XML 数字签名在电子公文交换中的应用*

罗 凌
(重庆师范大学 数学与计算机科学学院, 重庆 400047)

摘 要:本文探讨了 XML 数字签名的基本原理和语法格式以及 XML 数字签名与传统数字签名方法相比具备的优势,研究了其实现原理,然后在. NET 平台上实现了的 XML 数字签名,并将其运用到实际的办公自动化系统中,实现电子公文交换的安全性、完整性、不可否认性,而且由于 XML 数字签名自身的优势,使得数字签名更加灵活、实用。

关键词:XML;数字签名;电子公文
中图分类号:TP309 文献标识码:A 文章编号:1672-6693(2008)02-0046-04

我国电子政务建设已经走过了 10 年,它的广泛应用大幅度提高了各级政府和公共机构的工作效率,同时也带来了巨大的经济和社会效益。电子公文的交换是电子政务建设中一个重要的环节。电子公文通过网络传输,极大地提高了公文信息的传输速度和处理速度,从而大大提高了工作效率和信息资源的利用率。但是,由于网络具有联结形式的多样性、开放性、互连性等特征,致使网络易受黑客、恶意软件的攻击和病毒的入侵,造成电子公文信息的泄密、假冒、篡改、抵赖等诸多问题,因此,网上电子公文信息的安全性是一个至关重要的问题。

XML(EXtensible Markup Language,可扩展标记语言)被认为是网络数据交换和发布的标准格式,目前已广泛应用在应用程序之间交换数据的各种编程环境[1-4],如电子商务、电子政务等领域。作为 XML 应用的前提和基础的 XML 数据安全问题,也越来越受到人们的重视。针对 XML 特性开发的 XML 数字签名不仅可以像传统数字签名一样对任意类型的数据签名,保护数据的完整性、不可否认性以及提供身份鉴别,而且在处理 XML 文档签名的时候,表现出了许多传统数字签名所不可比拟的技术优势,从而满足更深层次的签名需求。

1 XML 数字签名

1.1 数字签名的工作原理

数字签名广泛应用在网络安全中,它以密码学为基础。密码学主要分为对称和非对称两大类,其区别在于加解密密钥是否相同。事实上,数字签名一般采用非对称密码算法。非对称密码是一种先进的密码思想,它采用一对数字相关的密钥来替代单个共享的私密密钥,以解决对称密码术的密钥交换和信任问题。在这个密钥对中,一个为私钥,另一个为公钥。私钥为用户私有,公钥通过某种机制公布,并且两者无关联(并非完全没有联系,是指从一个无法推得另一个)。由于它使用两种不同的密钥,因而称为非对称,并且因此可以用于消息认证和防抵赖。

在应用数字签名时,一般都会配合使用消息摘要算法,因为如果直接对原数据进行加密签名的话,会使签名十分冗长。所以先计算其摘要,再对摘要进行签名。消息摘要算法也是密码学中很重要的一个方面。它是一种单向函数,对原数据进行变换并获得摘要值(一般 512 位)。它的特点是攻击者无法针对一个摘要逆向生成产生此摘要的原数据,由此可知它是提供完整性服务的关键。

数字签名的具体工作原理如下。

1)被发送文件采用哈希算法对原始报文进行运算,生成报文摘要,不同的报文所得到的报文摘要各异,但对相同的报文它的报文摘要却是唯一的。

2)发送方用自己的私钥对摘要进行加密来形成发送方的数字签名。

3)这个数字签名将作为报文的附件和报文一起发送给接收方。

4)接收方首先从接收到的原始报文中用同样的算法计算出新的报文摘要,再用发送方的公钥对报文附件的数字签名进行解密,比较两个报文摘要,

* 收稿日期:2007-05-11 修回日期:2007-10-28
作者简介:罗凌(1976-),女,讲师,硕士,研究方向为网络信息系统、网络安全。

如果值相同,接收方就能确认该数字签名是发送方的。

1.2 XML 数字签名语法

XML 签名可以定义一系列 XML 元素,这些元素可以内嵌或以其他方式附加在任何 XML 文档中。这样,收件人可以验证收到的消息与发件人原本发送的消息是否相同。XML 签名的语法和处理规范是由 W3C 和 IETF 联合制定的。自 2002 年 2 月以来,它一直是正式的 W3C 推荐规范,并得到了广泛的应用。XML 签名的语法格式如图 1 所示(其中,"?"表示 0 次或 1 次出现,"+"表示 1 次或多次出现,"*"表示 0 次或多次出现)。

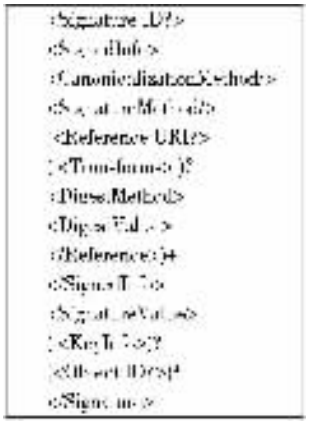

图 1 XML 数字签名的语法格式

其中 SignedInfo 是必需的,是实际签名的信息;CanonicalizationMethod 标识了一种算法,这种算法被用来规范化 SignedInfo 元素,然后该元素作为签名操作的一部分被编摘;SignatureMethod 是用于将已规范化的 SignedInfo 转换成 SignatureValue 的算法;Reference 元素都包括摘要方法和对已标识数据对象计算得出的摘要值,它还可能包括产生对摘要操作的输入的转换。Reference 的可选 URI 属性标识要签名的数据对象;Transforms 包括签名者用于数据对象的一系列转化;DigestMethod 是在应用 Transforms(如果已经指定它)之后对数据应用以产生 DigestValue 的算法。DigestValue 的签名是将资源内容与签名者密钥绑定的机制;KeyInfo 表示用于验证签名的密钥;Object 是可选元素,存储了封装签名或数据对象。

1.3 XML 数字签名和传统数字签名的比较

相对于 W3C 定义的 XML 数字签名,可以把其他不基于 XML 的数字签名称为传统数字签名(尽管这不是一个标准称谓)。基于 XML 特性开发的 XML 数字签名和传统数字签名相比,它们在处理任意类型的数据签名时,都能满足数据完整性、不可否认性、身份识别和认证等基本的安全要求。但是在处理 XML 文档签名时,XML 数字签名能够实现传统数字签名所不能实现的签名粒度,表现出强大的功能和技术优势。

1)待签数据的 URI 建模方式扩大了签名的作用范围,更符合分布式网络环境的资源特点。URI 可以引用任意数据类型的文档,不管这个文档是远程文档还是本地文档,甚至还可以引用一个 XML 文档的任意元素。所以利用 URI 不仅可以对整个 XML 文档签名,而且可以对 XML 文档的任意元素、甚至只对元素的内容签名,实现传统数字签名无法做到的细粒度签名,扩大签名的作用范围。

2)签名结果保持 XML 文档的结构,多种封装类型更便于数字签名的存储和管理。传统数字签名完全忽略了待签文档的数据类型以及内部数据结构,通常签名的结果只是返回一串二进制数据,没有特定的上下文信息,不具备足够的互操作性。而 XML 数字签名的结果返回一个 XML 元素,它把签名值以及所有的验证信息都用 < Signature > 元素及其子元素来表示,因此可以根据需要把 < Signature > 元素放入文档的任何位置而不会破坏 XML 文档的结构。根据签名元素和被签数据在同一 XML 文档中的位置关系,XML 数字签名定义了 3 种签名封装类型。当一个 XML 文档存在多个数字签名的时候,利用 XML 数字签名可以把多个数字签名保存在同一原始文档中,使存储和管理签名变得方便、快捷和高效。

3)签名密钥表示形式的语义清晰、易读,提高了签名的可移植性和自动验证的能力。XML 数字签名的主导设计思想是尽可能少地依赖某些用于处理签名的专用格式,以提高 XML 签名结果的可移植性。所以从一开始 XML 就尽量避开复杂、难读、难扩展的 ASN.1 表示形式,通过元素 < KeyValue > 及其子元素来简单清晰地表示签名密钥的所有信息。XML 数字签名不需其他专门工具,任何 XML 解析器都能解析 < KeyValue > 元素得到正确的签名密钥,提高了签名的可移植性和自动验证的能力,更能满足应用程序用 XML 来交换和发布网络数据的需要。

2 基于 XML 的数字签名在公文交换中的实现

电子公文在传输交换时,首先由发送方用户提

取自己的私钥,对要发送的 XML 格式的电子公文进行数字签名,生成数字签名的新的 XML 文档(文档中包含重要的数字签名后数据和进行解密的公钥)。接收方收到经过 XML 数字签名的 XML 文档后,首先提取文档中公钥进行解密,再和原始信息进行比较,如果一致说明该文档是完整的、没有被篡改的,则接收该电子文档;否则拒绝接收。XML 数字签名和验证的原理如图 2、3 所示。

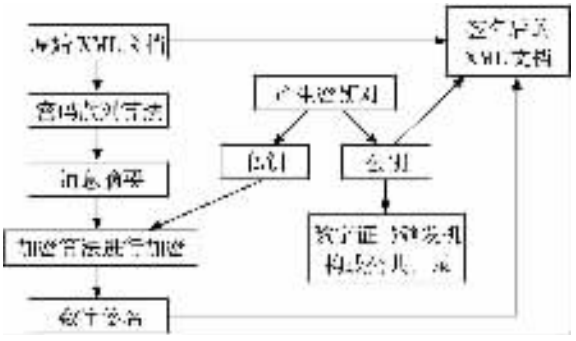

图 2　XML 数字签名

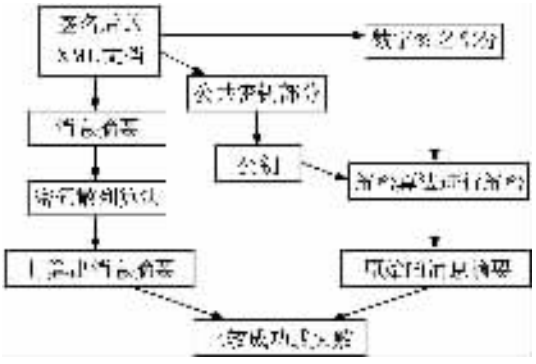

图 3　XML 数字签名的验证

由于目前的电子政务平台大都是基于 B/S 模式的,因此为了实现电子公文的 XML 数字签名和验证,本文采用了 ASP. NET 技术。ASP. NET 是建立在. NET Framework 之上的,. NET Framework 是一个安全、高性能与扩展性佳的运行环境[5]。ASP. NET 可以采用 VB、C#等模块化设计语言,并且在第一次执行时进行编译,之后的执行不需要重新编译就可以执行,所以执行速度比较快;ASP. NET 程序只能在服务器执行,客户端浏览器接收到的仅仅是 ASP. NET 程序执行后反馈的 HTML 文档。也就是说服务器端代码对用户是屏蔽的,代码的安全性比较高。XML 数字签名中使用的类在. NET Framework 中 System. Security. Cryptography. Xml 命名空间。这些类为 XML 签名提供了完整的支持,包括消息摘要、密钥对、数据加密等。

为了说明电子公文的 XML 数字签名的生成,首先给出一个用于电子公文交换的 XML 文件片段(test. xml)。

```
< ?Xml version = "1.0" >
<电子公文 >
  <标题 >关于环境保护的通知 </标题 >
  <发送部门 >生产办 </发送部门 >
  < 附件 > http ://localhost/file/关于环境保护的通知. doc
</附件 >
  ……
</电子公文 >
```

对于这个 XML 文件,可以对整个文件进行 XML 数字签名,但鉴于文件中“附件”的信息是至关重要的,因此仅仅考虑对“附件”中信息进行 XML 数字签名,即细粒度签名[6-7]。实现 XML 数字签名的代码如下。

1)从 XML 文件中读取私钥信息。

```
Dim myreader As New StreamReader(xmlprivatekeyfile) ' xml-
privatekeyfile 是保存了用户私钥的 XML 文件
    Dim str1 As String = myreader. ReadToEnd
        myrsa. FromXmlString(str1)
      myreader. Close()
mysignedxml. SigningKey = myrsa
```

2)保存要签名数据的 XML 签名的对象元素。

```
Dim dataobject As New DataObject
    dataobject. Data = newxml. ChildNodes
      dataobject. Id = " http ://localhost/file/关于环境保
护的通知. doc "
          mysignedxml. AddObject(dataobject)
      Dim myreference As New Reference
      myreference. Uri = " http ://localhost/file/关于环境
保护的通知. doc "
    mysignedxml. AddReference(myreference)
Dim mykeyinfo As New KeyInfo
```

3)从用户私钥导出公钥。

```
Dim publickey As New RSAKeyValue(myrsa)
    mykeyinfo. AddClause(publickey)
        mysignedxml. KeyInfo = mykeyinfo
    mysignedxml. ComputeSignature() ' 计算签名
Dim myxmlsignature As XmlElement
```

4)将 XML 数字签名应用到 XML 文件。

```
myxmlsignature = mysignedxml. GetXml
    myxmldocument = New XmlDocument
      myxmldocument. PreserveWhitespace = True
Dim myxmlnode As XmlNode = myxmldocument.
ImportNode(myxmlsignature, True)
        newxml. AppendChild(myxmlnode)
          newxml. Save(signedfilename)
```

当公文接收方在收到公文后首先进行公文的验

证。验证代码如下。

```
myxmldoc. Load(signedfilename)
    Dim mysignedxml As New SignedXml(myxmldoc)
    Dim mynodelist As XmlNodeList = myxmldoc.
GetElementsByTagName("Signature", "http://www.w3.org/
2000/09/xmldsig#")
    Dim myxmlelement As XmlElement = mynodelist(0)
    mysignedxml. LoadXml(myxmlelement)
  If (mysignedxml. CheckSignature) Then
  Response. Write("验证正确!")
 Else
Response. Write("验证错误!")
End If
```

3 结论

电子公文交换的安全性在电子政务建设中占据着重要的位置,本文探讨了 XML 数字签名的原理、优势和实现机制。利用 XML 数字签名不仅可以实现电子公文交换的安全性、完整性、不可否认性,而且由于 XML 数字签名自身的优势,使得数字签名更加灵活、实用。在为某单位开发的办公自动化系统中已经应用了该技术,取得了较好的效果。

参考文献:

[1] THORSTEINSON P.. NET 安全性与密码术[M]. 北京:清华大学出版社,2004.

[2] 刘华,周熙襄,钟本善. 利用 Java 和 XML 在 Lotus Domino Web 环境中实现跨平台数据交互[J]. 四川师范大学学报(自然科学版),2003,26(3):327-330.

[3] 曾莉红. 基于 Visual. NET 技术的网络课件的开发与设计[J]. 重庆师范大学学报(自然科学版),2005,22(1):27-30.

[4] DALVI D,GRAY J.. NET XML 高级编程[M]. 英宇,林琪,费广正,等译. 北京:清华大学出版社,2002.

[5] 陈惠贞,陈俊荣. ASP. NET 程序设计[M]. 北京:中国铁道出版社,2003.

[6] 奥海炜,伏总强. XML 数字签名在电子政务中的作用[J]. 西部探矿工程,2005(10):237-239.

[7] 叶晓彤. 基于 XML 部分加密的局部安全通信的实现[J]. 四川师范大学学报(自然科学版),2003,26(4):433-436.

Application of XML Digital Signature in the Exchange of Electronic Documents

LUO Ling

(College of Mathematics and Computer Science, Chongqing Normal University, Chongqing 400047, China)

Abstract: Electronic documents exchange is an important thing in E-government construction. It improves the translation and the handling speed of electronic documents which are translated through network. However, because of the diversity, opening and interconnection of network's connection way, electronic documents are easily attacked by hackers and hostile software. It results in the fact that the data of electronic documents may be filched, counterfeited, modified and disavowed. So the electronic documents security is the most important thing. XML has been recorded as network data exchanging and publishing standard. It has been applied in several programming environment of data exchange between application software, such as E-business and E-government. The paper discusses basic theory and syntax format of XML and the advantage of XML digital signature comparing with traditional digital signature, researches its realization theory then realizes XML digital signature on NET framework, also applies it to actual OA. It realizes the security, integrality, impossible disavowal of electronic documents interchange, meanwhile makes the digital signature more flexible and practical.

Key words: XML; digital signature; electronic documents

(责任编辑 游中胜)