Context-based Access Control for Ubiquitous Service Provisioning

Antonio Corradi, Rebecca Montanari, Daniela Tibaldi
{acorradi, rmontanari, dtibaldi}@deis.unibo.it
DEIS - Department of Electronics, Computer Science and Systems
University of Bologna - Italy
• **Access Control Issues** in Ubiquitous Environments
• **UbiCOSM** Security Framework
  • Security Model
  • Access Control Middleware
• **Case Study**: Mobile Office Application
• Conclusions and Future Work
Security Issues

- Wireless network connectivity and portable devices anywhere and at anytime access from various access devices

Novel access control challenges:

- Paradigm shift from subject-centric to context-centric access control

- Un-informative identity or not trustworthy
- Traditional identity-based access control models are inadequate for Ubiquitous Environments
- Static characterization of context
- Context as a trigger for policy evaluation

Hong Kong: September 28-30, 2004
UbiCOSM Security Framework

UbiCOSM
(Ubiquitous Context-based Security Middleware)

• Permissions directly associated with contexts

• **Context** = grouping mechanism for applicable permissions

**Goal:** Immediate *controlled visibility* of accessible resources and of other mobile users locally executing

Desired Resources | Allowed Resources

---

Hong Kong: September 28-30, 2004
Access Control Policies:

Specific context conditions → specific permissions

<association_Name(context_collection), permissions>

<security:permission rdf:about="http://lia.deis.unibo.it/UbiCOSM/security#permission">
  <security:Name>P1</security:Name>
  <security:Target rdf:resource="Printer X"/>
  <security:Action>print</security:Action>
</security:permission>
Access Control Policies

\(<\text{association\_Name(context\_collection), permissions}>\)

- **Business User** → P1, P2 \(<\text{Simple(Business User), (P1, P2)}>\)
- **Waiting Room** → P3 \(<\text{Or(Waiting Room, Auditorium), (P3)}>\)
- **Business User** → P4, P5 \(<\text{And(Business User, Auditorium), (P4, P5)}>\)
- **Attendee** → P6 \(<\text{Dependence(Attendee, Business User), (P6)}>\)

Hong Kong: September 28-30, 2004
Advantages

<association_Name(context_collection), permissions>

• Easy specification/update/revocation of permissions as the system evolves
• Permissions are dynamically applied simply adding/removing user association with context
• Context activation implies immediate permission activation
UbiCOSM Architecture

Java Virtual Machine

Heterogeneous Distributed System

UbiCOSM Facilities

- Policy Manager
- Authorization Enforcement Manager
- Policy Installation Manager
- Context-Aware Security Manager

CARMEN Facilities

- Directory
- Discovery
- Interoperability
- Event
- Identification
- Communication
- Migration
- Monitoring

Hong Kong: September 28-30, 2004
OR(Program Chair, AND(Waiting Room, Business User))
Case Study

Objectives
• provide familiar office environment visibility
• enrich mobile office interacting with local resources

Network Deployment Setting
• Wireless building network composed by several 802.11 network localities
• Wireless access devices: Toshiba e740 Pocket PCs

Hong Kong: September 28-30, 2004
Case Study

Access Control Policy

<And(Auditorium, Conference in Action, Business User), P1>

<security:permission rdf:about="http://lia.deis.unibo.it/UbiCOSM/security#permission">
  <security:Name>P1</security:Name>
  <security:Type>authorization.</security:Type>
  <security:Target rdf:resource="Spider Game"/>
  <security:Action>Access</security:Action>
</security:permission>
Case Study

Physical Context

Grants/Denies

Permission View

Request

Policy Manager

Authorization Enforcement Manager

Policy Installation Manager

Context-Aware Security Manager

CARMEN Context Monitoring Service

Hash - Table Repository

Hong Kong: September 28-30, 2004
Performance overhead to compute a permission view

<table>
<thead>
<tr>
<th>L</th>
<th>t(msec)</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>0.26</td>
</tr>
<tr>
<td>20</td>
<td>0.48</td>
</tr>
<tr>
<td>30</td>
<td>0.75</td>
</tr>
<tr>
<td>40</td>
<td>0.96</td>
</tr>
<tr>
<td>50</td>
<td>1.25</td>
</tr>
<tr>
<td>60</td>
<td>1.50</td>
</tr>
<tr>
<td>70</td>
<td>1.75</td>
</tr>
<tr>
<td>80</td>
<td>1.93</td>
</tr>
<tr>
<td>90</td>
<td>2.13</td>
</tr>
<tr>
<td>100</td>
<td>2.52</td>
</tr>
</tbody>
</table>

$L$ = Number of Logical Context
Conclusions

• UbiCOSM: a context-driven access control framework
  • to apply in Ubiquitous Environments
  • to protect resource access

Future Work

• Policy conflict detection
• Integration of UbiCOSM with mechanisms for inter-cell mobility prediction to anticipate user migration
Thank You!