Access control

Ramin Sadre

Access control

- We have seen that two attributes of a secure system are confidentiality and integrity
- To implement those attributes, most computer systems implement some kind of **access control**
  - Access control = Restrict the access to a resource to authorized users or programs
  - Resource can be data, CPU,...
- In a computer system, there are many access control rules, for example:
  - Only the DB admin is allowed to delete a database table
  - Only the root user is allowed to change the password of a user
  - Only user “Peter” is allowed to read files from /home/peter

Principle of least privileges

- Principle of least privileges = Define the access control rules such that users only have those access rights that they need to do their job
- Example:
  - DB admin can modify the database configuration but not the configuration of the web server
  - User “Peter” can access /home/peter but not /home/mary
  - Web server can access /home/www but not /home/peter

Implementing access control

- There are different ways to implement access control
- For example, in Unix-like OS:
  - The identity of the user is verified through a login with password
  - File permission flags specify who is the “owner” of a file and what a user is allowed to do with that file:

```
-rwxr-xr-x 1 ramin ramin 8328 Feb  1 23:16 test
-rw-r--r-- 1 ramin ramin  681 Feb  1 23:16 test.c
-rw-r--r-- 1 ramin ramin  233 Feb  6 13:31 test.py
-rw-rw-rw- 1 ramin ramin 2000 Apr 22  2020 test.txt
```

  - When a user wants to access the file, the OS verifies whether the user is authorized
- Other technique found in many OS: Access Control Lists (ACL)
  - ACL = list of users who are allowed to access a file

Breaking access control

- How do you (the attacker) get access to a resource if its access rules say that you don't have the permission?
- Many ways possible:
  - Physical (steal the computer)
  - Social engineering (convince the user to give the resource to you)
  - Exploiting wrongly implemented access control
  - **Privilege escalation** = a user obtains the access rights of another user with more rights
  - …