#### DBA Certification Course (Summer 2008)

### Chapter 2: Security in DB2

- Authentication
- DB2 Authorities
- Privileges
- Label-Based Access Control

# Objectives

After completing this chapter, you should be able to:

- explain where authentication is done (client or server), depending on configuration parameters.
- explain the rights of different server authorizations
- use GRANT and REVOKE for object privileges

This is mostly a short repetition from "Databases I".



• Graham G. Milne: DB2 9 Fundamentals exam 730 prep, Part 2: Security

[http://www.ibm.com/developerworks/edu/dm-dw-db2-cert7302.html]

• Carmen K. Wong, Stan Musker: DB2 Label-Based Access Control, a practical guide, Part 1

[http://.../developerworks/edu/dm-dw-dm-0605wong-i.html]

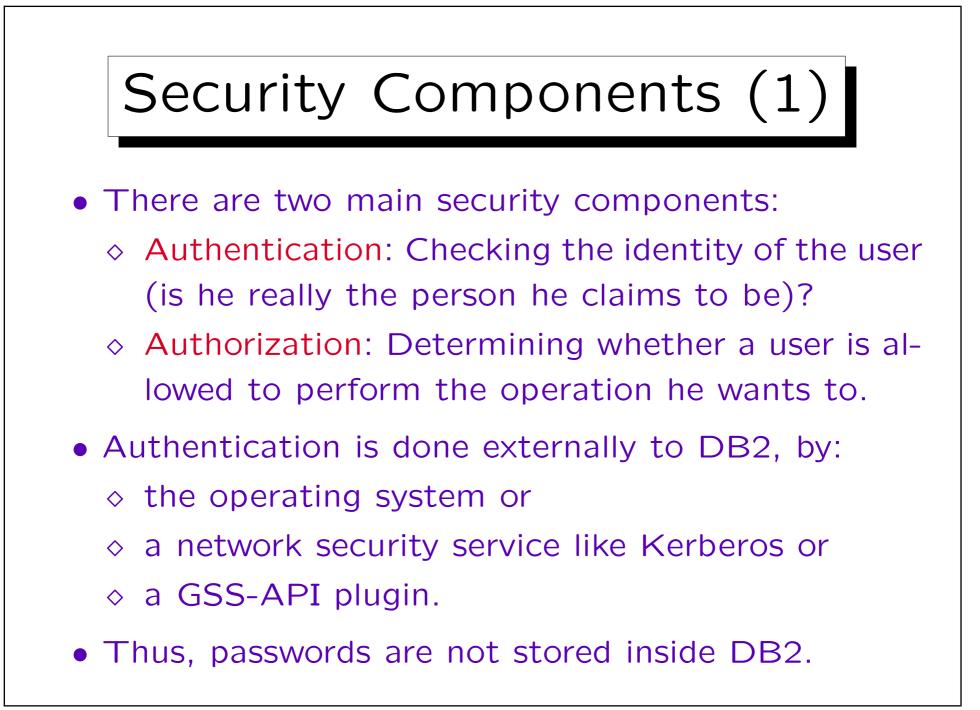
 Clara Liu, Raul Chong, Dwaine Snow, Sylvia Qi: Understanding DB2: Learning Visually with Examples

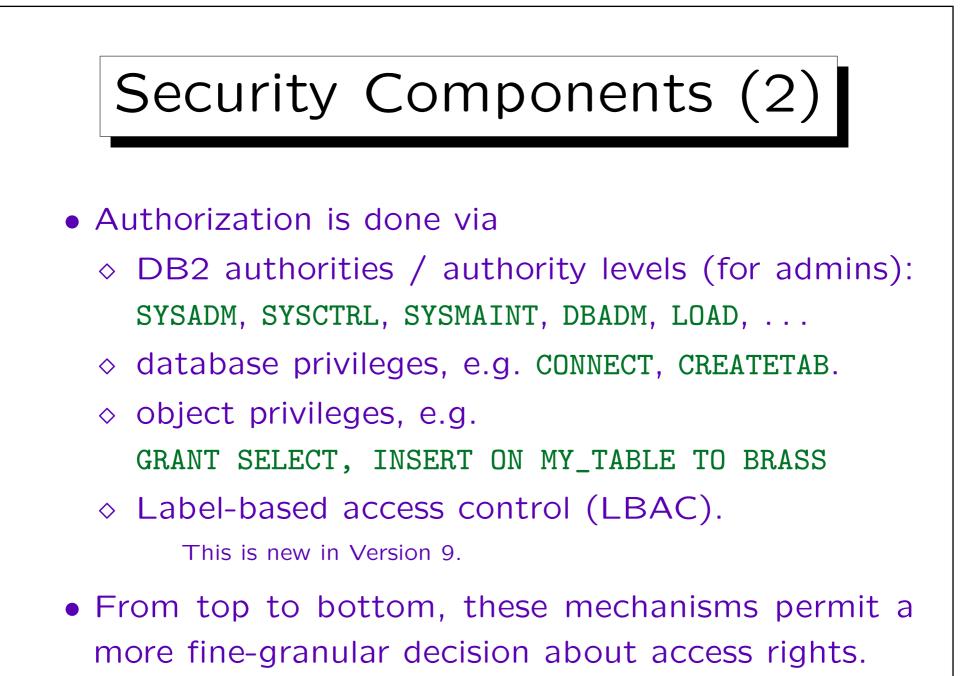
IBM Press/Pearson, 2005, ISBN 0-13-185916-1, 895 pages.





- 2. Authentication
- 3. DB2 Authorities and Database Privileges
- 4. Object Privileges
- 5. Label-Based Access Control







1. General Remarks

2. Authentication

3. DB2 Authorities and Database Privileges

4. Object Privileges

5. Label-Based Access Control

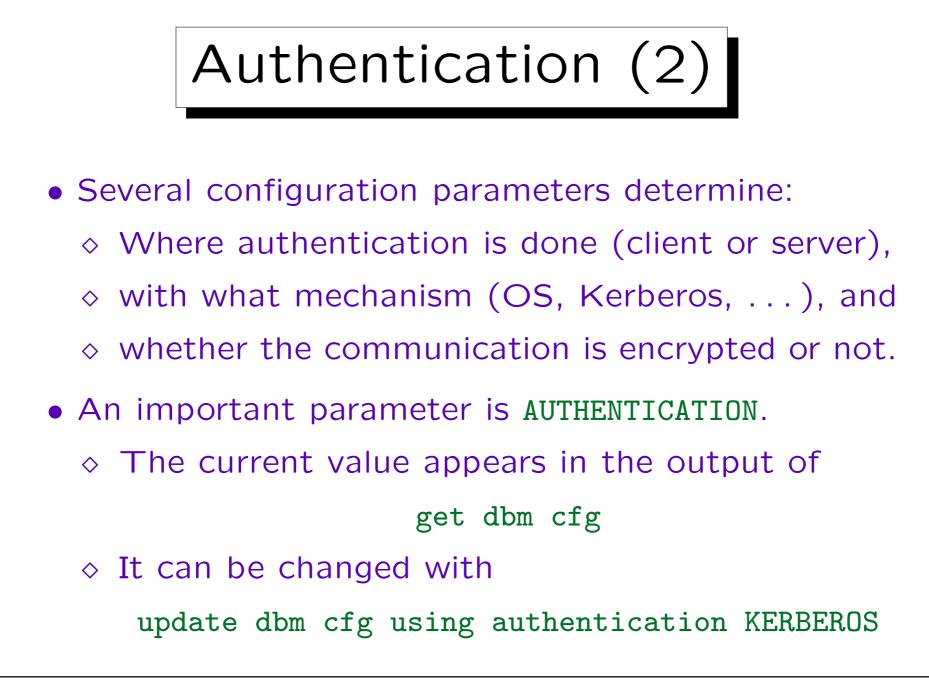


- A typical case is that the authentication is done on the server (by the operating system).
- When the user is logged in on the server, he/she can connect to the database without password:

connect to sample

• If the application program runs on a different machine (client), and a network connection to the server is used, it might be necessary to specify user and password for the server:

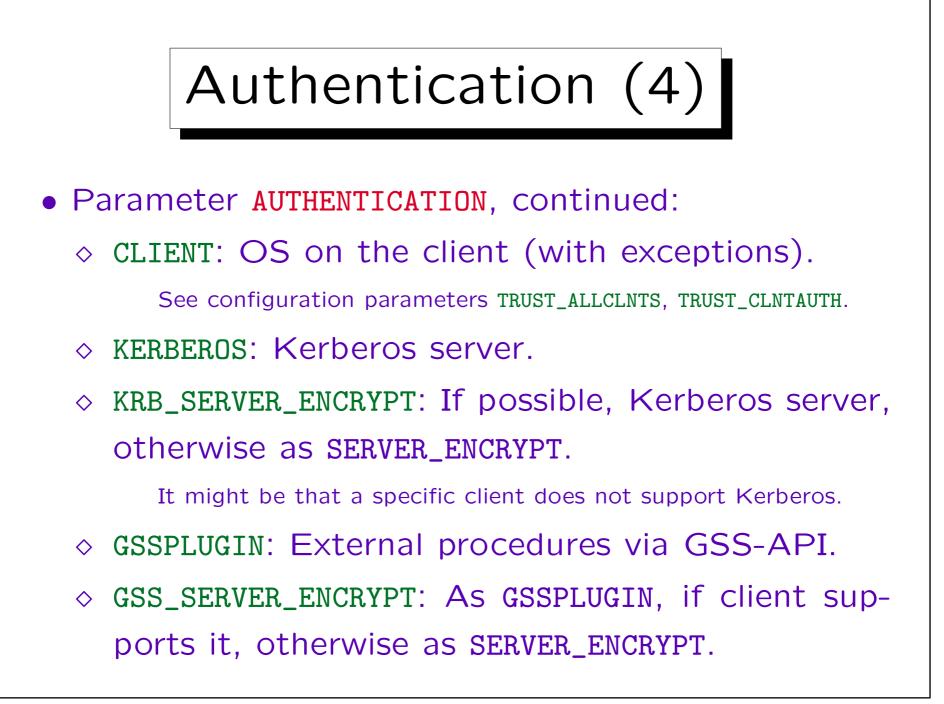
connect to sample user scott using tiger

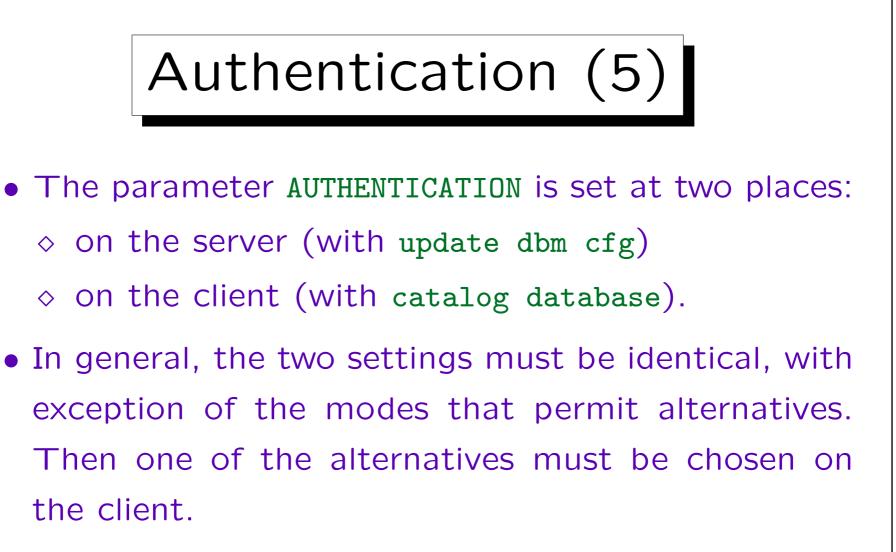




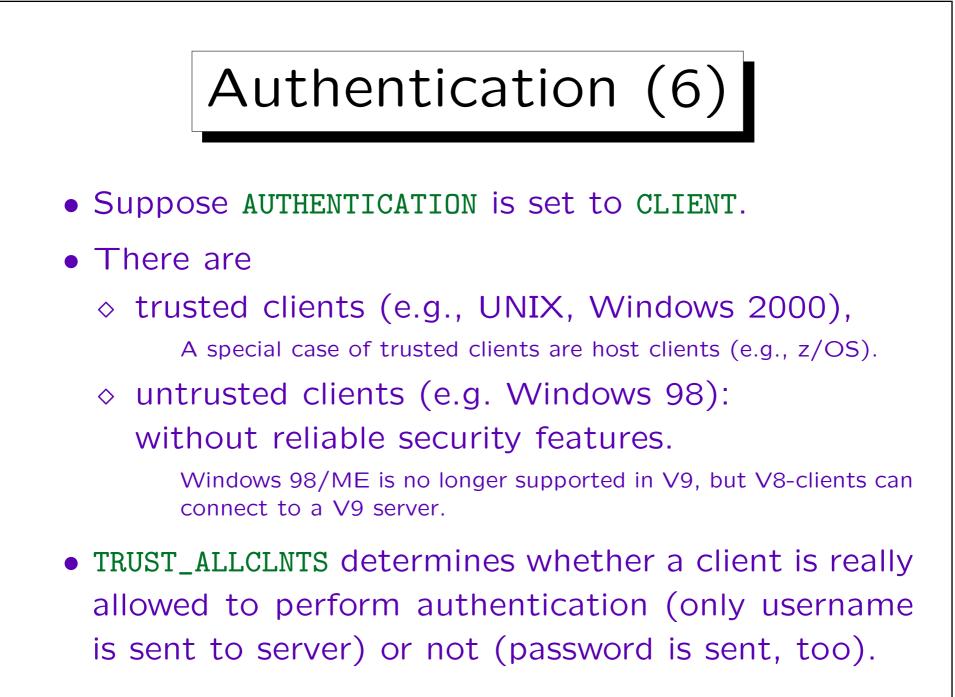
- Possible values of the DBM configuration parameter AUTHENTICATION are (continued on next slide):
  - $\diamond$  SERVER: OS on the server (default).
  - ◇ SERVER\_ENCRYPT: OS on the server, password is sent encrypted over the net.
  - ◇ DATA\_ENCRYPT: As SERVER\_ENCRYPT, but also data are sent encrypted over the net.
  - ◇ DATA\_ENCRYPT\_CMP: As DATA\_ENCRYPT, but older clients may connect with SERVER\_ENCRYPT.

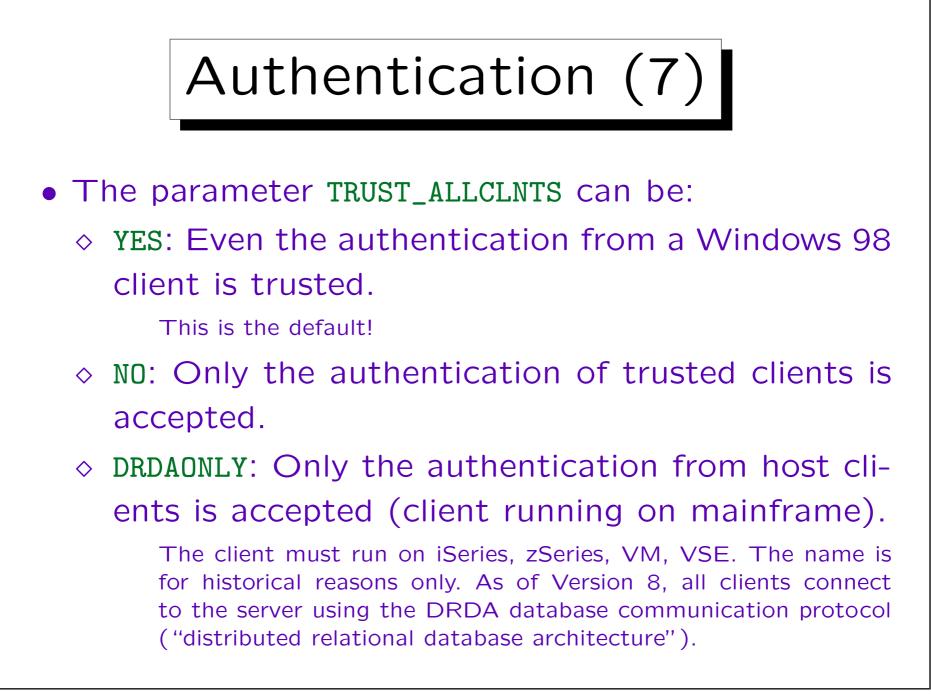
DATA\_ENCRYPT was new in Version 9.





Possible settings on the client are: SERVER, SERVER\_ENCRYPT, CLIENT, KERBEROS (with TARGET PRINCIPAL  $\langle Name \rangle$ ), SQL\_AUTHENTICATION\_DATAENC, SQL\_AUTHENTICATION\_DATAENC\_CMP, GSSPLUGIN.

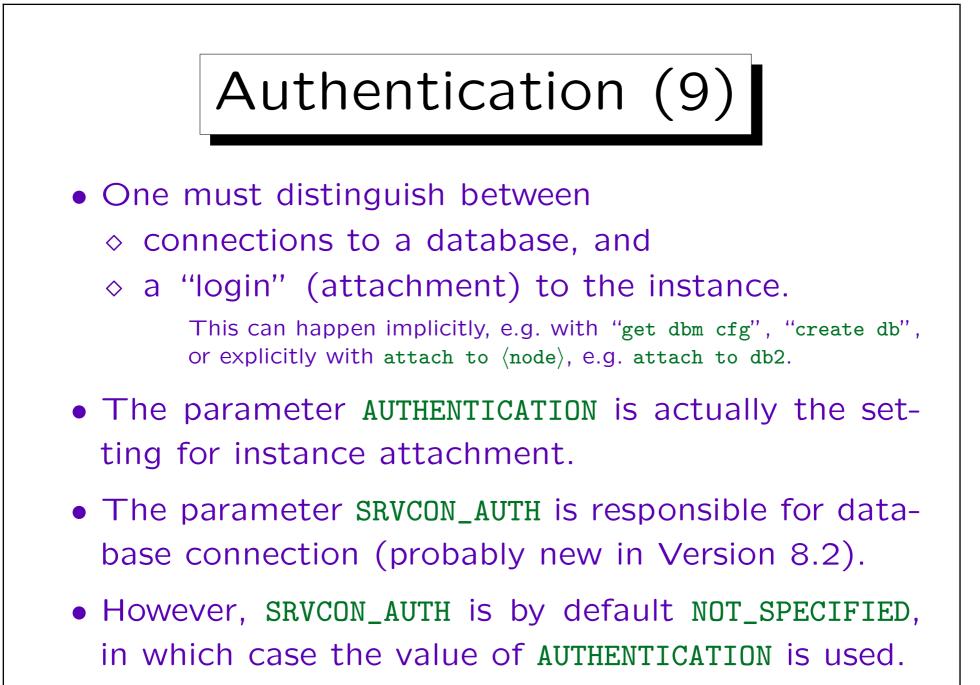






- Suppose a user is logged in at the client as user A, but wants to connect to the server as user B.
- Then one specifies user ID and password in the connect statement.
- The parameter **TRUST\_CLNTAUTH** determines where authentication is done in this case. It can be:
  - $\diamond$  SERVER: On the server.
  - $\diamond\,$  CLIENT: On the client.

Note that this is done only if AUTHENTICATION is set to CLIENT, and the client is trusted (or TRUST\_ALLCLNTS=YES). I.e. the other parameters have higher priority.



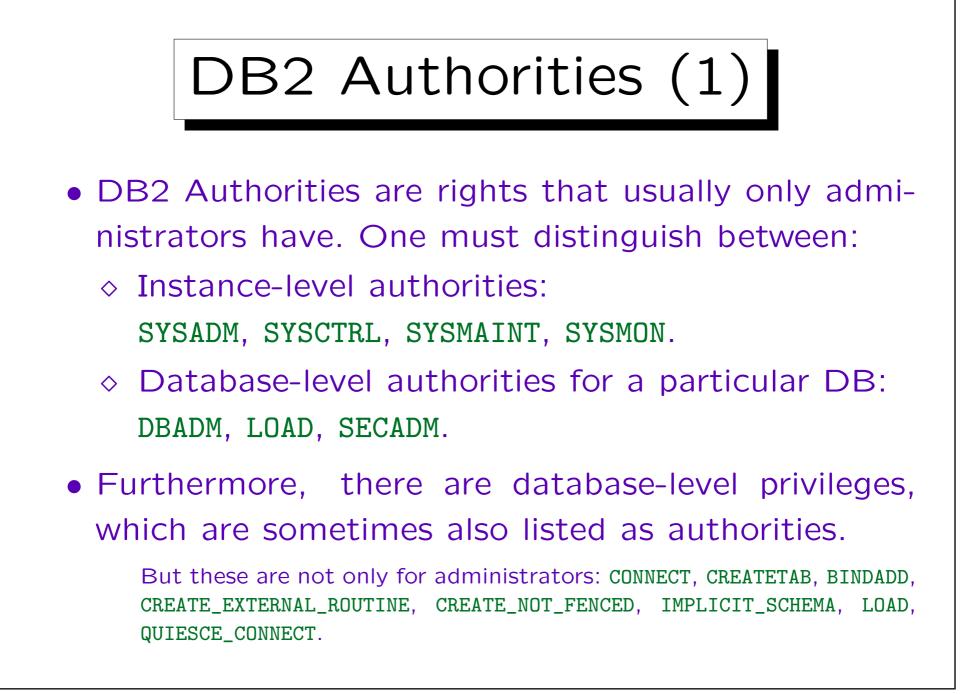


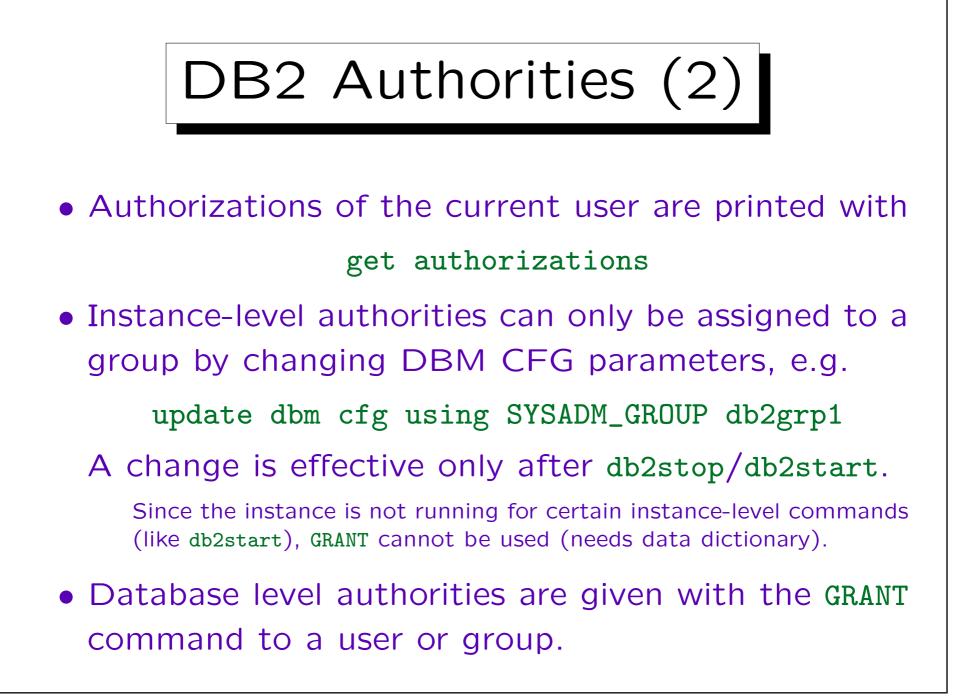
- 1. General Remarks
- 2. Authentication

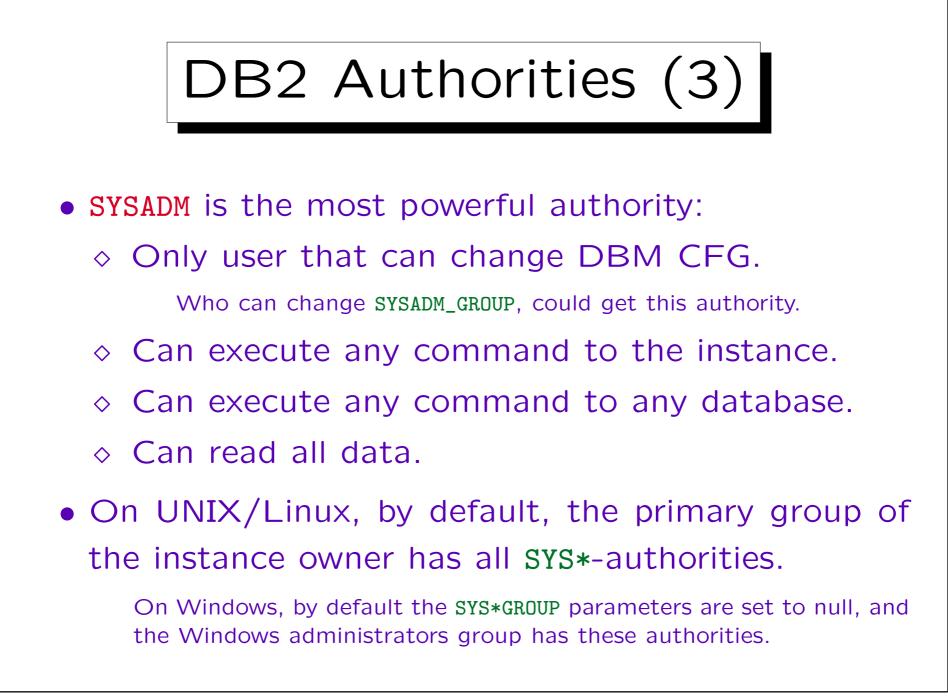
3. DB2 Authorities and Database Privileges

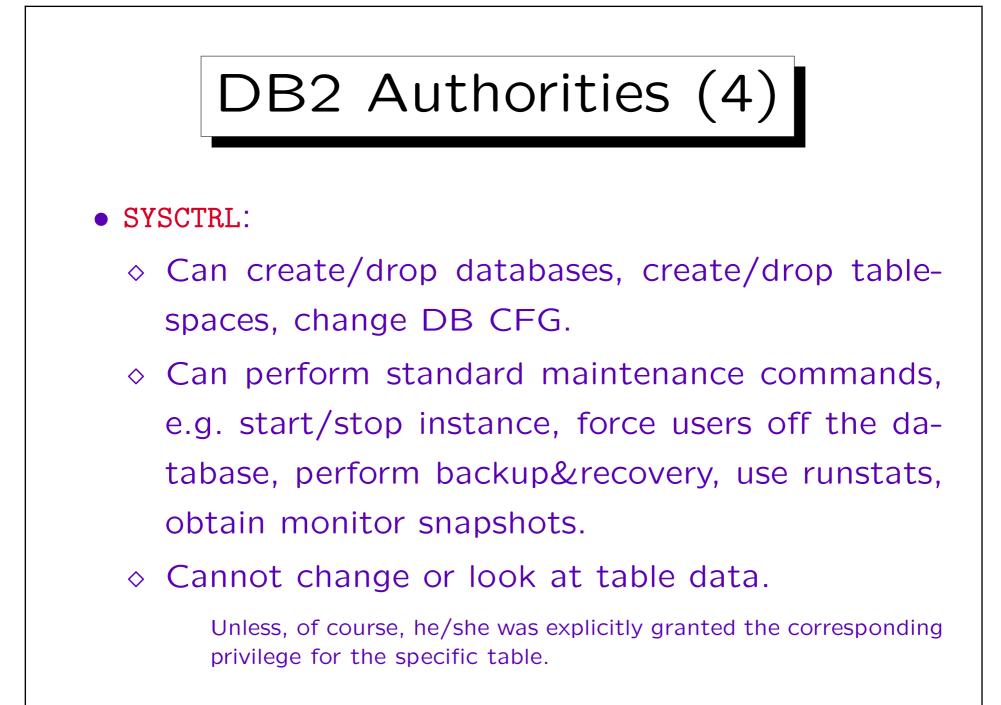
- 4. Object Privileges
- 5. Label-Based Access Control

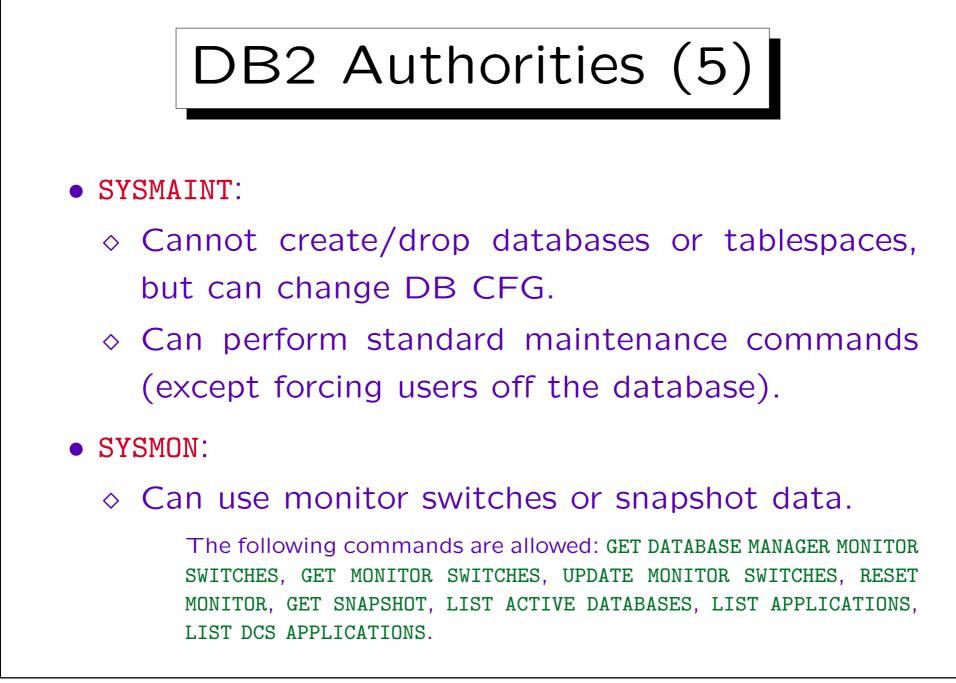
2 - 17

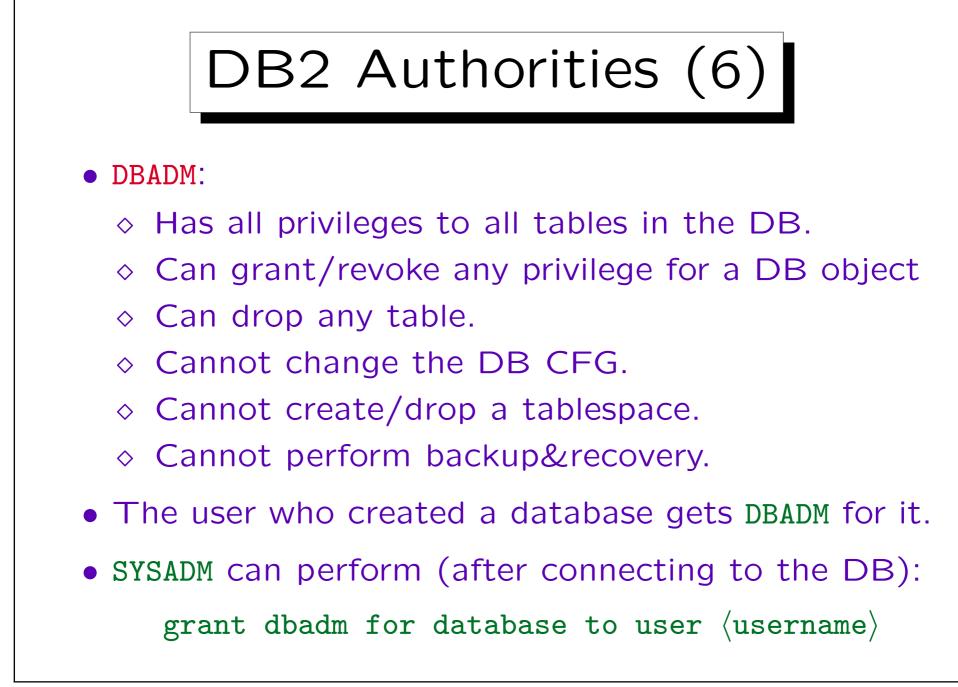


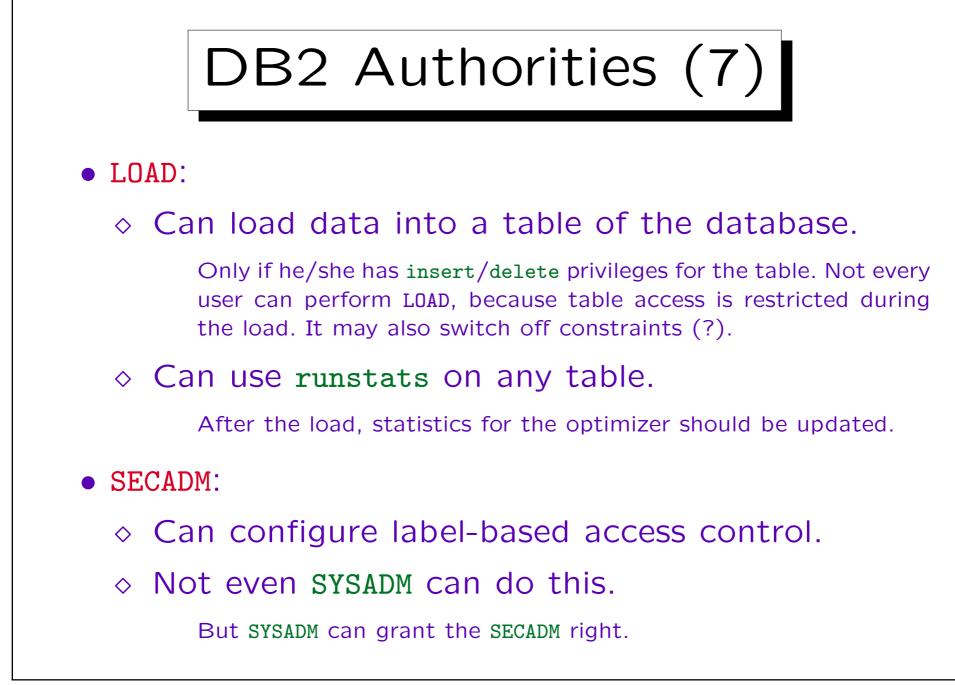


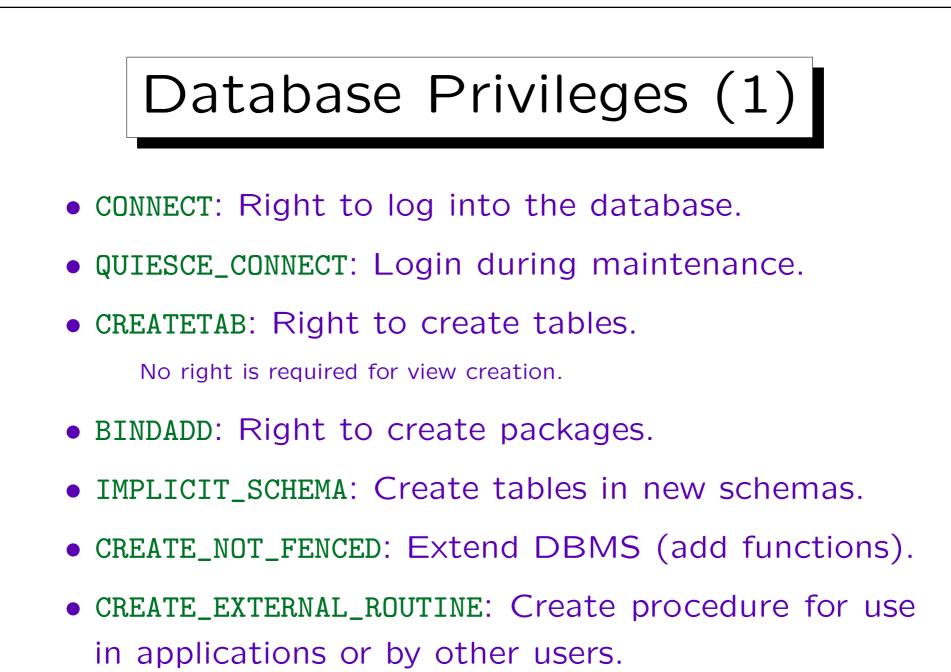


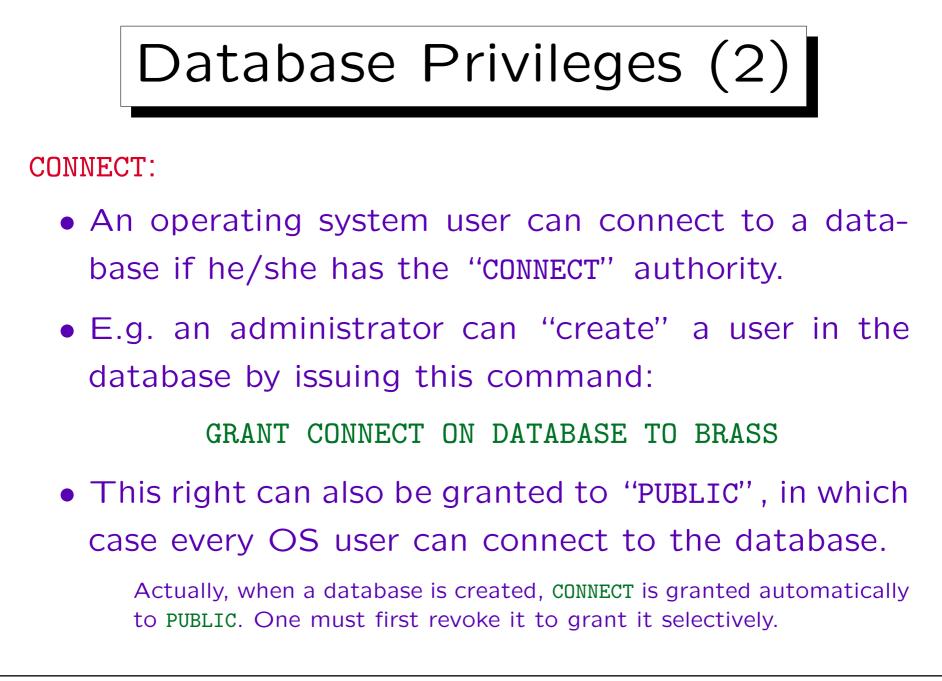








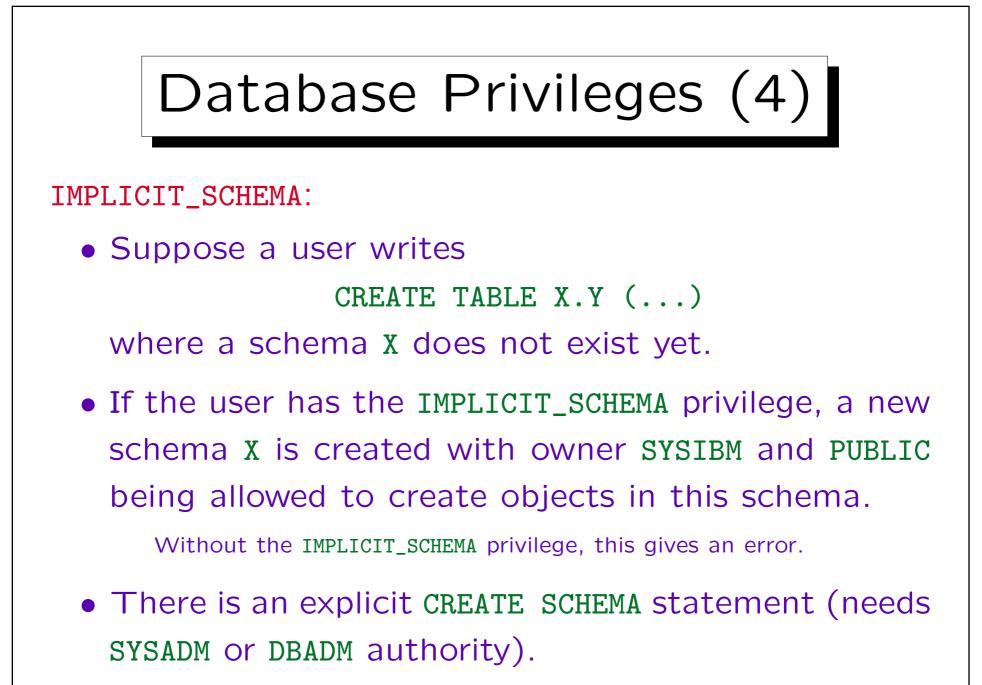




### Database Privileges (3)

BINDADD:

- When an application program with embedded SQL is compiled, a "package" is created in the database with the SQL statements (and access plans for them) of the application program.
- This is done with the command "BIND".
- BINDADD is the right to create new packages.



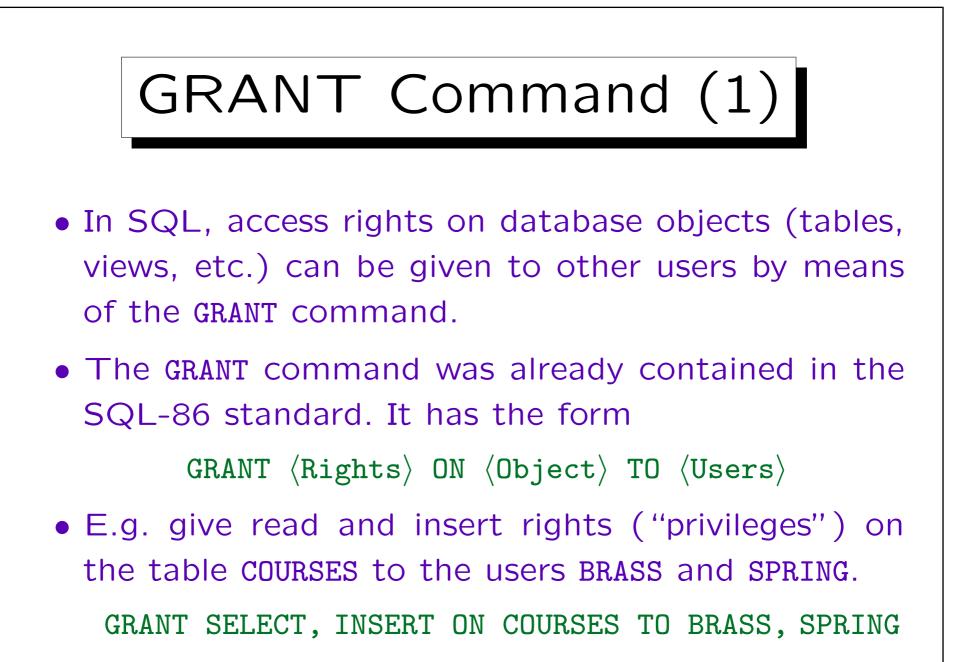
## Implicit Grants

- When a database is created, some privileges are automatically/implicitly granted to PUBLIC: CONNECT, IMPLICIT\_SCHEMA, and SELECT on the system catalog.
- One can use REVOKE to remove them from public, and then give them with GRANT to specific users.
- The user who created a database gets the following privileges automatically: DBADM, CONNECT, CREATETAB, BINDADD, IMPLICIT\_SCHEMA, CREATE\_NOT\_FENCED.

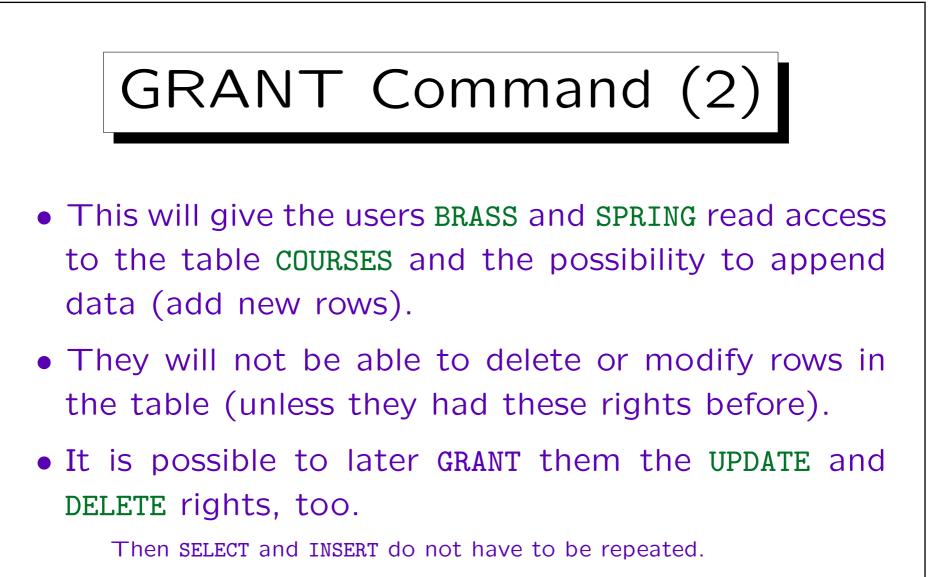
When one revokes DBADM, he still has the other privileges.



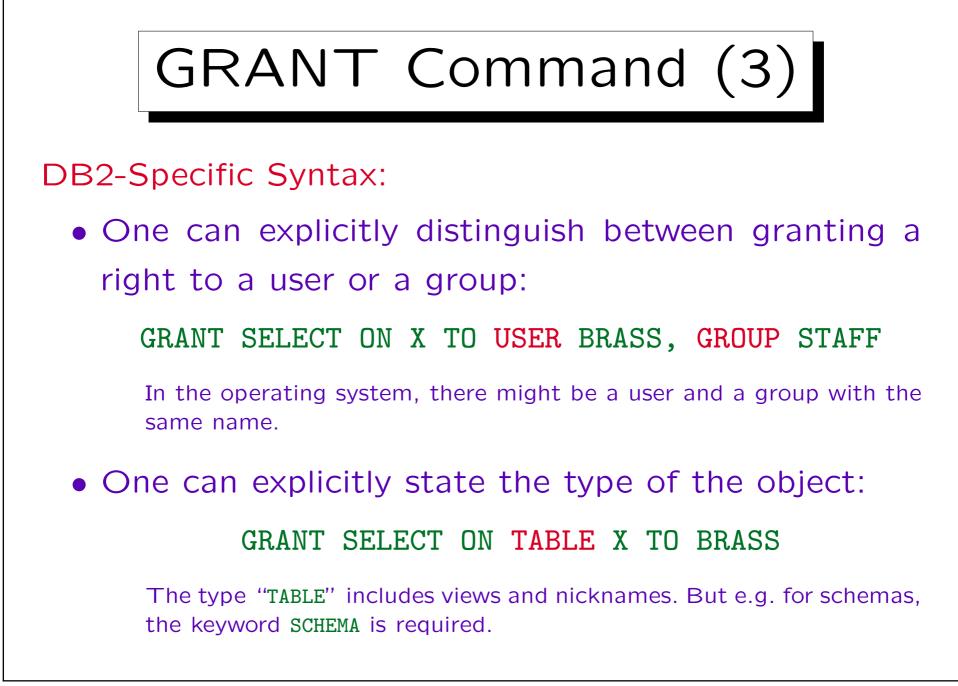
- 1. General Remarks
- 2. Authentication
- 3. DB2 Authorities and Database Privileges
- 4. Object Privileges
- 5. Label-Based Access Control

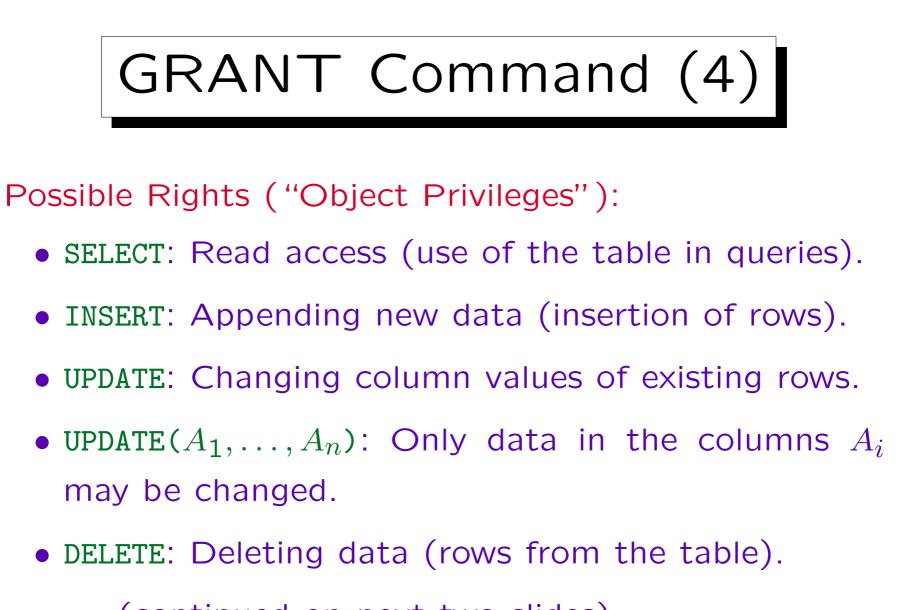


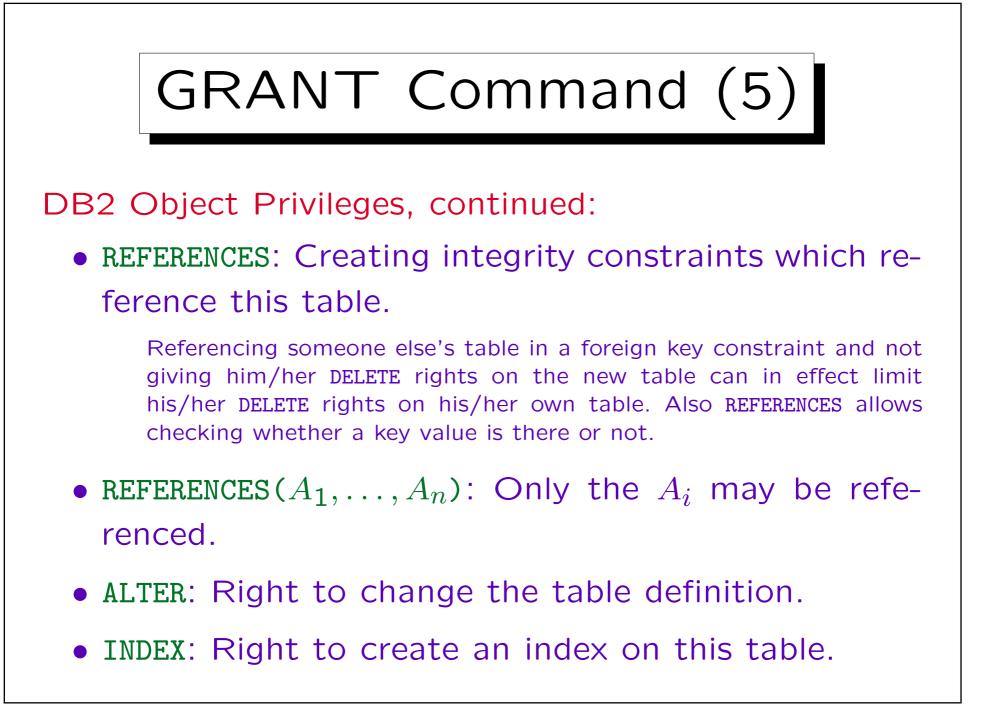
2 - 31



• The DBMS probably stores in a system table the user-command-object triples.







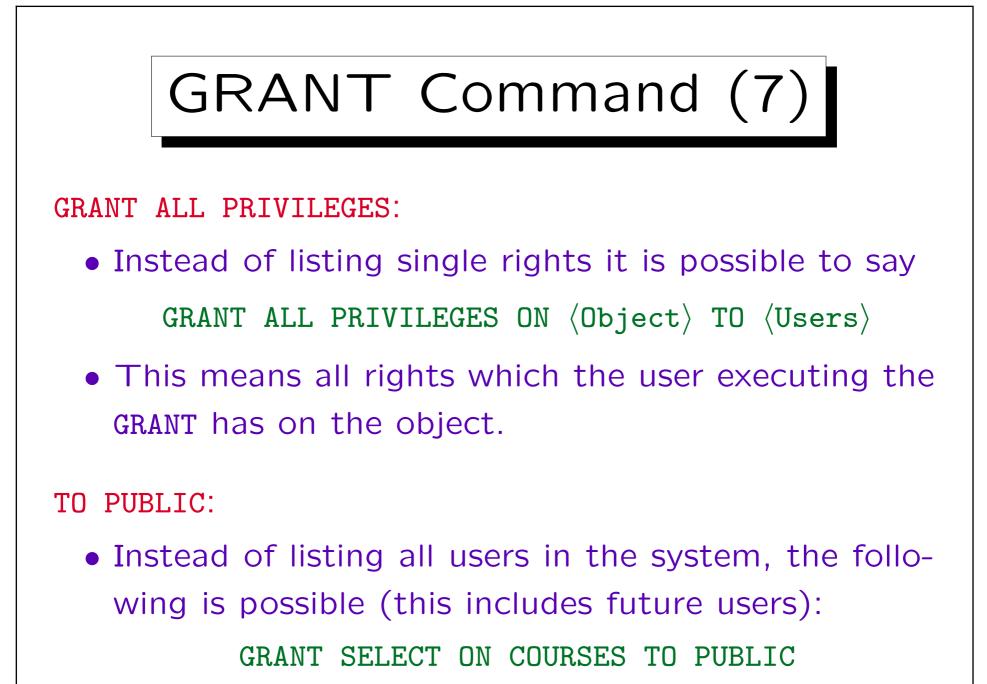


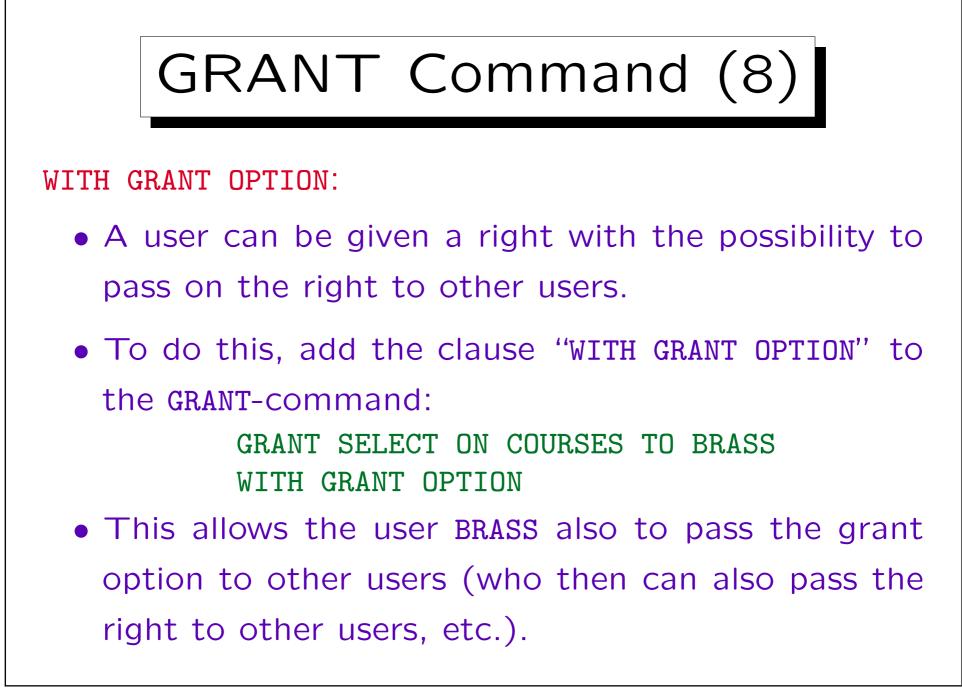
Rights for Procedures/Packages:

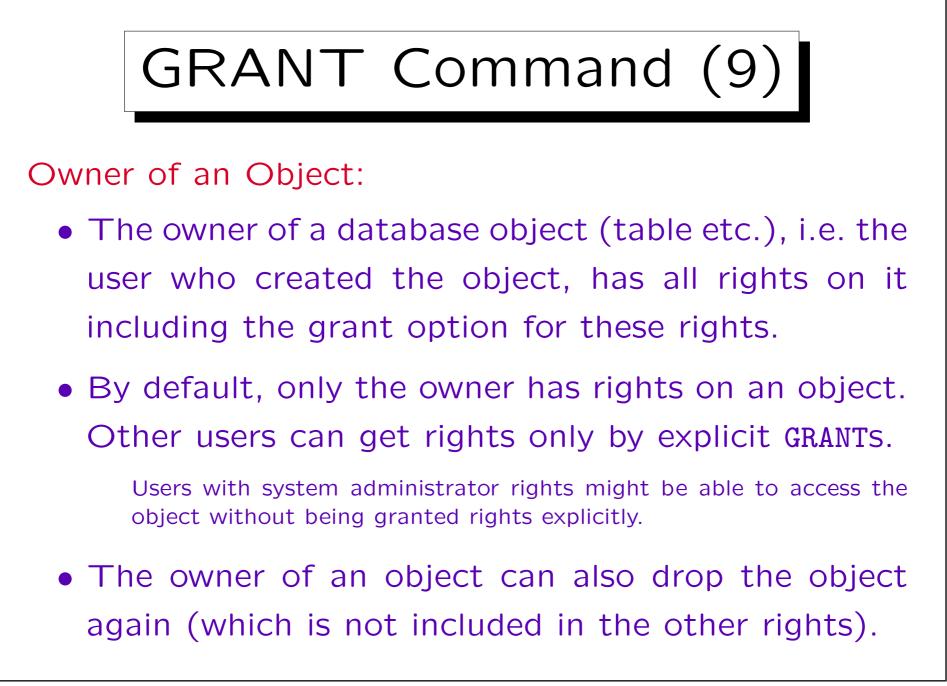
- EXECUTE: Right to execute the procedure etc.
- BIND: Reoptimize SQL statements in a package.

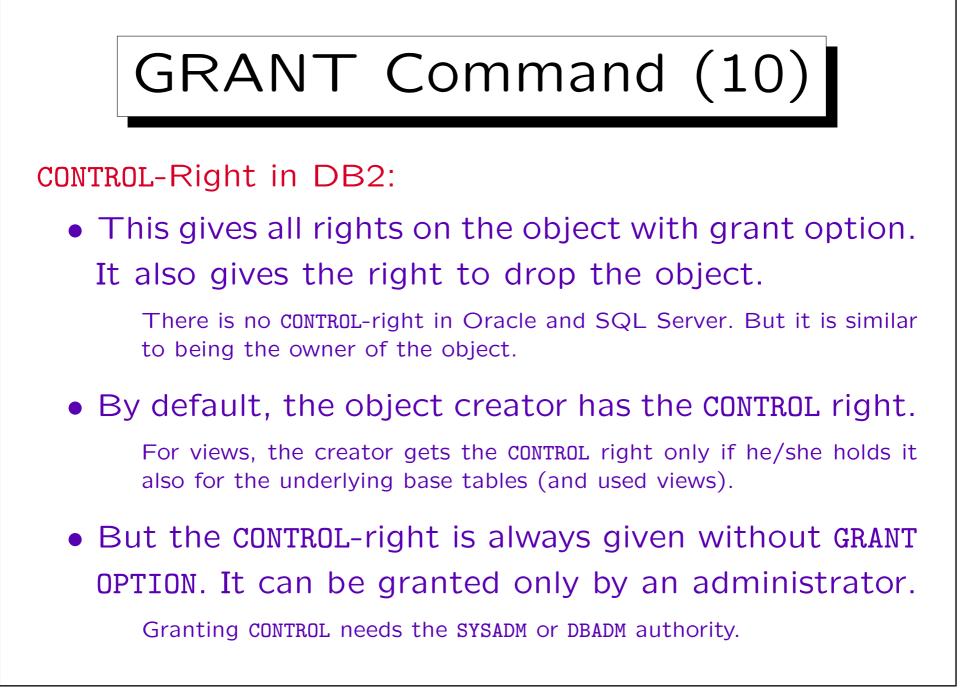
Rights for Schema Objects:

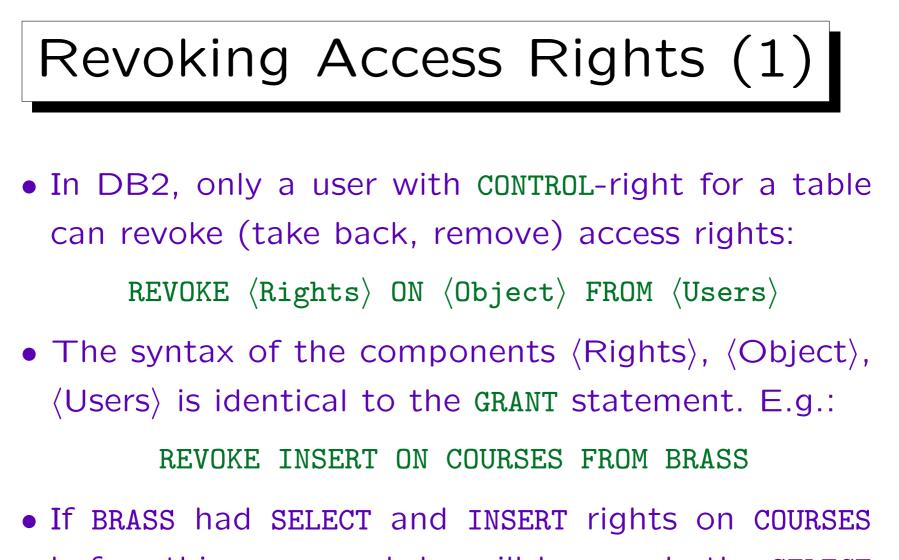
- ALTERIN: Alter any object in the schema.
- CREATEIN: Create objects in the schema.
- DROPIN: Drop any object in the schema.





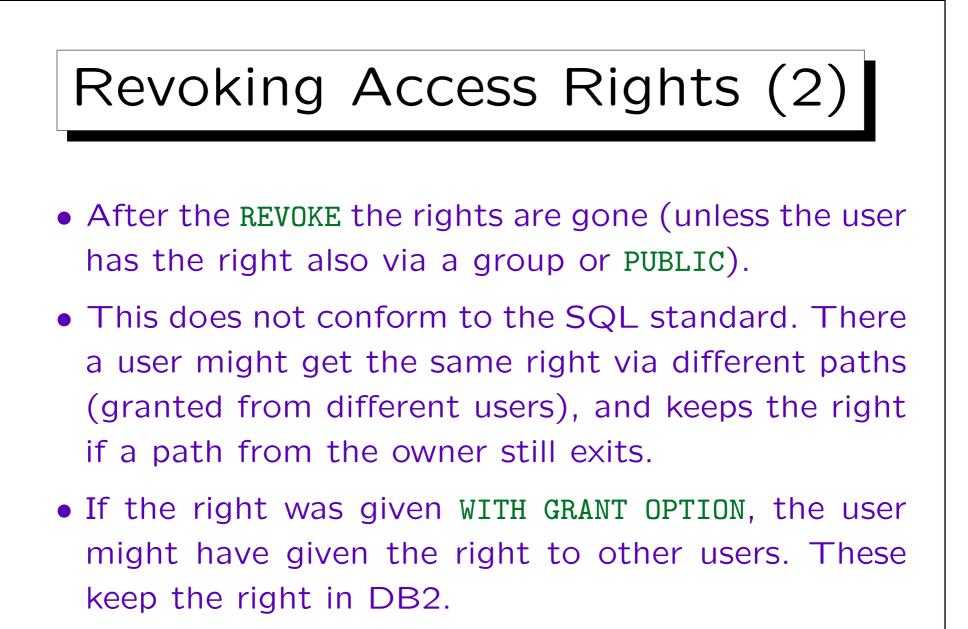




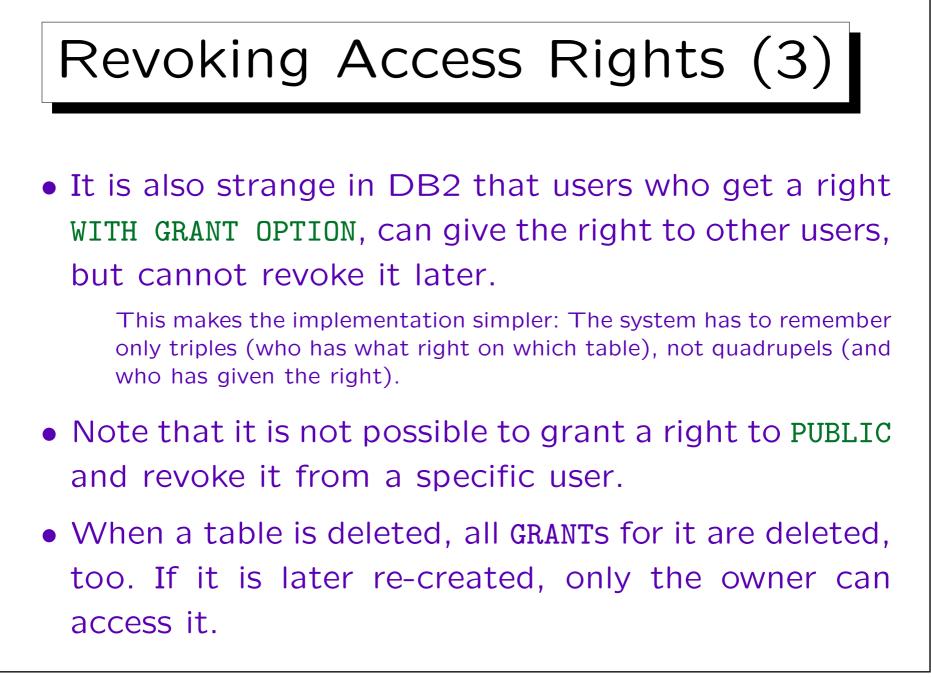


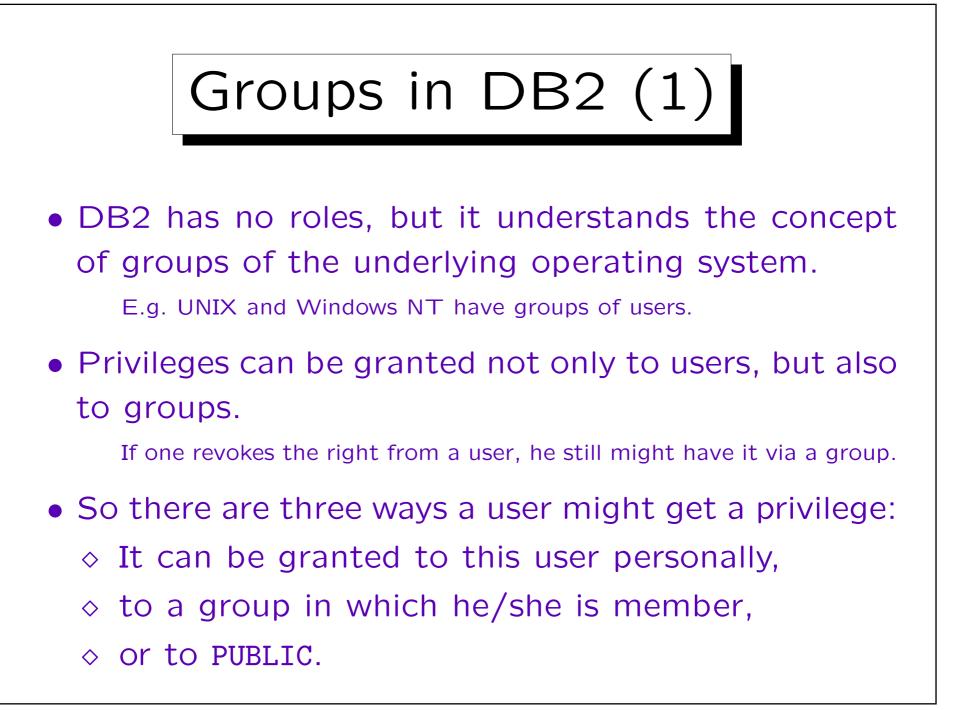
before this command, he will have only the SELECT right afterwards.

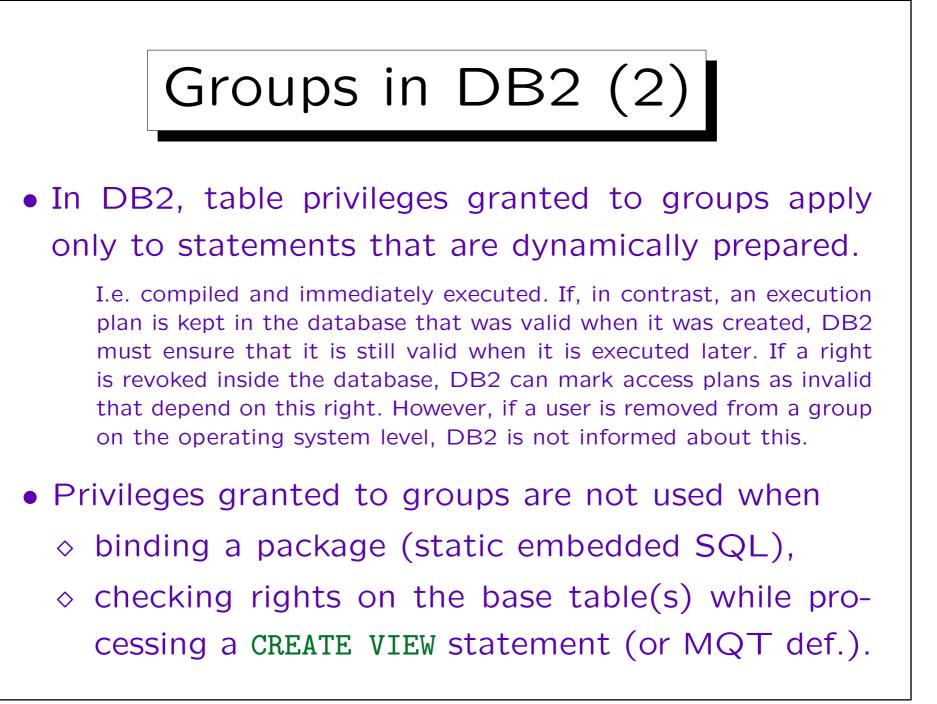
2 - 41



In the Standard, they would lose it if all paths are broken.



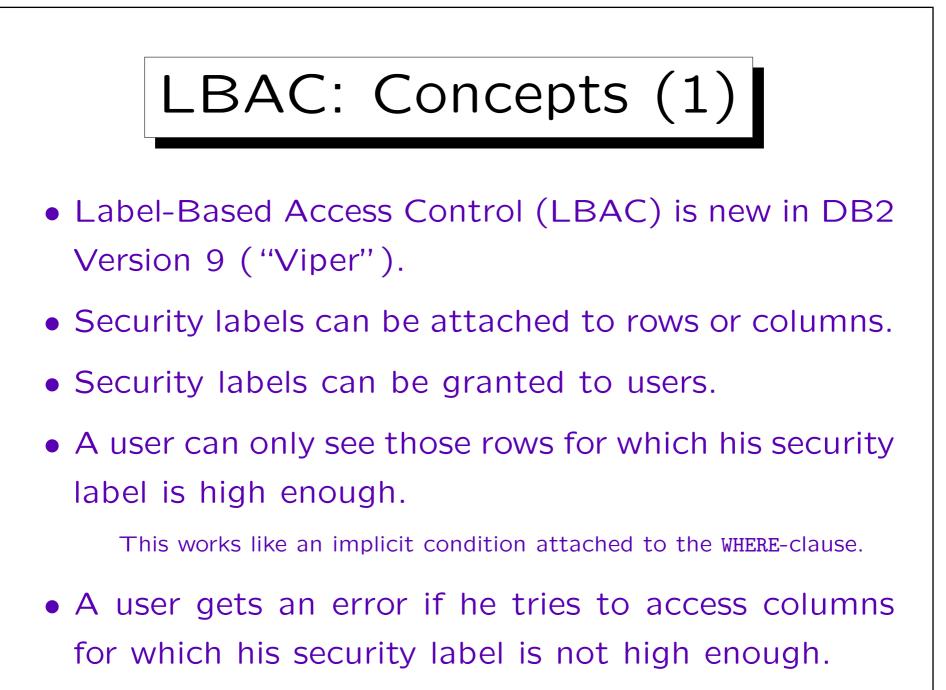


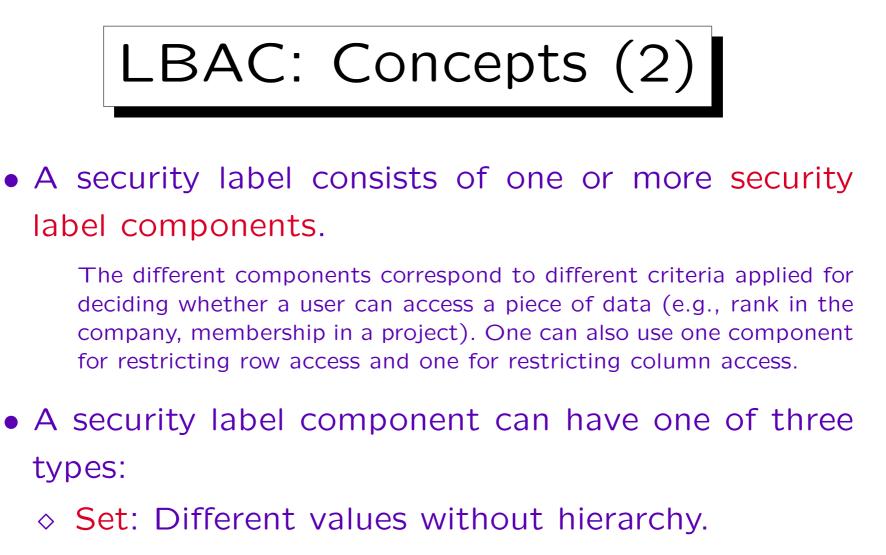




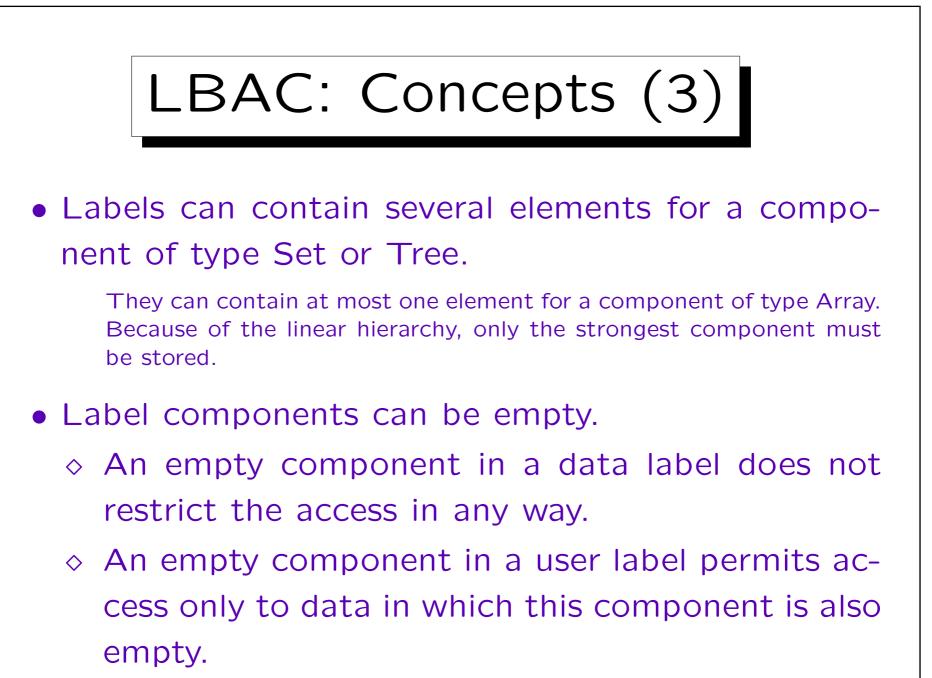
- 1. General Remarks
- 2. Authentication
- 3. DB2 Authorities and Database Privileges
- 4. Object Privileges

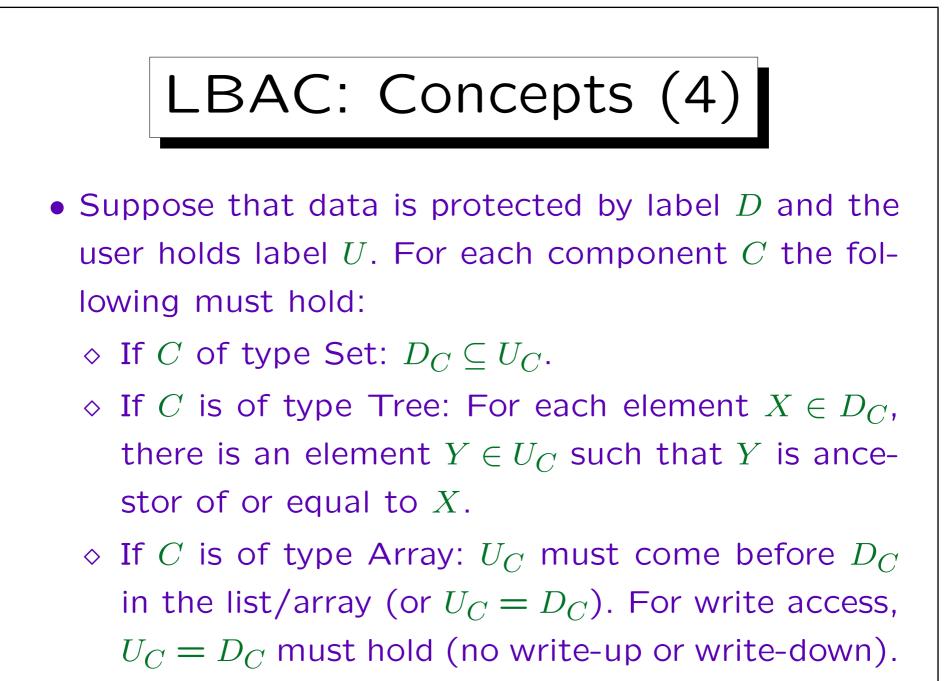
5. Label-Based Access Control

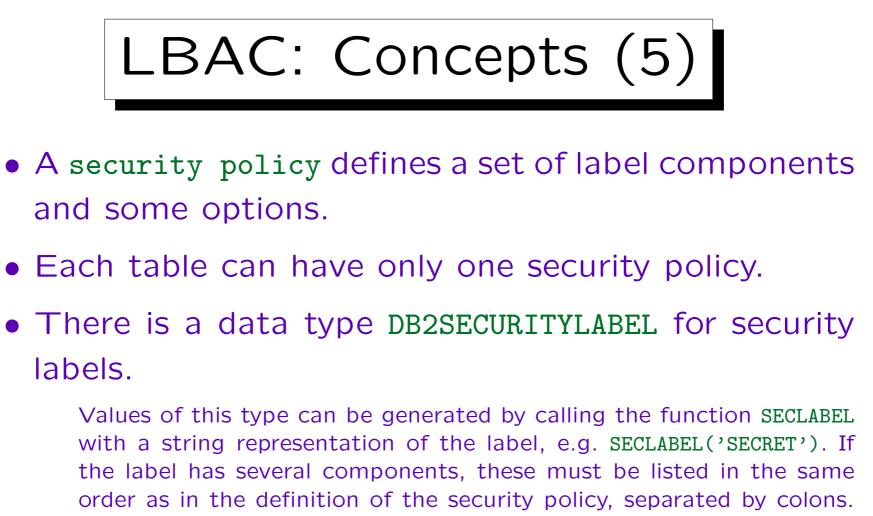




- ♦ Arrays: Different values with linear hierarchy.
- ♦ Trees: Different values with tree herarchy.

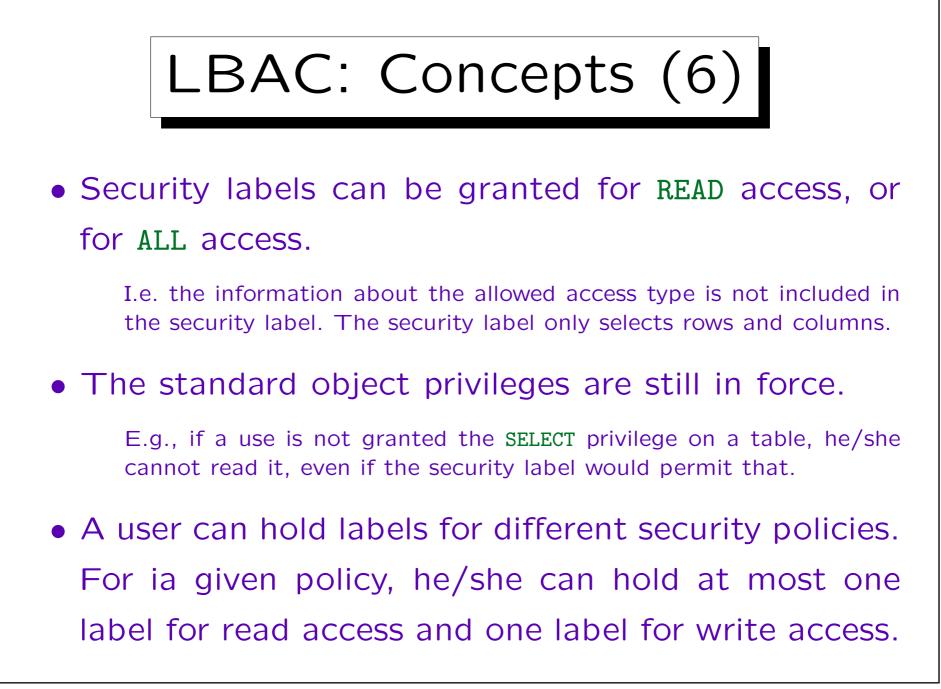


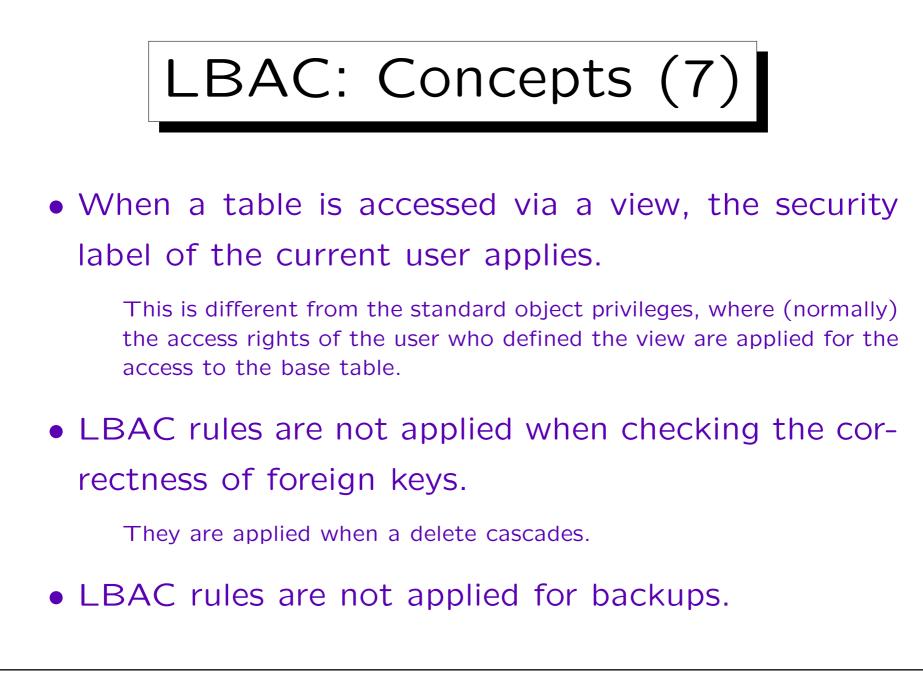




If a component has a set of values, this must be included in  $(\ldots)$ , and the elements separated by commas.

Defined (named) labels can be written as SECLABEL\_BY\_NAME('P', 'L'), where P is the policy and L is the label name.



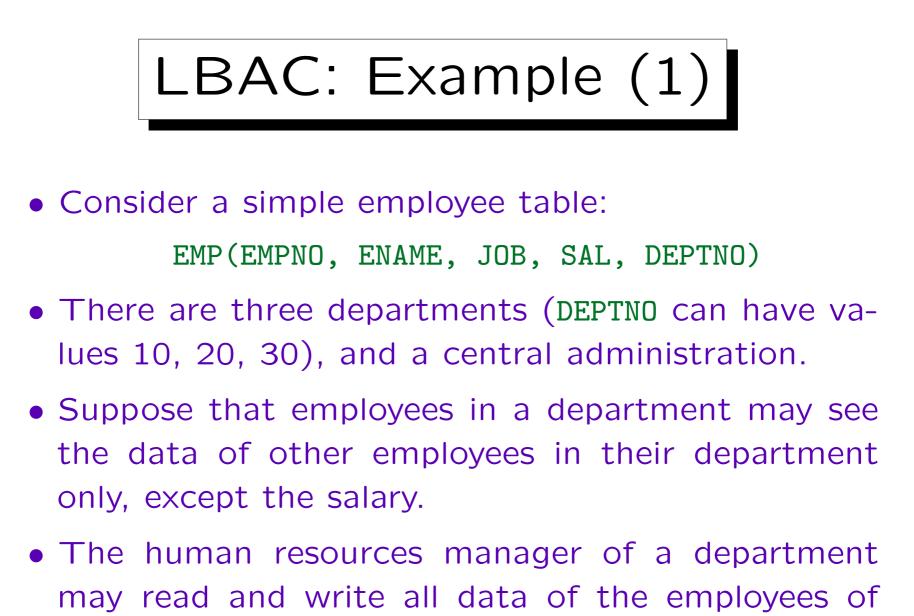


## LBAC: Concepts (8)

• Only the security administrator of the database (SECADM) can define security policies and labels.

Only SYSADM can grant SECADM. The database administrator DBADM does not automatically have SECADM.

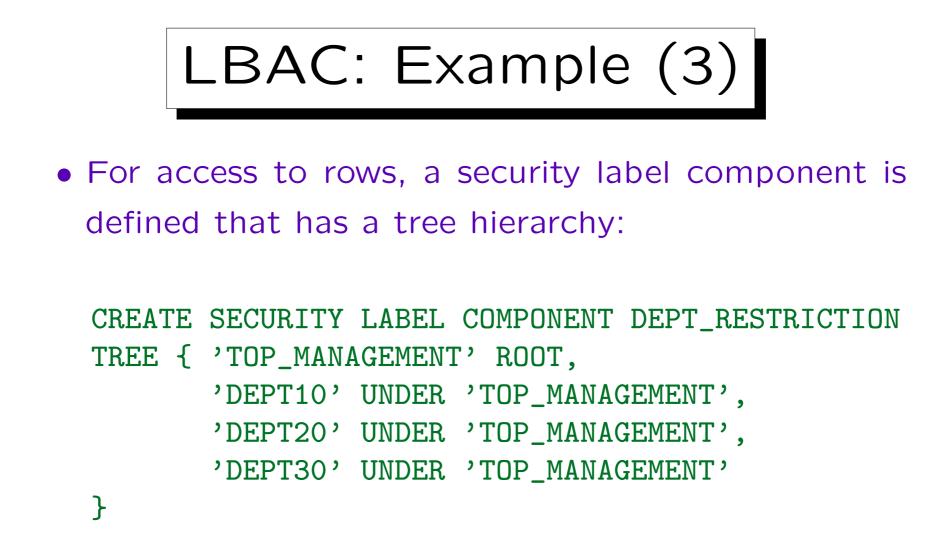
• It is possible to define exemptions for rules for the comparison of security labels.



his/her department (including the salary).

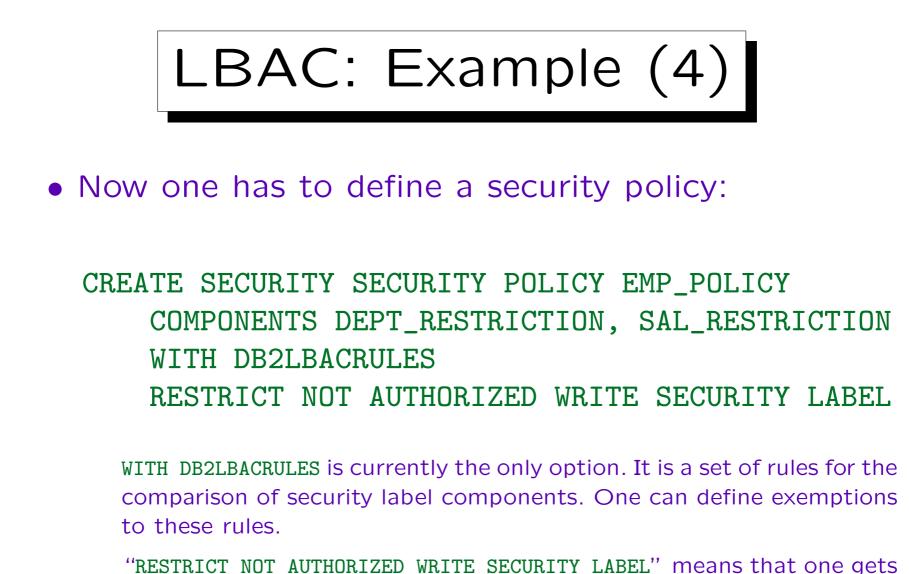
## LBAC: Example (2)

• Central administration may see data of all employees, but there are also persons who may not see the salary (i.e. the two restrictions are orthogonal).

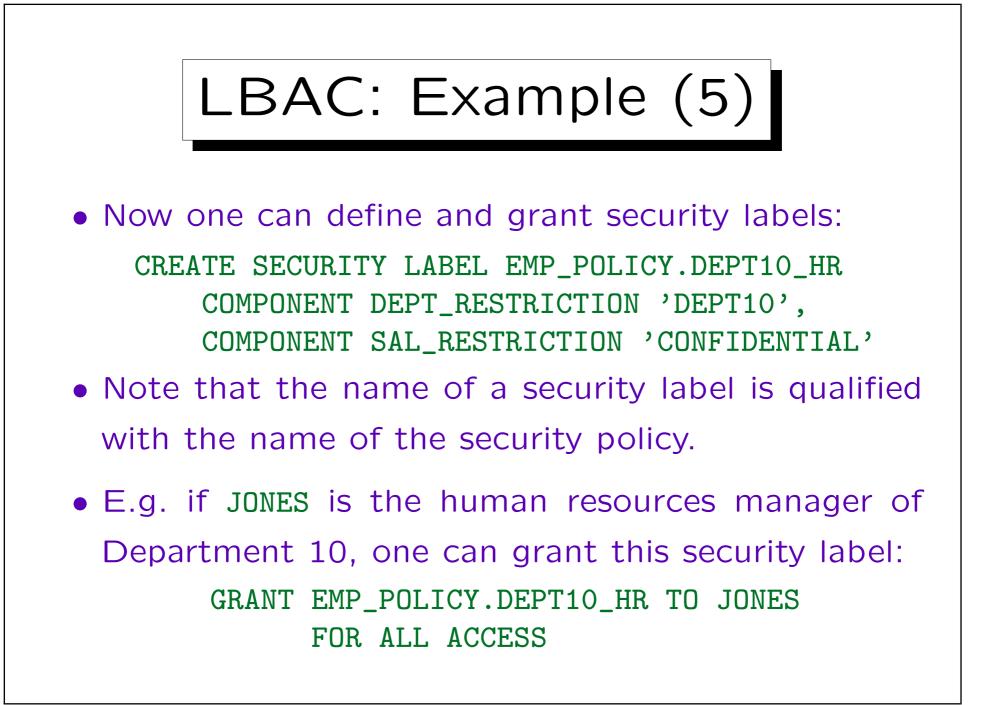


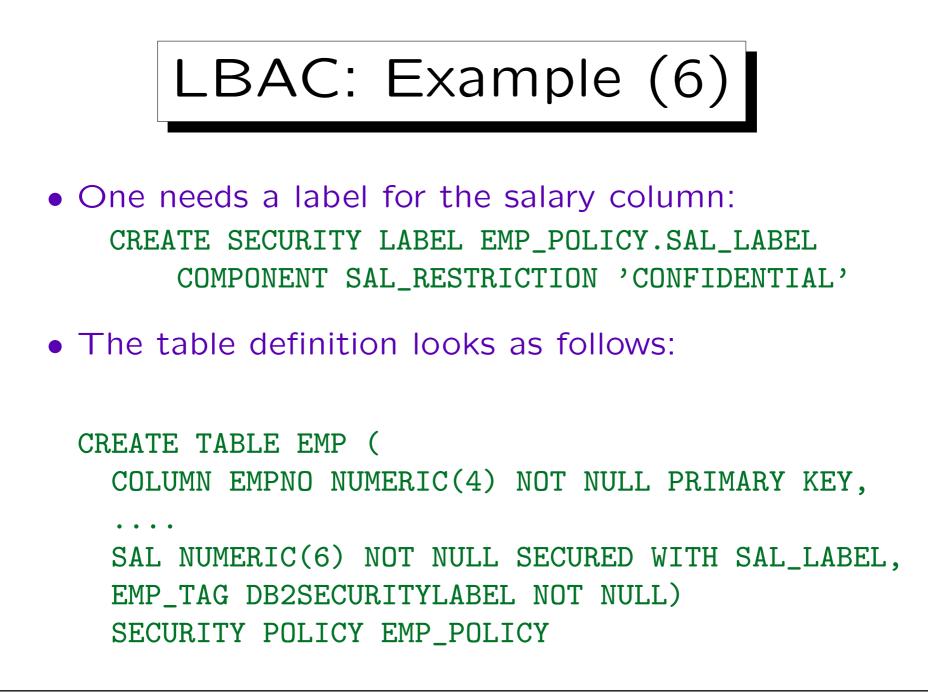
• For the salary, a single value suffices (that can be included or not included in a security label).

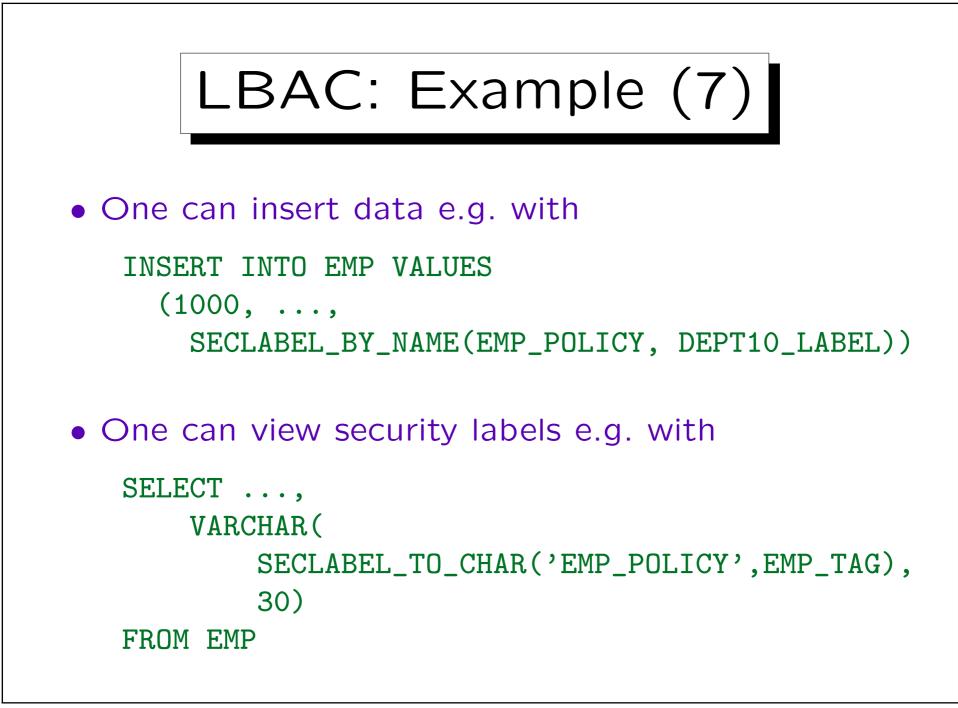
CREATE SECURITY LABEL COMPONENT SAL\_RESTRICTION
SET { 'CONFIDENTIAL' }

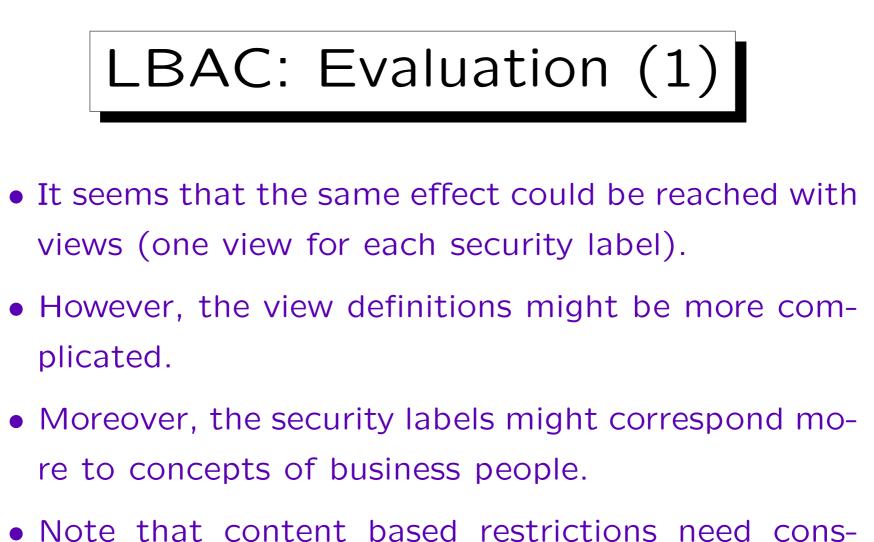


"RESTRICT NOT AUTHORIZED WRITE SECURITY LABEL" means that one gets an error if one tries to insert or update a security label for which one has no write permission. The alternative, which is also the default, is "OVERRIDE NOT AUTHORIZED WRITE SECURITY LABEL" which means that one's own security label is silently substituted in this case.









traints: One cannot use the department number itself as label.

## LBAC: Evaluation (2)

 The syntax for the common case that labels have only one component is unnecessarily complicated (one still must define labels and components separately).