Context-Aware Access Control for Pervasive Access to Process-Based Healthcare Systems

Vassiliki Koufi and George Vassilacopoulos

University of Piraeus
Department of Digital Systems

MIE Congress
May 25-28, 2008
Healthcare

- Healthcare is an increasingly collaborative enterprise involving a broad range of healthcare services provided by
  - many individuals and
  - organizations.

- Provision of readily access to integrated healthcare information at the point of care is needed.

- A system architecture is required that
  - enables collaboration and coordination among healthcare services, and
  - facilitates the mobility of healthcare professionals.
HDGPortal Application

- HDGPortal:
  - is a prototype Grid portal application,
  - is designed for being used with Personal Digital Assistants,
  - provides pervasive access to process-based healthcare systems, i.e. it is used to run healthcare processes which:
    - are implemented in the Business Process Execution Language (BPEL), and
    - invoke Grid database services, while on execution, in order to provide integrated access to healthcare information scattered on a Grid computing infrastructure.

Vassiliki Koufi et al, Department of Digital Systems, University of Piraeus
MIE2008
The need

- In healthcare applications tight matching of permissions to actual usage and need is essential.
- One important security requirement in HDGPortal is adherence to the least privilege principle.
  - It ensures that users assume the minimum sets of permissions required for
    - the execution of each task of a healthcare process selected, and
    - the execution of the relevant grid database services invoked by the task.
- Changes in contextual information should be sensed during task executions and relevant adjustments of user permissions should be fired in response to these changes.
Our Approach

- A context-aware access control mechanism is proposed that
  - meets the needs of situations, often occurred in healthcare delivery, where the information requested by an authorized user needs to be available when and where needed,
  - incorporates the advantages of broad, role-based permission assignment and administration across object types, as in RBAC, and
  - provides the flexibility for adjusting role permissions on individual objects during a BPEL process enactment according to the current context.

Vassiliki Koufi et al, Department of Digital Systems, University of Piraeus
MIE2008
Motivating Scenario

- Sample integration project concerned with the automation of a cross-organizational healthcare process spanning a health district.

- A health district consists of:
  - one district general hospital (DGH)
  - peripheral hospitals
  - health centers

- Patient referrals (e.g. for hospitalization, outpatient consultation or performing specialized medical procedures) are usually made among various healthcare providers within a health district.

- There is a need to ensure authorized access to tasks comprising the relevant healthcare processes and, then, to patient information requested through the execution of these services.
Sample Healthcare Process

- A healthcare process concerned with a radiological request issued by physicians on a ward round, for their patients.

- The radiological department:
  - receives each request,
  - schedules the radiological procedures requested, and
  - sends a message to the requesting physician notifying him/her on the date and time scheduled for its performance.

- The radiologist on performing the radiological procedure requested:
  - accesses the relevant part of the patient record,
  - issues a radiological report, incorporating both the radiological images and the associated assessment, and
  - sends the report to the requesting physician.
Sample Healthcare Process

Radiological request process model using IBM WebSphere Workflow

Vassiliki Koufi et al, Department of Digital Systems, University of Piraeus
MIE2008
Security Requirements

- Security requirements with regard to authorization:
  
  - *Restricted task execution*
    
    In certain circumstances the candidates for a task instance execution should be dynamically determined and be either a sub-group of the authorized users or only one, specific authorized user.

  - *Restricted grid database service invocation*
    
    Given that a role holder can execute a specific task, he/she should be allowed to exercise a dynamically determined set of permissions on certain data only which are accessible via the associated Grid database services.

Vassiliki Koufi et al, Department of Digital Systems, University of Piraeus
MIE2008
Access Control Architecture
Access Control Architecture

- Access control is provided at:
  - the BPEL task level, and
  - the Grid database level.

- **Middleware-based**
  - It is employed to mediate between subjects (healthcare professionals) and objects (BPEL tasks and Grid database services) and to decide whether access of a given subject to given object should be permitted or denied by taking into account the current context.
  - It consists of:
    - an external to the BPEL engine access control service that regulates user access to tasks, and
    - an external to OGSA-DAI, access control service that enhances its mechanism by adding context-awareness features.

Vassiliki Koufi et al, Department of Digital Systems, University of Piraeus
MIE2008
Access Control Architecture

- **Certificate-based**
  
  It relies on certificates which:

  - are issued to healthcare professionals,
  - are generated by Community Authorization Service (CAS) which is part of the Globus Toolkit which is installed on a server at the DGH site,
  - specify user-to-role assignments in the form of security assertions, expressed in Security Assertion Markup Language (SAML) (The roles used are functional, i.e. independent of the constraints held at the time of attempted access), and
  - accompany every request (either for task execution or Grid database service invocation) issued through HDGPortal.

*Vassiliki Koufi et al, Department of Digital Systems, University of Piraeus MIE2008*
Access Control Architecture

- Access control policies:
  - are used for the mapping of the roles to the relevant permissions,
  - are expressed by using the RBAC profile of eXtensible Access Control Markup Language (XACML),
  - are specified at the site where the target object (task or Grid database service) resides (tasks are hosted on the BPEL engine at the DGH site and Grid database services are hosted on the web servers at the hospital sites), and
  - assist in the derivation of the exact permissions a subject should acquire for performing a task.

- Permissions on both BPEL tasks and Grid database services are dynamically adapted by the constraints imposed by the current context.
Context Information Management

Contextual Information:

- is determined by a pre-defined set of attributes related to:
  - the user (e.g. user certificate, user/patient relationship),
  - the environment (e.g. client location and time of attempted access), and
  - the data resource provider, namely to the healthcare organization (e.g. local security policy).

- is collected by a Context Manager which has been implemented as a multi-agent system that consists of:
  - Service Integration Agent, and
  - Grid Resource Agent.

Vassiliki Koufi et al, Department of Digital Systems, University of Piraeus
MIE2008
Security Architecture

Security Architecture in HDGPortal

Vassiliki Koufi et al, Department of Digital Systems, University of Piraeus
MIE2008
Access Control Mechanism

- On issuing a request for a task execution,
  - the roles contained in the CAS certificate accompanying the request are extracted and
  - The roles’ relevant permissions regarding access to BPEL tasks are specified using a file storing the XACML policies. This file resides on the same server of the DGH site with the BPEL engine.

- Then, during task execution,
  - a request for invocation of the underlying Grid database services is issued
  - The request is accompanied by the same CAS certificate.
  - The roles extracted from this certificate are used in order to specify the relevant permissions regarding Grid database services using XACML policies stored in one file at each Grid node (i.e. healthcare organization) providing the portion of medical information requested.
Concluding Remarks

- Provision of readily access to integrated healthcare information at the point of care, introduces security risks especially with regard to authorization and access control.

- Hence, adherence to the least privilege principle is considered a prominent feature of systems developed.

- Access control mechanisms should provide tight, just-in-time permissions so that authorized users get access to specific objects subject to the current context.

- The access control mechanism presented in this paper
  - meets the aforementioned requirements,
  - ensures a tight matching of permissions to actual usage and need, and
  - is embedded into a Grid portal application, namely HDGPortal.
Thank you for your attention