基于指纹识别和 CAS 的单点登录模型技术研究*

吴贤平
(温州大学, 浙江 温州 325035)

摘 要: 针对普通 CAS 单点登录模型安全性较差的缺陷,系统地分析了指纹识别和 CAS 单点登录模型,提出了一个综合两者优势的 Web 单点登录系统模型 FP-CAS,探讨了用户登录流程的实施过程。该模型具有指纹安全系数高、不容易破解和 CAS 单点登录的多重优点。通过测试和实施表明,该改进模型能更有效地提高 Web 应用的安全系数,用户信息更加保密,安全与效率兼顾。

关键词: 单点登录; 中央认证服务; 指纹; FP-CAS
中图分类号: TP311 **文献标志码**: A **文章编号**: 1001-3695(2012)04-1381-03
doi:10.3969/j.issn.1001-3695.2012.04.050

Research on SSO model based on fingerprint and CAS

WU Xian-ping
(*Wenzhou University*, *Wenzhou Zhejiang* 325035, *China*)

Abstract: Aiming at the poor safety defects of the CAS single sign-on model, this paper analyzed the fingerprint identification system and CAS single sign-on model, proposed a comprehensive model integrating the both advantages for Web single sign-on system called FP-CAS, then discussed user login process, the implementation process. The fingerprint CAS model had a high safety factor, not easy to break and multiple CAS advantages. Finally, testing and implementation show that the improved model can be more effective in raising the safety factor of Web application, user information can be more confidential, security and efficiency are both takeh into account.

Key words: single sign-on; CAS(central authentication service); fingerprint; FP-CAS

随着 Internet 的高速发展和现代企业信息化建设和集成技术越来越完善,电子邮件系统、办公自动化 OA、ERP、人事管理、财务管理、Notes 系统、客户关系管理 CRM 及各种特殊业务系统等得到了广泛应用,企业用户迫切需要同时访问或集成多个应用系统,实现企业资源的共享与发布。各种异构的应用系统一般都是相互独立的,都有其不同的认证方式,造成用户需要在集成平台中的应用系统间频繁地切换进行多次登录,操作较复杂,不但给用户带来极大的不便,而且对平台的整体安全性造成了很大威胁,无法快速地整合和分析利用各系统相关业务信息;此外,用户在进行业务操作时,需要重复登录到不同的应用系统中并认证,造成用户数据大量重复和冗余,系统用户资源管理也不够统一,越来越不适应现代对高效自动化办公的需求,而且由于系统较多,用户账号或密码遗忘现象时有发生,或者一套简单用户名和密码多系统使用,造成保密强度降低等问题; 而在安全性和系统管理方面,为了提高整体安全性而被迫需要采取增加安全访问策略又导致系统的执行效率和系统的可用性大为降低,同时企业也需要大量的人力来分别管理和维护不同系统的用户信息。

基于安全和效率的因素,如何为企业用户提供安全快捷的集中式统一认证与授权方式,并建立安全、可靠、保密的 Web 应用系统,保证企业业务不受破坏和干扰的整合安全性已经成为企业开展信息化建设迫切需要解决的关键问题之一。单点登录[1](single sign-on,SSO)可以很好地解决企业异构系统之间的集成和用户数据统一管理和认证问题。所谓单点登录[2],就是指用户只需在 Web 应用系统[3]中进行一次身份认证,随后便可以访问其被授权的所有资源,而不需要再次触发其他的身份认证过程。单点登录不仅可以集成[4]各种应用系统,而且还能提高工作效率,更有效地管理系统。

CAS 技术为有效地实现大范围异构分布环境下的企业间系统协同提供了支撑平台[5]。在单点登录领域,有一个重要的而且是开源的模型——CAS 登录模型,本文针对 CAS 单点登录模型安全性不足的缺陷,通过对 CAS 模型以及指纹登录的安全可靠结合在一起进行分析比较,将两者优点互相融合,提出一种新的 Web 环境下的单点登录模型即 FP-CAS。该模型可以跨越多个不同的域传递用户的身份信息,完成用户身份的单点认证,最后对该模型的安全性进行了分析。

1 SSO 和 CAS 模型介绍

1.1 CAS 单点登录的体系机构

目前,单点登录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[6]、SAML[7]、OpenSSO、SourceID. NET、WebAuth。

CAS[8]是 Yale 大学发起的一个开源单点登录项目,旨在为 Web 应用系统提供一种可靠的单点登录方法,它是 JA-SIG 的一个开源的企业级单点登录解决方案。CAS 包含服务端 server 和客户端 client 两个模块,其中 CAS server 需要独立部署,为 SSO 提供服务支撑的 Web 应用, 主要负责对用户的认

收稿日期: 2011-08-31; **修回日期**: 2011-10-16 **基金项目**: 浙江省教育科学规划资助项目(SCG154)
作者简介: 吴贤平(1978-),男,浙江永嘉人,实验师,硕士,主要研究方向为计算机网络及应用(wuxianpinglaoshi@163.com).

证工作。CAS client 支持多种客户端,包括 Java、Acegi、. NET、PHP、Perl、Apache、uPortal、Ruby 等。

CAS 应用广泛,具有独立于平台的、易于理解、扩展和改进的特点:a)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;b)简化应用认证用户身份的流程;c)将用户身份认证集中于单一的 Web 应用,让用户简化他们的用户基本信息管理,提高安全性;当应用需要修改身份验证的业务逻辑时,不需要在各单独系统中维护或修改源代码。

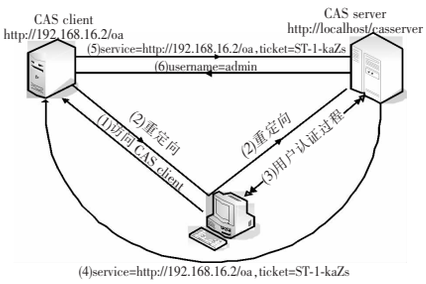

图 1 CAS 单点登录过程示意图

1.2 CAS 的实现原理

如图 1 所示,CAS client 与受保护的客户端应用部署在一起,以 filter 方式保护受保护的资源。对于访问受保护资源的每个请求,CAS client 分析该 HTTP 请求中是否包含 service ticket(ST),如果没有,则说明当前用户尚未登录,于是将请求重定向到 CAS server 登录(http://localhost:8080/casserver/login)地址,并传递 service URL(即要访问的目的资源地址,如上述 oa),以便登录成功过后重定向到该地址。用户在图 1(3)步中输入认证信息,如图 2 所示。

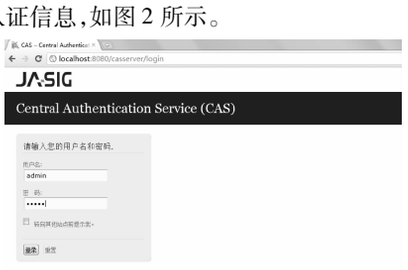

图 2 认证界面

如果登录成功,CAS server 随机产生一个唯一、不可伪造的 ST[9],并缓存以待再次访问资源时验证,如图 3 所示。

图 3 登录成功

然后 server 自动重定向到 service 指定的 URL,并为客户端浏览器设置一个 TGC(ticket granted cookie):TGT-1-NhDCOA2NFdL25RWcPfxVTqdF4V0zaqeUMCYeabb7hNwTjeittj-cas。

CAS client 在得到 service 和新产生的 ticket 过后,在第(5)(6)步中与 CAS server 进行身份验证,以确保该 ST 的合法性。CAS 这样就把这个 ticket 和成功登录的用户以及用户要访问的 service 联系起来,免去多次登录多个 client 的麻烦。

当成功登录到 CAS 服务器后,浏览器会存储 CAS 服务器返回的一个 cookie,其名字默认为“CASTGC”。当目标 Web 应用实施了 CAS SSO 之后,它们便需要借助于这一 cookie 实现 Web SSO 会话。由此建立了用户与 CAS 服务器之间的信任关系。如果用户需要退出,可以通过 http://localhost:8080/casserve/logout 退出 CAS 服务器。退出操作将导致浏览器中存在的 CASTGC cookie 被销毁,即销毁 CAS 与当前用户已建立的信任关系(Web SSO 会话)。事实上,由于本文使用的是 HTTP 操控 logout,因此浏览器中的 CASTGC cookie 并未被销毁。如果借助于 HTTPs 操控 logout,则浏览器中的 CASTGC cookie 便会被销毁掉。在未启用 HTTPs 时,如果使用 IE,可以通过关闭浏览器以达到销毁 CASTGC cookie 的目的。

在该协议中,所有与 CAS 的交互均采用 SSL 协议,确保 ST 和 TGC 的安全性。协议工作过程中会有两次重定向的过程,但是 CAS client 与 CAS server 之间进行 ticket 验证的过程对于用户是透明的。

CAS 可以方便地解决多个 Web 应用的单点登录,但同时也暴露出其局限性:a)验证票据使用浏览器 cookie 作为存储媒介,存在安全隐患;b)用户名/密码验证方式过于简单,安全性不高。

2 改进的 FP-CAS 模型设计

2.1 FP-CAS 模型优点

鉴于 CAS 单点登录模型基于用户名和密码的登录验证局限性以及安全性较差的缺点,且无法满足用户对认证信息高保密和高要求的需求,本文提出了一种基于指纹的 CAS 认证模型,它扩展了 CAS 的 server 和 client 端的验证和信息传递方式,是一种安全可靠的单点登录模型。

FP-CAS 模型利用指纹[10]特征码实现了用户身份的匹配和识别,将指纹身份认证技术和 CAS server 绑定部署,通过指纹识别、比对、认证实现对用户的身份确认,实现指纹登录、权限管理、用户身份识别等功能,为用户提供统一的信息资源认证访问入口,通过实施指纹单点登录功能,使用户只需一次登录就可以根据相应权限访问不同的应用系统,而且具有很高的安全可靠性。

FP-CAS 模型实现了密码和指纹的双因子认证方式,以便在用户指纹磨损的情况下无法识别指纹的时候有对应的保障方案,这样既解决了信息不可窜改、不可抵赖性,又进一步规范了用户的安全认证流程。用户只需在一处登录完成身份验证,即可访问其他所有相互信任的信息系统,显著降低用户认证信息的维护成本,减少因密码遗忘、丢失、被窃取等人为造成的信息泄密风险,提高业务系统易用性、安全性、稳定性。它利用人类独一无二的指纹特征进行用户身份识别与网络权限管理,改变了传统的“用户名 + 密码”身份识别方式,实现了 Web 与现实真实身份的人证合一,有效防止用户身份遭他人的非法冒用。该模型将指纹识别技术与系统用户权限管理机制有效结合,提供指纹认证接口调用,可以彻底杜绝他人通过密码、USBKey、动态密码卡等传统身份认证方式窃取、窜改用户授权资源。

2.2 FP-CAS 模型的整体架构

2.2.1 指纹比对算法

由于每个人的指纹在皮肤纹路的图案、断点和交叉点上各不相同,具有唯一性。依靠这种唯一性和稳定性,就可以把一个人同他的指纹对应起来,通过比较他的指纹和预先保存的指纹进行比较,以此验证他的真实身份。

采用指纹仪厂商提供的 OCX 控件采集指纹图像,获取指纹特征码并约定密钥 key,利用 MD5[11] 或者 3DES 算法进行采集时间戳和指纹特征码的加密,保证数据传输的安全。

指纹采集提交后在服务器端,根据约定的 key 和算法对密文进行解密,同时比对客户端时间戳与服务器时间的差异,如果超过规定范围则认为是一次不合法的请求,则指纹比对不通过。该接口提供给统一认证的浏览器端(用户客户端),同时也提供给其他第三方基于 B/S 架构模式的应用使用。

指纹比对算法如下:

a)调用指纹采集控件获得指纹特征图像。

b)根据得到的特征图像计算得出特征码(512 bit)。

c)根据客户端时间戳 yyyyMMddHHmmss 和特征码生成加密后的字符串,得到密文并提交给服务器。

d)服务器端获取混合字符串后,解密文本串,得到时间戳和指纹特征码,将该时间戳与解密得到的时间戳进行比对,如果一致,则进行特征码比对,否则返回认证失败的信息。

算法流程如图 4 所示。

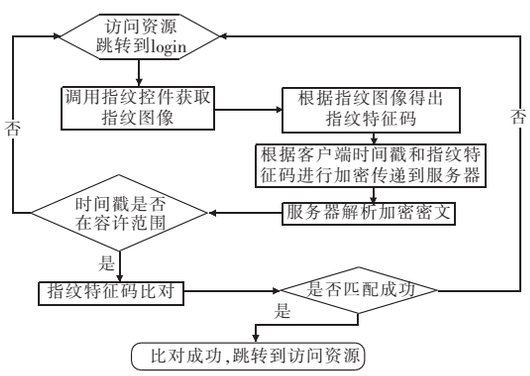

图 4　指纹比对流程

2.2.2　模型整体架构

模型整体架构及 FP-CAS 单个服务访问流程如图 5、6 所示。

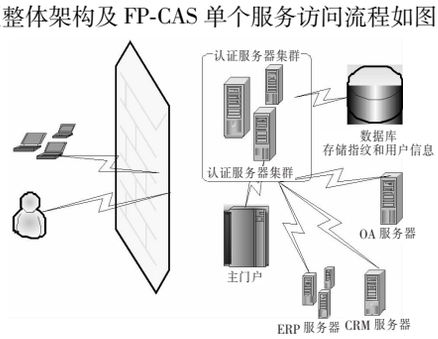

图 5　模型整体架构图

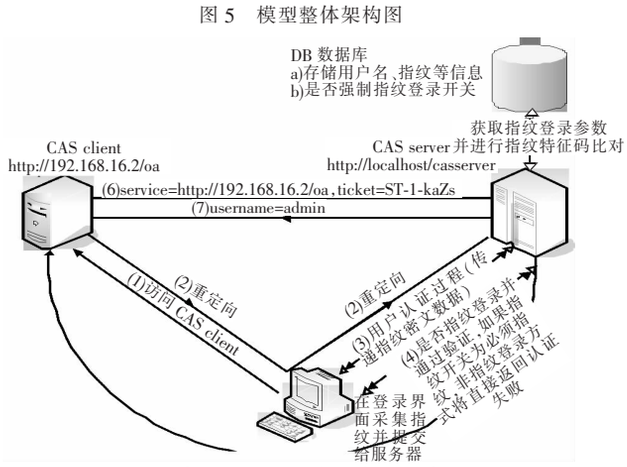

图 6　FP-CAS 单个服务访问流程图

主要原理[12]:用户第一次访问一个 CAS 服务的客户 Web 应用时(访问 URL:http://192.168.16.2:8888/oa),部署在客户 Web 应用的 AuthenticationFilter 会拦截此请求,生成 service 参数,然后 redirect 到 CAS 服务的 login 接口,URL https://casserver:8443/cas/login?service=http%3A%2F%2F192.168.16.2%3A8888%2Foa%2F,用户输入用户名和录入指纹、提交,等服务器认证成功后,CAS 服务器会向客户应用返回一个认证 cookie,并写入浏览器,将 session 缓存到服务器本地,同时生成一个 ticket 保存到服务器,最后将请求 redirect 回客户 Web 应用,URL 为 http://192.168.16.2:8888/oa/?ticket=ST-1-Bx6eyvj7cPPCfn0pMbuCwnbMvxpCBcNAIi6-11。这时客户端 TicketValidationFilter 过滤器处理,利用 httpclient 访问 CAS 服务的/serviceValidate 接口,将 ticket、service 都传到此接口,由此接口验证 ticket 的有效性,如果得到验证成功的消息,就会把用户信息写入 Web 应用的 session 里。至此为止,SSO 会话就建立起来了,以后用户在同一浏览器里访问此 Web 应用时,AuthenticationFilter 会在 session 里读取到用户信息,所以就不会去 CAS 认证。如果在此浏览器里访问别的 Web 应用时,AuthenticationFilter 在 session 里读取不到用户信息,会去 CAS server 的 login 接口认证,但这时 CAS 会读取到浏览器传来的 cookie,不需要重复登录,只是根据 service 参数生成一个 ticket 及 ticket 的交互验证。

2.2.3　重要扩展和模型实施

扩展后的指纹登录界面如图 7 所示。

图 7　CAS 指纹登录界面

输入用户名并点击“指纹登录”,这时激活指纹仪录入指纹并提交给 CAS server 验证。FP-CAS 一个最重要的扩展点即为扩展 CAS,提供一个基于指纹的身份认证程序,通过实现接口 AuthenticationHandler 达到此目的,并实现方法 boolean authenticate(Credentials credentials) throws AuthenticationException 来扩展指纹比对处理 FpAuthenticationHandler 方法。

Credentials 是由 client 提供给 CAS server 来证明自身身份的信息,传统的如一个用户名/密码对就是一个 Credentials,或者在 FP-CAS 模型中 3DES 加密算法生成的指纹特征码和用户名就是一个 Credentials。在程序的实现上,Credentials 被声明为一个可序列化的接口,仅仅起着标志作用,申明接口用 Java 代码描述如下:

```
interface Credentials extends Serializable { }
```

定义了一个传递用户名和指纹特征码的 Java 类:

```
public class FingerprintCredentials implements Credentials {
    private string username;
    private string fingerprint;
    //省略 setter,getter
}
```

其中 CAS server 验证核心代码如下所示:

```
boolean isFpMatch = false;
```

(下转第 1390 页)

的稳定性较低;相反,每个角色的行为概率分布比较密集,则该工作流模型的稳定性较高。其中,密集度用相对值表示为

$$\beta = \frac{|R_k^* - R_k^0|}{R_k^0} \tag{7}$$

当$\beta \leqslant 30\%$,工作流模型稳定;当$\beta > 30\%$,工作流模型不稳定。

最后可根据实际情况,估计该模型中四种角色执行行为的初始概率,并赋予其具体的数值,经过严格的数学计算,得到$\beta \leqslant 30\%$,因而该模型具有较好的稳定性。在此不再论述。

5 结束语

基于角色的工作流模型是合理的、稳定的,能够适应需求的多样化和流程的变动性,其中角色之间的交互提高了工作流管理系统的柔性和灵活性,在实际应用中有较好的适应性。本文在前人研究的基础上,强调了供需网环境中角色的概念及其属性特征,分析了在供需网模式下基于角色的工作流建模的可行性,提出了基于角色的供需网工作流模型,并结合一个简单的实例系统地总结了模型建模的步骤。最后该模型经马尔可夫链理论验证是稳定的,能够提高整个工作流的效率,实现流程的自动化。这种基于角色的工作流建模思想,有利于完善模型结构,扩大工作流管理系统的应用范围和适应能力,提高供需网系统内部的安全性和正确性。

参考文献:

[1] 徐福缘,何静,林凤,等. 多功能开放型企业供需网及其支持系统研究——国家自然科学基金项目(70072020)回溯[J]. 管理学报,2007,4(4):379-383.

[2] 何建佳,徐福缘. 面向和谐:管理的嬗变与多功能开放型企业供需网——基于复杂性、人类合作视角的分析[J]. 外国经济与管理,2009,31(3):16-22.

[3] 徐福缘. 大批量定制生产的理论与应用[M]. 上海:上海科学技术出版社,2008.

[4] 何建佳,徐福缘. 供需网:复杂性下管理根本问题的否思与创新[J]. 兰州学刊,2011(8):53-56.

[5] 何建佳,徐福缘. 基于角色的供需网工作流建模与分析[J]. 计算机应用研究,2010,27(10):3813-3815.

[6] KEITH T, PETER H, ROBERT J, *et al*. RolEnact: role-based enactable models of business processes[J]. Information and Software Technology,1998,40(3):123-133.

[7] KIM Y. Partnering process innterorganizational relations:roles of communication technology in the process of building organiza-tional partnerships[EB/OL]. (2000-10-09). http://www. msu. edu/user/kimyong2/interorg. htm.

[8] BIDDLE B, THOMAS E. Role theory: concepts and research[M]. New York:Wiley,1996.

[9] 赵卫东,黄丽华. 面向角色的多 agent 工作流模型研究[J]. 管理科学学报,2004,7(2):56-60.

[10] Workflow Management Coalition. WFMC-TC00- 1003, The workflow reference model[S]. 1995.

[11] 赵卫东,黄丽华,蔡斌. 基于角色的工作流研究[J]. 管理工程学报,2003,17(4):9-13.

[12] 汤双权,金可音,余青,等. 工作流过程模型研究[J]. 计算机技术与发展,2007,17(12):45-47.

[13] 何建佳,徐福缘. 面向复杂的大型集团企业知识管理系统的构建[J]. 中国人力资源开发,2011(7):19-22.

[14] ITU-TS. ITU-TS recommendation Z. 120: message sequence chart, ITU-TS [R]. 1996.

[15] 何建佳,徐福缘. 基于元胞自动机的自旋玻璃离散优化[J]. 系统工程,2011,29(7):91-99.

[16] 牟政,穆东. 基于马氏链的供应链稳定性评价[J]. 物流技术,2007,26(11):154-157.

(上接第 1383 页)

```
string username = credentials. getUsername( );
string fp = credentials. getFingerprint( );
//解析含特征码和时间戳的混合字符串
string timestamp = FpUtils. getTimeStamp( fp);
//比对特征戳,如果一致,则进行特征码比对
if( serverStamp. equals( timestamp) ){
//特征戳一致,进行指纹比对
return Fp_match( fp);
}
```

其中,Fp_match 为指纹比对的核心比较算法,最后在 deployerConfigContext. xml 配置文件中注册在 authenticationManager 的 authenticationHandlers 属性中配置 FpAuthenticationHandlers,即可完成 CAS 的指纹认证扩展模块,使 CAS 支持指纹认证模式。

3 结束语

本文提出一个基于应用 Web 服务的改进的 FP-CAS 单点登录模型,以一个受信任的第三方服务出现,支持指纹验证和普通用户名/密码验证的双因子身份认证方式,通过参数控制是否强制指纹登录和验证,具有较好的兼容性和扩展性,支持热插拔。FP-CAS 模型基于 Java 和 HTTP 开发,可以在无须对 Web 服务源码修改的情况下进行密码验证和指纹验证的切换和部署,对 Web 服务资源实施有效保护,兼容多种身份认证方式、容易部署、安全性强、能够免除服务提供方安全基础设施的重复建设以及具有良好的可扩展性等优点,具有较高的适用价值。

参考文献:

[1] FUGKEAW S, MANPANPANICH P. Adding SAML to two-factor authentication and single sign-on model for dynamic access control [C]//Proc of the 6th International Conference on Communications & Signal Processing. 2007:1-5.

[2] 李小平,阎光伟,王轩峰,等. 基于公开密钥基础设施的单点登录系统的设计[J]. 北京理工大学学报,2010,22(2):209-213.

[3] 李旭伟,汤丽萍,朱宏,等. B/S 架构的单点登录系统模型[J]. 四川大学学报,2006,38(2):132-136.

[4] PFITZMANN B, WAIDNER M. Analysis of liberty single-sign-on with enabled clients[J]. IEEE Internet Computing,2009,7(6):38-44.

[5] 张广胜,蒋昌俊,汤宪飞,等. 面向服务的企业应用集成系统描述与验证[J]. 软件学报,2007,18(12):3015-3030.

[6] 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.

[7] 陈天玉,谢冬青,杨小红,等. 基于 SAML 与 XKMS 的安全单点登录认证模型的研究与实现[J]. 计算机应用研究,2010,27(3):1019-1022.

[8] 赖慎禄,李新,及俊川. 可插入式单点登录技术的应用[J]. 计算机工程, 2008,34(14):121-123.

[9] 邱罡,张崇,周利华. 基于可信计算的 Web 单点登录方案[J]. 计算机科学, 2010,37(9):151-156.

[10] 汪同庆, 鲁军. 基于 MD5 算法和 Schnorr 协议的双因素身份认证系统[J]. 计算机应用研究, 2004,21(12):137-139.