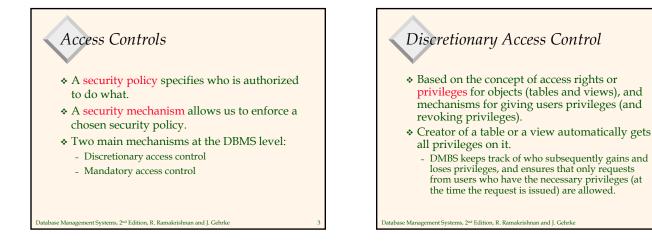
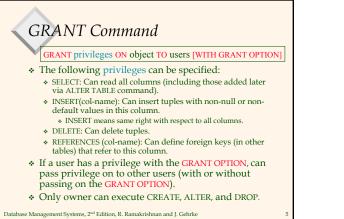
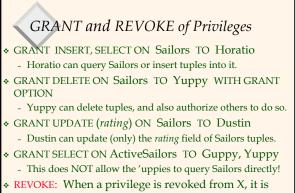


Introduction to DB Security Secrecy: Users should not be able to see things they are not supposed to. E.g., A student can't see other students' grades. Integrity: Users should not be able to modify things they are not supposed to. E.g., Only instructors can assign grades. Availability: Users should be able to see and modify things they are allowed to.

Database Management Systems, 2nd Edition, R. Ramakrishnan and J. Gehrke







also revoked from all users who got it *solely* from X. Database Management Systems, 2nd Edition, R. Ramakrishnan and J. Gehrke

GRANT/REVOKE on Views

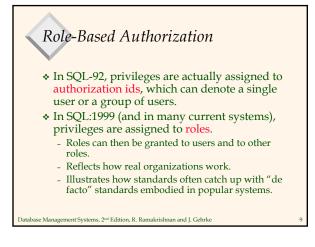
- If the creator of a view loses the SELECT privilege on an underlying table, the view is dropped!
- If the creator of a view loses a privilege held with the grant option on an underlying table, (s)he loses the privilege on the view as well; so do users who were granted that privilege on the view!

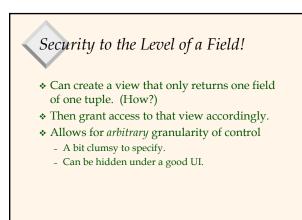
Database Management Systems, 2nd Edition, R. Ramakrishnan and J. Gehrke

Views and Security

- Views can be used to present necessary information (or a summary), while hiding details in underlying relation(s).
 - Given ActiveSailors, but not Sailors or Reserves, we can find sailors who have a reservation, but not the *bid*'s of boats that have been reserved.
- Creator of view has a privilege on the view if (s)he has the privilege on all underlying tables.
- Together with GRANT/REVOKE commands, views are a very powerful access control tool.

Database Management Systems, 2nd Edition, R. Ramakrishnan and J. Gehrke





Database Management Systems, 2nd Edition, R. Ramakrishnan and J. Gehrke

Mandatory Access Control Based on system-wide policies that cannot be changed by individual users. Each DB object is assigned a security class. Each subject (user or user program) is assigned a clearance for a security class. Rules based on security classes and clearances govern who can read/write which objects. Most commercial systems do not support mandatory access control. Versions of some DBMSs do support it; used for specialized (e.g., military) applications.

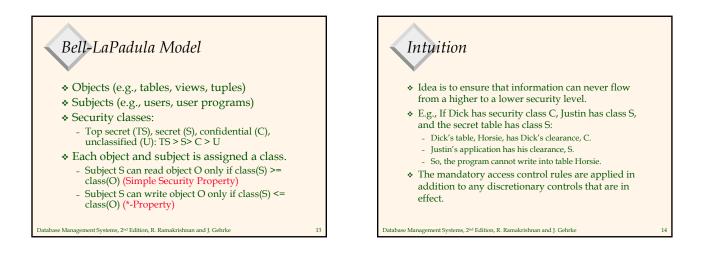
Database Management Systems, 2nd Edition, R. Ramakrishnan and J. Gehrke

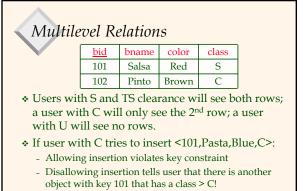
Why Mandatory Control?
 Discretionary control has some flaws, e.g., the *Trojan horse* problem:

 Dick creates Horsie and gives INSERT privileges to Justin (who doesn't know about this).
 Dick modifes the code of an application program used by Justin to additionally write some secret data to table Horsie.
 Now, Justin can see the secret info.

 The modification of the code is beyond the DBMSs control, but it can try and prevent the use of the database as a channel for secret information.

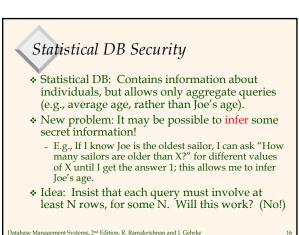
Database Management Systems, 2nd Edition, R. Ramakrishnan and J. Gehrke

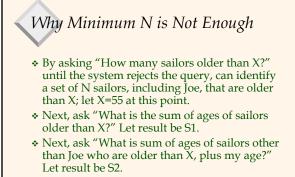




- Problem resolved by treating class field as part of key.

Database Management Systems, 2nd Edition, R. Ramakrishnan and J. Gehrke





♦ S1-S2 is Joe's age!

Database Management Systems, 2nd Edition, R. Ramakrishnan and J. Gehrke

17

