●李　宇（中国科学院 a. 研究生院；b. 文献情报中心，北京　100080）

多认证域认证与授权技术的发展

[关键词] 单点登陆；认证授权；信任协商

[摘　要] 认证和授权技术的发展已经进入了联合身份认证的时代。文章介绍了认证与授权技术的概念及其发展，提出在数字图书馆的网络环境下，认证授权比较流行的做法是由资源方创建一个访问控制列表。访问控制的方法包括源IP地址过滤、代理和基于数字凭证的方式。作者较为详细地介绍了单点登陆相关技术系统和跨认证域的单点登陆系统。提出在开放环境下认证和授权的理想方式是通过信任协商机制来完成，并阐述了几种典型的信任协商系统及其实现的要求。

[中图分类号] TP3
[文献标志码] A
[文章编号] 1005－8214(2007)02－0101－03

1　认证授权简介

认证与授权虽然含义并不相同，但由于它们的紧密关系，因此常常被用到一起。网络资源的访问控制及使用常常需要同时使用认证和授权服务。但无论逻辑上或者物理上，认证和授权都可以是分开的。

1．1　认证的定义

认证是网络用户建立对某个标识(例如用户名)拥有使用权的过程。有许多技术来认证用户，例如密码、生物特征识别技术、智能卡、数字证书等。而这个认证的标识和用户的真实姓名没有联系，用户可以选择使用多个标识。对于一个特定的组织而言，用户被授权使用一个标识意味着组织已经接受该用户对于该标识的权利。在单认证域的情况下，一个用户通常只有一个标识，但在多认证域的情况下，一个用户可能拥有很多标识，这些标识在默认的语义下都会具有特定的身份含义。用户可能需要决定向资源方呈现特定的标识以表现特定的身份。一个标识通常具有与之相关的属性，例如科研人员或者学生。这些属性和相应的主键在一般的认证系统中被放到数据库中，以方便检索，同时可以不时进行更改。认证的主要目的在于证明用户对于一个特定的标识具有拥有权。对于人的认证通常分为三类：生物特征，例如指纹、视网膜、DNA序列、语音、静脉血管分布等等独一无二的生物特征；用户拥有的事物，例如身份证、安全令牌、手机等等；用户所知道的事物，例如密码、个人识别号（PIN）等等。

1．2　授权的定义

授权，是决定一个标识及其相关的属性是否被允许执行一个特定的动作的过程。需要注意的是，允许执行动作并不代表动作一定能够被执行。例如很多数据库对于同一个机构能够并发访问的用户数量有限制，因此，即使用户已经被授权可以访问资源，但由于资源方的策略有可能导致用户访问资源失败。

在图书馆间开展对网络信息资源的馆际互借就需要严格而明确的用户授权。多个图书馆可以考虑通过中心化的或者分布式的共享认证授权服务对用户进行认证授权，精确地定位用户的需求，从而能够进一步提高个性化服务的服务质量。

2　访问控制的方法

认证授权往往被合而为一成为访问控制，在数字图书馆的网络环境下，认证授权比较流行的做法是由资源方创建一个访问控制列表，根据访问者可以提供的认证手段确认访问者并授权其访问特定资源。

1．1　源IP地址过滤

源IP地址过滤是一种相对简单而且有效的办法。由于进行资源购买的单位多为大学院校、科研院所等具有独立IP地址段并自行运营维护自己的网络，因此几乎所有的资源提供方都支持这种访问控制方式。IP地址欺骗相对来说难度比较高，因为网络系统大部分使用BGP协议进行路由协商，要进行IP地址欺骗就必须在路由层进行，不仅难度较大，而且也极容易被人发现。

1．2　代理

为了方便在校园外的教师或者出差在外的科研人员方便使用已经购买的资源，图书馆通常会设置代理服务器并给这些教师或者科研人员提供代理服务，使得资源方看来只是某个IP段内被允许的IP地址在进行正常的访问。通常图书馆设置代理服务器都会通知资源方该IP地址用于代理服务，以免由于流量过大而导致的该地址甚至是C类网段被资源方封锁，同时对使用代理的人员的访问过程进行记录，以防止资源的滥用和非法下载。

1．3　基于数字凭证的方式

为了加强安全和认证的可信度，像银行系统通常都使用基于公钥基础架构的X.509的数字证书来对客户方的身份进行验证。被广泛采用的公钥基础架构从安全角度而言是比较安全的，但是其实现及使用比常规的账号密码认证方式或者是代理服务器设置方式要复杂的多，不容易掌握，同时安全被限定在证书文件本身的安全上，如果计算机病毒或者木马程序窃取了用户的证书，同时又盗取了用户的账号密码，那就可以完全地伪装成用户进行破坏活动或者滥用资源。

中科院数字图书馆的随意通[1]服务，则使用了存储

在硬件 USB－KEY 的 X.509 证书，同时要求用户记住其账号和密码。该系统使用了与银行系统等同的强认证手段，从技术、管理等各个层次保证资源不被滥用，同时为科研人员提供了随时随地研究所有权限访问的全部资源的便利。

在数字图书馆领域谈到的认证与授权技术基本上等同于身份管理。[2] 身份管理指的是对一个或多个身份的整个生命周期的管理，从创建到销毁以及中间发生的事情，例如管理许可、特权和修改等。在用户获得相应身份的承认之后，一般会根据访问控制列表为用户进行授权，以允许其能够进行的操作。在数字世界中，特定应用程序、网络、系统等等的用户仅仅是一个通过身份验证后获得惟一身份的用户标识。随着系统和网络的数量以及复杂性的不断增长，管理数字身份已经成为一项重大的挑战。

3　单点登陆相关技术系统

在单点登陆的情况下，用户的身份由统一的单点登陆服务器认证，用户只需要登陆一次，就可以访问认证域中的所有网络资源和服务。单点登陆的优势在于：集中创建、销毁网络账户；统一分配、回收网络访问权限；自动完成详尽的日志和审核；有利于创建基于角色和基于策略的安全控制。

CAS（Central Authentication Service）[3] 中心认证服务。CAS 最早由耶鲁大学开发并基于 BSD 版权协议分发，其设计思想是使用一个可信的中心服务器对用户的单点登陆认证。CAS 的协议包含一个客户端浏览器、请求认证的应用服务和 CAS 服务器，当客户端访问受保护的应用时，会被应用服务自动指向 CAS 服务器，CAS 服务器使用类似 Active Directory 的目录服务机制来验证用户的 ID 和密码。如果 ID 和密码有效，则 CAS 服务器将一个称为票据（ticket）的随机数和用户 ID 重定向到应用服务，应用服务随后使用 HTTPS 链接 CAS，并提供获得的票据和用户 ID，CAS 随后告诉应用服务该票据是否有效。

JOSSO（Java Open Single Sign－On）项目。[4] 基于 J2EE 的支持单点登陆基础架构的开源软件，允许通过 SOAP 集成非 Java 的应用程序的认证，使用 Web 服务支持分布式的架构，支持不同的认证机制（例如基于账号密码的认证和基于 X.509 证书的认证）。

Pubcookie [5] Web 认证。Pubcookie 是一个支持机构内 Web 认证的开源软件，包含一个独立的登陆服务器和通用 Web 服务器（例如 Apache [6] 和 IIS [7]）的模块。这些组件能够把现有的认证服务（例如 Kerberos、LDAP 或者 NIS）变为支持机构内 Web 站点单点登陆的认证服务。

4　跨认证域的单点登陆系统

Web 环境下认证与授权技术目前发展的比较成熟的技术是单点登陆 SSO（Single Sign On），单点登陆使得用户在登陆了一个域之后，再使用其它域的资源时无需再次进行认证。

Shibboleth [8] 系统是一个典型的跨认证域的单点登陆系统。Shibboleth 是由 Internet2/MACE（Middleware Architecture Committee for Education）组织开发的基于 SAML 规范的支持联合身份管理的信任引擎中间件，并采用基于属性的授权框架对用户的请求进行授权。

Shibboleth 使用一套证书分发系统来关联服务提供者和标识提供者。这种基础架构保证了成员之间彼此是“认识”的，同时从技术层面保证了在通讯和加密签名时对方确实是自己想要通讯的那个实体。由标识提供者自行管理用户的身份和属性，以及揭示这些属性的要求，服务提供者通过对可选的 WAYF（“where are you from”）服务的查询来找到目标站点并和目标站点进行通讯从而获得用户确实属于该目标站点并取得其属性。

从架构及实现来看，Shibboleth 是一个基于开放标准的联合的身份管理系统。该架构的各方都自行指定各自的策略，在获取对方的应答之后，对获得的信息的判断全部取决于自己内部的策略评估机制是否允许揭示相关的资源或者服务，从而实现隐私保护的要求。整个架构将各参与方的策略的执行作为参与方的内部实现的黑箱，消息只是流经这些黑箱并由参与方内部进行判定。这些都没有考虑服务的多样性、背景以及当时的情景，在取得服务请求者的身份及相应的属性之后，是否提供服务完全由本地的策略进行决定，不再考虑外部环境因素可能造成的影响。

5　信任协商系统

开放环境下的认证和授权的理想方式，是通过信任协商机制来完成。信任协商是对传统环境下的认证授权方式的扩展，通过信任体系继承或者获取信任。信任协商不仅仅支持数字身份管理，也包含了单点登陆所需要的功能同时具有隐私保护的特点。信任协商通常包括了需要反复揭示的不同的数字证书，这些证书被用来逐步证明持有者的属性以建立相互的信任。而信任协商的主要工作，就是如何建立形式化的安全策略和证书，以决定一套证书集合是否满足了相关策略的要求，协商双方通过互相揭示数字证书和策略，逐步建立信任关系。

5．1　典型的信任协商系统

（1）以 Trust－Serv [9] 为代表的基于模型驱动的 Web 服务信任协商。介绍了一个基于 Web 服务的模型驱动的协商架构，并描述如何在数字图书馆中有效处理信任协商。模型选择了基于状态机的信任协商，并使用安全抽象进行了扩展。使用基于状态机的模型对高层次的规范进行表示，然后将它们翻译成适合于自动协商的格式。文章提供的框架同时支持协商策略的生命周期管理。同时，提供了一套策略改变的操作方法，在不中断当前的协商过程的前提下，对协商策略进行动态的改进。文章提供的方法以容器为中心的机制来实现，无论对于数字图书馆还是数字图书馆 Web 服务的开发者而言都是透明的，在提供可扩展的部署情况下简化了数字图书馆的开发和管理。Trust－Serv 对传统的基于身份管理的认证、授权系统做出了较大的改进，但抽象来看，仍然是一个身份管理的模型系统，其最大的特色是对策略的生命周期进行管理。

（2）基于策略的 PeerTrust [10] 语义网节点间的自动协商。使用语义网的基本规则层来建立简单而具有表达性的支持策略语言协商的分布式的可相互认证的节点，同时支持对访问控制策略的保护和协商战略。

（3）联合使用规则、本体和流程描述的 SweetDeal [11] 基于规则标记语言的商务合同表示方法，支持其创建、评估、协商及达成。SweetDeal 根据 MIT 的流程手册 [12] 使用本体和 RuleML [13] 来联合表达特定的商业应用领域，是使用语义 Web 服务的典型案例。

（4）基于 X－TNL 语言的 Trust－X [14] 信任协商系统。针对点对点环境设计的信任协商系统，通过自行设计的基于 XML 的语言 X－TNL，使用信任票据和协商树来进行运行时的协商检测。Trust－X 使用 XML 的命名空间来保证词汇的一致性。使用命名空间的证书类型系统使软件正确解释不同的证书纲要，以保证在没有可共享的通用本体的情况下依然可以运行。Trust－X 的证书分为证言或声明(证言指明拥有者的个人属性，声明则无须证明，只是提供更多的信息以支持决策)。X－TNL 的一个特点是使用了被称为“信任票据”的特殊证书。“信任票据”在成功完成协商后发布，以加速对同一资源的后继协商的速度。此外，X－TNL 根据策略预备的思想提供了灵活的策略保护的语义和机制。Trust－X 支持三种协商模式：一种是基于信任票据；一种是基于“协商树”的抽象数据结构，在运行时检查一个证书序列的揭示是否能成功完成协商；第三种模式是利用类似协商的特点，基于服务提供者对许多相似协商的处理方式，并提供了协商处理架构。

另外，TrustBuilder [15] 系统提供了协商战略的宽泛的类，并提供了一个和战略、语言无关的协商协议以保证在系统架构内定义的战略的互操作性。使用安全代理来管理协商，通过策略定义分层来支持敏感策略并使用动态策略保护隐私。

Unipro [16] 使用统一的纲要来模型化资源保护，体现了细粒度控制策略，并提供了更加灵活的授权要求的表达。

RT（Role－based trust management）[17] 基于角色的信任管理框架，强调分布环境下的安全问题。RT 提供了具有良好语义的策略语言，一个演绎引擎，并使用应用规范文档来保持策略术语的一致性。RT 定义了信任图协议以支持基于属性的访问控制 [18]（attribute－based access control (ABAC)）系统。RT 的优势在于包含了一个描述性的基于逻辑的语义基础，并且能够表达更多的证书类型以及更灵活的委托结构。

5．2　实现信任协商的要求

要实现信任协商，无论从语言角度，还是系统角度，都有一定的要求。

（1）语言要求。信任协商策略语言是依照句法结构要求和与之相关的语义编码成用于协商过程中交换的安全信息。良好的信任协商语言应该能够简化证书的规定，并能够通过灵活的揭示策略的规范来表达保护的要求，因此，他们应当支持：①良好定义的语义。简单、紧凑、正式的定义策略语言的语义，同时保证策略语言与实现无关。②单调性。要求当允许揭示特定资源的一套证书被找到后，更多的证书和策略的揭示应该在可能的情况下促使更多的资源被揭示。③证书联合证明。语言应当支持一套证书联合在一起证明某些属性。④认证。双方都可能包含多个被公钥声明和签名的证书所证明的身份，运行时证书的提交者必须证明其拥有与签名证书的公钥相对应的私钥。⑤属性值约束。证书能够与指定的证书类型元数据关联，以简化证书的管理。策略语言应该能够支持对特定类型证书的属性的值的正确性进行约束。⑥相互证书约束。策略可能比较并约束对方提供的不同证书的值。⑦敏感策略的保护。对敏感策略提供细粒度的保护，策略语言应支持对策略揭示的约束。⑧统一的形式和支持互操作的语法。XML 提供了语法上的互操作的可能性。[19]

（2）系统要求。协商系统通常被设计为包含多个模块的运行时系统，通常要求它们支持：①证书所有权。要求对方证明其拥有与签名证书的公钥相对应的私钥，同时保证通讯的安全。②证书验证。验证证书的完整性、有效期以及是否被撤销。③证书链发现。在需要更多的证书支持协商过程时，支持实时的自动发现和获取该证书。④隐私保护机制。仅向对方揭示成功协商所需要的最小的策略和证书集合。⑤支持可选的协商战略，提供多种选择战略尽可能保证协商成功。⑥快速协商战略。对于许多标准的场景其最终协商成功的证书和策略的揭示过程可以记录下来，双方在随后的协商过程中可以使用这些预计算的协商过程加快速度减少负荷。在理想情况下即使双方相互陌生，也可以自动选择和建议交换的策略和证书，加快协商成功的速度。

认证与授权技术的发展，已经进入了联合身份认证的时代，随着语义网技术的发展和进步，能够进行自由跨信任域进行认证授权的系统将为用户带来更方便、快捷和安全的互联网使用体验。

[参考文献]

[1] 中科院数字图书馆的随意通服务 [EB/OL]. [2006－03－19]. https://q.csdl.ac.cn.

[2] Solving the identity crisis [EB/OL]. [2006－03－19]. http://archive.infoworld.com/reports/36SRidentity.html.

[3] Central Authentication Service [EB/OL]. [2006－03－19]. http://tp.its.yale.edu/tiki/tiki－index.php?page＝CentralAuthenticationService.

[4] Java Open Single Sign-On Project [EB/OL]. [2006－03－19]. http://www.josso.org/.

[5] Pubcookie [EB/OL]. [2006－03－19]. http://www.pubcookie.org/.

[6] The Apache HTTP Server Project [EB/OL]. [2006－03－19]. http://httpd.apache.org/.

[7] Internet Information Services [EB/OL]. [2006－03－19]. http://www.microsoft.com/WindowsServer2003/iis/default.mspx.

[8] Shibboleth Project [EB/OL]. [2006－03－19]. http://shibboleth, internet2.edu.

[9] Trust-serv：model-driven lifecycle management of trust negotiation policies for web services [EB/OL]. [2006－03－19]. http://portal.acm.org/citation.cfm?id=988672.988680&coll=portal&dl=ACM & type=series&idx=SERIES968&part=series&WantType=Proceedings&title=www.

[10] W Nejdl, D Olmedilla, M Winslett. PeerTrust：Automated Trust Negotiation for Peers on the Semantic Web [C]// Workshop on Secure Data Management in a Connected World (SDM'04) Toronto, 2004. [EB/OL]. [2006－03－19]. http://www.learninglab.de/pdf/L3S_Project_peertrust.pdf.

[11] SweetDeal：representing agent contracts with exceptions using XML rules, ontologies, and process descriptions [EB/OL]. [2006－03－19]. http://www2003.org/cdrom/papers/refereed/p115/p115-grosof.htm.

（下转第 106 页）

Filtering），另一种是合作过滤（Collaborative Filtering）。综合两种方式的优点，面向用户的数字图书馆信息服务系统应采用基于混合模式的信息过滤(Hybrid Filtering)模型。它建立面向个人的用户模板和面向合作的公共模板，抽取信息特征作为可能的特征项，便于用户动态地修改模板；利用其它用户对文档的评价以及用户模板与文档的相似度来预测用户的接受程度。另外还考虑到推荐者的权威性和与用户兴趣的一致性。[9]

3．2．5　学科信息门户技术

学科信息门户是将特定学科领域的信息资源、工具与服务集成到一个整体服务系统中，为用户提供一个方便的信息检索和服务入口。面向用户的数字图书馆信息服务系统必须致力于学科门户的建设。具体有以下形式：①主题信息门户。以网络学科信息导航为主的，提供权威、可靠、规范和可持续的网络信息资源选择、描述和检索。②专业信息门户。以专业机构或图书情报服务系统为基础，根据专业机构性质或其信息服务要求，将各类资源（包括网络资源、数据库、文件系统、知识库、指南手册等）组合在统一门户下向用户提供服务。③跨学科信息门户。基于和支持多个学科信息门户之间的整合检索。④分布信息门户。基于信息门户体系，将多个分布门户整合一个集成门户体系，让用户通过信息门户体系方便地搜寻、调用和利用各种不同的信息资源和服务。⑤开放信息门户。不但支持基于学科信息门户的资源与服务集成，还进一步支持按照用户个性化需要定制信息门户，根据逻辑业务流程整合多个信息服务环节，支持多个信息门户之间的开放集成与定制。[10]

3．2．6　信息智能代理技术

智能代理技术是一种能够完成委托任务，模仿人的行为执行一定的任务，不需要或很少需要用户的干预和指导的智能计算机系统。面向用户的数字图书馆信息服务系统通过智能代理跟踪用户在信息空间中的活动，自动捕捉用户的兴趣爱好，主动搜索可能引起用户兴趣的信息并提供给用户。利用信息智能代理技术是实现面向用户的数字图书馆信息服务系统个性化信息服务的有效方法。[11] 其主要功能有：①个性化的信息管理代理库；②信息自动通知；③浏览导航；④智能搜索；⑤动态个性化页面。

[参考文献]

[1] 张晓林．分布式数字图书馆机制［J］．情报学报，2002（1）：63－70．

[2] Paepcke A，etc．Interoperability for Digital Libraries World Wide［J］．Communications of the ACM，1998，41（4）：33－43．

[3] 盛小平．国内外数字图书馆发展的比较研究［J］．中国图书馆学报，2001（6）：39－44．

[4] 耿骞．基于元数据的数字图书馆信息系统的研究［DB/OL］．北京师范大学硕士学位论文数据库，2001．

[5] 张晓林．数字图书馆机制的范式演变及其挑战［J］．中国图书馆学报，2001（6）：3－8，17．

[6] William Y．Arms，Christople Blanchi an Architecture for Information in Digital Libraries［J］．D－Lib Magazine，1997（2）．

[7] 郭海明，刘昆雄．数字图书馆信息服务系统构建探讨［J］．图书馆学、信息科学、资料工作，2004（5）：141－145．

[8] 赵四友．数字图书馆互操作性问题初探［J］．现代图书情报技术，2002（2）：8－10，24．

[9] 刘柏嵩．过滤研究［J］．现代图书情报技术，2003（6）：23－26．

[10] 张晓林．分布式学科信息门户中网络信息导航系统的规范建设［J］．大学图书馆学报，2002（5）：28－33，43．

[11] 庄鹏，等．代理模式实现数字图书馆个性化信息服务模型［J］．情报学报，2004（2）：25－30．

[作者简介] 郭海明（1973－），男，湖南茶陵县人，图书馆学硕士，馆员，发表学术论文20篇，参与国家级、省级课题3项，参编专业著作2部；邓灵斌（1972－），男，湖南祁东县人，武汉大学信息管理学院博士研究生，发表学术论文20余篇，参与国家级、省级课题多项。

[收稿日期] 2005－12－01　　[责任编辑] 肖　群

（上接第103页）

[12] MIT Process Handbood［EB/OL］．［2006－03－19］．http://ccs.mit.edu/ph/．

[13] RuleML［EB/OL］．［2006－03－19］．http://www.ruleml.org/．

[14] Elisa Bertino，Elena Ferrari，Anna Cinzia Squicciarini．Trust-X:A Peer-to-Peer Franework for Trust Establishment［J］．IEEE Tramsactions on Knowledge and Data Engineering，2004，16（7）：827－842．

[15] TrustBuilder Research Projects［EB/OL］．［2006－03－19］．http://isrl.cs.byu.edu/projects.html．

[16] T Tu，X Ma，M Winslett．PRUNES：An Efficient and Complete Strategy for Automated Trust Negotiation over the Internet［C］//Proc.7th ACM Conf．Computer and Communication Security．ACM Press，2000：210－219．

[17] Ninghui Li，John Mitchell，Will Winsborough．RT：A Role-based Trust－management Frameword［C］// Proceedings of The Third DARPA Information Survivability Conference and Exposition（DISCEX III）．April 2003．

[18] Winsborough W H，Jay Jacobs．Automated Rrust Negotiation Technology with Attribute－based Access Control［C］//DARPA Information Survivability Conference and Exposition．2003：60－62．

[19] Policy Language Requirements for Trust Negotiation［EB/OL］．［2006－03－19］．http://yoda.cs.byu.edu/pres/Policy%20Language%20Requirements%20for%20Trust%20Negotiation2.ppt．

[作者简介] 李宇（1977－），男，中国科学院文献情报中心博士研究生。

[收稿日期] 2006－04－04　　[责任编辑] 陈永平