

基于校园网的安全统一身份认证研究

郭政慧¹, 杜冬高²

(1. 河南理工大学 现代教育技术中心, 河南 焦作 454000; 2. 焦作大学, 河南 焦作 454000)

摘要:随着校园网的发展,校园网上的应用系统越来越多,而且这些系统的认证互相独立,不适应数字化校园网的发展方向。基于此,文章在分析常用的认证方案和对现有系统改动最小的基础上,提出一种校园网的安全单点登录方案,利用公钥基础架构(PKI)、轻量目录访问协议(LDAP)和集中式认证服务(CAS),实现数字化校园网的安全统一身份认证。

关键词:轻量目录访问协议;认证;单点登录;公钥基础架构

中图分类号:TP393 **文献标识码:**A **文章编号:**1005-8788(2010)05-0017-03

Research on unified security identity authentication based on campus networks

Guo Zhenghui¹, Du Donggao²

(Modern Education and Technology Center, Henan Polytechnic University, Jiaozuo 454000, China;

2. Jiaozuo University, Jiaozuo 454000, China)

Abstract: With the development of campus networks, there have been more and more application systems on the campus networks and these system authentications are independent to each other, not adapted to the development of the digitalized campus networks. On the basis of the analysis of the conventional authentication schemes and the minimum changes of the existing systems, this paper proposes a security single-point login scheme and realizes the unified digitalized security identity authentication based on campus networks by using PKI, LDAP, CAS.

Key words: LDAP; authentication; SSO; PKI

0 引 言

随着对校园网基础设施的不断投入与信息化的发展,校园网内的应用系统得到迅速发展,如办公自动化、校园网计费、财务信息查询、教务管理和图书借阅资料等系统。现实情况是这些系统各自独立,每个系统都有各自独立的认证系统,更不用说系统其他数据方面的融合。用户在每个系统中都有独立的账号信息,对用户来说账号密码太多,有时在不同的系统中相同用户名对应于不同用户个人。系统越多管理难度越大,而这些应用也迫切需要校园网统一身份认证系统的支持^[1-3],以适应数字化校园网的发展趋势。基于此,本文分析了几种常用认证系统后,提出一种单点登录(SSO)的统一身份认证方法。该方法能让用户登录一次即可访问加入到此认证系统中的所有应用系统,同时为了认证通信双方的身份,保证数据传输的机密性和完整性,认证过程采用了公钥基础架构(PKI)^[4]。认证系统的后台数据库采用高效的轻量目录访问协议(LDAP),它是X.500的简化版,而X.509标准最早也是X.500的一部分。就数据本身的特点而言,证书库适合存放于LDAP中,用户证书的的申请由用户相关的LDAP

信息产生,用户认证通过后,用户对应用系统的访问权限仍可由其应用系统直接控制。认证系统采用集中式认证服务(CAS),本文扩充了其功能,使其在原有用户名密码身份认证的基础上,同时增加了支持数字证书的身份认证。

1 常用的认证方式分析

1.1 一般认证

一般认证是指每套应用系统都有自己独立的认证系统,与其他系统互不融合,用户在访问多个应用系统时,需要输入不同应用系统相应的账号口令等信息。目前没有实现统一认证的各应用系统正是采用这种认证方法,而且各个系统的认证和授权方式均不相同。

1.2 LDAP 认证和 RADIUS 认证

LDAP起源于X.500,具有分布式目录信息树结构,可对用户身份信息和系统控制信息进行有效组织和管理。它是一种特殊的数据库系统,专门针对读取、浏览和搜索操作进行了特定的优化,目录中的信息是按照树形结构组织,LDAP的具体信息存储在条目(entry)的数据结构中,它具有区别名(DN)的属性(Attribute),LDAP系统结构如图1

所示。远程认证拨号用户服务(RADIUS)是一种运行于网络接入设备和认证服务器之间承载认证、授权、计费 and 配置信息的完全开放的协议,承载于用户数字报协议(UDP)之上的分布式系统,反对未经验证的访问。

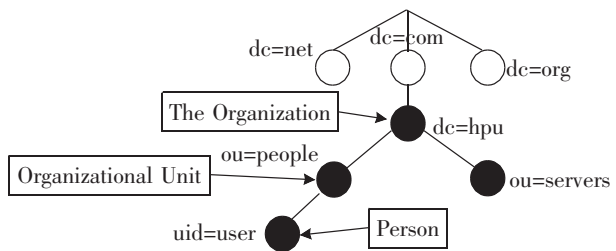


图 1 LDAP 系统结构图

这两种认证方法都是 C/S 模式,运行于传输控制协议/因特网互联协议(TCP/IP)之上,能用于对应用系统实行认证和一系列权限管理等功能。各种基于 LDAP 的开发包提供了操作 LDAP 的方法,如 Java、PERL 和 C 等环境开发包。RADIUS 也类似,它的后台数据库可以采用 LDAP,方便组织管理。这两种方法可以对不同应用系统进行认证授权,虽然用户账号信息统一了,但登录不同的系统时还得再次进行用户信息认证,不具备 SSO 特征行为。

1.3 Kerberos 认证

Kerberos 是一种网络认证协议,主要用于身份鉴别,只需验证一次身份信息即可访问多个服务,实现 SSO。它有一个第三方信任中心—密钥分发中心(KDC),如果身份验证通过,便可凭借此验证获得的票据来获得应用服务票据。Kerberos 协议提供对称密钥协商,以便进行安全通讯对话。Kerberos 认证过程如图 2 所示,一般实现基于 C/S 架构的 SSO 过程比较复杂,本文提出的认证过程是基于 Web 的,是简化过的 Kerberos,可实现跨域安全统一身份认证。Kerberos 的应用服务器票据是不保存在认证中心的,由客户端传给服务器,而本文的认证服务器票据是保存在认证中心的,而且只能使用一次。

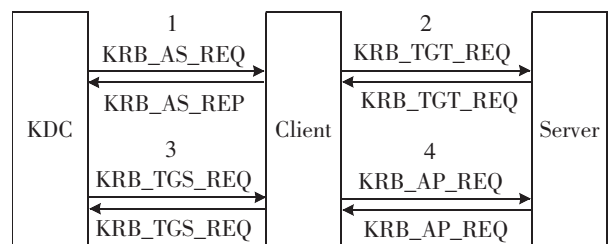


图 2 Kerberos 认证过程

2 证书库的实现方式

PKI 是目前网络安全建设的基础与核心,它由公开密钥技术、数字证书和数字证书认证中心(CA)等基本成分共同组成,用于实现身份认证、安全传输、不可否认性和数据完整性,采用证书进行密钥管理。证书库是 PKI 的数据中心,用于发布 CA 认证的 X.509 证书和证书吊销列表(CRL),CA 数字签名确保用户的可靠性,数字证书是经 CA 中心数字签名的包含公开密钥拥有者信息和公开密钥等信息的文件,CRL 用于控制用户公钥的有效性,证书持有者用相应私钥证明自己。证书中数据存放形式与 LDAP 数据存放形式相对应,呈属性-属性值对状态,LDAP 灵活的 Schema 定义及对象管理、方便扩展的应用能够有效地同 PKI 体系有机结合,还有灵活的检索机制,非常适合存放证书。

基于 LDAP 数据库^[5-6]的 PKI 证书库结构如图 3 所示,用户的全部实名制基本信息存储于 LDAP 中,CA 发布的证书和 CRL 也存储于 LDAP 中。用户申请证书时的信息来自于 LDAP,数据确认后的证书申请经 CA 签名,生成用于客户端登录的数字证书,采用标准的 PKCS#12^[7],它是受用户密码保护的安全证书的 pfx 格式,此证书由用户下载后导入到系统中,提供个人账户安全和个人身份识别。用户一旦申请数字证书成功,便可利用数字证书登录以保证账户的安全,同时用户还可以选择基于用户名密码的登录方式。推荐方式为证书登录,此时系统将自动从个人证书上读取身份信息并完成用户登录。数字证书申请时用户先采用用户名密码方式登录证书申请系统,只有证书申请签名成功,才能实现数字证书的 SSO。

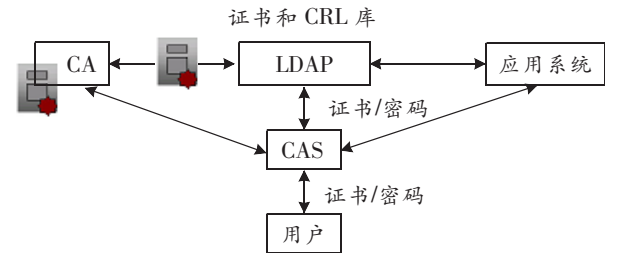


图 3 基于 LDAP 数据库的 PKI 证书库结构

3 SSO 认证方式的实现

SSO 是数字化校园应用系统服务整合的方案之一,用户只需一次性提供凭证,即可访问所有相互信任的应用系统。当前应用服务整合的最佳架构是

基于面向服务架构(SOA)的,利用 Web Services 来实现。校园网内的应用系统大多数是基于 Web,也就是 B/S 架构,CAS 是针对 Web 应用的一种 SSO 认证框架^[8],能通过浏览器实现对 B/S 架构应用的统一账号认证。CAS 的认证原理如图 4 所示,CAS Client 部署在应用服务端,以 Filter 方式保护受保护的资源。本文扩展的 CAS 认证过程如下:

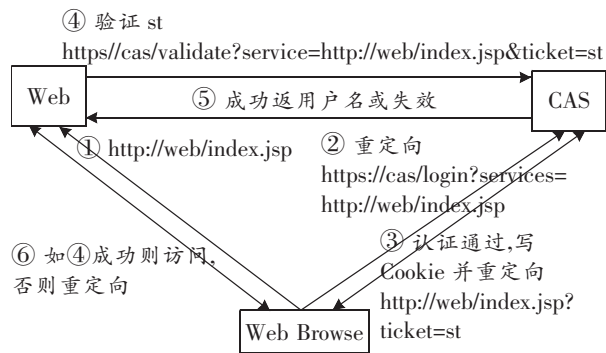


图 4 CAS 认证原理图

(1) 用户访问受保护的 Web 资源,CAS Client 分析该请求中是否包含 Service Ticket,如果包含,则跳到第(3)步;如果没有,则附带目标地址重定向到 CAS 认证中心。

(2) 如果用户已导入申请过的数字证书,弹出证书对话框让用户选择相应的证书,通过证书验证用户的身份,其中包括校验证书有效性、证书更新等;如果没有数字证书,则只能输入用户名密码登录。认证通过后写认证票据 Cookie(TGC),并把生成的 Ticket 附带目标地址后重定向。

(3) CAS Client 过滤器获取超文本传输协议(HTTP)访问请求,获得 Ticket,并向 CAS 验证 Ticket,如果有效,则访问应用服务;如果无效,则跳到第(1)步。

为了 TGC 的安全,访问 CAS 时采用 Https。如果用户申请了数字证书,可以选择用证书来进行认证,以保护账号安全,Ticket 采用一次性过程保证应用服务的安全。CAS 用不同方式认证用户信息时,需通过 LDAP 获取数据,如 CRL 和用户名密码等,这需要扩展用户认证接口,CAS 提供了认证统一接口和实现分离的方式,它与认证协议是分离的。CAS 提供扩展认证的核心接口是 AuthenticationHandler,有 support 和 authenticate 两种方法,support 验证传入的 Credentials 是否支持,然后 authenticate 进行认证。为了两种认证方式并存,实现

了 CAS 认证的证书和 LDAP 的 Credentials 接口,同时实现了相应的 CredentialsToPrincipalResolver 接口,如 X509CertificateCredentials 和 Abstract X509CertificateCredentialsToPrincipalResolver,利用相应的 CredentialsToPrincipalResolver 解析相应的 Credentials,确保数字化校园网安全统一身份认证。

4 结束语

随着数字化校园网的建设,相互独立的 B/S 应用系统已不适应数字化发展的趋势,需要把这些独立的应用系统以松散方式融合起来,而基于 SOA 架构,利用 Web Service 是当前最佳方案之一。其中 SSO 是实现数字化校园的本质基础要求,登录一次即可访问相互信任的应用系统。本文在分析比较几种常用认证方式的基础上,利用 PKI、LDAP、CAS,实现了数字化校园网的安全 SSO。其中用户信息的存储用高效访问 LDAP,CAS 的后台数据库和数字证书库都采用 LDAP,用户申请证书时,它的数据直接由 LDAP 中的相关用户信息提供,然后经 CA 签名发布于 LDAP 中,同时提供用户下载 pfx 格式数字证书。本文实现了基于 CAS 认证的用户名和证书认证两种方式并存,且证书认证优先级高于用户名密码方式,能提供账号安全登录,方便用户的使用,同时利用 Filter 保护有限的 Web 资源,对应用系统改动很少即可实现统一身份认证。

参考文献:

- [1] 马荣飞. 统一身份认证系统的研究与实现 [J]. 计算机工程与科学, 2009, 31(2): 145-149.
- [2] 季旻. 单点登录方案的研究与设计 [J]. 计算机工程与设计, 2009, (12): 2862-2864, 2914.
- [3] 李继勇. 一种单点登录协议的设计 [J]. 计算机工程, 2008, 34(14): 152-154.
- [4] 李小标. PKI/PMI 支持多模式应用的单点登录方案 [J]. 北京邮电大学学报, 2009, 32(3): 104-108.
- [5] 何朝辉. 基于 LDAP 的 PKI 证书的存储与备份 [J]. 计算机科学, 2005, 32(2): 66-68.
- [6] 郑洲. LDAP 目录服务在 PKI/PMI 中的应用 [J]. 计算机工程, 2004, 30(18): 49-51.
- [7] 彭英慧. 基于 PKCS#12 证书身份认证系统的实现 [J]. 计算机工程与设计, 2009, (8): 840-843.
- [8] 金伟祖. 基于 CAS 集群的单点失效问题解决方案 [J]. 计算机工程, 2010, 36(1): 51-54.