



Authorization

Database Authorization

- Make sure users see only the data they're supposed to see
- Guard the database against modifications by malicious users

Database Authorization

Users have privileges; can only operate on data for which they are authorized

- Select on R or Select(A_1, \dots, A_n) on R
- Insert on R or Insert(A_1, \dots, A_n) on R
- Update on R or Update(A_1, \dots, A_n) on R
- Delete on R

```
Update Apply  
Set dec = 'Y'  
where sID In (Select sID  
                From Student  
                where GPA > 3.9)
```

Apply: *update(dec), select(sID)*

Student: *select(sID, GPA)*

College

cName	state	enr

Student

sID	sName	GPA	HS

Apply

sID	cName	major	dec

```
Delete From Student  
Where SID Not In  
  (Select SID From Apply)
```

Student: Delete, Select(SID)

Apply: Select(SID)

College

cName	state	enr

Student

SID	sName	GPA	HS

Apply

SID	cName	major	dec

Select student info for Stanford applicants only

```
Create View SS As  
  Select * From Student ←  
  Where SID In  
    (Select SID From Apply ←  
     Where cName = 'Stanford')
```

Select(SS)

College

cName	state	enr

Student

sID	sName	GPA	HS

Apply

sID	cName	major	dec

Delete Berkeley applications only

```
Create View BA As  
  Select * From Apply  
  Where cName = 'Berkeley'
```

BA: Delete

College

cName	state	enr

Student

sID	sName	GPA	HS

Apply

sID	cName	major	dec

Obtaining Privileges

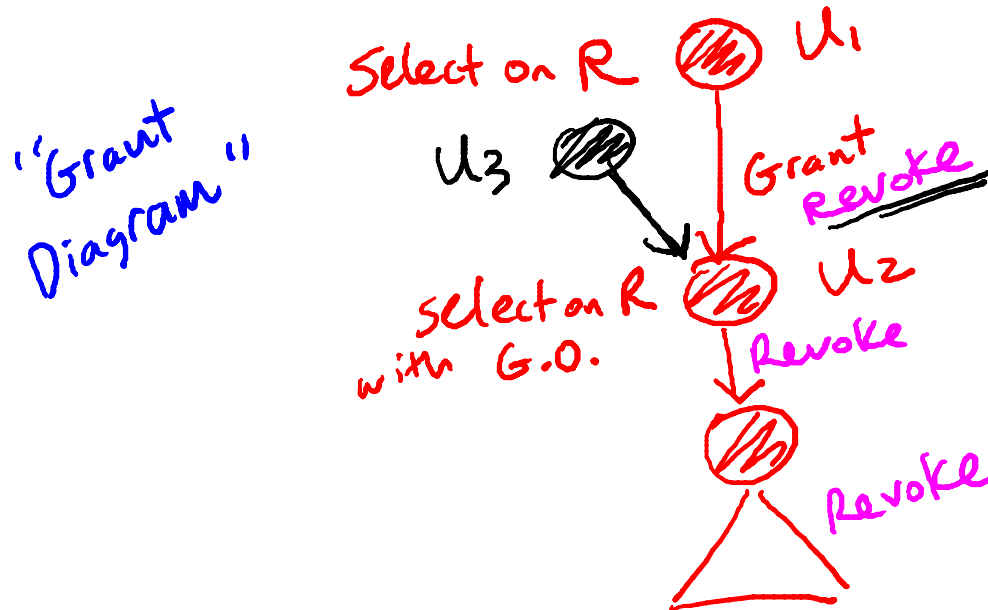
- Relation creator is owner ✓
- Owner has all privileges and may grant privileges

Grant privs On R To users
[with Grant Option]

Select(s10), Delete
 Select(A,B,C)
 Select(A,B)
 grant same or lesser
 to others
 public

Revoking Privileges

Revoke privs On R From users
[Cascade | Restrict]



Revoking Privileges

Revoke *privs* On *R* From *users*
[Cascade | Restrict]

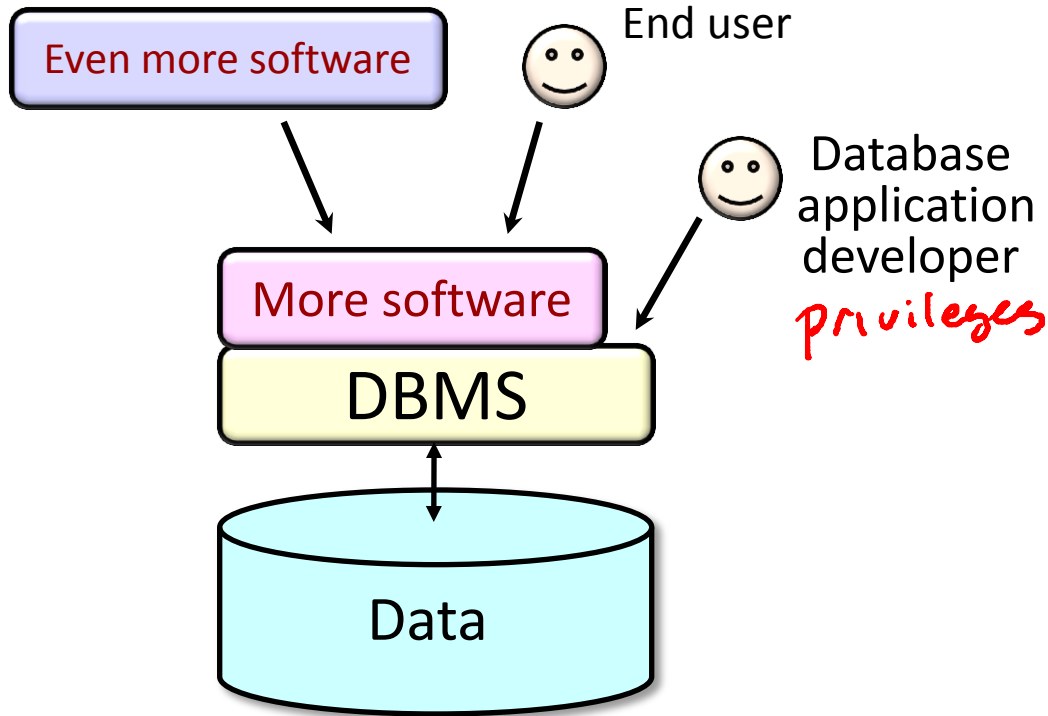
Cascade: Also revoke privileges granted from privileges being revoked (transitively), unless also granted from another source

Revoking Privileges

Revoke *privs* On *R* From *users*
[Cascade | Restrict] ←

Restrict: Disallow if Cascade would revoke any other privileges

Where Privileges Reside



Database Authorization

- Make sure users see only the data they're supposed to see
- Guard the database against modifications by malicious users
- Users have privileges; can only operate on data for which they are authorized
- Grant and Revoke statements
- Beyond simple table-level privileges: use views