Semantic security framework and context-aware role-based access control ontology for Smart Spaces


Shohreh Hosseinzadeh, Natalia Díaz-Rodríguez, Seppo Virtanen, Johan Lilius

University of Turku, Finland
Åbo Akademi University, Finland
Introduction

- Smart Spaces
- Security, Privacy and Context Awareness in Smart Spaces
Contribution

Granular triple-level mechanisms for security and privacy in Smart Spaces

2. Context-aware role-based access control scheme
Smart-M3

- Smart-M3 is a functional platform that provides a cross domain search extent for triple based information. Smart-M3 enables smart cross domain applications that rely on information level interoperability.
- Multi Device, Multi Platform, Multi Part
- [https://sourceforge.net/projects/smart-m3/](https://sourceforge.net/projects/smart-m3/)
1) Security framework architecture

1. Request
2. Authentication Engine
   - Queries + credentials + requested role
3. Critical
4. Access Control Engine
   - Normal
5. Inference Engine
   - Context Information
   - Users/roles
   - Security Policies
6. Extended Query
7. RDF Repository
   - Result (accessible triples)
8. Access Log
Security aspects supported:
Authentication, Authorization and Access control

Different steps:
(1) Access request from user
(2) Authentication engine assures authenticity
(3) If positive, request forwarded to Access Control Engine
(4) Execute access control rules: check if requester has rights to perform the requested action
(5) If positive the request is forwarded to the repository and access log
(6) The access log keeps record of the recent accesses.
(7) The result (accessible triple) is retrieved from the repository
(8) The result is sent to the user
2) Context Aware Role Based Access Control (CARBAC) ontology
## Comparison of access control ontologies and their Smart Space domains

<table>
<thead>
<tr>
<th>Reference &amp; Access control model</th>
<th>Context aware</th>
<th>Rule-based</th>
<th>Domain</th>
<th>Privacy control</th>
<th>Triple level control</th>
</tr>
</thead>
<tbody>
<tr>
<td>[22] Context-based</td>
<td>✓</td>
<td>✓</td>
<td>Pervasive Computing Environments</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>[14] Privacy-centric</td>
<td>X</td>
<td>✓</td>
<td>Heterogeneous administrative medical domains</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>OWL-S Services[1] Ontology-based</td>
<td>X</td>
<td>✓</td>
<td>Semantic Web services</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>[20] OPO Access Control List (ACL)</td>
<td>X</td>
<td>✓</td>
<td>Linked Data</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>[16] User Behavior and Capability Based Control Access</td>
<td>✓</td>
<td>✓</td>
<td>Smart Spaces</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>[19] SitBAC</td>
<td>✓</td>
<td>✓</td>
<td>Smart Spaces</td>
<td>✓</td>
<td>X</td>
</tr>
<tr>
<td>[23] Proteus, Context-centric</td>
<td>✓</td>
<td>✓</td>
<td>Pervasive Environments</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>[10] ROWLBACK</td>
<td>X</td>
<td>✓</td>
<td>Dynamic Environments</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>This work: CARBAC</td>
<td>✓</td>
<td>✓</td>
<td>Health and well-being SS</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Access Control Policies

- Expressed via rules
- At run-time, rules are executed, and decisions made on permission/prohibition of performing an action.
- For writing the access control rules, we used C Language Integrated Production System (CLIPS) v6.24
- 2 kinds of Access Control rules, defined by:
  a) Admin
  b) User for privacy protection purposes.
Example 1: Rules defined by the admin

(triple (Jack, hasRole, Doctor))
(triple (Maria, hasRole, Patient))
(triple (Maria, hasMedicalHistory, ?h)))

→

(assert (triple (Jack, roleHasReadPermissionOverData, ?h)))
(assert (triple (Jack, roleHasWritePermissionOverData, ?h)))
(assert (triple (Jack, roleHasUpdatePermissionOverData, ?h)))
(assert (triple (Jack, roleHasDeletePermissionOverData, ?h)))
Example 2: Rules defined by the user (highest priority)

(assert (triple (Jack, userHasReadPermissionOverData, ?h)))
(assert (triple (Jack, userHasUpdatePermissionOverData, ?h)))
(assert (triple (Jack, userHasDeletePermissionOverData, ?h)))
(assert (triple (Jack, userHasWritePermissionOverData, ?h)))
(assert (triple (Jack, userHasUpdateProhibitionOverData, ?h)))
(assert (triple (Jack, userHasDeleteProhibitionOverData, ?h)))
(assert (triple (Jack, userHasWriteProhibitionOverData, ?h)))

=>

(assert (triple (Jack, roleHasReadPermissionOverData, ?h)))
Example 3: Context aware access control rules

Doctor: restricted to only read the medical history of the patients outside the hospital, but cannot update/delete/write:

(triple (Jack, hasRole, Doctor))
(triple (Maria, hasRole, Patient))
(triple (Maria, hasMedicalHistory, ?h)))
(triple (LocationJack, hasValue, TrainStation))

(\rightarrow)

(assert (triple (Jack, roleHasReadPermissionOverData, ?h)))
(assert (triple (Jack, roleHasWriteProhibitionOverData, ?h)))
(assert (triple (Jack, roleHasUpdateProhibitionOverData, ?h)))
(assert (triple (Jack, roleHasDeleteProhibitionOverData, ?h)))
Avg exec. time for access control requests to the semantic information broker (M3 SIB)

Smart Space Application Protocol (SSAP) operations:
- Read
- Write
- Delete
- Update a triple
Conclusion

We proposed

- Flexible security framework
  - fine and coarse grained information level
  - Smart Space security and privacy ontology available: \( \text{https://github.com/NataliaDiaz/AccessControlOntology} \)
- Access control scheme for Smart-M3 based spaces
  - \( \text{http://sourceforge.net/projects-smart-m3/} \)
Future Work

- Security alert implementation with M3 pub/sub mechanism,
- Large scale deployment
- Micro-managing of personal data
- Data as a currency
- Integration into wearable camera & Egoshots dataset [https://github.com/NataliaDiaz/Egoshots](https://github.com/NataliaDiaz/Egoshots)
Thank you for your attention!

Shohreh Hosseinzadeh
shohos@utu.fi  University of Turku, Finland

Natalia Díaz-Rodríguez
ndiaz@decsai.ugr.es
https://about.me/NataliaDiazRodriguez

University of Granada, Spain and Åbo Akademi University, Finland
(currently data scientist intern at Stitch Fix)
References