

一种安全的语义 Web 服务模型研究

李程程, 张永胜, 刘广钰

(山东师范大学 信息科学与工程学院, 山东 济南 250014)

摘要:语义 Web 作为一个新兴的研究方向发展迅速, 语义 Web 服务技术也越来越受重视, 同时安全问题也成为语义 Web 服务技术中不容忽视的研究课题。分析了 Web 服务的安全现状, 根据语义 Web 服务的主要安全需求提出了一种安全的语义 Web 服务模型, 并详细介绍了模型的构成。模型应用安全本体并结合原有的安全基础设施, 使用 SSL/TLS 协议保证传输层的数据安全, 并使用 XML 数字签名规范、XML 加密规范与 SOAP 消息相结合保证数据机密性、完整性和不可否认性, 能够比较全面地为语义 Web 服务提供安全保障。

关键词:语义 Web 服务; 安全本体; 安全模型

中图分类号: TP393.08

文献标识码: A

文章编号: 1673-629X(2010)02-0171-04

Research on a Secure Semantic Web Services Model

LI Cheng-cheng, ZHANG Yong-sheng, LIU Guang-yu

(School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China)

Abstract: As an emerging researching direction, semantic Web develops rapidly, and semantic Web services technology is given more and more attention, at the same time, the security problem becomes a research subject can't be neglected in semantic Web services technology. Proposes one secure semantic Web services model and introduces the constitution of the model in detail. The model using secure ontology combined with intrinsic secure infrastructure, using SSL/TLS to guarantee the data security of transport layer, and using XML-signature, XML-Encryption combined with SOAP message to guarantee data confidentiality, integrity and undeniableness, and can provide comprehensive insurance of security for semantic Web services.

Key words: semantic Web services; security ontology; security model

0 引言

随着互联网技术的发展, 作为一种基于 Internet 开发标准的新型分布式计算模式, Web 服务以其良好的数据互操作性、扩展性和松散耦合性简化了复杂的软件应用方式, 为资源共享与协同工作提供了很好的支持, 受到许多专业人士的青睐, 企业对 Web 服务的应用也越来越广泛, 使得 Web 服务成为新一代电子商务的框架。但是随着 Web 服务广泛的应用也暴露出现有安全实现的弱点和局限性。由于 Web 服务经由 Internet 来进行信息交换, 因此存在着信息丢失、被窃听、被篡改等安全性风险, 而且 SOAP、UDDI、WSDL 等与 Web 服务相关的核心规范并不直接提供安全保护机制, 因此 Web 服务安全问题得不到保障。而且与

Web 服务相关的规范均缺乏语义支持, 计算机无法理解 Web 页面的内容, 从而无法有效而灵活地支持查找、组合和运行时对 Web 服务的监控等工作。

1998 年, 互联网的创始人 Tim Berners-Lee 提出在现有 Web 的基础上建设下一代 Web 的蓝图—语义 Web, 旨在使 Web 上的文本信息具有计算机系统可以理解的语义^[1]。在语义 Web 技术的推动下, 为了弥补 Web 服务缺乏语义描述这个不足, 语义 Web 服务随之诞生。语义 Web 服务为 Web 服务带来了丰富的语义, 但它并未消除 Web 服务中的安全隐患, 仍然面临信任、隐私等问题。业界针对这些安全隐患提出了许多相关规范, 但尚未提出完整的安全模型全面解决语义 Web 服务中的安全问题。文中针对语义 Web 服务中的一些主要安全需求提出了一种安全的语义 Web 服务模型, 应用安全本体并结合原有安全基础设施为语义 Web 服务提供了比较全面的安全保障。

收稿日期: 2009-05-14; 修回日期: 2009-08-11

基金项目: 山东省自然科学基金(Y2008G22)

作者简介: 李程程(1985-), 女, 山东临沂人, 硕士研究生, 研究方向为 Web 服务安全; 张永胜, 硕士, 副教授, 研究方向为 Web 服务安全、软件工程环境。

1 语义 Web 服务安全现状及相关规范

Web 服务是由 URI 标示的软件应用, 其接口和绑

定用 XML 来定义和描述并且可以被发现,与其它软件通过基于 Internet 的协议以 XML 消息交换的方式直接交互。

语义 Web 以一种机器可理解的方式来标示 Web 上的数据进而实现自动处理,使包含在它内部的信息拥有明确定义的语义,利用这种语义使机器和人能够更好地协作。语义 Web 服务是语义 Web 的一种应用,它将 Web 服务与语义 Web 集成起来,以一种明确的、计算机能够理解的包含语义的语言来描述 Web 服务的功能和内容,通过 Web 发布、定位和调用服务,是独立的、自描述的、模块化的应用。

作为典型的分布式应用,语义 Web 服务的主要安全需求与 Web 服务类似,包括:

1)数据机密性:数据在发送者和接收者之间传输时不被第三方所知。

2)完整性:信息在传输过程中不被有意或无意篡改,保证服务提供的信息是完整的、真实的。

3)认证与授权:服务具有访问控制功能,能够认证用户身份标识的有效性,用户只能访问或使用被授权的服务。

4)不可否认性:参与某次通信的一方事后不能否认曾发生过本次交换。

5)可用性:服务能够为授权使用者所正常使用。

针对以上安全需求,国内外一些标准化组织、公司和社会团体进行了大量相关研究,提出了很多安全规范,例如:W3C 的 XML 加密规范、XML 密钥管理规范, W3C 和 IETF 共同提出的 XML 签名规范, OASIS 提出的 SAML (Security Assertion Markup Language)^[2] 和 XACML (eXtensible Access Control Markup Language)^[3] 以及由 IBM、微软和 VeriSign 公司联合发布 Web 服务安全规范 (WS-Security)^[4] 等。这些安全规范也被应用于语义 Web 服务当中,满足了目前语义 Web 服务的一些安全需求。

2 安全本体

本体来源于本体论,最初属于哲学领域。近年来,本体论的研究日趋成熟并远远超出哲学范畴,逐渐与计算机技术紧密相连。在计算机领域比较公认的定义是 1993 年 Grube 提出的:本体是概念模型的明确的规范说明。1997 年 Brost 在此基础上又进行了改进,提出本体是共享概念模型的形式化的规范说明。为了提高数据的自动处理能力,在语义 Web 中引入的本体及相关技术成为解决语义层次上 Web 信息共享和交换的基础^[5]。

安全本体的目标是针对安全领域的知识,提供对

安全领域知识的共同理解,确定安全领域内共同认可的术语,并从不同层次的形式化模式上给出这些术语和术语之间相互关系的明确定义。根据 Web 服务安全需求以及 Web 服务安全体系中已具备的安全能力,安全本体提供了一种表示这些安全需求和安全能力的方法,在现有安全标准之上的更高抽象层次上总结了一些常用的与安全相关的标记。这些标记可以用来对 Web 资源、服务等进行注释。同时,这些安全本体也为实现自动的基于注释的假定推理奠定了基础。

根据 Web 服务安全的要求可以从不同角度设计多种安全本体:如以详细程度的不同来设计,可以设计描述或刻画相关对象详细程度高的参考安全本体,也可以设计详细程度低的共享安全本体;依照工作目标的不同设计领域安全本体、任务安全本体和应用安全本体。领域安全本体描述的是安全领域中的概念及概念间的关系,任务安全本体描述的是特定安全任务或行为中的概念及概念间的关系,应用安全本体既可以引用领域安全本体中的概念,又可以引用出现在任务安全本体中的概念用以描述特定的安全应用。至 2005 年, DAML Project 下的 DAML-S 安全工作小组已经开发了一些与安全有关的本体,比如凭证本体、安全机制本体、服务安全扩展本体、Agent 安全扩展本体及隐私本体等^[6]。

3 语义 Web 服务安全模型

文中提出一种安全的语义 Web 服务模型,在语义 Web 服务的发布、发现以及组合中应用多种不同类型的安全本体,并结合原有的安全基础设施以达到语义 Web 服务的主要安全需求,为语义 Web 服务提供比较全面的安全保障。

3.1 Web 服务安全基础设施

根据 Web 服务的安全需求,业界提出了许多相应的技术及安全规范,这些规范通常都能够解决某一方面的安全问题,将各种安全规范进行组合并结合 Web 服务特有的基础规范形成安全基础设施,能够全面地提高服务的安全性^[7]。文中采用的主要的安全基础设施如图 1 所示。

(1) SSL 协议 (安全套接字协议层) 是网景 (Netscape) 公司提出的基于 Web 应用的安全协议,它为 TCP/IP 连接提供数据加密、服务器认证、消息完整性以及可选的客户机认证。TLS 协议 (安全传输层协议) 用于在两个通信应用程序之间提供保密性和数据完整性。使用 SSL/TLS 协议保证传输层的点到点的数据安全。

(2) SOAP, WSDL 和 UDDI 是 Web 服务相关的基

本规范。SOAP 即简单对象访问协议,是一个轻型的分布式计算协议,它允许在分布式环境中交换信息,具有简单和可扩展的特点,用户可在 SOAP 消息头中自行添加用于描述安全性的数据。WSDL(Web 服务描述语言)用于定义 Web 服务,以及服务接口、服务访问地址和访问消息格式等。UDDI 即通用描述、发现和集成规范,它定义了一个通用服务信息注册中心软件,存储 XML 格式数据并管理各类服务元信息,以 Web 服务的方式提供基于元信息的服务发布和发现。

(3) WS-Security 提供了安全令牌和 SOAP 消息关联起来的通用机制,定义了如何利用 XML 数字签名和 XML 加密以及安全令牌来对 SOAP 消息进行加密盒签名。XML 加密规范描述了对数据的加密过程以及加密结果的 XML 表示。XML 数字签名规范描述了数字签名的 XML 表示以及计算、验证 XML 表示的数字签名的过程^[8]。以上三种机制保证 Web 服务消息通信的数据机密性、完整性和不可否认性。

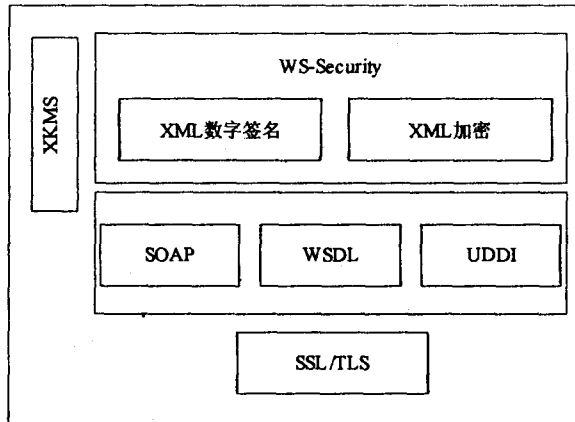


图1 Web 服务安全基础设施

(4) XKMS 规范对密钥、证书进行管理,包括注册、分发、撤销等等,它还允许客户通过 Web 服务取得密钥信息^[9]。

3.2 模型的结构

文中模型以 Web 服务三类基本角色:服务请求者,服务注册中心和服务提供者为基础构建,模型的具体构成如图 2 所示。

(1)在模型中设立安全中心这个角色,安全中心从属于服务注册中心,负责对服务提供者所提供的服务描述进行安全分析,并为服务描述提供安全优先级,可以根据主要安全能力由低到高分为零至五共六个等级,若服务提供者所提供的服务不能满足任何安全需求则安全优先级为零,若只能满足主要安全需求中的

一项则为服务描述分配安全优先级一,若主要的安全需求都可满足则优先级为五。

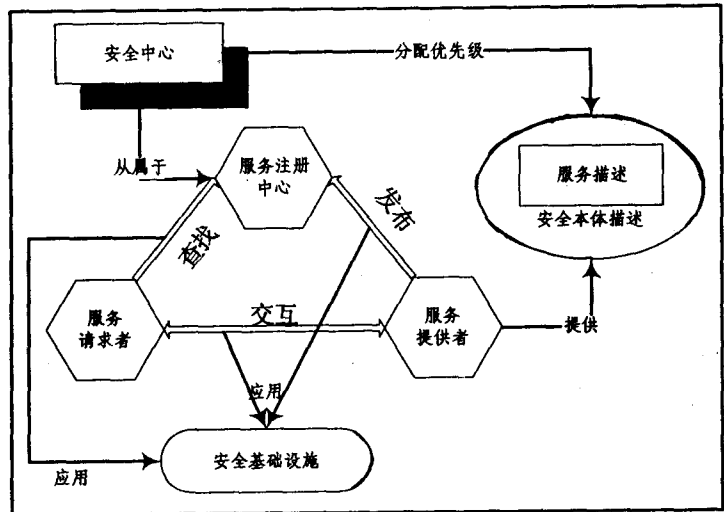


图2 安全模型

(2)服务提供者发布服务描述至注册中心时,在服务描述中添加安全本体描述,用以说明所提供服务的**安全需求和安全能力。服务提供者首先利用一定的散列算法计算服务描述的摘要,并对摘要进行数字签名,根据 XML 加密标准把原描述和签名后的描述加密发送至注册中心。注册中心收到消息后对消息进行解密,并验证消息中的数字签名,把摘要恢复为完整消息,与原消息进行对比,察看是否一致,若一致则保留消息继续通信,若不一致则丢弃这则消息,发送错误信息。

(3)服务请求者向安全注册中心搜索服务时,首先选择以安全为优先条件搜索还是以服务功能为优先条件搜索。若选择以安全为优先条件,搜索引擎将服务注册中心的服务按照安全优先级由高到低的顺序排列所有服务,并按照一定的发现算法从拥有高优先级的服务中进行查找,若不存在相匹配的服务则到下一级优先级服务序列中查找,依次类推。若选择以服务功能为优先条件搜索,则首先利用一定的发现算法查找服务,然后把查找到的服务以安全优先级进行排列,选择优先级较高的服务。

(4)服务请求者寻找到与自己的要求相匹配的服务描述后,通过服务描述中的接口或地址与服务提供者联系,商**费用和具体服务细节问题。双方在进行通信的 SOAP 消息中应用 XML 数字签名和 XML 加密等安全基础设施保证消息的机密性和完整性以及不可否认性等基本安全需求。

XML 数字签名的主要代码格式如下:

```
<Signature>
<SignedInfo>
```

```

<CanonicalizationMethod>
</CanonicalizationMethod> < SignatureMethod > </SignatureMethod> < Reference>
<Transforms></Transforms>
<DigestMethod></DigestMethod>
<DigestValue></DigestValue>
</Reference>
</SignedInfo>
<KeyInfo></KeyInfo>
</Signature>

```

其中 Signature 标签用于描述数字签名的完整信息; SignedInfo 标签记录被签名的信息; CanonicalizationMethod 标签使用 URI 唯一的标识该数字签名采用的 XML 数据的规范化法则; SignatureMethod 标签标明使用的签名算法; Reference 标签中的内容代表一个被签署的元素, 可以多次出现; KeyInfo 标签描述密钥特点。

XML 加密的主要代码格式如下:

```

<EncryptedData>
<EncryptionMethod></EncryptionMethod>
<KeyInfo>
<EncryptedKey></EncryptedKey>
<KeyName></KeyName>
</KeyInfo>
<CipherData>
<CipherValue></CipherValue>
<CipherReference></CipherReference>
</CipherData>
</EncryptedData>

```

其中 EncryptedData 标签用于描述一个加密数据包的完整信息; EncryptionMethod 标签中使用 URI 唯一地标识所采用的加密算法, 确保通信双方可以在加密算法上保持一致; KeyInfo 标签用于表达加密数据的密钥信息, 可选, 可以根据通信双方的约定, 记录密钥名称 (KeyName), 密钥值 (EncryptedKey), 数字证书, 甚至是获得密钥的转换方法描述, 从而确保密钥的安全性; CipherData 标记被

加密的数据。构造表示加密类型的 XML 元素结构时, 如果将加入的数据放入文档当中, 则要构造 CipherValue 元素, 内容编码方式为 base64 码, 若存在其他地方则构造 CipherReference 元素指示数据存放位置。

4 结束语

语义 Web 服务的研究才刚刚起步, 但不论学术界还是工业界都认为语义 Web 服务具有远大的前景, 随着语义 Web 服务的发展安全问题会越来越重要。文中提出了一种理论上的安全模型, 模型中应用安全本体结合原有的安全基础设施能够比较好地达到语义 Web 服务的主要安全需求, 进一步的研究是如何实现此模型。

参考文献:

- [1] Berners-Lee T, Hendler J, Lassila O. The Semantic Web[J]. Scientific American, 2001, 284: 5-10.
- [2] OASIS Security Services TC[EB/OL]. 2005[2008]. <http://www.oasis-open.org/specs/index.php#samlv2.0>.
- [3] OASIS eXtensible Access Control Markup Language (XACML)[EB/OL]. 2005[2008]. <http://www.oasis-open.org/specs/index.php#xacmlv2.0>.
- [4] Microsoft, IBM. VeriSign[EB/OL]. 2008[2008]. <http://www.ibm.com/developerworks/webservices/library/ws-security/>.
- [5] DAML Services[EB/OL]. 2004-10[2008]. <http://www.daml.org/services/owl-s/security.html>.
- [6] OASIS Web Services Security TC[EB/OL]. 2005[2008]. <http://www.oasis-open.org/specs/index.php#wssv1>.
- [7] 杨涛, 刘锦德, 谭浩. Web 服务安全基础设施的研究[J]. 计算机应用, 2006, 26(6): 1248-1253.
- [8] 杨欣, 沈建京. 语义 Web 服务安全研究[J]. 计算机科学, 2007, 34(2): 115-118.
- [9] Lee Feigenbaum, Herman I, Hongsermeier T, et al. The Semantic Web in Action[J]. Scientific American, 2007, 297: 90-97.

(上接第 170 页)

- Efficient String matching Algorithms for Intrusion Detection [C]//In Proceedings of IEEE Infocom. Hong Kong: [s. n.], 2004.
- [8] Garuba M, Liu Chunmei, Fraites D. Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems [C]//Fifth International Conference: New Generations. [s. l.]: IEEE Computer Society, 2008: 592-598.
- [9] 高朝勤, 陈元琰, 李梅. 一种面向入侵检测的快速多模式

匹配算法[J]. 计算机应用, 2008, 28(1): 82-84.

- [10] Caswell B, Iay Beale C, Foster, Posluns J. Snort2.0 入侵检测 [M]. 宋劲松, 等译. 北京: 国防工业出版社, 2004.
- [11] 1999 DARPA intrusion detection evaluation data set [DB/OL]. [2007-04-09]. <http://www.darpa.mil>.
- [12] Koziol J. Snort 入侵检测实用解决方案 [M]. 吴博峰, 孙默, 等译. 北京: 机械工业出版社, 2005.