[文章编号] 1004-325X(2006)01-0098-02

基于WEB SERVICE的统一认证系统设计与实现

Design and Realization of Single Sign-On Based on Web Service of Digital Library

张 军 (浙江大学计算机学院 浙江 杭州 310027)
林俊伟 (厦门大学图书馆 福建 厦门 361005)

[摘 要] 本文阐述建立统一认证的模型,实现读者一次认证后即可使用数字图书馆大部分资源及服务。
[关键词] 统一认证 网页服务 服务整合
[中图分类号] TP393.08;G250.76 [文献标识码] B
[Abstract] A Single Sign-On (SSO) solution based on web service was built and implemented in this paper. The SSO permits the readers to use the greater part resources and service of digital library as the readers passes the authentication.
[Key words] Single Sign-On; Web service; Integrated service

数字图书馆经过多年的研究和发展,形成了3种主流模式,即特种馆藏型模式、服务主导型模式和商用文献型模式[1]。高校图书馆一般都拥有大量的商购数据(网上联机出版物、全文数据库等)、自建数据(博、硕士论文及教学参考书等),这两类数字资源与网上免费资源一起,构成服务主导型数字图书馆的基础。目前厦门大学图书馆拥有的万方数据、CNKI及多媒体等本地数字资源量已超过15TB,拥有50多个网上联机数据库的使用权,还开放虚拟参考咨询和校外教职工访问入口,已经具备提供高质量服务的基础。但是,这些资源或有IP限制,或要求用户以用户名、密码登录后才能使用,读者常常需要分别进行登录后才能使用。因此急需一个统一的信息访问平台,即图书馆知识门户。门户系统的最大优势就是统一认证(Single Sign-On,SSO或Single Sign In, SSI,也称单点登录)和个性化服务。基于当前本馆实际情况,厦门大学图书馆急需实现统一认证,以提高服务能力和资源利用率。

1 统一认证技术

随着计算机技术、网络技术的提高,统一认证技术已有广泛的应用,如微软公司所提供的.NET Passport认证服务就实现了任何支持.NET Passport认证网站之间的统一认证,即用户只要一次登录就可以使用各网站的服务。统一认证基本模式如图1所示,当有用户访问网站上的某一网页时,网页检查用户认证信息,如果用户已经成功认证,则通过认证信息获取用户配置并允许用户使用网站内容;如果没有发现成功认证标识,网页将重新定向到认证服务器,显示用户认证页面供用户输入认证信息。

统一认证给用户、管理员带来极大便利的同时,也产生了一定的潜在威胁。主要体现在认证过程包括数据在网络上传递的过程,入侵者有可能通过监听而伪造登录信息;同时,网络暂时性的中断将导致认证失败;此外,统一认证系统一

领域,当然也包括图书情报领域,必然全方位与世界各国和地区进行交流与合作,这就要求我们在加强科技创新的同时,要加强科技信息在国际间的传播。因此,文摘的标准化也就越来越重要了。文摘标准化不仅是自动化研究的基础,能为期刊文献的数据加工、二次检索以及使读者快速获取文献信息提供极大的便利,而且能加速国际间的传播,提高我国图书情报界的地位。文摘编写规则(GB6447-86)已颁布多年,但我们许多作者对其并不了解,更没有按照其来规范摘要的写作。因此,有必要加强文摘标准化的宣传,增强作者文摘意识,提高文摘编写质量。

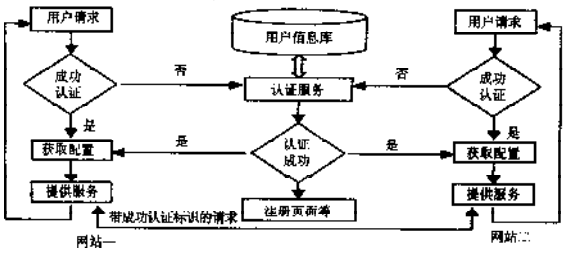
5.2 探索适合本专业论文的文摘规律 目前,对文摘的标准化,尽管出版了国家标准GB6447-86,但仍存在着不同的认识和看法,如社会科学与自然科学摘要的类型和要素应有哪些不同?期刊论文摘要篇幅的长短究竟以多少字为宜?摘要的主语与人称等问题。有必要对此展开充分的讨论,探索其规律,寻找最适合本专业期刊论文的文摘方法,进一步推进期刊工作的标准化、规范化。

5.3 编辑人员要严格要求 编辑人员在编辑加工中,要增强信息意识,对不符合要求的论文摘要要求作者重写,要有敏锐的洞察力获取一次文献中有价值的信息,并在摘要中充分表达出来,提倡写报道性摘要。作为图书情报核心期刊的编辑,更应在这方面做出表率。

参考文献:
1 国家标准局. GB6447-86文摘编写规则. 北京:中国标准出版社,1986
2 杜也力. 图书情报专业核心期刊论文文摘分析. 图书馆学、信息科学、资料工作,2002(6)
3 吕联钟. 图书馆学期刊文前摘要的编写方法. 鹭江职业大学学报,2001(1)

[作者简介]
吴漂生 男,1966年出生,馆员,毕业于南昌大学信息管理系,宜春学报图书馆期刊部主任,主要从事于信息检索研究,已发论文15篇。
[收稿日期:2005-07-26]

图1　SSO模式图



般共享用户信息库，也就是说，所有用户的信息全部集中存放于同一个数据库中。对于高校而言，将所有学校的用户数据全部存放在同一信息库内在实际应用中有一定困难。因此，实现高校间的统一认证需要对此技术进行一定的改造。

2　厦门大学图书馆SSO模型

根据本校实际情况及数字图书馆信息"共建、共知、共享"的原则，　厦门大学图书馆使用WEB SERVICE技术建立了安全性高、扩展性强的统一认证系统。整个系统由用户信息库、认证服务器、客户认证模块构成。具有如下特点：

(1) 基于简单认证机制中的口令认证机制，系统通过用户输入的用户名确认用户所属院校及身份，如00000000@xmu表明此用户是厦门大学用户，借阅证号为00000000，并确认对应的认证服务器。

(2) 采用一次性认证的机制，每次认证都有一个有效期。

(3) 实现认证在各应用及各院校之间的漫游。

(4) 认证过程无明文密码的传输过程，关键步骤采用安全传输。

(5) 有完善的认证接口，多种应用系统通过接口使用本认证系统进行用户身份的确认。

(6) 对于商用数据库，如果要求以用户名密码登录后才能使用的，则认证系统保留这些用户名密码，当用户使用这些资源的时候，系统自动登录供用户使用。

本系统实现了3种不同形式的认证，基本满足统一认证的功能要求。

模式一：本校用户访问本校数字化应用，应用系统接到请求后向本校的统一认证服务器发出认证请求，通过认证后开始为用户提供服务。

模式二：外校学生访问本校数字化应用，应用系统接到请求后识别出此用户所属的认证服务器(远程)，然后向该服务器发送认证请求，通过认证后开始为用户提供(受限)服务。

模式三：外校学生成功登录其本地应用后，通过应用上的交换链接直接访问本校应用，本校应用检测到登录信息后向外校认证服务器发出确认请求，确认登录信息有效后开始为用户提供(受限)服务。

3　关键技术

实现统一认证技术最核心的一点是用户成功登录后获取一个包含用户信息的令牌环(Token)在各个应用之间的传递。这一过程涉及安全传输、加密等多项技术。

就网络应用而言，不安全的环节主要包括提交用户信息、各应用系统与认证服务器之间的数据传输。SSL安全信道是当前较好的安全通信方式，但对于过大的数据量，SSL传输的性能会有较大的下降，所以，只有在身份验证和重要数据传输的时候才选用SSL。

认证流程采用请求—应答机制，客户(各应用系统)首先向认证服务器发一个认证预请求，以获得一个随机数，并将此随机数用在随后的认证数据包中。将用户密码经过单向加密成为客户与认证服务器之间的共享密码(Shared Secret，SS)。若认证成功，服务器的响应包是利用此SS对整个数据做校验，用户收到响应以后，也要做同样的校验，比较校验结果是否一致。若一致，说明结果是由真正的服务器所发，并接受此结果，否则亦当认证失败处理。采用此认证算法，系统对几种常见攻击手段都具有相当的防范能力：(1)窃听：认证协议中，对传输的用户名、口令等信息进行加密，双方用于验证的密钥从不在网络上传输；(2)篡改：在认证协议中客户端和服务器端之间进行的每一次数据交换，都要对数据包做带密钥的校验，校验不正确的数据包无条件丢弃；(3)重放：每一次认证开始由服务器产生一个随机数，在随后的加密和校验过程中该随机数作为其中一个变元，故每次认证请求都不同，攻击者即使窃听到一个成功的认证请求包，在下次使用时却失效了。

由于实现了跨校区的认证，系统必须具备识别用户所属院校的能力。系统将维护一个对应表，内容即为院校简称与所用认证服务器URI。假设厦门大学的简称为xmu，对应的认证服务器为http://210.34.4.2:8080/webservice/，则表内保存此记录。用户采用"借书证号@xmu"作为其用户名进行登录，从而实现对用户所属院校的判别。各院校之间对应表每日同步。

同时，系统要求稳定的网络环境，一旦应用服务器与认证服务器特别是远程的认证服务器之间发生网络故障，系统无法完成用户认证工作。因此，系统设计为因技术原因导致无法认证则对本校读者提供非个性化但无限制的服务，对外校读者提供有限服务，如暂时不提供全文内容等。

厦门大学图书馆将统一认证技术引入数字化项目中，已经成功实现"我的图书馆"、"校外教职工访问"、"个人定制"等项目与服务之间的统一认证，用户真正做到"一次登录，各处使用"，极大地提高了服务能力，方便了用户。同时，厦门大学也正计划与福建省各高校进行合作，争取在省内各高校之间通过统一认证技术共同提高服务能力和资源利用率。

参考文献：

1 郑巧英，杨宗英. 服务主导型数字图书馆模式研究. 津图学刊，2003(1)

2 Chris Dunne. build and implement a single sign-on solution. http://www-106.ibm.com/developerworks/web/library/wa-singlesign/，2005.4.18

3 茅维华，谢金宝. Web应用单一登录的类Kerberos实现. 计算机应用与软件，2004(2)

4 夏思洵，董传良. 基于证书的信息门户单一登录. 计算机应用与软件，2004(4)

5 王新房，邢　毅，刘萍萍. Liberty的单一登录多方认证机制及其安全性分析. 微电子学与计算机，2004(10)

[作者简介]

张　军　男，1969年生，副研究馆员，现任浙江大学图书馆采访中心主任，先后在专业学术期刊发表论文数十篇。

林俊伟　男，1978年生，2001年毕业于株洲工学院计算机系，现工作于厦门大学图书馆信息技术部，工程师。

[收稿日期：2005-07-19]