第 30 卷 第 3 期 华侨大学学报(自然科学版) Vol. 30 No. 3
2009 年 5 月 Journal of Huaqiao University (Natural Science) May. 2009

文章编号: 1000-5013(2009)03-0351-03

企业应用系统整合中的 CAS 单点登录技术

宋 鹏, 余金山

(华侨大学 计算机科学与技术学院, 福建 泉州 362021)

摘要: 针对企业应用系统单点登录的需要,提出一种基于中央认证服务器(CAS)的单点登录技术方案. 系统中,认证管理器通过责任链模式管理认证执行者,客户端浏览器与认证服务器之间采用 HTTPS 协议,认证服务器与平台应用服务器之间采用 HTTP 协议. 在访问业务系统时,相关信息的传递均结合时间戳、关键信息加密签名和 SSL 加密通道技术. 在自动认证完成后,业务系统可根据需要设定是否继续走安全套接层协议(SSL)加密通道,既保证单点登录过程中信息传递的保密性和真实性,又兼顾业务系统访问的安全与效率.

关键词: 单点登录; 企业应用系统; 身份映射; 中央认证服务器

中图分类号: TP 393.094 **文献标识码**: A

1 CAS 技术

目前,单点登录(SSO)是比较流行的企业业务整合的解决方案之一,而常见的单点登录技术有 Kerberos[1],SAML,CAS(中央认证服务器). CAS 是美国耶鲁大学开发的单点登录系统[2],能为多个 Web 应用提供单点登录基础设施,同时可以为非 Web 应用但拥有 Web 前端的功能服务提供单点登录的功能[3]. 它将用户身份认证集中于单一的 Web 应用,简化密码管理,从而提高安全性. 当需要修改身份验证的业务逻辑时,避免了对代码的修改[4].

CAS 包含服务端(Server)和客户端(Client)两部分. CAS Server 需要被独立地部署,负责完成对用户的认证工作. 它既可能是到数据库检索一条用户帐号信息,也可能是在 XML 文件中检索用户密码. 对这两种情况,CAS 均提供一种灵活但统一的接口/实现分离的方式,而 CAS 究竟采用何种认证方式是与 CAS 协议分离的,即认证的实现细节可以自行定制和扩展.

CAS Client 负责部署在客户端(Web 应用)上. 当接收到对本地 Web 应用受保护资源的访问请求,并且需要对请求方进行身份认证时,Web 应用不再接受用户名密码等类似的凭证(Credentials),而是重定向到 CAS Server 进行认证. CAS Client 的优势也在于,它对包括 Java,Net,ISAPI,Php,Perl,uPortal, Acegi,Ruby,VBScript 等多种客户端的支持. 可以看出,CAS 设计理念先进,并对客户端有着广泛的支持. 但是,Web 应用具有复杂多样,因此要将 CAS 部署到 Web 应用中,还涉及到 Web 应用的改造、应用授权、身份映射等问题.

2 应用系统单点登陆的实现方法

2.1 授权认证系统总体技术架构

图 1 为系统总体技术架构. 企业应用系统大都包含财务、办公自动化(OA)、工作流审批、人事等系统,实际整合中需要通过一个统一的门户进行展现,如图 1 中的 Portal Server. 轻量级目录访问协议(Light Directory Access Protocol,LDAP)目录服务器提供认证数据源,身份映射数据库提供统一帐户与应用系统用户信息的映射. 整合中,各应用系统单点登陆的实现有如下 4 个步骤.

收稿日期: 2008-07-11

通信作者: 余金山(1952-),男,教授,主要从事软件工程及人工智能应用的研究. E-mail:yjs@hqu.edu.cn.

基金项目: 福建省自然科学基金资助项目(A0810013)

(1) 用户登录应用系统的时候,首先要通过用户认证过滤.如果用户通过认证服务器认证,则直接进入票据验证层;如果没有通过认证服务器的认证,则重定向到认证服务器的用户认证中心进行认证.

(2) 认证完成以后,会发送一个认证票据给客户端,同时把产生的票据保存到票据中心.

(3) 用户进入票据验证层,应用系统发送票据到认证服务器的票据中心进行票据验证.

(4) 当票据验证通过以后,用户进入用户授权中心,通过用户、角色等的权限,判断用户是否有权访问某个资源.

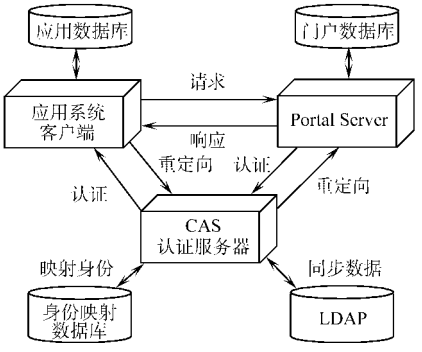

图 1 系统总体技术架构图

Fig. 1 System technique framework

2.2 用户认证中心设计

图 2 为用户认证中心设计图. 用户认证中心包括认证管理器、认证处理器、身份转换器.

(1) 认证管理器. 认证管理器是用户认证中心的管理者或者调度员,但它并不负责具体的认证操作,具体的认证操作由相关的认证执行者执行. 认证管理器通过责任链模式管理认证执行者.

(2) 认证处理器. 认证处理器负责具体的认证操作. 其使用 LDAP 目录服务器提供认证数据源. 设计一个认证 Handle 就是调用 LDAP 目录服务,从而实现认证功能. 在默认情况下,认证管理器可以设计多个认证 Handle,只要其中一个认证 Handle 认证通过,就不继续调用其他认证 Handle.

(3) 身份转换器. 在用户通过认证以后,将用户提供的用户名和密码转换为用户身份的转换器. 这里需要根据不同的认证提供不同的身份转换器.

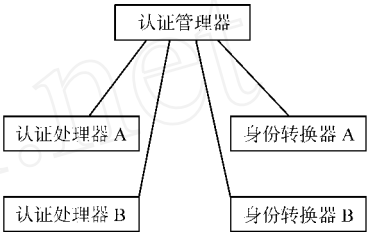

图 2 用户认证中心设计图

Fig. 2 Design diagram of the authentication center

2.3 业务系统的改造

图 3 为业务系统的改造图. 为了使企业中的应用实现单点登录,企业中的业务系统必须完成以下两方面工作. (1) 安装业务系统 SSO 客户端并配置证书和私匙,用以建立客户端与业务系统之间的 SSL 加密通道,并接受处理平台提供的加密签名的用户认证信息. (2) 提供映射接口和访问验证接口,并在平台进行配置. 映射信息主要是统一账户与业务系统用户信息(可能包括业务系统的用户名和密码)的对应关系.

用户统一认证过程采用 SSL 加密通道保证安全性,认证服务器负责 SSL 加密通道的建立. 对于口令认证方式,认证服务器配置为单向 SSL 加密通道,客户端不需要证书. 客户端浏览器与认证服务器之间采用 HTTPS 协议,认证服务器与平台应用服务器之间采用 HTTP 协议[5]. 在用户认证完成后,可根据需要设定客户端浏览器对平台的访问是否继续走 SSL 加密通道,充分兼顾安全与效率.

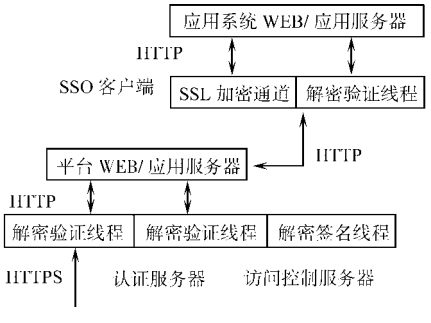

图 3 应用系统改造

Fig. 3 Transformation of application systems

2.4 应用系统间的用户映射

图 4 为映射工作流程图. 用户通过认证中心认证以后,在其第一次访问业务系统时,认证系统平台根据业务系统的配置会自动生成业务影射页面,要求用户进行映射关系配置. 其工作流程有以下 4 个步骤. (1) 用户输入业务系统的用户信息(可能包括业务系统用户名和密码). (2) 映射信息连同时间戳被平台的访问控制服务器进行加密和解密(业务系统证书加密,平台私匙签名,时间戳用于防止重放攻击). (3) 加密签名的映射信息通过 SSL 加密通道,传递至业务系统 SSO 客户端,并由其进行解密验证后交给业务系统验证. (4) 映射信息验证通过,则平台将用户统一帐户与业务系统用户信息建立对应关系,以备正常访问业务系统时使用.

如果用户完成了平台统一帐户与业务系统用户信息的映射[6],则在通过平台认证后,其访问业务系

统的流程有如下 3 个步骤. (1) 平台根据要访问的业务系统 ID 和会话(Session)中的用户统一帐户,查询用户的业务系统映射信息. (2) 将相应信息和时间戳由访问控制服务器加密签名并经由客户端,通过 SSL 加密通道,传递至业务系统 SSO 客户端,并由其进行解密验证后交给业务系统验证. (3) 业务系统验证通过后,自动跳转进入业务系统.

在访问业务系统时,相关信息的传递均结合时间戳、关键信息加密签名和 SSL 加密通道技术. 在自动认证完成后,业务系统可根据需要设定是否继续走 SSL 加密通道. 这既保证了单点登录过程中信息传递的保密性和真实性,有效防止了重放攻击,又兼顾了业务系统访问的安全与效率.

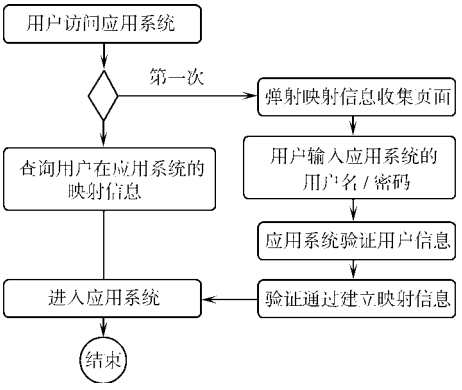

图 4　映射工作流程

Fig. 4　Flowchart of mapping

3　结束语

提出的 CAS 的企业应用单点登录整合方案,已经成功地应用到企业的应用系统整合中. 在前面的工作成果上建立一个面向应用的统一认证管理平台,为基于 J2EE 企业软件应用提供全面的安全访问策略,是今后的研究方向.

参考文献:

[1] 罗时飞. 敏捷 Acegi、CAS 构建安全的 Java 系统[M]. 北京:电子工业出版社,2007.

[2] 李小平,阎光伟,王轩峰,等. 基于公开密钥设施的单点登录系统的设计[J]. 北京理工大学学报,2002,22(2):209-213.

[3] 续　岩,季永志. 单点登录技术在 Web 应用中的研究与实现[J]. 计算机工程,2006(10):271-273.

[4] CHAMBERLIN N. A brief overview if single sign-on technology[J]. Government Information Technology Issue, 2000(1):3-7.

[5] GILMORE B, FARVIS K, MADDOCK J. Core middleware and shared services studies single sing-on report[EB/OL]. [2004-09]. http://www.jisc.ac.uk/index.cfm?name=porg_middss_studies,

[6] GROSS T. Security analysis of the SAML single sign-on browser/artifact profile[C]// 19 th Annual Computer Security Application Conference. [s.l.]:IEEE Computer Society,2003.

CAS Single Sign-On Technology for Integration of Enterprise's Application System

SONG Peng, YU Jin-shan

(College of Computer Science and Technology, Huaqiao University, Quanzhou 362021, China)

Abstract: In order to meet the single sign-on needs of the enterprise's application system, we propose a center authentication server (CAS)-based single sign on solution to integrate the Web applications. In the system, an authentication manager is given to manage the authentication executives through responsibility chain pattern, HTTP protocol is used for the communication between client browser and authentication server, and the communication between authentication server and application server; any information passing is processed with technology of time stamp, crypto-signature and security socket layer (SSL) cryptic channel when visiting a business system. The business system can choose to go through SSL cryptic channel or not by itself according to the need. Hence, not only the security and authenticity of the information passed in the process of single sign-on are guaranteed, the security and the efficiency of accessing to a business system are also ensured.

Keywords: single sign-on; enterprise's application system; identity mapping; center authentication server

(责任编辑:钱　筠　　英文审校:吴逢铁)