Privacy-Respecting Access Control (PRAC) in Collaborative Workspaces
Roadmap of Talk

- The “Privacy vs. Sociability” Dilemma
- Status Quo of Access Control Approaches to (Personal) Data
- Concept of Privacy-Respecting Access Control (PRAC) for Collaborative Workspaces (CWs)
- Example demonstration
The “Privacy vs. Sociability” Dilemma

Functional Triangle of Social software [PP09] based on [RK07]
The “Privacy vs. Sociability” Dilemma

- Sharing of (personal) information
  - advancing social lives of users
  - putting their privacy at risk

- Solution required that combines benefits from socializing Internet and privacy control

- Collaborative Workspaces (CWs):
  - Infrastructures enabling people to work together
  - Content is the focal point
Status Quo of Access Control Approaches

- Access control matrix, role-based access control, team/group-based access control

Problems:
- Administrative parties specifying access control rules → no user control
- Identity-based definition of access control → knowledge of particular users necessary → no user-controlled protection of the user’s privacy possible
Privacy Issues related to CWs

- Limited awareness of privacy issues
- Limited possibilities to determine access rules
- Social engineerung attacks (false identity)
- Surveillance of users
Prerequisites of PRAC

- No administrative party specifying access rules
- Potential interaction partners are not necessarily known by the contributor
- Other user may protect their privacy as well
- Access control has to be applicable to also fine-grained content structures
Idea of PRAC

- Unbinding the access control process from identities →
  - *Access Control Policies* specified by the user herself
  - *Certified Attributes*
  - Anonymous and unlinkable presentation

- Based on PRIME technologies

- Adaptation for collaborative scenarios
Example Scenario

Bob
Fitness Centre XYZ

Alice
Collaborative Platform

Hannes

Cred: OwnerThread
OR
Cred: OwnerContribution
OR
Cred: FriendOfBob
OR
Cred: MemberOfFitnessCentreXYZ

“Owner Contribution”

“FriendOfBob”

“MemberOfFitnessCentreXYZ”
Research Questions to be Addressed

- Selective Access Control
  - Technical feasibility of offering both approaches
  - Compromise between privacy and (social) interaction
  - Different user groups: e.g., concern, expertise etc.
  - AC based on certified properties vs. identities

- Privacy Awareness
  - Influence of provision of privacy awareness information on
    - kind of communication
    - kind of access control settings by the users
Realisation of a Demonstrator
Edit policy

[ Moderator Control Panel ]

**Fit For Summer**

*By Bob > Wed Aug 19, 2009 9:57 am*

Hey guys,

let’s talk about our sports activities here.

Bob

Privacy-Respecting Access Control in Collaborative Workspaces
Backup: Example (Edit Policy)
Backup: Example (Attribute Credential) 3|4
Backup: Example (Access Denied)
Privacy Issues related to CWs – Solved?

- Limited awareness of privacy issues
  - Comprehensive tools communicating awareness information
- Limited possibilities to determine access rules
  - In full user control → however: more user support necessary
- Social engineering attacks (false identity)
  - As long as we do not have any secured proof of identity → problem is not solved
- Surveillance of users
  - Improvement in terms of privacy
Thank you for your attention!
Backup: Content hierarchy of demonstrator
Backup: Example of ACP

1. **Forum:** [(cred:Admin-Forum) OR (everybody[default])] AND

2. **Topic:** [(cred:Moderator-SportsAndCars) OR (everybody[default])] AND

3. **Thread:** [(cred:Moderator-SportsAndCars) OR (cred:Owner-FitForSummer) OR (cred:Male)] AND

4. **Post:** [(cred:Moderator-SportsAndCars) OR (cred:Owner-PostFromHannes) OR (cred:memberOfFitnessCentreXYZ)]
How to specify credentials to be used within ACPs?

1. Globally defined set of credentials
   - Efforts comparable with knowing all user names
   - However: improvement in terms of privacy

2. Generally accepted standard for defining credentials
   - More complex approach
   - However: more flexibility for definitions of credentials and for specifying ACPs

→ Interesting research question
Backup : Collaborative Workspaces

- Platforms for collaborative and cooperative working
  - Sharing information
  - Jointly creating content
  - Developing ideas
  → Content

- In comparison: Social Network Sites
  - Provision of means to establish user profiles and connections between people
  → Identity
## Backup: Access Control Matrix

<table>
<thead>
<tr>
<th></th>
<th>File 1</th>
<th>File 2</th>
<th>File 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>User 1</td>
<td>r/w/x</td>
<td>r/ w</td>
<td>r</td>
</tr>
<tr>
<td>User 2</td>
<td>r</td>
<td>r/w/x</td>
<td>-</td>
</tr>
<tr>
<td>User 3</td>
<td>-</td>
<td>-</td>
<td>r/w/x</td>
</tr>
</tbody>
</table>

### Legend:
- **Capability List (CL)**
- **Access Control List (ACL)**