组合Web服务访问控制技术研究综述

上超望 赵呈领 刘清堂 王艳凤
(华中师范大学信息技术系 武汉 430079)

摘 要 访问控制技术是保证Web服务组合增值应用安全性和可靠性的关键技术。主要论述了组合Web服务访问控制技术的研究现状及其问题。首先论述了组合Web服务安全面临的挑战;接着基于层的视角对组合Web服务安全问题进行了分析;然后从组合Web服务访问控制体系构架、原子安全策略的一致性协同和业务流程访问控制3个方面分析了组合Web服务访问控制核心技术研究的进展;最后,结合已有的研究成果,指出了目前研究的不足以及未来的发展趋势。

关键词 组合Web服务,访问控制,框架,安全策略,业务流程
中图法分类号 TP393 **文献标识码** A

Survey on Access Control Technology of Web Services Composition

SHANG Chao-wang ZHAO Cheng-ling LIU Qing-tang WANG Yan-feng
(Department of Information Technology, Central China Normal University, Wuhan 430079, China)

Abstract Access control 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 in Web services composition environment. We firstly discussed the challenges to Web services secure composition. Subsequently we analysed the security problems concerning Web services composition from a hierarchical perspective. Then, we discussed the research progress on the key access control technology from three respects of Web services composition access control architecture, atomic security policy consistent coordination and business process authorization. Finally, the conclusion was given and the problems were pointed out, which should be resolved in future research.

Keywords Web services composition, Access control, Architecture, Security policy, Business process

1 引言

Web服务简化了复杂的软件应用方式,已成为面向服务的体系架构(SOA)中最成功、最流行的形式。组合Web服务提供了将分布式环境中的原子服务整合成新的大粒度增值服务的能力,它除了要处理合成过程中服务调用的顺序、服务间的数据流以及执行控制流之外,还必须提供整个整合服务的安全性、可靠性与可扩展性保障[1]。对于如何将潜在的不可信的服务合成为一个可信的应用或服务,组合Web服务安全面临众多挑战,主要表现在以下几个方面:

(1)组合Web服务的每个自治服务成员必须对自己的资源具有完全控制能力的独立个体,全局访问控制规则的实施必须尊重成员服务的局部独立控制权。

(2)成员Web服务在增值合成中互相并不"认识",如何在成员安全管理域之间实现跨应用的安全表述和集成?

(3)组合Web服务访问控制机制在业务流程级别和多Web服务协同级别的安全表述粒度会存在差异,组合服务的整体安全管理机制需要刻画各种不同粒度的资源与操作。

(4)多个Web服务集成涉及到了服务安全边界的跨越,为了解决不断发展中的新应用模式,组合服务的安全机制需要提供开放式体系结构,实现可扩展的安全访问机制。

Web服务组合技术的产生来源于它所蕴含的巨大价值,安全问题已经成为制约Web服务组合技术发展迫切需要解决的问题,访问控制是其中的关键部分,也是目前的难点[2]。

本文着重介绍了组合Web服务访问控制技术的研究现状和发展趋势。第2节基于Web服务协议栈分析了组合Web服务面临的安全问题,第3节重点讨论了组合Web服务的访问控制技术,最后总结全文并提出了需要进一步解决的问题。

2 基于层的组合Web服务安全问题分析

完整的Web服务体系需要一系列现有和新发展的开放协议与规范来支撑,它们构成了Web服务的协议栈。如图1所示,Web服务协议栈采用层级结构,从底层到高层分为:通信层,基于HTTP、SMTP、JMS和IIOP等协议在应用程序间递送XML信息;消息层,基于SOAP协议确保消息在任何网络连接终端都可以被理解;服务描述与发现层,通过WSDL实现抽象接口与具体实现分离,基于UDDI进行服务发布;

到稿日期:2010-11-30 返修日期:2011-03-03 本文受湖北省自然科学基金(2009CDA135),国家教育规划课题(BCA100024),武汉两型社会建设制度创新专项资金,华中师范大学自主科研基金专项项目"Web服务安全组合中的访问控制技术研究"资助。
上超望(1980-),男,博士,讲师,主要研究方向为信息安全、分布式计算等,E-mail:shangchaowang200650@yahoo.com.cn。

Web 服务组合层，基于 BPEL4W 将原本孤立的系统融入企业整体流程中。

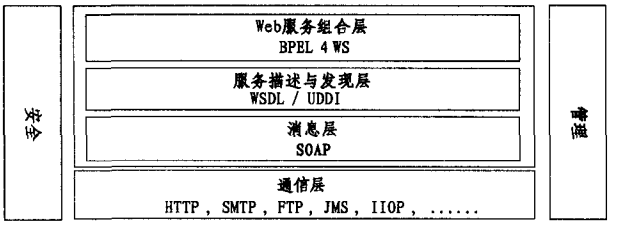

图 1 Web 服务协议栈结构图

Web 服务的协议栈为我们展示了从独立原子服务底层通信到多个服务基于设计逻辑协同应用中涉及到的各个技术，也为我们在服务组合级别基于层的思想认识组合 Web 服务安全问题提供了很好的视角。

通信层安全是组合 Web 服务实现系统安全耦合应用的基础，主要确保浏览器和 Web 服务器之间的重要数据传输，为高层的应用提供透明的服务，保证传输信息的私密性、可靠性和不可否认性[3]。

消息层安全机制通过对 SOAP 协议的扩展，在 SOAP 头消息中添加数字签名、加密信息和安全令牌等安全信息，确保 Web 服务环境下对消息的认证并保证消息的完整性、保密性[3]。

服务描述和发现层通过为独立原子服务提供细粒度的访问控制，控制用户对组合 Web 服务自治成员的访问和实现 Web 服务对用户的授权，捕获动态变化的安全需求，保证 Web 服务自治成员只能被具有访问权限的用户使用。

服务合成层是安全实现的最高层级，需要确保服务组合体可被合法主体按规定权限执行，对组合服务的协同访问进程进行授权约束，防止职权滥用和越权行为[4]。

3 组合 Web 服务访问控制中的关键技术

访问控制通过限制对关键资源的访问，授予系统合法用户访问资源所必需的操作权限，防止非法用户的侵入或因为合法用户的不慎操作而造成的破坏。组合 Web 服务牵涉到不同域中服务的整合与调用。弱封闭计算环境对组合 Web 服务安全提出了多方面的需求，涵盖了数据完整性、机密性、不可否认性、鉴别、审计、安全体系架构、业务流程授权、多策略一致的互操作等多个方面[5]。对于组合 Web 服务访问控制技术，本文将从以下 3 个关键技术进行阐述：组合 Web 服务访问控制体系构架；成员服务安全策略的一致性协同；组合 Web 服务业务流程安全授权等。

3.1 组合 Web 服务访问控制体系构架

针对松散耦合的计算环境，组合 Web 服务的安全体系架构需要能够考虑集中分布式环境中各成员服务的安全需求，构成一个 Web 服务多域动态协作的安全耦合环境。

一些组织和团体正在制定相关的安全规范。例如 W3C 制定的规范主要集中在 XML 的安全方面；OASIS 制定了 SAML 和 XACML 等来实现信任迁移与访问控制；IBM、Microsoft、VeriSign 等业界主流公司制定了 WS-* 系列规范等。由于业界的应用推动，目前 WS-* 系列安全规范具有比较大的前景。但是已有的 Web 服务安全规范只关注 Web 服务的某一项安全需求，需要合理的组合 Web 服务的安全框架[6]。

目前，有很多学者对组合 Web 服务的安全体系结构做了有益的研究与探索，提出了多个组合 Web 服务安全框架，并且各有特点。具有代表性的是吴敏[7]采用层次结构建模方法来降低安全 Web 服务系统分析和设计的复杂性，融合逻辑模型和实施模型两个方面，提出了一个 Web 服务的安全框架 WSSF(Web Services Security Framework)。Dong Huang[8]从组合 Web 服务运算执行角度来研究安全问题，忽略通信安全等底层的安全支持机制，提出了一个基于语义策略的组合 Web 服务安全框架 SPSFBP(Semantic Policy-Based Security Framework For Business Processes)，框架分为业务流程层、策略层和服务层。框架在策略层支持运行时策略的管理和执行，通过基于本体的策略来进行安全推理和策略协商。Michael M 等[9]从业务流程和服务两个层级提出了一种跨域服务组合访问控制架构模型 2LACFSC(Two-Level Access Control Architecture For Cross-Organisational Federated Service Composition)，并且给出了 2LACFSC 的初步解决方案。Charfi A 等[10]基于面向切面的思想对 BPEL4WS 进行扩展，提出了一种基于 WS-* 安全规范的服务安全组合框架 APCBPEL(Aspect-Based Process Container For Securing Web Services Composition)。APCBPEL 通过策略的流程部署来检测服务合成中全局安全策略和成员服务安全策略的一致性。本文作者[11]以 Web 服务协议栈为基础，采用层次结构建模方法从组合 Web 服务业务流程权限的动态授权管理和成员服务访问控制的一致性融合两个方面构建可信协同，把握用户对 Web 服务组合的安全需求。

企业研发方面，微软和 IBM 共同定义了一个 Web 服务安全概念性协议栈模型，该模型以 WS-Security 规范为核心，通过消息认证、消息完整性和消息机密性 3 种机制来扩展 SOAP 消息，保证 SOAP 消息的安全性，并通过定义 WS-Policy、WS-Trust 等规范，保证了上层应用系统的安全性[12]。

3.2 成员服务安全策略的一致性协同

组合 Web 服务的自治成员提供者都是独立的实体，他们对自己的资源具有完全的控制能力[13]。基于策略的 Web 服务访问控制机制能够使描述和实现机制相分离，也使分布式实体的安全访问规则跨域集成成为可能。组合 Web 服务构建于开放的动态环境中，各原子服务之间不存在直接的信任关系，原子服务之间相互依赖，以一种协同的方式运行。即使对每个原子服务的策略都加以正确的规定，多样化的区域策略之间协同实施时仍可能导致冲突[14]，进而影响服务合成的质量和健壮性，降低用户满意度。有效实现组合 Web 服务多域协同环境中成员安全访问策略一致的动态耦合一直是 Web 服务安全组合研究的热点问题[15]。

很多学者对组合 Web 服务计算环境下安全策略的一致协同问题进行了有益的研究，并且提出了多个解决方案，主要分为以下两个方面：

(1)基于原子服务策略融合的方式

基于原子服务策略融合的方式通过基于语法的一致性来消解多策略冲突问题，并将这些策略融合成为一个策略来提供一个统一的对外访问控制机制。代表性的是 Yau S 等[16]提出基于策略协商的新生资源适配协议和基于相似度的自适应融合算法来实现访问控制策略融合。Satoh F 等[17]基于谓词逻辑，在研究了自底向上、自顶向下的两种安全策略融合方法的基础上，提出了一种面向服务合成的安全策略自动创建

机制。Bruns G 等[18]则通过策略融合操作算子和策略精细检测来支持策略冲突分析，同时定义了一种策略融合语言来解决策略融合中的共有问题。

基于原子服务策略融合的方式之优点在于访问判决计算简单，及时响应能力强，但是面临的问题是对于资源众多的系统，尤其是在大型的企业级系统中，将所有的资源都放在单一的安全策略的控制下无法保证对系统资源的细粒度控制，融合策略维护难度比较大。

(2)基于原子服务策略形式化推理的方式

原子服务策略形式化推理的方式是在对策略进行解析和建模的基础上对策略决策规则进行推理。代表性的是 Benferhat S 等[19]在对访问控制策略的基本概念进行形式化定义的基础上，在策略层面通过规则与规则或策略与策略之间的横向关联关系来检测冲突，根据安全策略规则的分层采用了可能性逻辑和词典推测方式来处理策略中的冲突问题。Karat J 等[20]提出了一种跨异构域的三层访问控制策略管理框架，它将访问控制策略精细化为计算机系统中可以实现的规则和规则集合，并抽取规则集中的结构元素使用语法和逻辑操作来实现策略的一致性。Kamoda H 等[21]则提出了基于 Free Variable Tableaux(自由变量列表)的冲突检测方法，其基本思想是首先把策略规则转化为逻辑描述语言，然后判断策略之间是否产生冲突。

目前，美国普渡大学 Bertino E 教授领导的研究团队正从事开放环境下安全策略管理的研究，旨在建立一个跨域环境中安全策略的集成管理框架 EXAM[22]，其方法是在访问控制策略属性分析、策略相似性分析、策略分解和相融性计算的基础上，对弱封闭协同环境下多安全策略一致性推理问题进行研究。

基于原子服务策略形式化推理方式的优势在于准确性高、策略判决更新能力强，缺点是策略与策略之间的横向关联冲突计算方式对于全局规则下的隐性冲突考虑不足，同时执行上下文环境因素影响的考量也需要进一步完善。

3.3 组合 Web 服务业务流程访问控制

组合 Web 服务安全的另一个关键问题是业务流程访问控制。组合 Web 服务业务流程执行语言 BPEL4WS 综合了 XLANG 和 WSFL 的优点，将松散的服务捆绑组合成完整、功能强大的业务流程。但是 BPEL4WS 没有涉及访问控制机制，企业资源集成机构无法利用 BPEL4WS 语言所提供的设施进行权限管理，以保护关键资源，这在很大程度上影响了业务流程的可靠性、安全性[23]，也使得服务业务流程对访问控制的需求越来越迫切。

为建立可信的组合 Web 服务运行环境，研究者提出了很多适合 Web 服务组合业务流程的访问控制模型。典型的基于角色的工作流访问控制模型是 Thomas R K 等[24]提出的基于任务的访问控制模型 TBAC。TBAC 从任务的角度来构建安全的访问控制框架，在任务处理过程中提供动态实时的访问控制管理。Sandhu R 等[25]提出的基于角色的访问控制(RBAC)实现了用户与权限的逻辑分离，有效地提高了系统安全管理的效率，RBAC 的主要不足在于没有提供对业务流程的支持，难以满足业务流程管理系统的访问控制需求。Atluri V 等构造了一个基于 RBAC 的工作流授权模型(WAM)[26]，在 WAM 模型中工作流的每个任务都和某个适当的授权模板相联，保证了授权流与工作流的同步。

另外，将业务流程特点与访问控制模型融合，也是一个研究趋势，代表性的有 Wang Xin[27]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。Liu Peng 等[28]则将业务流程所捆绑的成员 Web 服务看作被保护对象，通过扩展经典的 RBAC 模型得到组合服务业务流程访问控制模型 WS-RBAC。Bertino E[29]基于 XACML 在安全策略设计时支持授权约束描述及其扩展，提出了基于角色的业务流程访问控制模型 RBAC-WS-BPEL。Han R F 等[30]在基于业务流程活动的基础上通过扩展 BPEL4WS 的安全策略规范来表述业务流程协同授权约束，提出了组合 Web 服务业务流程访问控制模型 UACM。

组合 Web 服务业务流程活动调用比一个单独 Web 服务调用需要更多的访问控制需求，必须遵循动态授权、最小权限原则和职责分离原则。上述研究为业务流程访问授权研究提供了很好的理论框架基础，然而，组合服务自治成员之间的动态协同性、分工性、依赖性和交互性特点导致了业务流程协同授权的分布化、复杂事务化，也对访问控制授权约束的一致性提出了更高的要求，这也将会是一个新的研究点[31]。

结束语 本文从访问控制体系构架、成员服务安全策略的一致性协同和业务流程访问控制 3 个方面论述了组合 Web 服务访问控制关键技术的研究现状及其问题。近年来在组合 Web 服务访问控制技术研究方面虽然取得了一些成果，但是组合 Web 服务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问题[32]。目前的研究还处于开始阶段，也需要其它相关技术的研究支持，例如安全策略的异构消解、安全事务匹配等，要发挥组合 Web 服务应有的潜能，仍然有许多工作要做。

参 考 文 献

[1] Smeureanu I, Diosteanu A. Knowledge Dynamics in Semantic Web Service Composition for Supply Chain Management Applications[J]. Journal of Applied Quantitative Methods, 2010, 5(1):1-13

[2] Shravani D, Suresh P V, Padmaja B R, et al. Web Services Security Architectures Composition and Contract Design Using RBAC [J]. International Journal on Computer Science and Engineering, 2010, 8(2):2609-2615

[3] Zein R, Camille G, et al. Policy-Driven and Content-Based Web Services Security Gateway[J]. International Journal of Network Security, 2009, 18(1):253-265

[4] Mohamed S, Kamal B, et al. Web Services Discovery in Secure Collaboration Environments[J]. ACM Transactions on Internet Technology, 2007, 8(1):52-74

[5] Christian E, Sebastian K, et al. Model Driven Development of Access Control Policies for Web Services[C]// Proc. of 2008 International Conference on Software Engineering and Applications. 2008:165- 172

[6] Hassan S G, Kadir W M, et al. AIMO: An Effective Approach to Support Semantic Web Service Discovery and Composition[J]. International Journal of Computational Science, 2009, 3(2):133-150

[7] 吴敏. WebServices 访问控制机制及其整合研究[D]. 上海：东华大学信息科学与技术学院，2006:29-40

(下转第 22 页)

national Colloquium on Automata, Languages and Programming. 2009:328-340

[56] Ivanov A O, Tuzhilin A A. Minimal networks: the Steiner problem and its geberalization[M]. CRC Press, 1994

[57] Hochbaum D S. Approximation Algorithms for NP-hard problems[M]. Boston, MA: PWS Publishing Company, 1996

[58] Halperin E, Krauthgamer R. Polylogarithmic inapproximability [C]// Proceedings of the 35th Annual ACM Symposium on Theory of Computing. 2003:585-594

[59] Bern M, Plassmann P. The Steiner problem with edge lengths 1 and 2[J]. Information Processing Letters, 1989, 32:171-176

[60] Prömel H J, Steger A. The Steiner tree problem: a tour through graphs, algorithms and complexity[Z]. 2002

[61] Polzin T, Daneshmand S V. Practical portioning-based methods for the Steiner problem[J]. Lecture Notes in Computer Science, 2006, 4007:241-252

[62] Faigle U, Kern W. Computational complexity of some maximum average weight problems with precedence constraints[J]. Operations Research, 1994, 42(4):688-693

[63] Ravi R, Sundaram R. Spanning trees short or small[J]. SIAM Journal on Discrete Mathematics, 1996, 9(2):178-200

[64] Chen J, Kanj I. On the effective enumerability of NP problems [C]// IWPEC. 2006:215-226

[65] Downey R, Fellows M. Fixed parameter tractability and completeness[M]. Complexity Theory: Current Research. Cambridge University Press, 1992

(上接第 15 页)

[8] Dong Huang. Semantic Policy-Based Security Framework for Business Processes[C]// Proc. of 2005 Semantic Web and Policy Workshop. 2005:27-31

[9] Michael M, Wolter V, Meinel C. Access Control for Cross-Organisational Web Service Composition[J]. Journal of Information Assurance and Security, 2007, 2(2):155-160

[10] Charfi A, et al. Using Aspects for Security Engineering of Web Service Compositions[C]// Proc. of In Proc. of the IEEE International Conference on Web Services. 2005:59-66

[11] 上超望, 杨宗凯, 等. 组合 Web 服务分层安全模型研究[J]. 计算机科学, 2010, 2(2):113-117

[12] Ivonne T, Christoph M. An Identity Provider to Manage Reliable Digital Identities for SOA and the Web[C]// Proc. of 2010 IEEE Symposium on Identity and Trust on the Internet. 2010: 26-36

[13] Demian A D, Ananthanarayana V S. Dynamic Web Service Composition Based on Operation Flow Semantics[J]. International Journal of Computer Applications, 2010, 26(1):4-14

[14] Kim K I, Choi W G, et al. A Collaborative Access Control Based on XACML in Pervasive Environments[C]// Proc. of 2008 IEEE Conference on Hybrid Information Technology. 2008:7-13

[15] Yannick C, Mohamed A M. Automatic Composition of Services with Security Policies[C]// 2008 IEEE Congress on Services. 2008:529-538

[16] Yau S, Chen Z. Security Policy Integration and Conflict Reconciliation for Collaborations among Organizations in Ubiquitous Computing Environments[C]// Proc. of 2008 IEEE Conference on Ubiquitous Intelligence and Computing. 2008:3-19

[17] Satoh F, et al. Security Policy Composition for Composite Services[C]// 2008 IEEE Conference on Web Engineering. 2008: 86-97

[18] Bruns G, Daniel S, et al. A Simple and Expressive Semantic Framework for Policy Composition in Access Control[C]// 2007 ACM workshop on Formal Methods in Security Engineering. 2007:12-21

[19] Benferhat S, et al. A Stratification Based Approach for Handling Conflicts in Access Control[C] //2009 ACM Symposium on Access Control Models and Technologies. 2009:189-195

[20] Karat J, et al. A Policy Framework for Security and Privacy Management[J]. IBM Systems Journal, 2009, 53(2):532-541

[21] Kamoda H, Yamaoka M, et al, Access Control Policy Analysis Using Free Variable Tableaux[J]. Journal of Transactions of Information Processing Society of Japan, 2006, 47(5): 1515-1529

[22] Bertino E, et al. EXAM-a Comprehensive Environment for the Analysis of Access Control Policies[J]. Journal of the ACM, 2009, 12(6):238-240

[23] Federica P, et al. An Access-Control Framework for WS-BPEL [J]. International Journal of Web Services Research, 2008, 5 (4):20-44

[24] Thomas R K, Sandhu R. Task-Based Authentication Controls (TABC): A Family of Models for Active and Enterprise-Oriented Authentication Management[C]// Proc. of 1997 IFIP Workshop on Database Security. 1997:165-172

[25] Sandhu R, Coyne E, et al. Role based access control models[J]. IEEE Computer, 1996, 29(2):38-47

[26] Atluri V, et al. Efficient Security Policy Enforcement for the Mobile Environment[J]. Journal of Computer Security, 2008, 16 (4):439-475

[27] Wang Xin, et al. BPEL4RBAC: An Authorisation Specification for WS-BPEL[C]// Proc. of 2008 Web Information Systems Engineering. 2008:381-395

[28] Liu Peng, Chen Zhong. An Access Control Model for Web Services in Business Process[C]// Proc. of 2004 Web Information Systems Engineering. 2004:292-298

[29] Bertino E, et al. Access Control and Authorization Constraints for WS-BPEL[C]// Proc. of 2006 International Conference on Web Services. 2006:275-284

[30] Han R F, et al. A United Access Control Model for Systems Collaborative Commerce[J]. Journal of Networks, 2009, 4(4): 279-290

[31] Farhan H, et al. QoS Based Dynamic Web Services Composition & Execution[J]. International Journal of Computer Science and Information Security, 2010, 7(2):147-153

[32] Hristo K. A Survey on Distributed Access Control Systems for Web Business Processes [J]. International Journal of Network Security, 2009, 9(1):61-69