维普资讯 http://www.cqvip.com

一种支持可信 Web 服务的应用框架*)

梁 英 沈传慧 韩燕波

(中国科学院计算技术研究所软件研究室 北京 100080)

摘 要 Web 服务技术给开发基于 Web 的应用带来了新的机遇和效益,但系统安全性却不利于其应用性。本文通过扩展 Web 服务安全规范实现了一种支持可信服务的机制,提出了电子商务和电子政务中 Web 服务安全性的实际解决方案。

关键词 可信 Web 服务,Web 服务安全性,SOAP,UDDI,WSDL

An Application Architecture Supporting Trusted Web Services

LIAGN Ying SHEN Chuan-Hui HAN Yan-Bo

(Institute of Computing Technology, Chinese Academy of Sciences, Beijing 100080)

Abstract The Web Services technology brings new opportunities and benefits for developing Web-based applications. However, the weakness in systems security hinders its applicability. In this paper a mechanism is implemented, which supports trusted Web Services by extending Web Services security specification. An experimental solution of Web Services security is also presented in the context of e-Business and e-Government application.

Keywords Trusted Web services, Web services security, SOAP, UDDI, WSDL

1 引言

随着电子商务和 B2B 应用的不断发展,企业应用系统要求可以在因特网环境下依据新的需求,快速、灵活地集成各种业务应用系统,并使之有机地协同提供服务。Web 服务将分布环境下的各种应用和资源封装成统一的 Web 服务形式,并且提供标准的服务使用方法。简化了复杂的软件应用方式,为分布环境下资源共享与协同工作提供了很好的支持。与此同时 Web 服务也带来了一些问题和挑战。其中,Web 服务的安全性已经成为 Web 服务大规模实际应用必须解决的关键问题。

Web 服务的安全性涉及到 OSI 网络模型中的应用层的安全。因此,不但需要下层安全规范的支持,还要有关于应用层的安全考虑。目前,现有的网络安全规范中,安全套接字层(SSL)[18]和传输层安全(TLS)[19]一起为 Web 服务提供了传输层的安全保证,是基于点到点的安全会话方式。IPSec[20]是一个用于网络层的安全标准,它用主机认证、数据完整性和数据机密性提供安全的会话。在基于 Web 服务的架构之中,信息可以来自不同的数据源,并通过中介体传输给多个目的源,数据在运行过程中不断地进行打包、解包处理。当传输层之外的中介体接收并转发数据时,数据的完整性和任何随数据流动的安全性信息都有可能丢失,使传统的信息安全技术显得束手无策。我们需要一种能够提供端对端安全性的 Web 服务安全体系架构。

本文结合相关的 Web 服务安全标准,提出了一种可信的 Web 服务的安全机制,该方案涉及到 Web 服务的三个核心技术(SOAP、WSDL、UDDI)以及 Web 服务的体系架构的安全性研究,主要考虑确保服务提供者的可靠性,服务调用过程的可靠性,以及服务授权访问的可靠性。我们将这些安全性研究结合起来,从整体上提出了一个 Web 服务安全机制,为电子商务、电子政务及行业应用提供了完整的 Web 服务安全解决方案。最后,我们将该安全机制在一站式个性化数字奥运综合服务平台(FLAME2008)[1,2]中进行了验证。

2 Web 服务的安全机制

2.1 Web 服务面临的挑战

2.1.1 Web 服务 其体系结构是一个松散耦合的分布式结构,采用了业界广泛支持的 XML 、SOAP、WSDL 和 UDDI 规范等开放标准;Web 服务描述了服务提供者、服务请求者、服务中介者三种角色,并提供了发布、查找、绑定三种基本操作。Web 服务提供者利用 WSDL 描述自己的 Web 服务,并将服务发布到 UDDI;Web 服务请求者利用 SOAP 消息向 Web 服务提供者发送使用服务的请求;Web 服务中介者的作用是在 UDDI 中查找满足服务请求者要求的服务。

2.1.2 网络安全存在的威胁 目前网络存在下面四个基本的安全威胁[21]:1. 信息泄漏:信息被泄漏或透露给某个未授权实体;2. 完整性破坏:数据的一致性通过未授权的创建、修改或破坏而受到损坏;3. 拒绝服务:对信息或其他资源的合法访问被无条件的阻止;4. 非法使用:某一资源被某个未授权的人或以某一未授权的方式使用。

2.1.3 Web 服务面临的挑战 Web 服务作为开放技术架构将是未来应用架构的一个极为重要的模式,它具有松散耦合与分布式、使用标准协议规范、高度可集成等特性,从而确定了 Web 服务日益成为主流的地位,但同样面临安全上的挑战[3]:

1. 服务提供者的可靠性:服务提供者是否经过身份认证? 提供的服务是否可靠?

2. Web 服务调用的安全性:Web 服务在调用过程中是否

*) 本文工作得到国家科技攻关计划(编号:2001BA105A1010-2)和国家十五攻关计划奥运科技专项(编号:2001BA904B07)的资助。

维普资讯 http://www.cqvip.com

可靠，发起服务调用的一方，即服务请求者是否可靠，服务请求者的权限是否符合。

3. 权限及访问控制：如何控制用户对 Web 服务的访问，避免服务的非法使用以及服务的拒绝访问。

由于基于 Web 服务的软件，不再受制于本地操作系统和数据库的限制，甚至可以不考虑具体的应用，因此，我们完全可以把信息安全独立出来，形成可信的基础架构，以各种不同的形式提供统一的认证系统，解决网络安全中的五个基本要求：机密性、授权、数据完整性、原始性证明和抗抵赖。

2.2 Web 服务安全的支撑环境

在 Web 服务技术框架中，技术规范在 Web 服务栈(Web Services Stack)的体系下协同共存(图 1)。其中，最底部是广泛使用的传输层和网络层的标准：TCP/IP、HTTP、SMTP 等；中间部分是目前开发的 Web 服务的相关标准协议，包括服务调用协议 SOAP、服务描述协议 WSDL 和服务发现协议 UDDI，服务工作流描述语言 WSFL 以及 Web 服务的安全协议等。右边部分是各个协议层的公用机制。

Web 服务安全技术贯穿 Web 服务栈的始终，对 Web 服务应用机制的安全性、可靠性起着关键作用。Web 服务安全规范主要包括：XML 数字签名、XML 加密、XKMS、SAML、XACML、WS-Security 等，它们共同支撑着 Web 服务的安全环境。

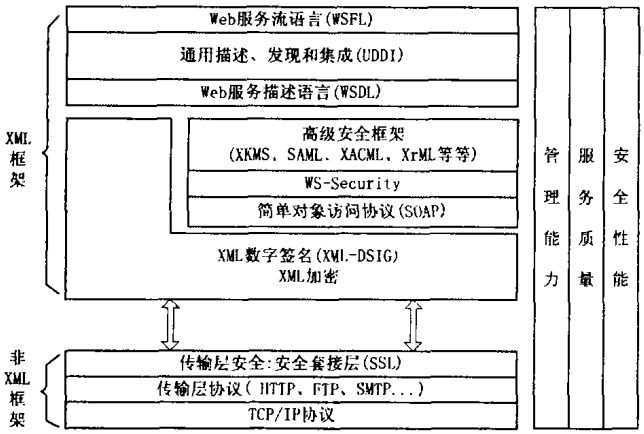

图 1 Web 服务栈

2.3 Web 服务安全规范

2.3.1 Web 服务安全协议、规范 目前 W3C、OASIS 正在加强 Web 服务安全性方面的工作力度，早期的一些安全解决方案现在已经被应用，如 IBM 的 alphaWorks、VeriSign 的 XML Trust Center。现有的 Web 服务安全规范包括：XML 密钥管理规范(XKMS)[4]、XML 数字签名[5]、XML 加密[6]、安全断言标记语言(SAML)[7]、可扩展访问控制标记语言(XACML)[8]和 WS-Security[9]等。随着 Web 服务的应用越来越广泛，对于安全的需求也日益强烈，新的标准将不断涌现。IBM、Microsoft 和 VeriSign 计划合作开发一种能保障下一代 Internet 商业服务更加安全的共同标准，将陆续推出一系列 Web 服务安全规范[10]：WS-Security 、WS-Policy、WS-Trust、WS-Privacy、WS-Secure Conversation、WS-Federation、WS-Authorization。其体系结构允许对规范进行混合匹配，使实现者能够只部署他们需要的部分。

2.3.2 协议规范安全性能比较 随着 Web 服务安全规范层出不穷的出现，采用什么标准使 Web 服务更加安全变得愈来愈重要。首先应该知道 Web 服务需要哪方面的安全，以及各安全规范的侧重点和不同点；其次要考虑相应的安全规范是否成熟，是否会带来风险；在此基础上定义安全策略和体系架构。在表 1 中，对各安全规范的安全覆盖范围进行了比较，从比较结果可以看出，WS-Security 规范更好地解决了认证、授权、机密性、完整性、抗抵赖等安全问题。

表 1 安全规范比较

	XML-Signature	XML Encryption	XKMS	SAML	WS-Security
认 证	★		★	★	★
授 权				★	★
机密性		★			★
完整性	★		★		★
抗抵赖	★				★

2.4 国内外相关研究及产品介绍

IBM、微软、VeriSign 等公司在此方面开展了大量的研制工作，并发布了相应的产品。IBM 在其 XML 安全套件 XSS4J[11](XML Security Suite for Java)中加入了 WS-Security 的实现，并支持 XACML。微软公司宣布了一项最新技术 TrustBridge[12]，该技术旨在通过 Kerberos 协议、WS-Security 规范，在不同的企业和组织之间建立身份联盟。VeriSign 公司的 XML 可信中心最近推出 TSIK1.7[13](Trust Services Integration Kit)，支持 WS-Security、XKMS、SAML、XML Encryption、XML-DSIG。Apache 推出开放源代码，支持 XML-DSIG。Systinet 公司的 WASP UDDI[14]，WASP Server 支持 WS-Security、SAML、XML Digital Signatures、XML Encryption、XKMS。

3 可信 Web 服务应用框架

3.1 可信 Web 服务平台体系架构

可信的 Web 服务环境的研究涉及到三个基本技术(SOAP、WSDL、UDDI)的综合环境的可信和授权研究，目前国内外机构几乎还没有做到把它们集成在一起，构造一个完整的可信 Web 服务环境。本文结合 Web 服务安全标准提出了一种如图 2 所示的可信 Web 服务平台体系架构。系统主要包括以下三个部件：

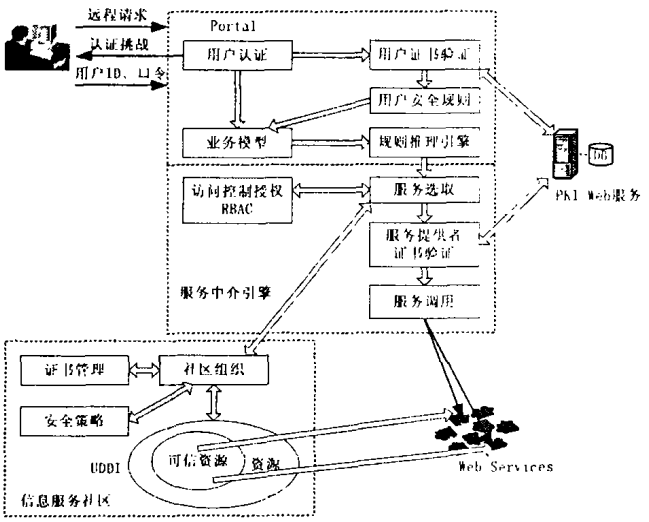

图 2 可信 Web 服务平台体系架构

1. 个性化服务配置环境 设计了以用户为中心的个性化服务配置环境，通过业务端编程工具及时获取和动态解析用户需求，设置用户安全规则，进行用户证书验证。

维普资讯 http://www.cqvip.com

2. 服务中介引擎　服务中介引擎是个性化服务配置环境的支撑体系，通过服务中介对服务进行动态选取、调度、组织，并对服务提供者证书进行验证，对用户进行访问控制，保障信息服务在可信的基础上相互协作、共享信息。

3. 信息服务社区　解决开放环境中资源的有序组织和资源的可信问题，对服务提供者证书进行管理，形成资源的多维视图，实现用户级资源可视化。

3.2 安全性考虑

在可信 Web 服务平台体系架构中，我们重点考虑实现以下几方面的安全：

1. 服务提供商的可信性　是指 Web 服务本身的可靠性、完整性以及对服务提供商的证书验证等。可以是利用 XKMS 协议由 PKI Web 服务提供证书认证。

2. 安全策略　建立了全方位的防御体系来保护服务提供商和服务使用者的利益。如服务的使用者可以对服务社区的资源按类进行可信性选择，可以对服务提出不同粒度的可信级别要求；服务提供商则可以根据自己的服务性质，设置不同的服务质量等级。服务提供者和服务使用者通过 SOAP 层的会话来形成一套完整的安全策略。

3. 授权及访问控制　是服务提供商对服务使用者的授权访问控制，服务提供商根据 WSDL 扩展机制中描述的安全策略，来限制用户对服务的访问级别。并通过 PKI Web 服务对用户的证书进行认证。

3.3 关键技术

3.3.1　基于 PKI/PMI 的可信 Web 服务代理　PKI/PMI 可信 Web 服务代理，由 PKI/PMI Web 服务和可信服务代理两部分组成。PKI/PMI Web 服务建立了有效的信任管理机制和授权控制机制，可信服务代理则在 Web 服务应用和 PKI/PMI Web 服务之间架起桥梁。

PKI/PMI Web 服务提供基于安全 XML 技术的 PKI/PMI 统一接口，这个接口把 PKI/PMI 的证书验证功能模块封装成 Web 服务的方式，它具有很多优点。首先，Web 服务具有比较统一的描述、发布、调用格式，这样可以屏蔽 PKI/PMI 认证服务底层的复杂性，提高整个可信架构的可靠性；其次，因为 Web 服务采用的技术规范（WSDL，SOAP，UDDI）都具有可扩展性，使得整个封装成 Web 服务的 PKI/PMI 功能模块可根据实际情况，方便地扩展相应功能；最后，由于整个 Web 服务安全架构中，每个功能模块都是以 Web 服务的方式出现的，这样，其它可信 Web 服务可用统一的方式使用信任与授权服务。

可信服务代理实现可信的数据传输和 Web 服务加载、运行、注册、查询等机制，简化 Web 服务、SOAP 消息与底层的 PKI/PMI 安全基础设施的结合。可信服务代理由一组可信代理组成，包括身份认证代理、证书验证代理、安全策略代理、授权和访问控制代理、服务注册代理和日志等几个部分，各代理之间通过相互协商与合作共同实现多可信代理的功能。

3.3.2　安全策略保障机制——WSDL 安全扩展　安全策略是可信 Web 服务平台的安全性因素之一，我们通过 WSDL[15]对服务的描述和 SOAP[16]头的安全扩展，使得安全策略更具用户导向性和更加动态。WSDL 是用来描述 Web 服务的一种 XML 语言，用于 Web 服务的描述、动态发布、查找及绑定。

在 WSDL 规范中，并没有提供一种直接的方法为服务使用者和提供者解决服务描述中与安全相关的问题。为此，我们提出了一种如图 3 所示的安全机制，当服务使用者提出服务请求时，可通过 WSDL 得到服务提供者的安全策略，并结合自己的安全策略形成应用安全策略，加入 SOAP 头作为应答向服务提供者发送。服务提供者安全管理机制根据这个联合的策略，为请求者提供服务。我们通过 WSDL 的扩展项来描述安全策略。

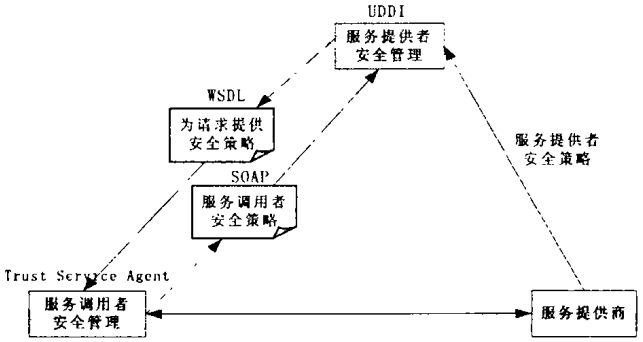

图 3　WSDL 安全机制

3.3.3　可信资源管理——UDDI 安全模型　UDDI[17]规范定义了 Web 服务的发布与发现的方法，目前的版本是 3.0，它与前几个版本显著区别有：对多注册中心环境的支持、策略与实现的分离、安全性功能、增强的查询。这些功能的增加，为资源的可信管理提供了保障。

UDDI 安全模型由注册中心和结点策略以及它们的实现集合定义，版本 3 增加了对所有核心数据类型的数字签名的支持以处理数据集成和可靠性问题。数字签名的使用改善了 UDDI 中的数据质量并为用户提供了在电子商务和其他应用程序中使用的 Web 服务所需的信任和保护。通过对注册中心内的数据进行数字签名，发布者现在可以确保没有人能够通过模仿签名盗用他们的数据（这些模仿签名很容易被查询程序弄错）。而且，一旦数据被一个发布者签名，用任何方式改变它都会破坏这个签名，通过验证签名，使用注册中心的查询程序还可以确信一个经过签名的实体是有效的，并且它是由这个签名所代表的发布者创建的。

在我们的 UDDI 可信性解决方案中主要考虑以下节点策略与数字签名的结合：

1. 策略规则　任何基于策略的系统的基本构件。它定义了一组根据一组条件映射的操作标准。

2. 策略授权　包括用于确定哪些策略集可以被委托给结点的策略。

3. 信息访问与控制　定义用户的注册与授权、隐私及其他内容等方面的策略。

4. API　定义了每个 API 集（查询、发布、订阅、保管以及其他）的数据机密性策略。

5. 用户策略　描述了用户发布限制和所有权转移方面的策略。

4 实例应用

2008 年奥运会将在北京召开，届时，除众多国内观众外，还将有来自全球的超过 1 万多名运动员、2 万多名记者、5 万多名国际游客以及国际官员和工作人员，这些特定人员对信息服务的要求各有特点，需要根据用户的不同需求进行服务的动态嵌入和无缝连接，整合各类社会信息资源，提供综合的、全面的、多语种的、个性化信息服务。

要想真正跨越数字奥运解决方案的门槛，Web 服务的可

维普资讯 http://www.cqvip.com

信性是我们面临的不可回避的问题。如何保障散落在网上不同地点的海量信息的可靠性和安全性，对于组织一体化的综合信息服务体系是一个极大的挑战。

面对这些挑战，我们研制了一个面向2008年奥运会、能够提供一站式个性化数字奥运综合服务平台(FLAME2008)，针对奥运会组织管理和备战过程中，信息系统和公众服务系统所涉及的组织与关联、不同信息系统的共享、集成与整合等方面遇到的安全问题，提供动态、按需方式的服务中介、配置和部署的安全机制，以满足各种用户的不同需求。图3展示的是FLAME2008原型系统中的安全解决方案。

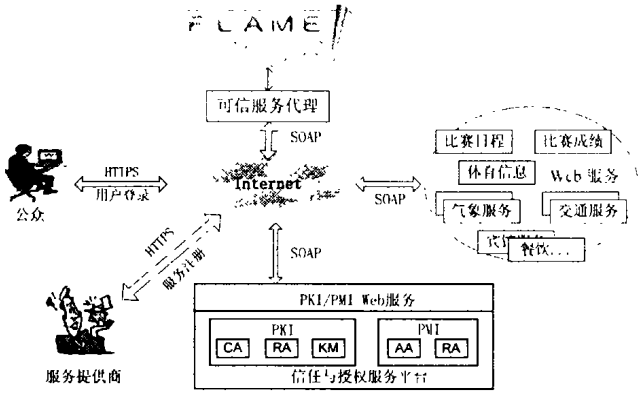

图3 一站式个性化数字奥运综合服务平台安全解决方案

在FLAME2008实例应用中，针对公众、记者、运动员、教练员、奥组委等不同用户群体的安全需求，系统通过可信服务代理和PKI/PMI Web服务构筑的可信环境，从以下几个方面保障整个信息平台服务调用的安全性。在服务注册时，在服务提供商注册服务时，对Web服务提供者的证书及服务的属性证书进行验证，以确保Web服务的可信性。用户登陆时，对Web服务请求者进行身份认证，获取用户的权限等级。服务调用时，通过可信代理，确保用户按照访问控制策略合法调用服务。

结束语 本文提出了基于SOAP、WSDL、UDDI综合环境的可信Web服务安全机制和解决方案，并在数字奥运综合信息服务系统上得已实施。在今后的工作中，我们还将尝试Web服务商务模式、计费模式的研究。随着Web服务技术的深入发展和动态电子商务模式的出现，Web服务安全技术将得到更广泛的应用。

参考文献

1 Han Y, et al. A User-centric Service Composition Platform for the Olympic Games Beijing 2008. International Workshop on Information Logistics, Germany, Dec. 2003

2 Han Y, et al. CAFISE: An Approach Enabling On-Demand Configuration of Service Grid Applications. Journal of Computer Science and Technology, to appear in July 2003

3 Glass G. The Web services (r)evolution—Applying Web services to applications. Nov. 2000. http://www-900.ibm.com/developerWorks/cn/webservices/ws-peer1/index_eng.shtml

4 Ford W, et al. XML Key Management Specification(XKMS) W3C Note30 March2001. http://www.w3.org/TR/xkms

5 Brown A, et al. SOAP Security Extensions: Digital Signature W3C NOTE 06 February 2001. http://www.w3.org/TR/SOAP-dsig

6 Imamura T, Dillaway B, Simon E. XML Encryption Syntax and Processing W3C Recommendation 10 December 2002. http://www.w3.org/TR/xmlenc-core

7 Hallan-Baker P, Maler E. Assertions and Protocol for the OASIS Security Assertion Markup Language(SAML) OASIS Standard, Nov. 2002. http://www.oasis-open.org/committees/tc_home.php? wg_abbrev=security

8 http://www.oasis-open.org/committees/tc_home.php? wg_abbrev=xacml

9 Atkinson B, Della-Libera G. Web Services Security (WS-Security) Version 1.0, April 5, 2002. http://www.verisign.com/wss/wss.pdf

10 Della-Libera G, Dixon B. Security in a Web Services World: A Proposed Architecture and Roadmap. April 7, 2001, Version 1.0. http://www-106.ibm.com/developerworks/webservices/library/ws-secmap

11 IBM Corp. XML Security Suite. http://www.trl.ibm.com/projects/xml/xss4j

12 Microsoft Corp. Microsoft's Federated Security and Identity Roadmap. June 2002. http://www.microsoft.com/presspass/press/2002/Jun02/06-06TrustbridgePR.asp

13 VeriSign Corp. Trust Services Integration Kit (TSIK) 1.4. July 26, 2002. http://www.xmltrustcenter.org/developer/verisign/tsik/index.htm

14 Systinet Corp. WASP UDDI 4.5.2, 2003. http://www.systinet.com/doc/wasp_uddi/uddi

15 Christensen E, Curbera F. Web Services Description Language (WSDL) 1.1 W3c Note 15 March 2001. http://www.w3.org/TR/wsdl

16 Box D, Ehnebuske D. Simple Object Access Protocol (SOAP) 1.1 WCNote08 May 2000. http://www.w3.org/TR/SOAP

17 Bellwood T, Clément L. UDDI Version 3.0 UDDI. Published Specification, 19 July 2002. http://uddi.org/pubs/uddi_v3.htm.

18 Freier A O, Karlton P, Kocher P C. The SSL Protocol Version 3.0. IETF(draft-ietf-tls-ssl-version3-00.txt), Nov. 1996

19 Dierks T, Allen C. The TLS Protocol Version 1.0. IETF (draft-ietf-tls-protocol-02.txt), March 1997

20 Kent S, Atkinson R. Security Architecture for the Internet Protocol. IETF (draft-ietf-ipsec-sec-01.txt), March 1997

21 冯登国. 计算机通讯网络安全. 清华大学出版社, 2001