Data Sharing in Social Networks

Clara Bertolissi, Alba Martinez Anton, Nicola Zannone

SACMAT’23, June 7-9, Trento, Italy
Privacy of multi-user shared content

What options has Bob to protect his privacy?

- Ask Alice to modify the visibility of her photo
- Delete the tag
- If the solution is not satisfying, report to the social network

A photo posted by Alice of her party
Social networks challenges

Multi-party content
A piece of data has several co-owners.

Sharing and resharing content
The data can be “replicated”.

Compounds objects
Some data cannot exist without other piece of data.
Idea: compound objects with multiple controllers
Objective and contributions

▶ **Objective:**
Propose a fine-grained access control model for multi-user system

▶ **Contribution:**
Extend attribute-based access control with provenance information

Specifications  Evaluation  Validation
The Open provenance Model

- upload
  - wasGeneratedBy (photo)
  - wasControlledBy (owner)

- photo p1
  - wasDerivedFrom (photo)
  - used (photo)
  - wasControlledBy (owner)

- tag
  - wasGeneratedBy (tag)
  - wasControlledBy (id_involved)

- Alice

- Bob

- Charlie
Extension for Social Networks

- New dependencies
- Relations between users
- Dynamic systems.

Evaluation graph

SACMAT'23, June 7-9, Trento, Italy - Data Sharing in Social Networks
Policy definition: ABAC extended with path conditions

- **User policies**
  - Give the user preferences

\[
p_{\text{photo,Alice}} = (\text{owner} \lor \text{host} = \text{Alice}, \text{type} = \text{photo}) \land \text{action} = \text{view} \lor \text{areRelated}^2(\text{Alice}, \text{user}_{id}, \text{friend}), 1
\]

\[
p_{\text{tag,Bob}} = (\text{resource}_{target} = \text{Bob}, \text{type} = \text{photo} \lor \text{tag}), \text{action} = \text{view} \land \text{areRelated}(\text{Bob}, \text{user}_{id}, \text{friend}), 1
\]

- **System policies**
  - Give the way that preferences have to be combined for evaluate an access

\[
p_{\text{photo,SN}} = (\text{type} = \text{photo}), \text{action} = \text{view}, p_{\text{photo,host}}
\]

\[
p_{\text{photo,SN}} = (\text{type} = \text{photo}), \text{action} = \text{view}, \text{dov}(p_{\text{photo,owner}}, p_{\text{photo,host}}, \text{dov}(\text{uri}(x, y)) \land \text{contributedTo}(y, x, \text{tag}_{target}))
\]
Charlie wants to see Alice’s photo

\[ q = \{(\text{user_id},\text{Charlie}), (\text{resource_id}, p1), (\text{action}, \text{view})\} \]

Algorithm Steps:
- Evaluation of the system policy
- Search of the sub-objects in the provenance information and their controllers
- Evaluation of the access to the sub-objects
- Return the list of the available objects

The algorithm returns: \([[p1, \text{permit}], [p1t1, \text{deny}]]\)
Algorithm to evaluate requests

**INPUT**
Query / Set of policies

- Evaluate query against the set of policies
  - Permit

  - Yes: Add object to the visibility list
  - No: Evaluate sub-query with the set of policies

  - Evaluate sub-query with the set of policies
    - Yes: Add sub-object to the visibility list
    - No: Search for sub-objects in the Provenance graph

- Search for sub-objects in the Provenance graph
  - Yes: Sub-objects
  - No: Permit

- Permit
  - Yes: Add sub-object to the visibility list
  - No: Action view

- Action view
  - Yes: Permit
  - No: OUTPUT Visibility list

**OUTPUT**
Visibility list
Prototype architecture
Prototype: Some Results

- Limited impact of the number of post and photos
- Important impact of the number of sub-objects

... but in real life ...

- Number of sub-objects often limited, or displayed bit by bit

SACMAT’23, June 7-9, Trento, Italy - Data Sharing in Social Networks
Conclusion & Future work

✓ Fine-grained access control for sharing data in OSN
✓ Integration into an XACML architecture
✓ Extension for transient relationship
✓ Conflict resolution and management