Behavior Based Access Control Model for Distributed Healthcare Environment

Mohammad Hosein Yarmand
Kamran Sartipi
Douglas Down
{yarmanmh, sartipi, downd}@mcmamster.ca

Dept. of Computing and Software
McMaster University, Canada

CASCON
November 2, 2009

Summary

Sensitivity of clinical data and strict rules regarding data sharing have caused privacy and security to be critical requirements for using patient profiles in distributed healthcare environments. The amalgamation of new information technology with traditional healthcare workflows for sharing patient profiles has made the whole system vulnerable to privacy and security breaches. Standardization organizations are developing specification to satisfy the required privacy and security requirements. In this research we present a novel access control model based on a framework designed for data and service interoperability in the healthcare domain. The proposed model for customizable access control captures the dynamic behavior of the user and determines access rights accordingly. The model is generic and extensible in the sense that an access control engine dynamically receives security effective factors from the subject user, and identifies the privilege level in accessing data using different specialized components within the engine. Standard data representation formats and ontologies are used to make the model compatible with different healthcare environments. The access control engine employs an approach to follow the user's behavior and navigates between engine components to provide the user's privilege to access a resource. A simulation environment is implemented to evaluate and test the proposed model.

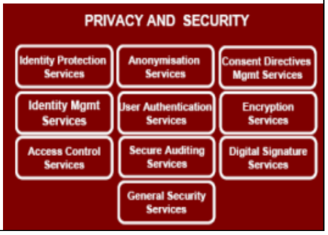
Problem Statement

> *Access Control is any mechanism by which a system grants or revokes the right to access some data, or to perform some action.*

- Motivations
  - Access control in distributed systems
    - Heterogeneous environment
    - Various requirements
    - Dynamic administration
      - Organization specific privacy rules
      - Context awareness
      - Generality
      - Sequence control
      - Decentralization
      - Flexibility of policies
      - Auditing
      - Dynamic Administration
  - Specifications for the healthcare security

Security in Healthcare Standards

- **Standards Organizations**
  - HL7
  - Canada Health Infoway
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Integrating the Healthcare Enterprise (IHE)
  - SNOMED and LOINC Committees
- **Canada Health Infoway**:
  - P&S Requirements
  - P&S Conceptual Architecture
- **HL7**:
  - Scenario Driven Access Control
- **IHE**:
  - Audit Trail list

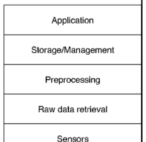

PRIVACY AND SECURITY
Identity Protection Services
Anonymisation Services
Consent Directives Mgmt Services
Identity Mgmt Services
User Authentication Services
Encryption Services
Access Control Services
Secure Auditing Services
Digital Signature Services
General Security Services

Access Control Models

- **Existing access control models**
  - Role Based Access Control
  - Team Based Access Control
  - Content Based Access Control
  - Scenario Based Access Control
  - Attribute Based Access Control
  - Context Aware Access Control
  - Context Sensitive Access Control
- **Healthcare specific security issues**
  - Audit Trail
  - Patient Consent
  - Flexibility in Emergency Situations

Context-aware Systems

- Context
- Context-aware Systems
- **Layered conceptual framework for context aware systems:**
  - Sensors layer: a collection of sensors
  - Raw data retrieval layer: responsible for the retrieval of raw context data
  - Preprocessing layer: responsible for:
    - Reasoning and interpreting contextual information
    - Aggregation or composition
    - Solving conflicting sensing
  - Storage layer: organizes data which is offered to public through an interface.
  - Application layer: the actual reaction on different events and context-instances



User Behavior

User Behavior is defined as a sequence of actions, where each action represents a collection of user's attributes.

- An action performed by user can be defined using the following attribute tuple:
  **<Person,
  Role,
  Location of User,
  Location of Server,
  Time of Day,
  Team,
  Delegation,
  Requested Profile Status,
  Service Invocation Type,
  Requested Data Type,
  Login/out>**
- **We define two types of behavior**:
  - **Time-span behavior**: recording the sequence of actions performed during a specified time (last five hours, during a day, a month, etc.)
  - **Snapshot behavior**: recording the attributes of the same action in consecutive days

Behavior Based Access Control

- Make access control decision based on:
  - a single action tuple
  - the comparison of *common behavior* and *daily behavior*

Common Behavior is defined as the behavior that a user is expected to follow based on the analysis of his behavior history.

Daily Behavior is defined as the behavior which is recorded for a given user from the beginning of a day.

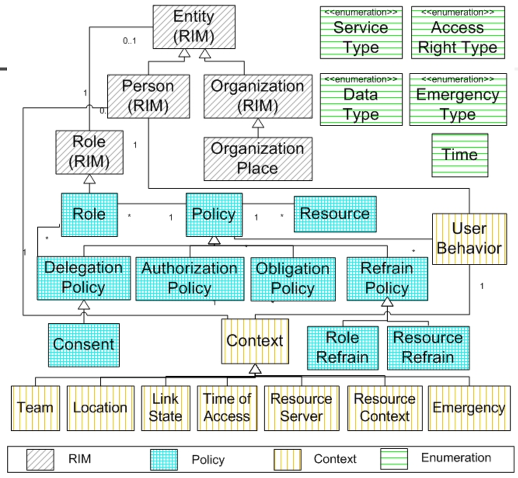
- Formal definitions
  - Action: $A \subseteq U \times R \times C \times T \times D \times RC \times Res \times OP \times DT \times L$
  - Behavior: $B: U \longmapsto 2^A$
  - Access Request: $AR \subseteq U \times reqPerm \times B(u) \times A$
  - Access Control Policy: $ACP \subseteq Subject \times P \times Constraint$

Decision Making Algorithm

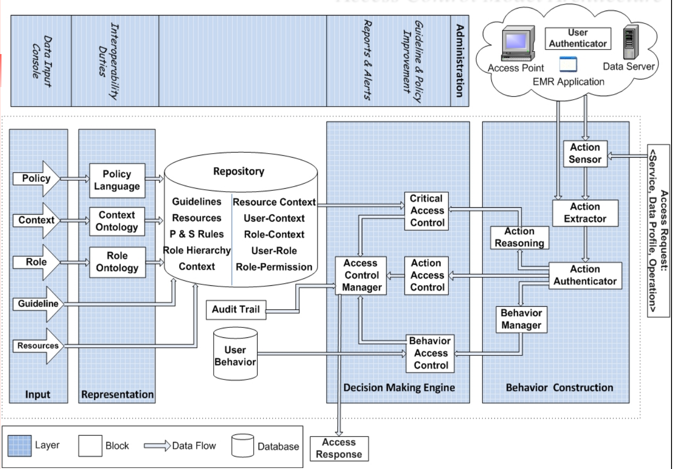
Algorithm 1 Access Control Mechanism $(< u_i, p_e, b(u_i), a >\in AR)$

```
ses := SessionUser^{-1}(u_i)
RArray := SessionRole(ses)
TRArray := SessionTeamRole(ses)
for all r ∈ RArray ∪ TRArray do
    PArray := PArray ∪ all permissions that are in relation PA with r
end for
if p_i ∈ PArray then
    if (∃< u_j, p_f, l >∈ ACP. u_i = u_j ∧ p_e = p_f ∧ l is true by checking AC ∧ BC ∧ LC) then
        Grant Access and Update b(u_i)
    else
        Deny Access and Update b(u_i)
    end if
end if
```

Security Effective factors Class Diagram



Access Control Model Architecture



Implementation

- Implementation stages:
  - Scanner and parser for specification files
  - Engine for specification language
  - Extract behavior from simulated data
  - Make access control decision
- Implementation tools:
  - Java – Eclipse – MySql – Protégé – OWL
- Rei specification files:
  - Ontology – Instance – policy
- Rei ontologies:
  - Policy – Meta policy – Entity – Deontic – Action – Constraint – Analysis

Future Work

Conclusion and Future Work

- We designed and implemented a behavior based access control model for heterogeneous distributed environments
- The model satisfies the security requirements in the healthcare domain
- Evaluate the model in a real world case study
- Improve the analysis and algorithms introduced for different components of the architecture