Authorization in Object-oriented Databases

Anna Vapen
David Hall
December 2008

Authorization

• “the permission or power given to sb to do sth: enter a security area without authorization”
  Oxford Advanced Learner’s Dictionary

• authorization is the concept of allowing access to resources only to those permitted to use them.

Authorization

Real world example

Roles: Manager, researcher, PR person, employee

Manager
Can read/write any document
PR
Can read/write public PR material and non-public PR material (work in progress)
Employee
Can only read public PR material
Researcher
Can read public PR-material and read/write research material

Real world example

Documents
Strategic documents
PR
Secret
Research
PR material
Public PR material
Employee
Future ads

Authorization model in relational DBs

• Coarse-grained
• Units of authorization:
  – Relation (record)
  – Attribute (field)

Object orientation

• Classes (composite*)
• Objects
• Inheritance
• Versions

* leads to class-composition hierarchy
**Objects**

- Unique id.
- State (values of attributes)
- Behavior (methods)
- Instance of a class (may be a primitive)

**Class-composition**

- Car
  - Wheel
    - Rim
    - Tire

**Inheritance**

- Class hierarchy (single inheritance)
- Class lattice (multiple inheritance)

**Methods**

- Authorize users to call methods within a class.
- Also must check any operations performed by the method (e.g. reading/writing attribute values)

**Instances**

- Want to read all instances of a class except one or a few?

- Employees shouldn’t be able to see future ads.

**Database granularity hierarchy**

Rabitti, F., Bertino, E., Kim, W., Woelk, D. 1991
Basic authorization concepts

- \((s,o,a) \in S \times O \times A\)
- \(F: S \times O \times A \to \{\text{True, false}\}\)
- Subject (an user or group of users)
- Authorization object (single object, group of objects, entire database)
- Authorization type (read, update, create, ...)

Implicit authorization

- Rabitti, Woelk, Kim 1988
- Rabitti, Bertino, Woelk, Kim 1991
- Explicit setting \(<s,o,a>\) triplets
- The rest of \(<s,o,a>\) combinations are implicitly defined
Weak authorization
Rabitti, F., Bertino, E., Kim, W., Woelk, D. 1991

Strong authorization
Rabitti, F., Bertino, E., Kim, W., Woelk, D. 1991

Positive/negative authorization
Rabitti, F., Bertino, E., Kim, W., Woelk, D. 1991

Implicit authorization
- Pros:
  - No need to store all combinations
  - No need to set all combinations
- Cons:
  - Sometimes hard to grasp why a specific authorization is determined as it is
  - Conflicts
  - Computational overhead

Applied real world example
Manager: Can read/write any document

Researcher: Can read public PR-material and read/write research material
Applied real world example

PR person: Can read/write public PR material and non-public PR material

Employee: Can only read public PR material

Alternatives

- Access policies implemented by methods
  - Guard functions and proxy functions
  - Method implementor and method principal
- Media access control (MAC)
  - Single-level models
  - Multilevel models

Discuss

Questions:
- What problem are they trying to solve?
- What solution do they suggest?
- What are the limitations of this solution?

Papers:

Rabitti, F., Bertino, E., Kim, W., Woelk, D. 1991 Object lattice for versions of objects

Versions
**Exercise scenario**

In this scenario there is a **bank** where there are **employees** and a **manager**. The bank has several **customers** that have one or several **accounts** each. There are two types of accounts: **savings accounts** and **fund accounts**. A savings account can be either a **salary account** or a **long-time savings account**, while a fund account can be **equity fund account** or a **fixed-income fund account**.

**Exercise scenario**

Every sub-type of account has an **interest** that can only be changed by the manager. Customers can **withdraw money** from their salary account and see their **account balance** on any of their accounts.

**Exercise scenario**

The employees at the bank can see the account balance of the customers and they can also **open** and **close** accounts, but opening and closing of accounts (together with viewing of the balance done by the employees on other accounts than their own) can only be done between 9 and 15 Monday to Friday.

**Exercise tasks**

1. Draw a graph that shows the different account types, their variables and methods. Show the access rights for a manager, an employee and a customer by marking explicit / implicit, weak / strong and positive / negative authorization in the graph.
2. Draw a role lattice showing shared and non-shared rights of managers, employees and customers.