基于邮局机制的 Web 服务安全集成模型的研究*)

孟庆华[1,3]　丁永生[1,2]
(东华大学信息科学与技术学院　上海 201620)[1]
(数字化纺织服装技术教育部工程研究中心　上海 201620)[2]
(潍坊学院计算机科学与技术系　山东潍坊 261041)[3]

摘　要　根据邮局服务的特征及其安全控制机制，提出了 Web 服务与安全的统一集成模型。设计了 Web 服务流安全环控制机制，用于保障 Web 服务动态合成过程中，群体 Web 服务安全的协同统一、Web 服务实体多项安全技术的集成管理以及 Web 事务的无缝连接。

关键词　Web 服务流，安全环，邮局服务，安全通道

Study on an Integrated Security Model for Web Services Based on Mechanism of Post Offices

MENG Qing-Hua[1,3]　DING Yong-Sheng[1,2]
(College of Information Sciences and Technology, Donghua University, Shanghai 201620)[1]
(Engineering Research Center of Digitized Textile & Fashion Technology, Ministry of Education, Shanghai 201620)[2]
(Department of Computer Sciences and Technology, Weifang University, ShandongWeifang 261041)[3]

Abstract　According to characteristics and its security control mechanism of post offices, we put forward an integrated model for Web services and its security. We also design closed security-ring mechanism for Web service flow in the model, in order to unify the security policies of community Web services, to integrity various security technology, and to contact transactions of Web services seamlessly.

Keywords　Post office service, Closed security-ring, Web service flow, Secure channel

1　引言

随着电子商务、电子政务、远程教育等网络服务的日益普及，Internet 已经发展成为事务网络、服务网络。面向服务的网络体系架构也越来越引起人们的研究兴趣，于是网络安全体系的研究也由保障信息的完整性、机密性、真实性、不可否认性，逐渐转变成保证服务的完整性、稳定性、真实性和不可否认性。因此，如何保证服务的动态安全，根据灵活的服务机制设计相应的安全策略就成为了研究重点。

为了保证 Web 服务的安全，W3C、OASIS 等有关标准化组织制定了一系列的安全标准及相关的安全描述语言[1,2]，IBM 和 MICROSOFT 也联合制定了 Ws-* 系列安全规范。XML-Signature 保证了数据的完整性[3]，XML-Encryption 保证了 XML 文档的机密性[4]，SAML (Security Assertion Markup Language)定义了实体在域间交换授权和认证的有关机制[5]，Ws-Security，Ws-Policy，Ws-Trust 和 Ws-Privacy 从 Web 服务的安全策略、信任管理、机密保护等方面也给出了相应的安全性标准[6~10]。但这些安全标准是静态的、组件式的，只是解决了一定范围内的安全问题。随着 Web 服务的合成优化及语义 Web 发展，服务的动态安全和整体安全又面临新的挑战[11]。

为了得到更加准确可靠、效率更高的“普适 Web 服务”，需要对 Web 服务优化整合与智能集成，但如何同时保证群体 Web 服务安全策略的统一，Web 服务实体多项安全技术的集成管理以及 Web 事务的安全无缝连接，这些都是随着 Web 服务组合过程中出现的新问题[12]。这些问题仅靠以上的安全标准不能彻底解决，需要人们针对 Web 服务组合提出服务与安全的统一整合框架。

邮局服务是人类社会最广泛的智能普适服务，它不仅具有高度兼容统一的特点，而且跨不同国家高度异构，又能保持服务的整体安全，这些特点都是我们完善 Web 服务与动态安全的追求目标。

因此，本文针对 Web 服务组合过程中服务与安全统一整合问题，借鉴邮局服务的有关原理尝试解决 Web 服务中的动态安全问题。基于邮局服务联盟框架和其安全控制机理，详细讨论了 Web 服务流安全环控制模型和安全环控制机制。

2　邮局服务模型

2.1　邮局服务

全球邮局服务无处不在，不同的国家和地区组成统一的邮政联盟，提供简单、安全、高效的邮局服务。邮局服务是跨国界的，它有着高度的异构性；邮局服务遍布地球的各个角落，有很好的普适性；邮局服务种类和手续基本保持不变，有很强的稳定性和兼容性；不管人们选择哪种邮局服务，邮局基本都可以保证物品信件的正确投递或回执确认，表现为邮局服务的完整性；邮局对不同安全级别的投递要求，会以不同的代价去实现，表现为邮局服务的服务质量保证(QoS)。邮局服务联盟的普适性、异构性、稳定性、完整性和本身服务的

*)基金项目：国家自然科学基金重点项目(60534020)，国家自然科学基金(60474037，60004006)，教育部新世纪优秀人才支持计划。孟庆华　博士研究生，从事网络和信息安全等研究。丁永生　博士，教授，博士生导师，从事智能系统、网络智能、NDA 计算、生物网络结构等研究。

QoS特点都为Web服务的组合优化、安全集成提供了很好的借鉴意义。

2.2 邮局服务内部运作机制及其安全控制策略

邮局服务以满足用户的服务质量为驱动，整体协调邮局内部资源，它们有着统一的服务安全控制策略，有分布式的服务监控记录和应急措施。邮局服务最常见的信件服务为平信、挂号信、特快专递等，图1为这几种邮件的服务质量安全控制流程图。

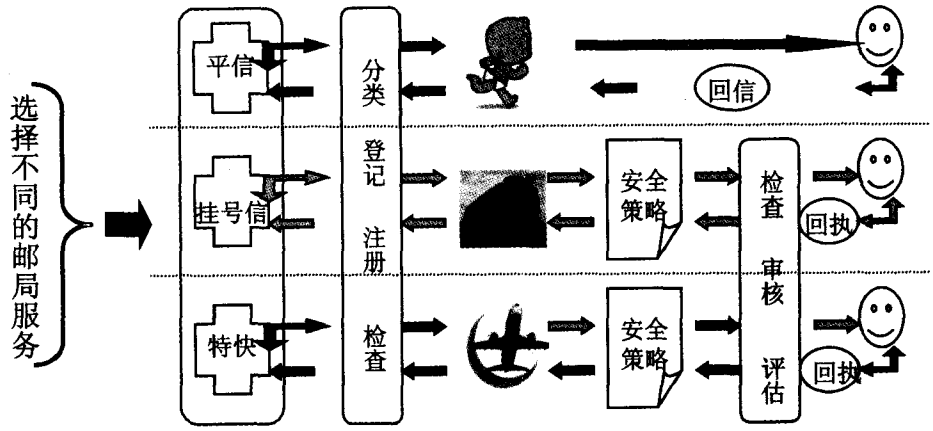

图1 不同种类邮局服务的安全控制闭环

分析以上几种邮件服务的特点可以看出，对于每一种不同质量的信件服务，都有着一整套的安全服务控制策略，这些安全控制过程表现为一个个完整的安全控制环，不同的安全控制环穿过不同的处理层次，组成动态的安全通道。这种安全闭环的特性有：

1)安全等级的闭环：在用户享受的邮局服务中，邮局的服务质量和采取的安全措施根据不同的服务种类而不同，而且这些信件在不同的安全措施的保护下保持彼此的隔离，即不同种类的邮件在不同的安全等级的“通道”中打包运输、管理、控制。

2)事务完整性闭环：终端用户的业务是完整的，无论哪种服务，终端用户平信的确认，挂号、特快的回执都构成事务的完整闭环。

3)服务监管闭环：在挂号信、特快专递的服务中，邮局都有邮件的到达检测、登记、投递等一系列的记录，它们构成闭环。一旦发生服务中断，可以根据这些监控纪录来恢复服务的继续，依靠这些记录保证邮局服务的可恢复性和容错性。

3 基于邮局服务的Web服务流的安全集成模型

根据邮局服务联盟的特点，我们设计了一种Web服务流安全控制集成模型，如图2所示。该模型分为4层：

(1)Web服务入口层：此层模拟了邮局大厅的服务入口功能。用户通过合法身份鉴定后，指定服务流的安全等级，由唯一性安全ID来标识Web服务流，然后根据Web服务流的服务质量要求，对Web服务进行注册、定位和路由，在相应的安全通道内接受相应的安全管理、审核和检查。此层是唯一允许用户跨不同安全等级Web服务进行操作的入口，但要求用户必须显式改变服务流的安全等级。

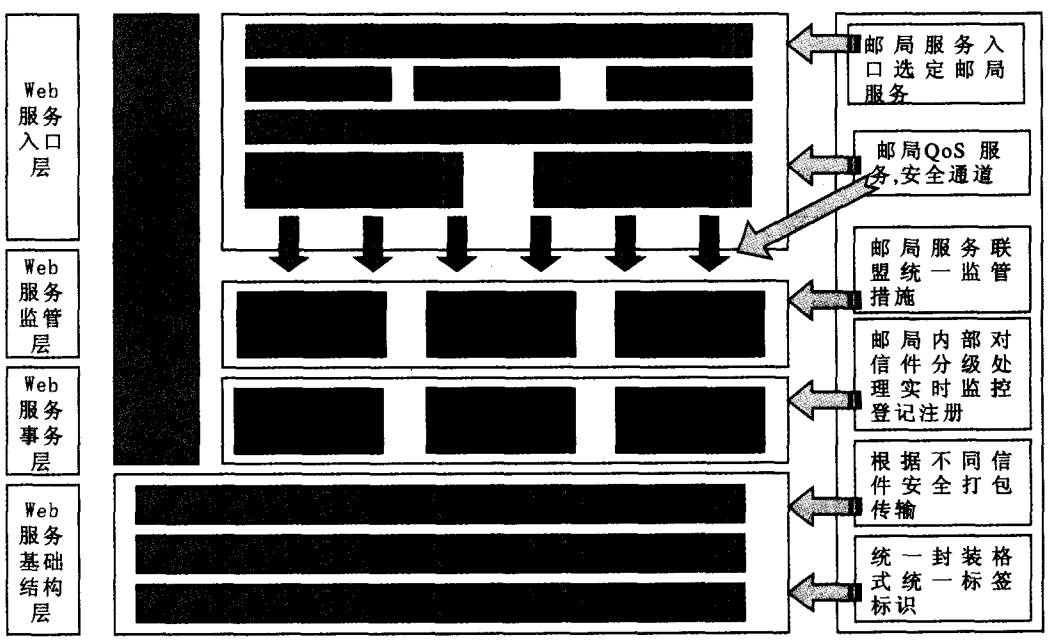

图2 Web服务流安全控制集成模型

(2)Web服务监管层：模拟了全球邮局服务联盟，对于高度异构的Web服务流实施统一监管。对Web服务流的安全闭环进行在线检测，来保障Web服务的动态安全，可以对网络攻击事件进行自我感知，同时对服务流中出现的错误进行

自我调整及恢复。

(3)Web服务事务层:模拟了邮局内部信件统一处理与协同工作的机理,为满足Web服务商业业务需求而构建的安全层。对Web服务请求,以事务的形式向一系列Web服务实体提交,由这些Web服务实体对事务进行协同处理,同时要对所有操作进行严格审核和记录,如果处理有误或不完整可进行事务回滚,并实时在线恢复。事务层按照自己的内部策略,有约束地对安全资源进行处理,保证了Web服务的事务完整性。

(4)Web服务基础结构层:利用有关Web服务标准对Web服务封装,同时借用WS-Security等有关安全规范来保证服务流细节的可靠性、安全性。

4 Web服务流的安全环控制机制

4.1 Web服务安全策略控制环

根据邮局内部运行和安全控制策略,设计了Web服务流安全控制环机制,如图3所示。Web服务流的安全环控制实施分三个层次进行:里面为内核层,主要完成Web服务的安全封装,根据服务请求的不同服务质量进行投递;中间为控制层,包括了Web服务安全模型的四个管理层次,分别进行Web服务管理、服务监管、事务处理、安全基础结构控制;外层为策略层,在Web多个服务实体之间进行安全策略控制。

策略层保证Web服务流安全环依然有着邮局服务控制环的三个特征(见表1):1)安全等级闭环,主要是指只有相同安全等级的服务流才可以在安全通道内交互,不同安全等级的服务流必须显式更改安全等级,在较低的安全通道进行事务的处理,这样可防止内容隐蔽通道的出现,而且在更改安全等级时需要做服务流的状态净化处理,这样可以预防时间隐蔽通道的出现;2)事务的完整性闭环,主要保持服务的完整、业务的连续处理,保证服务的可用性和稳定性;3)服务监管闭环,主要保证安全策略的正确执行,保证服务的正确授权,保护用户的隐私和机密。

研究Web服务流的各种情况可以发现,各种网络攻击都破坏了Web服务流的安全闭环。这些网络攻击我们定义为服务流的开环、自杀环、畸环、交叉环、伪闭环、交错环等(见表1),发现这些情况的存在都意味着潜在的入侵攻击或出现的网络服务故障等。

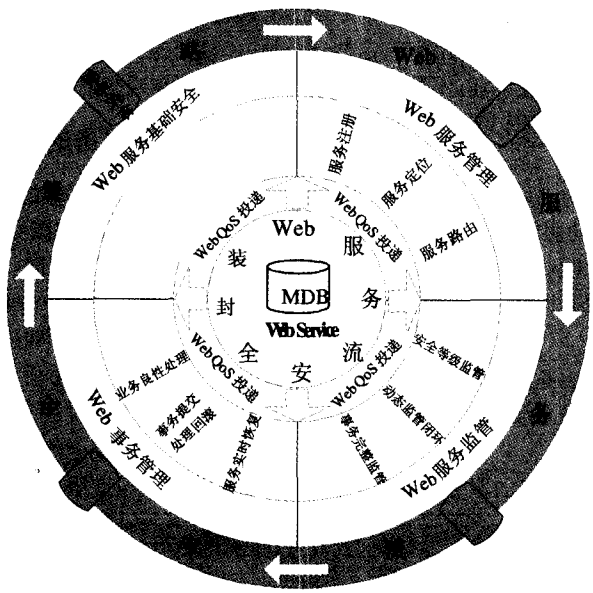

图3 Web服务流安全策略控制环

表1 服务流的安全环控制

	安全等级闭环	事务完整性闭环			服务监管闭环	
预防事件	交错环	开环	自杀环	交叉环	畸环	伪闭环
攻击事件	隐蔽通道 机密泄密	服务流中途截获;伪造服务流;服务流调包	拒绝服务攻击	脏数据的产生	恶意服务;非法服务器截获	中间人攻击
有关安全标准集成	XML-Encryption XML-Signature SSL, TLS, IPsec, Https	Ws-Federation Ws-Coordination Ws-Atomic Transaction Ws-Business Activity			Ws-Security Ws-Privacy Ws-Policy, Ws-Trust	
防范措施	在服务流安全监管层对Web服务流进行全局监控,对各种入侵实时检测、予以响应恢复。					

开环指的是服务流中途截获,或服务流出现假冒,服务包在层次间访问点检测验证失败被丢弃,均无法形成闭环。自杀环为用户主动有意发送大量服务请求包,目的在于阻塞某一服务端口,以造成拒绝访问服务攻击。畸环指的是服务流的确是访问闭环,但在中途遭遇恶意服务或被非法Web服务器刺探Web信息流携带的机密造成信息泄漏。交叉环指的是不同的服务流同时访问某一数据时可能出现脏数据的情况。伪闭环指的是服务流表面上是闭环但实际上出现了中间人攻击。交错环是指不同安全等级的服务流出现安全通道的交错,出现隐蔽通道,造成机密信息泄漏的情况。

因此,充分保证Web服务流的安全闭环,一方面可以采

(下转第113页)

战，这在项目信息管理中形成“信息孤岛”的同时，在资源分配和占有方面导致大型项目重复购置资源，而中小型项目却因资金不足而严重缺乏资源，使得项目资金和资源浪费和短缺现象并存，因此而严重制约了信息技术在项目管理中的应用，进而影响项目的建设和国家的经济发展。网格技术的引进不仅为系统集成提供了分布式、动态环境下协同工作更广阔的平台，也为项目广义资源的高度共享和有效利用奠定了基础。项目网格作为项目管理系统集成的支撑技术将成为这一发展的必然产物。

结束语 国内外学术和业界对项目管理系统集成方法上已有广泛的研究，但在综合运用本体论和网格技术等进行新一代集成方法研究方面尚未形成规模，也未见像样的研究成果。在全球项目管理信息化集成化的大环境下，能充分利用现代新技术的发展成果，借鉴国外项目管理的先进经验，并在其基础上根据我国国情进而创新，无疑具有重要的意义。我们近期对这一课题非常关注并进行了必要的研究。不难看出，基于本体论的系统集成方法和项目网格的研究正像本体论和网格计算理论一样，会有一段曲折的路，但其研究前景是喜人的，最终研究结果的成功是乐观的。

参 考 文 献

1 费奇，余明晖. 信息系统集成的现状与未来. 系统工程理论与实践，2001，3：75～78

2 Jaafar A. Life-cycle project management：A proposed theoretical model for development and implementation of capital projects. Project Management Journal，2000，31(1)：44～52

3 何清华，陈发标. 建设项目全寿命周期集成化管理模式的研究. 重庆建筑大学学报，2001，23(4)

4 Zhu Y，Augenbroe G. A Conceptual Model for Supporting the Integration of Inter-Organizational Information Processes of AEC Projects. Automation in Construction，2006，15(2)：200～211

5 Lee S-H ，Jeong Y-S. A System Integration Framework through Development of ISO 10303-based Product Model for Steel Bridges. Automation in Construction，2006，15(2)：212～228

（下转第 120 页）

（上接第 108 页）

取相应的 Web 安全标准和安全技术来主动保护 Web 服务流的安全闭环；另一方面还可以在安全分层模型中监控 Web 服务流的工作情况，对 Web 服务流各种意外情况实时检测、响应和恢复。

4.2 安全通道

为了保证安全闭环的三个属性，我们集成现有的安全规范组建了安全通道，不同安全等级的信息流封闭在相应的安全通道内进行访问及处理，如图 4 所示。安全通道分为三层，分别保证 Web 服务流安全闭环的三个属性：1）内层利用常规的安全技术 XML-Encryption，XML-Signature，SSL，TLS 和 IPsec 对不同等级的安全信息流加密传输，保证 Web 服务流安全等级闭环；2）中间层利用有关的安全规范 Ws-Security，Ws-Coordination，Ws-Policy 和 Ws-Trust 实施信任管理和安全策略的监管，实现 Web 服务流的监管闭环；3）外层利用 Ws-Federation，Ws-Atomic Transaction，Ws-Business Activity 和 Ws-Coordination 来保证 Web 服务流的事务完整性闭环。安全通道的组建不仅仅是安全规范的简单组合，而是这三种安全闭环属性的统一集成。

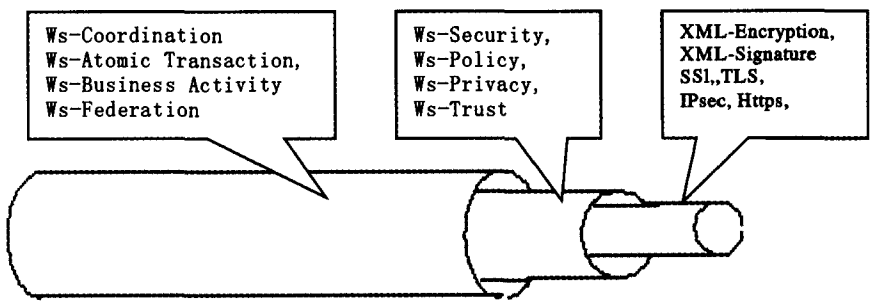

图 4 Web 服务流安全通道

结语 本文针对 Web 服务组合过程中服务安全整合的问题，基于邮局服务联盟框架及其安全控制机理，提出了 Web 服务流安全环控制模型和安全环控制机制。Web 服务流安全控制模型分 4 个层次协同控制 Web 服务静态和动态安全，安全环控制机制包括 3 个方面：安全等级闭环、服务完整性闭环、服务监管闭环。本文为动态 Web 服务组合中安全和服务的统一整合提出了一种可行的框架，可用于解决动态服务与动态安全的统一问题。

参 考 文 献

1 http://www.w3.org/Encryption/2001，6

2 OASIS Security Services TC. http://www.oasis-open.org/committees/tc_home.php? wg_abbrev=security. 2002，6

3 Box D，Curbera F，Hondo M，et al. Web Services Security. http://www-106.ibm.com/developerworks/library/ws-polfram/. 2003，3

4 XML-Signature Syntax and Processing. http://www.w3c.org/TR/2002/REC-xmldsig-core-20020212/；2002，2

5 OASIS-SAML Token Profile. http://www.oasis-open.org/committees/ 7837/WSS-SAML.pdf. 2004，4

6 Atkinson B，Della-Liberal G. Web Services Security (WS-Security) Version 1.0. http://msdn.microsoft.com/library/en-us/dnglobspec/html/ws-security.asp? Frame=true. 2002，7

7 Web Services Security Policy Language (WS-Security Policy). http://msdn.microsoft.com/ws/2002/12/ws-securitypolicy/. December 2002，4

8 Microsoft. Microsoft's Federated Security and Identity Roadmap. http://msdn.microsoft.com/library/default.asp? url=/library/en-us/dnWebsrv/html/wsfederate.asp? Frame=true. 2002，5

9 Web Services Secure Conversation Language (WS-Secure-Conversation). http://msdn.microsoft.com/ws/2005/02/ws-secure-conversation/2005，2

10 Web Services Trust Language (WS-Trust). http://msdn.microsoftcom/ws/2004/04/ws-trust/. April 2004，8

11 Abad M，Fournet C. Private authentication. Theoretic Computer Science，2004，322(3)：427～476

12 Bhatia R，Joshi D，Bettino E，Glamour A. Access control in dynamic XML-based Web-services with X-RBAC. In：The first international conference on Web services，Las Vegas，2003，6：23～26