GAAA-AuthZ components to support Complex Resource Provisioning (CRP)

Yuri Demchenko <demch@science.uva.nl>
System and Network Engineering Group
University of Amsterdam

POSPHORUS kick-off meeting, 17-18 October 2006, Poznan
Outline

- Background information - Affiliated and previous projects
  - Moving to multi-domain dynamic AAA service infrastructure
- GAAA-AuthZ components to support dynamic security context mngnt
  - Extended AuthZ ticket format
  - AuthZ security context management with GAAAPI
- Using TCG Trusted Computing and Trusted Network Connect platforms (TNC) for extending trusted application domain
- Issues to discuss

- Additional information
  - Using XACML policy format for multidomain access control administration

GAAA – Generic Authentication, Authorization, Accounting
GAAA-AuthZ – GAAA AuthZ Framework
Background information – Affiliated and previous projects

- **EGEE-I and EGEE-II**
  - EGEE gLite Java Authorisation Framework (gJAF)
    - gJAF extension to support SAML attributes, AuthZ session and full XACML policy functionality
    - Integration with the GT4-AuthZ framework
  - LCG/EGEE Operational Security and EGEE Grid Security Infrastructure

- **OGSA-AuthZ WG contribution**
  - Dynamic AuthZ service infrastructure and components

- **GigaPort NG Research on Network**
  - Gap analysis of Authorisation services functionality for Optical LightPath Provisioning (OLPP)

- **Collaboratory.nl project - industry funded project**
  - Multidomain resource administration for Collaborative applications
EGEE gJAF components and connection to the Grid Service

Grid Service

Service Gateway (SOAP Msg Interceptor)

PIP chain (extracts attributes)

PIPs

User/Local Attr

VO Attr

External Attr Call

PIPs

External Attr Auth (e.g. Shibboleth)

PIP chain (makes decision)

PDP chain (makes decision)

AuthZ Decision Combination

PDP (BL)

PDP

Ext. PDP Callout

Ext. PDP (e.g. G-PBox)

AuthZ Decision

Call from SrvGw or Msg Interceptor

AuthZ Attr/Data

Srv Request

PDP

PAP
AuthZ service operation in Grid/WS based applications

- Security/Access control services integrated with the Workflow via Web Services ports and messages definition
- Message-level Security services are linked to SOAP header
- Linking dynamically all components of the access control system
- Policy is attached to any component of the service description in WSDL format
- Interacting services will fetch policy document and apply restrictions/rules to elements, which declared policy compliance requirements
AuthZ ticket/assertion for extended security context management – Data model (1) - Top elements

Required functionality to support multidomain provisioning scenarios

- Allows multiple Attributes format (semantics, namespaces)
- Establish and maintain Trust relations between domains
  - Including Delegation
- Ensure Integrity of the AuthZ decision
  - Keeps AuthN/AuthZ context
  - Allow Obligated Decisions (e.g. XACML)
- Confidentiality
  - Creates a basis for user-controlled Secure session
- TicketID attribute
- Decision element and Resource attribute
- Conditions Element and validity attributes
- Extensible element ConditionAuthzSession
  - Any AuthZ session related data
- Subject element to keep AuthN security context and Subject Attributes
- Delegation element to allow permissions/AuthZ decision delegation to other Subjects or groups/community
ConditionAuthzSession element contains extendable security context information for a particular AuthZ Session defined by the SessionID

- Contains reference to the Policy and may include also the Policy itself
AuthZ ticket main elements

**<Decision>** element - holds the PDP AuthZ decision bound to the requested resource or service expressed as the ResourceID attribute.

**<Conditions>** element - specifies the validity constrains for the ticket, including validity time and AuthZ session identification and additionally context

  **<ConditionAuthzSession>** (extendable) - holds AuthZ session context

**<Subject>** complex element - contains all information related to the authenticated Subject who obtained permission to do the actions

  **<Role>** - holds subject’s capabilities

  **<SubjectConfirmationData>** - typically holds AuthN context

  **<SubjectContext>** (extendable) - provides additional security or session related information, e.g. Subject’s VO, project, or federation.

**<Resources>/<Resource>** - contains resources list access to which is granted by the ticket

**<Actions>/<Action>** complex element - contains actions which are permitted for the Subject or its delegates

**<Delegation>** element – defines who the permission and/or capability are delegated to: another Subjects or community attributes define restriction on type and depth of delegation

**<Obligations>/<Obligation>** element - holds obligations that PEP/Resource should perform in conjunction with the current PDP decision.
AuthZ ticket format (proprietary) for extended security context management

<?xml version="1.0" encoding="UTF-8"?>
TicketID="c8a5f22d19d1f148cf4200ef8f3e4fd2b3">
  <AAA:Decision ResourceID="http://resources.collaboratory.nl/Philips_XPS1">Permit</AAA:Decision>
  <!-- SAML mapping: <AuthorizationDecisionStatement Decision="*" Resource="*" -->
  <AAA:Actions>
    <AAA:Action>cnl:actions:CtrlInstr</AAA:Action>
    <AAA:Action>cnl:actions:CtrlExper</AAA:Action>
  </AAA:Actions>
  <AAA:Subject Id="subject">
    <AAA:SubjectID>WHO740@users.collaboratory.nl</AAA:SubjectID>
    <!-- SAML mapping: <Subject>/NameIdentifier -->
    <AAA:SubjectConfirmationData>IghAvw8YomTqB9Ege9JRNnl84AggaDkOb5W4U6</AAA:SubjectConfirmationData>
    <!-- SAML mapping: EXTENDED <SubjectConfirmationData/> -->
    <AAA:Role>analyst</AAA:Role>
    <!-- SAML mapping: <Evidence>/<Assertion>/<AttributeStatement>/<Assertion>/<Attribute>/<AttributeValue -->
    <AAA:SubjectContext>CNL2-XPS1-2005-02-02</AAA:SubjectContext>
    <!-- SAML mapping: <Evidence>/<Assertion>/<AttributeStatement>/<Assertion>/<Attribute>/<AttributeValue -->
  </AAA:Subject>
  <AAA:Delegation MaxDelegationDepth="3" restriction="subjects">
    <!-- SAML mapping: LIMITED <AudienceRestrictionCondition> (SAML1.1), or <ProxyRestriction>/<Audience> (SAML2.0) -->
    <AAA:DelegationSubjects> <AAA:SubjectID>team-member-2</AAA:SubjectID> </AAA:DelegationSubjects>
  </AAA:Delegation>
    <!-- SAML mapping: <Conditions NotBefore="*" NotOnOrAfter="*" -->
    <AAA:ConditionAuthzSession PolicyRef="PolicyRef-GAAA-RBAC-test001" SessionID="JobXPS1-2006-001">
      <!-- SAML mapping: EXTENDED <SAMLConditionAuthzSession PolicyRef="*" SessionID="*" -->
      <AAA:SessionData>put-session-data-Ctx-here</AAA:SessionData>
      <!-- SAML EXTENDED: <SessionData/> -->
    </AAA:ConditionAuthzSession>
  </AAA:Conditions>
  <AAA:Obligations>
    <AAA:Obligation>put-policy-obligation(2)-here</AAA:Obligation>
    <AAA:Obligation>put-policy-obligation(1)-here</AAA:Obligation>
  </AAA:Obligations>
</AAA:AuthzTicket>
Security context management in multidomain AuthZ: Context dependent information and existing mechanisms

- Context dependent information/attributes:
  - Policy
  - Trust domains and authorities
  - Attributes namespaces
  - Service/Resource environment/domain
  - Credential semantics and formats

- Mechanisms to transfer/manage context related information
  - Service and requestor/user ID/DN format that should allow for both using namespaces and context aware names semantics
  - Attribute format (either X.509/X.521 or URN/SAML2.0 presentation)
  - Context aware XACML policy definition using the Environment element of the policy Target element
  - Security tickets and tokens used for AuthZ session management and for provisioned resource/service identification
  - Security federations for users and resources, e.g. VO membership credentials
GAAA-AuthZ/GAAAPI components to support dynamic security context management (1)

- GAAAPI is a collection of components to support PEP and PDP interaction, implemented in Java
GAAAPI components to support dynamic security context management (2)

- Context Handler (CtxHandler) that calls to a namespace resolver (NS Resolver) and attribute resolver (AttrResolver), which in its own can call to external Attribute Authority Service (AAS) to validate presented attributes or obtain new ones

- Triage and Cache to provide an initial evaluation of the request, including the validity of the provided credentials
  - Used for handling AuthZ tickets/tokens, and also for AuthZ session management by evaluating service requests versus the provided AuthZ ticket/token claims

- Ticket Authority (TickAuth) generates and validates AuthZ tickets or tokens on the requests from PEP or PDP
  - to support AuthZ session, tickets are cached by TickAuth directly or by PEP/PDP

- Policy Information Point (PIP) that provides resolution and call-outs to related authoritative Policy Authority Points (PAP)
Extending trusted application domain with TCG and TNC

- TCG Trusted Computing platform (TCG) and Trusted Network Connect platform (TNC) can create a basis for trusted user/authority and resource/provider platforms introduction
  - TPM ensured remote platform integrity will allow to initiate trusted provisioning/AuthZ session for AAA services
  - Includes three stages
    - (1) Remote platform inspection/verification (TCG and TNC)
    - (2) Starting User session and Virtual WorkSpace Service (VWSS)
      - Provides secure executive environment for the user applications
    - (3) Starting Application session (GAAA-AuthZ)
      - Ensure Integrity and Confidentiality for the user application data
Using standard and available components

- Layer 1 - TCG and TNC platform
- Layer 2 - Grid Virtual WSS (Globus GT4)
- Layer 3 - GAAA-AuthZ AuthZ session support
Summary and Issues to discuss

- GAAA-AuthZ/GAAA-P model and basic GAAA_tk components are available to support Complex Resource Provisioning and dynamic AuthZ services invocation
  - Need some work to integrate with the GMPLS control plane
  - Provisioning scenario and provisioning/AuthZ session
  - Extending AuthZ ticket format for basic GMPLS scenarios

- Policy format for multidomain GMPLS provisioning use case
  - XACML policy profile – is XACML usable here?

- TCG Trusted Computing platform (TCG) and Trusted Network Connect platform (TNC)
  - Can we benefit from these technologies?
• XACML Special policy profiles for RBAC and Complex Resources management
XACML Special profiles for RBAC and complex Resources

- **XACML RBAC profile**
  - defines policies that require multiple Subjects and roles combination to access a resource and perform an action
  - implements hierarchical RBAC model when some actions require superior subject/role approval to perform a specific action
  - can significantly simplify rights delegation inside the group of collaborating entities/subjects

- **XACML Hierarchical Resource profile**
  - defines policy format for hierarchically organised resources, e.g. file system or XML-based repositories

- **XACML complex Resource profile**
  - allows for complex request to multiple resources having the same request context, however decision is provided per resource

- **XACML3 Policy Administration and Delegation profile**
XACML Policy structure

- XACML Policy format

```
PolicySet
  Policy
    {Rules}
    ...
  Policy
    {Rules}
  ...
Policy Target
  {S, R, A, (E)}

XACML Policy
  Rule Combination
    Algorithm
  Policy Target
    {S, R, A, (E)}
  Rule ID#1
    Rule Target
      {S, R, A}
    Condition
      AttrDesignat
      Match List
    Rule ID#n
```
RBAC AuthZ policy: XACML Policy generation conventions

- Policy Target is defined for the Resource
- Policy combination algorithm is “ordered-denial-override” or “deny-override”
- Rule Target is defined for the Action and may include Environment checking
  - Rule’s Condition provides matching of roles which are allowed to perform the Action
- Access rules evaluation
  - Rules are expressed as permissions to perform an action against Subject role
  - Rule combination algorithm “permit-override”
  - Rules effect is “Permit”
- Subject and Credentials validation – is not supported by current XACML functionality
  - Credential Validation Service (CVS) – proposed GGF-AuthZ WG development
<PolicySet>
  <Target/>
    <Description>Permit access for CNL3 users with specific roles</Description>
    <PolicyIssuer>
      <Attribute AttributeId="urn:oasis:names:tc:xacml:1.0:subject:subject-id" DataType="http://www.w3.org/2001/XMLSchema#string">
        <AttributeValue>urn:oasis:names:tc:xacml:3.0:issuer:cnl:VLab031:trusted</AttributeValue>
      </Attribute>
    </PolicyIssuer>
    <Target><Resources><Resource>
      <ResourceMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:anyURI-equal">
        <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#anyURI">
          http://resources.collaboratory.nl/Phillips_XPS1
        </AttributeValue>
        <ResourceAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:resource:resource-id" DataType="http://www.w3.org/2001/XMLSchema#anyURI"/>
      </ResourceMatch>
    </Resource></Resources></Target>
      <Target><Actions><Action>
        <ActionMatch MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ViewExperiment</AttributeValue>
          <ActionAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:action:action-id" DataType="http://www.w3.org/2001/XMLSchema#string"/>
        </ActionMatch>
      </Action></Actions>
      <Condition FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-at-least-one-member-of">
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-bag">
          <AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">analyst</AttributeValue><AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">guest</AttributeValue>
        </Apply><SubjectAttributeDesignator AttributeId="urn:oasis:names:tc:xacml:1.0:subject:role" DataType="http://www.w3.org/2001/XMLSchema#string" Issuer="CNL2AttributeIssuer"/>
      </Condition>
    </Rule>
  </Policy>
</PolicySet>