组合Web服务分层安全模型研究

上超望[1] 杨宗凯[1] 刘清堂[1,2] 赵呈领[1,2]
(华中师范大学教育信息技术工程研究中心 武汉 430079)[1]
(华中师范大学信息技术系 武汉 430079)[2]

摘 要 随着Web服务技术的应用与发展,组合Web服务的安全问题日益突出。已有的Web服务安全规范只是指定实现单独的自治Web服务安全需求应该遵循的协议,尚没有一个被广泛接受的组合Web服务安全体系架构。指出了现有的Web服务组合安全框架研究的不足,分析了组合Web服务的安全模型的要求。针对Web服务应用模式,提出了一种基于Web服务协议栈的组合Web服务分层安全模型(HSM-WSC),并对每个层的安全功能进行了论述。HSM-WSC模型具有灵活性和可扩展性,能够满足Web服务组合的安全需求。最后还给出了HSM-WSC模型的实施机制。

关键词 安全模型,Web服务组合,可信协同,业务流程
中图法分类号 TP393 **文献标识码** A

Research on Hierarchical Security Model of Web Services Composition

SHANG Chao-wang[1] YANG Zong-kai[1] LIU Qing-tang[1,2] ZHAO Cheng-ling[2]
(Research Center for Education Information on Technology, Central China Normal University, Wuhan 430079, China)[1]
(Dept. of Information Technology, Central China Normal University, Wuhan 430079, China)[2]

Abstract With the development and application of Web services technologies, the security issues of Web services composition are increasingly prominent. The present security specifications of Web services are only specified for a single Web service, and there is no architecture for security of composite Web services being approved by most people. The insufficiency of present research on Web services composition security architecture was pointed out and the requirements of Web service composition security were analyzed. We proposed a hierarchical security model for Web services composition (HSM-WSC) based on Web services stack according to the Web service application mode, and analyzed the security function of each layer in the model. This model has the advantages of flexibility and extensibility, and satisfies various requirements of secure composite Web services. The paper also described the Implementation architecture of HSM-WSC in the end.

Keywords Security model, Web services composition, Reliable cooperation, Business process

Web服务组合有效地合成分布于网络中的各种功能服务,形成功能强大的企业级流程服务,以实现企业间的优势互补和资源共享,是Web服务发展过程中的一个重要步骤。组合Web服务所处的环境更为开放和松散,各种不确定性因素更多,为有效访问带来了许多新的安全挑战[1]。

在Web服务安全领域,一些组织和团体正在制定相关的安全规范。其中,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,主要是用于实现访问控制;IBM, Microsoft, VeriSign等业界主流公司制定了WS-*系列规范。由于业界的应用推动,WS-*系列安全规范具有比较大的前景。然而,已有的Web服务安全规范只是关注某一个Web服务的安全需求,目前还没有一个被广泛接受的组合Web服务的安全体系架构。

组合Web服务的安全体系架构,也就是集中分布式环境中各成员服务的安全需求,构成一个Web服务多域动态可信协作的安全耦合环境[2]。本文基于Web服务协议栈,提出了一种组合Web服务分层安全模型(HSM-WSC),介绍了相关研究工作和进展,讨论了组合Web服务分层安全模型的需求,详细描述了HSM-WSC模型,并给出了模型在Web服务可信组合实施环境中的原型系统。

1 相关工作及HSM-WSC模型的提出

1.1 相关研究工作

目前,有很多学者对组合Web服务的体系结构做了有益的研究与探索,并且提出了多个组合Web服务安全框架,各自有不同的特点并依据不同的安全规范。代表性的是:吴敏[3]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,提出了一个Web服务的安全框架WSSF。然而,WSSF没有考虑多个异构Web服务访问控制机制的有效管理和一致的可信协同问题。Huang Dong[4]提出了一个

到稿日期:2009-03-19 返修日期:2009-05-25 本文受国家高技术研究发展计划(863计划)(2008AA01Z127,2008AA01Z131),国家自然科学基金项目(60673010)资助。
上超望(1980—),男,博士生,主要研究方向为信息安全、分布式计算等,E-mail:shangchaowang200650@yahoo.com.cn。

基于语义策略的组合 Web 服务安全框架，框架分为业务流程层、策略层和 Web 服务层。该框架在策略层支持运行时策略管理和执行，通过基于本体的策略来进行安全推理和策略协商。然而，该框架只是从组合服务运算执行的角度来研究安全问题，没有谈及底层的安全机制支持实施问题，比如通信安全。Michael Menzel[5]等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模型，需要进一步给出具体解决方案。Anis Charfi[6]等基于面向切面的思想对 BPEL 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。他们的方案通过策略的流程部署来检测服务组合中组合服务安全策略和成员服务安全策略的一致性，但是没有考虑到分布式异构访问控制模型的互操作问题，不能完全适应弱封闭环境下 Web 服务的可信组合问题。现有的研究从某些方面提出了组合 Web 服务安全架构的思路，但均未系统全面地给出解决方案，不能满足分布式环境下组合 Web 服务的安全耦合需求。

1.2 HSM-WSC 的提出

Web 服务体系结构基于服务提供者、服务注册中心和服务请求者 3 种角色之间的交互，涉及发布、发现和绑定操作，这些角色和操作一起作用于 Web 服务构件、Web 服务软件模块及其描述[7]。服务提供者定义 Web 服务的服务描述并把它发布到服务注册中心。服务请求者使用发现操作来从服务注册中心检索服务描述，然后使用服务描述与服务提供者进行绑定并调用 Web 服务实现或同它交互。为加强 Web 服务的安全性，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，保证了 SOAP 消息的安全性，通过定义 WS-Policy，WS-Trust 等规范，保证了上层应用系统的安全性[8]。目前，Web 服务安全相关产品研究的企业大都只注重于安全和管理的某一方面。建立一种基于全局观点的、可扩展的并且能够与今后 Web 服务新技术兼容的 Web 服务组合安全模型是十分必要的。

2 组合 Web 服务的分层安全模型(HSM-WSC)

2.1 HSM-WSC 模型的要求

(1)自治 Web 服务访问控制机制独立性

每个自治 Web 服务的提供者都是独立的实体，他们必须对自己的资源具有完全的控制力。分布式计算环境需要在这些独立的安全域中进行互操作，全局访问控制规则的实施不能以失去局部独立控制权为代价。

(2)高度可定制

跨域的服务请求者和提供者之间并不“认识”。当由多个 Web 服务根据提供的不同功能一起完成用户的需求时，就涉及到 Web 服务安全边界的跨越。通用层次的访问控制表征组合服务安全管理的整体特点，部分访问控制表征行业或特定领域的安全特性。这种定制化特点必须反映于组合服务安全架构之中。

(3)跨应用的集成

分布式计算环境中组合 Web 服务需要集成多种异构的服务种类，例如 RMI，CORBA，.NET 等，每个安全自治域对外提供的服务方式都不相同。那么，如何在这些安全管理域之间实现跨域以及跨应用的安全表述和集成？

(4)安全访问控制粒度的可伸缩性

通信安全组合 Web 服务涉及到业务流程多任务协同、多 Web 服务协同和单个自治 Web 服务等级别，不同层面对资源的保护粒度会存在差异[9]。良好的访问控制管理机制，必须对各种不同粒度的资源和操作都能够加以刻画，为多 Web 服务跨域的安全交互与协商提供良好的基础。

(5)兼容性

组合 Web 服务不仅要与用户交互，也要与业务流程中涉及的各个异构系统进行交互。由于有各种各样的异构系统，模型应将这些异构系统统一对待，能够解决这些信息系统所面对的企业或机构的整体应用。这就需要组合 Web 服务安全模型能够提供开放式体系结构，实现可扩展的安全访问机制。

2.2 HSM-WSC 模型层级与功能

HSM-WSC 模型以 Web 服务协议栈为基础，采用层次结构建模方法，通过对服务组合的自治成员异构的访问控制机制进行统一描述，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 服务的可靠传输和访问控制等安全要求，在进行组合 Web 服务的安全方案规划中兼顾目前和未来的发展需求。

HSM-WSC 模型有可信执行层、可信协同层、访问控制管理层和通信安全层 4 个子层，每一层所对应的 Web 服务协议栈以及功能描述如图 1 所示。

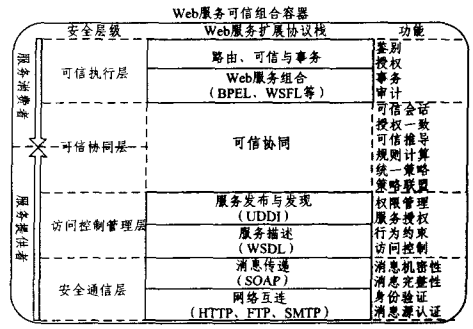

图 1 HSM-WSC 模型图

(1)可信执行层

可信执行层主要帮助企业管理安全的组合 Web 服务应用，包括 Web 服务组合和路由、可信执行与事务管理等。可信执行层主要功能如下。

鉴别：基于口令、挑战/应答、Kerberos、X.509 证书、智能卡和生物特征等认证技术验证客户的真实身份与其所声称的身份是否相符，以防止非法人员对系统进行主动攻击；

授权：确保服务组合业务流程任务能被合法主体按规定权限执行，对业务流程任务的执行进行授权约束；

事务：基于事务处理机制确保松耦合环境下运行结果的可靠性和后台数据的一致性，并能及时解决运行时发生的各种异常；

审计：对系统的执行情况和历史记录进行审计，找到出现问题和所受攻击的来源，并帮助系统安全管理员采取合适的措施，防止职权滥用和越权行为。

(2)可信协同层

可信协同层通过对组合服务中跨域的异构访问控制机制进行统一描述，从组合 Web 服务业务流程任务权限的动态授权管理和成员服务的可信一致两个维度，研究 Web 服务组合服务多层次的安全访问架构。可信协同层主要功能如下。

可信会话:组合服务业务流程任务授权一致与组合服务自治成员在策略一致的情况下用户与组合服务系统的一次对话过程,用户通过会话来获得组合 Web 服务增值功能;

授权一致:表达组合 Web 服务业务流程任务之间基于分工性、依赖性和交互性的授权协同及其序关系约束;

可信推导:通过 Web 服务访问控制策略规则建模,提取影响组合 Web 服务访问控制策略非一致的规则因子,基于策略规则一致与执行中上下文环境因素影响的一致间的动态协作,进行多策略冲突的检测与消解计算;

规则计算:通过描述逻辑表示授权规则和访问控制策略,进行权限的推导、冲突解决、访问控制和完整性约束检查;

统一策略:统一的访问控制描述与实现机制相分离,消除多自治域访问控制策略规则在概念语义层次上的异构,保证访问控制策略在不同的终端被一个或多个机制所执行;

策略联盟:策略联盟是基于身份信息的访问控制策略共享联盟实体,成员服务在一个联盟里为了共同目标而组成动态联盟,计算和管理他们的安全访问控制信息。

(3)访问控制管理层

访问控制管理层通过提供细粒度的访问控制并增加互操作性方法,来控制用户对组合 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。访问控制管理层主要功能如下。

权限管理:定义指定权限的访问对象与访问的操作类型,管理自治服务提供者对于服务访问者访问权限的分配和回收。对于进入权限模块进行权限分配和回收的用户,必须首先检验其权限的合法性;

服务授权:通过分配和取消操作来完成用户权限的授予及取消,在访问控制处理时对消息进行授权过滤。当截获到 SOAP 请求消息时,它将依据特定的规则对这则消息进行评估测试处理。然后根据评估测试的结果来允许或拒绝请求消息,或对用户的请求进行相关更改后允许其请求;

行为约束:支持部分服务组合上下文描述,一旦前提条件满足,则组合服务业务流程访问自治服务的任务 Action 立即激发,避免激发时机的不确定性;

访问控制:根据用户或上下文信息的动态变化,适时更新访问控制决策,确保服务请求者在服务和属性上都得到许可。

(4)通信安全层

组合 Web 服务的分层安全模型实现系统安全耦合应用的实现基础,用来确保通信中的数据安全,抵抗窃听、篡改、假冒、重放、业务否认等安全攻击,确保数据的机密性、完整性、可用性、消息源认证性和不可否认性,为高层多个 Web 服务访问控制策略协同与实施提供机制保障。通信安全层主要功能如下。

消息机密性保障:利用 XML 加密和安全性令牌来保持部分 SOAP 消息是机密的,保证任何第三方不能读取消息的有效载荷;

消息机完整性保障:保证保护数据以防止未授权的改变、删除或替代,服务提供者需要确认收到的请求是真正由客户发来的,XML 消息的完整性可通过 XML 签名来获得;

身份验证:通过在 SOAP 标头传递安全性令牌(Security Token)来验证用户身份。对信息或数据的发送者/接收者进行鉴别,保证信息交换过程的有效性和合法性;

消息源认证:使用时间戳(Timestamps)和共享密钥来加密报文摘要,保证消息是来自于已知的源并且不是重复消息,实现更加安全可靠的 SOAP 消息。

2.3 HSM-WSC 模型的特点

(1) HSM-WSC 模型能够集成多种分布式异构安全机制,降低实现组合 Web 服务的风险性,加强 Web 服务之间的交互能力;

(2)层次化结构使 HSM-WSC 模型具有模块化、开放性和有效性的特点,为不同层次的安全信息共享和交互奠定体系结构基础;

(3) HSM-WSC 模型可以根据不同的应用需求选择不同的安全功能模块,降低系统的复杂性,提高系统灵活性;

(4) HSM-WSC 模型具有良好的可伸缩性。新的安全技术和规范可以很方便地融入该模型,便于在进行组合 Web 服务的安全方案规划中兼顾目前和未来发展。

3 HSM-WSC 模型的实施

HSM-WSC 模型已在实验环境中得以实施,图 2 给出了该模型在 Web 服务可信组合实施中的原型系统。系统通过访问控制描述与实现机制相分离来进行策略的一致性判决,以授权任务的一致协同为中心实现业务流程访问控制,增加了任务信息库。下面对该系统进行全面描述。

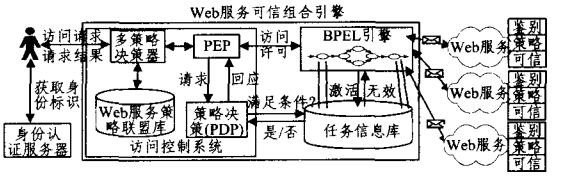

图 2 HSM-WSC 模型在组合 Web 服务安全访问中的原型系统

3.1 访问控制系统组成

HSM-WSC 模型实施的原型系统由以下几部分构成:身份鉴别服务器 IAS(Identity Authentication Server)、多策略决策器 MDM(Multipolicy Decision Maker)、Web 服务策略联盟库 WSPAB(Web Service Policy Alliance Base)、业务流程访问控制执行点 PEP(Policy Enforcement Point)、业务流程访问控制决策点 PDP(Policy Decision Point)、BPEL 引擎(BPEL Engine)、任务信息库 TI(Task InformationBase)等。

3.2 系统运行流程

(1) 客户端要求进入系统之前,首先向身份鉴别服务器 IAS 证实自己的身份,获取身份认证信息(在这里只提出身份认证,忽略实现问题)。客户端得到身份认证之后,向 Web 服务可信组合引擎发出组合服务访问请求。为了确保请求信息在传输过程中的安全,一般需要对消息进行加密和签名处理。

(2)Web 服务可信组合引擎收取请求信息并进行可信性验证,然后将请求消息传给多策略决策器 MDM。MDM 从 Web 服务策略联盟库 WSPAB 中取得相关请求的策略信息,并进行一致性计算。如果组合 Web 服务的自治成员之间访问控制决策有冲突,则在组合服务运行之前就拒绝;如果没有策略决策冲突,则将请求传给业务流程访问控制执行点 PEP。

(3) 业务流程访问控制执行点 PEP 接收请求并将请求传给流程任务访问控制决策点 PDP。PDP 首先查询任务信息库 TI,根据 TI 中保存的任务信息,如任务当前的状态、执行该任务的角色以及该任务的约束等,分析判断用户能否执行该任务。如能执行,参照系统授予 PEP 执行该任务所需的

(下转第 153 页)

先调度对整体加工时间影响较大的关键路径上的工序和长用时工序，使产品的调度效率得到提高。理论分析和实例表明，所提出的算法对解决复杂产品综合调度问题能获得令人满意的效果且算法复杂度不超过二次多项式，因此该算法简便可行，容易实现。该算法改进后可推广应用于存在相同设备的复杂产品综合调度问题。

参 考 文 献

[1] Croce F D, Ghirardi M, Tadei R. An improved branch-and-bound algorithm for the two machine total completion time flow shop problem[J]. European Journal of Operational Research, 2002, 139:293-301

[2] El-Bouri A, Shah P. A neural network for dispatching rule selection in a job shop[J]. The International Journal of Advanced Manufacturing Technology, 2006, 31:342-349

[3] Gao Jie, Gen Mitsuo, Sun Linyan. Scheduling jobs and maintenances in flexible job shop with a hybrid genetic algorithm[J]. The International Journal of Advanced Manufacturing Technology, 2006, 17:493-507

[4] Amirthagadeswaran K S, Arunachalam V P. Improved solutions for job shop scheduling problems through genetic algorithm with a different method of schedule deduction[J]. The International Journal of Advanced Manufacturing Technology, 2006, 28:532-540

[5] Mattfeld D C, Bierwirth C, Kopfer H. A search space analysis of the Job Shop Scheduling problem[J]. Annals of Operations Research, 1999, 86:441-453

[6] Huang Wenqi, Kang Yan. A Short Note on a Simple Search Heuristic for the Diskspacking problem[J]. Annals of Operations Research, 2004, 131:101-108

[7] 谢志强，刘胜辉，乔佩利. 基于 ACPM 和 BFSM 的动态 Job-Shop 调度算法[J]. 计算机研究与发展，2003，40(7)：977-983

[8] 谢志强，周勇，杨光. 动态生成优先工序集的多产品制造过程优化控制[J]. 电机与控制学报，2008，12(6)：734-738

[9] Wu Chih-Sen, Li Der-Chiang, Tsai Tung-I. Applying the Fuzzy Ranking Method to the Shifting Bottleneck Procedure to Solve Scheduling Problems of Uncertainty[J]. The International Journal of Advanced Manufacturing Technology, 2006, 31:98-106

[10] Xie Zhi-qiang, Ye Guang-jie, Zhang Da-li, et al. New Nonstandard Job Shop Scheduling Algorithm[J]. Chinese Journal of Mechanical Engineering, 2008, 21(4):97-100

[11] 谢志强，刘秋杉，丛景，等. 基于缩短装配设备空闲时间的车间装配方法[J]. 黑龙江大学：自然科学学报，2007，24(3)：291-300

[12] Xie Zhi-qiang, Ye Guang-jie, Liu Yong, et al. Study on Job Shop Scheduling with Many Function-Same Machines[C]// Proceedings of the 2007 IEEE international Conference on Mechatronics and Automation. ICMA2007. Harbin, 2007:1278-1282

(上接第 115 页)

最小权限，同时收回用户拥有的其他权力；如不能，拒绝用户的任务请求。然后，访问控制执行点 PEP 将执行结果回送给多策略决策器 MDM，作为下次用户访问的参考。MDM 再将决策结果返回给用户。

(4) Web 服务组合业务流程中每个任务由系统按一定的逻辑顺序自动执行[10]。当轮到某个任务执行时，由系统自动标识，然后等待访问主体激活。如果任务被激活，任务此时的状态信息就写入任务信息库。此后任务的状态信息及其它相关信息都由系统自动记入任务信息库。一旦任务处于终止态或夭折态，系统在任务信息库中标志该任务已终止，启动后续任务准备执行。

(5)如果组合服务业务流程任务被激活，启动任务与自治 Web 服务成员之间的会话，自治服务成员收取组合服务引擎发送的用户身份信息与服务功能请求信息，并进行可信验证。然后到策略库中查找主体策略文件，从中析取访问权限信息并依此作出判决。如果是许可(permit)，则将当前自治 Web 服务功能执行结果返回给组合服务引擎，同时根据需要调用属性更新模块对用户或者服务属性进行更新；如果是拒绝(deny)，则将 deny 决策返回给组合服务引擎。

结束语 组合 Web 服务构建于分布式协同环境中，需要有效的安全机制保障，现有的组合 Web 服务安全机制并不能满足需求。本文提出了一种 4 层 Web 服务组合安全模型(HSM-WSC)。HSM-WSC 模型能够集成多种分布式异构安全机制，通过层次化的结构为组合 Web 服务从底层消息安全到多服务柔性安全的耦合奠定了基础。文中还给出了模型实施的原型系统。HSM-WSC 模型具有模块化、可伸缩性和灵活性等特性。多种异构访问控制机制的可信协同是组合 Web 服务访问控制安全的关键。下一步的工作将是设计出高效的多策略协同计算模型，准确、全面地刻画组合服务的动态安全行为，以更好地满足 Web 服务跨边界可信组合的实际需求。

参 考 文 献

[1] Joachim B, Barbara C, et al. Towards Secure Execution Orders for Composite Web Services[C]// Proc. of 2007 IEEE International Conference on Web Services. 2007:489-496

[2] Carminati B, Ferrari E, et al. Security Conscious Web Service Composition with Semantic Web Support[C]// Proc. of the First International Workshop on Security Technologies for Next Generation Collaborative Business Applications. 2007:695-704

[3] 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

[4] Huang D. Semantic policy-based security framework for business processes[C]// Proc. of the Semantic Web and Policy Workshop. 2005:27-31

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

[6] Charfi A, Mezini M. 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

[7] 孔维梁，等. 基于二维 QoS 模型的 Web 服务组合[J]. 计算机科学，2008，35(11)：131-13

[8] Anoop S, Theodore W, Karen S. NIST Special Publication 800-95[EB/OL]. Guide to secure web services. Recommendations of the National Institute of Standards and Technology. August 2007. http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf

[9] Chun S A, Atluri V, Adam N R. Using Semantics for Policy-based Web Services Composition[J]. Journal of Distributed and Parallel Databases, 2005, 18(1):37-64

[10] 陈风珍，洪帆. 基于任务的访问控制(TBAC)模型[J]. 小型微型计算机系统，2003，24(3)：621-624