Database Security: Research and Practice

Elisa Bertino, Sushil Jajodia and Pierangela Samarati

Presented By: Mike Wood

Outline
- Motivation
- Access Control
- Multilevel Relational Data Model
- Concurrency and Object Oriented issues
- Conclusions

Why not just a firewall?
- Not immune to penetration
- Insider attacks
- Defense-In-Depth - a security design principle

Protection System Components
- Authentication
  - confirm user identity
- Access Control
  - Protect resources based on user identity
- Encryption
  - Communication and data privacy / integrity
- All non-trivial, but focus on AC

Outline
- Motivation
- Access Control
- Multilevel Relational Data Model
- Concurrency and Object Oriented issues
- Conclusions

Access Control
- Subjects == users
- Objects == resources
  - Files, tables, subjects
  - AC governs a subject's access to objects
Discretionary Access Control
- Users grant authorizations to other users for access to objects
  - Centralized
  - Ownership based
  - Decentralized
- Key advantage: flexibility
- Key disadvantage: flexibility

DAC extensions
- Groups - similar to roles
- Non cascading revoke
- Negative authorizations
- Enriched semantics for auth. override
  - Strong overrides weak
  - Specific weak overrides general weak

Mandatory Access Control
- Ordered classes
  - Top Secret > Secret > Confidential …
- Subjects and objects assigned a class
- No read-up
  - Subject can only read objects of the same or lower class
- No write-down
  - Subject can only write objects of the same or higher class

MAC - categories
- Example categories = { Ace, Bar }

Group discussion
1. As explained in the paper access classes can be associated to:
   - a relation as a whole
   - individual tuples
   - individual attributes
   - individual elements(attribute values )
   - If you were to choose what kind of association would you choose and what are some of the factors that will influence your choice?

Outline
- Motivation
- Access Control
- Multilevel Relational Data Model
- Concurrency and Object Oriented issues
- Conclusions
Multilevel Relational Model
- Idea: use MAC for AC on data
  - Attribute and tuple granularity
- Assign a class to the tuple and each attribute in the tuple

Multilevel Relation Example

<table>
<thead>
<tr>
<th>Name</th>
<th>C_Name</th>
<th>Department</th>
<th>C_Department</th>
<th>Salary</th>
<th>C_Salary</th>
<th>TC</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bob</td>
<td>Low</td>
<td>Dept1</td>
<td>Low</td>
<td>10K</td>
<td>Low</td>
<td>Low</td>
</tr>
<tr>
<td>Ann</td>
<td>High</td>
<td>Dept2</td>
<td>High</td>
<td>20K</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Sam</td>
<td>Low</td>
<td>Dept1</td>
<td>Low</td>
<td>15K</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>

Attribute Classifications
- Tuple Classification

Multilevel Relation Constraints
- No access to a value: appear as NULL
- Entity integrity
  - Attributes for PK must be uniformly classified
  - Non-key attribute classification must dominate key attribute classification

Polyinstantiation
- Problem: tuples with same key data, but different classifications
- Solution: keep multiple instances

Invisible Polyinstantiation
- Low inserts a tuple
- Avoids signaling channels
  - High blocks Low
- Avoids integrity issue
  - Low deletes High

Visible Polyinstantiation
- High inserts a tuple
  - Visible b/c High can read Low tuples
- Avoids denial of service
  - Low blocks High
- Avoids signaling channel
  - High deletes Low
Group Discussion

2. The assignments of access classes to attributes values introduces the notion of multilevel relations. The question is
   - Why would people want multilevel relations or polyinstantiations?
   - Can you name a scenario in which they would work particularly well or poorly?

Concurrency Issues

- Signaling channels with co-operative transactions
  - High transaction modulates abort of Low transaction
  - delay time = signal

Discussion

Although lots of work in security is done we all have witnessed how vulnerable the databases and especially web-databases are to malicious attackers. (example recently hackers accessing over 8 million credit card numbers)

- Why is that happening?
- Is it because the database systems are not secure enough,
- Is it because the people administrating db are not capable enough to implement security practices.
- or is it because of a lack of collaboration between different parts in the process.

Discussion

The paper introduced different and quite sophisticated authorization models (negative authorization, temporal authorization, or authorization with exceptions).

- My question is how feasible is to implement such models in the industry? What are some techniques that might help to reduce the cost of those algorithms?

Object Oriented Issues

- As discussed, OODB is dead, so who cares…
Outline

- Motivation
- Access Control
- Multilevel Relational Data Model
- Concurrency and Object Oriented issues
- Conclusions

Conclusions & Future Work

- No real wrap up
- Future work
  - Temporal constraints
  - RBAC and Separation of Duty
  - Derived authorizations
  - Administration and audit tools