

组合 Web 服务访问控制策略合成

姜皇勤^{1,2*}, 张红旗^{1,2}, 任志宇^{1,2}, 单棣斌^{1,2}

(1. 信息工程大学, 郑州 450004; 2. 河南省信息安全重点实验室, 郑州 450004)

(* 通信作者电子邮箱 jhuangqin@163.com)

摘要:针对 Web 服务多域环境下组合服务的访问控制策略合成问题, 首先提出基于属性的 Web 服务访问控制策略描述框架, 并结合原子属性值限制的属性描述方法, 对服务访问控制策略进行了形式化表达。然后, 通过分析服务组合描述文档中的控制结构, 并研究访问控制策略合成算子和访问控制策略规则的合成运算, 提出组合 Web 服务访问控制策略合成方法, 实现了组合服务访问控制策略的合成。最后, 结合实例给出组合 Web 服务的访问控制策略合成流程, 验证了合成方法的实用性。

关键词: Web 服务; 服务组合; 访问控制; 策略合成

中图分类号: TP393.08 **文献标志码:** A

Access control policies composition for composite Web services

JIANG Huang-qin^{1,2*}, ZHANG Hong-qi^{1,2}, REN Zhi-yu^{1,2}, SHAN Di-bin^{1,2}

(1. Information Engineering University, Zhengzhou Henan 450004, China;

2. Henan Province Key Laboratory of Information Security, Zhengzhou Henan 450004, China)

Abstract: For access control policy composition problem of composite services in Web services multi-domain environment, the attribute based Web services access control policy description framework was proposed and the services access control policies were formally expressed with atomic attribute value constraint. After analyzing the control structures in services composition description document, combining the access control policy composition operators with access control policy rule composition operation, the composite Web services access control policies composition method was designed to compose the composite service access control policies. Finally, the Web services access control policy composition process was given and the practicability of composition method was verified through a case.

Key words: Web services; services composition; access control; policy composition

0 引言

Web 服务的可组合性蕴藏着巨大的价值, 它可将分布式环境下的 Web 服务按需组合成具有更强功能的组合服务, 实现复杂信息系统的综合集成。目前, Web 服务组合技术^[1-2]大多仅满足服务组合的功能性需求, 但对安全性考虑不足, 为保证组合服务的安全, 需结合各组件服务的访问控制需求对其进行访问控制。实现组合服务访问控制的关键是对参与组合的各组件服务的访问控制策略进行合成, 生成一致的组合服务访问控制策略。通过分析组合服务的访问控制策略, 服务请求者只需一次提交所需的属性就能完成多个服务的访问授权, 可防止在组合服务执行过程中多次提交属性所造成的额外开销; 并且服务提供者可以在不触发组件服务的情况下验证服务请求者的合法性, 防止在组合服务运行阶段因不满足某一组件服务的访问控制策略, 而导致的服务调用失败所造成的资源浪费。组合 Web 服务访问控制策略的合成问题, 已成为服务组合技术发展过程中迫切需要解决的关键问题, 研究组合 Web 服务的访问控制策略合成在保证组合服务的安全性和减小额外开销等方面具有重要意义。

本文针对组合 Web 服务访问控制策略合成中的策略形

式化描述、策略合成方法、策略合成流程等问题进行了深入研究, 提出基于属性的 Web 服务访问控制策略描述框架, 实现了 Web 服务访问控制策略的统一形式化描述。基于此框架, 结合服务组合描述文档中的控制结构, 给出了适合组合 Web 服务访问控制策略合成的算子, 并研究了访问控制策略规则的合成运算, 提出了组合 Web 服务访问控制策略合成方法, 实现了对组合服务中各组件 Web 服务访问控制策略的合成。

1 相关研究

目前, 国内外学者对单个 Web 服务的访问控制问题开展了大量研究, 但针对组合 Web 服务访问控制的研究相对较少, 尚未很好地解决组合 Web 服务访问控制策略的合成问题。组合 Web 服务访问控制策略的合成问题已逐步成为组合服务访问控制领域研究的热点^[3-4]。

文献[5]较早地将基于属性的访问控制 (Attribute Based Access Control, ABAC) 模型引入到 Web 服务的访问控制中, 实现了对单个 Web 服务的访问控制, 但未考虑组合 Web 服务访问控制策略的合成问题。文献[6]提出组合 Web 服务的分层安全模型, 分析了组合 Web 服务的安全需求, 但未给出组合 Web 服务访问控制策略的描述和合成方法。文献[7]给出

收稿日期: 2012-06-25; 修回日期: 2012-08-06。

基金项目: 国家 973 计划项目 (2011CB311801); 河南省科技创新人才计划项目 (114200510001)。

作者简介: 姜皇勤 (1987-), 男, 四川眉山人, 硕士研究生, 主要研究方向: 访问控制、身份认证; 张红旗 (1962-), 男, 河北遵化人, 教授, 博士生导师, 博士, 主要研究方向: 授权管理、等级保护、网络安全; 任志宇 (1974-), 女, 河南汤阴人, 讲师, 博士研究生, 主要研究方向: 授权管理; 单棣斌 (1982-), 男, 河北邯郸人, 讲师, 硕士, 主要研究方向: 身份认证。

了用于服务组合的访问控制系统,在一定程度上满足了动态 Web 服务环境下的安全需求,但未详细描述生成组合服务访问控制策略的具体方案。文献[8]在基于 Web 服务业务流程执行语言(Web Services Business Process Execution Language, WS-BPEL)的服务组合中引入基于角色的访问控制(Role Based Access Control, RBAC)模型进行访问控制,给出一种称为 RBAC-WS-BPEL 的访问控制架构,但其研究是基于 RBAC 模型的,在访问控制的动态性和控制粒度方面存在局限性。文献[9]使用谓词逻辑研究了组合服务的安全策略合成方法,提出面向服务合成的安全策略自动创建机制,但未给出访问控制策略合成的具体算子,且未考虑服务组合语言的控制结构。文献[10]指出组合 Web 服务的访问控制策略一般由其所有组件服务的访问控制策略合成产生,但其仅描述了组合服务访问控制策略的合成过程,没有给出详细的策略合成方法。文献[11]提出了经典的策略合成代数,其基本思想是将访问控制策略定义成主体、客体、操作三元组的集合,用并、交、差等算子抽象地描述策略合成,但其不能刻画涉及属性值计算的策略合成场景。文献[12]提出了基于属性的策略合成代数,能支持传统的策略合成,增强了策略合成代数的表达能力,但其在访问控制策略表达中没有考虑环境因素,并且未与组合 Web 服务的实际应用相结合。

综上所述,目前针对组合 Web 服务访问控制策略合成的研究大多仅关注某些方面的需求,对服务访问控制策略的形式化描述、服务组合的控制结构、策略合成方式等因素考虑不足,没有形成系统全面的服务访问控制策略合成方法。因此,深入全面地研究组合 Web 服务访问控制策略的合成问题具有重要的理论和实际意义。

2 基于属性的 Web 服务访问策略描述框架

Web 服务组合通常涉及多域之间服务的整合与调用,组合 Web 服务系统的复杂、跨域、动态等特征给访问控制带来了新的挑战。ABAC 模型根据实体的属性动态地进行授权,域内外的服务请求者以提交属性的统一方式实现授权,能很好地满足组合 Web 服务访问控制的多域、动态、细粒度等需求。因此,本文引入基于 ABAC 的 Web 访问控制策略描述框架,实现了服务访问控制策略的统一形式化描述。

定义 1 原子属性。原子属性是属性值限制关系的表达式,是实体属性描述的最小单元。本文引入限制域^[13]的概念描述原子属性值的限制关系。原子属性值限制的结构为 $x\theta c$, 其中 x 为变量,表示属性类型; θ 为限制符号,表示属性类型所具有的属性值; c 为常量,表示属性值。原子属性值的基本限制符号集合为 $\{=, \neq, >, \geq, <, \leq, \in, \subset, \subseteq, \supset, \supseteq\}$, 限制符号集合可以根据实际需要进行扩展。

定义 2 实体属性。实体属性是相应实体的原子属性构成的元组。令 $ATTR(s)$ 、 $ATTR(r)$ 、 $ATTR(e)$ 和 $OP_TYPE(r)$ 为实体属性,则 $ATTR(s) = \langle SA_1, SA_2, \dots, SA_k \rangle$, $ATTR(r) = \langle RA_1, RA_2, \dots, RA_m \rangle$, $ATTR(e) = \langle EA_1, EA_2, \dots, EA_n \rangle$, $ATTR(op) = \langle OPA_1, OPA_2, \dots, OPA_l \rangle$, 其中 s, r, e 和 op 分别表示主体、资源、环境和资源操作等实体, $SA_k (1 \leq k \leq K)$, $RA_m (1 \leq m \leq M)$, $EA_n (1 \leq n \leq N)$ 和 $OPA_l (1 \leq l \leq L)$ 分别表示相应实体的原子属性。

定义 3 访问控制策略规则。访问控制策略规则是由 s, r, e 和 op 等实体的属性构成的元组,其形式为 $\langle ATTR(s), ATTR(r), ATTR(e), ATTR(op) \rangle$, 访问控制策略规则中各实

体属性的原子属性之间的关系为合取关系,其功能是规定具有属性 $ATTR(s)$ 的主体 s , 在属性为 $ATTR(e)$ 的环境 e 下是否能够对属性为 $ATTR(r)$ 的资源 r 进行属性类型为 $ATTR(op)$ 的操作。

定义 4 访问控制策略。访问控制策略 POL 是从 $ATTR(s)$ 、 $ATTR(r)$ 、 $ATTR(e)$ 和 $ATTR(op)$ 到集合 $\{true, false\}$ 的映射。访问控制策略的最小单元是访问控制策略规则,访问控制策略是由若干访问控制策略规则构成的集合。本文的访问控制策略只规定正向授权的情况,即在某一访问请求下,若映射的值为真,则允许此访问请求,否则拒绝此访问请求。访问控制策略 POL 的形式化定义如下:

$$POL: 2^{ATTR(s)} \times 2^{ATTR(r)} \times 2^{ATTR(e)} \times 2^{ATTR(op)} \rightarrow \{true, false\}$$

3 组合 Web 服务访问控制策略合成方法

为建立组合 Web 服务的访问控制策略合成方法,首先分析服务组合的基本控制结构,给出相应的访问控制策略合成算子,对不同类型的策略合成进行形式化描述;然后定义访问控制策略规则的合成的运算,并详细介绍其运算方法和步骤;最后结合服务组合的基本控制结构和相应的策略合成算子,实现组合 Web 服务访问控制策略的合成。

3.1 服务组合控制结构

服务组合的基本控制结构^[14]包括顺序(Sequence)、并行(Flow)、选择(Switch)、触发(Pick)、迭代(While)等,如图 1 所示。 S_1 和 S_2 表示组件服务,控制结构的入口代表由组件服务 S_1 和 S_2 形成的逻辑上的组合服务 S_c , 实际的组合服务可能由多个组件服务或组合服务结合服务组合控制结构进一步组合而成。服务组合控制结构的主要作用是控制组合服务中各组件服务的执行顺序,使各组件服务协调一致地完成组合服务的功能。

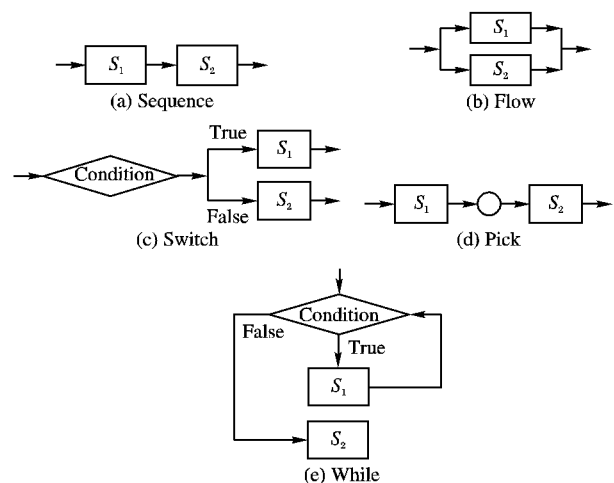


图 1 服务组合的基本控制结构

顺序控制结构表示组合服务中一个或多个组件服务必须串行执行。并行控制结构表示组合服务中各组件服务并行执行,各组件服务之间不存在依赖性。选择控制结构中,当一个或多个条件分支满足时执行该分支对应的组件服务,当所有条件分支均不满足时执行默认的组件服务。触发控制结构的功能是根据分支关联的事件的出现情况,选择一组或一个服务执行。迭代控制结构的功能是当循环执行条件满足时循环执行内部包含的组件服务;当循环执行条件不满足时,执行指定的组件服务。

3.2 访问控制策略合成算子

结合服务组合过程中的控制结构,本文引入 $(+, \&, \Pi_c, \theta_w, \sigma_c)$ 等访问控制策略合成算子实现组合服务中各组件服务访问控制策略的合成。生成组合 Web 服务的访问控制策略时,需对各组件服务的访问控制策略进行合成,所涉及的符号和含义如表 1 所示。访问控制策略的合成本质上是对访问控制策略规则中各实体属性元组中原子属性的合成。

表 1 相关符号及含义

符号	含义
Ps_1	组件服务 S_1 的访问控制策略
Ps_2	组件服务 S_2 的访问控制策略
Pc	组合服务 S_c 的访问控制策略
Rs	服务访问请求
R_Y^P	被服务访问控制策略 P 允许的服务访问请求
R_N^P	被服务访问控制策略 P 拒绝的服务访问请求
a_{s_1}	组件服务访问控制策略 Ps_1 中的访问控制策略规则
a_{s_2}	组件服务访问控制策略 Ps_2 中的访问控制策略规则
a_c	组合服务访问控制策略 Pc 的访问控制策略规则

1) $+$ 算子。

$$Pc = Ps_1 + Ps_2 = \{a_c \mid a_c \in a_{s_1} \cup a_{s_2}, a_{s_1} \in Ps_1, a_{s_2} \in Ps_2\}$$

其含义是若 Rs 被策略 Ps_1 允许或被 Ps_2 允许,则被合成的访问控制策略 Pc 允许;否则被合成的访问控制策略 Pc 拒绝,可形式化地表达为:

$$Pc = Ps_1 + Ps_2 \Leftrightarrow \begin{cases} R_Y^{Pc} = R_Y^{Ps_1} \cup R_Y^{Ps_2} \\ R_N^{Pc} = Rs - R_Y^{Pc} \end{cases}$$

2) $\&$ 算子。

$$Pc = Ps_1 \& Ps_2 = \{a_c \mid a_c \in a_{s_1} \cap a_{s_2}, a_{s_1} \in Ps_1, a_{s_2} \in Ps_2\}$$

其含义是若 Rs 同时被 Ps_1 和 Ps_2 允许,则被合成的访问控制策略 Pc 允许;否则被合成的访问控制策略 Pc 拒绝,可形式化地表达为:

$$Pc = Ps_1 \& Ps_2 \Leftrightarrow \begin{cases} R_Y^{Pc} = R_Y^{Ps_1} \cap R_Y^{Ps_2} \\ R_N^{Pc} = Rs - R_Y^{Pc} \end{cases}$$

3) Π_c 算子。

$$Pc = \Pi_c(Ps_1) = \{a_c \mid a_c = a_{s_1}, a_{s_1} \in Ps_1, Rs \text{ satisfies } c\}$$

其本质是在原有策略基础上增加额外的限制,其含义是若 Rs 被 Ps_1 允许且满足外部条件 c ,则此 Rs 将被合成的访问控制策略 Pc 允许;否则此 Rs 也将被合成的访问控制策略 Pc 拒绝,可形式化地表达为:

$$Pc = \Pi_c(Ps_1) \Leftrightarrow \begin{cases} R_Y^{Pc} = R_Y^{Ps_1}, Rs \text{ satisfies } c \\ R_N^{Pc} = Rs - R_Y^{Pc} \end{cases}$$

4) θ_w 算子。

$$Pc = Ps_1 \theta_w Ps_2$$

其含义是合成的访问控制策略 Pc 中包含的访问控制策略规则是 Ps_1 和 Ps_2 中的访问控制策略规则在 θ_w 下的计算结果。引入该算子的目的是根据实际的访问控制策略合成需求,对定义 1 中的限制符号集合 θ 确定的运算规则进行 w 扩充,增强访问控制策略合成算子的表达能力和扩展性,可形式化地表达为:

$$Pc = Ps_1 \theta_w Ps_2 = \{a_c \mid a_c = a_{s_1} w a_{s_2}, a_{s_1} \in Ps_1, a_{s_2} \in Ps_2\}$$

5) σ_c 算子。

$$Pc = \sigma_c(Ps_1, Ps_2)$$

其含义是若满足外部条件 c ,则合成的访问控制策略 Pc 按 Ps_1 评估 Rs ;若不满足外部条件 c ,则合成的访问控制策略 Pc 按 Ps_2 评估 Rs ,可形式化地表达为:

$$Pc = \sigma_c(Ps_1, Ps_2) \Leftrightarrow \begin{cases} Pc = Ps_1, Rs \text{ satisfies } c \\ Pc = Ps_2, Rs \text{ not satisfies } c \end{cases}$$

3.3 访问控制策略规则合成

访问控制策略的合成不是简单的策略叠加,而需结合定义在原子属性上的二维算子对访问控制策略中的策略规则进行约简、冲突处理等才能生成组合 Web 服务访问控制策略。访问控制策略规则合成步骤包括访问控制策略规则预处理、原子属性合成运算和访问控制策略规则最终处理。

1) 访问控制策略规则预处理。

令 a_1, a_2 为任意两个访问控制策略规则,为支持异构策略的合并,引入符号 Δ 对 a_1, a_2 进行扩展预处理^{[12]405}, Δ 表示实体属性中此原子属性为空,表明访问控制策略中未考虑该原子属性。使用 Δ 符号对访问控制策略规则进行扩展的方法是:首先固定 $a_1(a_2)$ 中对应实体属性的某个原子属性,在 $a_2(a_1)$ 的对应实体属性中查找与固定原子属性类型相同的原子属性,若找到相同类型的原子属性,则提取 $a_2(a_1)$ 中此相同的原子属性生成原子属性对;若在 $a_2(a_1)$ 中未找到与固定属性类型相同的原子属性,则用 Δ 填充 $a_2(a_1)$ 中缺省的原子属性并生成原子属性对;循环采用同样的方法对 $a_1(a_2)$ 中剩余的原子属性进行处理,直到 $a_1(a_2)$ 中所有实体属性的原子属性处理完毕。令 a'_1, a'_2 为用 Δ 符号进行扩展后的访问控制策略规则,则生成的原子属性对 $(SA_i, SA'_i), (RA_j, RA'_j), (EA_p, EA'_p)$ 和 (OPA_q, OPA'_q) 具有相同属性类型或其中某一原子属性为 Δ ,且 $a'_1 = [\langle SA_1, \dots, \Delta, \dots, SA_k \rangle, \langle RA_1, \dots, \Delta, \dots, RA_m \rangle, \langle EA_1, \dots, \Delta, \dots, EA_n \rangle, \langle OPA_1, \dots, \Delta, \dots, OPA_l \rangle]$, $a'_2 = [\langle SA'_1, \dots, \Delta, \dots, SA'_k \rangle, \langle RA'_1, \dots, \Delta, \dots, RA'_m \rangle, \langle EA'_1, \dots, \Delta, \dots, EA'_n \rangle, \langle OPA'_1, \dots, \Delta, \dots, OPA'_l \rangle]$ 。

2) 原子属性合成运算。

访问控制策略规则预处理步骤完成后,需要对访问控制策略规则中实体属性的各原子属性对进行合成运算。原子属性对的合成运算需综合考虑访问控制策略的合成方式、原子属性的限制符号 θ 、属性值 c 、定义在属性值 c 域上的运算等。令 $e_i^\wedge, f_j^\wedge, g_p^\wedge$ 和 h_q^\wedge 为定义在原子属性 $SA_i (i = 1, 2, \dots, k), RA_j (j = 1, 2, \dots, m), EA_p (p = 1, 2, \dots, n)$ 和 $OPA_q (q = 1, 2, \dots, l)$ 的属性值域上的二维算子,其功能是完成原子属性值的合成;记 $w = (\langle e_1^\wedge, e_2^\wedge, \dots, e_k^\wedge \rangle, \langle f_1^\wedge, f_2^\wedge, \dots, f_j^\wedge \rangle, \langle g_1^\wedge, g_2^\wedge, \dots, g_p^\wedge \rangle, \langle h_1^\wedge, h_2^\wedge, \dots, h_q^\wedge \rangle)$, 则访问控制策略规则的合成结果可表示为 $a'_1 w a'_2$, 原子属性合成运算的原理为 $SA''_i = e_i^\wedge(SA_i, SA'_i) (i = 1, 2, \dots, k), RA''_j = f_j^\wedge(RA_j, RA'_j) (j = 1, 2, \dots, m), EA''_p = g_p^\wedge(EA_p, EA'_p) (p = 1, 2, \dots, n), OPA''_q = h_q^\wedge(OPA_q, OPA'_q) (q = 1, 2, \dots, l)$ 。若参与组合的组件服务的访问控制策略合成方式为 $Pc = Ps_1 + Ps_2$, 则 $e_i^\wedge, f_j^\wedge, g_p^\wedge$ 和 h_q^\wedge 等算子的功能需满足集合运算的“并”语义;若策略合成方式为 $Pc = Ps_1 \& Ps_2$, 则 $e_i^\wedge, f_j^\wedge, g_p^\wedge$ 和 h_q^\wedge 等算子的功能需满足集合运算的“交”语义;若策略合成方式为 $Pc = \Pi_c(Ps_1)$ 或 $Pc = \sigma_c(Ps_1, Ps_2)$, 则 $e_i^\wedge, f_j^\wedge, g_p^\wedge$ 和 h_q^\wedge 等算子的功能是在外部条件 c 确定后,由相应的策略合成方式确定;若策略合成方式为 $Pc = Ps_1 \theta_w Ps_2$, 则 $e_i^\wedge, f_j^\wedge, g_p^\wedge$ 和 h_q^\wedge 等算子的功能由扩展的访问控制策略合成方式中的算子 θ_w 确定。为方便理解,以

$f_3^A(RA_3, RA'_3)$ 为例描述单个原子属性对的合成过程, 根据原子属性对中是否含有符号 Δ 分两种情况进行讨论: 1) 当 $RA' = \Delta$ 时, 若令 f_3^A 的功能是取并集, 则无论原子属性限制符号是何种类型, 原子属性合成结果为 $RA''_3 = f_3^A(RA_3, \Delta) = RA_3$ 。2) 当 $RA_3, RA' \neq \Delta$ 时, 若令 f_3^A 在原子属性限制符号 $\theta \in \{=, \neq\}$ 时的功能为求数值类型的属性值的平均值, 则合成结果为 $RA''_3 = f_3^A(RA_3, RA'_3) = \{x_3\theta c''_3 \mid c''_3 = \text{average}[c_3, c'_3]\}$; 若令 f_3^A 在 $\theta \in \{>, \geq, <, \leq, \in, \subset, \supset, \supseteq\}$ 时的功能为求原子属性值的交集, 则合成结果为 $RA''_3 = f_3^A(RA_3, RA'_3) = (x_3\theta c_3) \wedge (x'_3\theta c'_3)$ 。若原子属性合成后的某一原子属性为空, 表示在该算子下的原子属性合成存在冲突, 即参与合成的访问控制策略存在冲突, 则需重新确定策略合成方法, 并选择相应的策略合成算子进行策略合成, 对此我们将另文讨论。

3) 访问控制策略规则最终处理。

原子属性合成运算产生的访问控制策略规则 $a'_1wa'_2$ 若包含 Δ 符号, 型如 $a'_1wa'_2 = [\langle SA''_1, \dots, \Delta, \dots, SA''_i \rangle, \langle RA''_1, \dots, \Delta, \dots, RA''_p \rangle, \langle EA''_1, \dots, \Delta, \dots, EA''_p \rangle, \langle OPA''_1, \dots, \Delta, \dots, OPA''_q \rangle]$, 则为方便无歧义地将合成的访问控制策略规则转化为统一形式化描述的访问控制策略, 需要对 awa' 进行非 Δ 投射得到最终的访问控制策略规则, 非 Δ 投射是 Δ 扩展的逆过程, 其功能是删除访问控制策略规则中的 Δ 符号。

3.4 组合服务访问控制策略合成

组合 Web 服务访问控制策略的合成, 需要结合服务组合描述文档中控制结构的特性和访问控制策略合成算子的功能, 将策略合成算子用于表达服务组合过程中组件服务访问控制策略合成的关系, 并运用 3.3 节的访问控制策略规则合成算法对合成策略进行处理, 得到最终的组合服务访问控制策略。本文将服务组合控制结构与组合服务访问控制策略的合成关系归纳为四类进行分析: 顺序与并行控制结构、选择控制结构、触发控制结构、迭代控制结构。

1) 顺序与并行控制结构。

顺序与并行控制结构中组件服务访问控制策略合成的共同点是: 访问请求 Rs 能否成功访问组合服务 S_c 是由组件服务 S_1 和 S_2 的访问控制策略 Ps_1 和 Ps_2 共同评估决定的, 即组合服务 S_c 的访问控制策略 Pc 应该是各组件服务访问控制策略的“交集”。所以, 这两种控制结构的组件服务访问控制策略合成可以统一用 $\&$ 算子表达为:

$$Pc = Ps_1 \& Ps_2$$

2) 选择控制结构。

选择控制结构中访问请求 Rs 能否成功访问组合服务 S_c 是由组件服务 S_1 和 S_2 所对应的条件约束 c 和其访问控制策略 Ps_1 和 Ps_2 共同决定的。当满足条件约束 c 时, 组合服务 S_c 的访问策略 Pc 由 Ps_1 确定; 当不满足条件约束 c 时, 组合服务 S_c 的访问策略 Pc 由 Ps_2 确定, 此控制结构的组件服务访问控制策略合成可以用 σ_c 算子表达为:

$$Pc = \sigma_c(Ps_1, Ps_2)$$

3) 触发控制结构。

触发控制结构中访问请求 Rs 能否成功访问组合服务 S_c 是由组件服务 S_2 所对应的执行条件约束 c 和组件服务 S_1 、 S_2 的访问控制策略 Ps_1 和 Ps_2 共同评估决定的。当不满足执行条件约束 c 时, S_2 一直处于阻塞状态; 只有满足执行条件约束 c 时, S_2 才能执行。组合服务 S_c 的访问控制策略 Pc 的产生需要

综合考虑执行条件约束 c 和访问控制策略 Ps_1 和 Ps_2 , 此控制结构的组件服务访问控制策略合成可以用 Π_c 和 $\&$ 算子表达为:

$$Pc = (Ps_1 \& \Pi_c(Ps_2))$$

4) 迭代控制结构。

根据迭代控制结构的特点分两种情况讨论: 1) 若访问请求 Rs 在初始时不满足循环执行条件约束 c , 则 Rs 直接跳转到执行指定组件服务 S_2 , 由 S_2 的访问控制策略 Ps_2 评估 Rs 能否成功访问。2) 若 Rs 在初始时满足循环执行条件约束 c , 则执行过程可分为循环内部执行和循环外部执行两个阶段进行讨论。 Rs 跳转到循环内部后, 循环内部组件服务 S_1 的一次或多次执行所对应的访问控制策略相同, 因此循环内部可以简化为对 S_1 的访问控制策略 Ps_1 的一次评估; 当执行到不满足循环执行条件时 Rs 跳转到 S_2 , 则由 Ps_2 评估决定 Rs 能否成功访问。组合服务 S_c 的访问控制策略 Pc 的产生需要综合考虑执行条件约束 c 和访问控制策略 Ps_1 、 Ps_2 , 此控制结构的组件服务访问控制策略合成可以用 σ_c 和 $\&$ 算子表达为:

$$Pc = \sigma_c(Ps_1 \& Ps_2, Ps_2)$$

4 组合 Web 服务访问控制策略合成流程

在 Web 服务环境下, WS-Policy^[15] 提供了描述服务安全策略的标准方法。服务访问控制策略通常也以策略断言的形式在 WS-Policy 文档中定义^[16], 并将其绑定到 Web 服务描述语言 (Web Services Description Language, WSDL) 文档, 以使服务请求者在服务请求时能够获取服务的访问控制策略。下面给出一个简单的实例验证组合 Web 服务访问控制策略合成方法的实用性。假设某学术会议主办方的会议注册服务是由不同管理域的 Web 服务组合而成的, 其服务组合描述文档如图 2 所示。为对自身提供的服务实施保护, 车站、财务、宾馆、旅行社、餐饮公司等不同管理域的服务提供者都要自治地制定符合自身安全需求的服务访问控制策略。 P_{Ticket} 、 $P_{Student}$ 与 $P_{NonStudent}$ 、 P_{Room} 、 $P_{Attractions}$ 、 P_{Dining} 分别表示车票预订、学生与非学生注册费缴纳、房间预订、景点预订、餐饮预订等服务的访问控制策略。它们都是从对应服务的 WS-Policy 文档中提取, 并经统一形式化描述的访问控制策略。 Pc 表示会议注册服务 (组合服务) 的访问控制策略, 它由各组件服务访问控制策略合成产生。

结合会议注册服务的实例, 组合 Web 服务访问控制策略合成流程如下: 首先解析会议注册服务的组合描述文档, 提取其服务组合控制结构和所有相关组件服务的信息; 根据各组件服务信息获得各组件服务的 WSDL 文档, 并从它们所绑定的 WS-Policy 文档中提取各组件服务的访问控制策略, 采用基于属性的 Web 服务访问控制策略描述方法统一形式化地描述为 P_{Ticket} 、 $P_{Student}$ 与 $P_{NonStudent}$ 、 P_{Room} 、 $P_{Attractions}$ 、 P_{Dining} 。然后, 根据会议注册服务的组合控制结构, 结合服务访问控制策略合成算子, 利用组合 Web 服务访问控制策略合成方法, 自底而上逐层将服务组合流程中各组件服务的访问控制策略进行合成。在此例中, 会议注册服务的组合描述文档内学生和非学生注册费缴纳服务的控制结构为选择控制结构, 应选择 σ 算子对 $P_{Student}$ 与 $P_{NonStudent}$ 策略进行合成, 其外部条件 c 为 IsStudent, 即 ID 是否是学生; 景点预订和餐饮预订服务的控制结构为并行控制结构, 应选择 $\&$ 算子对 $P_{Attractions}$ 、 P_{Dining} 策略进行合成; 其他组件服务的控制结构均为顺序控制结构, 应选择 $\&$ 算子对其余策略进行合成。会议注册组合服务的访

访问控制策略可以用策略合成算子表示为: $P_c = P_{Ticket} \& \sigma_{IsStudent}(P_{Student}, P_{NonStudent}) \& P_{Room} \& (P_{Attractions} \& P_{Dining})$ 。接着,利用访问控制策略规则合成方法对各层访问控制策略进行约简,生成约简后的各层组合服务访问控制策略,直到产生整个组合服务的访问控制策略。最后,将形式化描述的会议注册服务的访问策略转化成 WS-Policy 文档中的策略形式,并绑定到会议注册服务的 WSDL 文档中,完成整个组合 Web 服务访问控制策略合成流程。组合 Web 服务的访问控制策略合成流程如图 3 所示,整个策略合成流程可以与 Web 服务的运行框架良好地融合,能很好地满足服务组合过程中访问控制策略的合成需求。

```
<process name="Conference Registration Services">
  <partnerLinks>
    <partnerLink name="Ticket Booking Service"/>
    <partnerLink name="Student Registration Fee Paid Service"/>
    <partnerLink name="NonStudent Registration Fee Paid Service"/>
    <partnerLink name="Room Booking Service"/>
    <partnerLink name="Attractions Booking Service"/>
    <partnerLink name="Dining Reservations Service"/>
  </partnerLinks>
  <variables>
    <variable name="ID" messageType="tns:RequestMessage"/>...
  </variables>
  <sequence>
    <invoke partnerLink="Ticket Booking Service" operation="Booking"/>
    <if>
      <condition>
        getVariableData("ID")="Sstudent"
      </condition>
      <invoke partnerLink="Student Registration Fee Paid Service" operation="Paying"/>
    </if>
    <else>
      <invoke partnerLink="NonStudent Registration Fee Paid Service" operation="Paying"/>
    </else>
    <invoke partnerLink="Room Booking Service" operation="Booking"/>
    <flow>
      <invoke partnerLink="Attractions Booking Service" operation="Booking"/>
      <invoke partnerLink="Dining Reservations Service" operation="Reservations"/>
    </flow>
  </sequence>
</process>
```

图 2 会议注册服务组合描述文档

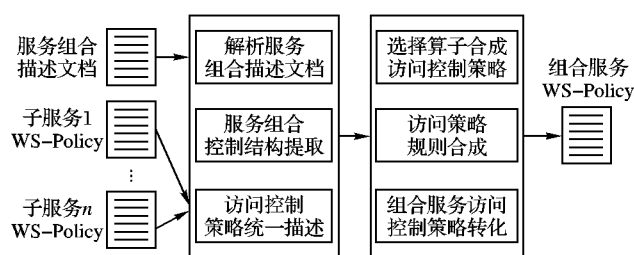


图 3 组合 Web 服务访问控制策略合成流程

5 结语

以 Web 服务为基础构建的分布式信息系统中,Web 服务访问控制策略的合成问题有着实际的研究背景。本文对该问题进行详细分析,并建立基于属性的 Web 访问控制策略描述框架,满足了 Web 服务环境下访问控制策略的描述需求;在分析组合服务控制结构的基础上引入访问控制策略合成算子,并结合访问控制策略规则合成方法,提出组合 Web 服务访问控制策略合成方法,实现了服务组合过程中各组件服务访问控制策略的合成。然而,在 Web 服务多域应用场景下,可能存在多种策略合成方式,并且参与服务组合的各组件服务的访问控制策略之间可能存在冲突,所以仍需进一步研究合成算子的选择和合成策略的冲突消解问题,并对策略合成

方法进行扩展以适应不同的应用需求。

参考文献:

- [1] KUZU M, CICKLI N K. Dynamic planning approach to automated Web service composition[J]. *Applied Intelligence*, 2012, 36(1): 1-28.
- [2] DMELLO D A, ANANTHANARAYANA V S, SALIAN S. A review of dynamic Web service composition techniques[J]. *Communications in Computer and Information Science*, 2011, 133(3): 85-97.
- [3] 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.
- [4] 上超望, 赵呈领, 刘清堂, 等. 组合 Web 服务访问控制技术综述[J]. *计算机科学*, 2011, 38(10): 13-15.
- [5] YUAN E, TONG J. Attribute Based Access Control (ABAC) for Web services [C]// *Proceedings of the 2005 IEEE International Conference on Web Services*. Washington, DC: IEEE Computer Society, 2005: 561-569.
- [6] 上超望, 杨宗凯, 刘清堂, 等. 组合 Web 服务分层安全模型研究[J]. *计算机科学*, 2010, 37(2): 113-115.
- [7] SRIVATSA M, IVENGAR A, MIKALSEN T A, *et al.* An access control system for Web service compositions [C]// *Proceedings of the 2007 IEEE International Conference on Web Services*. Washington, DC: IEEE Computer Society, 2007: 1-8.
- [8] BERTINO E, CRAMPTON J, PACI F. Access control and authorization constraints for WS-BPEL[C]// *Proceedings of the 2006 IEEE International Conference on Web Services*. Washington, DC: IEEE Computer Society, 2006: 275-284.
- [9] SATOH F, TOKUDA T. Security policy composition for composite services [C]// *Proceedings of the 2008 IEEE International Conference on Web Engineering*. Washington, DC: IEEE Computer Society, 2008: 86-97.
- [10] AGARWAL S, SPRICK B. Access control for semantic Web services[C]// *Proceedings of the 2008 IEEE International Conference on Web Services*. Washington, DC: IEEE Computer Society, 2008: 770-773.
- [11] BONATTI P, de CAPITANI DI VIMERCATI S, SAMARATI P. An algebra for composing access control policies[J]. *ACM Transactions on Information and System Security*, 2002, 5(1): 1-35.
- [12] 林莉, 怀进鹏, 李先贤. 基于属性的访问控制策略合成代数[J]. *软件学报*, 2009, 20(2): 404-414.
- [13] LI N, MITCHELL J C. Datalog with constraints: A foundation for trust management languages [C]// *Proceedings of the 5th International Symposium on Practical Aspects of Declarative Languages*. Berlin: Springer-Verlag, 2003: 58-73.
- [14] PAPAZOGLU M P. Web 服务: 原理和技术[M]. 龚玲, 张云海, 译. 北京: 机械工业出版社, 2009: 224-227.
- [15] W3C. WS-Policy (1.5) framework [EB/OL]. [2012-05-20]. <http://www.w3.org/TR/2007/REC-ws-policy-20070904>.
- [16] BERTINO E, SQUICCIARINI A C, PALOSCIA I, *et al.* WS-AC: A fine grained access control system for Web services [J]. *World Wide Web: Internet and Web Information Systems*, 2006, 9(2): 143-171.