



*Syahrul Imardi, MT*

# #8

## MATAKULIAH **KEAMANAN PERANGKAT LUNAK**

### Praktikum (1) Access Control



# Technical Controls

# Preventive Technical Controls

- Digunakan untuk mencegah orang/program yang tidak berhak untuk mendapatkan akses terhadap resources komputer.
  - Access control software (Access Control List - ACL)
  - Antivirus (Security) software.
  - Library control systems.
  - Passwords.
  - Smart cards.
  - Encryption.
  - Dial-up access control and callback systems.

# Strong Password

Choose a password:  Password strength: **Weak**  
Minimum of 8 characters in length.

Re-enter password:

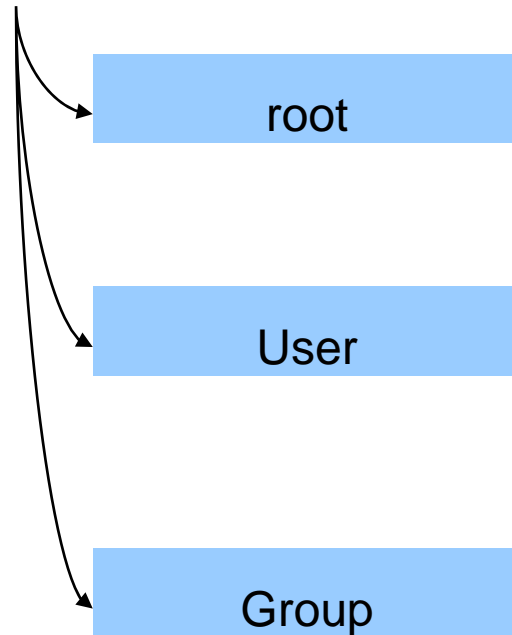
Choose a password:  Password strength: **Fair**  
Minimum of 8 characters in length.

Choose a password:  Password strength: **Weak**  
Minimum of 8 characters in length.

Choose a password:  Password strength: **Strong**  
Minimum of 8 characters in length.

- Panduan umum membuat “strong password” :
  - A minimum password length of 12 to 14 characters if permitted
  - Generating passwords randomly where feasible
  - Avoiding passwords based on repetition, dictionary words, letter or number sequences, usernames, relative or pet names, romantic links (current or past), or biographical information (e.g., ID numbers, ancestors' names or dates).
  - Including numbers, and symbols in passwords if allowed by the system
  - If the system recognizes case as significant, using capital and lower-case letters
  - Avoiding using the same password for multiple sites or purposes
  - Avoid using something that the public or workmates know you strongly like or dislike

## User account in Linux



root

kontrol system file, user, sumber daya (devices) dan akses jaringan

User

account dengan kekuasaan yang diatur oleh root dalam melakukan aktifitas dalam system.

Group

kumpulan user yang memiliki hak sharing yang sejenis terhadap suatu devices tertentu.

```
dnd@riyaniezt: ~/Desktop
File Edit View Search Terminal Help
dnd@riyaniezt:~/Desktop$ ls -l
total 440
-rw-rw-r-- 1 dnd dnd 600 Sep 29 09:49 algo_pagi
-rw-r----- 1 dnd dnd 356294 Sep 21 13:19 jadkul- 20141R.pdf
-rw-rw-r-- 1 dnd dnd 108 Okt 9 12:01 javame8.txt
-rw-r--r-- 1 dnd dnd 15036 Sep 24 07:12 MyJadwal - 20141R.xlsx
-rw-rw-r-- 1 dnd dnd 7811 Okt 8 07:19 MyJadwal.xlsx
-rwxrwxrwx 1 dnd dnd 21210 Agu 29 15:09 Notulen_290814.odt
drwxrwxr-x 7 dnd dnd 4096 Okt 13 15:44 RPL_21
-rw-rw-r-- 1 dnd dnd 302 Okt 13 15:27 rpl_21_131014
-rw-rw-r-- 1 dnd dnd 177 Okt 3 11:52 tgs_SD
-rw-rw-r-- 1 dnd dnd 123 Sep 22 17:43 transaksi_prodi
-rw-rw-r-- 1 dnd dnd 2699 Sep 23 02:17 transaksi_prodi2
-rwxrwxrwx 1 dnd dnd 600 Agu 22 09:14 ubuntu_tutouch
-rwxrwxrwx 1 dnd dnd 618 Agu 22 08:04 vboxreload-genimotion
-rw-rw-r-- 1 dnd dnd 171 Sep 11 12:10 Wifi
dnd@riyaniezt:~/Desktop$
```



- Permission in Files and Dir
  - For normal files:
    - r = permission to read the contents of the file,
    - w = permission to modify the contents of the file,
    - x = permission to execute the file.
  - For directories:
    - r = permission to list the filenames in the directory,
    - w = permission to create or delete files in the directory,
    - x = permission to access the directory.



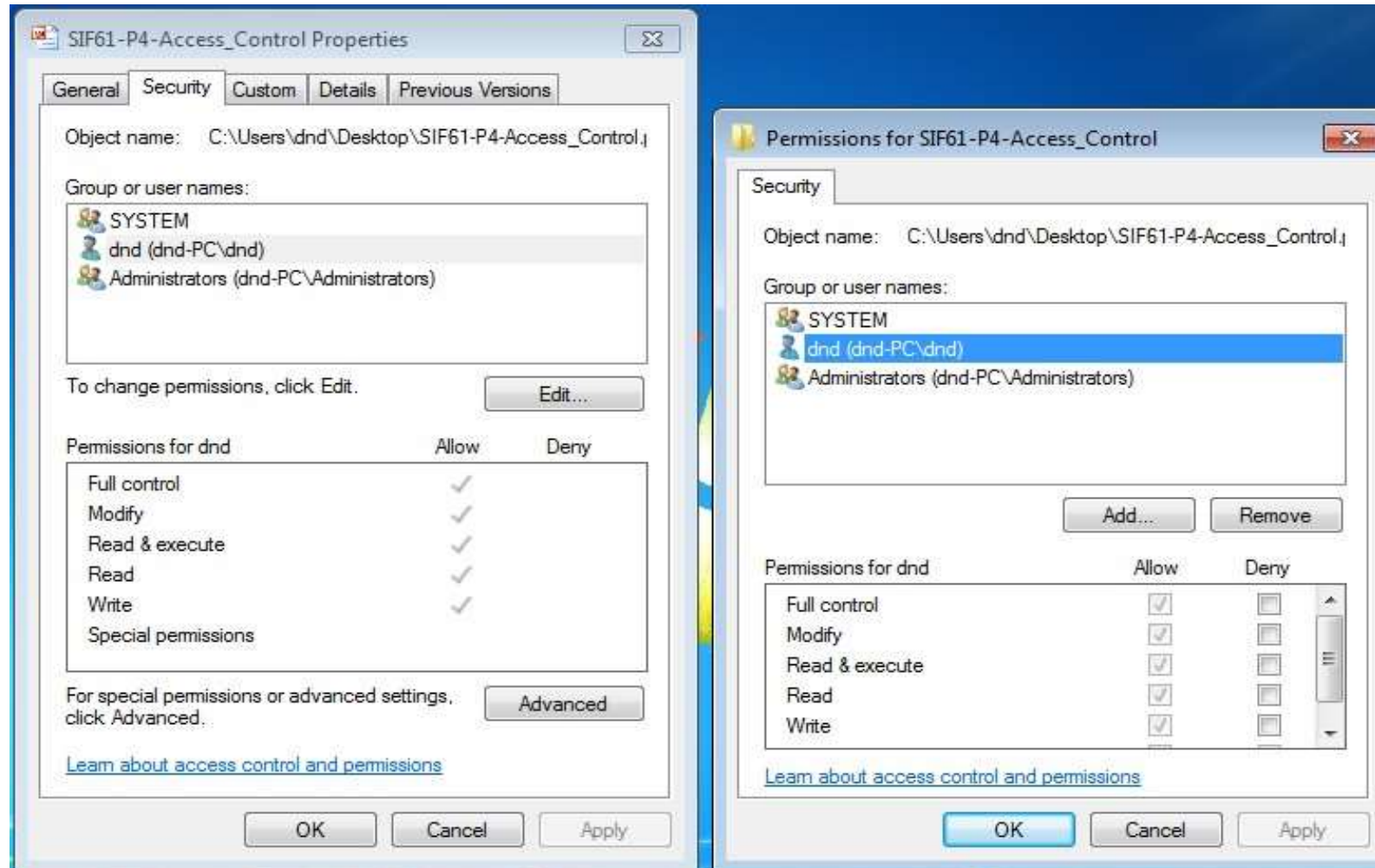
- contoh lain :

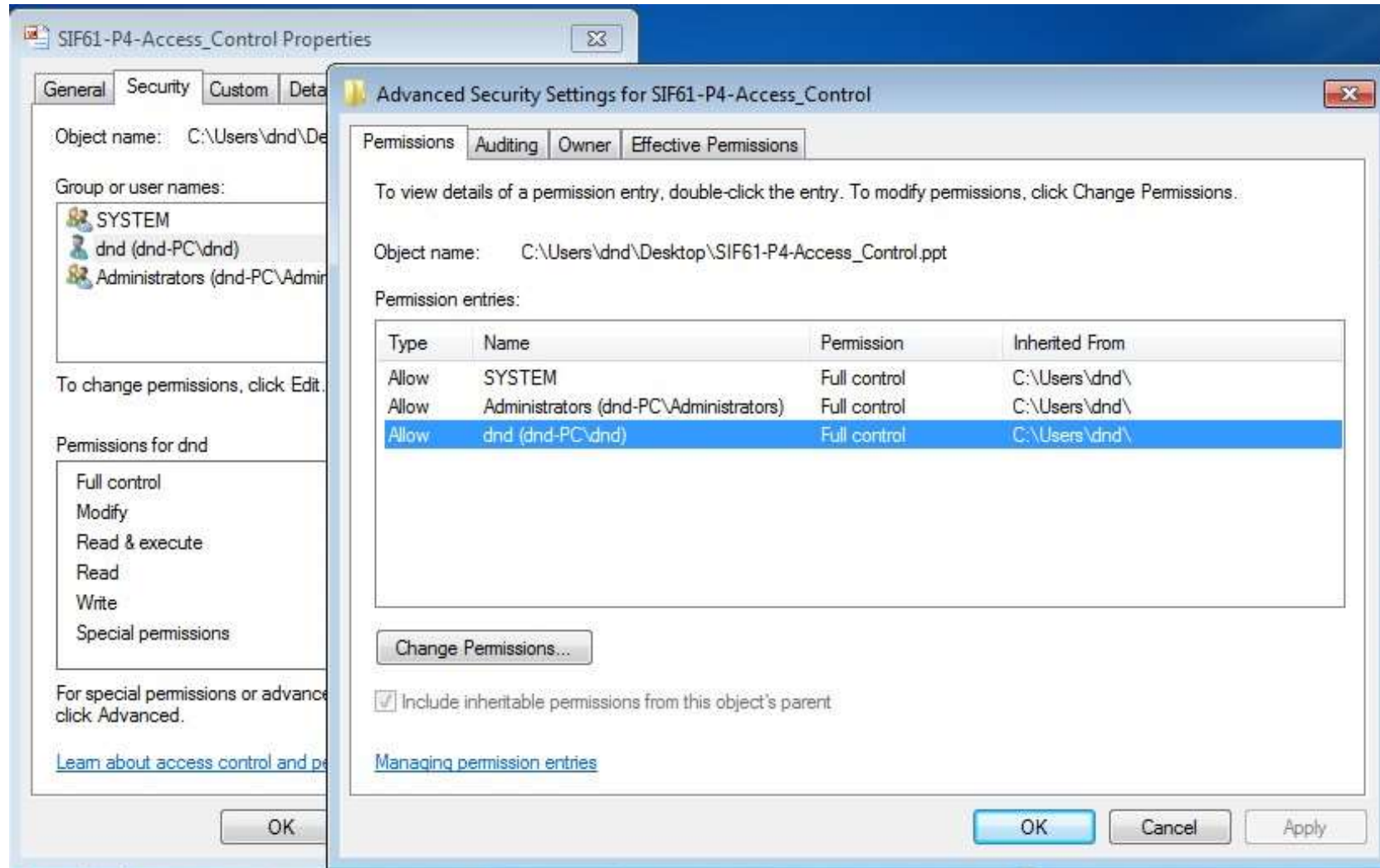
ACL	Keterangan
-rwxrwxrwx	a file that everyone can read, write and execute (and delete).
-rw-----	a file that only the owner can read and write - no-one else can read or write and no-one has execution rights (e.g. your mailbox file).

## ACL in Windows

- Microsoft and IBM DOS variants seperti MS-DOS, PC DOS, Windows 95, Windows 98, Windows 98 SE & Windows Me tidak mempunyai file permissions, hanya file attributes (read only) yang bisa di set siapa saja.
- Microsoft Windows NT dan turunannya (NTFS), termasuk Windows 2000, XP dan setelahnya sudah menggunakan ACL, dengan fungsi dasar seperti di Linux tetapi lebih kompleks ( menambahkan konsep tokens dan security attributes)
- Secara umum lebih fleksibel dari UNIX, karena dapat mendefinisikan perijinan baru.

- ACL di Windows dikenal dengan istilah Access Control Entries (ACEs)





- Object-object di Windows yang dapat diamankan dengan permissions :
  - Files and directories on NTFS volumes
  - Registry keys (but not values)
  - Network shares
  - Printers
  - Services
  - Active Directory objects
  - Processes

# Detective Technical Controls

- Memberi peringatan bahwa ada indikasi pelanggaran atau gangguan terhadap keamanan (secara teknis), misalnya :
  - Audit Trail (Logging)
  - Intrusion Detection Systems
    - Sebuah alat atau software memonitor jaringan atau aktivitas sistem dari ancaman, bahaya, aktivitas mencurigakan atau pelanggaran aturan yang menghasilkan laporan kepada bagian manajemen.

# Administrative Controls

# Preventive Administrative Controls

- Security awareness and technical training.
- Separation of duties.
- Procedures for recruiting and terminating employees.
- Security policies and procedures.
- Supervision.
- Disaster recovery, contingency, and emergency plans.
- User registration for computer access.



# Detective Administrative Controls

- Security reviews and audits.
- Performance evaluations.
- Required vacations.
- Background investigations.
- Rotation of duties.

## TECHNICAL CONTROLS

### Preventive

- Access control software
- Antivirus software
- Library control systems
- Password
- Smart card
- Encryption
- Dial-up access control & callback systems

### Detective

- Audit trails
- Intrusion-detection expert systems

## ADMINISTRATIVE CONTROLS

### ■ Preventive

- Security awareness & technical training
- Separation of duties
- Procedures for recruiting and terminating employees
- Security policies & procedures
- Supervision
- Disaster recovery & contingency plans
- User registration for computer access

### ■ Detective

- Security reviews and audits
- Performance evaluation
- Required vacations
- Background investigation
- Rotation of duties

- Access Control, Micki Krause, Harold F. Tipton  
<http://www.cccure.org/Documents/HISM/001-002.html>
- [http://en.wikipedia.org/wiki/Access\\_control](http://en.wikipedia.org/wiki/Access_control)
- [http://en.wikipedia.org/wiki/Intrusion\\_detection\\_system](http://en.wikipedia.org/wiki/Intrusion_detection_system)
- [http://en.wikipedia.org/wiki/Access\\_control\\_list](http://en.wikipedia.org/wiki/Access_control_list)
- [http://en.wikipedia.org/wiki/Filesystem\\_permissions](http://en.wikipedia.org/wiki/Filesystem_permissions)
- <https://helgeklein.com/blog/2009/03/permissions-a-primer-or-dacl-sacl-owner-sid-and-ace-explained/>