虚拟信息资源体系的用户使用管理

张晓林

文摘：本文介绍了虚拟信息资源体系的用户使用管理的基本概念、基本功能、基本技术机制和典型范例。

关键词：虚拟信息资源体系，资源共享体系，用户使用管理，身份认证，使用授权

Access Management of Virtual Information Resources Systems

Abstract: This paper describes the access management in virtual information resource systems, analyzes its concepts, functions, and technical mechanisms, gives illustrative examples.

Keywords: Virtual information resource systems, Resource sharing systems, Access management, Authentication, Authorization

1．虚拟信息资源体系及其用户使用管理

1.1 虚拟信息资源系统

随着以出版商、文摘索引商和发行商为主导的网络化数字化信息资源的迅速推广，图书情报系统的发展主流已逐渐过渡到以虚拟信息资源系统建设为主[1-3]。这种系统特点是：a. 系统资源包括数字化期刊、文摘索引库、书目库、本地数字文献库、电子课件库、FTP 文件库、Web 网站等；b. 资源提供者包括出版商、文摘索引商、检索服务商、学术研究机构或其它图书馆，资源可能存放在资源提供者的服务器上或拷贝到服务提供者（例如图书馆）服务器上，通过网络提供使用；c. 服务提供者一般面向较大规模的并可能不断变化的用户群（例如学校的师生）来提供资源服务；d. 资源使用往往基于服务提供者对使用权的购买（而不是资源购买或占有）；e. 多个服务提供者往往组成联合系统合作购买数字化资源，而且这类系统可能提供集成化服务，包括统一的界面、使用管理、使用审计等。

比较典型的虚拟信息资源系统有加州数字化图书馆（CDL）[4]、弗吉尼亚虚拟图书馆（VIVA）[5]、校际合作联盟虚拟电子图书馆（CIC VEL）[6]、乔治亚州图书馆联机教育系统（GALILEO）[7]、加州州立大学软件与电子信息资源系统（SEIR）[8]等。另外，许多传统的图书馆系统或校园信息系统，也由于购买网络化信息资源的使用权并通过网络连接这些资源和提供相应服务而具备虚拟信息系统的主要特点。

1.2 虚拟信息资源体系的用户使用管理

一般地，一个虚拟信息资源系统往往连接多个分布的具有不同使用条件的资源提供者，服务于多个用户群（它们对多个资源可能具有不同权限），而且某些用户可能同时隶属于不同用户群。为了有效管理这种复杂环境下用户对资源的使用，虚拟信息资源系统必须建立用户使用管理机制，其核心功能包括：身份认证（Authentication），即确定请求资源者是否有合法身份；使用授权（Authorization），即确定该用户使用所请求资源的权限。另外，使用审计（Accounting）作为审计、支付和评价的基础往往也是使用管理的重要部分。

不同应用环境下的虚拟信息资源系统可能有不同的用户使用管理机制。为了全面考察用户使用管理机制，Clifford Lynch 提出了分析评价使用管理机制的基本要求[9]，包括：

a. 促进对信息资源的方便、有效使用。因为用户使用管理的根本目的是促进用户对资源的充分和有序的使用，因此从用户角度讲，这种机制应该基于通用的网络环境，尽量避免特殊技术、设置、地域等限制，操作简单，稳定可靠；对资源和服务提供者而言，这种机制应该不过分增加运行和维护负担、能方便地设置和调整用户群及其权限参数、能支持多种通

信协议和使用平台等。

b. 保障认证和授权的强度。这要求身份不易伪造或假冒，身份和授权数据不易丢失，整个管理系统不易受攻击或在受攻击情况下不会出现重大安全损害，能对不同用户或同一用户的不同使用权限进行详细划分、管理和控制，有利于保护版权和使用合同的权利。

c. 保护隐私权。在身份认证和使用授权中系统会收集有关的用户数据，这些数据往往受到法律、道德规范和具体机构制度的保护，信息系统应保证用户隐私不被侵犯，这实际上涉及到用户使用管理机制在对这些数据的收集程度（能收集到什么）、收集权限（由谁收集）、使用权限（谁能怎样使用这些数据）、管理责任（谁应如何管理这些数据）等方面的管理机制和约束强度。

d. 有利于对使用情况的审计。资源和服务提供者都希望能对使用情况进行审计，包括哪些用户使用了什么资源和哪些资源得到了多大程度的利用。准确的审计是服务提供者分析用户需求、分析资源价值、优化资金分配的依据，也是资源提供者了解资源利用程度、优化资源建设的基础，当然还是双方进行结算和支付的依据。但不同的使用管理机制对审计的数据内容、谁进行统计分析、数据的方便使用和安全保障等有不同的影响，而且这个问题容易与隐私权保护发生冲突。

2．用户使用管理的基本技术

目前，虚拟信息资源系统在身份认证上主要采用通行词控制（password）、IP 地址过滤（IP address filtering）、代理服务（proxy server）、电子证书认证（certificate access）等方式，在使用授权上往往通过一个或若干集成的用户参数数据库来控制，这个数据库还可与用户经费分配或支付机制相连接。

2.1 通行词控制方法

通行词控制是我们熟悉的使用管理技术，它技术简单容易使用，用户已经熟悉，不受地理位置限制，容易与授权数据库衔接并在其支持下根据具体通行词对用户授权进行仔细划分，有可能收集详细的使用数据。但是，这种方式依赖用户通行词数据库进行检验，这个数据库的安全构成对整个体系的最大威胁。而且，如果这个数据库处于资源提供者端（例如出版社），服务提供者（例如大学）需要持续地与资源提供者交换不断变化的身份数据，并担心隐私保护问题；如果这个数据库位于服务提供者端（例如大学），资源提供者必须不停地连接这个数据库进行检验，而且在多个机构联合组成系统时可能要求建立复杂的用户通行词数据管理和控制体系。如果用户可以使用多个资源，这可能意味着用户拥有多个不同的通行词（从而给用户带来麻烦）；或者每个用户使用唯一通行词，则必须有详细的授权数据库及授权检验机制。另外，用户容易遗失、遗忘或被盗用通行词，应用过程中通行词以明文形式传送等，都会造成安全隐患。当然，现在已广泛应用 SSL（安全套接层协议）[10]来对通行词传递过程进行加密。

2.2 IP 地址过滤方法

IP 地址过滤允许某个 IP 地址范围（例如一个校园网）的所有用户无限制地使用指定的资源（可能有“同时使用人数—concurrent users”的限制）。IP 地址过滤在技术上方便易行，对用户透明，资源和服务提供者能对使用进行有效控制，能有效保护隐私，安全保障也相对容易（虽然存在 IP 地址欺骗，但对学术信息资源来说尚不构成主要问题）。但是，IP 地址过滤不能满足 IP 地址范围外合法用户的使用要求，例如住在校园之外的教师或学生、在外开会或合作研究的教师、远程教育的师生等（当然，可以通过在公共 ISP 上为自己的用户群建立专用 IP 空间来部分解决这个问题）。IP 地址过滤的另一个问题是它难以对 IP 地址范围内的用户进行具体和细致的使用授权，致使所有用户有相同权限，可能夸大某些资源的可能用户群（以及相应的合同费用）。另外，它难以对使用资源情况进行细致审计。

2.3 代理服务方法

代理服务有两种主要方式，一是物理代理，在局域网上设置代理服务器，并设置浏览器使其所有请求都经过该代理服务器，再由它传递给相应的资源提供者。二是应用代理，可看成是“ 认证网关 ”（Authentication Gateways），用户连接上这种网关，完成相应的身份认证，然后由代理服务器将用户与资源提供者连接起来并管理相应的通信过程。物理或应用代理和资源提供者间可以依据 IP 地址、通行词、电子证书等方式进行认证。代理服务容易与授权管理系统相结合，能利用机构内存在的各种身份登记系统，并在提供集成接口、支持复杂授权、支持使用审计等方面具有优势。但是，在物理代理情况下需要在用户端进行设置，应用代理则要建立身份登记和认证系统，而且代理服务器的安全要求、可靠性、易管理性和运行效率等方面要求很高。

2.4 电子证书方法

在虚拟信息资源系统应用较广泛的主要是 Kerberos 体系和基于 X.509 的 PKI 体系。

2.4.1 Kerberos 认证体系

Kerberos[11-12]结构和过程如图 1 所示，包括用户（客户端 client，c）、认证服务器（Authentication Server，AS）、服务许可证服务器（Ticket Granting Server，tgs）和应用服务器（Application Server，又称 verifier，v）组成，其基本原理和过程如下：

第一阶段，用户向 AS 申请与 tgs 的会话密钥和认证许可证：

① c 首先向 AS 发出请求，请求中给出用户标识符 c（通常是用户通行词）。

② AS 检查用户标识库，核实 c 为合法用户后，生成一个 c、tgs 间会话密钥 $K_{c,\ tgs}$；同时生成认证许可证 $T_{c,\ tgs}$（通常有若干小时有效期），用 tgs 的密钥 K_{tgs} 加密（只有 tgs 才能解读）；然后将会话密钥 $K_{c,\ tgs}$ 和 tgs 名用用户密钥 K_c（通常是用户通行词）加密，与经过 K_{tgs} 加密的认证许可证一起传给用户。具体内容包括：$\{K_{c,\ tgs}$，tgs，$time_{exp}$，$n\}K_c$，$\{T_{c,\ tgs}\}K_{tgs}$。

c 收到答复，用 K_c 解密获得会话密钥 $K_{c,\ tgs}$，在机器上保存 $K_{c,\ tgs}$ 和认证许可证，可在许可证有效时间内向 tgs 申请针对多个应用服务器的服务许可证。用户通行词不再保留。

第二阶段，用户向 tgs 申请针对应用服务器 v 的服务许可证：

③ c 向 tgs 发出服务许可证请求，给出应用服务器 v、时间戳 ts（用会话密钥 $K_{c,\ tgs}$ 加密）、AS 给 tgs 的认证许可证 $T_{c,\ tgs}$，最后用 tgs 自己的密钥 K_{tgs} 加密。

④ tgs 用 K_{tgs} 解密得到会话密钥 $K_{c,\ tgs}$，利用 $K_{c,\ tgs}$ 解密时间戳，验证时间信息，验证成功后生成用于 c、v 间相互认证的会话密钥 $K_{c,v}$；同时生成服务许可证 $T_{c,\ v}$，用 v 的密钥 K_v 加密（只有 v 才能解读）；然后将 c、v 间会话密钥等信息用 c、tgs 间会话密钥 $K_{c,\ tgs}$ 加密，与经过 K_v 加密的服务许可证一起传给用户。

c 收到 tgs 应答后用 $K_{c,\ tgs}$ 解密获得 c、v 间会话密钥 $K_{c,v}$ 和服务许可证 $T_{c,\ v}$。

第三阶段，用户向应用服务器 v 申请服务：

⑤ c 向 v 发出服务认证请求，请求信息中包括为：时间戳 ts、校验和 ck、可选密钥 $K_{subsession}$，均用会话密钥 $K_{c,\ v}$ 加密，然后与 $T_{c,\ v}$（服务许可证）一道用 K_v 加密。

⑥ v 收到服务认证请求后，用 K_v 解密获得 c、v 间会话密钥 $K_{c,v}$，然后用 $K_{c,\ v}$ 解密时间戳和校验和，并予验证，成功时可认为 c 得到认证，接受 c 的接入；而且双方拥有共同的会话密钥 $K_{c,v}$，可用来对后续数据传送进行加密解密。

Kerberos 方式基于对称密钥对认证信息进行加密，可对统一管理的网络环境中的多种应用服务进行认证，认证信息安全性强，并可通过与授权数据库的连接实现授权控制；它还可对传输数据加密，而且运行效率较高、厂商支持较成熟。但它依赖一个“ 核心 ”认证服务器，该服务器存放所有认证信息而成为安全隐患，另外它更多地用于像校园网这类相对封闭的网络环境（虽然 Kerberos 5 也提供跨网域的交叉认证）。

2.4.2 PKI 认证体系

PKI 体系[13]是利用公共密钥方式、基于 X.509 电子证书[14]的分布式认证系统，由证书持有者（Subscriber，s，又称 end entity）、认证登记中心（Registration Authority，RA）、认证中心（Certification Authority，CA）、证书存储系统（Certificate Repository，CR）、应用系统（Applications，a，又称 relying entity）组成，其基本原理和过程如下：

① 任何需要电子证书的个人或服务器 s 首先向本地 RA 进行申请。

② RA 根据有关政策（往往是脱机地）审查 s 身份（例如身份证、学生证等），对合格者生成唯一的公钥-私钥对（public-private key pair），并通过安全方式将该公钥-密钥对交给申请者（例如用智能卡或软盘装载，由 s 或其管理者亲自领取）。

③ s 将自己的公钥-私钥对以加密形式安装在自己计算机上（只有 s 持有的特殊口令才能启用），并与 RA 进行持有验证（proof of possession），即用自己的私钥加密一段数据、由 RA 用相应公钥解密，从而确认只有 s 才持有该公钥-私钥对。

④ RA 根据 s 情况建立 X.509 电子证书内容，包括证书序号、申请者、申请者公钥、证书发放者、证书有效期等，交本地 CA 进行数字签名。

⑤ CA 利用自己的私钥对 s 电子证书进行加密（即数字签名），担保该证书的有效性。

⑥ CA 将经过自己签名的电子证书传给 s 安装在自己计算机上，同时将该证书存储到证书存储系统 CR 予以公布。

⑦ 当应用系统需要认证 s 时，它可向 s 或 CR 索取 s 的证书，利用 CA 的公钥解密证书，得到 s 的公钥，然后利用 s 的公钥与 s 进行持有验证，确认只有 s 才持有该公钥-私钥对，从而完成身份认证。

另外，s 根据需要可向 CA 申请更新电子证书（启用新的公钥-私钥对）或为电子证书延长有效期。在知道或怀疑证书不安全时 s 或 RA 或 CA 可申请撤消证书，CA 将被撤消的证书组成撤消证书名单（Certificate Revocation List），发给 CR 予以公布。如果应用系统不知道本地 CA 的公钥（例如应用系统是远程系统），该系统可索取该本地 CA 的电子证书（由其上层 CA 签名认证），用该上层 CA 的公钥解读来获取。

PKI 体系分布式认证功能强，可以通过多个 CA 在广泛环境下进行层级或交叉认证，认证信息安全性强，具有数字签名功能，而且 X.509 本身可包含授权信息（虽然多数应用都另外建立授权服务器）。但是，PKI 要求在用户计算机上安装公钥-私钥对和电子证书，且依赖一个相对完整、互相信任的 RA/CA/CR 体系，尤其是向用户交递公钥-私钥对并妥善保管中往往存在安全隐患，另外涉及的加密算法可能受到有关政府的出口限制。

3．用户使用管理组织模式和实例分析

3.1 用户使用管理组织模式

虚拟信息资源系统用户使用管理的组织模式主要有三种：

a. 基于资源供应商的模式（supplier-side management），这时认证和授权主要由资源提供者进行，比较多地采用通行词和 IP 地址过滤，用户数据库或合法 IP 地址表由资源提供者管理。这种方法已较普遍，所以容易接受和实施，技术和管理相对容易，对服务提供者负担较轻（除了需要提供用户数据），但可能给需要使用多个资源的用户或需要进行复杂权限管理的服务提供者带来麻烦，隐私保护存在隐患，服务提供者进行使用审计也较困难。

b. 基于服务提供者的模式（service-provider-side management），直接由服务提供者进行认证和授权，往往用通行词、代理服务和电子证书等，用户数据管理也在服务提供者端。这种方法容易与现有身份登记机制和正在兴起的集成化身份认证体系融合，有利于对多种资源的复杂使用权限进行管理，较利于隐私保护，使用审计较方便，但需要服务提供者建立有效可靠的管理机制，对于涉及多个服务提供者的合作系统而言这个机制会更复杂。

c. 基于中介系统的模式（intermediary-side management），即由一个介于资源提供者和

服务提供者之间的可信赖系统来管理用户数据、进行认证和授权。这种机制在多个服务提供者联合购买和使用多个资源的时候能减轻服务和资源提供者双方的负担，但对中介系统的安全性、运行效率、用户数据保护等方面要求非常严格，而且依赖服务提供者、资源提供者和中介系统间的信任和良好合作。

3.2 用户使用管理组织模式部分实例分析

（1）基于资源提供者端的以通行词或 IP 地址过滤为主的使用管理机制在出版商、文摘索引商或发行商提供的资源系统中已很普遍，例如 ProQuest 系统[15]主要采用通行词方法和 IP 地址过滤方法控制使用，而且通行词可对应于专用帐户（private accounts，为具体用户设置，不受设备和地域限制）或公用帐户（public accounts，供公众在指定计算机上使用），两者常常具有不同的权限。ProQuest 还建立 ProQuest Secured Access 服务，让图书馆下载有关程序并在图书馆网站上建立身份认证系统，然后通过这个网站接入和认证远程用户，并将远程用户连入 ProQuest、为远程用户提供连接 ProQuest 的临时安全通道。

（2）GALILEO系统[16]由美国佐治亚州各大学、中学、职业技术学院及公共图书馆组成，提供公共数据库和只限各成员机构授权用户使用的数据库。对于后者，在各成员机构与数据库提供者的使用合同基础上，使用管理有两种：在大中学校园、公共图书馆、学校远程教学点可通过IP地址过滤来接入和使用；对大学的教师、学生和职员可发放远程接入通行词，每季度更改一次，但通行词只通过大学图书馆的专门管理人员根据各自的具体政策和认证方法向得到授权的用户发放。美国印地安那州的INSPIRE系统[17]也是通过IP地址过滤接入州内各学校、机构、图书馆用户和使用州内ISP的本州居民，同时通过发放电子证书为使用州外ISP（例如AOL）的本州居民提供认证服务。

（3）英国的ATHENS[18-19]是基于中介系统的用户使用控制系统，它服务于英国250多个高等教育机构的一百多万用户，所覆盖的资源包括JANET的四个数据中心及其40多个大型数据库（例如INSPEC、EI等）、检索商数据库（例如OCLC的FirstSearch）和其它数据库中心。它通过集中的服务帐号数据库和用户认证数据库实施管理，前者记载各校具体购买的资源名称、连接方式、帐号、认证方式（IP地址过滤或通行词）、服务限制、期限等，后者记载各校每个合法用户的基本数据、授权权限和对应的ATHENS通行词，而这个通行词往往是在该用户的本校通行词前加上ATHENS专门的三位机构代码。各校管理者可上载或联机修改用户认证数据。当用户接入某一资源时，输入自己的ATHENS通行词，资源提供者将它传给ATHENS进行认证（利用SSL进行加密），如果该用户属于某校合法用户，ATHENS把相应学校的IP地址或通行词及该用户授权权限传给资源提供者，为该用户建立使用权。用户只需一个通行词，不受地理限制，可方便连接使用获得授权的多个资源。现在，ATHENS又成为NESLI[20]（National Electronic Site License Initiative）的使用管理机制。NESLI是一个协同购买数字化期刊资源的体系，并统一通过SwetsNet[21]的数字化期刊集成服务来实际获取期刊数据。这时，用户仍只需输入他的ATHENS通行词，经过ATHENS认证后转换为相应的SwetsNet帐号和认证数据，连接SwetsNet来获取相应数字化期刊资源。

（4）美国哥伦比亚大学提出了一种基于认证中介服务器的系统[22]。用户首先启动事先设置的浏览器安全通信模块（该模块将“ 代理 ”用户），利用加密方式连接校园认证中介 broker，输入自己的通行词；broker 连接相应的身份登记系统验证用户，并生成相应的临时私钥和临时电子证书（包括针对资源提供者的认证数据和针对具体用户的授权数据、broker 定义的用户临时身份、broker 地址等），传回用户模块；用户利用这个证书在 SSL 方式下连接资源提供者进行认证获得服务；如果必要（例如资源提供者需要用户电子邮件地址以传送数据文件），资源提供者可将用户电子证书送往 broker，由 broker 在相应身份登记系统中检索有关数据后送往资源提供者。这种机制既可利用用户个人通行词对多种服务进行认证，又保证用户个人通行词从不传给资源提供者；既通过 broker 充分利用现有身份登记系统，又

不造成新的运行瓶颈，同时在需要时可为资源提供者提供用户的有关数据（当然要服务有关政策规定）。

另外，许多大学正在建立基于 PKI 的认证体系，支持包括虚拟信息资源利用在内的校内外多种服务与应用，例如加州大学的 PKI 认证与授权机制[23]、科罗拉多大学的 UMI PKI[24]、卡内基-梅隆大学的 NetBill 系统[25]、昆士南技术大学的 Oscar PKI[26]等。

参考文献：

[1] 张晓林。网络环境下的文献资源共享。《世纪之交图书馆事业回顾与展望》，北京图书馆出版社，1999.7

[2] 张晓林。学术信息交流体系的重组与大学信息服务模式的再造。《大学图书馆学报》，2000.1

[3] 张晓林、党跃武、李桂华。网络化数字化基础上的学术信息交流体系及其影响。《图书馆》，待发

[4] Ober, John. The California Digital Library. D-Lib Magazine, March 1999 (http://www.dlib.org/dlib/papers/march99/09ober.html，参见http://www.cdlib.org)

[5] Virtual Library of Virginia (http://www.viva.lib.va.us)

[6] CIC Virtual Electronic Library (http://NTX2.cso.uiuc.edu/cic/cli/accessvel.html)

[7] Galileo (http://www.galileo.peachnet.edu/galileo)

[8] SEIR (http://www.co.calstate.edu/irt/seir/)

[9] Lynch, Clifford. A White Paper on Authentication and Access Management Issues in Cross-organizational Use of Networked Information Resources. Coalition for Networked Information, 1998

[10] Secure Socket Layer (http://home.netscape.com/eng/ssl3/index.html)

[11] Neuman, B. C. and Tso, T. Kerberos: An Authentication Service for Computer Networks. IEEE Communications. 32(9):33-38, Sept., 1994

[12] Kohl, J. T. and Neuman, B. C. The Kerberos Network Authentication Service. Internet RFC 1510, Sept, 1993 (http://www.cis.ohio-state.edu/htbin/frc/rfc1510.html)

[13] RFC 2459. Internet X.509 Public Key Infrastructure. (http://www.cis.ohio-state.edu/htbin/frc/rfc2459.html)

[14] ITU-T Recommendation X.509 (1997 E): Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997

[15] Proquest's Access Plans. (http://www.umi.com/hp/Support/PQD/)

[16] GALILEO Access Policies. (http://www.peachnet.edu/galileo/accesspol.html)

[17] Indiana's Virtual Library Inspire (http://www.inspire-indian.net/)

[18] Wiseman, Norman. Implementing a National Access Management System for Electronic Services. D-Lib Magazine, March, 1998 (http://www.dlib.org/dlib/papers/march98/03wiseman.html)

[19] ATHENS (http://www.athens.ac.uk/)

[20] National Electronic Site License Initiative. (http://www.nesli.ac.uk/)

[21] SwetsNet. (http://www.swetsnet.nl 北美 http://www.swetsnet.com/)

[22] Glenn, A. And Millman, D. Access Management of Web-based Service. D-Lib Magazine, Sept. 1998 (http://www.dlib.org/dlib/papers/sept98/09glenn.html)

[23] University of California Authentication & Authorization Architecture, 1998

[24] University of Colorado ISSCS. UMS Public Key Infrastructure Analysis, 1998

[25] Carnegie Mellon University NetBill. (http://www.ini.cmu.edu/netbill/)

[26] Oscar PKI project (http://www.dstc.qut.edu.au/MSU/projects/pki/index.html)

本文最初发表在《现代图书情报技术》2000 年第 5 期第 7-11 页。