

数据交换传输安全模型设计及实现

贾丽艳, 魏衍召

(天津大学 计算机科学与技术学院, 天津 300072)

摘要:在 Web Services 应用中, 保证数据交换传输的安全性和完整性非常重要, 而当前技术下的 Web Services 却在安全性方面存在着一些不足。为了保护在 Web Services 中消息交换的安全传递, 文中通过 X. 509 证书实现了 Web Services 消息签名和加密, 阐述了利用 WSE3.0 构建安全 Web Services 的方法, 设计并实现了一种基于策略的可扩展系统安全架构, 其中采用了证书管理、数据同步以及用户校验三种机制。在实现架构的过程中, 将安全通信主体分为 Web 服务端和服务应用端, 并通过对系统安全性的分析验证, 证明此架构具有良好的安全性。随着信息化技术的发展, 安全架构中安全策略的应用会越来越广泛和深入。

关键词:Web 服务; 数字证书; 安全; 策略

中图分类号: TP399

文献标识码: A

文章编号: 1673-629X(2012)01-0209-04

Design and Implementation of Security Model in Transmission of Data Exchange

JIA Li-yan, WEI Yan-zhao

(School of Computer Science and Technology, Tianjin University, Tianjin 300072, China)

Abstract: It is vital to protect the integrity and security in transmission of data exchange of Web Services, while the Web data transmission is insufficient to be transmitted successfully and safely because of the current developing of Web Services. In order to protect the data security of message transmission in Web Services and aiming at an entire description of constructing a safe Web Services with WSE through the X. 509 certificate's signatures and encryption, designs the system's security frame, which uses three mechanisms of certificate management, data synchronization and user validation. In the realization of the architecture, the secure communication parts are divided as the Web Service end and the service application end, and through the analysis of system security, have proved that the structure enhances message transmission security of Web Services. With the development of information technology, the security policy in security architecture will become more and more extensive and in-depth.

Key words: Web Services; digital certificate; security; policy

0 引言

随着信息技术的快速发展, Web 服务技术的应用越来越广泛, 其安全问题也日益受到重视^[1]。而目前大多数 Web Services 的传输层都使用 HTTP 协议, SSL (Secure Socket Layer 安全套接层)/TLS (Transport Layer Security 安全传输层) 作为 HTTP 协议原有的安全机制, 也被广泛应用于 Web Services 的安全服务^[2]。

目前系统间进行交互的 Web 服务主要依赖于传统的 SSL/TLS 方案, 虽然能够确保身份认证、数据保密性以及完整性^[3], 但无法提供端到端的保护、灵活的

认证机制及消息级安全等安全特性, 同样无法保证消息的不可抵赖性。因此, 为了能够保证 Web Service 的消息级安全, 必须要保护端点间传输的 SOAP 消息的安全^[4]。

针对上述状况, 选择基于消息级的安全通信, WSE3.0 集成了这一基于消息级的安全通信所需的协议以及各种技术, 因此选用 WSE3.0 作为实现系统安全性的基础, 采用用户名/密码以及 X. 509 证书的安全策略^[5]。

1 Web 服务安全性相关技术

1.1 WS-Security 规范

WS-Security 通过对 SOAP 消息扩展, 在消息头部加入安全元素 < security > 及其子元素, 这些子元素可以是身份标识的安全令牌^[6], 也可以是签名和加密的安全元素, 分别用来提供身份认证、消息完整性、数据

收稿日期: 2011-05-28; 修回日期: 2011-09-04

基金项目: 天津市科技支撑计划重点项目 (10ZCGYSF01300)

作者简介: 贾丽艳 (1986-), 女, 内蒙古通辽人, 硕士研究生, 研究方向为计算机应用技术; 导师: 许林英, 副教授, 主要从事计算机数据库方向和网络方向的教学简介简介与研究。

机密性的安全保护^[7]。

1.2 身份验证机制

用户令牌验证 (Username Token) 是用于传递调用方凭据的最常见方法之一,在 WS-Security 中定义了 Username Token 元素^[8]。用户在发送请求的时候,在 Soap head 中加入自己的用户名及密码,接收请求的 Service 通过之前与 Client 建立的共享密码来验证密码的合法性从而实现鉴别用户的功能^[9]。

X.509 证书^[10]能够确切地说明用户的身份,是公钥基础设施的重要组成部分,它使用 PKI 将证书映射到程序中的当前用户。利用证书证明身份容易遭到重放攻击,所以,最好强制发送方发送消息的同时使用其私钥对消息进行签名。当消息接收方收到消息后,根据发送方的公钥解密消息,从而验证签名的有效性,说明消息确实来自发送方,达到验证的目的。

1.3 WS-Policy

WS-Policy 定义了一个简单的 XML 结构,由几种属性和元素组成,这些属性和元素提供一种方法来组织和合并任意复杂度的策略断言^[11]。此外,WS-Policy 还定义了一个标准形式的策略表达式和一组可以创建更紧凑的策略表达式的规则^[12]。

1.4 WSE3.0

WSE3.0 的体系结构模型基于处理入站和出站 SOAP 消息的过滤器管道^[13],它根据定义的安全断言和消息的出入方式自动选择响应的过滤器进行消息的安全处理。最为重要的是,WSE3.0 具有可扩展性,支持自定义安全断言,用户根据自身的需求,定制合适的安全策略及相关的输入输出过滤器进行 SOAP 消息保护,使得 WS-Security 的灵活性得到了充分的体现^[14]。

WSE3.0 的策略框架分析常用的安全场景,提供了 6 种预先定义好的安全操作所组成的安全策略,用户可根据实际需要,选择一种来实现安全需求,从而保证消息完整性、保密性以及身份验证。

在系统安全架构中采用上述技术实现 Web 服务的安全性,架构中安全 Web 服务的内部模块设计如图 1 所示。

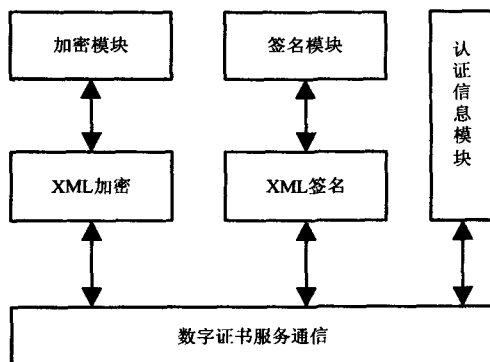


图 1 安全 Web 服务内部模块

2 交互系统安全架构设计

在工程建设交易市场中,市级工程建设交易信息平台 Web 服务主要用于与省级建设工程管理系统进行交互,市级系统用户经校验合法后,可登陆系统并向省级管理系统的 Web 服务 HbzbbDexSjzService 发出调用请求,请求 HbzbbDexSjzService 接受提交的项目信息,HbzbbDexSjzService 接收到请求后,通过用户口令检查其合法性,若用户为系统已有用户且合法,则 HbzbbDexSjzService 接受提交请求,将项目数据保存到数据库中并返回生成的省办项目编码。两系统交互的概要流程如下:

Hb_SaveSjzXx 为省级建设工程管理系统保存市级项目信息方法类,其中包含 Save_Project 方法,此方法用于保存项目信息。

HbzbbDexSjzService_Common 为中间层业务类,用于确保两系统交互过程中用户合法性。其中包含 Get_Password 方法、Check_user 方法。用户登录系统后,首先调用 Get_Password 方法根据用户名获得其对应的密码,然后调用 Check_user 方法来判断此用户在省级系统中是否为合法用户,实现鉴别用户的功能。

Hb_Service 为 Web 服务类,其中包含 SetXmxx 方法,此方法用于返回一个省办的项目编码。

CustomerUsernameTokenManager 为安全令牌管理类,通过用户提供的用户名和密码验证其的身份,并解密用户发来的消息,实现消息传递安全。

为安全起见,系统采用用户安全令牌和 X.509 证书相结合的安全策略,可以将各种相关协议和加密机制有机地结合起来,从而实现对消息的认证并保证消息的完整性、保密性。在系统中涉及到的部分为:省级系统的 Web 服务和市级系统的客户端。

WSE 的安全机制可以通过两种方法实现:一种是在 .NET 开发环境中利用代码来实现,可以实现为满足服务而提出的特定要求,但后期若需要改变策略,需要重新编译程序;一种是通过 WSE 的配置工具进行设置,即使用 XML 策略文件^[15],这种方法可以在程序部署后,根据不同的需要灵活地选择和使用策略。本架构中选择第二种方式来实现安全机制,可实现系统的可扩展性和易维护性。并使用了 MutualCertificateAssertion 和 UsernameForCertificateAssertion 两种安全策略断言,其中 UsernameForCertificateAssertion 在服务端使用 X.509 证书进行验证,在客户端使用用户名令牌进行验证的方式实现 Web 服务的安全。

3 架构中 Web 服务端实现

在 Web 服务端部署含有私钥的 X.509 证书,证书要存储在本机存储中。因为在 ASP.NET 中,现有用户

是在安装时自动生成的,无法访问此用户对应的口令。如果将证书存储在当前用户存储中,由于没有用户的口令,在服务器端证书的私钥就很有可能无法访问到。部署的证书用来验证当前用户的身份,同时解密消息,得到对方发送的数据。

选用用户检验策略断言和 X. 509 证书相结合的方式,实现用户身份认证以及在加密前对 SOAP 消息进行签名。

3.1 XML 文件的配置

ASP.NET 配置数据存储在命名为 Web.config 的 XML 文件中,它可以出现在应用程序的每一个目录中,使用这个文本文件,无论应用程序是否已经部署,都可以方便地修改配置数据,为实现 WSE 安全机制,需要编辑 Web.config 中相关元素配置。

在 ASP.NET 中,默认不对如何处理配置文件内的设置作任何操作。因此,在网络配置文件中指定配置是必要的。<configSections>元素是常规设置架构,用来指定配置节和命名空间声明,在其中指定配置后,ASP.NET 会将配置数据的处理委托给配置节处理程序,架构中根据 WSE3.0 指定 microsoft.web.services3 作为处理程序,在配置节<microsoft.web.services3>中配置 WSE3.0 相关属性。

在 ASP.NET 指定配置节后,需要为配置节指定根元素。在<system.web>元素中,可以指定各种配置元素,这些元素配置 ASP.NET Web 的应用程序并可以控制其行为。其子元素<webServices>控制 ASP.NET Web 服务及其客户端的行为,默认情况下,可配置所应用的任何 Web 服务,<soapExtensionImporterTypes>为其可选子元素,用来指定要与配置文件范围内的所有 XML Web services 一起运行的 SOAP 扩展。

在<configSections>指定的配置节<microsoft.web.services3>中,包含两个子元素,<policy>元素指定策略文件,架构中用到的网络服务策略定义在策略文件 wse3policyCache.config 中,在<policy>中指定此文件。<security>为第二个子元素,它可通过自身的子元素<securityTokenManager>实现 WSE 安全设置,在<securityTokenManager>中指定自定义安全令牌管理类 CustomerUsernameTokenManager,当 WSE 每次接收到令牌后,就会调用自定义类检验令牌,实现安全机制。

3.2 安全策略的声明

利用 WSE 机制进行策略配置,系统会自动生成一个策略配置文件 wse3policyCache.config,它用来保存系统中所配置的安全策略。在 wse3policyCache.config 中,有两个元素<extensions>、<policy>,通过它们的配置可实现 WSE 安全策略的实现。在<extensions>中,指出策略声明类的名称,有助于编写自定义的声明;在

<policy>中,指定对 SOAP 消息使用何种策略,定义策略声明 HbServicePolicy。

3.3 安全令牌管理类的创建

若使用系统自带的用户令牌管理类,密码会以明文的方式进行传送,这很有可能会被他人窃取,丧失安全性。为了防止密码以明文方式传送,自定义一个安全令牌管理类,它是继承 UsernameTokenManager 的新类,重载 AuthenticateToken 方法。首先使用 UsernameToken 创建一个角色关系方法,在 AuthenticateToken 方法中,通过已知的用户名查找对应的密码并将其返回给调用者,为 WSE 的使用奠定基础。服务端接收到 SOAP 消息后,WSE 调用 VerifyToken 方法,同样返回一个密码,使用得到的密码与传递过来的密码进行比较,验证用户的合法性。AuthenticateToken 方法的重写实现如下:

```
protected override string AuthenticateToken ( UsernameToken token)
{
    //通过用户名返回客户端 UsernameToken 传递的用户密码
    byte[] password = System.Text.Encoding.UTF8.
    GetBytes(token.Username);
    Array.Reverse(password);
    return Convert.ToBase64String(password);
}
```

3.4 安全 Web 服务的实现

在 Web 服务方法 SetXmxx 中引用已配置的安全策略文件,方法如下:

```
[ WebService ( Namespace = " http://hbjs.
com/" ) ]
[ WebServiceBinding ( ConformsTo = WsiProfiles.
BasicProfile1_1 ) ]
[ Microsoft.Web.Services3.Policy ( " HbServicePolicy" ) ]
```

中间层业务类 HbzbDexSjzService_Common 包括为 Web 服务实现的一部分,包含的 Get_password 方法在安全令牌管理类中要被调用,Check_user 方法在 Web 服务方法中也要得到调用。

4 服务应用端实现

在市级系统即客户端配置含有 Web 服务端公钥的 X.509 证书,客户端在传递消息时,使用 WSE3.0 创建的随机对称密钥对 SOAP 消息签名,再使用服务端 X.509 证书的公钥对其进行加密处理。

4.1 XML 文件的配置

在网络配置文件中要添加的元素包括有<config-

Sections>、<microsoft. web. services3>。在<configSections>中创建自定义节点<microsoft. web. services3>,在<microsoft. web. services3>中指定策略文件 wse3policy Cache. config。通过添加这两个元素完成客户端 XML 文件的相关配置。

4.2 安全策略的声明

系统使用 UsernameForCertificateAssertion 安全断言实现用户身份的认证,用 X. 509 证书对 SOAP 消息加密。因此,客户端需要指定相应的 X. 509 证书。在 XML 文件中配置<extensions>、<policy>元素,同在服务端相同,在<extensions>中指定策略声明,在<policy>中指定策略声明 SjzCliPolicy。在客户端,还需要在<policy>的子元素<serviceToken>中指定其要配置的证书。

4.3 安全策略代理类的应用

在项目中添加 Web 引用 HbzbDexSjzService,可以看到在此文件夹下生成三个文件,Reference. cs 文件,以及相应的 disco 和 wsdl 文件。其中 Reference 文件中包含了两个代理类,一个是 Hb_ServiceWse,这是系统的安全策略代理类,用于提供安全策略;另一个是 Hb_Service,为 Web 服务代理类,用来提供 Web 服务。项目中的 Reference 文件是在配置好策略以后引入的,能够将普通的 Web service 的代理类转变成成为支持 WSE 的代理类,即安全策略代理类 Hb_ServiceWse 自动继承 Microsoft. Web. Services3. WebServicesClientProtocol 类,此时的安全策略代理类即可支持 WSE 的功能。

在客户端代理类的使用同本地类一样,可以直接调用,通过调用代理类可访问服务器上提供的服务,实现安全策略。所以,在市级系统中调用 Web 服务时,首先要使用安全策略代理类 Hb_ServiceWse 声明一个策略对象,使用它调用 Web 服务中的 SetXmxx 方法,并设置需要使用的安全策略。

系统在客户端使用的是用户名令牌进行验证的方式实现 Web 服务的安全,因此在应用中要实现安全方案需要使用含有用户名和密码的安全令牌^[16],再使用市级系统中使用的安全策略,示例代码如下:

```
//声明安全策略代理类对象
```

```
SjzCli. HbDataExchange. Hb_ServiceWse SjzCliUser  
= new SjzCli. HbDataExchange. Hb_ServiceWse();
```

```
//创建 UsernameToken,得到安全令牌
```

```
UsernameToken token = new UsernameToken(user-  
name, password);
```

```
//设置客户端证书及安全令牌
```

```
SjzCliUser. SetClientCredential( token );
```

```
//应用策略
```

```
SjzCliUser. SetPolicy( "SjzCliPolicy" );
```

```
//调用 Web 服务,使用 SetXmxx 方法
```

```
DataSet ds = SjzCliUser. SetXmxx( username, Pro-  
ject)。
```

5 系统安全性分析

5.1 应用端直接远程调用

服务应用端的用户若不登陆系统而直接访问 Web 服务,则 Web 服务端通过用户校验机制,判断出其未登录,给出未登录提示,并告知其没有访问权限,如图 2 所示。

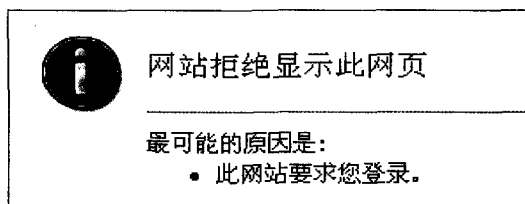


图 2 直接远程调用提示

5.2 启用消息跟踪

在服务应用端对 WSE 应用程序的配置文件进行更改,启用消息跟踪机制,并指定输出文件,如下所示:

```
<diagnostics>
```

```
<trace enabled="true"
```

```
input="C:\temp\service-in. trace"
```

```
output="C:\temp\service-out. trace" />
```

```
<detailedErrors enabled="true" />
```

```
</diagnostics>
```

在上面定义好的目录 input 和 output 中,可以看到启用安全机制后的 SOAP 消息,其中,客户端的 SOAP 消息显示在 service-out. trace 中,服务器端的 SOAP 消息显示在 service-in. trace 中。通过查看这两个 SOAP 消息格式,观察到 SOAP 消息已被签名和加密。

6 结束语

文中分析市级工程建设交易信息平台与省级建设工程管理系统采用 Web 服务进行的数据交互过程,结合基于策略的可扩展系统安全架构,论述了安全架构建设交易信息系统中的实现,最后对系统安全性进行了分析验证。

系统安全架构中为了实现数据同步以及用户校验,选用了 X. 509 证书,其中需要服务双方使用密钥对消息解密以及进行身份验证,这会使系统的性能降低。如何均衡安全及性能,使系统更加完善,是今后需要研究的热点问题。

参考文献:

- [1] Chen S, Zic J, Tang K, et al. Performance evaluation and mod-

(下转第 216 页)

参考文献:

- [1] 任艳娜, 闻素红, 刘 斌, 等. NET 与 Web 服务解析[J]. 计算机技术与发展, 2006, 16(1): 196-197.
 - [2] 李程程, 张永胜, 李 静, 等. 一种简单的 Web 服务安全通信模型研究[J]. 计算机技术与发展, 2010, 20(9): 158-160.
 - [3] OASIS. Web Services Security: SOAP Message Security1. 1 [S/OL]. 2006-02-01 [2010-05-10]. <http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf>.
 - [4] OASIA. WS-Trust1. 4 [S/OL]. 2009-02-02 [2011-05-11]. <http://docs.oasis-open.org/wss/v1.1/was-v1.1-spec-os-SOAPMessageSecurity.pdf>.
 - [5] 张俊妍, 陈启买. SOAP 协议性能与安全的研究进展[J]. 计算机技术与发展, 2009, 19(6): 163-167.
 - [6] 胡佳辉. 基于 UDDI 的 Web 服务平台研究[J]. 计算机技术与发展, 2006, 16(11): 7-12.
 - [7] 高文婕, 赵逢禹. 基于 SOAP 消息的过度加密攻击检测算法[J]. 计算机工程, 2011, 36(22): 129-131.
 - [8] Chonka A, Zhou Wanlei. Defending grid web services from XDoS attacks by SOTA [C]//Proc of the Seventh Annual IEEE International Conference on Pervasive Computing and Communications. [s. l.]: [s. n.], 2009.
 - [9] Lindstrom P. Attacking and Defending Web Services[R]. [s. l.]: [s. n.], 2004.
 - [10] Vorobiev A, Han Jun. Security Attack Ontology for Web Services [C]//Proceedings of the IEEE Second International Conference on Semantics, Knowledge and Grid. [s. l.]: [s. n.], 2006.
 - [11] Jensen M, Gruschka N, Herkenhoener R. A survey of attacks on web services [C]//Computer Science - Research and Development (CSR D). [s. l.]: [s. n.], 2009: 185-197.
 - [12] 高文婕, 赵逢禹. 基于 SOAP 消息的过度加密攻击检测算法[J]. 计算机工程, 2010, 36(22): 128-131.
 - [13] Jensen M, Gruschka N, Herkenhoner R, et al. SOA and Web Services: New Technologies, New Standards - New Attacks [C]// Proceedings of the Fifth European Conference on Web Services. [s. l.]: [s. n.], 2007.
 - [14] 王伟平, 李 昌, 段桂华. 基于正则表示的 SQL 注入过滤模块设计[J]. 计算机工程, 2010, 37(5): 158-160.
 - [15] Padmanabhuni S, Singh V, Kumar K M S, et al. Preventing Service Oriented Denial of Service (PreSODoS): A Proposed Approach [C]//ICWSapos 06 International Conference on Web Services. [s. l.]: [s. n.], 2006: 577 - 584.
 - [16] Sidharth N, Liu Jigang. IAPF: a framework for enhancing Web services security [C] //Proc of the 31st Annual International Computer Software and Applications Conference. [s. l.]: [s. n.], 2007.
 - [17] Xu Jun, Lee W Y. Sustaining availability of Web services under distributed denial of service attacks [J]. IEEE Trans on Computers, 2003, 52(2): 195-208.
- +++++
- (上接第 212 页)
- eling of web services security [C]//Proceedings of the IEEE International Conference on Web Services (ICWS 2007). [s. l.]: [s. n.], 2007: 431-438.
 - [2] 汪红波, 袁利永, 汪红刚. 基于用户令牌实现 Web 服务身份验证[J]. 计算机与数学工程, 2006, 34(10): 79-82.
 - [3] 续亚锋, 陈志国, 李 涵. 用 WSE 构建安全可靠的 Web Services [J]. 计算机技术与发展, 2008, 18(8): 155-158.
 - [4] 董国栋. Web Service 消息级安全研究[D]. 青岛: 中国海洋大学, 2008.
 - [5] 赵会洋, 王 爽, 魏士伟. 网络安全模型中认证策略的研究 [J]. 计算机技术与发展, 2010, 20(4): 171-174.
 - [6] Brown K. WSE 3. 0 中的安全性功能 [EB/OL]. 2005. <http://www.microsoft.com/china/MSDN/library/WebServices/WebServices/WSESecurity.aspx?mfr=true>.
 - [7] 孟 伟, 张 瑕, 李军怀, 等. Web 服务安全模型研究与实现[J]. 计算机工程与应用, 2006(26): 134-136.
 - [8] 李程程, 张永胜, 刘广钰. 一种安全的语义 Web 服务模型研究[J]. 计算机技术与发展, 2010, 20(2): 171-174.
 - [9] 柳翠寅, 刘 霞. XML 签名技术的研究与应用[J]. 计算机应用与软件, 2007, 24(4): 36-38.
 - [10] OASIS Standard Specification. OASIS Web Services Security 3 X. 509 Certificate Token Profile 1. 1 [EB/OL]. 2006. <http://www.doc88.com/p-14385135283.html>.
 - [11] Hollunder B. Domain-Specific Processing of Policies or: WS-Policy Intersection Revisited [C]//2009 IEEE International Conference on Web Services. Los Angeles, USA: [s. n.], 2009: 6-10.
 - [12] Web Services Enhancements (WSE) 3. 0 的新功能 [EB/OL]. 2005. <http://blog.csdn.net/hiyaolee/archive/2005/11/13/528496.aspx>.
 - [13] 李 婧, 赵逢禹. 基于策略断言的 SOAP 消息的部分签名和加密[J]. 计算机工程与设计, 2009, 30(8): 1914-1917.
 - [14] 魏文红, 吴清江. WSE 加密在 Web 服务中的应用[J]. 计算机与现代化, 2005(12): 56-58.
 - [15] 胡晓红, 付永军, 张志平. 基于策略的 Web 服务安全解决方案研究[J]. 微计算机信息, 2008, 24(15): 93-94.
 - [16] Xiong Pengcheng, Fan Yushun, Zhou Mengchu. Web Service Configuration Under Multiple Quality-of-Service Attributes [J]. Automation Science and Engineering, 2009, 6(2): 311-321.