

# 一种改进的 XML 签名技术的研究及其实现

乔加新

(安徽财经大学 信息工程学院, 安徽 蚌埠 233041)

**摘要:**在深入分析 XML 签名规范的基础上,针对 XML 签名规范在解决业务链的多方通信过程中 XML 敏感数据安全问题不足,提出了一种改进的 XML 签名技术,研究实现它们的工作原理。同时设计了基于 XML 改进签名技术的 XML Schema,并给出了发送方 XML 整体签名和各接收方分别验证的实现过程,可以很好地满足业务链中一方对所提供给它各方的多个 XML 敏感数据进行整体签名、部分验证的要求,保证了这些数据在多方通信过程中的确定性、完整性和不可否认性。

**关键词:**XML 签名;XML 整体签名;XML 分别验证

**中图分类号:**TP393

**文献标识码:**A

**文章编号:**1673-629X(2007)11-0131-04

## Research on an Improved XML Signature Technology and Its Implementation

QIAO Jia-xin

(School of Information Engineering, Anhui University of Finance & Economics, Bengbu 233041, China)

**Abstract:** In thorough analysis XML signature, presents an improved XML signature technology to solve the XML data security problem which cannot be perfectly solved with XML signature specification in multi-communication of the operation chain. Researches its working principle. XML Schema based on an improved XML signature is designed. Gives the process of XML united-signature at sender and partial-validation at acceptor. It can resolve the authenticity, integrity and non-repudiation of the data in the multi-operation chain based on the XML communication.

**Key words:** XML signature; XML united-signature; XML partial-validation

## 0 引言

可扩展置标语言(eXtensible Markup Language, XML)作为一种用来描述数据的标记语言,具有对数据进行统一描述的强大功能;同时可扩展性、结构化语义以及平台无关性的特点充分满足了互联网和分布式异构环境的需求,成为网络数据传输和交换的主要载体,有力地推动了电子商务等网络应用的发展<sup>[1]</sup>。

在以 Web 服务(Web Services)为架构的业务流程中的业务链的多方通信过程中往往会存在一方要提供不同的信息给多方,同时下游业务方所需的信息可能要经过上游业务方的多次转发,一份文件可能会经过很多中间人,这迫使上游传送文件的业务方必须信任这些中间人对于该份文件内容的处理。根据 XML 签名规范,消息的发送方可以通过一次签名同时保证所

有信息的完整性,但是消息接收方只能将这所有的信息作为一个整体进行验证,而不能得知自己的那部分信息是否完整。要分别判断各自的那部分信息的完整性,只能通过对这些信息分别签名,但是这又牺牲了效率,即只能实现对信息进行整体签名、整体验证,部分签名、部分验证。针对上述问题,在 XML 签名技术的基础,提出 XML 整体签名技术,具有信息发送方对 XML 文档的整体签名、信息接收方分别验证的功能,同时中间业务方可以根据业务的需要对接收到的 XML 文档进行增加或删除内容,也增加了整个业务处理的灵活性。

## 1 XML 签名技术

XML 签名可以用于对包括 XML 文档在内的任何内容进行签名,被签名的数据内容称为数据对象。数据对象的签名结果加上数字签名信息以 XML 元素的形式存放在文档中,称为签名元素。签名元素为 Signature,它是 XML 签名的核心标记,Signature 元素速记

收稿日期:2007-02-06

基金项目:安徽省教育厅自然科学基金项目(2006KJ049B)

作者简介:乔加新(1975-),男,安徽蚌埠人,讲师、硕士研究生,研究方向为计算机控制、网络安全。

形式的结构如下所示<sup>[2]</sup>:

<Signature ID? > '数字签名的根元素'  
<SignedInfo> '签名信息核心元素'  
< Canonicalization Method/> '规范化方法描述元素'  
< SignatureMethod/> '签名算法'  
(< Reference URI? > '元素描述被签名对象的信息'  
(< Transforms>)? '签名数据对象来摘要算法'  
< DigestMethod> '签名数据对象的签名算法'  
< Digest Value> '资源内容与签名者密钥绑定的机制'  
</Reference>)+ '出现一次或多次'  
</SignedInfo>  
< SignatureValue> '生成的数字签名值'  
(< KeyInfo>)? ', 可选元素, 验证签名的密钥'  
(< Object ID? >)\* '可选元素, 包括数据对象其它子元素'  
</Signature>

当 XML(或其中的一部分)经过数字签名之后,得到的 XML 签名用<Signature>元素表现出来,根据原文档与这个数字签名的关系可以将 XML 签名分为以下几种类型:

(1)封外签名(Enveloping signature)。<Signature>元素中包含了被签名数据对象元素。被签名的元素成为了<Signature>元素的子元素。

(2)封内签名(Enveloped signature)。<Signature>元素成为被签名数据的子元素。<Signature>元素通过它的子元素——<Reference>元素提供的信息引用被签名的元素。

(3)分离签名(Detached signature)。<Signature>元素与被签名的元素各自独立存在。被签名的元素和<Signature>元素可以同属于一个文档,或者<Signature>元素也可以在另一个完全不同的文档中。

## 2 改进的 XML 签名技术

采用 XML 传输数据时,发送端 A 产生需要提供给其他各业务方的明文信息——Info(A-B)、Info(A-C)、Info(A-D)、…、Info(A-X)、…、将这些信息放在一个 XML 文档中,使用改进的签名技术对 XML 文档进行整体签名,然后发送给各消息接收方<sup>[3~5]</sup>。为了实现数据确认性、完整性以及不可否认性,下面分别研究它们的工作原理。

信息发送端 A 改进签名的工作原理如图 1 所示,

其具体实现过程为:

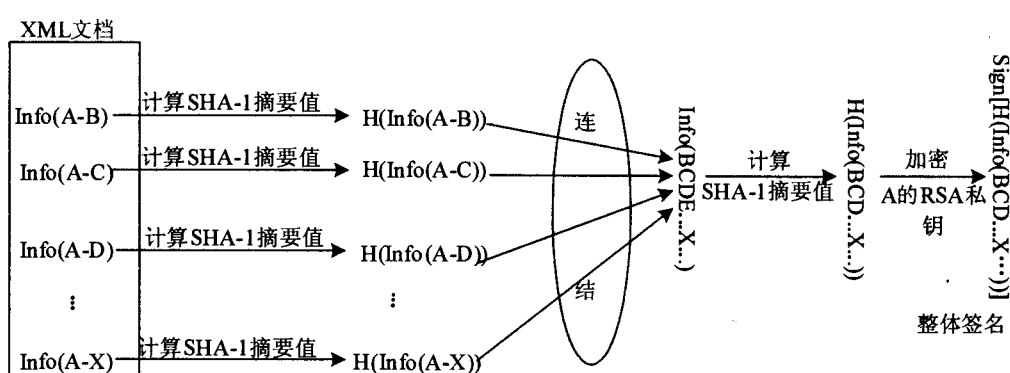


图 1 改进签名工作原理

1)信息发送端 A 使用 SHA-1 摘要算法分别生成这些信息的摘要,记为: $H(\text{Info}(A-B))$ ;  $H(\text{Info}(A-C))$ ;  $H(\text{Info}(A-D))$ ; …;  $H(\text{Info}(A-X))$ ; …。

2)连结所有这些敏感信息的摘要值:Info(BCD…X…),对其进行 SHA-1 摘要计算,生成这些连结信息的摘要值,记为  $H(\text{Info}(\text{BCD}\cdots\text{X}\cdots))$ 。

3)使用自己的 RSA 私钥对  $H(\text{Info}(\text{BCD}\cdots\text{X}\cdots))$  进行加密,生成 Info(BCD…X…)的签名值,记为:Sign[H(Info(BCD…X…))].即为这些信息的整体签名。

各信息接收方所得到的信息可由 A 方直接发送,也可以是它的业务上家转发,其中某一方(X)得到 A 方提供给自己的那部分 Info(A-X),其他各方信息的摘要:  $H(\text{Info}(A-B))$ 、 $H(\text{Info}(A-D))$ 、…; 整体签名值:Sign[H(Info(BCD…X…))],为了保证接收信息的确认性、完整性和不可否认性,接收方需要对信息进行分别验证,分别验证的工作原理如图 2 所示,其具体过程为:

(1)接收方 X 对 Info(A-X)进行 SHA-1 摘要计算,得到 Info(A-D)的摘要值: $H(\text{Info}(A-D))$ ;

(2)将  $H(\text{Info}(A-X))$ 与接收到  $H(\text{Info}(A-B))$ 、 $H(\text{Info}(A-C))$ 、 $H(\text{Info}(A-D))$ 、…相连接,得到连结值 Info(BCD…X…);

(3)对连结值 Info(BCD…X…)进行 SHA-1 的摘要计算,得到摘要值  $H(\text{Info}(\text{BCD}\cdots\text{X}\cdots))$ ;

(4)X 方使用 A 的公钥对 Sign[H(Info(BCD…X…))]进行解密,得到  $H(\text{Info}(\text{BCDE}\cdots\text{X}\cdots))$ 。将这两个  $H(\text{Info}(\text{BCD}\cdots\text{X}\cdots))$  进行比较,若相同,则表明 Info(A-X)信息是由 A 提供的,而且没有被篡改。

## 3 改进 XML 签名技术的实现

在 XML 签名规范的基础上对 XML 整体签名的语法和处理规则进行实现,将 XML 整体签名用 Unit- edSignature 元素来表示,定义了如下速记形式的结构:

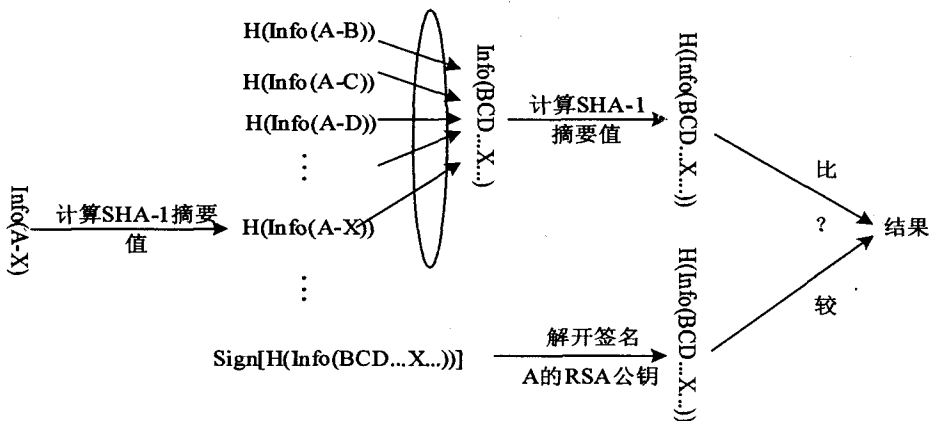


图 2 分别验证工作原理

个业务方的信息的摘要值及相关信息,包括两个子元素——DigestInfo 元素和 DigestValue 元素。DigestInfo 表示生成摘要的相关信息, DigestValue 表示摘要值,其中 DigestValue 的类型是 ds: DigestValueType。SubDigest 元素有两个属性——Id 属性和 To 属性, To 属性的值表示该

SubDigest 元素应由“谁”来处理。

(4) DigestInfo 元素。DigestInfo 表示生成摘要的相关信息,包括三个子元素——CanonicalizationMethod 元素、DigestMethod 元素和 DigestReference 元素。其中 CanonicalizationMethod 元素表示规范化计算摘要数据对象的算法信息,其类型为 ds: CanonicalizationMethodType; DigestMethod 元素表示摘要算法的信息,其类型为 ds: DigestMethodType; DigestReference 元素表示被计算摘要的数据对象信息。

(5) DigestReference 元素。DigestReference 元素表示被计算摘要的对象的信息, URI 属性和 ds: Transforms 元素用来描述如何得到被计算摘要的内容。可选的 ID 属性可以允许从其他地方指向该 DigestReference 元素。

(6) Signature 元素。其类型是 ds: SignatureType, 用来表示整体签名的签名信息和值。其中 Reference 元素的子元素 Transforms 用来表示如何得到那些要被连接的所有的摘要值, DigestMethod 和 DigestValue 分别表示对连接值的摘要算法和摘要值; SignatureMethod 元素表示整体签名的签名算法; SignatureValue 元素表示整体签名值。

(7) UnitedSignatureObject 元素。其类型是 ds: Object, 用来放置其他信息,可能包括数据对象、时间戳等。

### 3.2 改进 XML 签名实现过程

在 XML 文档信息发送方,根据 XML Schema 构建 XML 整体签名文档,其实现过程主要为:

(1) 设计 SubDigest 元素。包括选择摘要计算数据对象,规范化该数据对象,选择摘要算法,计算摘要值,设计 DigestInfo 元素;设计指定规范化数据对象算法的 ds: CanonicalizationMethod 元素,设计表示摘要算法的 ds: DigestMethod 元素,设计表示如何得到摘要计算数据对象的 DigestReference 元素(包括指定表示数据对象的引用属性 URI 和表示转换列表的子元素 ds:

```
<UnitedSignature Id? > '整体签名根元素
  <SubDigests> '各信息集合元素
    (<SubDigest id? > '各信息元素
      <DigestInfo> '生成摘要的相关信息
        <DigestReference (URI=? )? > '生成摘要的相关信息
          (<Transforms>) * '如何得到被计算摘要的内容
        </DigestReference>
      </DigestInfo>
      <DigestValue>
    </SubDigest>) +
  <ds:Signature> '整体签名的签名信息和值
  <UnitedSignatureObject> * '用来放置其他信息
</UnitedSignature>
```

UnitedSignature 元素是 XML 整体签名的核心元素,包括 SubDigests, Signature 和 UnitedSignatureObject 子元素。SubDigests 元素包括多个 SubDigest 子元素, SubDigest 代表某信息的摘要信息; Signature 元素包含联接摘要信息,以及整体签名信息和值; UnitedSignatureObject 元素放置其他信息,可能包括数据对象、时间戳等。

### 3.1 改进 XML 签名的 XML Schema 设计

进行 XML 模式设计时,相对于 DTD 文档, XML Schema 具有很强的描述能力、扩展能力和处理维护能力,又因为 XML 整体签名是基于 XML 签名技术的, XML 整体签名文档的 XML 模式要在 XML Signature 的 XML 模式的基础上扩展,采用 XML Schema 来描述 XML 整体签名文档的元素,包括以下内容<sup>[6~8]</sup>:

(1) UnitedSignature 元素。UnitedSignature 元素是 XML 整体签名的根元素,有三个子元素——SubDigests 元素、Signature 元素和 UnitedSignatureObject 元素。

(2) SubDigests 元素。SubDigests 元素表示发送给所有业务方的摘要信息,至少包含一个 SubDigest 元素。SubDigests 元素必须出现而且只能出现一次。

(3) SubDigest 元素。SubDigest 元素表示发送给某

Transforms); 标明此元素应交给哪个业务方处理, 用业务方的代号来表示 To 属性的值。设计 DigestValue 元素。

(2) 将各个 SubDigest 元素放在一起, 生成 SubDigests 元素。

(3) 设计 ds:Signature 元素(其中, 用 ds:Reference 元素来表示需要连接的所有的子摘要和联接摘要值; 用 ds:SignatureValue 元素表示整体签名值)。

(4) 设计 UnitedSignatureObject 元素。用来放置其他信息, 包括数据对象、时间戳等。

(5) 设计 UnitedSignature 元素。

### 3.3 XML 分别验证实现过程

各消息接收方收到 XML 整体签名文档以及自己感兴趣的信息, 根据 XML Schema 分别验证自己接收数据的完整性和发送者身份认证。具体实现过程:

(1) 从 SubDigests 元素中通过 SubDigest 元素的 To 属性值找到本业务方应处理的那些 SubDigest 元素。

(2) 通过 SubDigest 元素的 DigestInfo 子元素的 DigestReference 元素得到被计算摘要的数据对象。其间, 要通过 DigestReference 的 URI 属性表示的数据对象引用和子元素 ds:Transforms 元素表示的转换列表得到目标数据对象。

(3) 根据 Digest 元素所给出的规范化算法规范化上面所得的数据对象, 并根据 Digest 元素给出的摘要算法计算规范化后的数据对象的摘要值。

(4) 用此摘要值替换 DigestValue 元素的内容。

(5) 验证 ds:Signature 元素。

(上接第 130 页)

动程序返回的只是记录, 需要对它们进行再处理, 因此, 还需要缓冲发出数据访问的对象的信息, 以及其他一些额外的信息, 为应用层数据型对象在模式映射层的组装预备了必要的信息, 这个过程称为数据访问结果的半格式化。

(4) 低层访问执行者。

低层访问执行者接收 SQL 语句<sup>[6]</sup>, 访问数据库, 并把结果半格式化到结果缓冲。

### 3 结束语

对象模式到关系模式转换的软件框架给开发者一个面向对象的编程视图, 利用软件框架提供的 API 可以对关系数据库进行应用层对象的直接存取, 大大提高了软件开发效率, 并可以在对数据不迁移的情况下

### 4 结束语

设计实现的一种改进的 XML 签名技术具有整体签名、分别验证的功能, 解决了基于 XML 通信技术的业务链中多方通信时的身份认证和 XML 数据完整性、交易防抵赖的保护。它所具有的技术优势使其在以电子商务为代表的网络应用中有很好的前景。

#### 参考文献:

- [1] Harold E R. XML 宝典[M]. 马云, 钟萍等译. 北京: 电子工业出版社, 2002.
- [2] W3C. XML - Signature Syntax and Processing[EB/OL]. 2002-02-12. <http://www.w3.org/TR/xmldsig-core/>.
- [3] Mertz D. 密码学简介: 第一部分[EB/OL]. 2002-04-26. <http://www-900.cn.ibm.com/developerWorks/cn/cnedu.nsf/security-onlinecourse-bytitle/>.
- [4] Mertz D. 密码学简介: 第二部分[EB/OL]. 2002-05-17. <http://www-900.cn.ibm.com/developerWorks/cn/cnedu.nsf/security-onlinecourse-bytitle/>.
- [5] Mertz D. 密码学简介: 第三部分[EB/OL]. 2002-05-24. <http://www-900.cn.ibm.com/developerWorks/cn/cnedu.nsf/security-onlinecourse-bytitle/>.
- [6] XML Schema Part 0: Primer. W3C Recommendation[EB/OL]. 2001-05-02. <http://www.w3.org/TR/xmlschema-0/>.
- [7] XML Schema Part 1: Structures. W3C Recommendation[EB/OL]. 2001-05-02. <http://www.w3.org/TR/xmlschema-1/>.
- [8] XML Schema Part 2: Datatypes. W3C Recommendation[EB/OL]. 2001-05-02. <http://www.w3.org/TR/xmlschema-2/>.

对系统进行升级。

#### 参考文献:

- [1] Johnson J L. Database: Models, Languages, Design[M]. 北京: 电子工业出版社, 2004, 5.
- [2] 赵致格, 王枯民, 雍俊海. 面向对象数据库中对象的存储和操作算法[J]. 计算机辅助设计与图形学学报, 1998, 10(1): 15-21.
- [3] 王学荣, 曾晓勤. 从面向对象数据库模式到关系数据库模式的转换[J]. 计算机工程与科学, 2003, 25(5): 100-107.
- [4] 毕南楠, 方昌始. 一种新的面向对象数据库建模框架[J]. 计算机与数字工程, 2006, 34(7): 67-70.
- [5] Blaha M, Premerlani W, Shen H. Converting OO Models into RDBMS Schema[J]. IEEE Software, 1994(1): 28-39.
- [6] 王学荣, 曾晓勤. 面向对象数据库的查询转换成关系数据库的查询[J]. 计算机工程与应用, 2002(20): 176-182.