

Policy-based Access Control to Data Services in Service-oriented Architecture and Grid

a report by

Dr Yuri Demchenko

Senior Researcher, Advanced Internet Research Group, University of Amsterdam

Dr Yuri Demchenko is a Senior Researcher with the Advanced Internet Research Group (AIRG) at the University of Amsterdam. He is contributing to the development of the generic authentication, authorisation, accounting (AAA) architecture in application to open collaborative environment and computer grids. His major projects are Collaboratory.nl (CNL) and EGEE (Enabling Grid for E-Science). His active topics of interest and contribution include distributed policy-based access control infrastructure, dynamic trust and policy management in service-oriented architecture (SOA), virtual organisation security architecture, and using SAML and XACML distributed authorisation. He is also contributing to the research on operational security for XML Web services and grids. Dr Demchenko graduated from the National Technical University of Ukraine Kiev Polytechnic Institute (KPI) in 1981, receiving a diploma in instrumentation and measurement. In 1989 he received a CandSc (Techn.) degree. He has been active in Internet and computer networking since 1992.

Introduction

Many research and industry areas require efficient processing and exchange of large amounts of data to enable multi-organisation cooperative research and project development. Service-oriented architecture (SOA)¹ is increasingly considered as a platform for building heterogeneous interoperable data services that have uniform access to information/data stored in distributed databases and other data repositories. SOA/grid architecture can provide common infrastructure and services for data access, integration, provisioning, cataloging and security services, altogether often referred to as middleware.

SOA and its two major implementations, XML Web services architecture (WSA)² and open grid services architecture (OGSA),³ represent all services in a common way using Web services description language (WSDL) as a description language and simple object access protocol (SOAP) as a messaging protocol.¹ Common description and exchange formats allow uniform services description and their abstraction from the hosting platform.

Common security architecture for WSA and OGSA defines extended use of policies for manageable security services.⁴ Policies are created and controlled by a designated service administrator or by an organisation owning service or resource. Policies allow for adjustable security services and can be used for service negotiation. In grid environments, policies are typically managed by virtual organisation (VO), which provides attributes and identity management services for member organisations.⁵ VO is created on the basis of an agreement and combines users, resources and associated services. Due to the potentially complex structure of VO or other association of services and resources in SOA, access control services must be designed to handle multiple policies related both to service level and resource level.

Data Services in SOA and Basic Security Requirements

Data services in SOA and grid are represented by the data storage element (DSE) and data themselves.⁷ The

DSE is responsible for saving/retrieving files to/from local storage, which can be anything from a disk to a mass storage system and database with their specific data access interfaces. Additionally, the catalogue and/or metadata services can be provided to assist with location of requested data or content. Due to the potentially large volume of initial data used in some research projects, grid-based applications may also use a replica storage element, which contains an authentic copy of the original data.

Integrating DSE into SOA

The DSE implements the storage resource management (SRM) interface, which provides data access and management functions including local storage access control. In SOA, DSE is accessible via the Web services interface, which exposes all DSE functionality as services and allows for service virtualisation. In grid, data services can be associated with the VO, which can define common access policy. It is also perceived that DSE may apply some access restriction at the SRM level that may not be exposed at the service level policy. Possible issues for such restrictions may include limited number of requests at the same time, priority or ban-list, etc.

Security and Access Control

WSA/OGSA provide standard security services that can be bound to the service instance at the time of service invocation based on the WSDL data service description. At runtime, related services check requestor/request authentication, credentials and permissions and make an authorisation decision based on designated security policies. Consequently, security context is conveyed to the next service and finally to the SRM interface, which in turn may apply some other access restrictions that are not exposed in the service access control policy.

Service/Resource Security Zone Model

With SOA, the middleware provides a medium for conveying a service request and delivering a service (or its product) in a controlled and secure way to the requestor. In such a model, the service or resource is placed at the back-end of interacting components and services.



Figure 1: Service/Resource Site Security Zones

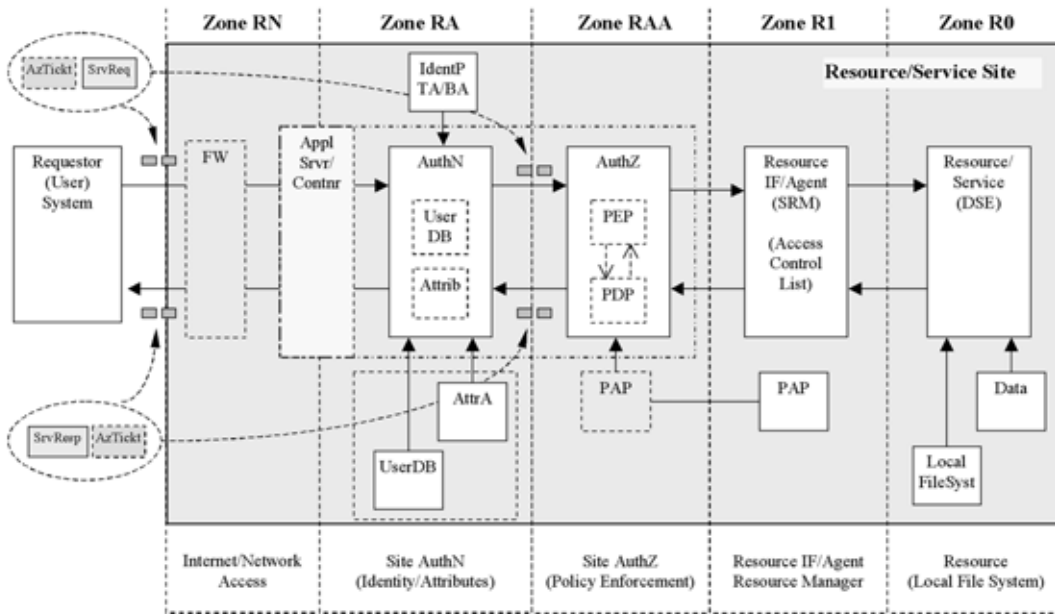


Figure 1 illustrates how major access control components interact in a typical Web services implementation using an application server or servlet container to provide multilayer security protection. The following security zones can be defined for the service/resource site:

- Zone R0 – Zone controlled by the resource itself, which includes local data storage and a local file system; this is the zone of the resource trust level.
- Zone R1 – Zone that includes resource agent, e.g. SRM interface in DSE, and other subsystems controlled and trusted by the resource, and can work under administrative privileges; this includes the policy that is specified by the resource and stored in the policy authority point (PAP). The resource agent can also use its own access control service, which is not exposed in the SOA relations/description.
- Zone RA and Zone RAA – Zones protected respectfully by authentication (AuthN) and authorisation (AuthZ) services. AuthN service verifies requestor/request credentials using the database of registered users (UserDB) and may issue associated attributes requesting the attribute authority (AA). AuthZ services includes the policy decision point (PDP) as a central policy-based decision-making authority, the policy enforcement point (PEP) providing resource-specific authorisation request/response handling and policy-defined obligations execution, and the PAP as a policy storage. Depending on particular implementation, AuthN and AuthZ services can be implemented as part of an application server or servlet container, e.g. in the form of message level filters, SOAP interceptors, etc., or run as application components or separate services in the container.
- Zone RN – Zone that includes network access

facility and is open to the world; it may also contain the firewall, which is controlled by the firewall policy and protects the resource site from external attacks against the network components and malicious input to the resource services.

Proposed security zones definition can be applied for both distributed and local host-based security services. However, their relationship to the specific security zone should be maintained by proper trust relations or credentials path.

The proposed security zone model extends other existing models, such as the URL security zones used in Microsoft Internet Explorer security model,⁷ or the security realms concept used in the Java Servlet specification⁸ and implemented in the popular servlet container Apache Jakarta Tomcat,⁹ and provides better granularity required for consistent security analysis of XML Web services and grid applications.

It is important to note that the requestor or request authentication can be done as a separate procedure before the authorisation or as an initial step of the requestor/subject verification during authorisation. In the distributed access control infrastructure, in order to optimise performance, the authorisation service may also issue authorisation ticket (AuthzTicket) based on the positive decision of the AuthZ service and can be used for evaluating the following similar requests by the PEP.⁴

Policy-based Access Control Using the RBAC Model

The authorisation service is a key part of the managed security in an open-service-oriented environment. Authorisation is typically associated with a service provider or resource owner. Figure 1 shows major

modules that participate in the service request evaluation and constitute a framework for a role-based access control (RBAC) authorisation service.¹⁰

In a simple scenario, the PEP sends a decision request to the designated PDP and, after receiving a PDP decision, relays a service request to the resource. The PDP identifies an applicable policy instance and retrieves it from the PAP, collects the required context information and evaluates the request against the policy. During this process, it may need to validate the presented credentials locally, based on established trust relationships, or call external AuthN service and AAs.

For distributed multi-domain applications an authorisation service can operate in pull or push modes, as defined by the generic authentication, authorisation, accounting (AAA) architecture¹¹ in which correspondingly the authorisation decision is requested by a resource service, or a requestor preliminary obtains the authorisation ticket from the trusted authorisation service. It subsequently presents the ticket together with the authorisation context to the resource or service.

A typical access control use-case may require a combination of multiple policies and multi-level access control enforcement, which may take place when combining newly-developed and legacy access control systems into one integrated access control solution. Reference 12 explains how multiple policy evaluation and/or policy combination can be undertaken in a distributed access control system.

Using XACML and SAML for Policy Expression, Security Assertions and Messaging

It is important that access control service implementation uses existing standards for policy expression, security assertions and messaging, which are represented by two complementary OASIS standards: XACML^{13,14} and SAML.¹⁵

eXtensible access control mark-up language (XACML) defines rich policy format for the generic RBAC and simple request/response messages format for PEP-PDP communication. XACML policy is specified for the so-called target triad 'subject-resource-action'. XACML resource is expressed as the uniform resource identifier (URI) and can address both DSE location and particular data element content, which is specifically important for controlling access to sensitive or privacy-concerning information, such as in biomedical applications.

XACML policy format can also include actions that must be taken on the positive or negative PDP decision in the form of an obligation element, which is an optional element of the policy. This functionality

is important for possible integration of the access control system with the logging or auditing facilities.

A decision request sent in a request message provides context for policy-based decision. The complete policy applicable to a particular decision request may be composed of a number of individual rules or policies. A few policies may be combined to form the single policy applicable to the request. However, the response message may contain multiple result elements related to individual resources.

New XACML specification 2.0¹⁴ defines three special profiles that can extend XACML functionality in evaluation of complex requests, which can be used for fine-grained data access control.

XACML Multiple Resources Profile

Allows for complex requests to multiple resources sharing the same request context, in this case the single resource element will contain composition of all resources to be evaluated together. Request processing may involve decomposing the one complex resource request into many individual resource requests before evaluation by the PDP.

The XACML Hierarchical Resource Profile

Specifies how XACML can provide access control for a resource that is organised as a hierarchy, e.g. file systems, XML documents, or organisational resources.

The XACML RBAC profile describes how to build policies requiring multiple subjects and role combinations to access a resource and perform an action. Multiple subject elements in XACML allow flexibility when implementing a hierarchical RBAC model for such cases when some actions require superior subject/role approval to perform a specific action.

Although XACML defines request/response messages format, it does not provide any suggestions about using one or another transport container or protocol and security mechanisms to protect message security, i.e. authenticity, integrity and confidentiality.

However, all required functionality is available in another XML-based format, security assertion mark-up language (SAML), for security assertions. It is a logical and widely used solution to combine XACML policy-based decision-making and SAML security assertion and communication mechanisms. Recently published SAML 2.0 specification¹⁵ provides even better security and improved functionality for access control services, compared with SAML 1.1:

- improved assertion security through better integrity and secure context management;

- number of specified authentication context profiles including X.509, Kerberos, PGP, XMLdsig, SSL, IP, Smartcard, mobile telephony, timesynch, etc; and
- special SAML profile for XACML¹⁶ that introduces the new elements XACMLAuthzDecisionStatement/Query, XACMLPolicyStatement/Query, which may directly include XACML request/response messages or policy statements.

In the above access control model, SAML can be used as a security assertions format in particular for AuthzTicket expression used for performance optimisation. AuthzTicket can be expressed as native SAML authorisation assertion or as XACMLAuthzDecisionStatement, which simplifies integration with XACML.

Practical use of XACML and SAML will require definition of own assertion types and will attribute name spaces for all assertion and policy components. Another area where XACML may need extensions for practical implementations is adding RBAC session management and the validation of security

tokens presented as attributes confirmation or security context into the policy decision request.

Conclusion

Emerging SOA and grids provide a good platform for building distributed interoperable data services and allow the use of basic security services provided as middleware services. When implementing XML-based technologies, it is easier to ensure the compatibility of basic security services, such as authentication, authorisation, and corresponding formats of metadata, policies, messages, etc. Generic AAA architecture and the RBAC model allow the building of fine-grained policy-based access control and separate policy definition and management from the access control service, which can be delegated to the resource owner.

XACML policy expression format and SAML security assertions format are two industry standards that provide a solid basis for building compatible manageable access control services in SOA. ■

References

1. *Service-Oriented Architecture*, http://en.wikipedia.org/wiki/Service_Oriented_Architecture
2. Booth D, "Web Services Architecture", *World Wide Web Consortium Working Group Note*, 11 November 2004, available from <http://www.w3.org/TR/ws-arch/>
3. Foster I, et al., "GFD.30, The Open Grid Services Architecture, Version 1.0," *Global Grid Forum*, 25 January 2005, available from <http://www.gridforum.org/documents/GWD-I-E/GFD-I.030.pdf>
4. "Security in a Web Services World: A Proposed Architecture and Roadmap", *A joint security whitepaper from IBM Corporation and Microsoft Corporation*. April 7, 2002, Version 1.0. – <http://www-128.ibm.com/developerworks/webservices/library/ws-secmapp/>
5. Demchenko Y, "Virtual Organisations in Computer Grids and Identity Management" Elsevier Information Security Technical Report Volume 9, Issue 1, January-March 2004, pp. 59–76.
6. Kunszt P, McCance G, Nienartowicz K, Frohner A, "Grid Data Services for Production Grids", <http://www.nesc.ac.uk/events/GGF10-DA/programme/papers/DataAreaArticle-GGF10-final.pdf>
7. URL Security Zones, MS Internet Explorer, MSDN, Microsoft, <http://msdn.microsoft.com/library/default.asp?url=/workshop/security/szone/urlzones.asp>
8. JSR-000154 Java™ Servlet 2.4 Specification (Final Release), <http://www.jcp.org/aboutJava/communityprocess/final/jsr053/>
9. Tomcat Security overview and analysis, <http://www.cafesoft.com/products/cams/tomcat-security.html>
10. "Information Technology - Role Based Access Control", Document Number: ANSI/INCITS 359-2004, InterNational Committee for Information Technology Standards, 3 February 2004, p. 56.
11. Laatz de C, Gross G, Gommans L, Vollbrecht J, Spence D, "Generic AAA Architecture", *Experimental RFC 2903*, Internet Engineering Task Force, August 2000.
12. Demchenko Y, Gommans L, de Laatz C, Oudenaarde B, Tokmakoff A, Snijders M, "Job-centric Security model for Open Collaborative Environment", *Proceedings of the 2005 International Symposium on Collaborative Technologies and Systems*, (2005), IEEE Computer Society, pp. 69–77.
13. OASIS eXtensible Access Control Markup Language (XACML), http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml
14. 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
15. "Assertions and Protocols for the OASIS Security Assertion Markup Language", (SAML) V2.0, OASIS Committee Draft 03, 14 December 2004, <http://www.oasis-open.org/committees/download.php/10627/sstc-saml-core-2.0-cd-03.pdf>
16. SAML 2.0 profile of XACML, OASIS Committee Draft 02, 11 November 2004, http://docs.oasis-open.org/xacml/access_control-xacml-2.0-saml_profile-spec-cd-02.pdf