

Short paper: Using Workflow for Dynamic Security Context Management in Complex Resource Provisioning

Yuri Demchenko¹, Leon Gommans¹, Cees de Laat¹, Arie Taal¹, Fred Wan¹

¹ *System and Network Engineering (SNE) Group, University of Amsterdam*

Kruislaan 403, NL-1098 SJ Amsterdam, The Netherlands
{demch, lgommans, delaata, taal, wan}@science.uva.nl

Abstract

This paper presents ongoing research and current results on developing a flexible access control infrastructure for complex resource provisioning in Grid-based collaborative applications and on-demand network services provisioning. In both cases workflow can provide required orchestration of multiple Grid or Web services representing individual resources across multiple administrative and security domains and along the whole multistage provisioning process. Workflow management tools can be used to change dynamically security context such as resource dependent security policies and user attributes. The paper describes how such required functionality is achieved in developing GAAA-P profile for provisioning. The paper is based on experiences gained from the major Grid based and Grid oriented projects such as EGEE, NextGrid, Collaboratory.nl and GigaPort Research on Network.

1 Introduction

The Generic AAA (Authentication, Authorisation and Accounting) Authorisation framework (GAAA-AuthZ) [1] provides a conceptual basis for developing an extendable service oriented access control infrastructure using standard protocols and formats for security credentials and policy expression.

With wider use and deployment of the Grid and Web Services there is increasing need for security services to be dynamically bound to the services in the Service Oriented Architecture (SOA) and configurable depending on executing task or user request. This should respond to industry demand for dynamic customer-driven service provisioning and consequently security services.

This work is based on two major use cases that define basic GAAA-AuthZ functionality in providing flexible dynamic access control infrastructure: Optical Light Path Provisioning (OLPP) [2] and Grid-based Collaborative Environment (GCE) [3], - which will be further referred as a complex resource provisioning (CRP). Significant improvement in the performance and manageability/automation of the service and resource provisioning can be achieved with the use of workflow management technologies and tools. When integrated with the service provisioning model, the workflow can also be used for managing changing security context

used in access control such as access control policy, user identity and attributes.

Proposed in this paper approach and technical solutions are based on an extended gap analysis undertaken in the framework of the SURFnet GigaPort Research on Network (GigaPort-RoN)¹ project to identify general and specific requirements to access control infrastructure for on-demand OLPP which is considered as an important component of high performance computing and Grid based collaborative applications [2].

2 Workflow Control and Security Context Management in CRP

Typically provisioning process comprises of 4 steps: resource lookup, complex resource composition (including options), reservation of individual resources and their association with the reservation ID/ticket, and finally provisioning or delivery. The reservation ID/ticket created at the reservation stage actually defines a security association between user/customer and service provider(s) that will exist for all period when the complex resource or service is used. The reservation and optionally delivery stages may require execution of complex procedures that may also require individual resources authorisation. This can be achieved by using workflow as a framework for combining executive procedures and security services with necessary security context management.

Recently, technologies and tools for managing scientific workflow and business processes are attracting great interest among e-Science community and in the business world. The paper [4] provides comprehensive overview and analysis of available Scientific Workflow Management Systems (SWMS) and their use for experiments automation. With the Web Services development, industry has been focused on developing the business process management and execution framework for Web Services. Workflow description standardisation is currently ongoing in the framework of the OASIS Web Services Business Process Execution Language (WSBPEL) TC based on early proposed BPEL4WS standard by leading industry players such as IBM, Microsoft, Oracle, and others [5].

Currently available BPEL and SWMS

¹ <http://www.gigaport.nl/info/network/ron.jsp>

implementations can simplify a major part of the provisioning process automation but there are no available solutions for integrating workflow and security services to provide reliable services or resources.

3 Extending GAAA-AuthZ for Dynamic Security Context Management

Currently GAAA-AuthZ and GAAA Toolkit (GAAA_tk) have two basic implementations: (1) for GCE that uses static Role-Based Access Control (RBAC) policy implementation in XACML; and (2) for Bandwidth-on-demand (BoD) provisioning that uses AAA-language based driving policies for controlling the provisioning process including simple access policy control. This creates a solid foundation for further GAAA-AuthZ extension to provide integrated functionality for CRP.

Proposed GAAA-AuthZ extensions for CRP features two basic profiles: a RBAC profile for collaborative applications targeted for fine-grained access control to shared resources, and a GAAA-P profile for complex resources/services provisioning in a multidomain distributed service-oriented environment.

To support dynamic security context change, the GAAA_tk should provide advanced configuration management capability based on a generic authorisation service operational model. Adding workflow processing functionality in GAAA-P profile in combination with rich policy evaluation capability in GAAA-RBAC profile will allow for complex multi-domains policy evaluation and complex provisioning algorithms execution. GAAAPI module of the GAAA_tk provides common functionality to both profiles that allows flexible policy evaluation context collection, credentials evaluation and communication between potentially distributed Policy Enforcement Points (PEP) and Policy Decision Points (PDP). GAAA-P uses GAAA-RBAC subsystem for general policy evaluation and adds flow control with the Flow Control Engine (FCE) that can together provide Rule Based Engine (RBE) functionality in the CRP process.

With the workflow and policy separation, the service request evaluation against the provisioning or individual policy can be done at three levels depending on the involved security context:

- one step (or instant) request evaluation by simply checking the request against a provided AuthZ ticket or instant push-policy;
- request evaluation against a resource policy by the PDP that uses XACML [6] as a static access control policy format specified for the so-called policy target (subject, resource, action, (environment));
- complex request evaluation that requires multiple policies evaluation in the sequence described by the provider or request specific (business) flow; in this case the FCE take care about driving the evaluation and provisioning process.

4 Integration with the GT4 and gLite Authorisation Frameworks

The aim of further GAAA_tk development is to be compatible with both Globus Toolkit Authorisation Framework² (GT4-AuthZ) and EGEE gLite Authorisation Framework³ what should allow using popular Grid middleware in CRP and collaborative applications.

GAAA_tk based applications can benefit from using a number of features specific to GT4/OGSA Security Infrastructure that include support for different types of secure credentials, in particular, X.509 Proxy and Attribute Certificates, VOMS credentials, Access Control Lists (ACL), and Grid specific access control methods such as gridmap file, identity or host based. On the other hand, GAAA_tk can add to the GT4 Authorisation Framework such functionality as authorisation session management, authorisation tickets and tokens handling, complex XACML policies evaluation, flexible trust domains and request semantics configurations and management.

5 Conclusion and Further Development

The current GAAA_tk implementation and its on-going development targets the two use cases mentioned above: OLPP and GCE. In the future the aim is the integration with higher level workflow management tools such as BPEL by accepting calls or requesting workflow/context related information from the workflow control engine via standard WSDL interface. However, to achieve better performance in such an integrated infrastructure, the integration and interaction between security services and workflow controlled processes should be done at lower layer. This may require special BPEL extensions to call security policy evaluation in business process decision points, and/or re-factoring the AAA-language for the driving policies to be able to express static access control policies and lower level flow control language. This is a current focus of ongoing research and developments at the SNE Group at the University of Amsterdam.

The origin and the target of this work are major European and national funded projects EGEE, Collaboratory.nl and GigaPort-RoN in which the authors are actively participating. However, described in this paper approach and proposed solutions can be useful for other Grid or Web Services based applications that need to combine business (or scientific) process management and security services.

6 References

- [1] RFC 2904, Informational, "AAA Authorization Framework" J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M.

² <http://www.globus.org/toolkit/docs/4.0/security/authzframe/>

³ <http://glite.web.cern.ch/glite/security/>

Holdrege, D. Spence, August 2000 - <ftp://ftp.isi.edu/in-notes/rfc2904.txt>

- [2] Filling the Gap with GAAA-P: Gap Analysis of Authorisation technologies and solutions for Optical Light Path Provisioning, Gigaport-NG RoN Technical report. Y. Demchenko, L. Gommans, B. van Oudenaarde. Available at <http://staff.science.uva.nl/~demch/analytic/airg-gp6-ron-gap-aaa-12.pdf>
- [3] Policy Based Access Control in Dynamic Grid-based Collaborative Environment, by Y. Demchenko, L. Gommans, C. de Laat, A. Tokmakoff, R. van Buuren. – Accepted paper for the 2006 International Symposium on Collaborative Technologies and Systems (CTS2006).
- [4] Zhiming Zhao et al, “Including the State of art scientific workflow management systems in an e-Science environment”, available at <http://staff.science.uva.nl/~zhiming/project/vl-e/ZhaoZ-UvA-e-Science-workflow-paper.pdf>
- [5] OASIS Web Services Business Process Execution Language (WSBPEL) TC - http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wsbpel
- [6] Godik, S. et al, “eXtensible Access Control Markup Language (XACML) Version 2.0”, OASIS Working Draft 04, 6 December 2004, available from http://docs.oasis-open.org/xacml/access_control-xacml-2_0-core-spec-cd-04.pdf