NC STATE UNIVERSITY Computer Science

CSC 405
Introduction to Computer Security

Topic 6. Database Security

Agenda

- Discretionary access control in DBMS
- Mandatory access control and multi-level databases
- Database inference control

NC STATE UNIVERSITY Computer Science

Topic 6.1 DAC in DBMS

Outline

- Relational model
- Grant and revoke
- Extension to the basic model
- Questions/comments in reviews

Basic Relational Concepts

- Data is organized as a collection of tables, called RELATIONS
  - Example: two relations - EMP, DEPT
  - EMP: name, title, department
  - DEPT: department, location
- Each row (or record) of a relation is called a TUPLE
- Each relation has a unique name
- Each attribute has a unique name within a relation
- All values in a relation are atomic (indecomposable)
  - As a consequence , we have two tuples for a user

Examples

EMP	Name	Title	Dept
	Tom	Prof	ECE
	Tom	Prof	CS
	Adams	Prof	ECE
	Smith	Inst	CS

DEPT	Name	Location
	CS	Wither Hall
	ECE	Daniels Hall
	Math	Harrelson Hall

Relation Schemes

- A relational database consists of 2 relation schemes:
- EMP(Name, Title, Dept)
- DEPT(Name, Location)
- Schemes: structure of the database
- Structured Query Language (SQL)
- SQL "data definition" statements are used to create relations

```
CREATE TABLE EMP
    (Name CHAR(15) NOT NULL,
    Title CHAR(4),
    Dept CHAR(10),
    PRIMARY KEY (Name))
```

```
CREATE TABLE DEPT
    (Name CHAR(10) NOT NULL,
    Location CHAR (15),
    PRIMARY KEY (Name))
```

SQL

- The SELECT statement

```
SELECT   Name
FROM     EMP
WHERE    Dept = `ECE'
```

Tom
Adams

- Joins

```
SELECT   *
FROM     EMP, DEPT
WHERE    EMP.Dept= DEPT.Name
AND      Dept.Location = `Wither Hall'
```

Tom	Prof	CS	Wither Hall
Smith	Inst	CS	Wither Hall

Views

```
CREATE VIEW EMP_LOCATION
    AS SELECT   Name, Dept, Location
    FROM        EMP, DEPT
    WHERE       EMP.Dept  = DEPT.Name
```

EMP_LOCATION

Name	Dept	Location
Tom	ECE	Daniels Hall
Tom	CS	Wither Hall
Abrams	ECE	Daniels Bldg
Smith	CS	Wither Hall

- Views are "virtual" relations. They can be used to customize relations and to provide security

Discretionary Access Controls

- Decentralized administration
  - Users can protect what they own
  - The owner may grant access to others
  - The owner may define the type of access (read/write/execute) given to others

Access Control Mechanisms

- Identification and Authentication (I&A)
- Security through Views
- Stored Procedures
- Grant and Revoke
- Query Modification

Identification and Authentication

- Identification provided by DBMS can be distinct from that provided by the underlying OS
  - Example: MS SQL server
    - Two options
      - I&A through the OS
      - Separate I&A

Security Through Views

EMP

NAME	DEPT	SALARY	MANAGER
Smith	Toy	10,000	Jones
Jones	Toy	15,000	Baker
Baker	Admin	40,000	Harding
Adams	Candy	20,000	Harding
Harding	Admin	50,000	None

Users are allowed to access partial information (such as the Toy dept data), but not the detailed information.

Example

```
CREATE VIEW TOY_DEPT
  AS  SELECT  NAME, SALARY, MANAGER
  FROM       EMP
  WHERE      DEPT = 'Toy'
```

TOY_DEPT

NAME	SALARY	MANAGER
Smith	10,000	Jones
Jones	15,000	Baker

Example

```
CREATE VIEW  TOY_EMP_MGR
  AS  SELECT  EMP,  MANAGER
  FROM       EMP
  WHERE      DEPT = 'Toy'
```

TOY_EMP_MGR

NAME	MANAGER
Smith	Jones
Jones	Baker

Example

```
CREATE VIEW AVSAL(DEPT, AVG)
   AS  SELECT  DEPT, AVG(SALARY)
   FROM        EMP
   GROUP BY  DEPT
```

AVSAL

DEPT	AVG
TOY	12,500
CANDY	20,000
ADMIN	45,000

Stored Procedures

- Right to execute compiled programs
- GRANT RUN ON program_A TO ADAMS
- Suppose program_A needs to access the relation EMP. Adams can execute program_A even though he does not have permission to access EMP

Query Modification

- Adams:
  GRANT SELECT ON EMP TO THOMAS WHERE SALARY < 15000
- THOMAS:
  SELECT *
  FROM EMP
- DBMS:
  SELECT *
  FROM EMP
  WHERE SALARY < 15000

The Grant Command

- GRANT <privilege> ON <relation> TO <users> [WITH GRANT OPTION]
  - GRANT SELECT ON EMP TO ADAMS
  - GRANT SELECT ON EMP TO ADAMS WITH GRANT OPTION
  - GRANT SELECT, UPDATE(SALARY) ON EMP TO JIM, JILL
- Applied to base relations as well as views

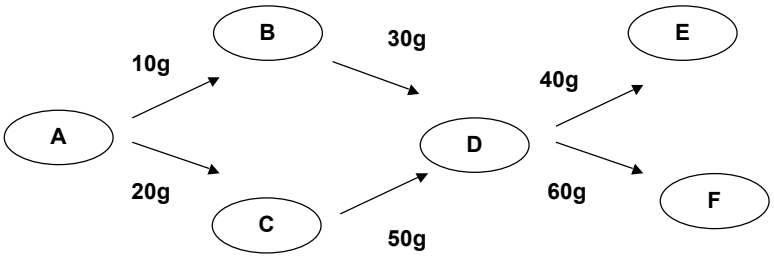
The Revoke Command

- REVOKE <privileges> [ON <relations>]
  FROM <users>
  - REVOKE SELECT ON EMP FROM TOM
  - REVOKE UPDATE ON EMP FROM SMITH
  - REVOKE RESOURCE FROM ABRAMS
  - REVOKE DBA FROM SMITH

Semantics of Revoke

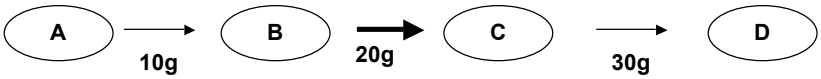
- A sequence of grant command follow by a revoke operation
  - $G_1, G_2, \ldots, G_n, R_h$
- Semantics
  - Equivalent to: $G_1, G_2, \ldots G_{h-1}, G_{h+1}, G_n$

Time-stamped Authorizations

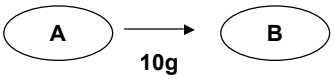


Cascading Revocation

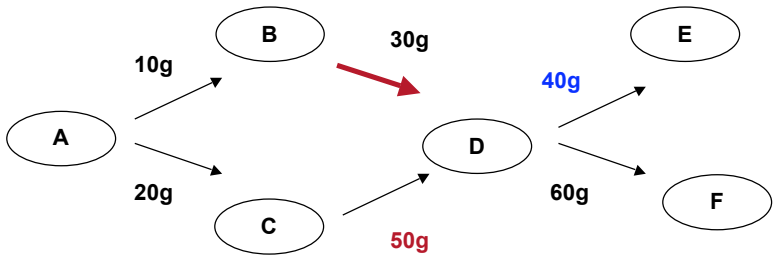
Grant sequence:



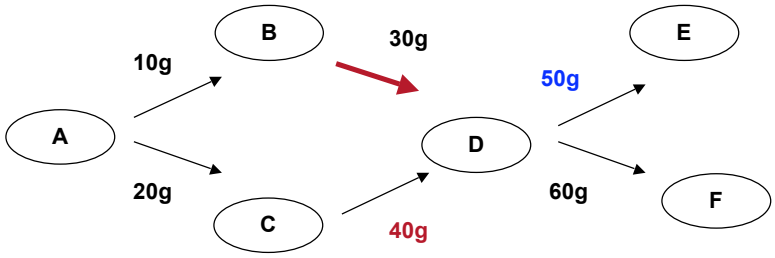
B revokes privilege from C :



Timestamps Make a Difference



Timestamps Make a Difference



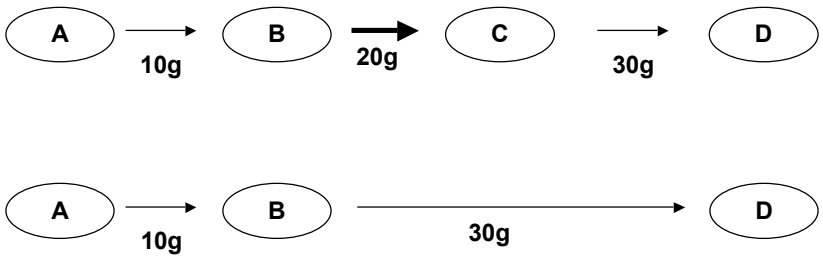
Further Extension

- Make cascading optional
- Permit negative authorizations

The Revoke Command

- REVOKE <privileges> [ON <relations>] FROM <users> [CASCADE]
  - REVOKE SELECT ON EMP FROM TOM
  - REVOKE UPDATE ON EMP FROM SMITH CASCADE
  - REVOKE RESOURCE FROM ADAMS
  - REVOKE DBA FROM SMITH CASCADE

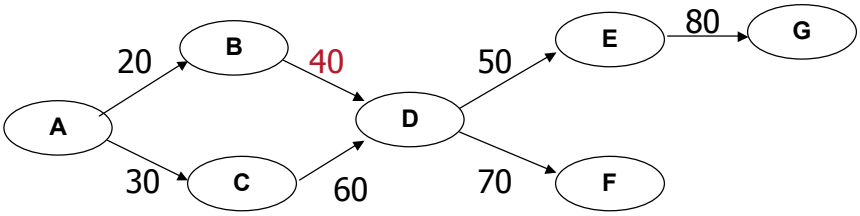
Non-cascading Revocation



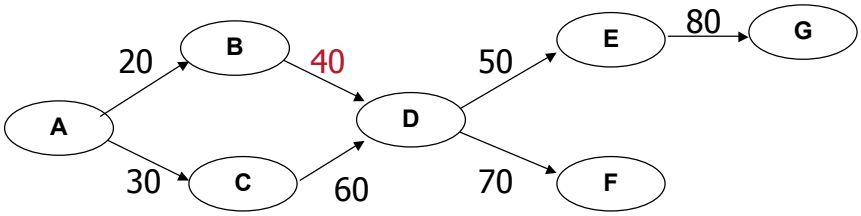
Why Non-cascading Revoke

- Reasons for revoke
  - Task is done. No need to have the privilege anymore
  - Task is still in progress. But a member left the project (e.g., promoted)

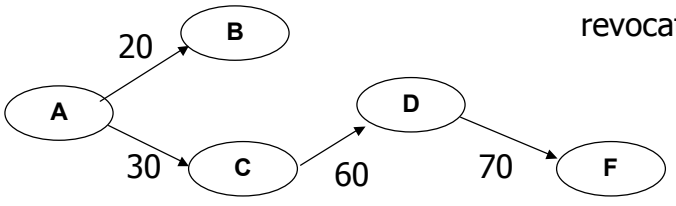
Example



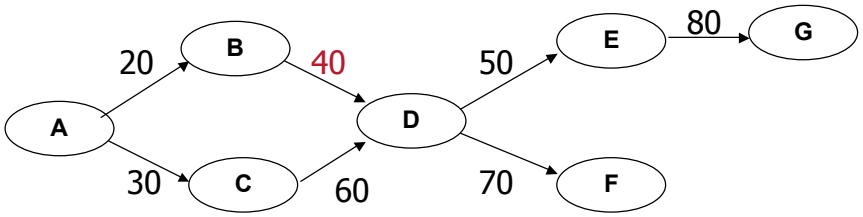
Example



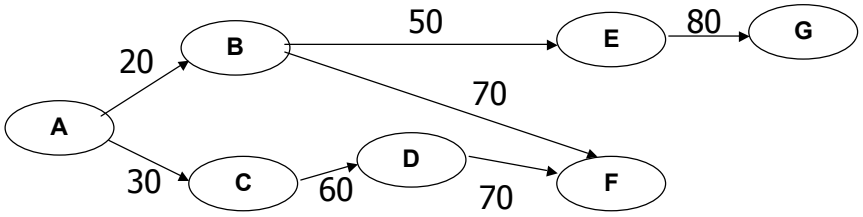
After cascading revocation



Example



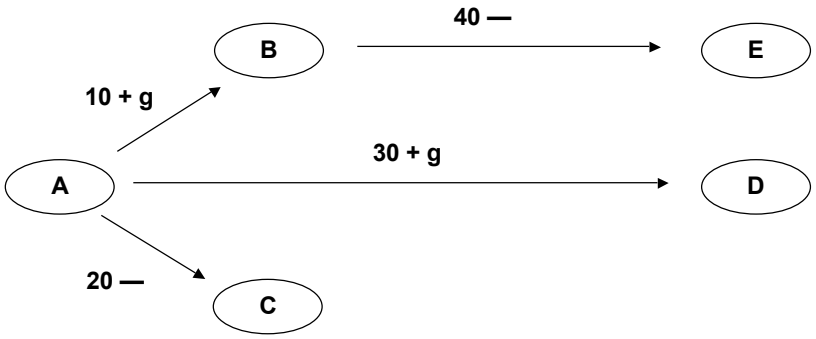
After non-cascading revocation



Why Positive & Negative Authorization

- Closed world policy
  - Cannot access unless explicitly granted the right
- Negative authorization
  - User A should not be allowed to read table Emp
  - Need explicit deny policies

Positive & Negative Authorizations

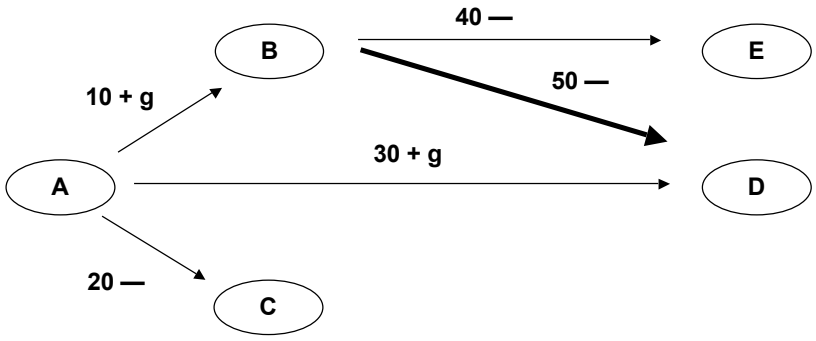


Complication

- It is possible to have two authorizations
  - Grant A privilege p
  - Deny A privilege p
- Negative authorizations override positive authorizations

Problem 1

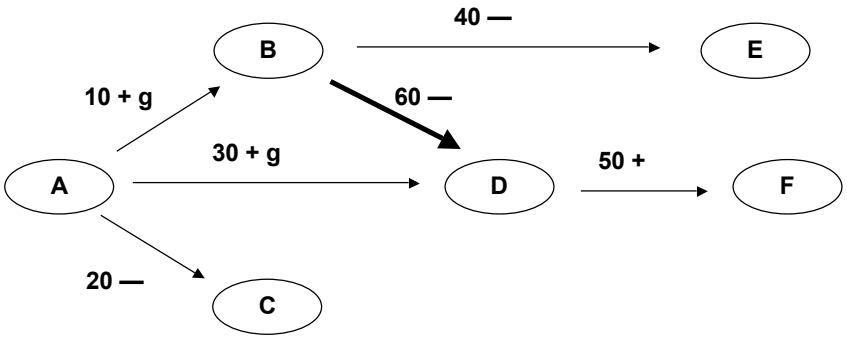
User B gives D negative authorization at time 50 :



In our model, positive authorization granted by A to D becomes blocked, but we do not delete the authorization.

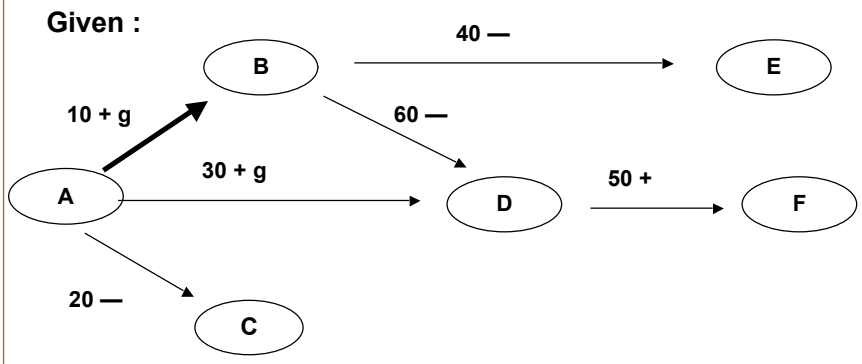
Problem 2

Suppose D receives negative authorization from B at time 60 :



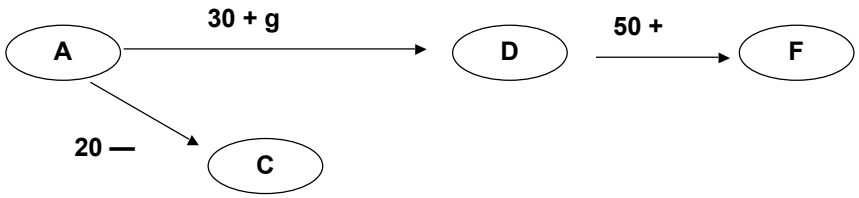
What about the privilege given to F by D?
Under our approach, it becomes blocked, but we do not delete it.

Revocation When Negative Authorizations Are Present



Suppose A revokes B' s privilege.

Cascading Revocation When Negative Authorizations Are Present



Non-cascading Revocation When Negative Authorizations Are Present