校园网络单点登录系统应用研究①

Research and Application of Single Sign on System in Campus Network

曹世华 赵 方 (杭州师范大学网络中心 杭州 310012, 北京邮电大学软件学院 北京 100876)

摘 要: 提出了一种基于 Active Directory 和 kerberos 协议的单点登录系统。校园网络规模不断扩大,各种基于校园网络的应用系统也越来越多,而每个应用系统都有自己独立的用户验证系统,这给校园网络统一管理和用户使用带来不便,也就提出了用户对校园网络统一身份认证的要求。在研究了校园网络单点登录和用户统一管理的需求,设计了一个安全、可靠、高效的适用于校园网络内的的安全认证架构,进行用户的统一授权管理。

关键词: 单点登录 统一认证 Kerberos Active Directory 校园网

随着信息技术和网络技术的快速发展,各种基于校园网络的应用系统不断涌现,这给高校的信息化建设提供了很大的帮助和服务。而校园网络和应用系统往往是由不同时期、不同人员建设开发的,相对来说缺乏整体的规划,出现了分离的、独立的、异构的应用系统等。用户在访问系统之前,首先要经过身份认证系统认证,然后访问控制系统分配给用户访问系统和资源的权限和级别。然而每个应用系统都有独立的用户认证数据库,要求用户进行相应的安全认证,并且不同的系统要求用户提供不同的用户信息进行身份认证。

为此相关国内外文献提出了单点登录技术[1-3],该技术是为解决这些问题而提出的。笔者根据校园网络安全和用户需求,分析并提出了一种单点登录的统一身份认证系统。

1 单点登录的提出

高校在其信息化建设过程中,建立起一系列的基于校园网络的信息系统如办公自动化、FTP 系统、教务管理、图书资料借阅管理、电子邮件系统、一卡通系统等应用,其中每个系统都需要用户进行身份的认证并且对不同身份分配不同的权限。按照传统的开发模式,每个应用系统都必须开发各自独立的用户认证模块,用户也不得不记忆不同应用系统的账号和口令,这种认证方式存在很多的缺点:消耗开发成本和延缓应用开发进度;用户需记忆多个账户和口令;无法统一认证和授权;无法统一分析用户的应用行为等。例如,用户 A 需要同时使用 X 系统与 Y 系统,就必须在 X 系统与 Y 系统中都创建用户 A ,这样在 X 、Y 任一系统中用户 A 的信息更改后必须同步至另一系统。如果用户 A 需要同时使用 10 个应用系统,用户信息在任何一个系统中做出更改后就必须同步至其他 9 个系统。用户同步时如果系统出现意外,还要保证数据的完整性,因而同步用户的程序可能会非常复杂。

单点登录技术的应用使得以上问题得到根本的解决。单点登录(SSO,Single sign on),是一种统一身份认证和授权机制,单点登录是指用户只需要在网络认证系统中登录一次,即通过一次用户安全验证后,再访问其他应用中的受保护资源时,不再需要重新登录验证,而这些网络资源包括分布在整个校园网络中不同应用系统的的一切数据资源。使用单点登录的优势在于:

(1) 简化使用流程

用户使用应用系统时,能够一次登录,多次使用。用户不再需要每次输入用户名称和用户密码,也不需要牢记多套用户名称和用户密码。单点登录平台使得

① 基金项目:国家 973 基金项目(2003CB314806);863 基金项目(NO. 2006AA10Z253)

用户使用系统变得简单、易用，从而提高工作效率。

(2)便于统一管理

系统管理员只需要维护一套统一的用户账号，方便、简单、更安全。相比之下，系统管理员以前需要管理很多套的用户账号。每一个应用系统就有一套用户账号，不仅给管理上带来不方便，而且，也容易出现管理漏洞。

(3)简化应用系统开发

所有的应用程序无论新旧，可以不需要或只需要很少的改动就可以适应新的认证方式，迁移至单点登录平台的用户认证服务，简化开发流程。单点登录平台通过提供统一的认证平台，实现单点登录。

2 单点登录认证系统设计与实现

基于校园网络统一身份认证的需求，要求用户能在整个网络中单点登录，首先要求用户操作方便，并且要求认证速度快，能够在很多人同时登录时，保证服务器的稳定和安全。根据以上分析和校园网的需求，可以采取服务器端保存客户信息的方法，这样可以减少或避免用户密码在网络中的传输，以保证用户系统安全。

本文提出的一种单点登录系统中采用了 Windows 登录、活动目录(Active Directory)和 Kerberos 认证机制。如图1所示，

单点登录的系统结构主要分为：用户端、认证中心、用户信息数据库(活动目录)、应用系统。

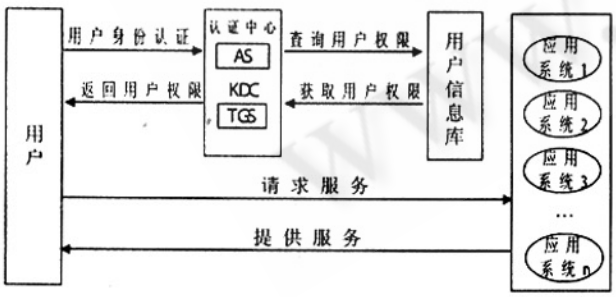

图1 单点登录认证结构

用户信息采用加密后集中存放在用户信息库中，我们这里采用的是 Windows2003 的活动目录(Active Directory)，活动目录是 Windows2000 及以上网络操作系统提供目录服务，是 Windows 2003 网络体系的基本结构模型，也是 Windows 2003 网络操作系统的核心支柱，是一个全面的目录服务管理方案，也是一个企业级的目录服务，具有很好的可伸缩性和安全性。活动目录采用了 Internet 的标准协议，它与操作系统紧密地集成在一起。活动目录不仅可以管理基本的网络资源，比如计算机、用户账户、打印机等，它也充分考虑了现代应用的业务需求，为这些应用提供了基本的管理对象模型，比如用户账户对象具有办公电话、手机、住址、部门、电子邮件等属性。几乎所有的应用都可以直接利用系统提供的目录服务结构，而且活动目录也具有很好的扩充能力，允许应用程序定制目录中对象的属性或者添加新的对象类型。它主要具有如下的特点：

a) 信息以安全形式保存，每个活动目录中的对象有一个访问控制表(ACL)，在其中有资源的列表和访问权限。

b) 由活动产生的全局类目使查询更加灵活。任何支持活动目录的客户都可以查询这个类目。

c) 将目录复制到所有域控制器，意味着对域名的访问更容易，而且可靠性更好。

d) 由对象组成的层次结构，其中任何一个对象(根目录除外)又被另外的对象包含。

e) 因为它的基础是 X.500，所以它可以在不同的协议基础上进行通信，通信协议包括简便的目录访问协议3(LDA P3)，用于名字定位的 HTTP DNS。

f) 通过域名和目录分类信息。

g) 活动目录上的信息不仅能够在同域中查询，还能够在其他相互信任的域或更大的范围内进行查询。

认证中心采用 Kerberos 认证机制，Kerberos 是由美国麻省理工学院(MIT)提出的基于可信赖的第三方的认证过程。Kerberos 提供了一种在开放式网络环境下进行身份认证的方法，它使网络上的用户可以相互证明自己的身份。Kerberos 采用对称密钥体制对信息进行加密，其基本思想是：能正确对信息进行解密的用户就是合法用户。当用户进行登录，Kerberos 对用户进行初始认证，通过认证的用户可以在整个登录期间得到相应的服务。Kerberos 既不依赖用户登录的终端，也不依赖用户所请求的服务的安全机制，它本身提

供了认证服务器来完成用户的认证工作。

Kerberos 机制最大的特点是采用相互认证机制，即客户端不仅要证明自己是合法用户，服务器也要向客户端证明自己是值得信赖的合法服务提供者，还有每次的会话密钥都不相同，大大提高了系统的安全性。

该认证方式原理如图 2 所示。Client：客户端，用户，用 c 表示。Server：服务器端，用 s 表示。KDC：密钥分配中心，包括 AS 和 TGS。AS：认证服务器。TGS：票据服务器。

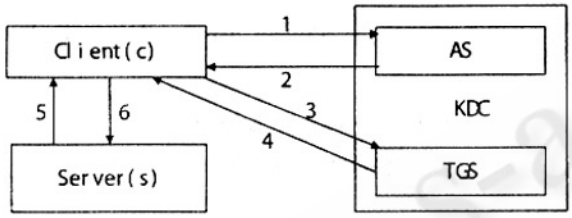

图 2 Kerberos 认证原理

(1) 用户想要获取访问某一应用服务器的许可证时，先以明文方式向认证服务器 AS 发出请求，从客户端发送用户名 c 和服务器名 TGS，表示要使用该用户名获得访问该 TGS 的许可证

c - >AS:c,TGS

(2) AS 在本地库内查找该用户名和密钥，AS 根据该用户名，在目录数据库中取得该用户的密钥 Kc(一般为用户密码的单向 hash 函数)和 TGS 的密钥 Ktgs，AS 产生一个会话密钥 Kc,tgs，并生成 TGS 的许可证 Tc,tgs，最后，AS 发出响应消息：一部分是用 Kc 加密的会话密钥 Kc,tgs，另一部分是 TGS 的许可证 Tc,gs，并且向 TGS 发出响应，此过程服务器用于认证用户的身份：

AS - >c:{Kc,tgs, Tc,tgs}Kc; AS - >TGS:{Kc,tgs, Tc,tgs}Kc;

(3) 用户在本地输入的密码生成 Kc，从获得 AS 返回消息解密得到 Kc,tgs，并且拥有 Tc,tgs，用户如果需要访问某个应用服务器的许可证，需要向 TGS 提交 Tc,tgs 和新产生的鉴别码 Ac,tgs。

c - >TGS: Tc,tgs, Ac,tgs

(4) TGS 用 Kc,tgs 解密 Tc,tgs ，并用 Kc,tgs 解密 Ac,tgs，通过比较时间戳的有效性来确定用户的请求是否合法，如果合法，TGS 生成用户要求的应用服务器 Server 的使用许可证 Tc,tgs，同时，发出响应消息：一部分是用 Kc,tgs 加密的 Kc,s，另一部分是服务器的许可证 Tc,s，并且在本地生成访问控制列表。

TGS: - >C: {Tc,s}Kc,{Kc,s}Kc,tgs

(5) 用户用自己持有的 Kc,tgs 解密收到的信息，得到 Kc,s，用 Kc 解密得到 Tc,s，当请求应用服务器时，提交 Tc,s 及鉴别码 Ac,s.

c - >s: {Tc,s},Ac,s.

(6) 应用服务器用自己持有的 Kc 解密用户发来的 Tc,s，得到 Kc,s，用 Kc,s 加密 time stamp(时间戳)+1 发给用户，用户通过比较时间戳的有效性来实现对 Server 的认证。

经过以上步骤，双方完成了相互的身份认证，并且拥有了会话密钥。其后进行的数据传输将以次会话密钥进行加密。Kerberos 将认证从不安全的客户端移到了集中的认证服务器上，为开放网络中的两个主体提供了身份认证，并通过会话密钥对通信加密。对于复杂的网络系统采用统一的身份认证管理。

在单点登录系统中，用户是一个客户端，开始登录应用系统时，如果没有访问票据，就转到 AS(认证服务器)处认证，在 AS 后端采用活动目录存储用户认证信息，返回给用户会话密钥，然后用户持会话密钥到 TGS(票据服务器)取得访问服务器的票据，然后再去访问应用系统。用户持有票据以后，再访问别的应用服务器，只需要提供访问票据即可，在票据中含有用户的登录信息，在后端的活动目录中，用户的信息被统一管理，用户身份统一认证、统一授权。在认证过程中，因为传输的不是口令，而是票据，票据传输带有个人的鉴别码，攻击者几乎不可能对用户行为进行模仿，因而有效地防范了网络窃听攻击，由于数据包中包含了时间戳和加密过的密钥，可以避免重复攻击。

这里需要指出的事，单点登录系统的用户验证方式可以是多样的，包括静态口令和智能卡或 USB_Key、指纹识别、动态口令令牌、数字证书等。管理员可以配置不同的应用需要使用不同的认证级别，在方便用户使用的同时考虑安全性和管理费用。比较优秀的单点登录不是将复杂的多次登录过程映射整合在一台认证服务器上的单一账号上，而是通过配置用户访问不同

应用的策略实现安全性。管理员为个人和用户组规定允许对网络资源进行恰当的访问的策略。如果单点登录用户当前的已登录级别低于要访问的应用系统所需要的认证级别时，单点登录系统会要求用户进行更高级别的认证。

3 结论

在校园网内，通过 Kerberos 结合 Active Directory（活动目录）实现单点登录认证系统，解决了用户单点登录的统一认证授权管理问题，使用户使用网络更方便。同时由于 Kerberos 本身就是一种比较安全的认证方式，解决了传统认证方式单方面认证的缺点，使用户和服务器双方相互认证对方，所以还能有效地解决安全问题，该方案比较适合于中小型规模的校园网络，对于大型校园网络的高并发响应，笔者建议采用 LDAP（轻量级目录访问协议）服务器来存放用户信息。

参考文献

1 Volchkov A. Revisiting single sign on a pragmatic approach in a new context. IT Professional, 2001, 139 - 145.

2 皮晓东. 单点登录的研究与实现[J]. 计算机与应用软件，2007，(6)：156 - 158.

3 常潘，沈富可. 基于 LDAP 的校园网络统一身份认证的实现[J]. 计算机工程，2007，(5)：281 - 283.

4 宫恩辉，朱巧明，李培峰. LDAP 和 Kerberos 在统一身份认证中的应用[J]. 苏州大学学报，2006，(4)：52 - 55.

5 Jennifer G. Steiner, An Authentication Service for Open Network Systems[J]. Project Athena MIT of Technology, 1988, 1：7 - 8.

6 曹世华. Active Directory 和 Kerberos 的校园网络统一认证的实现. 杭州师范大学学报，2007，(4)：309 - 312.

7 曹建春，姜建国. Kerberos5 在 Windows2000 网络中的应用[J]. 现代电子技术，2003，17：87 - 91.

8 The Kerberos Network Authentication Service (V5), RFC1510.