Architecture-Centered Composition of Adaptive and Dependable Enterprise Security Services

Yi Deng
Konstantin Beznosov
Center for Advanced Distributed Systems Engineering (CADSE)
School of Computer Science
Florida International University
{deng,beznosov}@cs.fiu.edu
Outline

- Overview of CADSE
- Architecture-Centered Composition of Application Authorization Service - Research Approach
- Preliminary Research Results
- The next steps
CADSE Goals

• To establish a streamlined program that integrates basic research, applied R&D, graduate education and training
  – Establish proper balance between basic research with applied R&D
  – Use real-world problems to guide basic research and to facilitate technology transfer
  – Use R&D to facilitate and complement basic education
  – Integrate research & education with industry collaboration
CADSE Overview

- Personnel: 3 professors, 4 postdocs and research associates, close to 20 graduate students
- Facility: 5 research labs total over 3500 sq. ft, over 50 workstations, servers and other equipment
- Funding: Over $3 million research funding from various Federal agencies and industry
Current Projects

• Distributed object technology
• Enterprise system development based on CORBA
• Software Security
• Software architecture and domain specific architecture
• Formal engineering methods, software verification and testing
• Distributed multimedia Information systems
Outline

• Overview of CADSE
• Architecture-Centered Composition of Application Authorization Service - Research Approach
• Preliminary Research Results
• The next steps
Composibility of Secure Enterprise Systems

• Support for integration
• Uniform administration of enterprise security policies
• Assurance to end-to-end properties
  – security policies, performance, availability, etc
• Support for continuous evolution
  – add or change system/components
  – change policies or business process, etc
Problems in Application-Level Security

- Must handle fine grain, complex, dynamic policies
- Embedded in application systems today
  - multiple points of control
  - problems in administration
  - expensive life-cycle
What Solutions Available Today?

- Middleware security architectures
  - CORBA, EJB, DCE, DCOM
- Resource Access Decision (RAD) specification
  (to be discussed later)
- Open issues
  - support for fine-grain, complex policies
  - dynamic changes and configuration
  - performance and availability concerns
  - end-to-end properties assurance
Framework of Our Approach

Enterprise Security Architecture (structural basis of composition)

Constraint Patterns (behavioral basis of composition)

Modeling & Analysis Methods (Assessment & Assurance to composition)
Distributed Security Architecture: Research Issues

• Focus on CORBA-based Application Authorization Service (AAS) Architecture
  – Configurability
    • support dynamic policy changes
    • support different distributed, e.g. Internet based e-commerce, environments
  – Adequate performance (distributed authorization and load balancing)
  – High availability (replication and fault tolerance)
  – Application composibility
Aspect-Oriented Models of Security Service

Performance analysis

Policy Assurance Analysis

Availability Assessment

Performance Aspect Model

Behavior Aspect Model (Policy)

Behavior Model (Availability)

Reachability Analysis

Base Architecture Model of Distributed AAS

Architectural Model of RAD Framework

Policy Completeness Analysis
Outline

• Overview of CADSE
• Composition of Adaptive and Dependable Application Authorization Service - Research Approach
• Preliminary Research Results
  – Research in application authorization service
  – An example
  – Modeling and analysis of AAS
• The next steps
Framework of Resource Access Decision Facility

1. Application Request
2. Authorization request
3. Reply to authorization request
4. Reply to application request

Client
Target Object (ADO client)
Access Decision Object

Middleware
Application Client
Application System
Authorization Service
RAD Components

1: access_allowed

2: get_policy_decision_evaluators

3: get_dynamic_attributes

4: combine_decisions

5: * evaluate

Application System

Access Decision Object

Policy Evaluator Locator

DynamicAttributeService

DecisionCombinator

PolicyEvaluator
Current Results

- Conceptual architecture of RAD
- A prototype CORBA-based Application Authorization Service (CAAS)
  - CORBA-based
  - highly configurable
  - portable (Java)
- Performance experiments
- Support for different types of policies
  - federations, multi-policy, RelBAC
CAAS Configuration Examples

Process/Object

Client Host

Application Process

Authorization Process

Server Host

CAAS

Process/Process

Client Host

Application Process

CAAS Authorization Processes

Server Host

DAS

DC

PEL

PE

Host/Object

Client Host

Application Process

Authorization Process

Server Host

CAAS

Authorization Host

Process/Process/PE

Client Host

Application Process

CAAS Authorization Processes

Server Host

Authorization Host

PE Process

PE Host

2/14/00

CADSE/FIU
### An Example: Initial Policies

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P-1</td>
<td>Any caregiver can read patient’s name.</td>
</tr>
<tr>
<td>P-2</td>
<td>Registration clerk can modify patient name and demographic information.</td>
</tr>
<tr>
<td>P-3</td>
<td>Nurse can read patient’s name and demographic information, modify current episode demographic information, can read current episode regular records and current episode regular test results.</td>
</tr>
<tr>
<td>P-4</td>
<td>Technician can modify current episode regular and sensitive test results.</td>
</tr>
<tr>
<td>P-5</td>
<td>Assistant physician, in addition to what a nurse can do, can also read all regular records of patients.</td>
</tr>
<tr>
<td>P-6</td>
<td>Physician, in addition to what assistant physician can do, also can modify current episode regular and sensitive records, and read regular and sensitive records and test results from previous episodes.</td>
</tr>
<tr>
<td>P-7</td>
<td>Psychiatrist, in addition to what a physician can do, also can modify mental information.</td>
</tr>
</tbody>
</table>
Modeling with RBAC

Role Hierarchy

Psychiatrist

Physician

Physician Assistant

Registration

Nurse

Technician

Care-giver

User to Role Assignment Relation (UA)

<table>
<thead>
<tr>
<th>Roles</th>
<th>Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Psychiatrist</td>
<td>✓</td>
</tr>
<tr>
<td>Physician</td>
<td>✓</td>
</tr>
<tr>
<td>Physician Assistant</td>
<td>✓</td>
</tr>
<tr>
<td>Nurse</td>
<td>✓</td>
</tr>
<tr>
<td>Registration Clerk</td>
<td>✓</td>
</tr>
<tr>
<td>Technician</td>
<td>✓ ✓</td>
</tr>
<tr>
<td>Care-giver</td>
<td>✓</td>
</tr>
</tbody>
</table>

2/14/00  CADSE/FIU
# Permission Assignment (PA) Relation

<table>
<thead>
<tr>
<th>Roles</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>PN</td>
</tr>
<tr>
<td>Psychiatrist</td>
<td></td>
</tr>
<tr>
<td>Physician</td>
<td></td>
</tr>
<tr>
<td>Physician Assistant</td>
<td></td>
</tr>
<tr>
<td>Nurse</td>
<td></td>
</tr>
<tr>
<td>Registration Clerk</td>
<td>W</td>
</tr>
<tr>
<td>Technician</td>
<td></td>
</tr>
<tr>
<td>Care-giver</td>
<td></td>
</tr>
</tbody>
</table>

2/14/00 CADSE/FIU 21
Base Architecture Model

Sample constraints (reachability):

P2 → AF P5, P7 → AF P9, P8 → AF P10, P11 → AF P9, P6 → AF P3
Composition of DC&PEs based on RBAC Policies

P13 Attributes
P14 Decisions from PE
P15 Attributes received by RBAC PE
P16 Decision made by RBAC PE
T6 DC invokes RBAC PE
T7 RBAC PE passes decision to DC
Behavior Model of Policy Evaluator

Constraints:

\[
\forall (SA, op, rsn, d) \Box P15.(SA, op, rsn) \land (res \notin RES) \rightarrow \Diamond P16.d \land (d = 'U')
\]

\[
\forall (SA, op, rsn, d) \Box P15.(SA, op, rsn) \land (res \in RES) \land (\exists rl \in SA, (rl, op, rsn) \in PA)
\rightarrow \Diamond P3.d \land (d = 'Y')
\]

\[
\forall (SA, op, rsn, d) \Box P15.(SA, op, rsn) \land (res \in RES) \land (\forall rl \in SA, (rl, op, rsn) \notin PA)
\rightarrow \Diamond P3.d \land (d = 'N')
\]
System-wide Constraint Decomposition

System-wide Constraints (access control policies) = PE Component Constraints (policies assigned to PE) .AND. DC Component Constraints (combination rules)
Compositional Analysis of Behavior Model

- Component analysis
  - each component analyzed individually against component constraints
- Composition analysis
  - composition constraints defined on multiple components verified based on composition of component analysis
- Analysis driven by satisfaction of architectural constraints.
## New Policies

<table>
<thead>
<tr>
<th>No.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2-1</td>
<td>Any <strong>care-giver</strong> can read patient’s name.</td>
</tr>
<tr>
<td>P2-2</td>
<td><strong>Registration clerk</strong> can modify patient name and demographic information.</td>
</tr>
<tr>
<td>P2-3</td>
<td><strong>Nurse</strong> can read patient’s name and demographic information.</td>
</tr>
<tr>
<td>P2-4</td>
<td><strong>Attending nurse</strong>, in addition to the rights of any other nurse, can modify current episode demographic information, can read current episode regular records and current episode regular test results.</td>
</tr>
<tr>
<td>P2-5</td>
<td><strong>Technician</strong> can read patient’s name and modify current episode regular test results.</td>
</tr>
<tr>
<td>P2-6</td>
<td><strong>Related technician</strong>, in addition to the rights of any other technician, can modify current episode sensitive test results.</td>
</tr>
<tr>
<td>P2-7</td>
<td><strong>Attending assistant physician</strong>, in addition to what a nurse can do, can also read all (i.e. from the current and previous episodes) regular records and all regular test results, as well as to modify current episode regular records.</td>
</tr>
<tr>
<td>P2-8</td>
<td><strong>Attending physician</strong>, in addition to the rights of attending assistant physician, can modify current episode sensitive regular records and can read all regular and sensitive records from previous episodes.</td>
</tr>
<tr>
<td>P2-9</td>
<td><strong>Attending psychiatrist</strong>, in addition to what an attending physician can do, also can modify mental information.</td>
</tr>
<tr>
<td>P2-10</td>
<td><strong>Patient relative</strong> can read patient’s current episode demographic and patient’s name.</td>
</tr>
<tr>
<td>P2-11</td>
<td><strong>Patient guardian</strong> can read previous episode regular data.</td>
</tr>
<tr>
<td>P2-12</td>
<td><strong>Patient spouse</strong> can read previous episode sensitive data.</td>
</tr>
<tr>
<td>P2-13</td>
<td><strong>Patient representative</strong> can read previous episode regular data provided that patient gives a consent.</td>
</tr>
</tbody>
</table>
Relationship Hierarchy

- Patient
  - Spouse
  - Guardian
  - Relative

- Attending Physician
  - Assistant Attending Physician
  - Attending Nurse
  - Related Care-giver
  - Related Technician
# Relationship to Permission Assignment Relation

<table>
<thead>
<tr>
<th>Relationships</th>
<th>PN</th>
<th>DD</th>
<th>CDD</th>
<th>CRR</th>
<th>CSR</th>
<th>CRT</th>
<th>CST</th>
<th>PRR</th>
<th>PSR</th>
<th>PRT</th>
<th>PST</th>
<th>AMD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attending Psychiatrist</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
</tr>
<tr>
<td>Attending Physician</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attending Physician Assistant</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Attending Nurse</td>
<td></td>
<td></td>
<td>RW</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Related Technician</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>RW</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Related Care-giver</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Patient</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spouse</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Guardian</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Relative</td>
<td>R</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2/14/00 CADSE/FIU 29
DC&PEs Model for Relationship-based Policies

P13  Attributes
P14  Decisions from PE’s
P15  Attributes received by RBAC PE
P16  Decision made by RBAC PE
P17  Attributes received by RelBAC PE
P18  Decision made by RelBAC PE
T6   DC invokes RBAC PE
T7   RBAC PE passes decision to DC
T8   DC invokes RelBAC PE
T9   RelBAC PE passes decision to DC
Performance Model of Policy Evaluator

(Transition $pe$ is associated with stochastic firing times.)

Constraint:

$\forall (x, y) \Box P15.x \rightarrow \Diamond P16.y \land (\text{Expectation}(y - x) \leq 10)$
The Next Steps

• Distributed AAS architecture
  – prototype of distributed and CORBA-based AAS

• Case study
  – real life policies in healthcare (HIPAA)
  – sample application(s)
  – workload and scenario simulation
  – collaborators: NIST, Las Alamos National Lab

• Aspect-oriented modeling framework for security services
  – collaborator: University of Illinois at Chicago