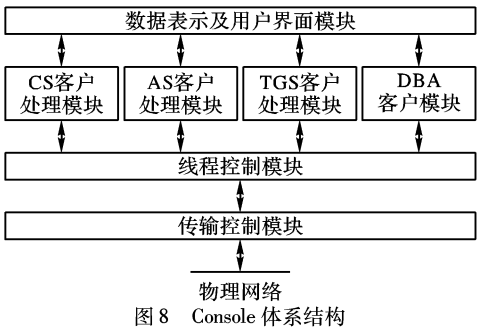

图 8　Console 体系结构

Console 部分是提供给用户的使用程序,用户可以通过 Console 进行单点登录,进入不同的操作系统和数据库系统,进行配置和管理。Console 部分包括传输控制模块、线程控制模块、AS 客户处理模块、TGS 客户处理模块、CS 客户处理模块、DBA 客户处理模块、数据表示模块等。

其中密钥管理模块用于检查并使用存储在本地的单点登录会话密钥,同时验证 Agent 会话密钥的正确性。

AS 客户模块负责向认证服务器发送用户名和密码,完成单点登录。TGS 客户模块向认证服务器申请具体的 Agent 应用服务票据,检查并保存返回的相应的资源访问票据和会话密钥。

数据表示模块与 DBA 客户处理模块协同工作,接收并分析用户输入的访问和管理请求,发送给合适的 Agent,并根据返回结果,生成图形、文字等界面信息,展现给操作用户。

7　结语

本文讨论的设计方案,可以用于局部范围内的单点登录和操作系统、数据库资源管理,但适用的范围基本上局限于一个企业网或校园网,还不能扩展到更大范围的网络环境。上述模型和实现是基于单台认证服务器的系统,如果是有多台认证服务器,如何使它们之间可以建立信任关系,使之由一个认证服务器所管理的客户可以访问在另一个认证服务器管理域中的资源,还有待进一步研究。

参考文献:

[1] KOHL J, NEUMAN C. The Kerberos Network Authentication Service (V5), RFC1510[S], 1993.

[2] LINN J. Generic Security Service Application Program Interface, RFC 1508[S], 1993.

[3] WRAY J. Generic Security Service API: C-bindings, RFC1509[S], 1993.

[4] HALLER N, ATKINSON R. On Internet Authentication, RFC1704 [S], 1994.

[5] LINN J. The Kerberos Version 5 GSS-API Mechanism, RFC1964 [S], 1996.

[6] MENEZES A, VANOORSCHOT P, VANSTONE S. Handbook of Applied Cryptography[M]. CRC Press, 1996.

[7] KRAWCZYK, BELLARE, CANETTI. HMAC: Keyed-Hashing for Message Authentication, RFC 2104[S], 1997.

[8] TRICKEY F. Single Sign-On: Fantasy or Reality?[M]. CSI Advisory Council, 1997.

[9] HURSTI J. Single Sign-On[D]. Department of Computer Science, Helsinki University of Technology, 1997.

[10] Microsoft Corporation. Single Sign-On in Windows 2000 Networks [Z], 1998.

[11] CAMILLO. Unified Single Sign-On[D]. Department of Computer Science, Helsinki University of Technology, 1998.

[12] LINN J. Generic Security Service Application Program Interface Version 2, Update 1, RFC2743[S], 2000.