Using XML based security tickets and tokens

or

SAML demystified

Yuri Demchenko <demch@science.uva.nl>
AIRG, University of Amsterdam
Outline

- Fine grained access control with Generic AAA Authorisation framework and RBAC
  - Combined push-pull and agent-push models using AuthZ tickets and tokens
- GAAAPI implementation detail and ticket/token examples
  - Collaboratory.nl Authorisation service
- Prospective integration with GT4 and gLite Authorisation Frameworks
Distributed Security Architecture for Open Collaborative Environment (OCE) and used technologies

- Based on the Job-centric security model
  - Job description format – to be compatible with WS-Agreement and GGF JSDL (Job Submission Description Language)
- Extended RBAC functionality including RBAC administration tool (using GAAA Toolkits)
- GAAA RBE and AAA policy expression
  - XACML Request/Response messaging
  - Migration to XACML based policy exchange and combination
- SAML 2.0 based AuthzTicket format
- XML Signature and XML Encryption for JobDescription and AuthzTicket security
- Policy binding to WSDL and AuthZ portType definition
  - Using WS-Security Framework and OGSA/WSRF
- TODO: Adding VO and VOMS functionality - for user and resource attributes management
RBAC: main components and dataflow – XACML model

PEP/AEF - Policy Enforcement Point (authorisation enforcement function)
PDP/ADF - Policy Decision Point (authorisation decision function)
PIP - Policy Information Point
AA - Attribute Authority
PAP - Policy Authority Point
Site AuthZ service implementing RBAC and combined pull-push model

Issues to be addressed:
- PEP and PDP chaining
- Policy combining
- Multiple domains
Site AuthZ service implementing combined agent and push model for complex resource

Issues to be addressed:
- Multi-component and multidomain resources
- Policy push and/or token based access control
Implementation suggestions for OCE

- PDP and PAP must share common namespace
- Policy and respectively PAP should be referenced in the request message explicitly or known to PEP and PDP a priori
- Every PEP in the chain of policy enforcement should take care of the whole request evaluation/enforcement by calling to a single (master) PDP. PEP should not do multiple decision combination.
- Only one PDP should provide a final decision on the whole request
- However, PEP may have a possibility to request different PDP types based on request semantics/namespace and referred policy
- When using ticket/token based access control model, the PEP should understand and have a possibility to validate the AuthZ ticket issued by trusted PDP
  - The AuthZ ticket should have validity and usage restriction and contain information about the decision and the resource.
- For the further validation of the AuthZ tickets/token, the PEP may cache the ticket locally to speed-up the validation procedure.
Traditional Access Control model –
setting up trust and authority relations

- Policy, attributes semantics and namespaces are known a priory to all participating parties
  - A requestor knows what information to present to adhere to a specific policy and in what format (although PEP may act as ASM)
- PEP and PDP locations are known and interacting parties are known
- Trust relations between PDP, AA and resource are established
  - Resource trusts PDP’s decision that can be delivered to a Resource in a form of AuthzTicket or based on default trust between PEP and Resource
  - Root of policy enforcement hierarchy, like in real life, belongs to the resource owner

This approach is not sufficient for effective Service Oriented Architecture (SOA)
Open policy enforcement model in WSA/SOA using WS-Policy attachment mechanisms

- 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
- Provides a basis for mutual authorisation
<definitions xmlns="http://schemas.xmlsoap.org/wsdl/">
    <... snip long namespace declaration ...>
    xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy"
    xmlns:cnl="http://cnl.telin.nl/cnl" xmlns:policy="cnl-policy-schema.xsd"
targetNamespace="http://cnl.telin.nl/cnl">
    <message name="ViewExperimentRequest" wsp:PolicyURIs="cnl-policy-02example.xml">
        <part name="coordinateX" type="xs:string"/>
        <part name="coordinateY" type="xs:string"/>
        <part name="zoom" type="xs:int"/>
    </message>
    <wsp:PolicyAttachment...>
        <wsp:AppliesTo>
            <x:DomainExpression/> +
        </wsp:AppliesTo>
        <wsse:Security>... </wsse:Security> ?
        ...
    </wsp:PolicyAttachment>
    <wsp:UsingPolicy wsdl:Required="true"/>
</definitions>
Trust relations in distributed AAA infrastructure

Trust/credentials chain and delegation between major modules:

User =>

=> HomeOrg.staff(TA2) =>

=> Job.members =>

=> Member.roles =>

=> Role.permissions

The process of obtaining required permissions to perform requested action by the user:

User => AuthN(HomeOrg.staff, Job.members) =>

=> AuthZ(Member.roles, Policy.permissions) =>

=> Resource.permissions
Implementation suggestions for OCE Job-centric security model

- Root of trust and authority belong to the Resource
- Trust anchor TA2 embedded into the Job Description is the main trust anchor shared between the resource and the customer.
  - In more business integrated model the signed order may contain TA1
  - Both TA2 and TA1 may have the same trust path to the root/resource
- To become a shared trust anchor for the resource and the customer trust domains, the Order or JobDescription must contain mutually signed credentials/certificates
- Although the main PEP operation assumes authorisation decision request from the trusted PDP, in general PEP may accept an AuthzTicket from the trusted external PDP
Before deploying security infrastructure

• Design conventions and agreements
  • Key distribution and trust establishing
    ◆ In search of simple consistent model
  • Policy definition including subject, attributes, actions semantics and namespaces
    ◆ Compatibility with existing, e.g. SAML, XACML
  • Security credentials format
    ◆ Standard vs proprietary
  • Protocols and Messages format
    ◆ SOAP + XACML Request/Response
      vs
    ◆ SOAP + SAML + XACML
Authorisation Service operation in a CNL2 Demo system

1. Login
2. JNLP
3. JNLP
4. getJobInfo()
5,10 startSession()
6,9 startSession()
7,8 requestDecision()
11,14 goLeft()
12,13 checkAuthZStatus()

Note: we assume SSL TCP connections all over.
Tickets/Tokens handling in AuthZ system

- AuthzTicket is issued by PDP and may be issued by PEP
- AuthzTicket must be signed
- AuthzTicket contains all necessary information to make local PEP-Triage Request verification
- When using AuthzTokens, AuthzTickets must be cached; Resolution mechanism from token to ticket must be provided
Mapping between CNLAuthzTicket, XACML Request/Response and SAML2.0 Authorization Assertion

SAML 2.0 vs SAML 1.1
- Better security features
- Issuer and Subject are top level elements
- Encrypted elements for Subject, Attributes, Evidence
- Special profile for XACML

General problems for AuthZ
- Attributes can be placed only as deep as 5 level down: Assert/AzStm/Evid/AttrAsrt/Attr/AttrValue
- Ambiguous location for PolicyURIs and SessionID
- SAML1.1 ConfirmationData element is extensible type – compatibility problems
CNLAuthzTicket example – 1011 bytes

```xml
<cnl:CNLAuthzTicket xmlns:AAA="http://www.AAAarch.org/ns/AAA_BoD"
PolicyURIs="CNLpolicy01" SessionIndex="JobXPS1-2005-001"
TicketID="c24d2c7dba476041b7853e63689193ad">
    <!-- Mandatory elements -->
    <cnl:Decision
        ResourceID="http://resources.collaboratory.nl/Philips_XPS1">Permit</cnl:Decision>
    <cnl:Validity NotBefore="2005-02-13T01:26:42.699Z" NotOnOrAfter="2005-02-14T01:26:42.699Z"/>
    <!-- Additional elements -->
    <cnl:Subject Id="subject">
        <cnl:SubjectID>WHO740@users.collaboratory.nl</cnl:SubjectID>
        <cnl:SubjectConfirmationData>SeDFGVHYTY83ZXxEdsweOP8Iok</cnl:SubjectConfirmationData>
        <cnl:JobID>CNL2-XPS1-2005-02-02</cnl:JobID>
        <cnl:Role>analyst@JobID;expert@JobID</cnl:Role>
    </cnl:Subject>
    <cnl:Resource>http://resources.collaboratory.nl/Philips_XPS1</cnl:Resource>
    <cnl:Actions>
        <cnl:Action>cnl:actions:CtrlInstr</cnl:Action>
        <cnl:Action>cnl:actions:CtrlExper</cnl:Action>
    </cnl:Actions>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ... </ds:Signature>
</cnl:CNLAuthzTicket>
```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315"/>
    <ds:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
    <ds:Reference URI="">
      <ds:Transforms>
        <ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
        <ds:Transform Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20010315#WithComments"/>
      </ds:Transforms>
      <ds:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
      <ds:DigestValue>nRNrzZDiw/2aDnKXFEHSeoiXnsc</ds:DigestValue>
    </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue>
    0IZt9WsJT6an+tIxhhTPtiztDpZ+iynx7K7X2Cxd2iBwCUA0n61Szv81DKl1Wsq75IsHfusnm56zT3fhKU1zEUsob7p6oMLM7hb42+vjfvNeJu2roknhIDzruMrr6hMDsIfaotURepu7QCT0sADm9IfX89Et55EeSE9oE9qBD8=
  </ds:SignatureValue>
  <ds:KeyInfo> << ... snip ... >> </ds:KeyInfo>
</ds:Signature>
RSA `<ds:KeyInfo>` element – 1010 bytes (total signed ticket with KeyInfo - 3078 bytes)

```
<ds:KeyInfo>
  <ds:X509Data>
    <ds:X509Certificate>
      MIICADCCAWkCBEGX/FYwDQYJKoZIhvcNAQEEBQAwRzELMAkGA1UEBhMCTkwGCTAXBgNVBAMTEENv
      bGxhYm9yYXV0cnkubmwxHTAbBgNVBAMTFEFBFQXV0aHJ1YWNoIFNlY3VyaXR5MB4XD
      TA0MTExNTAw
      NDYxN0XDTA1MDIxMzAwNDYxNFOwRzELMAkGA1UEBhMCTkwGCTAXBgNVBAMTEENvbGxhYm9yYXRv
      cnkubmwxHTAbBqNVBAMTFEFBFQXV0aHJ1YWNoIFNlY3VyaXR5MGfMA0GCSqGSIb3DQEBAQUA
      ADBiQKBgQDDrBhvMr1nD9eqi7U7m4yIRxfvjAKv33EpuajvTKHlpKUgLjbcBC3jNJ4F7a0GiXQ
      cVbuF/aDxf/yCUJXQktxFxK0Sm77WVeSe10cLc1hYfUSAg4mudtfsB7rAj+czNNvdr6RLFpS9YF
      lv5ptGASbwHjU02HnArEGL2K+0AwIDAQABMA0GCSqGSIb3DQEBAUA4GBADHKqkOW4mP9DVo
      bMvf4qXth7yv8o3zo17+nq1B9Tqf/bVNLmk8vNo5fWRHbpnHIFGfTk31nrJk8kEZeofvwAeW9s
      lgQtY6f10xvsMPKHxFjJD1Z1LkHRViJl/slz5a7pKlqIXLRsPFRziTksemRXB/fT8K4zM14pzQ2g
      HicO
    </ds:X509Certificate>
  </ds:X509Data>
  <ds:RSAKeyValue>
    <ds:Modulus>
      3Q6wYV2q9Zw/Xqou105uMoyEcX74wCr99xKbmo70yh6S1IC423AQtzSeBe2tBo10HFW7hf2g8f8
      nSFCV0JLbxcStEpu+11XknpdHC3NYWH1EgIOJrbX7Ae6Wl/gszZ1Xa+kSxaUvWBRJb+abRmjrkm
      8B41NNh5WkxbIviTAM=
    </ds:Modulus>
    <ds:Exponent>AQAB</ds:Exponent>
  </ds:RSAKeyValue>
</ds:KeyInfo>
```
CNLAuthzToken example – 293 bytes

```
<cnl:CNLAuthzToken TokenID="ed9d969e1262ba1d3a7f33dbd670dd94">
  <cnl:TokenValue>
    0Izt9WsJT6an+tIxhhTPtiztDpZ+iynx7K7X2Cxd2iBwCUTQ0n61Szv81DKl1Wsq75IsHfusnm56zT3fhKU1zEUsob7p6oMLM7hb42+vjfvNeJu2roknhIDzruMrr6hMDsIfaotUREpu7QCT0sADm9IfX89Et55EkSE9oE9qBD8=
  </cnl:TokenValue>
</cnl:CNLAuthzToken>
```

- CNLAuthzToken is constructed of the CNLAuthzTicket TicketID and SignatureValue
- CNLAuthzToken use suggests caching CNLAuthzTicket’s
    <Condition xsi:type="typens:cnl:session-id">JobXPS1-2005-001</Condition>
  </Conditions>
  <AuthorizationDecisionStatement Decision="Permit" Resource="http://resources.collaboratory.nl/Philips_XPS1">
    <Action Namespace="urn:oasis:names:tc:SAML:1.0:action:cnl:action">cnl:actions:CtrlInstr</Action>
    <Action Namespace="urn:oasis:names:tc:SAML:1.0:action:cnl:action">cnl:actions:CtrlExper</Action>
    <Evidence>
      <Assertion AssertionID="f3a7ea74e515ffe776b10a7eef0119d7" IssueInstant="2005-02-15T14:53:23.542Z" Issuer="cnl:subject:CNLAAAauthority" MajorVersion="1" MinorVersion="1"></Assertion>
      <AttributeStatement>
        <Subject>
          <NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress" NameQualifier="cnl:subject">WHO740@users.collaboratory.nl</NameIdentifier>
          <SubjectConfirmation>
            <ConfirmationMethod>signed-subject-id</ConfirmationMethod>
            <ConfirmationData>
              PBL1R0aZRt2mq79j1j8eDpJ5VT6BxxWBtSAPc5BPnIsfHRU0OOpWQowXBlw2TmOZdJGNzFWhMinz
              XU3/w5dLjv+siO2JGfyZ7U9eqkMGqY8VlzI5uRuUaarr7AIRv9/DPlksJMNDZ5DnGosMc+zYqn
              KogfMqHK+DkJwFH6U</ConfirmationData>
          </SubjectConfirmation>
        </Subject>
          <AttributeValue xsi:type="typens:cnl:job-id">CNL2-XPS1-2005-02-02</AttributeValue>
        </Attribute>
      </AttributeStatement>
    </Evidence>
  </AuthorizationDecisionStatement>
</Assertion>
CNLAuthnTicket example – 1752 bytes

<cnl:CNLAuthnTicket xmlns:AAA="http://www.AAAarch.org/ns/AAA_BoD"
  TicketID="f35585dfb51edec48de0c7eadb11c17e">
  <!-- Mandatory elements -->
  <cnl:Subject Id="subject">
    <cnl:SubjectID>WHO740@users.collaboratory.nl</cnl:SubjectID>
    <cnl:SubjectConfirmationData>
      0+qQNAVuZW4txMi8DH6DFy7eLMGxSfKDJY6ZnY4UW5Dt0JFtat1EprUtnjCkzrJUMvWk9qtUznasDdUG+P4ZY7dgab+PHiU91ClusZbztu/ZIjNqCnw5su1BQLTumC8ZTtYKKJi4WWes+bMMbP8mFNPm
      +M7F4bJIPBfLcxf0bk4=
    </cnl:SubjectConfirmationData>
  </cnl:Subject>
  <!--Optional elements -->
  <cnl:SubjectAttribute attrname="urn:cnl:subject:attribute:job-id">
    CNL2-XPS1-2005-02-02
  </cnl:SubjectAttribute>
  <cnl:SubjectAttribute attrname="urn:cnl:subject:attribute:role">
    analyst@JobID;expert@JobID
  </cnl:SubjectAttribute>
</cnl:CNLAuthnTicket>
CNLAuthnToken is constructed of the CNLAuthnTicket TicketID and SubjectConfirmationData which is encrypted SubjectID value

CNLAuthzToken must be self-sufficient and doesn’t require caching CNLAuthnTicket’s
Integrating with existing Access Control and other tools

• Policy mapping between XACML, AAA Policy Language and other formats
• GT4 Authorization Framework
• EGEE gLite Authorisation Framework
AAA Policy and RBAC/XACML Policy

[Diagram showing the structure of AAA Policy and RBAC/XACML Policy]

- **CNL AAA Policy**
  - Subject
  - Resource/Environment
  - Rules

- **RBAC/XACML Policy**
  - **PolicySet**
    - **Policy**
      - {Rules}
    - ...
GT4 AuthZ framework: Implementation details

- Source code tree
  
  org.globus.wsrf.impl.security.authorization

- Still using grid-map file as a major option

- Special interface for PDP and PIP to interact with Interceptor

- Very simple example provisioning for XACML
  
  - Simple policy format
GT4 AuthZ framework: Multiple configured PDPs

GT4 implementation uses Interceptor concept
- Originated from POSIX AuthZ f/w
- Supported by Axis Handlers
- PEP function is (virtually) eliminated
- “Deny-override” vs “Permit-override” combination
- Configured by Interceptor PDP/PIP call-out list
- PDP are called directly or via PIP
Acknowledgements

This work is a part of research on development of the Generic AAA Authorisation framework by the Advanced Internet Research Group at the University of Amsterdam.

Credits for discussion, contribution and ideas to all AIRG group and in particular Bas van Oudenaarder, Leon Gommans, and David Group.