维普资讯 http://www.cqvip.com

一种基于扩展 X. 509 认证和角色访问控制的安全策略

A Security Strategy Based Extending X. 509 Authentication and Role-based Access Control

沈显君　冯　刚

(华中师范大学计算机科学系　武汉 430079)

Abstract　The X. 509 authentication and Role-based access control are analyzed and combined in this paper, then X. 509 authentication is extended and described in detail. The concrete actualizing process of security strategy based on X. 509 authentication and Role-based access control is also expatiated.

Keywords　X. 509 authentication, Role, Security strategy

1. 引言

随着 Internet 技术的发展，电子商务等新的基于 Web 的应用日益普及，安全问题变得至关重要。常用的弱身份鉴别如口令已经不能满足网络安全的需要，基于公共密钥体系(Public key infrastructure，PKI)的 X. 509 已被广泛用于安全电子交易(SET)、安全套接字层(SSL)、安全/多用途邮件扩展(S/MIME)、IP 安全(IPSec)等开放分布式环境，用以实现强身份鉴别。基于角色的访问控制(Role Based Access Control：RBAC)可以实现用户与访问权限的逻辑分离，提供强大而灵活的安全控制，因此将 X. 509 认证标准与基于角色的访问控制(Role Based Access Control：RBAC)的安全策略相结合，并对 X. 509 标准进行扩展，可以有效地解决基于网络的大规模应用系统所面临的日益复杂的安全问题。

2. X. 509 认证

X. 509 提供基于 X. 509 公钥证书的目录存取服务，1993 年 ITU 公布 X. 509 第二版，1995 年，ISO/IEC 公布 X. 509 第三版(V3)，增加密钥和策略信息、证书主体属性和发放者属性、证书路径限制等 14 项扩展域以满足基于各类应用的具体需要。X. 509 的最新版本是 ITU-T1997 年修订的第三版。

在采用 X. 509 证书的安全系统中，由 CA(Certificate Authority，证书管理机构)对证书发放、撤消等工作进行统一管理。认证(Certification)是将一个公共密钥与具体的个人、组织或其他实体、属性对应起来的过程。在公共密钥体系中，这种对应关系是通过证书实现的。证书的具体格式可随不同的标准而异，但最基本内容应包括证书主题、公共密钥、CA 标识、CA 数字签名等。证书主题是一个实体(如个人、公司、组织和国家等)或属性(如人员的访问许可权)。CA 标识是颁发证书的 CA 标识信息。CA 数字签名保证了证书的不可伪造性。首先将证书主题、公共密钥、CA 标识通过哈希函数进行处理得到哈希编码，再用 CA 的私有密钥进行加密后得到数字签名。通过证书，证书主题就和公共密钥一一对应起来。

证书有效性检查(validation)是验证一个证书是否仍然有效的过程，其具体细节因不同的 PKI(例如 X. 509 和 PGP)而异，但是也存在一些共同的基本特征，包括证书基本格式、CA 的组织结构、有效性检查方法、证书废除方法等。

3. 基于角色的访问控制模型

在基于角色的访问控制的应用系统中，系统安全管理员根据需要定义各种角色，并设置合适的访问权限，而用户根据其责任再被指派为不同的角色。这样，整个访问控制过程就分成了两部分，即访问权限与角色相关联，角色再与用户相关联，从而实现了用户与访问权限的逻辑分离。角色可以看成是一个表达访问控制策略的语义结构，它可以表示承担特定操作的资格，也可以体现某种权利与责任。由于实现了用户与访问权限的逻辑分离，基于角色的安全策略提供了一种灵活的、动态的方法，能够很好地适应大型网络应用系统特定的安全策略，能够根据组织结构或安全需求进行灵活的变化，且易于控制，既能有效地改进系统安全性能，又极大地减少了权限管理的负担。

RBAC 模型描述如下：

定义 1　用户：用户就是一个可以独立访问计算机系统中的数据或用数据表示的其他资源的主体。Users 表示一个用户集合。用户在一般情况下是指人，但有时也包括计算机或一些具有自治性的软件系统。

定义 2　权限：权限是对计算机系统中的数据或用数据表示的其他资源进行访问的许可。Permission 表示一个权限集合，基于角色的访问控制方法是策略中立的，可以看成是访问控制管理中的一个独立部件，它没有具体规定如何进行权限定义，可以使用特殊的方法，也可以直接使用强制访问控制或自主访问控制等方法。

定义 3　角色：角色是指一个组织或任务中的工作或位置，它代表了一种资格、权利和责任。Roles 表示一个角色集合，基于角色访问控制方法的思想就是把对用户的授权分成两部分，用角色来充当用户行使权限的中介。这样，用户与角色之间以及角色与权限之间就形成了两个多对多的关系。一个用户可以是很多角色的成员，一个角色也可以有多个用户。同样地，一个角色可以有多个权限，而一个权限也可以重复配置于多个角色，称这两个关系为用户委派和权限配置。

定义 4　用户委派：用户委派是 Users 与 Roles 之间的一个二元关系，假定 UA Users×Roles 是一个用户委派关系集合，那么(u，r)∈UA 表示用户 u 被委派了一个角色 r。

定义 5　权限配置：权限配置是 Roles 与 Permission 之间的一个二元关系，假定 PA Roles×Permission 是一个权限配置关系集合，那么(r，p)∈PA 表示角色 r 拥有一个权限 p。

4. 扩展的 X. 509 认证

扩展的 X. 509 采用 RSA 的公开密钥认证系统(Public Key Cryptoaraphy Standards)，在 PKCS 中，每个用户有两把

维普资讯 http://www.cqvip.com

密钥，一把是用户的私有密钥，一把是对其他所有用户公开的公开密钥，扩展的 X.509 采用 RSA 进行加密解密，用 MD5 杂凑算法对消息生成数字文摘，用密钥进行加密后形成数字签名。

由于 X.509 证书没有表示安全策略的域，无法将 X.509 证书与应用系统具体安全需要联系起来，因此对于 X.509 (v3)予以扩展，在其预留的扩展域中增加 Role、Userid 等安全策略信息，并对 Role、信用卡号等敏感信息进行加密。扩展的 X.509 证书由安全认证服务器产生，每份证书都包含系统用户的角色信息。

扩展的 X.509 证书的 ASN.1(Abstract Syntax Notation One)文法简要描述如下：

```
Certificate::=SEQUENCE{
    roleCertificate ROLECertificate,
    signatureAlgorithm AlgorithmIdentifier,
    signatureValue BIT STRING}
ROLECertificate::=SEQUENCE{
    version DEFAULT V3,
    serialNumber CertificateSerialNumber,
    signature AlgorithmIdentifier,
    issuer Name,
    validity ValidityDate,
    subject Name,
    subjectPublicKeyInfo
            SubjectPublicKeyInfonation,
    issuerUniqueID[1] IMPLICIT
            UniqueIdentifier OPTIONAL,
    subjectUniqueID[2] IMPLICIT
            UniqueIdentifier OPTIONAL
    extensions [3] EXPLICIT Extensions
            OPTIONAL }
Extension::=SEQUENCE SIZE
        (1…MAX)OF EXTENSION
AlgorithmIdentifier::= SEQUENCE
            {PCKS #1 MD5 with RSA}
ValidityDate::=SEQUENCE{
    Not Before Time,
    Not After Time}
Time ::= CHOICE {
     utcTime UTCTime,
     generalTime GeneralizedTime }
UniqueIdentifier::= BIT STRING
SubjectName::=SEQUENCE{
    Name OCTET STRING,
    Userid OCTET STRING}
Subject_Public_Key_Info::=SEQUENCE{
    Algorithm Algorithm Identifier ,
    Public Key:BIT STRING,
    Public Exponent INTEGER}
Extension::= SEQUENCE SIZE{
    Identifier Role,
      Critical BOOLEAN DEFAULT NO,
      Value ENCRYPTION STRING,
    Identifier Certificate Type,
      Critical BOOLEAN DEFAULT NO,
      Certified Usage Certified_Usage
    Identifier Authority Key Identifier,
      Critical BOOLEAN DEFAULT NO,
      Key Identifier BIT STRING}
Role::={OCTET STRING}
Certified_Usage::= OCTET STRING{SSL
    Client,E_Mail}
```

验证扩展的 X.509证书的过程可以用以下算法步骤来描述(假定通信双方都可以从目录服务器获取对方的公钥证书，或对方最初发来的消息中包含公钥证书)：

(1)用户 A 将消息发往 B，消息包括用户 B 的身份、一次性随机数 r_A、时戳 t_A、用 B 的公钥 PK_B 加密的会话密钥 $E_{PK_B}[K_{AB}]$、用 A 的公钥签署的其他信息 Signdata。

(2)B 根据自己的系统时钟检查当前收到的消息有效期，确认证书的新鲜性；

(3)B 验证 A 的其他一些必要的信息，例如验证证书的扩展信息等，确认 A 的身份、消息的真实性和完整性；

(4)B 向 A 发出应答消息，包括用户 A 的身份、A 发来的一次性随机数 r_A(使应答消息有效)、B 产生的时戳 t_B 和一次性随机数 r_B、用 A 的公钥 PK_A 加密的会话密钥 $E_{PK_A}[K_{BA}]$、用 B 的公钥签署的其他信息 Signdata。

(5)若双方无法建立同步，则 A 将对 B 发来的一次性随机数 r_B 进行签字后发给 B，以避免重放攻击。

5. 基于扩展 X.509认证和角色访问控制的安全策略实现过程

(1)Web 用户通过浏览器向 Web Server 发出登录请求，同时输入自己的用户名和口令。

(2)Web Server 接收用户请求之后，将用户信息传送给角色服务器，角色服务器查找角色数据库(Role DB)，验证用户名和口令，成功后，为用户进行权限配置，给用户委派角色，授予相应 Permission，激活该角色，然后通知 Web Server 用户登录验证通过，将用户的角色传送给安全认证服务器(Secure Authentication Server)。

(3)Web Server 根据用户的角色所规定的安全级别选择不同的加密/解密算法，动态生成加密/解密程序，传送到 Web 用户，从而在 Web 用户与 Web Server 之间建立由 Web Server 控制的安全通道。

(4)Web Server 在接到用户角色验证通过消息后，通知用户验证通过。

(5)用户通过安全通道将数据操作请求传给 Web Server，Web Server 将用户请求发给系统功能调度程序予以响应，功能调度程序对用户请求进行分析后，调用相应的功能模块进行处理。

(6)安全认证服务器将用户的角色加入到扩展的 X.509 证书中，调用 RSA 将用户所拥有的角色、用户名、口令等信息进行动态加密，调用 MD5算法生成数字签名。

(7)功能模块则根据具体情况决定是否向后台 DBMS 发送数据交换请求，若需要，则通知后台 DBMS 准备进行数据操作。

(8)若后台数据库服务器接受用户操作请求，向安全认证服务器请求安全认证。

(9)安全认证服务器将相应的公钥和私钥分别传送到 Web 用户和后台数据库服务器。安全认证服务器与后台数据库服务器取得联系，将用户角色信息传给数据库服务器并通知用户需要进行的数据操作，询问是否接受。如果数据库服务器接受，则启动认证确认模块对本次交易进行公证。

(10)在进行公证之前，安全认证服务器应通知 Web 用户和数据库服务器是否承认此次公证，如果双方均同意，则进行交易，将相应的信息予以记录备案，如 Role、Userid、Time、IP、数字签名等予以记录备案，存储在安全认证服务器中，以备查询，然后 Web Server 和数据库服务器之间开始会话，建立安全通道，进行数据交换。(安全认证服务器并非每次对数据库操作均进行公证，只有当用户或后台数据库发出公证请求后，安全认证服务器接到请求后才开始运作，提供服务，以提高效率。)

(11)Web Server 接受用户的数据操作请求并对其加密后传给数据库服务器，到达数据库服务器后进行解密，后台数据库服务器根据用户角色及其操作权限予以验证，验证合格后，根据该角色的权限予以响应，并将此次操作记录在日志文件中。数据库服务器返回操作结果之前也要进行加密。

(12)Web Server 收到后台数据库结果后解密，解密后的

(下转第72页)

维普资讯 http://www.cqvip.com

(UNESCO). Guidelines for establishment and development of multilingual scientific and technical thesauri for information retrieval. Palce de Fontenoy, Paris 7e, Dec. 1971
12 Ausin D. Progress towards standard guidelines for the construction of multilingual thesauri. In: Commission on the European Communities, ed. Third European Congress on Information Systems and Networks, volume 1, Verlag Dokumentation, May 1977. 341～402
13 Pashcenko N A, et al. Basic principles for creating multilanguage information retrieval thesauri. Automatic Documentation and Mathematical Linguistics, 1982, 16(3): 30～36
14 Neville H H. Alternatives to conventional multilingual thesauri. In: Verina Horsnell, ed. Report of a Workshop on Multilingual Systems, 1975. 10～12
15 Iljon A. Creation of thesauri for EURONET. In: Commission of the European Communities, ed. Third European Congress on Information Systems and Networks, volume 1, Verlag Dokumentation, May 1977. 417～437
16 Kitano H. Multilingual information retrieval mechanism using VLSI. In: A. Lichnerowicz, ed. RIAO 88 Program: User-Oriented Content-Based Text and Image Handling, volume 2, March 1988. 1044～1059
17 Ata B M A, et al. Sisdom: a multilingual document retrieval system. Asian Libraries, 1995, 493: 37～46
18 Cacares C. Russian-Spanish multisubject computer dictionary. Automatic Documentation and Mathematical Linguistics, 1986, 20 (2): 122～125
19 Benking H, Kampffmeyer U. Harmonization of environmental metainformation with a thesaurus-based multi-lingual and multimedial information system. In: Arthur Zygielbaum, ed. AIP Conf. Proc. 283, Earth and Space Science Information Systems, American Institute of Physics, 1992. 688～695
20 Lebowitz A I, et al. Multilingual indexing and retrieval in bibliographc systems: The AGRIS experience. Quarterly Bulletin of the International Association of Agricultural Libraries and Documentalists, 1991, 36(3): 187～192
21 Volodin K I, et al. Bilingual indexing of geological documents. Automatic Documentation and Mathematical Linguistics, 1991, 25 (6): 43～45
22 Semturs F. Information retrieval from documents in multilingual textual data banks. In: Third European Congress on Information Systems and Networks, Munich, May 1977. 463～467
23 Semturs F. STAIRS/TLS-a system for "free text" and "descriptor" searching. In: Everett H. Brenner, ed. Proc. of the ASIS Annual Meeting, volume 15, American Society for Information Science, Nov. 1978. 295～298
24 Rolling L. Multilingual systems: survey of the European scene. In: Verina Horsnell, ed. Report of a Workshop on Multilingual Systems, Oct. 1975. 4～5
25 Synellis C. TRANSLIN user survey report: [TRANSLIB technical report]. University of Patras Central Library, Rio 261 00 Patras, Greece, May 1995
26 Chachra V. Subject access in an automated multithesaurus and multilingual environment. In: Sally Mc Callum and Monica Ertel, eds. Automated Systems for Access to Multilingual and Multiscript Library Materials, International Federation of Library Associations and Institutions (IFLA), K. G. Saur, Aug. 1993. 63～76
27 Rolland-Thomas P, Mercure G. Subject access in a bilingual online catalog. Cataloging and Classification Quarterly, 1989, 10(1/2): 141～163
28 Marcus R S. Intelligent assistance for document retrieval based on contextual, structural, interactive Boolean models. In: RIAO 94 Conf. Proc. ings, Intelligent Multimedia Information Retrieval Systems and Management, Volume 2, Paris, Oct. 1994. 27～43
29 Buckley C, et al. Automatic query expansion using SMART: TREC 3. In: D. K. Harman, ed. Overview of the Third Text Retrieval Conference (TREC-3), NIST, Nov. 1994. 69～80
30 Hull D A, Grefenstette G. Experiments in multilingual information retrieval. In: Proc. of the 19th Annual Intl. ACM SIGIR Conf. on Research and Development in Information Retrieval, 1996
31 van der Eijk P. Automating the acquisition of bilingual terminology. In: Sixth Conf. of the European Chapter of the Association for Computational Linguistics, April 1993. 113～119
32 Lin Chunghsin, Che Hsinchun. An automatic indexing and neural network approach to concept retrieval and classification of multilingual (Chinese-English) documents. IEEE Transaction on Systems, Man and Cybernetics, 1996, 26(1): 75～88
33 Deerwester S, et al. Indexing by latent semantic analysis. Journal of the American Society for Information Science, 1990, 41(6): 391～407
34 Landauer T K, Littman M L. A statistical method for language-independent representation of the topical content of text segments. In: Proc. of the Eleventh Intl. Conf. Expert Systems and Their Applications, volume 8, Avignon France, May 1991. 77～85

(上接第58页)

数据，使用(3)中的算法加密后传送给 Web 用户，后者解密后得到操作结果。

通过以上过程，在 Web 用户与后台数据库之间建立了一条从前端 Web 用户到后端数据库服务器的安全通道，远程用户可以使用该通道进行多次安全的数据交换，直到事务完成，然后数据库服务器询问是否拆除安全通道，经 Web 端用户同意后拆除该安全通道，废除 X.509证书，同时后台 DBMS 从 Role DB 的"用户授权表"删除用户角色授权信息，回收角色功能。

结束语 随着 Internet 技术的发展，基于网络的大规模应用系统面临着日益复杂的数据资源安全管理以及大量的访问权限管理，基于扩展 X.509认证的角色访问控制提供了一种灵活、有效、易于扩展的安全管理策略。

由于 X.509认证的安全性主要取决于公钥证书的生成算法，进一步的工作将是在此基础上研究更合适的加密算法，同时对 X.509证书进一步改进以减少证书管理的负担，增加用户对证书主体的信任程度。

参 考 文 献

1 Ahn G, Sandhu R. Role-Based Authorization Constraints Specification. ACM Trans. on Information and System Security, 2000, 3 (4)
2 Herzberg A, et al. Access Control Meets Public Key Infrastructure, Or: Assigning Roles to Strangers. IEEE Symposium on Security and Privacy, Oakland, May 2000
3 Housely R. Internet X.509 Public Key Infrastructure: Certificate and CRL Profile(RFC 2459), Jan. 1999
4 Housely R. Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP. RFC2585, May 1999
5 Kent S, Atkinson R. Security Architecture for the Internet Protocol Nov. RFC 2401 1998