XML安全技术及一个新的基于XML的Web安全模型*)

陈 越 任年民 兰巨龙
(信息工程大学 郑州450002)

摘 要 简要介绍了XML加密、XML签名、密钥管理及访问控制等几种主要的XML安全技术,提出了一种基于XML应用的安全Web模型。

关键词 XML,XML加密,XML签名,XKMS,XACL,安全模型

XML Security Technologies and a New Secure XML-Based Web Model

CHEN Yue REN Nian-Min LAN Ju-long
(Information Engineering University,Zhengzhou 450002)

Abstract This paper briefly introduces some important security technologies for XML,such as XML-Encryption,XML-Signature, XML Key Management and XML Access Control etc. It proposes a security model of XML-based Web.

Keywords XML,XML-encryption,XML-signature,XKMS,XACL,Security model

1 引言

XML(可扩展标记语言)是SGML的一个优化子集[1]。它具有可扩展性、自描述性、开放性和灵活性等特点,从而大大优越于HTML,成为数据表示的一个开放标准,在几乎所有的电子商务系统和Web应用中扮演着重要的角色。随着XML的广泛应用,其安全问题也越来越得到重视。XML安全技术较为复杂,必须依照机密性(未经授权的用户不能访问数据)、完整性(数据在传送中未被改动)、可认证性(文档确实来自所声明的发送方)和不可否认性(发送方不能否认是他们发送的,也不能否认数据的内容)来保证XML文档的安全[2~5]。在解决这些安全需求时,必须结合XML文档自身的特点,有针对性制定各种安全策略、安全机制,并选择合适的算法。本文在对XML安全技术研究的基础上,提出了一种基于XML的Web安全模型,并给出了实现方案。

2 XML安全技术

目前,与XML安全相关的技术规范的主要有XML加密、XML签名、XML密钥管理(XKMS)和XACL等。

2.1 XML加密

XML加密是一个对明文加密产生密文以及对密文解密恢复明文数据的过程。它可以用来保证数据的机密性。XML加密的粒度要求精确到元素级,加密对象可以是XML文档的元素、元素的内容或者是任意数据。XML加密还要求对含有加密元素的XML文档能够进行嵌套加密。XML加密元素〈EncryptedData〉的数据格式及XML文档加密和解密过程见文[6]。由于XML文档中包含的数据可能过长,从而为攻击提供了足够的已知明文,因此必须选择可靠的算法以抵御明文攻击。DES和RSA分别是目前最为成熟的对称密钥算法和公共密钥算法。XML加密可以综合运用这两种算法,以解决对称密钥传递的安全性问题和RSA算法效率低的问题。目前,笔者已实现了对XML文档的基本的加密模块[13]。

2.2 XML签名

签名数据完整性、认证性和不可否认性的安全服务。XML对数字签名提出了新的需求。例如流程作业,XML文档在各部门依次流动,每个部门都有一个表示某种承诺或声明的数字签名,而各部门同时希望只对自己负责的那部分内容来签名,所以XML要求实现细粒度签名并且能够签名多个数据对象[7]。XML数字签名用元素Signature来表示,其格式见文[8]。XML签名使用URI来引用数据对象。签名可以包含该数据对象,也可以作为该数据对象的子元素放入其中,还可以与其分别作为XML

*)该课题得到河南省教育厅应用基础类研究项目"XML安全及其应用研究"(编号:20015200024)资助。陈 越 副教授,硕士生导师,主要从事数据库技术、路由协议等方面的研究。

文档的并列元素，因此必须注意 Signature 元素的命名以避免产生冲突。XML 签名和验证的基本过程见文[8]。XML 签名指定了一系列算法及其 URI，如消息摘要使用 SHA-1，消息认证使用 HMAC，而签名则可使用 RSA 或 PKCS1。XML 签名提供了一个非常灵活的数字签名机制，在具体实现中必须注意文档的转换，检查安全模型，还有算法、密钥长度和证书等。

2.3 XKMS

XKMS 基于易理解的、开放的、标准的方法为 XML 加密和签名应用添加了信任服务。

XKMS 为公钥的分发和注册指定了策略，它由两部分组成——XML 密钥信息服务规范(X-KISS)和 XML 密钥注册服务规范(X-KRSS)[9]。X-KISS 允许一个客户端来代理信服务在处理 XML 签名〈ds:KeyInfo〉元素时的部分或全部工作。客户端代理信任服务时，应用程序可以避免使用基础 PKI 建立信任关系时的语法及其复杂性。X-KRSS 定义了公钥信息的注册协议。该协议支持由持有者注册一个密钥对。客户端可能要求注册服务将信息与公钥绑定。该信息绑定可能包括名称、一个标识符或由实现程序定义的扩展属性。绑定信息的密钥对可能由客户端提前产生，或者支持密钥恢复，根据服务的请求而产生。该注册协议也可用于私钥的后续恢复。XKMS 指定了注册 RSA 和 DSA 密钥的方法，还定义了一个体系结构以扩展协议来支持其它的密码算法，如 Diffie-Helleman 和 Elliptic Curve 变量。

2.4 XACL

对于保存在本地或服务器端的 XML 文档，一种有效的安全方法就是访问控制。目前较为成熟的访问控制语言即 XACL[10,11]，为 XML 提供了一种成熟的访问控制机制。与其它策略语言相似，XACL 也是面向"对象-主体-操作-条件"的语言。主体可以是一个三元组(用户 ID、角色和团体)，角色和团体都采用层次结构。对象支持从整个 XML 文档中到其中的单个元素。基本操作有读、写、创建和删除。

XACL 利用 XML 文档及主体的层次结构特点，定义了授权传递策略和冲突解决策略。即对某一对象定义的授权可以沿主体、客体的层次结构向上或向下传递，并使用了传递选项来控制授权传递的深度。由于授权传递必须支持特例，可对某对象直接定义肯定或否定授权，因此在实现时可能会出现同一主体对同一对象具有相矛盾的授权，它可能是直接的，也可能是由于传递导致的，此即授权冲突。XACL 也定义了相应的冲突解决策略。

XACL 采用临时授权模型，如图1所示，它主要由访问评估模块和请求执行模块组成。该模型定义了临时操作，即系统执行某基本操作时，可能要求执行相应的临时操作，如审计、日志、数字签名、认证等。相关策略的实现可分四个步骤：(1)提交请求：包括主体、对象和操作。(2)访问评估：根据目标 XML 文档的相关策略和相关状态来评价访问请求。访问决定要表明允许或拒绝，还要指定附加的临时操作。(3)在请求执行模块中处理请求：执行访问决定中指定的基本操作和附加的临时操作。对非"读"操作，目标 XML 文档及相关的状态文件将被更新。(4)返回视图：对"读"操作，创建并返回对象视图，其中只包含允许请求者访问的节点。目前，笔者已根据上述模型实现了 XML 文档的访问控制系统[12]。

3 基于 XML 的 Web 安全模型

XML 安全对于基于 XML 的 Web 服务的开发具有至关重要的意义。基于 XML 的 Web 服务使用 XML 作为标准的数据表示格式，实现了跨平台的数据交换和处理，而且它通过完整的基于标准 Internet 协议的程序接口为网络应用程序提供信息与服务，可以方便地通过 Internet 访问。XML 安全克服了 Internet 固有的安全隐患，对于基于 XML 的 Web 服务，如 B2B、B2C 电子商务等必将起到大大的推动作用。本文综合考虑 XML 数据交换的安全和服务器端 XML 数据库的安全等问题，将我们的访问控制模型与 XML 加密、签名等技术相结合，提出了一个基于 XML 的 Web 安全模型，如图2所示。

3.1 基于 XML 的 Web 安全体系结构

本模型是一个基于 XML 的 Web 安全系统，用于提供 XML 数据的安全访问和保护用户间的 XML 数据交换。它包括应用层、安全层和数据层。

应用层主要是指用户，包括定义私有 XML 数据的用户，使用 XML 数据库的多个用户。

安全层包括一个访问控制模块、一个加密模块和一个数字签名模块，这些模块负责安全性能的实现。访问控制模块接收用户的请求，然后根据用户的活动角色、请求的操作类型和授权规则数据库中的规则对 XML 数据库进行检索或存储数据，它也负责维护和更新授权规则数据库。系统安全管理员定义的授权规则具有最高优先级，这些规则应用于所有的用户和服务器中的 XML 数据，DAC 规则只能由 XML 数据库中数据的所有者来定义和修改。系统安全管理员还负责用户和角色信息的管理和维护。加密模块遵循 XML 加密规范，可以使用合适的算法对数据进行元素级加密和嵌套加密。数字签名模块遵循 XML 签名规范，可使用相应的算法签名 XML 数据。加密和签名操作都是可选的，并且其执行顺序是任意的，在发送的消息中包含了操作及其执行顺序的信息，接收方可以据此来反向处理数据，最终得到所请求的信息。

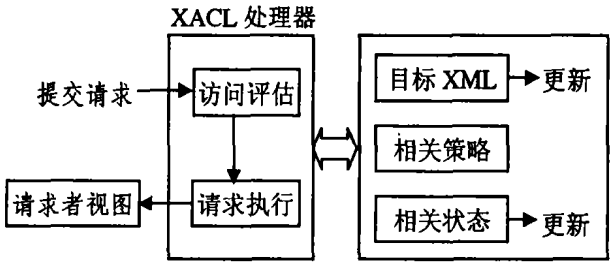

图1 临时授权模型

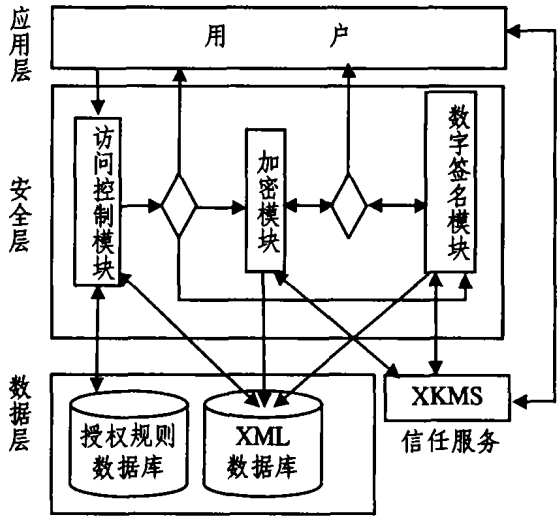

图2 基于 XML 的 Web 安全模型

数据层是一个 native XML 数据库，包括 XML 数据库(包括 Web 服务器为客户端提供的数据和客户端用来与其他用户交换所提交的数据)和授权规则数据库。数据库中的所有信息都存储为 XML 格式。

XKMS 模块是提供信任服务的第三方，它负责用户及其密钥的注册和管理。服务器和系统中注册的每个用户都被分配一个公钥和一个私钥。对于特定的用户组，XKMS 为其中的每个用户分配一个共享的私钥作为加密/解密的对称密钥。

该模型不仅提供了对基于 XML 的 Web 服务器中的 XML 文档的保护，并且可以保护 Web 用户间通过服务器进行 XML 数据交换。

3.2 对服务器中 XML 数据的安全访问

该模型能够提供对服务器 XML 数据库的安全访问，过程如下：当一个用户提交访问请求时，如果该请求要从 XML 数据库中获得某些信息，则访问控制模块根据授权规则数据库中的授权规则来评价该请求，计算访问决定，即该用户的当前活动角色对所请求的 XML 文档所拥有的肯定和否定授权。然后根据访问决定对 XML 文档进行裁剪，首先根据系统规则然后根据 DAC 来裁剪 DOM 树。该模块生成的结果数据可以作为用户视图直接返回给用户，也可以根据用户的要求或数据本身的安全需求进一步传送到加密模块或/和数字签名模块，进行加密或/和签名处理，这两个安全处理过程可以是任意的，只要增加相应的说明信息即可。在加密模块中，可以使用请求用户的公钥加密数据，而在签名模块中，则使用服务器方的私钥来签名。接收方收到数据后，根据安全处理程序信息，可对数据按顺序进行解密或/和验证。他能够使用自己的私钥解密数据以恢复明文，并能使用服务器方的公钥来验证签名。服务器和用户的密钥都是由 XKMS 来统一注册和管理的，它还可以负责发放安全证书等。通过这些方法，本模型能够实现数据的控制访问，能够保证数据本身的安全性，也实现了传输安全和服务器方认证。

3.3 保护 Web 用户间通过服务器的间接数据交换

本模型不仅支持对服务器中 XML 数据库的安全访问，还支持 Web 用户间基于 XML 的安全数据交换。首先，一个用户能够上传或更新他在服务器上的数据，此时，他可以定义 DAC 规则，允许其数据保存为加密状态或加密且签名的状态。在本模型中，基于用户之间使用对称加密技术，数据的加密密钥是由特定用户组共享的一个对称密钥，当组中的用户收到数据时，可以使用该密钥解密数据。用户也可以使用自己的私钥对 XML 数据进行签名，以使接收方能够验证。第二，用户可以检索服务器中的私有数据。处理过程如上一节内容所述，当一个用户发出一个请求，访问控制模块首先创建相应的 DOM 树并先后根据系统规则和 DAC 规则提取信息，如果数据本身是经过加密或签名的，则访问控制程序不能对该内容进行细粒度裁剪；如果数据本身是明文，则可以将结果数据作为用户视图发送给请求的用户，或者根据用户的需要或数据本身的安全需求，将其传递给加密模块(使用特定用户组共享的密钥)或数字签名模块(使用数据所有者的私钥)作进一步处理。这样，用户在 XKMS 的管理下就可以通过服务器间接地交换信息。

3.4 系统实现的讨论

本模型综合了多项安全技术，全面地保证了 XML 数据的完整性、机密性、认证性和不可否认性等需求。但是，灵活的访问控制、加密和数字签名机制可能引起复杂的访问控制规则和密钥管理问题。为了解决这些问题，本模型定义了一些元素来说明用户的安全需求，并提供相应的信息来表示模型的各个模块及其操作，还增加了一个接收器来判定合适的安全操作、操作顺序、密钥以及相应的算法以正确地处理数据。在本模型的实现中我们拟采用 SOAP(简单对象访问协议)来传送 XML 数据。SOAP 是一个基于 XML 的轻量级协议，用于分布

(下转第125页)

该应用集成组件中根据消息的标识，动态绑定相应的 AIC 处理程序的 dll 文件的路径和类名(包含命名空间)。

HAIP 主要有以下优点：

·采用可视化的流程定制和管理工具，医院业务流程的定义、重组都变得很容易。

·当规则发生改变时，只需要在规则库中进行修改而不需要变动整个业务流程。

·接口灵活，易于和不同的系统平台进行交互。采用 COM＋、WebService、Remoting 接口，提高了系统的兼容性和可扩展性。便于和 J2EE 平台以及 CORBA 平台集成。

·对于将来可能出现的系统来说接入集成平台将变得很容易。

·为应用程序的管理和监控提供了可靠的保证。

总结与展望 针对医疗应用集成过程中面临的问题，本文提出了一种解决方案 HAIP。它采用分布式的动态工作流系统设计框架，提供了可视化的工具，进行工作流的定制、监督和管理；消息映射工具很好解决了数据格式不一致的问题；业务系统间多种接口方式和 XML 的数据传输格式，有效地解决了系统异构问题，避免了出现信息孤岛现象。

在医疗应用集成过程中，不同的信息源在语法和语义上还存在不兼容的现象。为了更好地实现它们之间信息的共享和互操作，必须通过语义集成。而本体作为一种能在语义和知识层次上描述信息系统的概念模型建模工具，很适合于描述异构的、分布式环境下的信息资源。因此，基于本体的、具有语义特点的应用集成将是今后应用集成的发展方向。

参 考 文 献

1 Rao B N. Extreme Application Integration. EAI Journal, May 2002. 36～40

2 Corp H-P. Process Integration Architecture: Process automation with HP Changengine. 2000. http://www.ice.hp.com

3 顾沈明，徐妙君. 基于 Java 与 XML 的 B2B 平台模型研究. 计算机与现代化，2003(8)

4 Schulz K. Architecting Cross-Organisational B2B Interactions. IEEE Trans, 2000. 92～101

5 Berg J V, Schmidt J, Wendler T. Business process integration for distributed applications in radiology . IEEE Trans. , 2001. 10～19

6 郑淑芬. 电子商务整合方案实战—— Biztalk Server 2000 与 XML. 北京科海集团公司，2002

7 http://www.microsoft.com/china/biztalk/community/

8 Mugridge Wa, Grundy Ja, Hosking Ja, et al. Supporting information mapping in Health Informatics via integrated message transformation

9 林耀珍，Michael. 从系统需求到设计实作. NET 企业级应用系统，2004(3)

(上接第97页)

式环境中的信息交换。它的封装定义了一个框架结构来描述消息的构成以及如何对它进行处理，本模型的安全处理信息也被封装在其中，以给接收器提供足够的信息来处理数据。

结束语 本文提出的安全模型运用了当前较为成熟的几种 XML 安全技术，具有一定可扩展性，但在该模型中 XML 用户仅能通过 Web 才能进行安全通信，有一些局限性，需要在其上进行扩展以提供(端到端)P2P 模式的通信。

参 考 文 献

1 Bray T, et al. Extensible Markup Language (XML) 1.0. World Wide Web Consortium (W3C). http://www.w3.org/TR/REC-xml, W3C Recommendation 6 Oct. 2000

2 W3C. XML-Encryption Requirements. http://www.w3.org/2000/11/15-xml-encryption-req.html

3 W3C. XML Encryption Syntax and Processing. W3C Candidate Recommendation, Aug. 2002. http://www.w3c.org/TR/2002/CR-xmlenc-core-20020802/

4 W3C. XML-Signature Requirements. W3C Working Draft, Oct. 1999. http://www.w3c.org/TR/1999/WD-xmldsig-requirements-19991014.html/

5 W3C. XML-Signature Syntax and Processing W3C Recommendation, Feb. 2002. http://www.w3c.org/TR/2002/REC-xmld-sig-core-20020212/

6 Simon Ed, Madsen P, Adams C. An Introduction to XML Digital Signatures. http://www.xml.com/lpt/a/2001/08/08/xmldsig.html

7 W3C. XML Key Managment Specification (XKMS2.0). W3C Working Draft, March 2002. http://www.w3c.org/TR/2002/WD-xkms2-20020318

8 Hada S, Kudo M K. XML Access Control Language: Provisional Authorization for XML Documents. http://www.trl.ibm.co.jp/projects/xml/xacl/xacl-spec.html

9 Kudo M, Hada S. XML Document Security based on Provisional Authorization. 7th ACM Conference on Computer and Communication Security, 2000

10 Damiani E, Vimercati S D C, Paraboschi S, Samarati P. Design and Implementation of an Access Control Processor for XML Documents. In: Proc. of 9th WWW Conference, 2000

11 IBM alphaWorks. XML Security Suite. http://www.alphaworks.ibm.com/tech/xmlsecuritysuite

12 任年民，陈越. XML 文档的访问控制及其实现. 信息工程大学电子技术学院学报，2002(4)

13 王运成，陈越. XML 文档加密研究及其实现. 信息工程大学电子技术学院学报，2003(2)