Correctness Criteria of Database Fine-Grained Access Control

Elisa Bertino, Ninghui Li and Ting Yu

NSF Grant IIS-0430166

Problem

Fine-grained access control (FGAC) is increasingly needed by complex enterprise security and privacy policies. However, there currently exists no formal notion of correctness regarding query answering when fine-grained access control is enforced.

Approach

We propose and formally define three correctness criteria for fine-grained access control in relational databases.

We design efficient and correct query answering algorithms through both query rewriting and the modification of DBMS query engine.

- **Sound:** **query result consistent with that when no FGAC enforced**
- **Secure:** **no leak of information not allowed by FGAC policy**
- **Maximum:** **return as much information as possible whenever it is sound and secure**

Approach and Impact

New approach	Research Impact
• Correctness criteria for enforcing FGAC	• Theoretical foundation to evaluate FGAC enforcing techniques
• Sound and secure enforcement algorithm for cell-level access control	• Demonstrate the feasibility of correct and practical FGAC enforcement

Technical Description

Abstractly, an query answering algorithm *A* takes a database *D*, a policy *P*, and a query *Q*, and outputs a result *R*=*A*(*D*,*P*,*Q*). If an algorithm is secure, the a user cannot acquire information not allowed by *P*. We show that the notation of security we propose also applies to the situation where users may collude and issue multiple queries. We consider cell-level disclosure policy where each cell is marked as either accessible or inaccessible, and define new relation operators, namely, aggressive and conservative minus, to bound the information that is both secure and sound, given *D*, *P* and *Q*.

Q1 = select name, phone from Customer
Q2 = select name, phone from Customer
where age >=25
Q = Q1 – Q2

ID	name	age	phone
C001	Linda	32	111-1111
C002	Mary	29	222-2222
C003	Nick	v_1	v_2
C004	Jack	21	444-4444
C005	Mary	30	v_3

(a) Masked version of Customer

name	phone
Linda	111-1111
Mary	222-2222
Nick	v_2
Jack	444-4444
Mary	v_3

(b) Result of Q_{1-}

name	phone
Linda	111-1111
Mary	222-2222
Nick	v_2
Mary	v_3

(c) Result of Q_2^-

name	phone
Jack	444-4444

(d) $Q_- = Q_1 -_a Q_2$