

# XML 安全体系研究

杨 灵, 邹 娟

(仲恺农业工程学院 计算机科学与工程学院, 广东 广州 510225)

**摘 要:**随着 XML 的应用越来越广泛,其安全问题也变得尤为重要。现有的 XML 安全技术只能防止某个方面的安全问题,不能应对网络中的多重安全威胁。文中提出了一种基于各种 XML 安全标准的安全体系,详细介绍了各种技术,以及它们的安全防范的侧重点,为 XML 的应用提供了全方位的保护。针对网上购物系统的安全需求,提出了基于上面提到的安全体系的解决方案,通过该实例的应用,验证了文中提出的安全体系能够防范网络应用中的多种安全威胁。

**关键词:**XML;安全体系;安全规范

**中图分类号:**TP309.2

**文献标识码:**A

**文章编号:**1673-629X(2010)08-0137-05

## The Study of Architecture for XML Security

YANG Ling, ZOU Juan

(Dept. of Computer Science and Engineering, Zhongkai University of  
Agriculture and Engineering, Guangzhou 510225, China)

**Abstract:** As more and more extensive application of XML, its security issues have become particularly important. The existed XML security technology can only prevent a particular aspect of security issues. It can't address various aspects of network security threats. This paper presents a security architecture based on XML safety standards, then introduce all the technologies of this architecture in detail, and their emphasis for security protection, so when under this architecture it can provide a full range of protection for the application of XML. Finally, presents a solution for the online shopping system's security requirements which is based on security architecture of above. By the application of the online shopping, it confirmed the security architecture could prevent various security threats in the network application.

**Key words:** XML; security architecture; security specifications

## 0 引 言

可扩展标记语言(eXtensible Markup Language, XML)作为一种 Internet 上的信息交换格式,越来越多的公司在通过网络传输结构化数据时采用 XML。然而,XML 规范中只定义了数据格式,没有实现数据的安全保护,其 XML 数据是完全开放的,没有任何保护措施;另外,Internet 是公开的网络,任何人都可能截获甚至篡改网络上的数据。所以随着 XML 应用的增长,XML 的安全性也越来越受到人们的关注。

XML 安全性是指信息从客户机经过若干的中间机,最终到达目标机这个过程中对 XML 的保护。它应包括几个方面:机密性、完整性、真实性、防抵赖性和访问控制。为了实现这一目标,文中先提出了结合各种安全技术的 XML 安全体系,然后介绍了体系内各

组成部件的技术特点和应对的安全目标,以及各部件间的依赖关系。

## 1 XML 安全体系

W3C 和 IETF 等机构制定的一系列 XML 安全规范<sup>[1]</sup>(XML Security Specifications),包括 XML 加密、XML 数字签名、XKMS 密钥管理以及 Web Service 安全等。虽然,这些规范目前仍在不断完善,但是这些规范是垂直的,单一的使用某个规范不能从根本上解决安全问题,但把它们结合在一起,形成安全体系就可支持各种安全目标。该安全体系如图 1 所示。

### 1.1 SOAP

XML 是完全面向数据的,可以与任何通讯协议相结合,因此可以利用简单对象访问协议(Simple Object Access Protocol, SOAP)来实现 XML 数据的传输安全性。SOAP 以 XML 形式提供了一个简单、轻量的用于在分散或分布环境中交换结构化和类型信息的机制<sup>[2]</sup>。SOAP 不提供任何应用程序语义,它只是提供了一个用于定义应用程序语义的机制。

收稿日期:2010-01-25;修回日期:2010-04-23

基金项目:广东省自然科学基金项目(9151022501000008)

作者简介:杨 灵(1980-),男,江西人,工程师,硕士,研究方向为网络安全。

SOAP 包括三个部分: SOAP 封装、SOAP 编码规则和 SOAP RPC 表示。其中 SOAP 封装定义了 SOAP 消息中的内容是什么, 这些内容是否必须出现在 SOAP 消息中, 消息以什么形式组织, 谁发送的该消息, 以及由谁来接收并处理它。

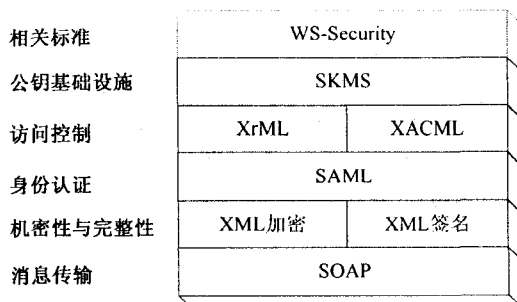


图 1 XML 安全体系

SOAP 是平台独立的协议, SOAP 通信基本上是从发送端到接收端的单向传输, 常常将 SOAP 封装起来绑定到相应的传输层协议(如 HTTP, SMTP)上传输, 这种方式类似于请求/应答模式。SOAP 消息是一个 XML 文档, 包括三部分: 封装、头和体。它的基本数据结构如图 2 所示。

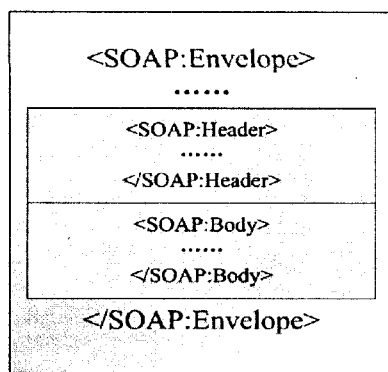


图 2 SOAP 的基本数据结构

①封装元素 < Envelope >: 它是必须出现的顶层元素, 它可以包含名域声明和限定名域的附加属性。

②SOAP 头 < Header >: 它是可选的, 必须以 < Envelope > 的第一个直接子元素出现; 因为交换 SOAP 信息的各应用方是物理位置上分散的, 且信息交换是临时发起的, 无法预先约定消息的要素, SOAP 头提供了这样的机制来向 SOAP 消息中添加某些要素; 同时 SOAP 还定义了一些属性来规范这些要素应由谁处理、是否可选等细节约定。

③SOAP 体 < Body >: 它包含真正要发送给接收者的信息, 是 SOAP 的核心所在, 所以必须以直接子元素出现。当存在 < Header > 元素时, < Body > 必须紧接着其后出现, 否则作为 < Envelope > 的第一个子元素出现。SOAP 体可以包含多个直接子元素, 如:

SOAP 定义的用来报告错误信息的 Fault 元素。当然用户可以自行定义 < Body > 的子元素, 也可以为直接子元素限定名域。

SOAP 提供了一个简单、灵活的消息交换机制, 消息的格式可以由交互双方协商而不必一致。利用这种网络信息交换机制, 可以实现 XML 的传输安全, 如: 端对端的信息传送、中间件的独立性、传输的独立性和驻留信息的安全性。同时还可以将 XML 加密、签名安全措施与 SOAP 结合使用。

## 1.2 XML 加密(XML Enc)

XML 加密的基础是 XML 加密规范<sup>[3]</sup>(XML Encryption Syntax and Processing), 该规范是由 W3C 制定并于 2002 年 9 月公布的推荐标准。它包括加密语法和处理规则两部分, 前者描述加密数据的表示形式, 后者描述加密的处理过程。XML 加密标准定义了加密和解密完整 XML 消息、部分 XML 消息, 甚至外部非 XML 资源的过程。其中, 加密结果和额外的信息都是以标准 XML 格式来表示, 所以其结果可用 XML 工具进一步处理, 如对同一文档的不同部分进行多重加密。

较之传统的 SSL, XML 加密引入了加密粒度的概念<sup>[4]</sup>, 即不再仅仅将信息作为整体来加密, 还支持对部分信息加密, 甚至仅仅加密一个元素。这样有利于敏感信息的管理, 可以通过对文件中不同的信息采取不同的密钥加密, 以区别不同级别的敏感信息, 当用户获得这样的加密文件时, 只能收到他所在级别的密钥, 因此只能解开自己有权限的那部分信息。如在电子商务中, 商家可能需要知道客户的名称和地址, 但无需知道任何正在使用的信用卡的各种详细信息, 而银行不需要知道商品详细信息一样。

XML 加密后的数据以 XML 格式表示使用。其中 < EncryptedData > 元素表示加密的数据, 其属性 Type 的值则表明了加密的主体, 如元素、内容等。< CipherData > 元素封装或引用原始加密数据, 如果是封装, 原始加密数据就是 < CipherValue > 元素的内容; 如果是引用, < CipherReference > 指定的 URI 就指向加密数据的位置。

使用 XML 加密可以保证信息的机密性。即使攻击者窃取到信息, 他只能看到加密后的信息, 由于不知道使用的加密算法和密钥, 他不能解密该信息, 从而保证了信息的机密性。

## 1.3 XML 签名(XML DSig)

XML 签名是对现有数字签名基础设施的扩展, 其基础是 XML 数字签名规范 (XML Signature Syntax and Processing)<sup>[5]</sup>, 该规范是由 IETF 和 W3C 联合制定, 并于 2002 年 2 月公布。该规范定义了 XML 数字

签名的处理规则和语法,无论是 XML 文档包括签名的内部或非签名处,还是其他为文档,都可提供对任何数据类型的完整性、消息认证、和/或签名者认证服务。

对数字内容进行签名的过程分为两个阶段。一是对数字内容进行整理,得到的结果放在一个 XML 元素中。这是为了保证内容一致但结构略有不同的两个文档所产生的签名摘要相同,如,其中一个文档中有多余的空白。二是挑选出整理的值,并对其进行签名。

XML 数字签名不同于其它的消息签署协议,如 PGP(Pretty Good Privacy),它支持仅仅签署 XML 树的特殊部分而不是整个文档。为了能用 XML 来表示数字签名,在 XML 规范中定义了<Signature>元素。利用<Signature>元素中的 URI 来表示数字签名的原始 XML(或其中的一部分),该元素包括了签名使用的类型、摘要值、签名值等其它必要信息以及验证签名所需的密钥的详细信息。其基本结构如表 1 所示。

表 1 基本结构

<Signature ID="...">
<SignedInfo>
<CanonicalizationMethod/>
<SignatureMethod/>
<SignatureValue>
(<Reference URI>
<DigestMethod>
<DigestValue>
</Reference>)
</SignedInfo>
(<KeyInfo>)
</Signature>

XML 数字签名服务作为 XML 文档数据完整性和不可否认性的永久证据。如果签名消息被修改,签名验证将不会成功,发送方也不能否认已经签署过该数据,因为签名的私钥是唯一的。

#### 1.4 安全性断言标记语言(SAML)

安全性断言标记语言(Security Assertion Markup Language, SAML) 是 OASIS 制定的,基于 XML 框架的,用于可信任域之间请求/响应身份验证和授权信息交换机制。它定义了系统实体针对某个主题所制定的断言的语法和语义<sup>[6]</sup>。它使用标准的方法来对验证、属性和授权信息进行 XML 编码,以及这些安全信息的传输协议。

SAML 语句被称作断言。它们是以 XML 结构表示的,并具有嵌套结构。因此一条单独的断言可能包含几个不同的与身份认证(识别)有关的信息项、授权决定和属性,其中属性包括凭证、组成员关系转移指示符等。SAML 断言描述了先前发生的身份认证结果。

SAML 允许信任域的成员保留认证和授权信息,并且如果需要,在授权后信任域可与其他域共享这些认证信息,而不管这些域之间使用的是什么平台,即 SAML 可以用于实现不同系统和平台间的单点登陆(SSO)。

SAML 提供认证功能可以有效地确认数据提供者的身份,主要用于信任关系的移植。但是由于它假设了参与者之间是互相信任的,所以它不保证机密性、完整性和传输中断言的不可抵赖性。

#### 1.5 扩展访问控制标记语言(XACML)

扩展访问控制标记语言(Extensible Access Control Markup Language, XACML)是 OASIS 制定的 XML 规范,它与 SAML 共同使用,它提供 XML 文档和其它电子资源中细粒度信息访问控制策略。XACML 规范定义了加密规则、为策略绑定规则的方法,并定义了在应用多个规则和策略的情况下的选择和组合算法<sup>[7]</sup>。

在配置时,XACML 首先建立一套规则和策略来决定某些类型的主体和属性的资源能访问的控制机制<sup>[8]</sup>。当有人请求资源时,通过与已建立的标准比较,来决定是否允许该请求使用该项资源。

XACML 中的访问控制列表是四元的——主体、目标对象、允许的行动、规定。主体可以包括用户 ID、组或角色名字。目标对象允许粒度为一个单独的 XML 文档元素。允许的行动可以是原始的读、写、创建或删除,这表现了 XACML 的主要限制,因为它没有提供指定域的权限类型。规定是一个规则激活后(无论是否定还是承认)必须执行的行动。这种行动可能包括初始化登陆、要求额外的凭据或发送警报。XACML 定义了表达这些规定的语言<sup>[6]</sup>。

XACML 提供了访问控制能力,限制哪种类型的用户可以对哪种类型的资源执行哪种操作,很好地隔离了敏感信息。

#### 1.6 扩展版权标记语言(XrML)

扩展版权标记语言(eXtensible Right Markup Language, XrML)是由 ContentGuard 公司提出一种版权描述语言,专门用来描述数字内容版权及版权使用限制的 XML 语言。

XrML 为目前使用最多的数字版权描述语法标准,主要目的在于提供一个国际通用的方式,来达到指定版权、使用条件与保护内容的目的。XrML 是一种有专利,但可免费使用的规范。

XrML 可应用于各种模式上的各种数字化资源,包括数字型态的内容、在线服务或应用程序等。所谓的数字权益是指行为方在某条件下对特定资源享有的某种权利。因而它包括四大元素:行为方主体(princi-

pal)、权利(right)、资源(resource)和条件(condition)<sup>[9]</sup>。它还可针对不同对象,提供多种授权方式及限定各种使用限制。并使用数字签章技术,让收到版权描述文件的数字内容使用者无法私自篡改版权描述文档的内容。在每份 XrML 许可(license)里有包含了一到多个授权(grant),用来允许经识别过的主要使用者(principal),在特定的条件(condition)下,有指定的权利(right),来使用特定的资源(resource)。

XrML 关注数字版权管理,但它与 XACML 重叠。XACML 是更复杂、也更灵活的规范。XrML 更容易使用,但不适合复杂的访问策略或规则设置。XrML 针对的是资源不可知的情况,而 XACML 提供明确的方式来参与已知资源的访问控制。

### 1.7 XML 密钥管理规范(XKMS)

XML 密钥管理规范(XML Key Management Specification, XKMS)是由 W3C 推荐的密钥管理规范,它定义了管理密钥的公钥基础设施(Public Key Infrastructure, PKI)的网络服务接口,来管理和类似 XML Enc、XML DSig 这样的协议一起使用的密钥。XKMS 是 PKI 在 XML 上的发展,它将传统 PKI 的两层应用模式转化为三层,在 PKI 用户与 PKI 提供者之间加入信任服务(Trust Service)中间层。它利用 XML 语法描述密钥和证书信息,通过 XKMS 消息将客户端对密钥和证书的操作部分或全部地委托给基于 Web 的信任服务,以简化公钥的注册、管理和查询服务,减少客户端应用程序设置的复杂性。因为向客户端屏蔽了底层 PKI 实现,从而降低与 PKI 建立信任关系的复杂度<sup>[10]</sup>。

XKMS 是基于 XML、SOAP 和网络服务描述语言的。它包含两个子协议:XML 密钥信息服务规范(XML Key Information Service Specification, X-KISS)和 XML 密钥注册服务规范(XML Key Registration Service Specification, X-KRSS)<sup>[11]</sup>。X-KISS 从使用的密钥服务器定位和检索出公钥,例如,加密或签名验证。应用程序也可以使用 X-KISS 来验证某个密码是否已被撤销。X-KRSS 定义了密码服务器上注册、撤销和恢复代管的密码的服务接口。

### 1.8 网络服务安全规范(WS-Security)

网络服务安全规范(Web Services Security, WS-Security)是一种提供在 Web 服务上应用安全的方法的网络传输协议。2004 年 4 月, OASIS 组织发布了 WS-Security 标准的 1.0 版本。WS-Security 描述了扩展 SOAP 消息来提供消息机密性和完整性<sup>[12]</sup>。该规范也提供和消息内容相关的通用安全令牌,该规范设计灵活,可支持多种令牌,如: Kerberos Tickets 和提供

消息鉴定的 X.509。该规范描述了怎样给二进制令牌编码、基于 XML 令牌的框架和怎样包含不透明加密密钥。WS-Security 还定义了防止消息重放的时间邮票。

WS-Security 将安全特性放入 SOAP 消息的消息头中,使用令牌的形式传递不同类型的声明(包括名称、身份、密钥、组、特权、功能等等)以及加密和数字签名信息。WS-Security 协议主要对 SOAP 消息的消息头部分做了扩展——加入了 wsse:Security 元素。其中针对安全的三个方面:身份认证、完整性和机密性分别定义了 Security Token, XML Signature 以及 XML Encryption Reference List 三个子元素。而在 SOAP 包中的需要加密的业务内容(通常会加密整个 SOAP 的主体)被经过 XML Encryption 处理过的元素(Encrypted-Data)所替代。这样就可以在应用层处理消息头,这样协议保证了端到端的安全。

WS-Security 包含了关于如何在 Web 服务消息上保证完整性和机密性的规约。应用程序开发者和协议设计者可以用不同的方式组合规范元素来实现不同的安全协议。

## 2 XML 安全体系在网络购物系统中的应用

在网上购物系统中,大量的信息采用 XML 文档形式(如:用户订单)来传递<sup>[13]</sup>。这时,可以采用 XML 加密的方式来保证敏感信息安全性,采用 XML 签名技术来保证文件收发的一致性和完整性。当用户接收到文件后,先验证 XML 签名,然后对文件进行解密,这样就得到了有权限的相关信息,为了实现传输安全,系统中文件都采用 SOAP 来传输。

在网络购物过程中要保证用户的注册的个人信息的保密性,即保护用户注册信息及其网络银行账户的信息不能泄漏,网络购物系统应具有下面的安全特性:

①保密性:系统应保证未经授权的第三方无法窃取相关信息,如:注册用户的信息、购物信息,以及银行账户信息。

②数据完整性:任何商品信息都必须是完整的,并且不能被管理方外的任何第三方修改。

③真实性:系统应该保证购物服务是可靠的、真实的,应对服务器端进行安全认证,防止伪装的购物进程提供服务。

④不可抵赖性:购物或者结算前应对用户进行安全认证,防止其他人伪装成某个注册用户进行订单或在线支付服务。

针对上述在线购物系统的安全性要求,采用文中提出的 XML 安全体系:采用 XML 加密保证购物中敏

感信息的保密性;采用 XML 签名来保证商品数据完整性;采用 XKMS 认证机制来保证不可抵赖性,由于介入了第三方的认证结构,同时也可以保证购物服务的真实性和可靠性。网上购物系统的安全架构如图 3 所示。

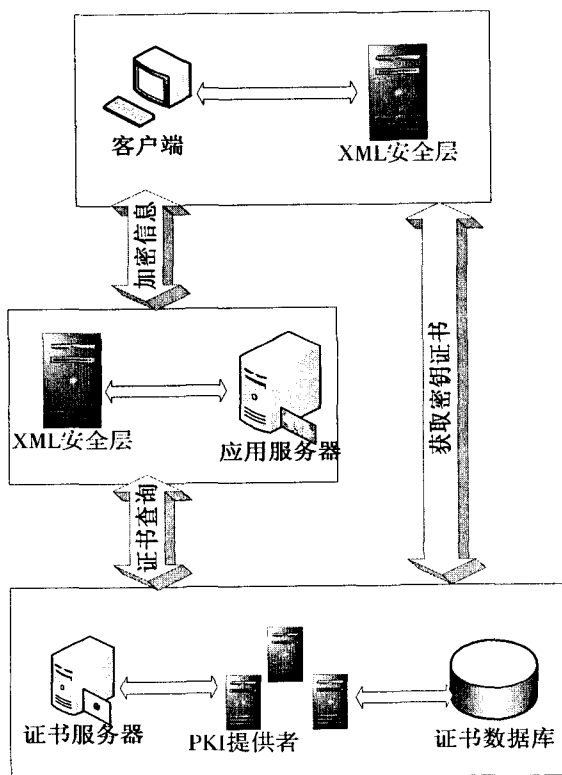


图3 系统安全架构图

网上购物系统的基本工作流程有4步:

①客户端向应用服务器发送信息时,它不能直接发送,必须通过 XML 安全层。首先,XML 安全层向 XKMS 证书服务器查询用户身份,成功后取得用户证书和密钥,然后根据证书和密钥对请求信息进行 XML 签名,最后将签名后的信息封装成 SOAP 包并发送给应用服务器端。

②应用服务器也不能直接处理接收的信息,它必须通过 XML 安全层来处理。XML 安全层先将 SOAP 包解封装,然后向 XKMS 证书服务器查询客户身份证书和密钥,再根据密钥对解封装后的信息进行 XML 解密,接着用证书解密后的信息进行验证签名操作,验证成功后将信息转发给应用服务器。

③收到信息后,应用服务器端通过 XML 安全层发送应答信息,它先将信息利用证书签名,再用密钥加密、封装成 SOAP 包后发送给客户端的 XML 安全层。

④收到应答信息后,客户端的 XML 安全层进行解封装、解密、验证签名等步骤后,得到原始的应答信息并转发给客户端。

### 3 结束语

XML 正逐步成为 Internet 数据交换的事实标准,如何利用现有的安全技术来开发 XML 应用已经成为人们研究的热点。虽然许多机构都提出了相应的安全规范,但是由于这些规范都是针对某个方面的安全问题的,要在实际开发中用好这些规范仍是一个急需解决的问题。文中的工作试图建立针对各种应用系统安全的一个通用的防范体系,集中探讨了使用的各种安全技术,如 XML 加密、签名、密钥管理规范的特点及其防范重点,对各种即将建立的应用系统的安全防护起到了指导作用。

#### 参考文献:

- [1] Dournaee B. XML 安全基础[M]. 北京:清华大学出版社, 2003.
- [2] Gudgin M, Hadley M, Jean - Jacques M, et al. SOAP Version 1.2. [EB/OL]. 2001 - 07 - 09. <http://www.w3.org/TR/2001/WD-soap12-20010709/>.
- [3] Eastlake D, Reagle J. XML Encryption Syntax and Processing Version 1.1. [EB/OL]. 2009 - 07 - 30. <http://www.w3.org/TR/2009/WD-xmlenc-core1-20090730/>.
- [4] 耿建勇, 鲁士文. 基于 XML 加密规范的安全数据交换的实现[J]. 计算机应用与软件, 2005, 22(2): 99 - 101.
- [5] Eastlake D, Reagle J, Solo D, et al. XML Signature Syntax and Processing (Second Edition). [EB/OL]. 2008 - 06 - 10. <http://www.w3.org/TR/2008/REC-xmlsig-core-20080610>.
- [6] Cantor S, Kemp J, Philpott R, et al. Security Assertion Markup Language(SAML) V2.0. [EB/OL]. 2005 - 03 - 01. <http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>.
- [7] Moses T. eXtensible Access Control Markup Language (XACML) Version 2.0. [EB/OL]. 2005 - 02 - 01. <http://docs.oasis-open.org/xacml/2.0/access-control-xacml-2.0-core-spec-os.pdf>.
- [8] 郑起莹, 沈建京. 基于 XACML 的 Web 服务安全访问控制模型[J]. 计算机工程与设计, 2007, 28(16): 3832 - 3836.
- [9] 陈利颐. XrML 实现第二代数字权益管理机制[J]. 上海交通大学学报, 2003, 37(增刊): 198 - 202.
- [10] 张亚忠, 徐良贤. XML 密钥管理规范[J]. 计算机工程, 2004, 30(21): 313 - 314.
- [11] 顾韵华, 傅德胜, 王 兴. XML 安全技术分析与应用[J]. 计算机科学, 2009, 36(5): 118 - 120.
- [12] Nadalin A, Kaler C, Monzillo R, et al. Web Services Security: SOAP Message Security 1.1. [EB/OL]. 2006 - 02 - 01. <http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>.
- [13] 刘小宽, 许敏佳. 基于 XML 的网络安全技术[J]. 计算机工程, 2006, 32(2): 164 - 166.