# **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.

•Sound: query result consistent with that when no FGAC enforced

•Secure: no leak of information not allowed by FGAC policy

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

•Maximum: return as much information as possible whenever it is sound and secure

#### **Approach and Impact**

New approach

- Correctness criteria for enforcing FGAC
- Sound and secure enforcement algorithm for cell-level access control

**Research Impact** 

- Theoretical foundation to evaluate FGAC enforcing techniques
- 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

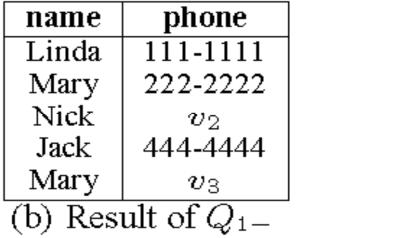
- Q1 = select name, phone from Customer
- Q2 = select name, phone from Customer where age >=25

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*.

$$Q = Q1 - Q2$$

D	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	$v_2$	
Mary	$v_{ m 3}$	
(c) Result of $Q_2^-$		

name
 phone

 Jack
 444-4444

 (d) 
$$Q_{-} = Q_1 - a Q_2$$



NSF Cyber Trust Principal Investigators Meeting March 16-18, 2008 New Haven, CT

