University of Wollongong

Research Online

Faculty of Engineering - Papers (Archive)

Faculty of Engineering and Information Sciences

1-1-2011

SOAC engine: A system to manage composite web service authorization

Haiyang Sun
Macquarie University

Weiliang Zhao
University of Wollongong, wzhao@uow.edu.au

Jian Yang
General Research Institute for Non Ferrous Metals,Ministry of Science & Technology, China,Macquarie University

Guizhi Shi
Macquarie University

Follow this and additional works at: https://ro.uow.edu.au/engpapers

Part of the Engineering Commons

https://ro.uow.edu.au/engpapers/5074

Recommended Citation

Sun, Haiyang; Zhao, Weiliang; Yang, Jian; and Shi, Guizhi: SOAC engine: A system to manage composite web service authorization 2011.
https://ro.uow.edu.au/engpapers/5074

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library: research-pubs@uow.edu.au

SOAC Engine: A System to Manage Composite Web Service Authorization

Haiyang Sun, Weiliang Zhao, Jian Yang, and Guizhi Shi

Department of Computing, Macquarie University, Australia
{haiyang.sun,weiliang.zhao,jian.yang,Guizhi.shi}@mq.edu.au

1 Introduction

The authorization of composite web services is different from traditional authorization in a close system due to the dynamic and complex relationships among service consumers and resources (component services). This demonstration is to show the functionality of a system named Service Oriented Authorization Control Engine (*SOAC Engine*).

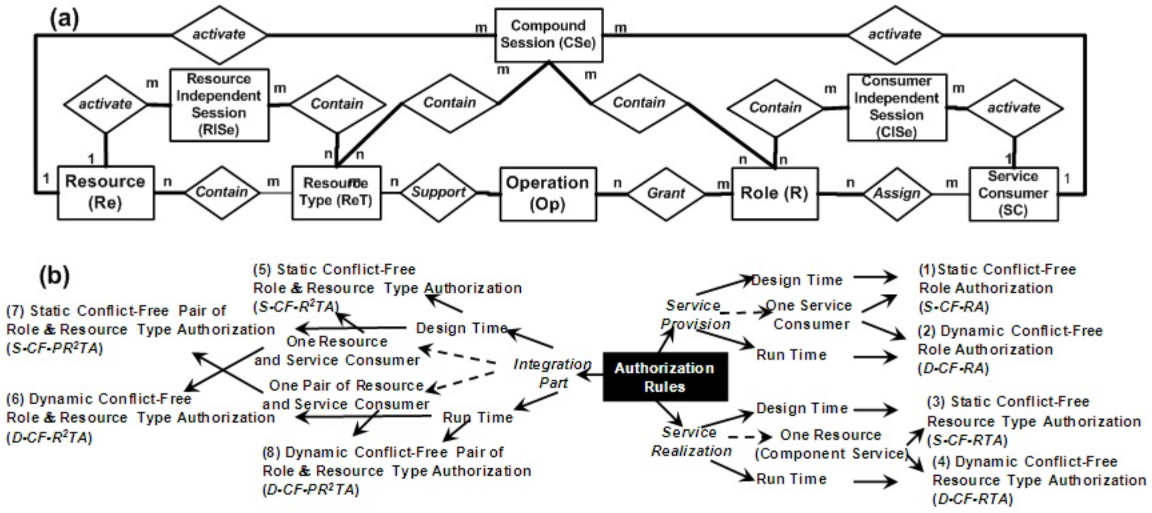
(a)
activate
Compound Session (CSe)
activate
Resource Independent Session (RISe)
Contain
Contain
Contain
Contain
Consumer Independent Session (CISe)
activate
activate
Resource (Re)
Contain
Resource Type (ReT)
Support
Operation (Op)
Grant
Role (R)
Assign
Service Consumer (SC)
m
n
1
(b)
(5) Static Conflict-Free Role & Resource Type Authorization (S-CF-R²TA)
(7) Static Conflict-Free Pair of Role & Resource Type Authorization (S-CF-PR²TA)
Design Time
One Resource and Service Consumer
Integration Part
One Pair of Resource and Service Consumer
(6) Dynamic Conflict-Free Role & Resource Type Authorization (D-CF-R²TA)
Run Time
(8) Dynamic Conflict-Free Pair of Role & Resource Type Authorization (D-CF-PR²TA)
Authorization Rules
Service Provision
Design Time
One Service Consumer
Run Time
(1) Static Conflict-Free Role Authorization (S-CF-RA)
(2) Dynamic Conflict-Free Role Authorization (D-CF-RA)
Service Realization
Design Time
One Resource (Component Service)
Run Time
(3) Static Conflict-Free Resource Type Authorization (S-CF-RTA)
(4) Dynamic Conflict-Free Resource Type Authorization (D-CF-RTA)

Fig. 1. (a) SOAC Conceptual Model and (b) Conflict-Free Authorization Rules

SOAC Engine has the following features: (1) *SOAC Engine* is developed based on our proposed conceptual model [1], SOAC (See (a) in Fig. 1), which is an extension of role based access control for the authorization of composite web services. In *SOAC Engine*, the authorization of a composite web service to a service consumer will consider "who can do what *under what kind of support*". (2) Two concepts, Role and Resource Type, are introduced in *SOAC Engine* in order to reduce the administrative overhead in the authorization management. They are mapped to component services and service consumers respectively based on their characteristics. (3) Authorization rules are embedded in *SOAC Engine* to prevent eight types of conflict of interest in terms of composite web service authorization at both design time and runtime (See (b) in Fig. 1).

A. Bouguettaya, M. Hauswirth, and L. Liu (Eds.): WISE 2011, LNCS 6997, pp. 334–335, 2011.
© Springer-Verlag Berlin Heidelberg 2011

2 System Architecture

The *SOAC Engine* (See Fig. 2) is developed with JAVA and Oracle, and resided in local web server which transfers the authorization messages between service consumer and the engine through `Application Interface`. `Authorization Management Interface` of *SOAC Engine* is used by administrator to (1) set the elements of SOAC and their relationships, (2) identify the conflicted relationships among elements, and (3) manage the authorization policies for both composite web service and resource. The *SOAC Engine* includes four component packages: (1) `Authorization Administrative Management` manages the elements of SOAC and their relationships, e.g., querying the assigned roles for specific service consumer. (2) `Credential Management` manages credentials for service consumers and resources. (3) `Authorization Decision Making` performs the policy compliance checking to make authorization decisions. The conflict of interest is checked in this packages. (4) The `Authorization Enforcement` controls the enforcement of authorization decisions related with the composite web service and its component services.

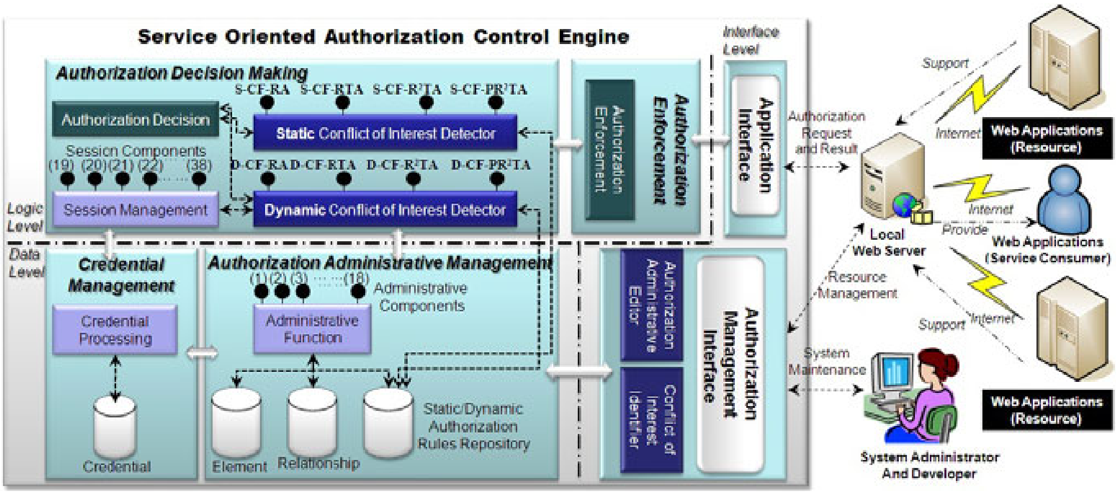
Service Oriented Authorization Control Engine
Authorization Decision Making
S-CF-RA
S-CF-RTA
S-CF-R^{2}TA
S-CF-PR^{2}TA
Authorization Decision
Static Conflict of Interest Detector
Session Components
(19) (20)(21) (22) (38)
D-CF-RA
D-CF-RTA
D-CF-R^{2}TA
D-CF-PR^{2}TA
Session Management
Dynamic Conflict of Interest Detector
Logic Level
Data Level
Credential Management
Credential Processing
Credential
Authorization Administrative Management
(1)(2)(3) (18)
Administrative Components
Administrative Function
Element
Relationship
Static/Dynamic Authorization Rules Repository
Interface Level
Authorization Enforcement
Authorization Enforcement
Application Interface
Authorization Administrative Editor
Conflict of Interest Identifier
Authorization Management Interface
Authorization Request and Result
Support
Internet
Web Applications (Resource)
Local Web Server
Internet
Provide
Web Applications (Service Consumer)
Resource Management
Support
Internet
Web Applications (Resource)
System Maintenance
System Administrator And Developer

Fig. 2. System Architecture of SOAC Engine

Reference

[1] Sun, H., Zhao, W., Yang, J.: Managing Conflict of Interest in Service Composition. In: Proceedings of CoopIS 2010, pp. 273–290. Springer, Heidelberg (2010)