一种Web服务通信安全的优化方案

李 霞[1] 张海涛[2] 王晓勇[1]
(辽宁工程技术大学电子与信息工程学院 葫芦岛 125105)[1] (辽宁工程技术大学软件学院 葫芦岛 125105)[2]

摘 要 综合应用Web服务安全标准,混合采用目前Web服务中的主要安全技术来优化Web服务架构,可实现Web服务通信安全。优化的服务架构通过设置业务网关实现身份验证和授权功能;通过扩展的SOAP协议实现消息传递的机密性、完整性和不可否认性。与侧重应用服务架构扩展技术和侧重应用协议扩展技术实现Web服务安全的方法进行比较,得出本优化方案加强了通信安全性。结合现有的研究成果,展望了未来Web服务安全的研究方向。

关键词 Web服务安全,Web服务架构,SOAP协议,SOAP扩展
中图法分类号 TP393.08 **文献标识码** A

Optimization Scheme of the Web Service Communication Safety

LI Xia[1] ZHANG Hai-tao[2] WANG Xiao-yong[1]
(Dept. of Electronic and Information Engineering, Liaoning Technical University, Huludao 125105, China)[1]
(Dept. of Software, Liaoning Technical University, Huludao 125105, China)[2]

Abstract Comprehensively applying Web services safety standards and now main Web service safety technology to optimize Web service structure can realizes Web service communication safety. The optimization service structure realizes identity authentication and authorization function by setting business gateway, and realizes confidentiality, integrity and nonrepudiation of the message by extending SOAP agreement. Compared with the technology which focuses on the service structure extension and the technology which focuses on the agreement expansion to achieve Web service safe, this optimization scheme strengthens the communication security. Combined with the research results, the future research direction of the Web service safety is prospected.

Keywords Web service security, Web service structure, SOAP agreement, SOAP expansion

Web服务通过Web服务描述语言WSDL来描述在线业务;通过简单对象接入协议SOAP完成跨平台的交互通信;通过统一描述、发现和集成UDDI实现业务注册和广泛环境内的业务发现和集成。随着Web服务的发展,安全问题成为制约其实际应用的主要障碍。基本的Web服务没有提供相应的安全机制,如W3C的初始SOAP版本没有提供安全性,传统的安全技术如VPN和SSL不能满足Web服务大范围事务处理和复杂交互的需求[1];而且SOAP、UDDI、WSDL等核心规范并不直接提供安全保护机制,因此Web服务数据的交换和传输存在严重的安全隐患。如何保证Web服务的安全成为当前亟需解决的重要问题。

1 Web服务概述

1.1 Web服务安全需求

Web Service涉及大量网络资源的使用。作为典型的分布式应用,其主要安全需求如下[2]:

(1)数据机密性:保证数据在发送者和接收者之间传输时不被没有经过授权的用户、实体或进程窃取信息。

(2)完整性:信息在传输过程中不被偶然或故意破坏,保证服务提供的信息是完整和真实的。

(3)身份认证:服务具有访问控制功能,能够认证用户身份标识的有效性,未能提供身份证明的实体将不能访问资源。

(4)授权:将不同的特权给予不同类型的用户,用户只能访问或使用授权的服务。

(5)不可否认性:参与某次通信的一方事后不能抵赖或否认对信息的发送。

1.2 Web服务架构

Web服务的基本架构定义了服务提供者、服务请求者、注册中心3类角色以及发布、查找、绑定3种操作。图1描述了基本的Web服务架构。

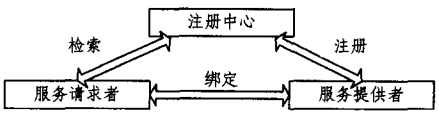

图1 Web服务架构

(1)角色

到稿日期:2011-09-20 返修日期:2011-11-22 本文受辽宁省教育厅高等学校科研项目(2009A349),辽宁省教育厅基金项目(2009A350)资助。

李 霞(1987—),女,硕士生,主要研究方向为Web服务、网络安全,E-mail:lixia4978@qq.com;张海涛(1974—),男,副教授,硕士生导师,主要研究方向为软件工程、嵌入式系统;王晓勇(1987—),男,硕士生,主要研究方向为网络安全、图形图像。

服务提供者(ServiceProvider)创建 Web 服务实体,为其它服务和用户提供服务功能,服务提供者在实现服务之后发布服务并且响应对其服务的调用请求。服务请求者(ServiceRequestor)是 Web 服务功能的使用者,它可以利用 Web 服务注册中心查找所需的服务并且向 Web 服务提供者发送请求,服务请求者可以是浏览器、窗体应用程序、后台程序等。服务注册中心(ServiceRegistry)是服务提供者和服务请求者的中介,是可搜索的服务描述注册中心。服务提供者在此注册并提供他们的 Web 服务清单,服务请求者可以从服务注册中心搜索所需 Web 服务。服务提供者、服务请求者、注册中心这 3 个角色是根据逻辑关系划分,在实际应用中角色可能会出现交叉或者互换,但组成 Web 服务完整体系的组件必须具有上述一种或多种角色[3]。

(2)操作

服务提供者通过发布操作(Publish)向服务注册中心注册自己的功能和访问接口,使服务可被服务请求者访问查询到。在查找(Find)操作中,服务请求者直接检索服务描述或在服务注册中心查询所要求的服务类型。对于服务请求者,可能会在两个不同的生命周期阶段中涉及到查找操作:在设计时为了程序开发而检索服务的接口描述;在运行时为了调用而检索服务的绑定和位置描述,Web 服务使用的最终目的是进行服务调用。在绑定操作(Bind)中,服务请求者使用服务描述中的绑定细节来定位、联系和调用服务,从而在运行时调用或启动与服务的交互。对于使用 Web 服务的应用程序,必定会发生以上 3 种行为,这些行为又可以单次或反复出现[3]。

2 Web 服务架构的优化

2.1 Web 服务常用安全技术

目前 Web 服务中采用的安全技术主要有以下几种[3-7]:

(1) 在客户端建立用户信任机制,执行服务时将相应的认证信息导入服务器。

(2) 在 SOAP 消息头中加入针对特定应用的安全表示(token),则可从中提取认证、信任信息。

(3) 在某个特定的应用领域内,对服务提供者的内部敏感数据进行加密;当其收到服务请求后直接在加密了的数据上进行相应的计算和处理,计算结果解密后返回给服务请求者。

(4) 从服务请求者的角度看,请求者需要提交必要的输入数据。考虑到客户信息的安全性,客户将需要提交的服务请求信息进行分块,每次仅提交一个输入数据块,返回的结果对应于该请求,经过多次服务请求,在结果返回之后,由服务请求者进行各次服务执行结果的集成,从一定程度上保证了客户信息的安全。

综上所述,WS-Security 规范本身并没有提出新的算法或安全模型,而是在利用现有的安全标准和规范的基础上提供了一个可扩展的框架。开发人员可以根据实际情况自由地将各种相关协议和加密技术、安全模型有机地结合起来,以实现消息的完整性、保密性和消息源认证等[8]。

2.2 Web 服务架构的优化

本文旨在对基础服务架构进行安全扩展,并把现有的可利用的安全技术纳入体系框架中。优化后的 Web 服务架构如图 2 所示。

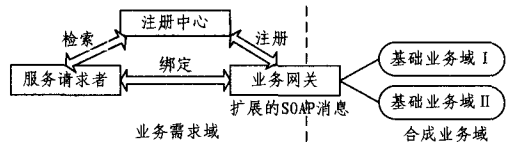

图 2 优化的 Web 服务架构

Web 服务安全架构的主体节点结构如图 2 所示,其中业务网关是安全功能的主要实施点,合成业务域由基础业务域 I 和 II 构成,用以表示业务体系结构层级构成的特征。优化后的 Web 服务架构主要是通过增加业务网关节点和对 SOAP 消息进行扩展来实现 Web 服务的通信安全。

2.3 业务网关原理

业务网关形成一个业务安全门户,主要实现身份验证和授权功能。可以利用两种方法实现服务请求者的身份验证:一种方法是通过标准的 Web 浏览器界面,服务请求者以 HTTP 或 HTTPS 协议的方式向业务网关提供用户名和口令对;另一种方法依赖公钥基础结构 PKI 的支持,由认证中心负责认证一个公钥是否属于一个特殊实体。业务网关对外部客户完成认证后生成相应的 SAML 身份验证断言,安全断言信息通过 SOAP 消息传递给基础业务域,基础业务域再依据 SAML 身份验证断言验证请求者身份,保证了任何回避身份验证系统直接给基础业务域发送 SOAP 消息的尝试都不会成功,从而实现了单点登录功能(Single Sign-on,SSO);此外,SAML 断言传递了身份验证的等级和用户的标识,因此允许基础业务自主决定相应的服务授权[9]。在合成业务域内通过 X.509 证书提供基础业务和业务网关间的安全机制。使用扩展访问控制标记语言 XACML 表示访问资源的规则。以基于角色的访问控制 RBAC 方式将资源的访问许可分配给主体对应的角色而不是主体本身,规定角色的层次,简化访问控制策略的定义和管理完成访问控制策略[10]。通过策略管理 GUI 对策略服务进行管理。

业务网关使用扩展的 SOAP 消息与业务提供域通信。扩展的 SOAP 消息与 HTTP 或 HTTPS 协议绑定,使用 XML 加密和 XML 数字签名规范对数据进行加密保护以实现数据完整性、机密性和不可否认性的安全功能。合成业务域内的通信都是基于扩展的 SOAP 消息的。Web 服务架构的安全结构如图 3 所示。

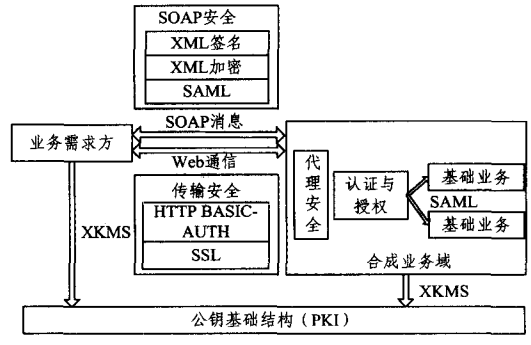

图 3 安全结构

2.4 SOAP 扩展原理

简单对象访问协议(SOAP)是一个轻型的分布式计算协议。作为 Web 服务最主要的组件,它的设计目标是简单性和可扩展性。每一个通过网络的远程调用都可以通过 SOAP 封装起来,然后绑定在传输层协议 HTTP,SMTP 等上面进行传送。SOAP 的规范虽然不涉及安全问题,但是允许安全问题作为协议扩展而被处理,从而增强 SOAP 消息安全性。为了保障 SOAP 消息安全,需要构造具有安全信息结构的 SOAP 消息报文。具体做法是对具有 XML 结构的 SOAP 消息报文进行自定义的改造重组,加入必要的自定义字段内容,如 XML 加密和 XML 数字签名,使其符合 XML-Security 规范和 WS-Security 规范的要求[11]。XML 签名和 XML 加密结合在一起,可以确保数据发送和接收的一致性,从而实现 Web 服务通信安全中的机密性、完整性和不可否认性。

在 Web 服务通信中消息传递的一次完整过程主要分为如下 4 个步骤:首先是调用端(Client)将调用信息进行序列化处理,生成 SOAP 消息(SOAP message),然后通过传输层传递到 Web 服务端(Service);在 Web 服务端对请求的报文进行反序列化(Deserialize),得到调用请求内容;然后 Web 服务端处理请求内容,生成返回结果,同调用端类似的报文发送操作一样,Web 服务端将返回的信息内容通过序列化生成相应的 SOAP 消息传递给调用端;最后调用端对返回的 SOAP 消息进行反序列化操作,得到返回的信息报文内容。经过这 4 个步骤,完成整个信息传输的过程。各个阶段以及发生时序如图 4 所示。

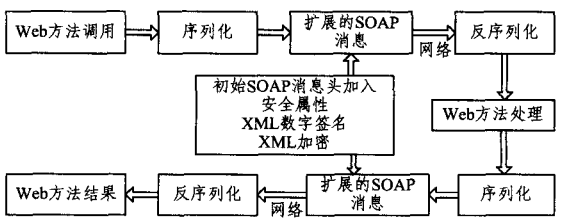

图 4 消息传递流程

因此,改造、重组 SOAP 消息报文就应该在 SOAP 消息序列化阶段对其进行自定义的序列化操作。相应地,在 SOAP 消息的反序列化阶段,对应自定义序列化的操作方法对 SOAP 消息进行反序列化操作,并对消息进行安全性检查得到原文信息内容。

利用 SOAP 扩展实现 SOAP 消息安全性的工作流程及主要代码如下。

(1)客户端

首先确定需要发送的 SOAP 消息并在消息头中加入随机序列号和时间戳;接着确定需要签名的内容,根据用户确定的签名算法以及密钥信息对需要签名的内容进行数字签名;再根据用户确定的加密密钥以及加密算法对消息进行加密;最后在消息头中添加发送时间戳生成完整的 SOAP 消息并发送。

(2)服务器端

收到 SOAP 消息后根据消息中的密钥信息对消息进行解密,查看消息是否被修改,是则丢弃,否则继续验证;然后检查消息头中的安全属性信息,查看是否为重传的消息,是则丢弃,否则继续验证消息;最后根据消息中的签名信息对消息进行签名认证。

(3)主要代码片段

a)实现签名的代码片段

```
//获取消息上下文
SoaPContext reqContext=RequestsoaPContext. Current;
//获得客户端 X509 令牌证书
X509SeeurityToken SignToken=ClientBase. GetClientToken();
//如果签名令牌获取出错,抛出异常
if(SignToken==null)
{
Throw new Exeeption("获取客户端证书出错!");
return;
}
//将客户端令牌加入 SOAP 消息
reqContext. Seeurity. Tokens. Add(SignToken);
//设置 Ttl 为 5 分钟
reqContext. Seeurity. Timestamp. TtlInseeonds=300;
//签名消息
MessageSignature sig = new MessageSignature ( SignToken. PrivateKey);
reqContext. Security. Elements. Add(sig)。
```

b)实现服务器端加密的代码片段

```
SoapContext reqContext=RequestSoapContext. Current;
X509SecurityToken EneryptToken = ServicesBase. GetserverToken
();
if(EneryptToken==null)
{
Throw new Exeeption("服务器令牌获取失败!");
return;
}
//加密消息
EneryptedData ene=new EneryptedData(EneryptToken. PublieKey);
reqContext. Seeurity. Elements. Add(ene)。
```

3 安全技术比较

本文将解决 Web 服务安全的问题平衡地分配给了两个主要安全功能实施主体:业务网关和扩展的 SOAP 协议。业务网关主要实现身份验证和授权功能,扩展的 SOAP 协议主要实现消息的机密性、完整性和不可否认性。相对于侧重依靠服务架构改进实现通信安全的技术,其充分利用了 SOAP 是一个基于 XML 的协议这一特性,将 XML 加密和 XML 数字签名技术运用于 SOAP 协议扩展以减轻服务架构的模块、硬件负担。考虑到 SOAP 是一个轻型的分布式计算协议,作为 Web 服务最主要的组件,它的设计目标是简单性和可扩展性。如果仅靠 SOAP 协议扩展实现服务安全,把 XML 加密和 XML 数字签名、身份验证和授权等安全因素全部作为扩展加入到 SOAP 头部中,不仅加大了协议改造、重组的难度,而且破坏了协议的简单性,所以最好通过设置业务网关实现身份验证和授权。本文这种将多种安全技术相融合、功能均衡分配的技术相比单纯侧重一种安全技术来说,性能稳定、功能强大、安全性较高。

(下转第 87 页)

行为分析[J]. 中文信息学报,2007,21(1):109-114
[21] 王惠. 词义·词长·词频—《现代汉语词典》(第5版)多义词计量分析[J]. 中国语文,2009,329:120-130
[22] Li Wen-jie, Qian Dong-lei, Lu Qin, et al. Detecting, Categorizing and Clustering Entity Mentions in Chinese Text [C]// Proceedings of SIGIR 2007. New York: ACM Press, 2007: 647-654
[23] Ling Xiao, Xue Gui-rong, Dai Wen-yuan, et al. Can Chinese Web Pages be Classified with English Data Source? [C]// Proceedings of WWW 2008. New York: ACM Press, 2008: 969-978
[24] 李晓黎,刘继敏,史忠植. 基于支持向量机与无监督聚类相结合的中文网页分类器[J]. 计算机学报,2001,24(1):62-68
[25] 冯是聪,单松巍,龚笔宏,等. "天网"目录导航服务研究[J]. 计算机研究与发展,2004,41(4):653-659
[26] 傅向华,刘国,陈冬剑. 一种核心子集选择训练的大规模中文网页分类方法[J]. 小型微型计算机系统,2011,32(8):1608-1612
[27] 段军峰,黄维通,陆玉昌. 中文网页分类研究与系统实现[J]. 计算机科学,2007,34(6):210-213
[28] Yahoo Directory[OB/OL]. http://dir.yahoo.com
[29] Andrei B, Marcus F, Vanja J, et al. A Semantic Approach to Contextual Advertising [C]// Proceedings of SIGIR 2007. New York: ACM Press, 2007: 559-566
[30] Bruce C W, Donald M, Trevor S. Search Engines: Information Retrieval in Practice [M]. Beiging: China Machine Press, 2009: 154, 291
[31] Zhang D, Dong Yi-sheng. Semantic, Hierarchical, Online Clustering of Web Search Results [C]// Proceedings of APWeb 2004. Berlin: Springer-Verlag, 2004: 69-78
[32] Claudio C, Stanisiaw O, Giovanni R, et al. A Survey of Web Clustering Engines [J]. ACM Computing Surveys, 2009, 41(3): 1-38
[33] Paul B. Visual structure-based web page clustering and retrieval [C]// Proceedings of WWW 2010. New York: ACM Press, 2010: 1067-1068
[34] 李文波,孙乐,张大鲲. 基于Labeled-LDA模型的文本分类新算法[J]. 计算机学报,2008,31(4):620-627
[35] 刘振鹿,王大玲,冯时,等. 一种基于LDA的潜在语义区划分及Web文档聚类算法[J]. 中文信息学报,2011,25(1):60-65,70
[36] Nie Jian-yun, Ren Fu-ji. Chinese Information Retrieval: Using Characters or Words? [J]. Information Processing & Management, 1999, 35(4): 443-462
[37] Peng Fu-chun, Huang Xiang-ji, Dale S, et al. Using Self-supervised Word Segmentation in Chinese Information Retrieval [C]// Proceedings of SIGIR 2002. New York: ACM Press, 2002: 349-350
[38] Schubert F, Li Hui. Chinese Word Segmentation and Its Effect on Information Retrieval [J]. Information Processing and Management, 2004, 40(1): 161-190
[39] GB2312-80. 信息交换用汉字编码字符集基本集[S]. 北京:国家标准总局,1981
[40] Peng Fu-chun, Huang Xiang-ji, Dale S, et al. Investigating the Relationship between Word Segmentation Performance and Retrieval Performance in Chinese IR [C]// Proceedings of COLING 2002. Stroudsburg: Association for Computational Linguistics, 2002: 1-7
[41] Wang Ding-ding, Li Tao, Zhu Sheng-huo, et al. Multi-Document Summarization via Sentence-Level Semantic Analysis and Symmetric Matrix Factorization [C]// Proceedings of SIGIR 2008. New York: ACM Press, 2008: 307-314
[42] 李静静,闫宏飞. 中文网页信息测试检索测试集的构建、分析及应用[J]. 中文信息学报,2008,22(1):30-36

(上接第61页)

结束语 本文通过对Web服务通信安全的分析,提出了解决Web服务安全问题的重要方法:Web服务架构优化与SOAP协议扩展相结合。Web服务架构通过设置业务网关实现身份验证和授权功能;加入安全性内容的SOAP协议实现机密性、完整性和不可否认性,从而全面、较好地实现了Web服务通信安全的5大需求。下一阶段的工作主要集中在综合使用其他的安全手段和措施进一步加强通信安全,如在Web服务器端通过对RequestSoapContext.Current值的判断,防止未通过Token验证的直接访问;在Web服务端禁止非SOAP协议的连接(例如HttpPost和HttpGet方式)请求等。这些都是下一步对于Web服务通信安全研究工作的主要方向。

参考文献

[1] Hardjono T, Weis B. The Multicast Group Security Architecture [Z]. Internet Draft, draft-ietf-msec-arch-05.txt, Internet Engineering Task Force, 2004-01
[2] 王晓峻,周晓峰,王志坚,等. 基于PKI/PMI的Web服务安全框架[J]. 计算机科学,2008,35(4):48
[3] W3C. WS-Policy(1.5) Framework[EB/OL]. http://www.w3.org/TR/2007/REC-ws-poliey-20070904,2007
[4] Diego Z G, Maria B F. Ontology-based Security Policies for Supporting the Management of Web Service Business Processes[C]// The IEEE International Conference on Semantic Computing. 2008
[5] 岳昆,王晓玲,周傲英. Web服务核心支撑技术:研究综述[J]. 软件学报,2004,15(3):429
[6] Boyens C, Günther O. Trust is not enough: Privacy and security in ASP and Web service environments[C]// Manolopoulos Y, et al, eds. Proc. of the 6th East European Conf. on Advances in Databases and Information Systems. Bratislava: Springer-Verlag, 2002: 8-22
[7] Thelin J, Murray P J. A public Web services security framework based on current and future usage scenarios[C]// Arabnia H, eds. Proc. of the Int'l Conf. on Internet Computing (IC2002). Las Vegas: CSREA Press, 2001: 825-833
[8] 杨怀洲,李增智. 基于Web Services的安全业务体系结构的设计[J]. 计算机工程,2005,31(20):146
[9] 王茜,吴黎明. 单点登录在Web服务安全中的应用[J]. 计算机工程,2008,36(8):179
[10] 贺正求,吴礼发,洪征,等. Web服务安全问题研究[J]. 计算机科学,2010,37(8):32
[11] 刘志都,贾橙涪,詹仕华. SOAP协议安全性的研究与应用[J]. 计算机工程,2008,34(5):142