CSIT115 Data Management and Security

CSIT882 Data Management Systems

Discretionary Access Control

Subject Coordinators: Dr Chen Chen, Dr Thanh Le

School of Computing and Information Technology -
University of Wollongong

Discretionary Acess Control

Outline

User management

Creating a new user

```
CREATE USER jamesb IDENTIFIED BY 'mi6';
```

Creating a user 'jamesb'

Dropping a user

```
DROP USER jamesb;
```

Dropping a user 'jamesb'

Altering a user

```
ALTER USER jamesb IDENTIFIED BY 'cia';
```

Altering a password of a user 'jamesb'

Listing the users

```
 SELECT USER FROM mysql.user;
```

Listing the names of users

```
+-----------+
| user      |
+-----------+
| csit115   |
| mysql.sys |
| root      |
+-----------+
```

Contents of mysql.user table

In HTML view press 'p' to see the lecture notes

Discretionary Acess Control

Outline

Database management

Creating a new database

Creating a database university

```
CREATE DATABASE university;
```

Dropping a database

Dropping a database university

```
DROP DATABASE university;
```

Accessing a database

Making a database university a default database and accessing a table COURSE

```
use university;
SELECT * FROM COURSE;
```

Accessing a table COURSE located at a database university

```
SELECT * FROM university.COURSE;
```

Database management

Listing all databases

Listing all databases

```
show databases;
```

Database names

```
+--------------------+
| Database           |
+--------------------+
| information_schema |
| csit115            |
| mysql              |
| ...                |
+--------------------+
```

Discretionary Acess Control

Outline

Privileges

A privilege is a right to perform an operation on a database or to access in a read or write mode a data object stored in a database

MySQL distinguishes the following groups of privileges

- Administrative (global) privileges enable the users to manage operation of the MySQL server
- Administrative privileges are global because they are not specific to a particular database

Global privileges

```
SHOW DATABASES, SHUTDOWN, PROCESS, CREATE USER, …
```

Privileges

MySQL distinguishes the following groups of privileges

- Database privileges apply to a database and to all objects within it
- Database privileges can be granted for the specific databases, or globally, so that they apply to all databases

-

Database privileges

```
CREATE, ALTER, DROP, SELECT, UPDATE, INSERT …
```

Privileges

MySQL distinguish the following groups of privileges

- Table privileges apply to a relational table and its columns
- Table privileges can be granted for the specific relational tables, or globally so that they apply to all tables in a given database

Table privileges

```
CREATE, ALTER, DROP, SELECT, UPDATE, INSERT …
```

A special privilege named `USAGE` is a synonym for no privileges granted to a user

Information about user account privileges is stored in the `user`, `db`, `tables_priv`, `columns_priv`, and `procs_priv` tables in the `mysql` database

To list all privileges we use a statement

Listing all privileges

```
show privileges;
```

Privileges

MySQL distinguish the following groups of privileges

- Column privileges apply to the columns in relational tables
- Column privilege must be followed by the column or columns, enclosed within parentheses

Column privileges

```
INSERT, REFERENCES, SELECT, UPDATE
```

Column privileges are stored in `mysql.columns_priv` table

Privileges

SQL statements `GRANT` and `REVOKE` can be used to assign/revoke the privileges to/from the database users

Granting a privilege to a user

```
GRANT privilege-type ON privilege-level TO  user[WITH GRANT OPTION];
```

Revoking a privilege from a user

```
REVOKE privilege-type ON privilege-level FROM user;
```

Revoking all privileges from a user

```
REVOKE ALL PRIVILEGES FROM user;
```

Revoking 'GRANT OPTION' privilege from a user

```
REVOKE GRANT OPTION FROM user;
```

Available privilege-types

All privileges

```
ALL,ALTER,ALTER ROUTINE,CREATE,CREATE ROUTINE,CREATE TABLESPACE,
CREATE TEMPORARY TABLES,CREATE USER,CREATE VIEW,DELETE,DROP,EVENT,EXECUTE,
FILE,GRANT OPTION,INDEX,INSERT,LOCK TABLES,PROCESS,PROXY,REFERENCES,RELOAD,
REPLICATION CLIENT,REPLICATION SLAVE,SELECT,SHOW DATABASES,SHOW VIEW,
SHUTDOWN,SUPER,TRIGGER,UPDATE,USAGE
```

In HTML view press 'p' to see the lecture notes

Privileges

The following privilege-levels are available: global privileges, database privileges, table privileges, column privileges

Global privileges are administrative privileges or apply to all databases on a given server

Global privileges are denoted by `*.*`

```
                                    Granting 'SELECT' privilege on all databases and all tables in the databases
GRANT SELECT ON *.* TO James;
                                      Granting all privileges on all databases and all tables in the databases
GRANT ALL ON *.* TO Harry;
                                     Granting 'USAGE' privilege on all databases and all tables in the databases
GRANT USAGE ON *.* TO Robin;
                                                                    Granting 'CREATE USER' privilege
GRANT CREATE USER ON *.* TO James;
                                                                  GRANTING 'SHOW DATABASES' privilege
GRANT SHOW DATABASES ON *.* TO James;
```

In HTML view press 'p' to see the lecture notes

Privileges

The following privileges can be granted only globally

Global privileges

```
CREATE TABLESPACE,CREATE USER,FILE,PROCESS,RELOAD,
REPLICATION CLIENT,REPLICATION SLAVE,SHOW DATABASES,SHUTDOWN,SUPER
```

Global privileges are stored in `mysql.user` table or in `information_schema.user_privileges` table

Privileges

The following privilege-levels are available: global privileges, database privileges, table privileges, column privileges

Database privileges are privileges that apply to all objects in a given database

Database privileges are denoted by `database-name.*`

```
Granting 'SELECT' privilege on all tables in 'csit115' database
GRANT SELECT ON csit115.* TO James;
```

```
Granting all privileges on all tables in 'university' database
GRANT ALL ON university.* TO Harry;
```

```
Granting write privileges on all tables in 'csit115' database
GRANT INSERT, UPDATE, DELETE on csit115.* TO Robin;
```

```
Granting 'GRANT OPTION' privileges on 'csit115' database
GRANT GRANT OPTION on csit115.* TO Robin;
```

Privileges

The following privileges are allowed at a database level

Database privileges

```
CREATE,DROP,EVENT,GRANT OPTION,LOCK TABLES,REFERENCES
```

Database privileges are stored in `mysql.db` table or in `information_schema.schema_privileges` table

Privileges

The following privilege-levels are available: global privileges, database privileges, table privileges, column privileges

Table privileges are privileges that apply to apply to all columns in a given table

Table privileges are denoted by `database-name.table-name`

```
                                    Granting 'SELECT' privileges on 'DRIVER' table in 'csit115' database
GRANT SELECT ON csit115.DRIVER TO James;
```

```
                                     Granting all privileges on 'COURSE' table in 'university' database
GRANT ALL ON university.COURSE TO Harry;
```

```
                                    Granting write privilege on 'ORDERS' table in 'university' database
GRANT INSERT, UPDATE, DELETE on csit115.ORDERS TO Robin;
```

```
                                    Granting 'GRANT OPTION' privileges on 'DRIVER' table in 'csit115' database
GRANT GRANT OPTION on csit115.DRIVER TO Robin;
```

Privileges

The permissible privileges at the table level are the following

Table privileges

```
ALTER,CREATE VIEW,CREATE,DELETE,DROP,GRANT OPTION,INDEX,INSERT,
REFERENCES,SELECT,SHOW VIEW,TRIGGER,UPDATE
```

Table privileges are stored in `mysql.tables_priv` table or in `information_schema.table_privileges` table

Privileges

The following privilege-levels are available: global privileges, database privileges, table privileges, column privileges

Column privileges are privileges that apply to apply to selected columns in a given table

Column privileges are denoted by
`(column-1, ... , column-n) ON database-name.table-name`

```
                    Granting 'SELECT' privilege on a column 'LNUM' in 'DRIVER table in 'csit115' table
GRANT SELECT (LNUM) ON csit115.DRIVER TO James;
```

```
                    Granting 'INSERT' privilege on the columns 'sname' and 'level' in 'SKILL' table in
                    'university' database

GRANT INSERT (sname, level) ON university.SKILL TO Harry;
```

```
                  Granting 'UPDATE' and 'REFERENCES' privileges on a column 'ordernum' in 'ORDERS' table in
                  'csit115' database

GRANT UPDATE(ordernum), REFERENCES (ordernum) on csit115.ORDERS TO Robin;
```

Privileges

The permissible privileges at the column level are the following

```
INSERT,REFERENCES,SELECT,UPDATE
```
Column privileges

Column privileges are stored in `mysql.columns_priv` table or in `information_schema.column_privileges` table

Discretionary Acess Control

Outline

Roles

A role is a named group of privileges

Roles are very useful when a group of privileges must be granted to a continuously increasing group of users

For example, assume, that user `James` must be granted a read privilege on a relational table `ITEM` and a write privilege on a relational table `ORDERS`

```
GRANT SELECT ON ITEM TO James;                Granting a read privilege on a table 'ITEM' to 'James'

                                          Granting a write privilege on a table 'ORDERS' to 'James'
GRANT INSERT, UPDATE, DELETE ON ORDERS TO James;
```

Now, assume that the same privileges must be granted to a user Kate

Then, we have to repeat both `GRANT` statements

```
GRANT SELECT ON ITEM TO Kate;                Granting a read privilege on a table 'ITEM' to 'Kate'

                                           Granting a write privilege on a table 'ORDERS' to 'Kate'
GRANT INSERT, UPDATE, DELETE ON ORDERS TO Kate;
```

In HTML view press 'p' to see the lecture notes

Roles

If the same privileges must be granted to another 100 users then we have to repeat `GRANT` statements 200 times

Instead, we can create a role `CUSTOMER` and grant it both privileges

```
CREATE ROLE CUSTOMER;
```

Create role 'CUSTOMER'

```
GRANT SELECT ON ITEM TO CUSTOMER;
GRANT INSERT, UPDATE, DELETE ON ORDERS TO CUSTOMER;
```

Granting the privileges to a role 'CUSTOMER'

And then grant a role `CUSTOMER` to `James` and `Kate`

```
GRANT CUSTOMER TO James;
GRANT CUSTOMER TO Kate;
```

Granting a role 'CUSTOMER' to 'James' and 'Kate'

Next 100 users can be granted in the same way a single role `CUSTOMER`

A concept of a role allows for simplification of discretionary access control

Any modification to a role `CUSTOMER` also affects the privileges of the users who have been granted a role `CUSTOMER`

In HTML view press 'p' to see the lecture notes

Roles

A role can be granted to another role creating a hierarchy of privileges

For example, assume that role `FREQUENT_CUSTOMER` must possess all privileges of a role `CUSTOMER` and additionally a `write` privilege on a relational table `DISCOUNT`

```
                                                    Create role 'FREQUENT_CUSTOMER'
CREATE ROLE FREQUENT_CUSTOMER;
```

```
                          Granting write privileges on a table 'DISCOUNT' to a role 'FREQUENT_CUSTOMER'
GRANT INSERT, UPDATE, DELETE ON DISCOUNT TO FREQUENT_CUSTOMER;
```

```
                                        Granting a role 'CUSTOMER' to a role 'FREQUENT_CUSTOMER'
GRANT CUSTOMER TO FREQUENT_CUSTOMER;
```

Grant a role `FREQUENT_CUSTOMER` to a user `Harry`

```
                                                 Granting a role 'FREQUENT_CUSTOMER' to a user 'Harry'
GRANT FREQUENT_CUSTOMER TO Harry;
```

Any modifications to a role `CUSTOMER` will be inherited by a role `FREQUENT_CUSTOMER`

In HTML view press 'p' to see the lecture notes

Discretionary Acess Control

Outline

Applications

Immediately after installation of the system there is one user `root` with no password and with all privileges granted

A user `root` connects without a password and sets up a new password

Connecting as a user 'root'

```
mysql -u root
```

Changing a password of a user 'root'

```
ALTER USER root IDENTIFIED BY 'root';
```

A user `root` creates a new user `jamesb`

Creating a new user

```
CREATE USER jamesb IDENTIFIED BY 'jamesb';
```

Applications

User `jamesb` has no privileges

Listing the privileges of a user 'jamesb'

```
SELECT user, select_priv, insert_priv, update_priv, delete_priv
FROM mysql.user
WHERE user='jamesb';
```

Privileges of a user 'jamesb'

```
+--------+-------------+-------------+-------------+-------------+
| user   | select_priv | insert_priv | update_priv | delete_priv |
+--------+-------------+-------------+-------------+-------------+
| jamesb | N           | N           | N           | N           |
+--------+-------------+-------------+-------------+-------------+
```

Applications

A user `root` grants all privileges to a user `jamesb` on all databases without `GRANT OPTION`

Granting all provileges on all tables in all databases to a user 'jamesb'

```
GRANT ALL ON *.* to jamesb;
```

User `jamesb` has all privileges but he/she cannot grant any privileges

Listing 'SELECT', 'INSERT', 'UPDATE', 'DELETE', and 'GRANT' privileges of a user 'jamesb'

```
SELECT select_priv, insert_priv, update_priv, delete_priv, grant_priv
FROM mysql.user
WHERE user='jamesb';
```

'SELECT', 'INSERT', 'UPDATE', 'DELETE', and 'GRANT' privileges of a user 'jamesb'

```
+--------+-------------+-------------+-------------+-------------+------------+
| user   | select_priv | insert_priv | update_priv | delete_priv | grant_priv |
+--------+-------------+-------------+-------------+-------------+------------+
| jamesb | Y           | Y           | Y           | Y           | N          |
+--------+-------------+-------------+-------------+-------------+------------+
```

Applications

A user `root` creates a database `mi6`

```
Creating a new database
CREATE DATABASE mi6;
```

A user jamesb connects to a database `mi6` and makes it a default database

```
Connecting as a user 'jamesb'
mysql –u jamesb –p –v –c
```

```
use mi6;
Making a database 'mi6' a default database
```

A user `jamesb` creates the relational tables `DEPARTMENT` and `COURSE`

A user `jamesb` has all privileges on the tables created

A user `root` has all privileges on the tables created by a user `jamesb`

Applications

A user `root` tests some privileges on the tables created by a user `jamesb`

Reading from 'DEPARTMENT' table in 'mi6' database

```
SELECT * FROM mi6.DEPARTMENT;
```

Deleting from 'COURSE' table in 'mi6' database

```
DELETE FROM mi6.COURSE;
```

A user `root` creates a new user `harryp`

Creating a new user

```
CREATE USER harryp IDENTIFIED BY 'harryp';
```

A user `root` grants to a user `harryp` a privilege `SELECT` (read) on all tables in a database `mi6`

Granting 'SELECT' privilege on all tables in 'mi6' database

```
GRANT SELECT ON mi6.* TO harryp;
```

Applications

A user `harryp` has a privilege `SELECT` on a database `mi6`

Listing 'SELECT', 'INSERT', 'DELETE' privileges of a user 'harryp' on a database 'mi6'

```
SELECT user, db, select_priv, insert_priv, delete_priv, update_priv
FROM mysql.db
WHERE user='harryp';
```

'SELECT', 'INSERT', 'DELETE' privileges of a user 'harryp' on a database 'mi6'

```
+--------+-----+-------------+-------------+-------------+-------------+
| user   | db  | select_priv | insert_priv | update_priv | delete_priv |
+--------+-----+-------------+-------------+-------------+-------------+
| harryp | mi6 | Y           | N           | N           | N           |
+--------+-----+-------------+-------------+-------------+-------------+
```

A user `root` grants to a user `harryp` the privileges `INSERT`, `UPDATE`, and `DELETE` (write) on `all tables` in a database `csit115`

Granting 'INSERT', 'UPDATE', 'DELETE' privileges on all tables in 'csit115' database

```
GRANT INSERT, UPDATE, DELETE ON csit115.* TO harryp;
```

Applications

A user `harryp` has `INSERT`, `UPDATE`, and `DELETE` (write) privileges on `all tables` in a database `csit115`;

Listing 'SELECT', 'INSERT', 'DELETE' privileges of a user 'harryp' on the databases 'mi6'and 'csit115'

```
SELECT user, db, select_priv, insert_priv, delete_priv, update_priv
FROM mysql.db
WHERE user='harryp';
```

'SELECT', 'INSERT', 'DELETE' privileges of a user 'harryp' on the databases 'mi6'and 'csit115'

```
+--------+---------+-------------+-------------+-------------+-------------+
| user   | db      | select_priv | insert_priv | update_priv | delete_priv |
+--------+---------+-------------+-------------+-------------+-------------+
| harryp | mi6     | Y           | N           | N           | N           |
| harryp | csit115 | N           | Y           | Y           | Y           |
+--------+---------+-------------+-------------+-------------+-------------+
```

Applications

A user `root` grants to a user `jamesb` the privileges `UPDATE` and `DELETE` on a table `DEPARTMENT` in a database `csit115`;

Granting 'UPDATE', 'DELETE' privileges on 'DEPARTMENT' table in 'csit115' database

```
GRANT UPDATE, DELETE ON csit115.DEPARTMENT TO jamesb;
```

Listing table privileges of 'jamesb' user

```
SELECT user, db, table_name, table_priv
FROM mysql.tables_priv
WHERE user='jamesb';
```

Table privileges of 'jamesb' user

```
+--------+---------+------------+----------------+
| user   | db      | table_name | table_priv     |
+--------+---------+------------+----------------+
| jamesb | csit115 | DEPARTMENT | Update,Delete |
+--------+---------+------------+----------------+
```

Applications

A user `root` grants to a user `jamesb` a privilege `REFERENCES` on a column `DNAME` in `DEPARTMENT` table in a database `csit115`;

Granting 'REFERENCE' provilege on 'DNAME' column in 'DEPARTMENT' table in 'csit115' database

```
GRANT REFERENCES (DNAME) ON csit115.DEPARTMENT TO jamesb;
```

Listing column privileges of a user 'jamesb'

```
SELECT user, db, table_name, column_name, column_priv
FROM mysql.columns_priv
WHERE user='jamesb';
```

Column privileges of a user 'jamesb'

```
+--------+---------+------------+-------------+--------------+
| user   | db      | table_name | column_name | column_priv  |
+--------+---------+------------+-------------+--------------+
| jamesb | csit115 | DEPARTMENT | DNAME       | References   |
+--------+---------+------------+-------------+--------------+
```

Applications

A user `csit115` creates a relational view `ITDEPT` in a database `csit115`

Creating a relational view

```
CREATE VIEW ITDEPT(DNAME, BUDGET, CHAIRMAN)
AS (SELECT *
    FROM DEPARTMENT
    WHERE DNAME='IT');
```

A user `root` grants to a user `jamesb` a privilege `INSERT` on a view `ITDEPT` in a database `csit115`;

Granting 'INSERT' privilege on 'ITDEPT' view in 'csit115' database

```
GRANT INSERT ON csit115.ITDEPT TO jamesb;
```

Applications

A user `jamesb` has a privilege `INSERT` on a view `ITDEPT` in a database `csit115`;

Listing table privileges of a user 'jamesb'

```
SELECT user, db, table_name, table_priv
FROM mysql.tables_priv
WHERE user='jamesb';
```

Table privileges of a user 'jamesb'

```
+--------+---------+------------+----------------+
| user   | db      | table_name | table_priv     |
+--------+---------+------------+----------------+
| jamesb | csit115 | DEPARTMENT | Update,Delete |
| jamesb | csit115 | ITDEPT     | Insert         |
+--------+---------+------------+----------------+
```

References

C. Coronel, S. Morris, A. Basta, M. Zgola, Data Management and Security, Chapter 9, Cengage Compose eBook, 2018, eBook: Data Management and Security, 1st Edition

T. Connoly, C. Begg, Database Systems, A Practical Approach to Design, Implementation, and Management, Chapter 7.6 Discretionary Access Control, Pearson Education Ltd, 2015

How to ... ? Cookbook, How to manage discretionary access control ? Recipes 9.1 and 9.2

MySQL 8.0 Reference Manual, https://protect-au.mimecast.com/s/VggDCr81kkt6lj8nCycpF-?domain=13.7.1.6 GRANT Syntax

MySQL 8.0 Reference Manual, https://protect-au.mimecast.com/s/rHqrCwV1ppHP3QGVu8z8Rh?domain=13.7.1.8 REVOKE Syntax