组合Web服务业务流程访问控制技术研究综述

上超望[1,2] 刘清堂[1] 王艳凤[1]
(华中师范大学教育信息技术学院 武汉 430079)[1]
(青少年网络心理与行为教育部重点实验室 武汉 430079)[2]

摘 要 业务流程访问控制是保证组合Web服务增值安全应用的关键技术,着重论述了组合Web服务业务流程访问控制技术的研究现状及问题。首先对组合Web服务业务流程安全需求进行了分析,然后从组合Web服务业务流程访问控制模型、业务流程运行时访问授权约束、业务流程协同访问授权的一致性检验3个方面分析了业务流程访问控制核心技术的研究进展。最后,结合已有的研究成果,指出了目前研究的挑战以及未来的发展趋势。

关键词 组合Web服务,业务流程,访问控制
中图法分类号 TP301.9 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.7.021

Survey on Access Control Technology of Composite Web Services Business Process

SHANG Chao-wang[1,2] LIU Qing-tang[1] WANG Yan-feng[1]
(School of Educational Information Technology, Central China Normal University, Wuhan 430079, China)[1]
(Key Laboratory of Adolescent Cyberpsychology and Behavior, Ministry of Education, Central China Normal University, Wuhan 430079, China)[2]

Abstract Access control of business process is one of the key technologies in secure and reliable Web services composition value-added application. This paper briefly reviewed the state of the research for access control of business process in Web services composition. We firstly analyzed the security problems concerning business process. Then, we discussed the research progress on the key access control technology from three respects of access control model of composite Web services business process, authorization constraint of business process in run-time and consistency detection in authorization coordination. Finally, the discussion of future directions and challenges was presented.

Keywords Composite Web services, Business process, Access control

1 前言

组合Web服务通过集成组件服务生成新的、满足复杂需求的增值服务,已成为Web服务技术不断向前发展的技术动力和研究热点[1]。业务流程语言(Business Process Expression Language, BPEL)是专为Web服务组合应用而制定的规范,它从全局角度灵活编排Web服务资源之间的执行序列与消息交互,目前已成为组合Web服务业务流程事实上的标准[2]。

组合Web服务构建于开放、自治和动态的环境中,业务流程的调用比组件成员Web服务调用需要更多的访问控制需求。合法用户的非规范访问和操作与非法用户恶意访问行为都可能对组合Web服务应用系统的安全性和稳定性造成危害,业务流程的访问控制问题已经成为制约组合Web服务增值应用的关键要素,也是目前的难点问题[3]。

本文将对组合Web服务业务流程访问控制技术的最新研究进展进行分析和综述,主要讨论访问控制模型、运行时访问控制授权约束和协同访问控制的一致性检验等关键问题,并对目前存在的挑战和研究前景进行了探讨和展望。

2 组合Web服务业务流程安全需求分析

IBM和Microsoft提出的Web服务协议栈以分层的方式呈现服务发布、发现、绑定和组合功能,也为我们理解业务流程安全机制与其他安全机制的交互作用及其所处地位提供了全景视图,如图1所示。

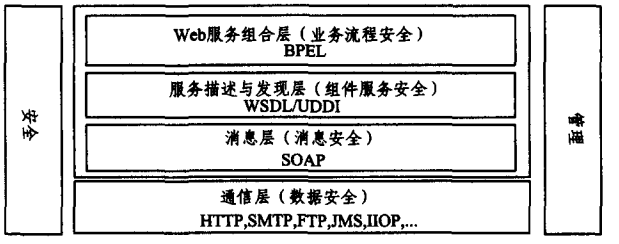

图1 Web服务协议栈结构图

在Web服务协议栈中,通信层确保浏览器和Web服务器之间重要数据传输的私密性和不可否认性,保护数据安全;消息层安全机制维护Web服务SOAP消息传递的完整性和机密性;服务描述和发现层涉及组件Web服务权限应用安全,在通信和消息层支持下实现Web服务资源的访问控制。

到稿日期:2014-07-05 返修日期:2014-09-25 本文受教育部人文社科项目(14YJA880058),国家自然科学基金项目(61272205),武汉市科技计划项目(2014060101010030)资助。

上超望(1980—),男,博士,副教授,主要研究方向为服务计算、数字版权,E-mail:scw@mail.ccnu.edu.cn;刘清堂(1969—),男,博士,教授,主要研究方向为数字版权、分布式计算;王艳凤(1965—),女,副高级馆员,主要研究方向为远程教育关键技术。

Web服务组合层是多Web服务安全集成应用的最高层，在BPEL流程的支持下，向下兼容服务描述与发现层、消息层和通信层的安全功能，实现分布式原子服务与业务流程的安全绑定和协同；向上和用户交互，确保用户访问在授权范围内执行。业务流程活动在数据流和控制流的驱动下经历状态变迁，是BPEL流程的基本单位，活动随着组合Web服务的销毁而销毁，具有协同性、交互性和时序性特点[4]。

与以系统为中心的访问控制机制不同，业务流程访问控制不仅要防范外部入侵，还要防止内部授权的非法使用，依据业务流程特征实现权限的连续性和可变性，捕获动态变化的安全需求[5]。具体说来，需要具备下面3项关键条件。

首先，组合Web服务业务流程的安全访问涉及用户、BPEL流程、活动、活动实例和组件服务等多个实体。访问控制机制应该能够合理规划这些实体，根据业务流程特点及时准确地进行权利许可的动态授予和回收，对不同粒度的资源访问与操作进行刻画，实现授权流和活动执行流的同步[6]，以防止安全泄露。

其次，BPEL业务流程活动在执行上下文驱动下进行状态迁移，业务流程活动所绑定服务资源的访问控制权限分配既要保证用户充分行使职权[7]，又不能超越权限范围，而应根据上下文环境实施主动的授权许可[4]，授予的权限只在流程活动实例的生命周期内有效。

最后，组合Web服务业务流程是在开放环境中由多个用户协作执行，业务流程活动之间存在分工权限执行的序关系和数据的交互传递关系[8]，为了避免个人的行动危及到组合Web服务系统的安全，一些敏感的流程活动需要不同的用户分离执行，以防止职权滥用[9]。

3 业务流程访问控制中的关键技术

在开放环境中，组合Web服务业务流程安全机制包含了丰富的内容[10]，依据组合Web服务业务流程安全需求分析，针对组合Web服务业务流程访问控制问题，本文将重点从以下3个关键的技术进行阐述：组合Web服务业务流程访问控制模型、业务流程运行时访问授权约束，以及业务流程协同访问授权的一致性检验。

3.1 组合Web服务业务流程访问控制模型

组合Web服务业务流程访问控制模型通过对业务流程安全所涉及的用户、客体、行为、授权、条件等概念进行规划和理论设计，从抽象层次描述安全策略所需的概念性框架。

目前，组合Web服务业务流程访问控制模型研究主要通过参考已有成熟模型来完成。利用基于角色的访问控制模型RBAC(Role Based Access Control)具有的便于管理、策略中立、支持权利和责任分离等特性，设计出的基于角色的业务流程访问控制模型是目前应用最为广泛的方式。典型研究如文献[11]在参数化RBAC模型基础上引入BPEL活动，提出自适应工作流访问控制模型AW-RBAC。文献[12]从访问主体的组织管理角度出发，在RBAC模型中嵌入团队和流程活动，提出面向团队执行的业务流程访问控制模型TEBM，构建层次性用户组织中可伸缩的访问控制策略。另外，文献[13]将业务流程整体作为RBAC数据元素集，提出了基于RBAC扩展的业务流程访问控制模型BPEL4RBAC。

另一种思想是利用基于任务的访问控制TBAC(Task Based Access Control)模型，将业务流程看成是多个任务组成的工作流，实现权限访问设计。代表性的如文献[14]直接借用TBAC模型将访问权限与活动绑定，在Web服务执行过程中提供动态实时的访问控制管理。文献[15]将BPEL流程动态执行特点与TBAC模型融合，将用户组织模型与BPEL模型融合，实现多层权限管理的业务流程访问控制约束。此外，文献[16]将角色的概念引入了TBAC活动、活动实例和执行依赖逻辑，提出角色和任务融合的流程访问控制RT-BAC(Role-Task Based Access Control)模型，利用流程会话实例实现权限的执行时控制和管理。文献[17]提出的方案和文献[18]的方法也沿用了这样的思路。

3.2 业务流程运行时访问控制授权约束

业务流程运行时访问控制授权约束通过用户和权限的动态指派，满足业务流程运行时通用的安全策略[19]。主要包括面向访问主体的动态职责分离约束和面向访问控制客体的动态权限约束。

(1)职责分离约束

职责分离约束通过对访问主体进行合理的组织分工来达到相互牵制和减少职权滥用的目的[20]。

静态职责分离过于苛刻和脱离实际，而动态职责分离可根据流程活动任务执行的环境动态指派执行者，是目前业务流程职责分离约束研究的主要内容。代表性的研究如魏永合[21]通过设定流程活动间的职责冲突关系，在业务流程运行阶段应用授权约束规则对授权执行计算，获取可以执行活动实例的无互斥用户集，从而实现职责分离。Samuel J B[22]在BPEL流程访问授权模型中引入条件约束，设置用户权限访问会话期职责良构建构的前置条件与过程条件，建立活动互斥和会话期用户集合互斥关系，使业务流程授权约束不仅支持活动级静态和动态职责分离，也支持活动实例级动态职责分离。David B等[23]利用用户工作向量表对执行期BPEL活动的角色进行差异化授权，避免给同一用户生成互斥的工作项，实现了职责分离约束。

(2)动态权限约束

动态权限约束确保特权授予和收回与活动执行同步，从流程活动基于依赖的衔接关系角度，满足动态授权；从单个活动安全执行角度，权限约束保障主体仅被授予完成当前流程活动访问所需的最小权限。

动态权限约束典型研究方案如文献[24]在RBAC的基础上提出的流程活动实例概念，通过上下文依赖描述流程活动实例之间的动态授权协同关系，同时依据权限生命周期与流程活动实例生命周期绑定实现权限的动态分配和撤销，以确保最小权限。Frederica P等[25]则将角色任务与许可矩阵相结合，通过矩阵关系数据表的映射计算出业务流程当前执行活动的最小权限和动态授权的布尔断言。另外，本文作者[26]根据Web服务组合计算环境中用户、资源、环境的属性信息，以UCON(Usage Control)模型为基础，基于授权、职责和条件3种运行时授权规则策略来检查BPEL流程活动与所绑定的Web服务执行信息，动态授予和回收业务流程访问权限，把握细粒度的动态权限约束需求。

3.3 业务流程协同访问控制的一致性检验

业务流程协同访问控制的一致性检验对动态执行环境下的业务流程授权进行合理性检测，确保活动访问授权要么全部执行，要么全部不执行，以维护组合Web服务业务流程访问控制策略的语义完整性。

文献[27]在不影响控制语义的情况下，将业务流程授权约束精细化为系统可实现的合理性规则和规则集合。利用最

小权限、动态授权和职责分离策略对授权约束合理性规则集进行约简，将业务流程活动访问的群体行为约束转变为集合运算，保障一致性协同授权目标的完成。Bertino E 等[28]将协同授权的安全需求表达成施加在用户和角色上的 XACML 约束准则，在业务流程活动授权策略属性分析、相似性分析和相融性计算的基础上，提出基于约束模型的一致性分析检测方法。文献[29]采用 Petri net 对业务流程活动协同授权执行的动态行为语义进行建模，对变迁或库所加入的活动授权偏序信息分析协同授权模型的状态变化和变迁的发生序列，实现协同授权约束一致性的动态检测。

另一种主要做法和趋势是利用图结构来提供精确语义，以实现可视化计算。典型的研究方案如文献[30]借助业务流程活动安全状态空间图，将业务流程协同访问授权的一致性检验转化为流程活动偏序执行状态图中闭合环的计算问题。文献[31]利用有向图对业务流程活动安全协同关系进行描述，通过有向图节点的覆盖关系来证明协同授权策略设置的正确合理性，获得流程协同授权的一致性断言。同样的思路在文献[32,33]中也可看到。

4 目前存在的挑战

组合 Web 服务的产生源于它所蕴含的巨大价值，业务流程安全已成为制约组合 Web 服务应用迫切需要解决的问题。目前组合 Web 服务业务流程访问控制仍存在挑战，主要表现在以下几个方面：

(1)业务流程访问控制模型的柔性设计问题。现有的访问控制模型无论是以 RBAC 还是以 TBAC 为基础，都是从传统的工作流的角度来设计访问控制模型，忽视了自治 Web 服务状态的可变性和持续性[34]。针对 Web 服务执行特点，加强 Web 服务对象的偏序交互特性和流程活动可持续权利的柔性使用控制研究，将是业务流程访问控制模型研究的热点[35]。

此外，现有的访问控制模型在业务流程每一次调整后都需要重新定义和描述各项安全约束[5,36]，如何柔性支持业务流程的动态变化，实现活动的动态添加、删除和多粒度授权修改，降低管理复杂度，还需要进一步探索。

(2)访问事务支持问题。业务流程内部逻辑设计决定了组合 Web 服务可能有多条执行路径[37]，如何在业务流程访问控制执行路径可变的情况下对活动实例异常终止或挂起进行监控，确保系统资源共享状态的一致性，对长事务所占用的 Web 服务资源有效进行并发调度[38]，动态提高系统的可靠性、容错性以及异常恢复将是一个关键的研究内容。

(3)跨域互操作问题。组合 Web 服务业务流程协同执行环境实现了单一管理域向多管理域的转变，不存在绝对信任的单一节点[7]，流程访问控制设计还必须面对用户跨自治域的角色管理与多重认证问题[39]。不同管理域的安全策略各异，如何实现业务流程多域执行时权限约束语义的描述、共享与提取[32]，仍是需要进一步研究的开放课题。

(4)用户隐私保护问题。组件服务在业务流程执行进程中必须频繁使用用户隐私数据，可能导致未经授权的用户隐私数据访问和误用问题，用户隐私保护问题不可回避。其中，面向用户的服务信任测量、隐私行为建模[12]、用户隐私策略与流程授权策略适配、用户隐私策略与协同服务策略容错[40]等，都是亟待解决的问题，具有广阔的研究空间。

结束语 组合 Web 服务为网络环境下大范围异构资源共享和集成提供了新的解决方案，但是流程本身的特性和开放环境的复杂性使得访问控制机制成为一个富有挑战性的课题。本文着重从业务流程访问控制模型、业务流程运行时授权约束和业务流程协同授权的一致性检验 3 个方面介绍了组合 Web 服务业务流程访问控制核心技术的研究现状及问题。

近年来，组合 Web 服务业务流程访问控制技术研究虽然取得了一些成果，但还面临不少挑战。特别是业务流程访问控制模型的柔性设计、业务流程安全访问事务支持、跨域互操作问题，以及用户隐私保护等，这些问题是组合 Web 服务业务流程安全应用中亟需解决的关键问题和未来的研究方向，也是我们正在从事的工作。

参 考 文 献

[1] 林日昶，赵文耘，等. 支持风险偏好的 Web 服务动态组合方法[J]. 中国科学：信息科学，2014，44(1)：130-141
Lin Ri-chang，Zhao Wen-yun，et al. Dynamic Web service composition approach supporting different risk appetites[J]. Scientia Sinica Information，2014，44(1)：130-141

[2] 余波. 应用 Petri 网改进 BPEL 程序的正确性[J]. 计算机应用研究，2011，28(9)：3348-3352
Yu Bo. Improving correctness of BPEL program with petri net [J]. Application Research of Computers，2011，28(9)：3348-3352

[3] Kristof G. Adaptive workflow composition in service-based systems[D]. Leuven：Katholieke university，2013
Yu Bo. Improving Correctness of BEPL Program with Petri net [J]. Application Research of Computers，2011，28(9)：3348-3352

[4] Roman K. Provision of service level agreements in human-enhanced service-oriented computing environments[D]. Vienna：Vienna University of Technology，2012

[5] Henrique J A，Jose J M. Performance evaluation of web services orchestrated with WS-BPEL4 People[J]. International Journal of Computer Networks & Communications，2010，2(6)：117-134

[6] Huy T，Uwe Z，et al. Compliance in service-oriented architectures：a model-driven and view-based approach[J]. Information and Software Technology，2013，54(5)：531-552

[7] Waldemar H，Patrick G，et al. An integrated approach for identity and access management in a soa context[C]// The ACM Symposium on Access Control Models and Technologies. 2011：21-30

[8] Anupa B，Prasanna N B. Intelligent compliance certification[J]. International Journal of Advanced Computer and Mathematical Sciences，2012，3(4)：394-404

[9] Emmanouela S，Anakreon M，et al. Rigorous analysis of service composability by embedding WS-BPEL into the BIP component framework[C]// Proc of 19th International Conference on Web Services. 2012：319-326

[10] Karsten T. A Unified framework for security visualization and enforcement in business process driven environments[D]. Stuttgart：University of Stuttgart，2011

[11] Leitner M，Rinderle M，et al. AW-RBAC：access control in adaptive workflow systems[C]// Proc of 6th International Conference on Availability. Reliability and Security，2011：27-34

[12] Jakob G. Team execution of multi-user workflows-modeling，dependability and optimization[D]. Munich：Technique University of Munich，2009

[13] Wang Xin. A framework to manage message level authorization in service oriented collaborative business processes[D]. Melbourne：Victoria University，2013

[14] Thomas R K, Sandahu R. Task-based authentication controls (TABC): a family of models for active and enterprise-oriented authentication management[C]//Proc of IFIP Workshop on Database Security. 1997:165-172

[15] Han R F, et al. A united access control model for systems collaborative commerce[J]. Journal of Networks, 2009, 4(4): 279-290

[16] Yu Ding-guo. Role and task-based access control model for Web service integration[J]. Journal of Computational Information Systems, 2012, 8(7): 2681-2689

[17] Rajender N, Gulshan A. An authorization mechanism for access control of resources in the web services paradigm[J]. International Journal of Advanced Computer Science and Applications, 2011, 2(6): 36-43

[18] Mark S, Jan M. Modeling process-related RBAC models with extended UML activity models[J]. Information and Software Technology, 2011, 53(2): 456-483

[19] Ganna M, Brucker A D, et al. Security and safety of assets in business processes[C]//Proc of the 27th Symposium on Applied Computing. 2013: 1667-1673

[20] Doglas R, Estrella J C, et al. Analysis of security and performance aspects in service-oriented architectures[J]. International Journal of Security and Its Applications, 2011, 5(1): 13-30

[21] 魏永合. 工作流环境下访问控制技术研究[D]. 沈阳: 东北大学, 2009
We Yong-he. Research on Technology of Access Control under Workflow[D]. Shenyang: Northeastern University, 2009

[22] Samuel J B. Modeling and enforcing workflow authorizations [D]. Zurich: Eth Zurich, 2012

[23] David B, Samuel J B, et al. Separation of duties as a service[C]// Proc of the 6th ACM Symposium on Information, Computer and Communications Security. 2013: 423-429

[24] Bernhand H, Stefan S, et al. Modeling and enforcing secure object flows in process-driven SOAs: an integrated model-driven approach[J]. Software and Systems Modeling, 2012, 5(2): 1-36

[25] Frederica P, Bertino E. An access-control framework for WS-BPEL [J]. International Journal of Web Services Research, 2008, 5(3): 20-43

[26] 上超望, 刘清堂, 等. 使用控制支持的组合 Web 服务业务流程动态访问控制模型研究[J]. 武汉大学学报(理学版), 2011, 57(5): 408-412
Shang Chao-wang, Liu Qing-tang, et al. A Research on UCON Enhanced Dynamic Access Control Model for the Business Process of Composite Web Services[J]. Journal of Wuhan University(Natural Science Edition), 2011, 57(5): 408-412

[27] Rafael A. An approach to data-driven detective internal controls for process-aware information Systems[C]//Workshop on Data Usage Management on the Web 2012. 2012: 20-25

[28] Bertino E, Martino D L, et al. Security for Web services and service-oriented architectures[M]. Berlin: Springer, 2010: 170-175

[29] Ahmed A. A compliance management framework for Business Process models[D]. Potsdam: University Of Potsdam, 2010

[30] Mohsen R. Security analysis for web services compositions [J]. International Journal of Scientific & Engineering Research, 2012, 3(5): 1-8

[31] Alberto C, Silvio R, et al. Automated validation of security-sensitive Web Services specified in BPEL and RBAC[C]//Proc of the 12th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing. 2010: 456-464

[32] Maria L, Juergen M, et al. SPRINT-responsibilities: design and development of security policies in process-aware information systems[J]. Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 2011, 2(4): 4-26

[33] Manuel M, Nicola D. Implementing workflow reconfiguration in WS-BPEL[J]. Journal of Internet Services and Information Security, 2013, 2(2): 73-92

[34] 许蕾, 徐宝文, 等. 一种面向用户需求的 Web 服务测试方法[J]. 计算机学报, 2014, 37(3): 512-522
Xu Lei, Xu Bao-wen, et al. A Testing Method for Web Services Focusing on User Requirement[J]. Chinese Journal of Computers, 2014, 37(3): 512-522

[35] Michel E J, Marc F, et al. Enforcing ASTD access-control policies with WS-BPEL processes in soa environments[J]. International Journal of Systems and Service-Oriented Engineering, 2011, 2(2): 37-59

[36] Ziyi S. Applying digital rights management to corporate information systems[D]. Lyon: National Institute of Applied Sciences, 2012

[37] Hristo K. A Survey on distributed access control systems for Web business processes[J]. International Journal of Network Security, 2009, 9(1): 61-69

[38] Fernando L, Julio D, et al. Towards automation of soa-based Business Process[J]. International Journal of Computer Science, Engineering and Applications, 2012, 2(2): 1-17

[39] Alfonso R, Eduardo F, et al. Secure business process model specification through a UML 2.0 activity diagram profile[J]. Decision Support Systems, 2011, 51(6): 446-465

[40] Zahra D, Behrouz T L. A model for specification, composition and verification of access control policies and its application to Web services[J]. Journal of Information Security, 2013, 3(2): 103-120

(上接第 67 页)

[12] 余维, 宋伟, 叶阳东. 因果链解耦的时间—概率模型[J]. 计算机集成制造系统, 2013, 19(10): 3536-3549
She Wei, Song Wei, Ye Yang-dong. Time-probability model for causal chains decoupling[J]. Computer Integrated Manufacturing Systems, 2013, 19(10): 3536-3549

[13] 吴欣, 郭创新. 基于贝叶斯网络的电力系统故障诊断方法[J]. 电力系统及其自动化学报, 2005, 17(4): 11-13
Wu Xin, Guo Chuang-xin. Power System Fault Diagnosis Approach Based on Bayesian Network[J]. Proceedings of the CenterSouth University-The Electric Power Supply Association, 2005, 17(4): 11-13

[14] 童晓阳, 谢红涛, 孙明蔚. 计及时序信息检查的分层模糊 Petri 网电网故障诊断模型[J]. 电力系统自动化, 2013, 37(6): 63-68
Tong Xiao-yang, Xie Hong-tao, Sun Ming-wei. Power systems fault diagnosis Model of Hierarchical fuzzy Petri Net of Check the meter and timing information[J]. Automation of Eletric Power Systems, 2013, 37(6): 63-68

[15] 孙静, 秦世引, 宋永华. 模糊 Petri 网在电力系统故障诊断中的应用[J]. 中国电机工程学报, 2004, 24(9): 74-79
Sun Jing, Qin Shi-yin, Song Yong-hua. Fuzzy Petri Nets and its Application in the Fault Diagnosis of Electric Power Systems [J]. Proceedings of the CSEE, 2004, 24(9): 74-79