SECURICHT
DESIGNED AND BUILT WITH MYSQL IN MIND

Darren Cassar B.Eng(Hons.) CMDBA LMIPP LSWPP
Data Losses

- Malicious v.s. Accidental
- Insider v.s. Outsider
- Businesses – Governments – Educational Institutes
- Types of losses:
  - Financial (acc nos/ cc nos)
  - Medical
  - Location
  - Social Security Numbers
  - Email Addresses
TO US
DATA IS SACRED
WE NEED TO PROTECT IT
User management

- How often do we audit user privileges and access levels?
- Do we forget to remove temporary privileges once the user is done with the task?
- How fast do we revoke access to former employees or compromised users?
MySQL security model

Privileges checking hierarchy

<table>
<thead>
<tr>
<th>Level</th>
<th>Permissions</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER</td>
<td>GRANTED - EXECUTE QUERY, DENIED check db table</td>
</tr>
<tr>
<td>DB</td>
<td>GRANTED - EXECUTE QUERY, DENIED check tables_priv table</td>
</tr>
<tr>
<td>TABLES</td>
<td>GRANTED - EXECUTE QUERY, DENIED check columns_priv table</td>
</tr>
<tr>
<td>COLUMNS</td>
<td>GRANTED - EXECUTE QUERY, DENIED - BLOCK</td>
</tr>
</tbody>
</table>
MySQL Security Model (PROS)

- Authentication against 'username'@'hostname'
- Password hashed by PASSWORD() function
- Wide range of privileges
- Intelligent control for requests of granting privileges (can’t grant what user doesn’t already have privileges on etc)
MySQL Security Model

Quotes from “High Performance MySQL 2nd Ed”

"..... MySQL doesn’t provide any functionality for **user groups or roles**, as they’re variously known in other database servers ..... "

"..... MySQL also doesn’t provide any way for an administrator to **enforce good password standards** ..... "
MySQL Security Model (LIMITS)

- Passwords limits are not available
  - No password size limit
  - No password history
  - No password complexity meter
  - No password minimum age
- Complex to manage
- No Roles
- Easily unsecured
- Obsolete grants are not removed
MySQL Security Model (SECURICH)

- Passwords limits are not available **PROVIDED**
  - No password size limit
  - No password history
  - No password complexity meter
  - No password minimum age

- Complex to manage **IMPROVED**

- No Roles **PROVIDED**

- Easily unsecured **SECURED**

- Obsolete grants are not removed **W.I.P**
PROS

- Open source
- Easily pluggable / un-pluggable
- Doesn’t remove any prior functionalities
- Enables roles
- Enables reserved usernames
- Enhances password security
- Enables user cloning
- Strengthens MySQL security model weaknesses
- Very easy to install, upgrade, manage and uninstall
PROS

• Lightweight – Doesn’t require special resources
• Self explanatory design
• Compatible with MySQL 5.0 onwards
• Friendlier display of `show grants`
• Embedded `help` - documentation
• Dynamic roles
• Enables temporary block and unblock user
• Stores user creation date and time
• Assumes no_auto_create
PROS

- Enables granting privileges on tables using regexp
- Enables revoking privileges on tables using regexp
- Outputs suggestions if error is encountered
- Option to kill user connections when revoking privileges
- Doesn’t permit grants to the ‘mysql’ database
- It doesn’t need Perl or other kind of compilers / interpreters.
LIMITATIONS

- Password length and complexity is not configurable
- Doesn’t work on versions 4.1 and earlier because it uses the information_schema and new password hashing
- Doesn’t support column level privileges (future feature)
- Doesn’t support functions privileges (works in progress)
- Can’t be installed on existing MySQL instances which already contain users (future feature)
- Emailing user about password expiry is in bash (not SQL)
- No GUI tools (Anybody in for it?)
Password setting by user requires old password (avoiding illegitimate password resetting)

Password needs to be not less than eight characters (not configurable yet)

Password complexity requires at least:
  - One letter
  - One number
  - One special character

Password history stores last five passwords

Password complexity is only NOT obeyed when password is changed by root
root@minime:/home/dcassar/securich_install# ./securich_install.sh

brought to you by Darren Cassar
http://www.mysqlpreacher.com

Enter version number (default 0.1.4 i.e. latest version):
Which kind of installation would you like to do?
1. Install from file on disk
2. Download and install (recommended)
Enter choice (default 2):
Installation starting
Resolving www.securich.com... 64.202.163.10
Connecting to www.securich.com|64.202.163.10|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 83494 (82K) [application/x-tar]
Saving to: 'securich.0.1.4.tar.gz'

100%[============================================>]
63,494 46.9K/s in 1.7s

2009-08-22 16:29:57 (48.9 KB/s) - ‘securich.0.1.4.tar.gz’ saved [83494/83494]
Do you wish to:
1. Do a fresh install
2. Upgrade from a previous version
Enter choice (default 1):

Enter mysql root Password (default ''): Would you like to connect using:
1. TCP/IP
2. Socket file

Enter choice (default 1):

Enter mysql Hostname/IP (default '127.0.0.1'):
Enter mysql Port (default '3306'): 5137

Installation complete

root@minime:/home/dassar/securich_install#
### Securich first appearance

```sql
mysql Sat Aug 21 16:38:08 2009 > show databases;
+--------------------+| Database           |
<table>
<thead>
<tr>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>information_schema</td>
</tr>
<tr>
<td>employees</td>
</tr>
<tr>
<td>mysql</td>
</tr>
<tr>
<td>securich</td>
</tr>
<tr>
<td>test</td>
</tr>
<tr>
<td>world</td>
</tr>
</tbody>
</table>
+--------------------+
6 rows in set (0.00 sec)
```
Check_roles

mysql Fri Aug 21 16:39:07 2009 > call check_roles();
+-----------+
| ID | ROLE  |
+-----------+
| 1 | read |
| 2 | write |
+-----------+
2 rows in set (0.01 sec)

Query OK, 0 rows affected (0.01 sec)

mysql Fri Aug 21 16:39:30 2009 > call create_update_role('add','dev','select');
Query OK, 0 rows affected, 6 warnings (0.25 sec)
mysql Fri Aug 21 16:39:58 2009 > call
    create_update_role('add','dev','insert');
Query OK, 0 rows affected (0.09 sec)

mysql Fri Aug 21 16:40:03 2009 > call
    create_update_role('add','dev','delete');
Query OK, 0 rows affected (0.09 sec)

mysql Fri Aug 21 16:40:07 2009 > call check_roles();
+-----------+
| ID | ROLE  |
+-----------+
|  1 | read  |
|  2 | write |
|  3 | dev   |
+-----------+
3 rows in set (0.00 sec)
Check_role_privileges

mysql Fri Aug 21 16:40:10 2009 > call check_role_privileges('dev');

+----------------------+
| PRIVILEGE             |
+----------------------+
| DELETE               |
| INSERT               |
| SELECT               |
+----------------------+

3 rows in set (0.00 sec)
Adding privileges to a role

mysql Fri Aug 21 16:40:32 2009 > call
    create_update_role('add','dev','update');
Query OK, 0 rows affected (0.09 sec)

mysql Fri Aug 21 16:40:44 2009 > call
    check_role_privileges('dev');

+-----------+  
| PRIVILEGE |  
+-----------+  
| DELETE    |  
| INSERT    |  
| SELECT    |  
| UPDATE    |  
+-----------+  
4 rows in set (0.00 sec)
Grant_privileges

mysql Fri Aug 21 16:42:24 2009 > call
  grant_privileges('john','localhost','employees','','all','dev','john@doe.com');

+----------------------------------------------|
| USER_PASSWORD                                  |
+----------------------------------------------|
| Password for user -- john -- contactable at --|
|   john@doe.com -- is -- d489a5ec765a --   |
+----------------------------------------------|

1 row in set (2.65 sec)
### Check_full_user_entries

```sql
mysql Fri Aug 21 16:45:37 2009 > call check_full_user_entries('john');
```

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>HOSTNAME</th>
<th>DATABASENAME</th>
<th>TABLENAME</th>
<th>ROLE</th>
<th>PRIVILEGE</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>john</td>
<td>localhost</td>
<td>employees</td>
<td></td>
<td>dev</td>
<td>DELETE</td>
<td>A</td>
</tr>
<tr>
<td>john</td>
<td>localhost</td>
<td>employees</td>
<td></td>
<td>dev</td>
<td>INSERT</td>
<td>A</td>
</tr>
<tr>
<td>john</td>
<td>localhost</td>
<td>employees</td>
<td></td>
<td>dev</td>
<td>SELECT</td>
<td>A</td>
</tr>
<tr>
<td>john</td>
<td>localhost</td>
<td>employees</td>
<td></td>
<td>dev</td>
<td>UPDATE</td>
<td>A</td>
</tr>
</tbody>
</table>

4 rows in set (0.03 sec)
Grant_privileges (regexp)

mysql Fri Aug 21 16:46:34 2009 > call  
grant_privileges('john','localhost','world','country*','regexp','dev','john@doe.com');  
Query OK, 0 rows affected, 1 warning (0.31 sec)

Note: This time it took way less time to grant and it didn’t supply a password!
### Check_full_user_entries (again)

```sql
mysql Fri Aug 21 16:47:07 2009 > call check_full_user_entries('john');
```

```sql
+----------+-----------+--------------+--------------------+------+-----------+-------+
| USERNAME | HOSTNAME  | DATABASENAME | TABLENAME          | ROLE | PRIVILEGE | STATE |
+----------+-----------+--------------+--------------------+------+-----------+-------+
| john     | localhost | employees    |                    | dev  | DELETE    | A     |
| john     | localhost | employees    |                    | dev  | INSERT    | A     |
| john     | localhost | employees    |                    | dev  | SELECT    | A     |
| john     | localhost | employees    |                    | dev  | UPDATE    | A     |
| john     | localhost | world        | country            | dev  | DELETE    | A     |
| john     | localhost | world        | country            | dev  | INSERT    | A     |
| john     | localhost | world        | country            | dev  | SELECT    | A     |
| john     | localhost | world        | country            | dev  | UPDATE    | A     |
| john     | localhost | world        | country_population | dev  | DELETE    | A     |
| john     | localhost | world        | country_population | dev  | INSERT    | A     |
| john     | localhost | world        | country_population | dev  | SELECT    | A     |
| john     | localhost | world        | country_population | dev  | UPDATE    | A     |
+----------+-----------+--------------+--------------------+------+-----------+-------+
```

12 rows in set (0.02 sec)
Grant_privileges (all tables)

mysql Fri Aug 21 16:47:10 2009 > call
grant_privileges('paul','localhost','employees','','alltables','read','john@doe.com');

+-----------------------------------------------------------------------------------------+
| USER_PASSWORD                                                                           |
+-----------------------------------------------------------------------------------------+
| Password for user -- paul -- contactable at -- john@doe.com -- is -- 878f5d4defebed6 -- |
+-----------------------------------------------------------------------------------------+
1 row in set (0.78 sec)

mysql Fri Aug 21 16:54:55 2009 > call check_full_user_entries('paul');

+----------+-----------+--------------+-----------------+------+-----------+-------+
| USERNAME | HOSTNAME  | DATABASENAME | TABLENAME       | ROLE | PRIVILEGE | STATE |
+----------+-----------+--------------+-----------------+------+-----------+-------+
| paul     | localhost | employees    | salary          | read | SELECT    | A     |
| paul     | localhost | employees    | salary_increase | read | SELECT    | A     |
| paul     | localhost | employees    | trade           | read | SELECT    | A     |
| paul     | localhost | employees    | vacancies       | read | SELECT    | A     |
+----------+-----------+--------------+-----------------+------+-----------+-------+
4 rows in set (0.02 sec)
mysql Fri Aug 21 17:02:20 2009 > call clone_user('paul','localhost','paul','ip.home.com','paul@laup.com');

+---------------------------------------------------
| USER_PASSWORD
+---------------------------------------------------
| Password for user -- paul -- contactable at --
paul@laup.com -- is -- 66e3ab90355abc6 -- |
+---------------------------------------------------
1 row in set (2.10 sec)
`mysql Fri Aug 21 17:02:53 2009 > call check_full_user_entries('paul');`  

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>HOSTNAME</th>
<th>DATABASENAME</th>
<th>TABLENAME</th>
<th>ROLE</th>
<th>PRIVILEGE</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>paul</td>
<td>ip.home.com</td>
<td>employees</td>
<td>salary</td>
<td>read</td>
<td>SELECT</td>
<td>A</td>
</tr>
<tr>
<td>paul</td>
<td>ip.home.com</td>
<td>employees</td>
<td>salary_increase</td>
<td>read</td>
<td>SELECT</td>
<td>A</td>
</tr>
<tr>
<td>paul</td>
<td>ip.home.com</td>
<td>employees</td>
<td>trade</td>
<td>read</td>
<td>SELECT</td>
<td>A</td>
</tr>
<tr>
<td>paul</td>
<td>ip.home.com</td>
<td>employees</td>
<td>vacancies</td>
<td>read</td>
<td>SELECT</td>
<td>A</td>
</tr>
<tr>
<td>paul</td>
<td>localhost</td>
<td>employees</td>
<td>salary</td>
<td>read</td>
<td>SELECT</td>
<td>A</td>
</tr>
<tr>
<td>paul</td>
<td>localhost</td>
<td>employees</td>
<td>salary_increase</td>
<td>read</td>
<td>SELECT</td>
<td>A</td>
</tr>
<tr>
<td>paul</td>
<td>localhost</td>
<td>employees</td>
<td>trade</td>
<td>read</td>
<td>SELECT</td>
<td>A</td>
</tr>
<tr>
<td>paul</td>
<td>localhost</td>
<td>employees</td>
<td>vacancies</td>
<td>read</td>
<td>SELECT</td>
<td>A</td>
</tr>
</tbody>
</table>

8 rows in set (0.03 sec)
Call help("")

mysql Fri Aug 21 17:03:38 2009 > call help('full_user_entries');
+---------------------------------------------------------------------------+
| Stored procedure requested does not exist or does not have a `help` entry | +---------------------------------------------------------------------------+
| Stored procedure requested does not exist or does not have a `help` entry | +---------------------------------------------------------------------------+
1 row in set (0.00 sec)

mysql Fri Aug 21 17:03:58 2009 > call help('check_user_entries');
+-------------------------------------------------------------------------------------
| DESCRIPTION +-------------------------------------------------------------------------------------
| check_user_entries('username'); (version 0.1.1) Checks the roles assigned to a particular user and on which database and from which host those privileges can be used | +-------------------------------------------------------------------------------------
1 row in set (0.00 sec)
Check_user_entries (not full)

```sql
mysql Fri Aug 21 17:04:16 2009 > call check_user_entries('paul');

<table>
<thead>
<tr>
<th>USERNAME</th>
<th>HOSTNAME</th>
<th>DATABASENAME</th>
<th>TABLENAME</th>
<th>ROLE</th>
<th>STATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>paul</td>
<td>ip.home.com</td>
<td>employees</td>
<td>salary</td>
<td>read</td>
<td>A</td>
</tr>
<tr>
<td>paul</td>
<td>ip.home.com</td>
<td>employees</td>
<td>salary_increase</td>
<td>read</td>
<td>A</td>
</tr>
<tr>
<td>paul</td>
<td>ip.home.com</td>
<td>employees</td>
<td>trade</td>
<td>read</td>
<td>A</td>
</tr>
<tr>
<td>paul</td>
<td>ip.home.com</td>
<td>employees</td>
<td>vacancies</td>
<td>read</td>
<td>A</td>
</tr>
<tr>
<td>paul</td>
<td>localhost</td>
<td>employees</td>
<td>salary</td>
<td>read</td>
<td>A</td>
</tr>
<tr>
<td>paul</td>
<td>localhost</td>
<td>employees</td>
<td>salary_increase</td>
<td>read</td>
<td>A</td>
</tr>
<tr>
<td>paul</td>
<td>localhost</td>
<td>employees</td>
<td>trade</td>
<td>read</td>
<td>A</td>
</tr>
<tr>
<td>paul</td>
<td>localhost</td>
<td>employees</td>
<td>vacancies</td>
<td>read</td>
<td>A</td>
</tr>
</tbody>
</table>
```

8 rows in set (0.02 sec)
### mysql db entries

mysql Fri Aug 21 17:14:44 2009 > select User,Host,Password from mysql.user;

<table>
<thead>
<tr>
<th>User</th>
<th>Host</th>
<th>Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>root</td>
<td>localhost</td>
<td>*6C387FC3893DBA1E3BA155E74754DA6682D04747</td>
</tr>
<tr>
<td>paul</td>
<td>localhost</td>
<td>*FE4F2D624C07AAEBB979DA5C980D0250C37D8F63</td>
</tr>
<tr>
<td>john</td>
<td>localhost</td>
<td>*55342CD6F138038B08C841B114ADF29F065C603F</td>
</tr>
<tr>
<td>msandbox</td>
<td>%</td>
<td>*6C387FC3893DBA1E3BA155E74754DA6682D04747</td>
</tr>
<tr>
<td>paul</td>
<td>ip.home.com</td>
<td>*FF53F581E636F43F7158A30B6BBF2422D632306E</td>
</tr>
</tbody>
</table>

5 rows in set (0.00 sec)

mysql Fri Aug 21 17:14:59 2009 > select * from mysql.db;

<table>
<thead>
<tr>
<th>Host</th>
<th>Db</th>
<th>User</th>
<th>Select_priv</th>
<th>Insert_priv</th>
<th>Update_priv</th>
<th>Delete_priv</th>
<th>Create_priv</th>
<th>Drop_priv</th>
<th>Grant_priv</th>
<th>References_priv</th>
</tr>
</thead>
<tbody>
<tr>
<td>localhost</td>
<td>employees</td>
<td>john</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
<td>N</td>
<td>N</td>
</tr>
</tbody>
</table>

1 row in set (0.00 sec)
SECURITY - DB Design
Darren Cassar

Skype: darren.cassar
Email: darren@darrencassar.com

URL: www.securich.com
Blog: www.mysqlpreacher.com