一个Web服务可信体系结构

刘玲霞 王东霞 黄敏桓
(信息系统安全技术重点实验室 北京 100101)

摘 要 Web服务的安全可信问题是影响其广泛应用的重要因素。已有的解决方案大多从安全角度出发,但对于服务面对攻击或安全威胁时仍能按照预期工作则缺乏考虑。从Web服务的安全可信需求出发,对安全的概念进行了拓展,提出了可信的目标和内涵。在此基础上,提出一个以安全交互、联合身份和分布策略为基础,以运维管理、共用机制为支撑的Web服务可信体系结构,其可为Web服务安全可信提供体系结构层面的支持。

关键词 Web服务,可信,体系结构,可信需求,机制
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2014.12.007

Trustworthy Architecture for Web Services

LIU Ling-xia WANG Dong-xia HUANG Min-huan
(National Key Laboratory of Science and Technology on Information System Security, Beijing 100101, China)

Abstract The security and trustworthiness issues of Web services are the important factors that influence its development. Most of the existing solutions are from the point of view of security, and lack of considering that services need to still work as expected when facing attacks or threats. In this paper, the notion of security was expanded from the requirement of Web services. The goal and the content of trustworthy were proposed to meet the requirement of Web services. A trustworthy architecture for Web services was proposed. The architecture is based on security interaction, federated identity, and distributed policies and supported by operating maintenance and shared mechanisms.

Keywords Web services, Trustworthy, Architecture, Trustworthy requirement, Mechanism

1 引言

Web服务具有松散耦合、高度互操作、可重用等特点,业已成为实现异构系统集成和跨平台互操作的热门技术。然而由于Web服务完全建立在开放的互联网标准协议之上,安全可信问题成为影响其广泛应用的重要因素。

Web服务技术采用新的体制、新的技术和新的应用模型,使其面临许多独特的安全问题。Web服务采用SOA架构,引入服务注册中心使服务请求者和服务提供者之间松散耦合,一方面使服务信息公开,从而带来更多的安全威胁;另一方面导致系统体制的变化,使得已有的传统安全保障方式难以满足SOA架构下应用的安全需求。Web服务技术通过XML、SOAP等新技术实现服务之间的互操作,一方面带来新的安全威胁,另一方面给安全带来互操作性等新要求。在Web服务应用中,服务可重用、可动态组合这种新的应用模式一方面增加了攻击的风险,另一方面也对安全提出了新的要求,即要求能够保证组合服务的安全。此外,Web服务面向Internet环境,一方面更易遭受攻击,另一方面力求在面对攻击或安全威胁时仍能按照预期工作。因此,如何为Web服务从体系结构层面提供安全可信支持成为研究的热点。

目前,许多标准化组织、研究机构和企业从不同角度寻求解决Web服务安全可信问题的方案。但现有解决方案大多从安全角度出发,对于服务面对攻击或安全威胁时仍能按照预期工作则缺乏考虑。本文从Web服务的安全可信需求出发,在对可信内涵进行深入分析的基础上,提出一个Web服务可信体系结构,从而为Web服务安全可信提供体系结构层面的支持。

2 研究现状

目前已有一些研究者分别从模型[1,2]、体系结构及标准[3,4]等角度出发对Web服务安全技术展开研究。针对Web服务安全体系结构的研究的典型代表是美国国防部的网络中心企业服务安全体系结构规范、全球网格论坛(Global Grid Forum,GGF)的网格安全基础设施及OGSA的安全体系架构。

美国国防信息系统局(Defense Information Systems Agency,DISA)于2004年发布了《网络中心企业服务安全体系结构》标准规范(0.3版),为向"网络中心"的转变提供了面向服务的信息安全参考架构,提出了安全核心企业服务基本框架,用以保障网络中心环境中的服务安全[5]。

网格安全基础设施(Grid Security Infrastructure,GSI)为网格计算环境提供基础的安全服务,是用于解决网格计算中

到稿日期:2013-12-19 返修日期:2014-01-28 本文受国家自然科学基金(61271252),中国博士后科学基金(2012M521834)资助。
刘玲霞(1977—),女,博士,讲师,主要研究方向为Web服务安全、网络技术,E-mail:lingxia_liu@tom.com;王东霞(1974—),女,博士,研究员,主要研究方向为网络技术、信息安全;黄敏桓(1971—),男,博士,研究员,主要研究方向为网络技术、信息安全。

安全问题的一个集成方案，已经成为 GGF 的标准[6]。GSI 提供传输级和消息级的安全策略，同时提供安全消息、安全会话和安全传输的保护策略，以保障信息的保密性和完整性。此外 GSI 同时支持服务端授权和客户端授权。GSI 的主要安全功能包括相互认证、通信加密、私钥保护、委托授权和单点登录。GSI 也存在一些不足，如实体之间的认证频繁且复杂，扩展性不佳。

Ian Foster 等人结合五层沙漏结构和 Web 服务，提出了开放网格服务体系架构(Open Grid Services Architecture，OGSA)[7]。OGSA 的体系架构体现了其“将一切都抽象为服务”的核心原则。对于安全也不例外，OGSA 将加密、访问控制、审计等各种安全机制都视为服务，这些服务使得(虚拟的)机构内部可以方便地实施安全相关策略。

IBM 针对企业业务流程中所面临的信息安全问题，基于 IBM 自身的 SOA 基础和业务场景，提出了面向服务的安全参考模型及架构[8]。该架构包括 IT 安全服务、安全策略基础设施、业务安全服务 3 个层次。其中 IT 安全服务包括身份服务、认证服务、授权和隐私服务、保密性和完整性服务、审计服务。安全策略基础设施包括策略管理、策略判决及增强、策略监控及报告。业务安全服务包括监管、风险和兼容性、信任管理、数据保护及泄露控制、系统和网络安全。

文献[9]提出了一组视图来支持面向服务安全体系结构的构建，包括身份视图、服务视图、消息视图、部署视图和业务用例生命周期视图(Identity View，Service View，Message View，Deployment View，Transaction Use Case Life Cycle View)。每个视图由域特定元素、约束、威胁、风险、漏洞和对策组成。

文献[10]提出了一个名为 SOSIE 的面向服务的安全体系结构。该体系结构由模块化的独立安全服务构成。这些独立的安全服务可以通过企业应用集成技术(Enterprise Application Integration，EAI)链接起来。

文献[11]提出了一个面向服务的安全体系结构。该体系结构从标准及实现角度给出面向服务的安全解决方案。

上述体系结构大多是从如何保障服务安全的角度出发，对于服务的可信问题，即服务面对攻击或安全威胁时仍能按照预期工作则关注甚少。

3 可信需求

目前，研究者对可信的定义和内涵尚未达成共识。常见的可信定义和内涵包括[12]：

• Dependability

其概念源自可靠性(Reliability)，在早期主要关注硬件错误，后来扩展到软件错误，随后将错误的概念推广到由安全威胁引发的错误。从其概念的发展可以看出，它侧重于安全属性中的可用性，与安全是相互交叉的关系。

• Trusted

可信计算早期的研究主要集中在操作系统自身的安全机制以及支撑操作系统的硬件环境上。其主要的研究思路是：将可信计算芯片作为可信根，利用可信的传递性，通过信任链将可信关系逐渐扩展到硬件平台、操作系统、应用(远程应用)，从而构建一个可信的系统。其主要的研究目标是解决计算机和网络结构上的不安全问题，从根本上提高其安全性。

• Trustworthy

在 1999 年美国信息系统可信委员会(Committee on Information Systems Trustworthiness)的《Cyber 空间可信》(Trust in Cyberspace)研究报告和 2009 年美国国土安全部的《Cyber 安全研究路线图》(A Roadmap for Cybersecurity Research)中使用 Trustworthy 来表示系统的多维需求。2011 年美国总统执行办公室发布《可信 Cyber 空间：联邦 Cyber 空间安全研究与发展规划的战略计划》(Trustworthy Cyberspace：Strategic Plan For The Federal Cybersecurity Research And Development Program)，其主要目标是研究“改变游戏规则”的技术，可以有效压制当前对 cyber 系统的攻击，并为更好地应对未来 cyber 系统安全所面临的挑战奠定科学基础。从其主要目标来看，可信是对安全概念的拓展，要求系统能够应对各种安全威胁，并在受到安全威胁的情况下仍能按照预期工作。

文献[13]指出一个可信的网络应该是网络系统的行为及其结果是可以预期的，能够做到行为状态可监测，行为结果可评估，异常行为可控制。其属性包括：安全性、可生存性和可控性。

综上，“可信”一词在不同的研究背景下有不同的内涵。对这几种常见的可信概念及其含义进行分析，结合 Web 服务的安全可信需求，在对安全概念进行拓展的基础上，我们明确了可信目标：一个可信的系统指的是在遭受敌方攻击的情况下按照预期工作的系统。为了实现上述可信目标，系统除了需要具备安全性外，还需具备可生存性和可维性。这 3 个基本属性之间紧密联系，构成一个有机的整体：通过安全机制，降低系统的脆弱性；通过可生存机制，在系统脆弱性不可避免以及攻击和破坏行为客观存在的情况下，提供多样性等提高服务生存性的机制，提高关键服务的持续能力；通过可维机制，提高系统的灵活应变能力，保障系统的安全运行。

Web 服务的安全目标包括：

• 机密性。防止服务之间交互的信息不泄露给非授权方；

• 完整性。防止服务之间交互的信息不被非授权篡改；

• 可用性。保证服务被可靠地访问和使用；

• 抗抵赖性。保证参与各方不能否认其实施过的行为；

• 认证。角色在接受服务请求之前或接收到请求响应时，对交互方的身份进行鉴别；

• 授权。根据获得的身份信息和访问控制策略信息决定用户是否有特定类别的权限访问特定类别的服务；

• 可审计性。将历史事件和角色主体相关联；

• 互操作性。角色之间的安全机制保持互操作性；

• 跨域性。角色可以为跨域的请求提供服务。

此外，还需通过相应的管理机制和可生存性机制实现可维和可生存目标。

4 可信体系结构

根据 Web 服务的可信需求，设计相应的可信机制来满足可信目标。可信需求及相应的可信机制如表 1 所列。

表1 可信需求及相关机制

可信需求	属性	可信机制
安全性	机密性	加密机制
	完整性	签名机制
	可用性	消息可靠传输机制，服务可用机制
	抗抵赖性	签名机制
	认证	身份＋安全上下文＋认证机制
	授权	身份＋策略＋安全上下文＋授权机制
	可审计性	日志＋审计机制
	互操作性	标准
	跨域性	身份＋策略＋跨域认证＋跨域授权
可维性		管理机制
可生存性		冗余机制＋多样性机制＋动目标机制

从表1可以看出，Web服务通过消息与其它参与方交互，因此安全交互是Web服务安全的基础。为了实现服务之间及服务与其它角色的安全交互，联合身份和分布策略也是保障Web服务安全的重要内容。在此基础上，Web服务需要相关的运维管理机制来提供可维性，需要冗余等共用机制等来提供可生存性。因此，从满足Web服务的可信需求出发，提出了一个以安全交互、联合身份和分布策略为基础，以运维管理、共用机制为支撑的Web服务可信体系结构，如图1所示。

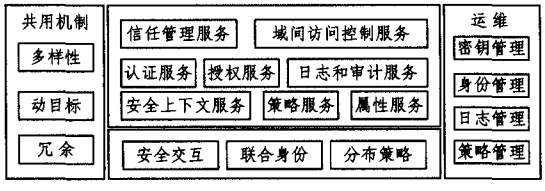

图1 Web服务可信体系结构图

根据Web服务的技术机制，将安全机制分成3个部分：消息安全、核心安全服务和扩展安全服务。

消息安全负责为Web服务提供端到端的消息传递安全。目前可以通过WS-Security系列标准来确保基于SOAP的消息交互安全。

核心安全服务由提供单一安全功能的原子安全服务组成，包括：

·属性服务。属性服务为各种属性（主要包括主体属性、系统资源属性和应用环境属性）提供标准的访问机制，支持基于属性的决策和其它应用；

·策略服务。策略服务用于准确地表示和匹配各参与方的安全策略，从而为服务和资源提供基于策略的授权和访问控制；

·安全上下文服务。安全上下文服务确定服务在交互式环境中的安全环境，为跨多个Web服务共享“安全上下文”提供机制；

·日志和审计服务。日志和审计服务负责对服务的活动情况等进行记录和审计；

·认证服务。认证服务主要根据身份和安全上下文来识别访问者的身份；

·授权服务。授权服务主要根据访问者的身份和相关策略来决定是否让其访问相关服务。

扩展安全服务由面向应用的安全服务组成，主要保证跨域服务访问的安全性，包括：

·信任管理服务。信任管理服务为不同信任域的服务交互提供无需用户干预的信任关系管理；

·域间访问控制服务。访问控制保证服务的机密信息和敏感操作只能被授权的请求者获取和调用。访问控制服务采用基于属性的访问控制，能够感知安全上下文等环境属性，实现复杂的、细粒度的访问控制。

此外，系统在攻击无法避免的情况下，还需要主动响应技术（例如动目标机制）来降低系统被攻击的几率，增加攻击者成本，增强系统的安全性。系统还需要一些机制（例如多样性机制、冗余机制等），来确保核心关键服务的可生存性。除了这些机制外，还需要相应的管理机制来实现可维性，包括密钥管理、身份管理、日志管理和策略管理。

本文提出的可信体系结构在满足Web服务安全性的基础上，增加了冗余等机制来保证Web服务的可生存性，从而能更好地应对Web服务面临的安全威胁，增强Web服务的安全性。

结束语 Web服务的安全可信问题成为影响其广泛应用的重要因素，对于整个Web服务技术的成功至关重要。本文从Web服务的安全可信需求出发，在深入分析典型可信概念的基础上，指明了Web服务可信的目标及内涵。针对Web服务可信目标，提出了一个以安全交互、联合身份和分布策略为基础，以运维管理、共用机制为支撑的Web服务可信体系结构，它可为Web服务安全可信提供体系结构层面的支持。

下一步，将以此可信体系结构为指导，进一步研究安全可信机制的部署和可信体系结构评估方法，为可信服务的开发和管理提供有效的支持。

参考文献

[1] Sabbari M, Alipour H S. A security model and its strategies for web services[J]. International Journal of Computer Applications, 2011, 36(10): 24-31

[2] 吴波. SOA安全关键技术研究[D]. 长沙：国防科学技术大学，2009

[3] Gerić S, Hutinski Ž. Standard based service-oriented security[C]// Proceedings of the 18th International Conference on Information and Intelligent Systems. Hrvatska, FOI, 2007: 327-335

[4] 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)：32-38

[5] Defense Information Systems Agency. A security architecture for net-centric enterprise services (nces) version 0.3[R]. USA: Defense Information Systems Agency, 2004

[6] Globus. Overview of the grid security infrastructure [EB/OL]. [2013-9-5]. http://www.globus.org/security/overview.html

[7] Foster I, Kishimoto H, Savva A. The open grid services architecture, Version 1.5[R]. USA: Global Grid Forum, 2006

[8] A, Ashley P, Borrett M, et al. Understanding soa security design and implementation[R]. USA: IBM, 2007

[9] Peterson G. Service oriented security architecture[J]. Information Security Bulletin, 2005(10): 325-330

[10] Opincaru C, Gheorghe G. Service oriented security architecture [J]. Enterprise Modelling and Information Systems Architectures, 2009, 4(1): 39-48

[11] Geric S. Security of Web services based service-oriented architectures[C]// MIPRO, 2010 Proceedings of the 33rd International Convention. Croatia, IEEE, 2010: 1250-1255

[12] Liu Ling-xia, Wang Dong-xia, Huang Min-huan, et al. A multi-dimensional trustworthy reference framework for network[C]// Proceedings of the 2012 Second International Conference on Instrumentation & Measurement, Computer, Communication and Control. China: IEEE, 2012: 1614-1618

[13] 林闯，彭雪海. 可信网络研究[J]. 计算机学报，2005，28(5)：751-758