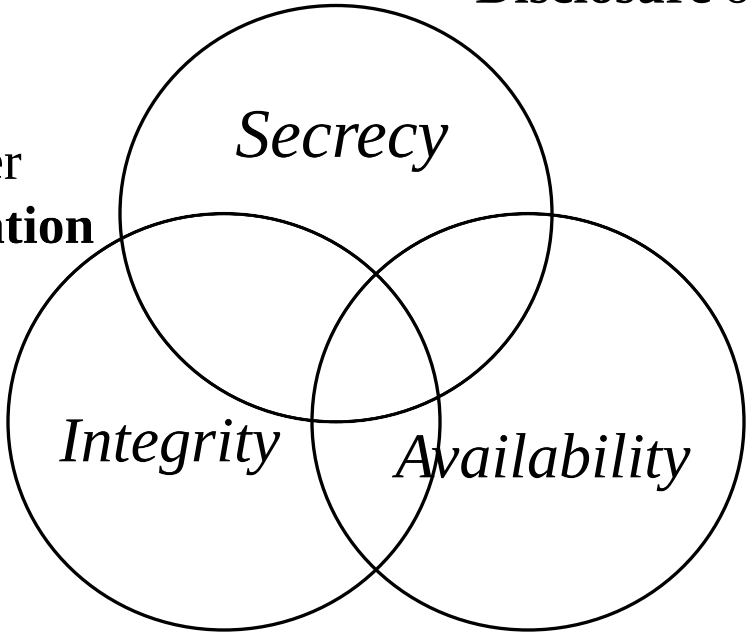
DATABASE SECURITY

Security Objectives

Prevent/detect/deter improper
Disclosure of information

Prevent/detect/deter
Improper **modification**
of information



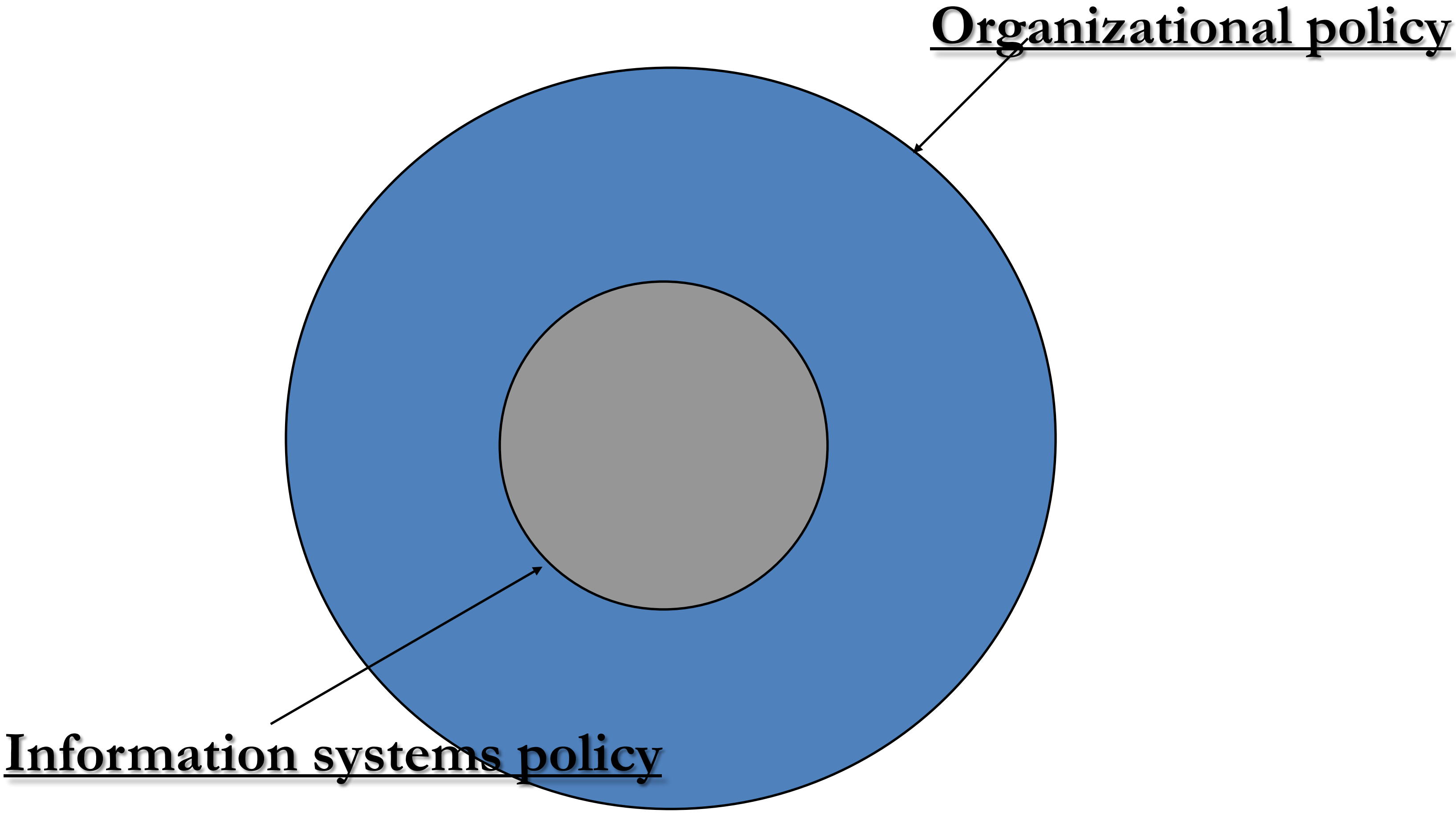
Secrecy

Integrity

Availability

Prevent/detect/deter improper
Denial of access to services

Policy



Organizational policy

Information systems policy

Databases

- Collection of
  - interrelated data and
  - set of programs to access the data
- Convenient and efficient processing of data
- Database Application Software

Database Security

- Protect Sensitive Data from
  - Unauthorized disclosure
  - Unauthorized modification
  - Denial of service attacks
- Security Controls
  - Security Policy
  - Access control models
  - Integrity protection
  - Privacy problems
  - Fault tolerance and recovery
  - Auditing and intrusion detection

Protection of Data Confidentiality

- Access control – which data users can access
- Information flow control – what users can do with the accessed data
- Data Mining

Access Control

- Ensures that all direct accesses to object are authorized

- Protects against accidental and malicious threats by regulating the read, write and execution of data and programs

Access Control

Requires:

- Proper user identification
- Information specifying the access rights is protected form modification

Access Control

- Access control components:
  - Access control policy: specifies the authorized accesses of a system
  - Access control mechanism: implements and enforces the policy

HOW TO SPECIFY ACCESS CONTROL?

Access Control

- Subject: active entity that requests access to an object
  - e.g., user or program
- Object: passive entity accessed by a subject
  - e.g., record, relation, file
- Access right (privileges): how a subject is allowed to access an object
  - e.g., subject *s* can read object *o*

Protection Object

- Database
- Relation
- Record
- Attribute
- Element

Advantages vs. disadvantages
of supporting
different granularity levels

Relation-Level Granularity

Confidential relation

Person-name	Company-name	Salary
Smith	BB&C	$43,982
Dell	Bell	$97,900
Black	BB&C	$35,652

Tuple-level Granularity

Works

Person-name	Company-name	Salary	
Smith	BB&C	$43,982	Public
Dell	Bell	$97,900	Conf.
Black	BB&C	$35,652	Public

Attribute-Level Granularity

Works

Person-name Publ.	Company-name Publ.	Salary Conf.
Smith	BB&C	$43,982
Dell	Bell	$97,900
Black	BB&C	$35,652

Cell-Level Granularity

Works

Person-name	Company-name	Salary
Smith P	BB&C P	$43,982 C
Dell C	Bell C	$97,900 C
Black P	BB&C C	$35,652 C

Access Control Policies

- Discretionary Access Control (DAC)
- Mandatory Access Control (MAC)
- Role-Based Access Control (RBAC)

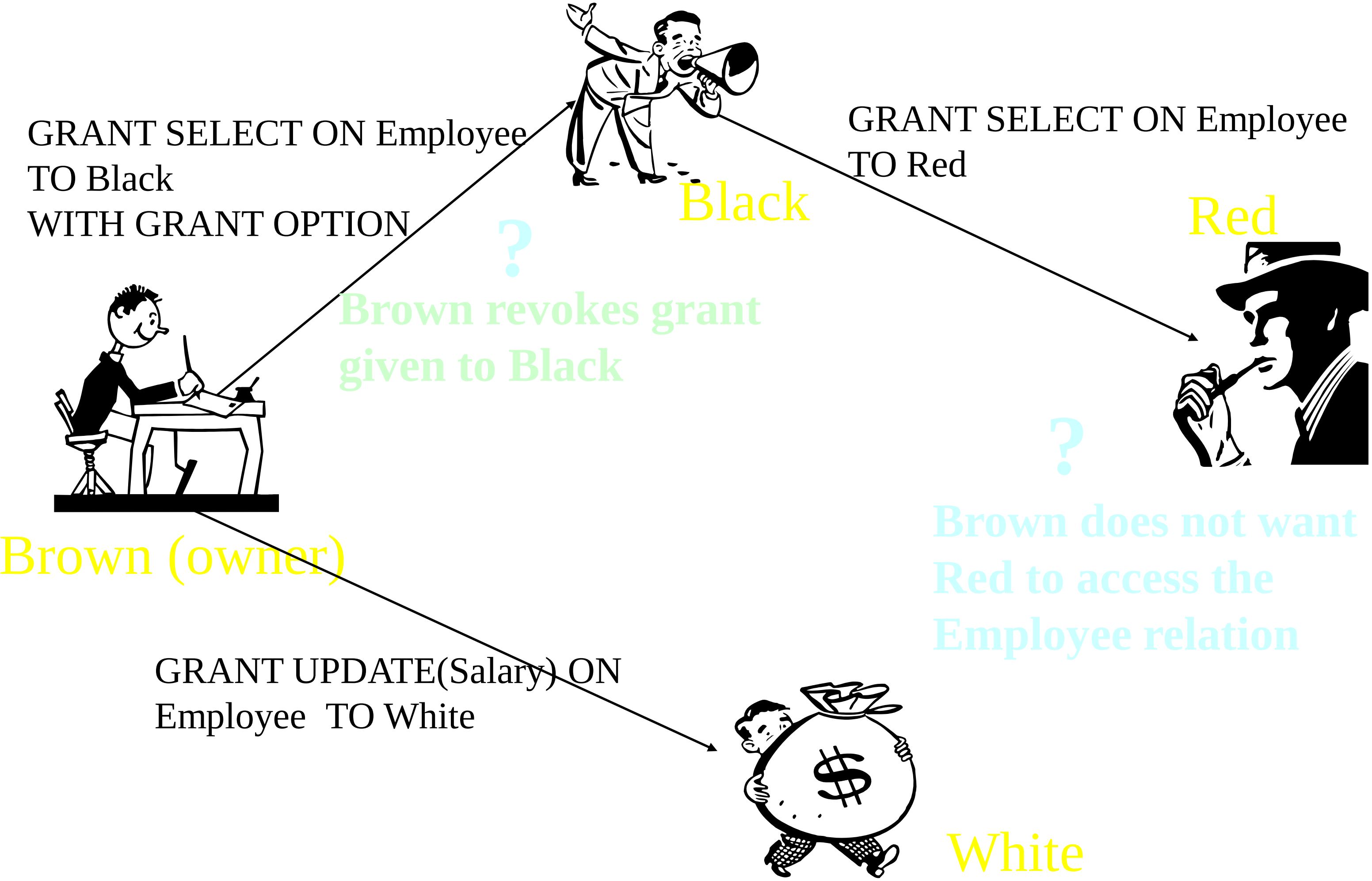
Discretionary Access Control (DAC)

- *For* each subject access right to the objects are defined
  - (subject, object, +/- access mode)
  - (Black, Employee-relation, read)
- User based
- Grant and Revoke
- Problems:

  - Propagation of access rights

  - Revocation of propagated access rights

DAC by Grant and Revoke



GRANT SELECT ON Employee
TO Black
WITH GRANT OPTION

Black

GRANT SELECT ON Employee
TO Red

Red

?

Brown revokes grant given to Black

Brown (owner)

?

Brown does not want Red to access the Employee relation

GRANT UPDATE(Salary) ON
Employee TO White

White

Implementation

Access Control List (column)
(ACL)

File 1	**File 2**
Joe:Read	Joe:Read
Joe:Write	Sam:Read
Joe:Own	Sam:Write
	Sam:Own

Capability List (row)

Joe: File 1/Read, File 1/Write, File 1/Own, File 2/Read
Sam: File 2/Read, File 2/Write, File 2/Own

Access Control Triples

Subject	Access	Object
Joe	Read	File 1
Joe	Write	File 1
Joe	Own	File 1
Joe	Read	File 2
Sam	Read	File 2
Sam	Write	File 2
Sam	Own	File 2

Access Control Mechanisms

- Security through Views
- Stored Procedures
- Grant and Revoke
- Query modification

Security Through Views

- Assign rights to access predefined views

```
CREATE VIEW Outstanding-Student
AS SELECT NAME, COURSE, GRADE
FROM Student
WHERE GRADE > B
```

Problem:

Difficult to maintain updates.

Stored Procedures

- Assign rights to execute compiled programs
- **GRANT RUN ON <program> TO <user>**

Problem:

Programs may access resources for which the user who runs the program does not have permission.

Grant and Revoke

GRANT <privilege> ON <relation>

To <user>

[WITH GRANT OPTION]

- GRANT SELECT * ON *Student* TO Matthews
- GRANT SELECT *, UPDATE(GRADE) ON *Student* TO FARKAS
- GRANT SELECT(NAME) ON *Student* TO Brown

GRANT command applies to base relations as well as views

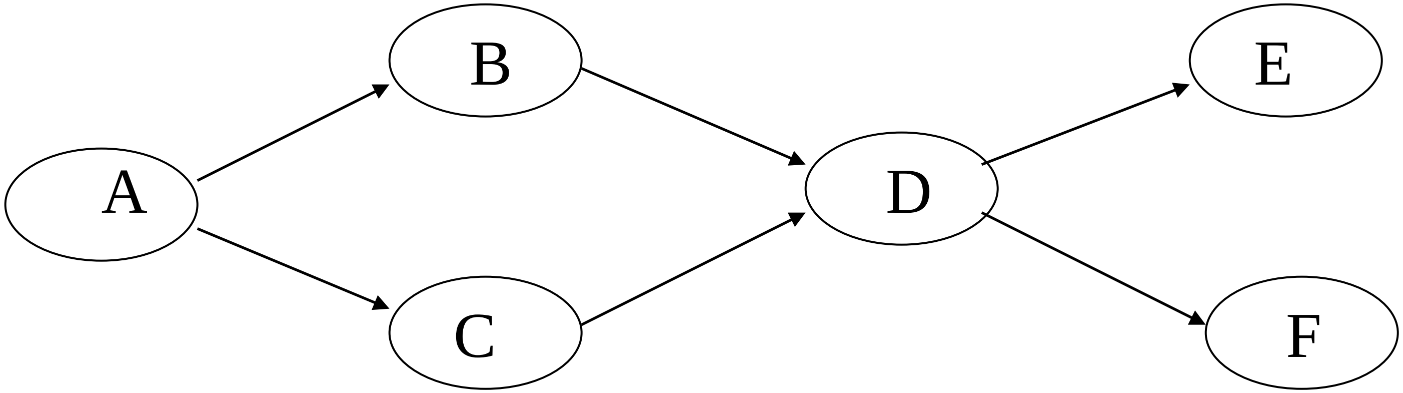
Grant and Revoke

REVOKE <privileges> [ON <relation>]

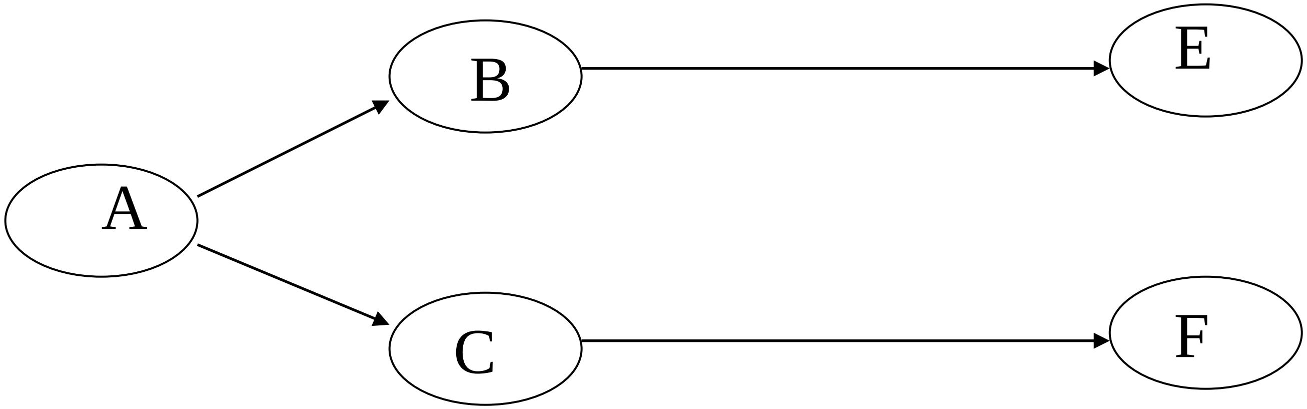
FROM <user>

- REVOKE SELECT* ON *Student* FROM Blue
- REVOKE UPDATE ON *Student* FROM Black
- REVOKE SELECT(NAME) ON *Student* FROM Brown

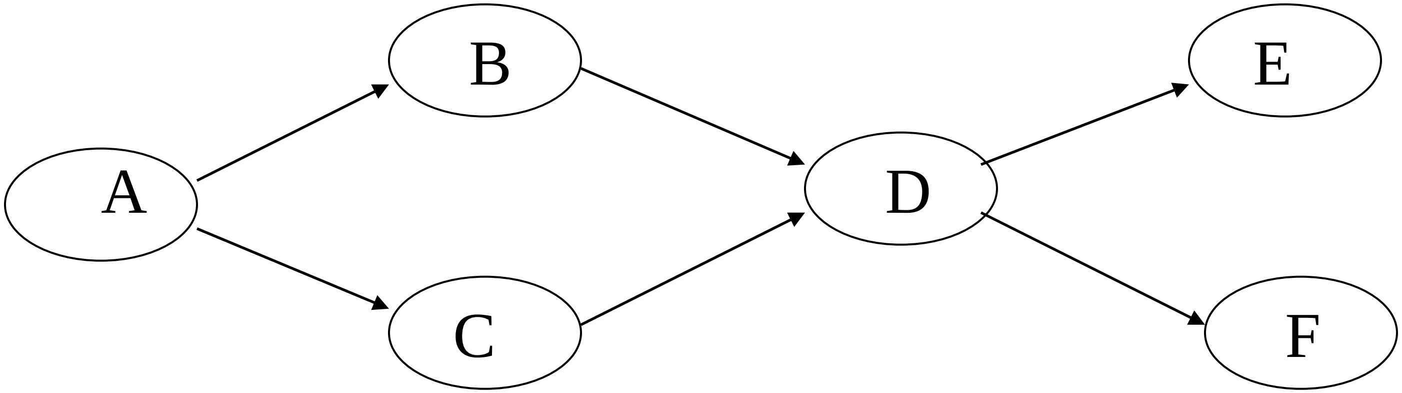
Non-cascading Revoke



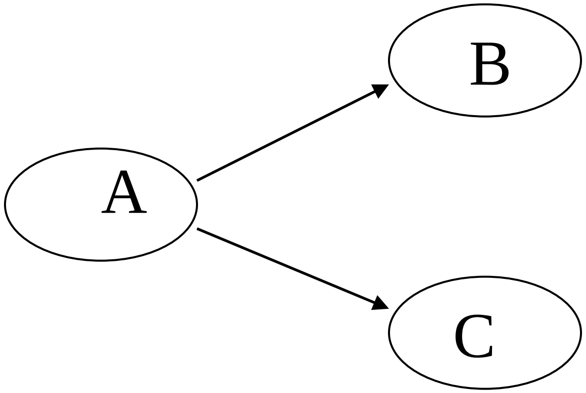
A revokes D’s privileges



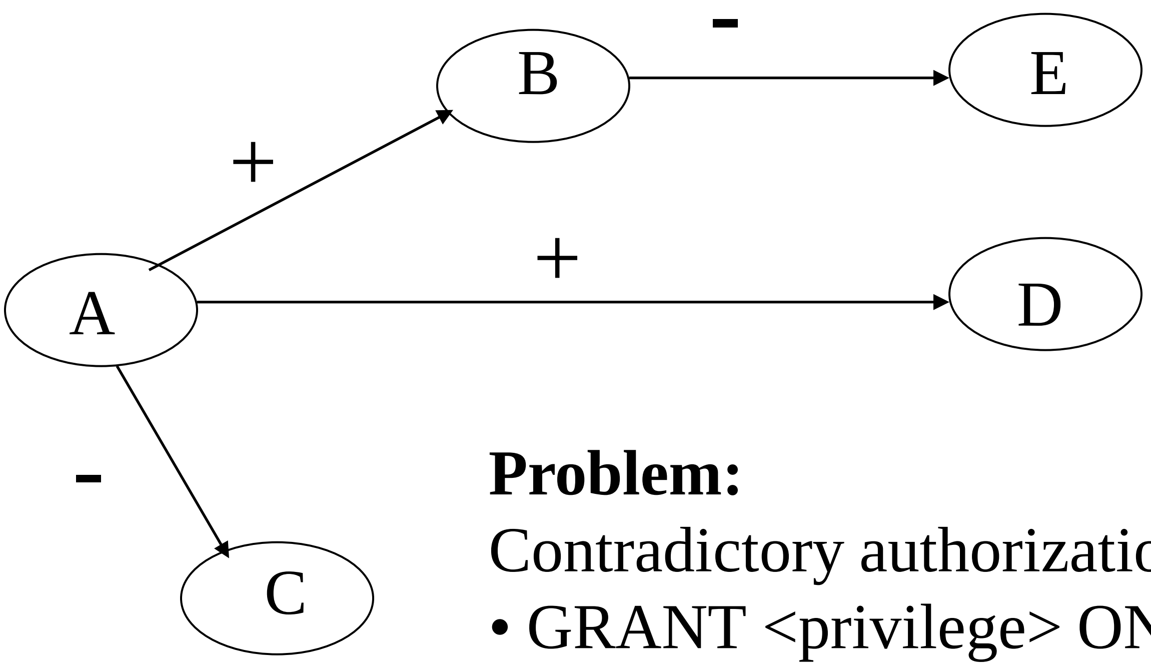
Cascading Revoke



A revokes D’s privileges



Positive and Negative Authorization

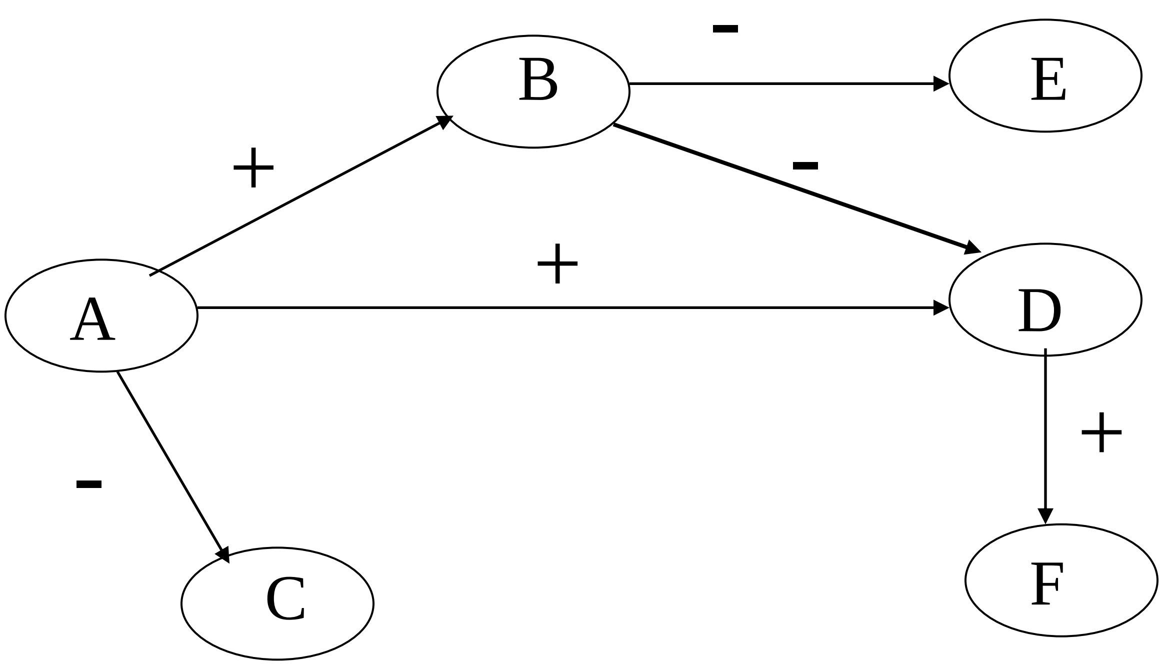


Problem:

Contradictory authorizations

- GRANT <privilege> ON *X* TO <user>
- DENY <privilege> ON *X* TO <user>

Negative Authorization



What should happen with the privilege given by D To F?

Query Modification

- GRANT SELECT(NAME) ON *Student* TO Blue WHERE COURSE="CSCE 590"

- **Blue's query:**

  SELECT *

  FROM *Student*

- **Modified query:**

  SELECT NAME

  FROM *Student*

  WHERE COURSE="CSCE 590"

DAC Overview

- Advantages:
  - Intuitive
  - Easy to implement
- Disadvantages:
  - Inherent vulnerability (look TH example)
  - Maintenance of ACL or Capability lists
  - Maintenance of Grant/Revoke
  - Limited power of negative authorization

Mandatory Access Control (MAC)

- Security label
  - Top-Secret, Secret, Public
- Objects: security classification
  - File 1 is Secret, File 2 is Public
- Subjects: security clearances
  - Brown is cleared to Secret, Black is cleared to Public
- Dominance (≥)
  - Top-Secret ≥ Secret ≥ Public

MAC

- Access rights: defined by comparing the security classification of the requested objects with the security clearance of the subject
- If access control rules are satisfied, access is permitted
- Otherwise access is rejected
- Granularity of access rights!