**Identifying Less-stringent, Appropriate Confidentiality Levels for Information Systems Data**

PI: Robyn Lutz, rlutz@iastate.edu
Researcher: Jingwei Yang, jwyang@iastate.edu
Dept. of Computer Science, Iowa State University
Mentor: Dan Hasty, John Deere and Nick Multari, Boeing

---

**I. MOTIVATING EXAMPLE**

- “New user” refers to a user under a new contextual condition, which has not been considered and specified in the original confidentiality requirements.
- Example confidentiality requirement: Development resources of project A shall be accessible only to its owner developers.
- Possible new user: A developer from a new project B wants to reuse previous development work in project A, but cannot access the resources.

**II. PROBLEM**

- Although requirements specification should not include considerations for design, in practice, confidentiality requirements are usually specified with regards to available access control mechanisms.
- Limitations in adopted access control mechanisms are brought into confidentiality requirements. Sometimes, a simple binary access control design cannot fully describe the complex nature of the data access scenario.
- Extra cost on management and maintenance, due to imprecise confidentiality requirements specification.

**III. SOLUTION**

1. Identifying uncertainty factors:
   - Time, location, and other contextual factors.
2. Modeling uncertainties:
   - Use Fuzzy Multi-Level Security (Fuzzy MLS) Model (J. Clark et al., 2010)
3. Specifying confidentiality requirements:
   - Define new requirements relaxation alternatives.

**IV. CASE STUDY**

- A developer’s story: John is a project manager in company A. His team is using a collaborative development environment on their current project α. In several occasions, John found that they were not able to get access to their development resources.

1) Mason, a developer from company B, who is their collaborative partner, came to John’s group for on-site development work. However, he was not recognized as a member of the group by the system, and could not get access to development resources.

2) John was not able to read a new requirements document when he was at the local airport.

3) On several components, they decided to reuse the previous design of project β developed by another group, but they were not able to, because none of them are the original developers.

- What causes these problems? The development environment was not properly designed; especially its original confidentiality requirements were specified too stringently.
- By using our relaxation operators, we can better specify those requirements:

1) When the estimated risk of disclosing resources to user X (Mason) ≤ threshold, access shall be granted.
2) AT the local airport, the clearance of a project manager shall be lowered only to level 4 (which is still higher than the clearance of requirements specification documents).
3) Resources of project β shall be visible to other project manager AFTER a decade.

**V. BENEFITS**

<table>
<thead>
<tr>
<th>Specifying</th>
<th>More Flexible Requirements Operators</th>
<th>More Precise Confidentiality Requirements</th>
<th>Better Balance between Confidentiality and Availability</th>
<th>Lower Management &amp; Maintenance Cost</th>
</tr>
</thead>
</table>