基于 SOAP 协议的 Web Services 安全性扩展实现*

李慧盈，张长海，李德昌
(吉林大学 计算机科学与技术学院，吉林 长春 130012)

摘　要：通过对 Web 服务的架构进行分析，研究了建立安全性模型的基本途径。基于 Web 服务安全性模型的主体是 SOAP 的安全性，从而提出了对于 SOAP 进行安全扩展以达到信息安全交换的一种实现方法，该方法确保了网络服务的完整性和安全性。

关键词：Web 服务；简单对象访问协议；可扩展标记语言；安全套接字层；数字签名
中图法分类号：TP311.133.1　　**文献标识码**：A　　**文章编号**：1001-3695(2006)01-0106-02

Realize on SOAP-based Security of Web Services

LI Hui-ying, ZHANG Chang-hai, LI De-chang
(College of Computer Science & Technology, Jilin University, Changchun Jilin 130012, China)

Abstract: Through analyze the framework of Web Services, the fundamental principles of building security model are studied. Since the main part of Web Services security model is SOAP security, a way to solve safety SOAP-based information exchange is provided through extending the security of SOAP that ensures the integrity and security of new and existing Web Services.
Key words: Web Services; SOAP; XML; SSL; Digital Signature

为了能在任何时间、任何地点访问到服务，软件就必须在网络上提供，并且不能受平台限制。所以用 XML 封装数据和对象，用 SOAP(简单对象访问协议)作为方法调用协议的 Web 服务就成了最佳的选择。有了 Web 服务，Internet 才能真正地为企业应用、商业应用乃至个人的桌面应用提供最佳的互连交互作用。虽然诸如 SOAP，WSDL(Web 服务描述语言) 和 UDDI(统一描述、发现和集成) 之类的 Web 服务核心技术能够使连接应用程序所必需的集成基础架构简化和标准化，但它们并不直接提供保护企业资产所必需的安全性机制。也就是说，Web 服务可以让你通过因特网连接把自己所拥有的功能当作服务出售给其他人。可是一旦我们把功能作为 Web 服务发布在因特网上，那么任何人显然都能使用它，反过来，如果要阻止某些人使用你的 Web 服务(保证只有付费顾客能使用你的 Web 服务) 又该怎么办呢？正是认识到了这一点，开发一个全面 Web 服务的安全性模型至关重要。

1　Web Services 架构

国际权威组织 W3C(世界互联网联盟) 给出了 Web Services的标准定义：Web Services 是被 URI 确定的一个软件应用，它的接口和封装是可以被 XML 定义描述和发现并且支持与使用 XML 消息通过网络协议的其他软件应用进行直接交换[1]。Web Services 技术是建立在 XML，SOAP，WSDL，UDDI 基础之上的分布式应用架构[2,3]。Web Services 整体架构如图 1 所示。

图 1 是从分层的角度来描述 Web Services 的整体架构。与网络的分层结构相同，上一层需要下一层的支持，而安全性、可管理性、服务质量则需要在各个层次都有所体现。安全机制对于松散耦合的对象环境非常重要，因此需要对诸如授权认证、数据完整性(如签名机制)、消息源认证以及事务的不可否认性等进行详细研究。

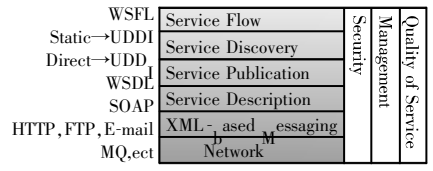

图 1　Web Services 的整体架构

2　Web Services 安全性模型

Web 服务安全性模型(图 2) 引入了一个由各个相互联系的规范组成的集合[4]，这些规范描述了把安全性功能程序放到 Web 服务环境中的方法。体系结构被设计成允许对规范进行混合匹配，使实现者仅能够部署他们需要的那部分。这些规范中的第一个 Web 服务安全性(WS-Security) 文档提供了把消息完整性和机密性功能程序添加到 Web 服务中所必需的基本元素，并且提供把安全性令牌[5](如数字证书) 关联到 SOAP 消息的方法。

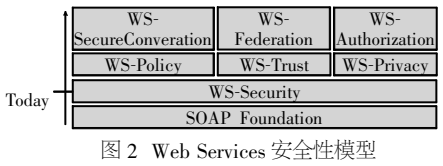

图 2　Web Services 安全性模型

(1) 初始规范

①WS-Security。该规范描述如何向 SOAP 消息附加签名和加密报头。另外，它还描述如何向消息附加安全性令牌(包括二进制安全性令牌，如 X.509 证书和 Kerberos 票据)。

收稿日期：2004-11-20；修返日期：2005-03-08
基金项目：国家“973”计划资助项目(G1999045708)

②WS-Policy。该规范描述了决定企业应用程序必须如何与另一个企业应用程序集成在一起的业务、安全性、隐私权和信任策略。

③WS-Trust。该规范描述了如何在 Web 服务环境中建立企业之间的信任关系。

④WS-Privacy。该规范描述了如何把隐私权策略以及首选项与 Web 服务相关联。

(2) 后继规范

①WS-SecureConversation。该规范描述了如何将集合消息作为更复杂的企业事务的一部分安全地交换。

②WS-Federation。该规范描述了一个模型,该模型用于把不兼容的安全性机制或部署在不同域中的、类似的机制集成在一起。

③WS-Authorization。该规范描述了如何在 Web 服务基础架构中提供应用程序授权请求和决定。

Web 服务安全性模型的主体是通过向 URI 标志的服务端点发送 SOAP 消息、请求特定的操作并接收 SOAP 消息响应(包括错误的暗示)访问 Web 服务[6]。那么 SOAP 的安全性就成为 Web 服务安全中至关重要的部分。

3　SOAP 安全性扩展

SOAP 是在分散或分布式的环境中交换信息的简单的协议,是一个基于 XML 的协议。它包括四个部分: ①SOAP 封装(Envelop),封装定义了一个描述消息中的内容是什么,是谁发送的,谁应当接收并处理它以及如何处理它们的框架; ②SOAP 编码规则(Encoding Rules),用于表示应用程序需要使用的数据类型的实例; ③SOAP RPC 表示(RPC Representation),表示远程过程调用和应答的约定; ④SOAP 绑定(Binding),使用底层协议交换 SOAP 信封的约定。

图 3 是 SOAP 的消息结构和安全机制[7]。图③中①代表传输层的安全(如 HTTPS)用来确认身份。②代表 SOAP 的消息安全机制,包括授权认证、数据完整性和机密性。③代表被分出来的 SOAP 体(Body)的安全性。

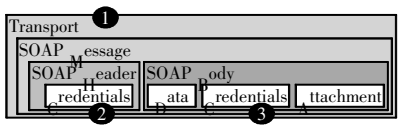

图 3　SOAP 的消息和安全机制

由于 SOAP 层安全处于传输层和应用层之上[6],因此对 SOAP 层的安全性进行扩展,把关于安全的基本要求应用到整个的 SOAP 信息中,包括 SOAP 头(Header)以及 SOAP 体(Body),是解决 Web 服务安全性的一个重要策略。而对于 SOAP 进行安全性扩展,数字签名(Digital Signature)又是一个很好的解决方案。

4　数字签名的实现

数字签名是使用加密算法制成的数字标签,此标签通过密钥制成,而且不访问密钥,就不可能仿制标签。通常使用私钥签名文件,并使用同一私钥打开别人发送来的加密文件。数字签名能够实现以下功能: 收方能够证实发方的身份; 发方事后不能否认所发送的报文; 收方或非法者不能伪造、窜改报文。

现在对 SOAP 进行扩展,在 SOAP 的头元素的扩展命名空间中加入数字签名。

```
< SOAP-ENV: Envelope
xmlns: SOAP-ENV = " http: / / schemas. xmlsoap. org/ soap / envelope/" >
< SOAP-ENV: Header >
< SOAP-SEC: Signature
xmlns: SOAP-SEC = " http: / / schemas. xmlsoap. org/ soap / security/ 2000-
12" >
< ds: Signature xmlns: ds = " http: / / www. w3. org /2000 /09/ xmldsig
#" >
< ds: Reference URI = " #Body" .. / >
< / ds: Signature >
< / SOAP-SEC: Signature >
< / SOAP-ENV: Header >
< SOAP-ENV: Body
xmlns: SOAP-SEC = http: / / schemas. xmlsoap. org/ soap / security /2000-12
SOAP-SEC: id = " Body" >
< m: GetLastTradePrice xmlns: m = " some-URI" >
< m: symbol > IBM < / m: symbol >
< / m: GetLastTradePrice >
< / SOAP-ENV: Body >
< / SOAP-ENV: Envelope >
```

SOAP 头元素的扩展命名空间中加入安全特征,通过扩展,在方案中加入一个新的元素,这个元素在 Schema 中可以不用改变。如果要在 SOAP 1.1 协议中进行加密性扩展,可以在命名空间中引入适当的标准实现,如 XML 加密算法(XML Encryption)[6] 等。SOAP 头元素 SOAP-SEC 使用的 XML 命名空间[8] 如下: http: / / schemas. xmlsoap. org/ soap/ security/ 2000-12,命名空间的前缀 "SOAP-SEC" 就指向这里。

5　结束语

随着 Web 服务应用的日益广泛,对 Web 服务增加安全性的需要就变得更加明了。本文阐明了一个集成的 Web 服务安全性模型的原理并通过扩展和利用(而不是代替)现有的安全性技术,给出了实现一个基于 SOAP 安全信息交换的方法。SOAP 信息也可以使用其他安全技术,更多的 SOAP 安全规范正在不断地研究和完善之中。随着 SOAP 安全性的增强,它为 Web 服务高层规范提供了一个更安全的消息传送通道。

参考文献:

[1] eb Services Description Requirements[EB/OL]. http: / / www. w3. org/ TR/ 2002/ WD-ws-desc-reqs-20021028, 2002-10.

[2] Judith M. Myerson. Web Services Architectures[M]. Chicago: Tect Publisher, 2002.

[3] Web Services and Application Frameworks[EB/OL]. http: / / www. webservicesarchitect. com/ content/ articles/ samtani04print. asp, 2002-03.

[4] A Joint Security Whitepaper from IBM Corporation and Microsoft Corporation[EB/OL]. http: / / www. ibm. com/ developerWorks/ WebServiceZone, 2002-04.

[5] SOAP Security and Reliability, Issues and Solutions[EB/OL]. http: / / www-10. lotus. com/ ldd/ sandbox. nsf/ f72790492fc99f0e852567ec006aa062/ e111cb977249584385256b7a00082b1b/ $FILE/ ad307. pdf, 2002-03.

[6] Building Secure Web Services with Microsoft SOAP Toolkit 2. 0[EB/OL]. http: / / alphaworks. ibm. com/ tech/ webservicestoolkit, 2001-07.

[7] W3C SOAP Data Signature Draft[EB/OL]. http: / / www. w3. org/ TR/ SOAP-dsig, 2002-11.

[8] XML-Signature Syntax and Processing[EB/OL]. http: / / www. w3. org/ TR/ 2000/ CR-xmldsig-core-20001031, 2000-10.

作者简介:

李慧盈(1978-),女,吉林长春人,博士研究生,主要从事计算机软件理论、网络及应用技术研究; 张长海(1948-),男,吉林长春人,教授,博士生导师,主要从事计算机软件理论研究; 李德昌(1948-),男,吉林长春人,教授,硕士生导师,主要从事网络与分布式操作系统的教学和研究。