开源单点登录与角色权限管理的融合研究应用①

黄永生　张祖平　龙　军　(中南大学 信息科学与工程学院 湖南 长沙 410083)

摘　要： 单点登录是解决网络环境下门户系统安全认证的一种有效策略。在分析 Central Authentication Service (CAS)的体系结构、认证流程的基础上，对 CAS 进行了扩展，把粗粒度的角色权限管理机制引入到 CAS 中，提出了粗粒度、松耦合的基于角色权限管理的 CAS。使 CAS 不仅能快速完成统一身份认证，而且还具有权限控制功能,从而提高了整个系统的可用性与安全性。

关键词： 单点登录;CAS;身份认证;权限控制;松耦合

Fusion of Open Source and Role Based Access Control

HUANG Yong-Sheng, ZHANG Zu-Ping, LONG Jun

(School of Information Science and Engineering , Central South University, ChangSha 410083, China)

Abstract: Single Sign-On (SSO) is an efficient and secure authentication solution for portal system. This paper analyses the architecture and authentication process of CAS. By extending the CAS, a mechanism of coarse-grained Role Based Access Control is added to CAS. This paper proposes a new model of CAS, which has a coarse-grained and loosely-coupled Role Based Access Control. The extended CAS cannot be used for authentication, but can also be used for authorization, which increases availability and heighters the security of the system.

Keywords: single sign-on; CAS; identity authentication; authorization; loosely-coupled

1　引言

当前企业的应用系统越来越多，用户经常需要访问多个应用系统。由于各个应用系统有独立的用户认证模块，用户要进入各个系统就必须分别认证身份[1]。对于用户而言，每进入一个系统要登录一次，这无疑耗费大量的时间，同时需要记大量的用户信息,或者一套简单用户信息多系统使用，又造成保密强度降低的问题；对于系统管理员，需要大量的时间分别管理和维护不同系统的用户信息；对于开发人员，需要为每个应用系统设计和开发用户认证模块。单点登录就是为解决这些问题而产生的。单点登录是指用户只要一次性登录成功，就可穿梭于多个应用系统，而不必再登录[2]。

目前,单点登录的产品主要有: SUN 公司的 Open SSO，Yale University 的 CAS，Microsoft 的.Net Passport，BEA 的 WebLogic，基于 SAML 的 OpenSAML[3]。

相比之下，由于 CAS 设计理念先进、体系结构合理、平台独立性、客户端支持广泛、配置简单、支持多种认证方式等，已经成为单点登录领域著名的软件产品。在进行实际系统的设计与开发时，考虑到已经运行的网络评审平台的各个应用子系统是不同的开发语言实现的，运行的支撑平台也不同，认证系统需要跨平台以及支持多语言，还要能方便地进行扩展和定制，所以选用了 CAS 来单点登录功能。然而 CAS 只专注于身份认证，并没有授权功能，这对于网络评审平台来说，暴露太多信息给非授权用户，势必会降低系统的安全性[4]，同时用户会看到大量对自己没用的

① 基金项目:国家自然科学基金(60873081,60970095,M0921005);湖南省自然科学基金(07JJ6122)
收稿时间:2010-02-03;收到修改稿时间:2010-03-15

信息，也给用户体验带来了影响。为了进一步增强系统的安全性和提高用户体验，本文提出了基于角色权限管理的 CAS。

2 中央认证服务CAS

Central Authentication Service (CAS,中央认证服务)是耶鲁大学开发的开源单点登录项目，并且有大量的实际部署,是一个非常成熟可靠的SSO解决方案。

2.1 AS 的体系结构

在 CAS 的体系结构中,有 3 种实体: 用户浏览器，Web 应用，CAS 服务器。Web 应用程序不处理用户的登录，否则就是多点登录了，所有的登录都在 CAS 服务器进行。

(1) 用户浏览器：它需要满足三个条件才能在 CAS 中使用，一是支持 HTTPS；二是支持 HTTP 重定向；三是能存储 Cookie；

(2) Web 应用(Web Application)：装载了 CAS 客户端的应用程序。它只向已通过 CAS 服务器认证的用户提供服务。

(3) CAS 服务器(CAS Server)：单点登录服务的核心，验证用户名/密码等凭证，CAS 的认证方式跟协议是分离的，而且认证方式的实现细节可以自己扩展和定制。

2.2 AS 处理流程

CAS 的处理流程都是围绕服务票据 ST(Service Ticket)展开的。用户首次登录的处理流程主要分为两个部分：CAS 生成票据 ST，Web 应用验证票据 ST。

(1) CAS 生成票据 ST

生成服务票据 ST 是整个流程的核心,票据有一定的有效期，同时是很难猜测的，具体流程见图 1。

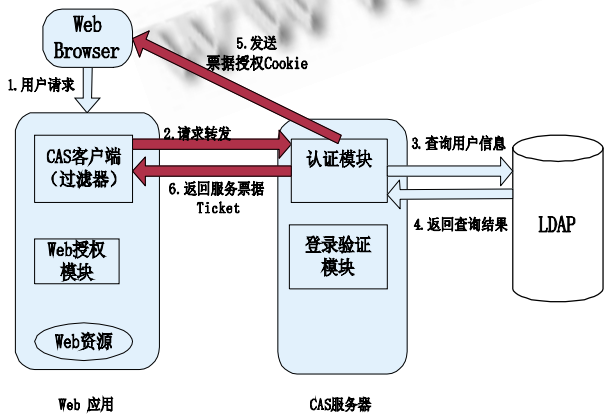

图 1 CAS 生成票据 ST

① 用户首次访问 CAS 下的某个 Web 应用；

② 如果用户没有登录，Web 应用重定向用户到 CAS 认证服务器，显示给用户的是 CAS 的登录界面，它要求用户输入用户名/密码等身份信息；如果用户已经登录了,就会直接生成服务票据 ST,跳转到第 6 步，不用再输入用户密码信息，即实现单点登录；

③ CAS 获取用户名/密码等身份信息，然后通过某种认证机制进行认证。通常认证机制是 LDAP；

④ 认证模块获得认证结果；

⑤ 如果认证成功，为了实现单点登录，CAS 要向浏览器发送一个的“票据授权 Cookie”，用来表明用户已经成功登录 CAS；

⑥ CAS 服务器创建一个很长的、随机生成的字符串，称为“服务票据”。这个票据是一次性使用的凭证，它使用一次后将会被删除。之后 CAS 重定向用户到原来的Web应用,把这个票据作为参数传给该Web应用。

(2) Web 应用验证票据 ST

Web 应用收到票据之后，它的过滤器(CAS 客户端)会向 CAS 服务器发送一个验证请求，来验证票据 ST 是否合法。这是通过将票据和 Web 应用的地址作为参数传递给 CAS 的校验 URL 来实现的。如果验证成功，CAS 返回一个 NetID 给 Web 应用，Web 应用接收到 CAS 返回的 NetID，最终把用户请求的资源返回给用户。

3 基于角色权限管理的CAS

由于 CAS 只有身份认证，并没有授权功能。而对在安全方面要求较高的系统中，显然是不够的，原因有两个：一是对于不同角色的用户，能够单点登录的 Web 应用是不同的，尽量避免将用户权限之外的应用系统暴露给用户；二是由于网络评审平台要求不同角色的用户所看到的平台页面也不一样，即根据角色来进行用户的访问控制，可以提高系统的安全性。要满足这些要求，只有在认证的时候就进行权限控制才能做到。

由于网络评审平台 Web 应用系统多，用户庞大，CAS 服务器的访问量很大，如果权限控制太细，势必会影响系统的性能；为了方便以后的扩展和提高代码复用性，权限控制模块不能太依赖 CAS，只使用 CAS 提供的接口就行了，所以提出了粗粒度、松耦合的基于角色权限管理的 CAS，改进后协议的体系结构如图

2 所示：

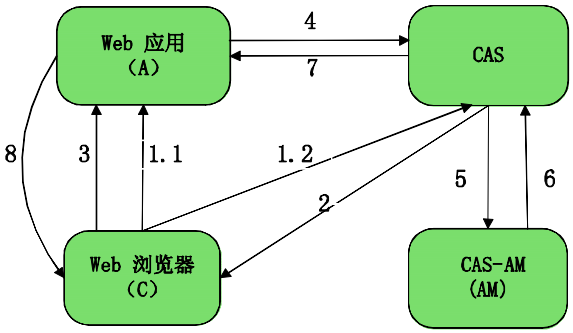

图 2　改进后协议的体系结构

3.1 后协议的说明

(1.1) C→A: ServiceA;

/* 用户向 A 发出请求。C：Web 浏览器；A：We 应用; ServiceA：A 下面的某个具体的服务。 */

(1.2) C→CAS：IDc|| ServiceA;

/*用户被重定向到 CAS，并要求提供身份信息。CAS：中央认证服务；IDc：用户身份信息。 */

(2) CAS → C: TGCc[IDTGC||Namec||IPc||Domainc||LoginTimec||ExpireTimec]||STc;

/* CAS 对用户身份验证成功后，向 C 写入一个票据授权 Cookie，用来表明用户已经登录。 TGCc：票据授权 Cookie(Ticket Granting Cookie),包含 ID，用户名(不含密码信息)，用户 IP，域名，登录时间，到期时间; STc：C 访问 A 的服务票据，是认证成功后由 CAS 生成的随机数。*/

(3) C→A: STc;

/* 用户拿着服务票据(STc)去访问 A。*/

(4) A→CAS: STc || ServiceA;

/* A 发送请求到 CAS，来验证用户提供的服务票据(STc)是否有效。*/

(5) CAS→AM: IDc|| ServiceA;

/* CAS 发送请求到权限管理模块(AM)，来验证用户是否有访问 ServiceA 的权限。*/

(6) AM→CAS: IDc||Priviledgec;

/* 权限管理模块(AM)回应 CAS 的请求，返回用户是否有访问 ServiceA 的权限。*/

(7) CAS→A: NetID [Namec ||Successc] ;

/* CAS 回应 A，如果认证成功并有权限，返回 NetID。NetID：包含用户名，认证是否成功。*/

(8) A→C: Resultc.

/* A 回应 C，如果认证成功，返回用户所请求的资源，否则重定向到 CAS 的登录页面 */

3.2 议的实现方案和处理流程

为了实现改进后的协议，我们提出了下面的实现方案：

(1) 引入一个扩展的 CAS 权限管理模块(CAS-Authorization Management, CAS-AM)，独立于 CAS 协议，角色信息保存在数据库中(可以是任意类型的数据库)；

(2) CAS-AM 作用于验证票据 ST 时，如果验证票据成功，则调用 CAS-AM 进行权限控制；

(3) CAS-AM 根据用户名，在角色数据库中查找用户相应的角色，得出用户的访问权限，并判断用户是否具有访问该 Web 应用的权限。

由上面的实现方案可得到新的处理流程，具体流程见下图 3：

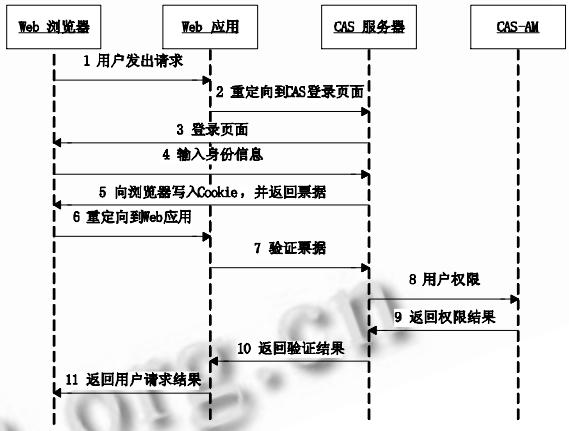

图 3　改进后协议的处理流程

因为增加了权限控制的功能，CAS 服务器上要提供与权限管理模块(CAS-AM)的接口，用来发送查询用户权限的请求和接收 CAS-AM 返回的结果，这样即使用户可以通过认证，如果管理员没有对其进行授权，仍然是不能访问到 Web 应用的任何资源，相当于增加了一个安全锁，从而增加系统的安全性。同时对于人员按部门权限来管理很方便，如果员工从一个部门调到另一个部门，只要改变用户角色就可以了。

4　CAS单点登出

CAS3 之后的版本开始支持单点登出，一旦 Ticket Granting Cookie(TGC)到期，就会自动单点

登出，但是对单点登出的支持并不完全。只有浏览器与 Web 应用的会话是由 Web 应用来维持的，才能实现单点登出，而如果浏览器与 Web 应用的会话是由浏览器的 Cookie 来维持的，并不能实现单点登出，这势必会存在潜在的风险，因为有时表面上用户登出了，但实际上是一种对用户的欺骗，用户并没有真正的退出。

4.1 底解决单点登出的问题

目前，因为当浏览器与 Web 应用的会话是由浏览器的 Cookie 来维持的，CAS 还不能实现单点登出。这时可以利用 Cookie 技术实现单点登出：

(1) 当 Web 应用接收到 CAS 服务器验证票据所返回的成功信息后，在向浏览器返回所要访问的内容之前，先向浏览器写入一个“会话 Cookie”，有效期跟 Ticket Granting Cookie 一样；

(2) Web 应用响应用户的每个请求时，都检查“会话 Cookie”是否存在到期，到期就重定向到 CAS 服务器登录页面，否则用户可以继续访问 Web 资源；

(3) 一旦向用户发送单点登出请求，CAS 服务器自动向该用户已经登录的 Web 应用发送 POST 请求，要求终止该用户的会话，Web 应用收到请求，设置浏览器“会话 Cookie”到期，由(2)可知，用户就不可能再访问 Web 应用的资源了。

5 结束语

粗粒度、松耦合的基于角色权限管理的 CAS 的提出，使得 CAS 不仅完成身份认证，而且具有权限控制功能。在单点登录时就对用户进行粗粒度的权限控制，尽量确保 Web 应用的安全，同时可以根据角色来呈现不同的页面，这样不同角色的用户所看到的平台页面也不一样。这样就很好地满足了网络评审平台的需求，提高了系统的可用性与安全性。同时也对单点登出进行研究，利用 Cookie 技术，真正实现了单点登出，一旦用户单点登出，不可能再访问 CAS 下的任何 Web 应用，进一步提高了系统的安全性。

由于所有的认证都集中在认证中心进行，目前单点登录系统都存在一个共同的隐患，那就是一旦认证服务器被攻击或者出了故障，将会影响所有的 Web 应用，甚至整个系统瘫痪[5]。因此，将来的工作就是提高认证服务器防范攻击和故障恢复的能力，实现单点登录系统的高可用性。

参考文献

1 Wu KX, Yu XL. A Model of Unite- Authentication Single Sign-On Based on SAML Underlying Web. 2009 Second International Conference on Information and Computing Science. Washington: IEEE Computer Society, 2009,211－213.

2 朱瑞丹.单点登录在企业门户应用中的实现[硕士学位论文]. 杭州:浙江大学, 2007.

3 周晓寰.基于 SAML 的 WEB 单点登录系统(WEB SSO)的研究与实现[硕士学位论文].北京:北京邮电大学, 2007.

4 Juntapremjitt S, Fugkeaw S, Manpanpanich P. An SSO-Capable Distributed RBAC Model with High Availability across Administrative Domain. 22nd International Conference on Advanced Information Networking and Applications. Washington: IEEE Computer Society, 2008,121－126.

5 续岩,季永志.单点登录技术在 WEB 服务中的研究与应用.计算机工程, 2006,32(10):271－273.