A Group-Centric Model for Collaboration with Expedient Insiders in Multilevel Systems

Khalid Zaman Bijon, Ravi Sandhu, Ram Krishnan
Institute for Cyber Security
University of Texas at San Antonio

May 22, 2012
International Symposium on Security in Collaboration Technologies and Systems

World-Leading Research with Real-World Impact!
Who are expedient insiders?
- Any outside Collaborators, i.e. Domain specialists, cyber-security experts, etc.

Difference with respect to true insiders
- Transient rather than persistent
- Information sharing is based on need-to-consult basis
- Less commitment than long time employees

What are the Challenges?
1. Information selection for collaboration
2. Restrict unnecessary access
3. Import results
Collaboration Process #1

- Assign to a place in existing organizational structure

Top Secret

Secret

Classified

Unclassified

Outside Collaborators

Sharing more information than necessary
Open to more true-insiders than necessary

World-Leading Research with Real-World Impact!
Collaboration Process #2

- Individual Sharing Collaboration

Scalability is the main Issue!

World-Leading Research with Real-World Impact!
Group Centric Collaboration

Organization

Collaboration Group with Expedition Insider

Outside Collaborators

Just Right Sharing Scalable

World-Leading Research with Real-World Impact!
Group Centric Collab. (cont.)

Operational aspect

• User-Subject Model
  • User: human in the system
  • Subject: Programs/processes on behalf of user

• Subject Model
  • Read-Only Subject (can not write object but read from multiple groups)
  • Read-Write Subject (can write but limited read capability)

Administrative aspect

• Membership Management
  • True Insider: Regular employee
  • Expedient Insider: Collaborators, Consultants

• Object-Version Model
  • write creates a new version
  • Security classification of versions (same?)

• Group Lifecycle
  • Objects Management
  • Lattice Structure
  • G-SIS specification
## True Insiders Vs Expedient Insiders

<table>
<thead>
<tr>
<th>True Insiders</th>
<th>Expedient Insiders</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Simultaneously hold membership in multiple groups and organization</td>
<td>1. Can get membership to multiple groups but not in organization</td>
</tr>
<tr>
<td>2. Retain the same organization clearance when joining a new group</td>
<td>2. Assigned a single clearance for every group they join</td>
</tr>
<tr>
<td>3. Can access all objects that</td>
<td>3. Can access all objects that</td>
</tr>
<tr>
<td>- Satisfy dominance relation</td>
<td>- Satisfy dominance relation</td>
</tr>
<tr>
<td>- in organization or joined groups</td>
<td>- in joined groups only</td>
</tr>
</tbody>
</table>
Operational Semantics

Administrative Model

Operational Model

Organization

Collaboration Group

Outside Consultants

World-Leading Research with Real-World Impact!
## Read-Only Vs Read-Write Subject

<table>
<thead>
<tr>
<th>Read Only</th>
<th>Read Write</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Can not write, read is restricted by BLP simple security property</td>
<td>1. Can read and write, however, write is restricted by BLP strict * property</td>
</tr>
<tr>
<td>2. User determines the security clearance (&lt;= user’s clearance)</td>
<td></td>
</tr>
<tr>
<td>3. Can read objects across groups</td>
<td>3. restricted within the same group it was created</td>
</tr>
<tr>
<td>4. Can not create new object</td>
<td>4. Can create new object and object inherits its clearance</td>
</tr>
<tr>
<td>5. Read operation does not create new object versions</td>
<td>5. Only a write operation always create a new version of the respective object, however, does not change the classification of the version</td>
</tr>
</tbody>
</table>

*Real-World Impact!*
## Merge Vs Import Operation

<table>
<thead>
<tr>
<th></th>
<th>Merge</th>
<th>Import</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Can applicable only to previously added version</td>
<td>1. Only to the newly created versions</td>
<td></td>
</tr>
<tr>
<td>2. Does not create new objects</td>
<td>2. Always creates a new object</td>
<td></td>
</tr>
<tr>
<td>3. Does not change the object classification</td>
<td>3. New object inherits classification from importing one</td>
<td></td>
</tr>
</tbody>
</table>

**Organization**

- **New object**

**World-Leading Research with Real-World Impact!**
### Attribute Specification

**Global Sets and Symbols:**
- SL: Finite lattice of security levels with dominance ordering $\succeq$
- CG: Finite set of existing groups
- U: Finite set of existing users
- O: Finite set of existing objects
- S: Finite set of existing subjects
- UNIV$_V$: The universal set of versions (an infinite set)
- Org: The organization (a constant symbol)

**User Attributes:** $\text{Att}(U) = \{\text{clearance, ug, orgadmin, cgadmin, utype}\}$
- clearance: $U \rightarrow SL$
- ug: $U \rightarrow 2^{CG}$
- orgadmin: $U \rightarrow \{\text{True, False}\}$
- cgadmin: $U \rightarrow 2^{CG}$
- utype: $U \rightarrow \{\text{Insider, Expedient_Insider, null}\}$

**Objects Attributes:** $\text{Att}(O) = \{\text{classification, origin, versions}\}$
- classification: $O \rightarrow SL$
- origin: $O \rightarrow CG \cup \{\text{Org}\}$
- versions : $O \rightarrow 2^{\text{UNIV}_V}$

**Subject Attributes:** $\text{Att}(S) = \{\text{clearance, owner, belongsTo, type}\}$
- clearance : $S \rightarrow SL$
- owner: $S \rightarrow U$
- belongsTo: $S \rightarrow CG \cup \{\text{Org}\}$
- type: $S \rightarrow \{\text{RW,RO}\}$

**Object Version Attribute:** $\text{Att}(O, V) = \{\text{vMember, classification}\}$
- vMember : $O \times \text{UNIV}_V \rightarrow 2^{CG \cup \{\text{Org}\}}$
- classification: $O \times \text{UNIV}_V \rightarrow SL$

/* These are partial function defined only for the versions that exist for each object*/
Possible Enhancement

- Join Insider operation could modify clearance
  - A manager of the organization could be a group director, etc.

- Add object operation could modify classification
  - A secret object might get top secret classification in collaboration group

- Add object could sanitize information
  - Organization might not want to share actual object
Conclusion & Future Work

A novel method to manage expedient-insider collaboration in multi level systems

Advantage of Group Centric Collaboration Model

- Selective information sharing
- Controlled flow back of results
- Does not interfere with the main lattice structure
- Easier to manage collaborations

Future Work

- Collaboration group with multiple organizations, expedient insiders, etc.
  - Merging different organization’s structures

World-Leading Research with Real-World Impact!
Thank You 😊