文章编号：2096-1472(2018)-09-44-04
DOI:10.19644/j.cnki.issn2096-1472.2018.09.013

一种安全高效的跨域单点登录系统设计与实现

吴君楠，黎铁军，袁　远，隋荣恒
(国防科技大学计算机学院，湖南 长沙 410073)

摘　要：针对现有跨域单点登录系统存在的安全性不高、兼容性较差等问题，本文设计实现了一种安全高效的跨域单点登录系统。该系统通过多因子用户身份认证方法，结合票据加密传输，有效提升了系统安全性；并提供插件方式承接第三方应用系统，降低了开发成本。安全性分析与性能评测表明，该系统较同类系统安全性更高，性能更优，具有较好的应用前景。

关键词：单点登录；身份认证；跨域
中图分类号：TP39　**文献标识码**：A

Design and Implementation of a Secure and Efficient Cross-Domain Single Sign-On System

WU Junnan,LI Tiejun,YUAN Yuan,SUI Rongheng
(*College of Computer*,*National University of Defense Technology*,*Changsha* 410073,*China*)

Abstract: The existing cross-domain single sign-on systems have the problems of low security and poor compatibility. To address this issue,this paper designs and implements a secure and efficient cross-domain single sign-on system.The proposed system enhances system security by multi-factor user identity authentication and token encryption transmission.The system also provides plug-in interface to third-party application system,largely reducing development cost.Security analysis and performance evaluation show that the system has higher security and better performance than the existing systems,and has a good application prospect.

Keywords:single sign-on;authentication;cross-domain

1 引言(Introduction)

随着信息化技术的飞速发展，各行业的信息化建设都取得了显著成效，不但构建了信息化基础设施平台，还部署了诸如办公自动化、人事、财务、采购、仓库、研发等各种应用管理系统，极大提高了工作效率。但随着应用系统的增多，缺乏统一认证机制导致用户身份信息管理繁杂的问题日益突显。对用户来说，需要记忆多个用户名和密码，多次注册和多次登录，效率低，体验差；对管理者来说，每个应用系统存储独立的用户信息，导致信息冗余，增加了维护难度和成本。为了解决上述问题，单点登录(SSO，Single Sign-On)[1]技术应运而生，它允许用户只登录一次，便可使用系统中所有已授权的应用系统，具有方便高效的特点，同时结合统一认证机制和统一用户管理功能，可提高系统的安全性，降低运维开销。在实际部署中，应用系统通常都采用B/S架构，拥有各自的域名，单点登录系统需要使用跨域传递单点登录验证信息，因此跨域单点登录成为研究的热点。

目前主流的国外跨域单点登录系统解决方法有：自由联盟计划Liberty Alliance Project[2]，所有联盟成员公共访问“公共域Cookie”，且其仅使用用户名口令认证方式，安全性不高，容易遭受字典攻击[3]；Microsoft .NET Passport[4]，采用类似Kerberos身份认证方式[5]，集中认证分布授权，首先对用户ID进行认证，然后设置Passport域的Cookies(包含Passport unique ID的信息)，当Passport使用密钥加密后，服务器返回给用户包含其profile信息，使用其参与.Net Passport的密钥对其加密，参与.Net Passport收到传来的请求后，由服务器组件解密传来的信息，这样把用户身份认证保留在客户端的Cookies中。但是该方式仅适用于.Net应用服务器，兼容性不好，且容易遭受重放攻击[6]；耶鲁大学的CAS系统，使用SpringMVC和Webflow重量级的单点登录架构，成本过高。国内的有神州融信开发的UTrustSSO系统[7]和吉大正元的统一用户管理系统等。总体而言，当前的跨域单点登录系统大多基于单一身份认证方式，存在安全性不高、兼容性较差和开发成本高等问题。

本文针对现有跨域单点登录系统存在的问题，设计实现了一种安全高效的新型跨域单点登录系统，具有安全性高、兼容性好等特点。(1)针对单一身份认证方式问题，采用了多因子的身份认证方法，结合CA证书、管理员Ukey、PIN码，以及用户名和密码，对用户身份的开展多重认证，有效克服了单一认证方式安全隐患；(2)针对用户验证信息跨域传输不可靠的问题，采用SHA256加密算法与消息摘要的方式对票据进行加密传输，有效防止了重放攻击和字典攻击；(3)针对现有框架与应用兼容适配难度大的问题，提供基于Restful接口

基金项目：国家自然科学基金青年基金项目(No.61402514).

的插件形式客户端，用于第三方应用系统集成，较大降低了开发复杂性和成本，提高系统兼容性。

本文接下来的组织结构如下：第2节对单点登录的方法实现进行了详细描述，第3节进行了安全性分析；第4节进行性能评测，第5节总结全文和展望未来工作。

2 设计与实现(Design and implementation)

2.1 功能设计

单点登录系统按照功能模块划分，可以将其分为四类模块：客户端模块、身份认证模块、用户管理模块和单点登录模块。系统功能模块，如图1所示。

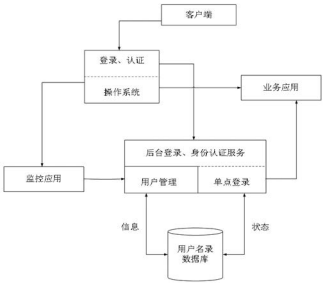

图1 单点登录系统功能模块图

Fig.1 Function module diagram of single sign-on system

(1)客户端模块

即Client，通过图形化显示交互技术，提供给用户进行相关功能的操作，并将用户的操作指令发送给服务端进行处理。主要分为两个部分：第一部分是硬件实体，由“Ukey”及支撑其安全可靠运行的“Ukey驱动程序”和整合于其中的“在线监测”程序所组成，用来获取用户Ukey证书，以及用户输入的PIN码等信息；第二部分是应用实体，由基于B/S构架的“浏览器”、Ukey和在线监测程序进行交互的“用户认证插件”，以及“单点登录插件”所组成。

(2)身份认证模块

其主要功能是验证访问用户的身份合法性，采用多因子的认证方法，对CA证书、管理员Ukey、PIN码，以及用户名和密码开展多重认证，并以最终返回的DN值作为用户身份有效性的唯一标识。身份认证模块的主要内容包括：对合法持有身份认证Ukey的用户在当前系统内进行身份认证Ukey注册；对使用应用系统用户的身份合法性进行初步认证；根据身份认证结果返回身份认证相关信息(用户唯一标示信息，即，DN值)。

(3)单点登录模块

其主要功能是免除多应用系统内需要进行反复登录的繁琐过程，实现在任一应用登录，多个应用间游弋。根据用户在用户统一管理模块中的注册信息，以及用户与应用之间的授权关系，完成用户在多个应用间的快速切换任务，省去了用户每访问一个应用都需要进行重新登录的繁琐过程。单点登录模块的主要内容包括：实现系统内各个应用间的单点登录；根据用户所授权应用的不同，实现在授权应用间的一次登录随处游弋功能；实现在线检测机制，用户因故离线后，自动切断应用服务、注销当前用户的应用登录状态，保证数据安全不外泄；实现超时自动登出机制，当用户在客户端的一段时间内(1800秒)持续无操作后，自动退出单点登录。

(4)用户统一管理模块

用户统一管理后台基于B/S构架开发，主要承担系统内所有用户的管理任务，同时还提供所有应用的授权管理工作，并与单点登录服务和身份认证服务合力构成整个用户统一管理模块。用户统一管理模块的主要内容包括：为普通用户提供应用统一入口门户；系统用户新增、修改、删除、查询等管理工作；实现用户注册与认证一体化；记录平台内用户的操作历史信息，如新增、删除、变更、注销等；针对用户不同需求，实现用户与应用的授权绑定操作；实现用户统一管理平台与应用之间的用户名录同步功能。

2.2 流程设计

单点登录系统实现了用户一次验证随处游弋的功能，其具体流程设计如图2所示。

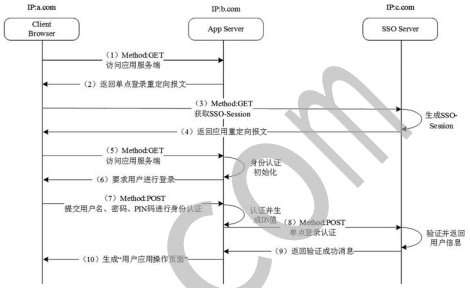

图2 单点登录系统流程图

Fig.2 Flow chart of Single sign-on system

(1)用户通过客户端浏览器访问应用服务端。

(2)应用服务端收到访问请求后向客户端返回单点登录重定向报文。

(3)客户端根据返回的状态和跳转路径，访问单点登录服务端，获取SSO-Session。

(4)单点登录服务端将盐值、应用唯一标识码和自定义字符合并，再通过SHA256加密算法哈希后生成SSO-Session，然后将URL携带的参数传给Http报文，并在Cookie域中设置SSO-Session用于标定当前需要单点登录的用户，最后向客户端返回应用重定向报文。

(5)客户端根据返回的Http数据报文中的URL继续访问应用服务端。

(6)应用服务端进行身份认证初始化后生成“用户登录页面”要求用户进行登录。

(7)用户填写用户名、密码、PIN码后提交给应用服务端。

(8)应用服务端使用PIN码获取用户Ukey中的CA证书，当验证错误出现三次时Ukey将会被锁定，若获取成功则将证书传给身份认证服务端进行验证得到DN值(用户的标识信息)，应用服务端将DN值，以及用户名、密码发送给单点登录服务端进行单点登录验证。

(9)单点登录服务端将用户名、密码和DN值进行验证匹配，若验证成功则返回验证成功消息给应用服务端，同时查询该用户已经授权的所有应用信息，并配合客户端的SSO-Session和应用ID建档保存，以备用户切换应用时快速查询并使用。

(10)应用服务端生成“用户应用操作页面”返回给客户端。

在“用户应用操作页面”中，用户通过点击应用图标即可跳转至应用服务端，由于浏览器的Cookie同源策略，应用服务端将之前生成的SSO-Session发送给单点登录服务端进行验证，验证成功后即可访问而不需要再次登录，此时就完成了单点登录一次验证随处游弋功能。

2.3 数据库配置

由于单点登录服务提供所有应用系统的用户信息统一验

证与登录入口，需要存储大量的用户信息和应用信息，本文采用Mysql数据库对其进行统一管理和存储。该数据库主要包含以下三个数据表：用户信息表、应用信息表和应用—用户关系映射表。

(1)用户信息表，用以存储所有用户信息，主要包含用户名、用户ID、密码和用户DN值等表项信息。其中用户名表示用户的唯一自定义名称，通过该值来完成用户信息的检索；用户ID则完成与该用户已授权应用的映射查找；密码表项为经过杂凑算法加密后的密码值；用户DN值存储身份认证返回的用户DN值。

(2)应用信息表，用以存储所有应用信息，主要包含应用名称、应用ID、应用URL地址和应用唯一标识码等表项信息。应用ID为该表检索字段，用以检索当前应用的所有信息。

(3)应用—用户关系映射表，用以存储应用ID与用户ID的映射关系，主要包含了应用ID、用户ID和映射关系ID等表项信息。映射关系ID表示当前映射条目的编号。用户ID与应用ID为多对多的映射关系，一个用户可对应多个应用，而多个应用亦可对应多个用户。

在用户首次成功登录后，根据用户名在用户信息表中查找对应的用户ID，而后在应用—用户关系映射表中查找该用户ID所有对应的应用ID，最后根据应用ID在应用信息表中获取该应用的所有信息，并显示在“用户应用操作页面”上。当用户需要访问某个授权应用时，只需点击应用图标，通过应用URL地址，即可进入应用。

2.4 界面实现

(1)用户登录界面

用户通过访问用户统一管理平台，进入用户登录界面，此界面要求用户输入用户名、密码和PIN码进行登录身份验证，如图3所示。

图3 用户登录界面

Fig.3 User login interface

(2)用户应用操作界面

用户登录成功后进入用户应用操作界面，如图4所示。此界面显示用户已授权可以使用的所有应用，当用户点击某一应用图标时，即可访问相应的应用。

图4 用户应用操作界面

Fig.4 User application interface

3 安全性分析(Security analysis)

安全性是跨域单点登录系统的核心指标，本文从机密性、完整性和可用性三个方面考虑系统的安全问题。

(1)机密性

机密性是指保护用户信息不被泄露。传统方法大多采用单一认证方式，容易遭受窃听和攻击。本文通过用户从可信任证书颁发机构相关部门获得“CA证书”和管理员Ukey，保证了证书的唯一性和机密性，再通过PIN码、用户名和密码多重认证，使用户身份更具安全性。

(2)完整性

完整性是指消息传输时不被非法的用户进行增删改查。传统方法大多采用对称密钥和非对称密钥来加密，存在密钥泄露造成用户信息被篡改的可能。本文采用SHA256加密算法与消息摘要的方式，使用盐值、应用唯一标识码和自定义字符合并，再使用SHA256加密算法哈希后生成票据，对票据进行了一次性临时加密传输，保证消息在传输过程中不被篡改。

(3)可用性

可用性是指用户一经授权则可以访问所需要的全部信息。本文通过对授权用户设置唯一的SSO-Session，使用接收到的用户名检索对应的用户注册信息，再根据该用户的注册信息中密码表项和用户DN值表项与接收到的密码和DN值进行比对，比对成功后根据用户ID检索该用户已经授权可以使用的所有应用信息，并在单点登录服务端建档保存，最后通过URL重定向携带SSO-Session，实现了应用跨域访问，从而保证了数据的可用性。

4 性能评测(Performance evaluation)

单点登录系统性能指标主要包括吞吐量和点击率等，在本节中，我们与基于Kerberos技术的单点登录系统[8]进行比较，因为两者均是采用单点登录第三方独立认证的方式。首先用模拟的方式对我们的单点登录原型系统进行测试并得到相应的测试结果，而后将测试结果与基于Kerberos技术的测试结果进行比较分析，最后得出结论。

4.1 测试环境及方法

本次测试环境构建，如采用B/S构架，客户端采用Windows 7 64位操作系统、Firefox浏览器和UkeyScriptablePlugin浏览器插件，服务端采用CentOS 7.0操作系统、Apache 2.0 Handler Web服务器和Mysqlnd 5.0.12-dev数据库。

本文采用Mercury LoadRunner[9]作为模拟测试工具，以系统负载数、每秒连接数、平均吞吐量和每秒点击数作为性能测试指标。LoadRunner的主要参数设置为：并发用户数量100和200，用户登录时间每秒两个，登录时长五分钟。

4.2 测试结果及分析

图5和图6分别代表100并发用户和200并发用户负载数，其中紫色代表运行状态，黄色代表完成状态，红色代表错误状态。从图中可知，当并发用户数达到100，用户全部登录成功，当并发用户数达到200，用户仍全部登录成功，且系统能支持5分钟内100并发用户或200并发用户同时登录，系统性能高，运行状态良好。

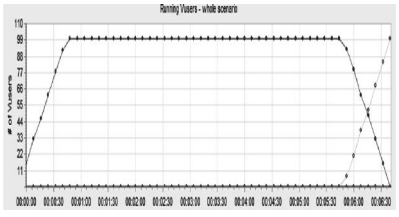

图5 100并发用户负载数

Fig.5 100 concurrent user Running Vusers

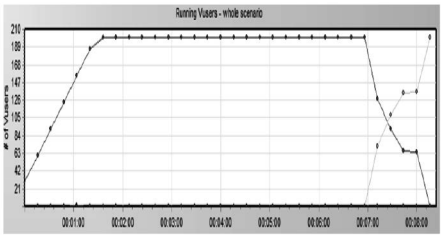

图6 200并发用户负载数

Fig.6 200 concurrent user Running Vusers

图7和图8分别是100并发用户和200并发用户的每秒连接数，每秒连接数是指在运行过程中每秒建立的TCP/IP连接数，用以评估服务器的处理能力。其中绿色代表建立连接数，黑色代表关闭连接数。由图可以看出不同并发用户数时，系统能正常响应用户请求，当并发用户为200时，波动比较大，这是因为并发用户数量小时，系统处理比较稳定。

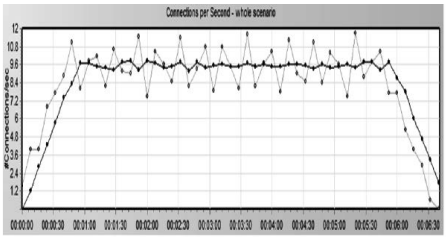

图7 100并发用户每秒连接数

Fig.7 100 concurrent user connections per second

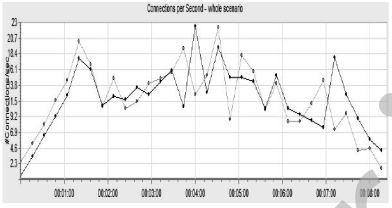

图8 200并发用户每秒连接数

Fig.8 200 concurrent user connections per second

在图9和图10中，“方法一”表示本文提出的方法，“方法二”表示基于Kerberos技术的方法。其中，每秒点击数是指运行过程中虚拟用户每秒向Web服务器提交的HTTP请求次数，通过它可以评估虚拟用户产生的负载量，判断系统是否稳定；吞吐量是指运行过程中服务器每秒处理的数据量，用以评估服务器在流量方面的处理能力。测试结果表明，相比于“方法二”，本文所采用的方法在系统平均吞吐量和每秒点击数两项指标上分别提高了7.3%和8.7%以上。我们认为，主要是Kerberos繁琐的认证机制所致，本文采用基于Restful接口插件形式客户端，达到平滑承接应用系统的效果，不但降低了开发复杂性，且提高了系统兼容性。

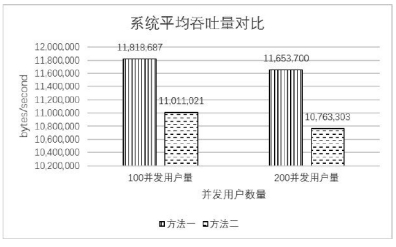

图9 系统平均吞吐量对比图

Fig.9 Comparison chart of system average throughput

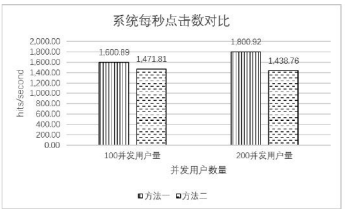

图10 系统每秒点击数对比图

Fig.10 Comparison chart of system hits per second

5 结论(Conclusion)

本文分析了现有跨域单点登录身份认证机制存在的问题，以及跨域单点登录的传输问题，提出了一种基于多因子的跨域单点登录的方法，实现了该跨域单点登录原型系统。该系统使用Restful接口形式，将单点登录客户端做成一个独立的第三方插件，实践表明，本文提出的跨域单点登录系统安全高效。该系统适用于各行业信息化建设，具有较广的应用前景。对于系统其他功能比如用户日志管理、用户名录同步和用户组织架构等功能的完善是本文的下一步工作。

参考文献(References)

[1] 隋荣恒,袁远,黎铁军,等.基于密码令牌的单点登录系统[C].NCCET 2017:Proceedings of the 21th National Conference on Computer Engineering and Technology and the 7th Microprocessor Forum,2017:46-49.

[2] Olivier Pereira,Florentin Rochet,Cyrille Wiedling. Formal Analysis of the FIDO 1.x Protocol[C].FPS 2017:Foundations and Practice of Security,2017:68-82.

[3] Abdalla M,Bresson E,Chevassut O,et al.Provably secure password-based authentication in TLS[C].ACM Symposium on Information Computer and Communications Security ASIACCS'06,2006:35-45.

[4] Sean Simpson,Thomas GroB.A Survey of Security Analysis in Federated Identity Management[C].Privacy and Identity 2016:Privacy and Identity Management,2016:231-247.

[5] Zhen Zhong Wang,Yao Wang.Research and Design of Campus Network Unified Identity Authentication System Based on Kerberos[J].Advanced Materials Research,2012(546):1086-1089.

[6] C.L.LIN,H.M.SUN,and T.HWANG. Attacks and Solutions on Strong-Password Authentication[J].IEICE Transactions on Communications,2001,84(9):2622-2627.

[7] 贾淑红,刘万军.基于Kerberos协议的单点登录系统设计[J].计算机应用,2007(S1):10-12.

[8] 李立.统一身份认证系统的设计与实现[D].电子科技大学,2012:65-66.

[9] Abhijit Bora,Subhash Medhi,Tulshi Bezboruah.Investigations on Failure and Reliability Aspects of Service Oriented Computing Based on Different Deployment Techniques[J]. Advanced Computational and Communication Paradigms,2018(475):535-543.

作者简介：

吴君楠(1991-)，女，硕士生.研究领域：计算机应用.

黎铁军(1977-)，男，博士，研究员.研究领域：计算机体系结构.

袁　远(1980-)，男，博士，副研究员.研究领域：计算机体系结构.

隋荣恒(1989-)，男，本科，工程师.研究领域：计算机应用.