Syahrul Imardi, MT

STMIK Amik Riau

#6

MATAKULIAH

KEAMANAN PERANGKAT LUNAK

Access Control

P6

STMIK Amik Riau

MATAKULIAH
KEAMANAN PERANGKAT LUNAK

Syahrul Imardi, MT

Pertemuan 6 : Access Control

Pembahasan

STMIK Amik Riau

- Ruang Lingkup
- Types of Information Security Control
  - Physical
  - Technical
  - Administrative

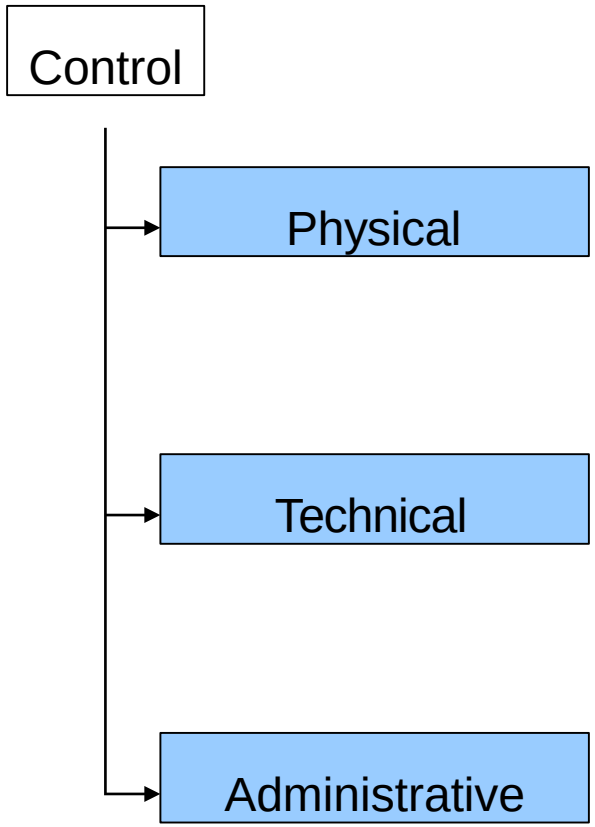
Ruang Lingkup

(wikipedia)

- Physical Security
  - Pengamanan komputer, data atau informasi secara fisik
  - Sudah banyak dibahas pada meteri sebelumnya, di review sebentar
- Computer Security
- Telecomunication
- Public Policy, dll

Types of Information Security Controls

(Micki Krause, Harold F. Tipton)



Penggunaan kunci, penjaga keamanan, tanda pengenal, alarm & alat sejenis untuk mengontrol akses komputer, peralatan terkait (termasuk utilities), danfasilitasnya dari berbagai ancaman, perusakan, kegagalan beroperasi baik karena manusia, kecelakaan, kebakaran, bencana alam atau lingkungan.

Penggunaan pengamanan yang melibatkan komputer hardware, software, perangkat komunikasi dan perangkat yang bersangkutan. Sering disebut juga Logical Control

Berbagai peraturan, manajemen, prosedur operasi atau ketentuan keamanan lainnya yg dibuat untuk menyediakan level proteksi terhadap resources informasi yg dapat diterima.

STMIK
Amik Riau

Physical Controls

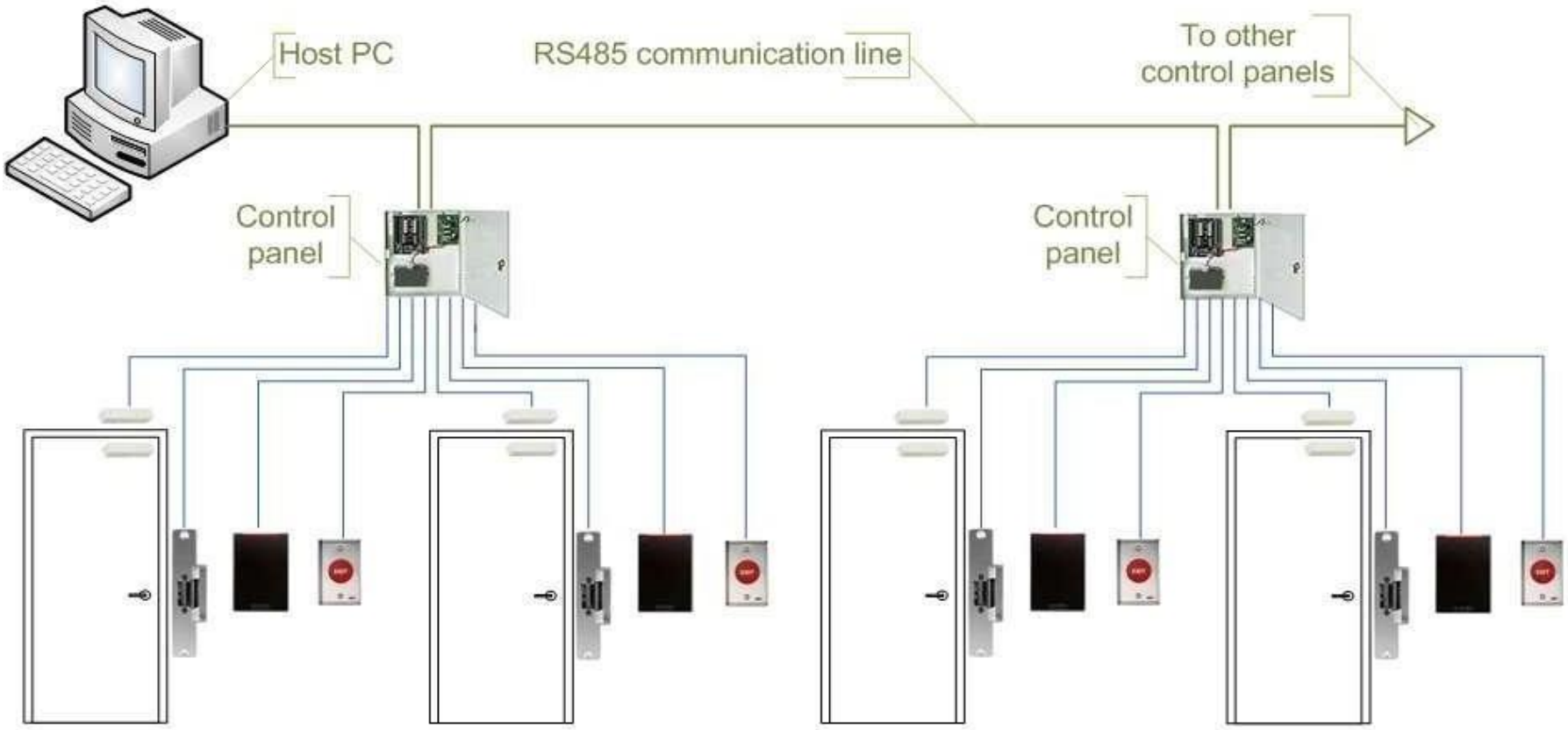
Preventive Physical Control

STMIK Amik Riau

- Usaha untuk mencegah akses dari pihak yang tidak berhak dan dari resiko bencana alam/lingkungan:
  - Backup files and documentation.
  - Pagar pembatas (Fences).
  - Security guards.
  - Badge systems.
  - Double door systems.
  - Locks and keys.
  - Backup power.
  - Biometric access controls.
  - Site selection (pemilihan tempat yang tepat)
  - Fire extinguishers (perangkat pemadam kebakaran)

Physical Security

- Access control system diagram, using serial controllers



Detective Physical Controls

STMIK Amik Riau

- Memberi peringatan bahwa ada indikasi
- pelanggaran atau gangguan terhadap
- keamanan (fisik), misalnya :
  - Motion detectors.
  - Smoke and fire detectors.
  - Closed-circuit television monitors (CCTV)
  - Sensors and alarms.

Perangkat Smoke & Motion Detector

CCTV


Wall Mount Dome Camera
Fixed Camera in Outdoor Housing
Integrated Dome Camera
Integrated Dome Camera
Integrated Dome Camera on Pole Mount
Wall Mount Dome Camera
Wall or Ceiling Mount
Fixed Camera Shown with Lens
4 Camera Transceiver for Video over Twisted Pair Wire
Passive Twisted Pair Transmitter
Wall or ceiling camera mount
Pan - Tilt -Zoom Controller
Spot Monitor
8 Channel Digital Recorder / Multiplexer

STMIK
Amik Riau

Technical Controls

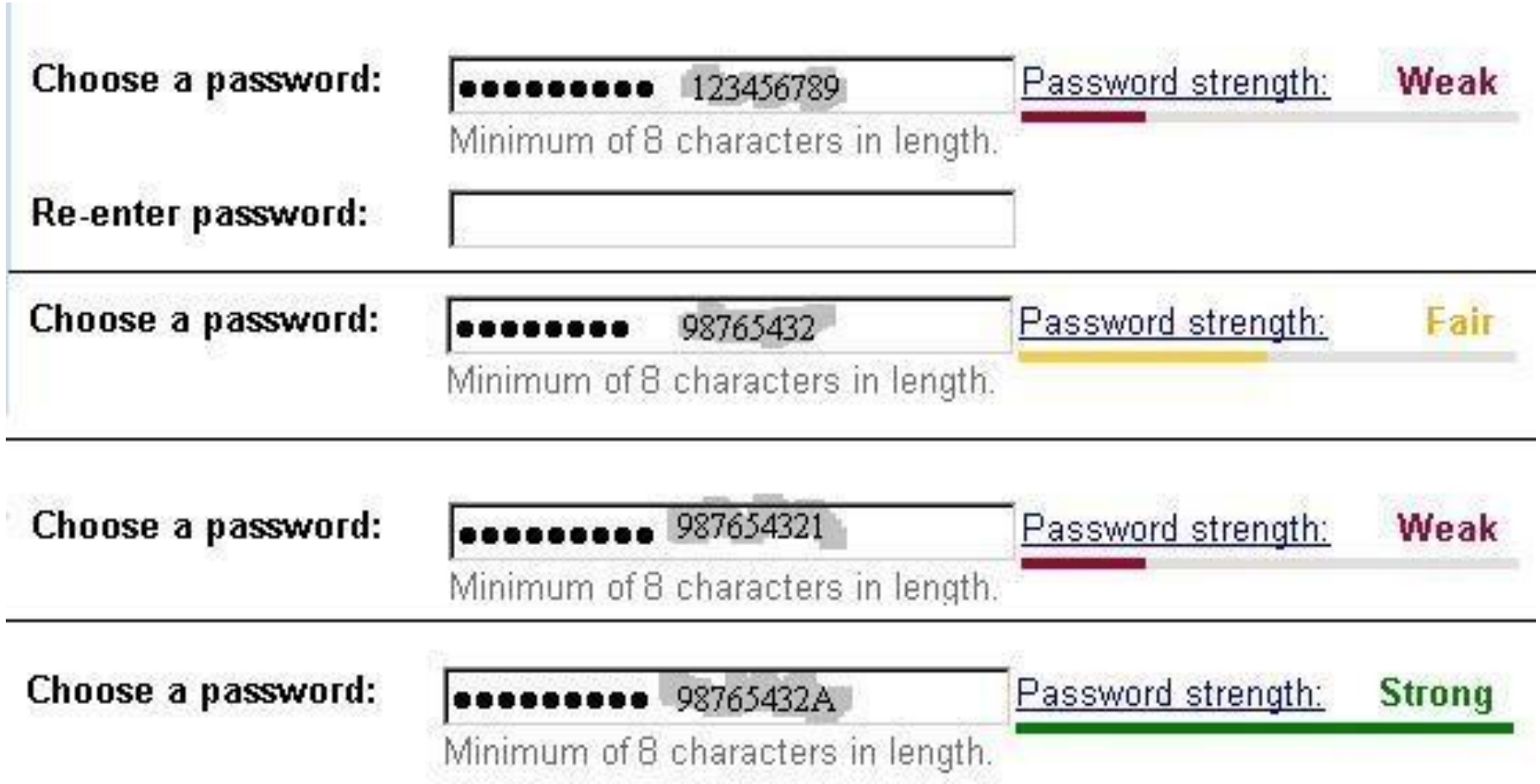
Preventive Technical Controls

STMIK Amik Riau

- 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

STMIK Amik Riau



- 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

Access Control Matrix (ACM)

STMIK Amik Riau

- Diperkenalkan pertama kali oleh Butler W. Lampson 1971
- Semua proses (subject) dan file (object) didaftar dalam sebuah Matrik dengan hak akses tertentu.

- Terdiri atas Object (O) dan Subject (S)
  - Object = entity2 yang dilindungi (file, device)
  - Subject = objek aktif (user, proses)

- Relationship antara O dan S adalah melalui RIGHTS (hak = R) ditandai dengan:
  - r(s,o) – dimana s∈S (s eleman dari set S), o∈O
  - r(s, o) ⊆ R (setiap elemen r(s, o) juga merupakan elemen R)

- Contoh : Sebuah sistem dengan 2 file dan 2 proses.
  - Sekumppulan hak akses – r,w,x,a,o (read, write, execute, append, own)

	File 1	File 2	Process 1	Process 2
Process 1	r,w,o	r	r,w,x,o	w
Process 2	a	r,o	r	r,w,x,o

- Dapat menjadi sangat besar dan tidak efisien untuk penggunaan umum, sehingga jarang digunakan

Access Control List (ACL)

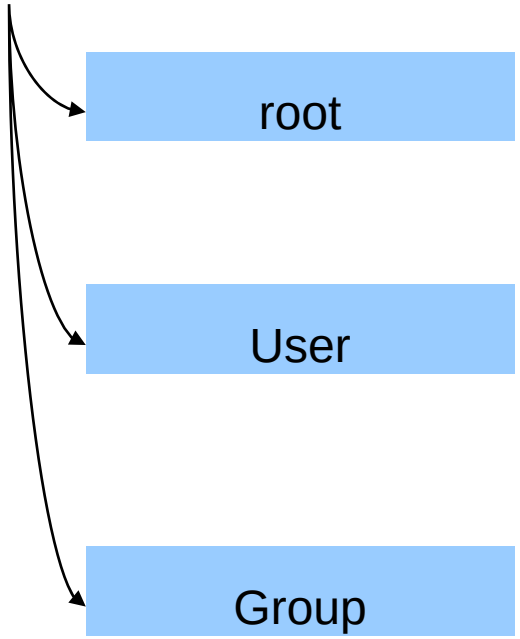
STMIK Amik Riau

- Merupakan daftar perijinan (permissions) yang terikat dengan sebuah object
- ACL menentukan/menunjukkan user atau proses yang mana yang diijinkan mengakses object termasuk operasi apa yang diijinkan terhadap object tersebut

ACL in Linux/UNIX

STMIK Amik Riau

User account in Linux



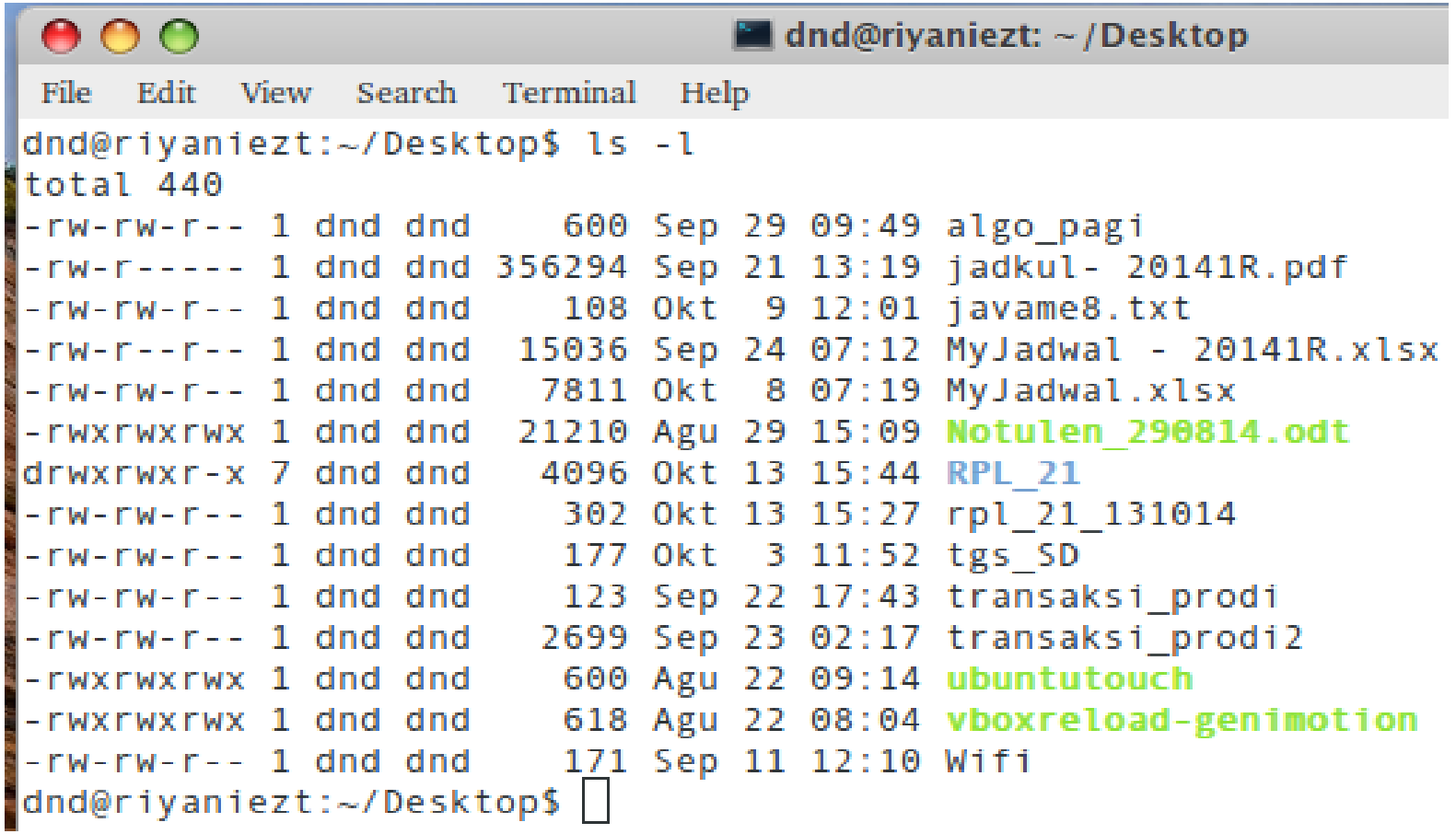
kontrol system file, user, sumber daya (devices) dan akses jaringan

---

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

---

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 ubuntutouch
-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.

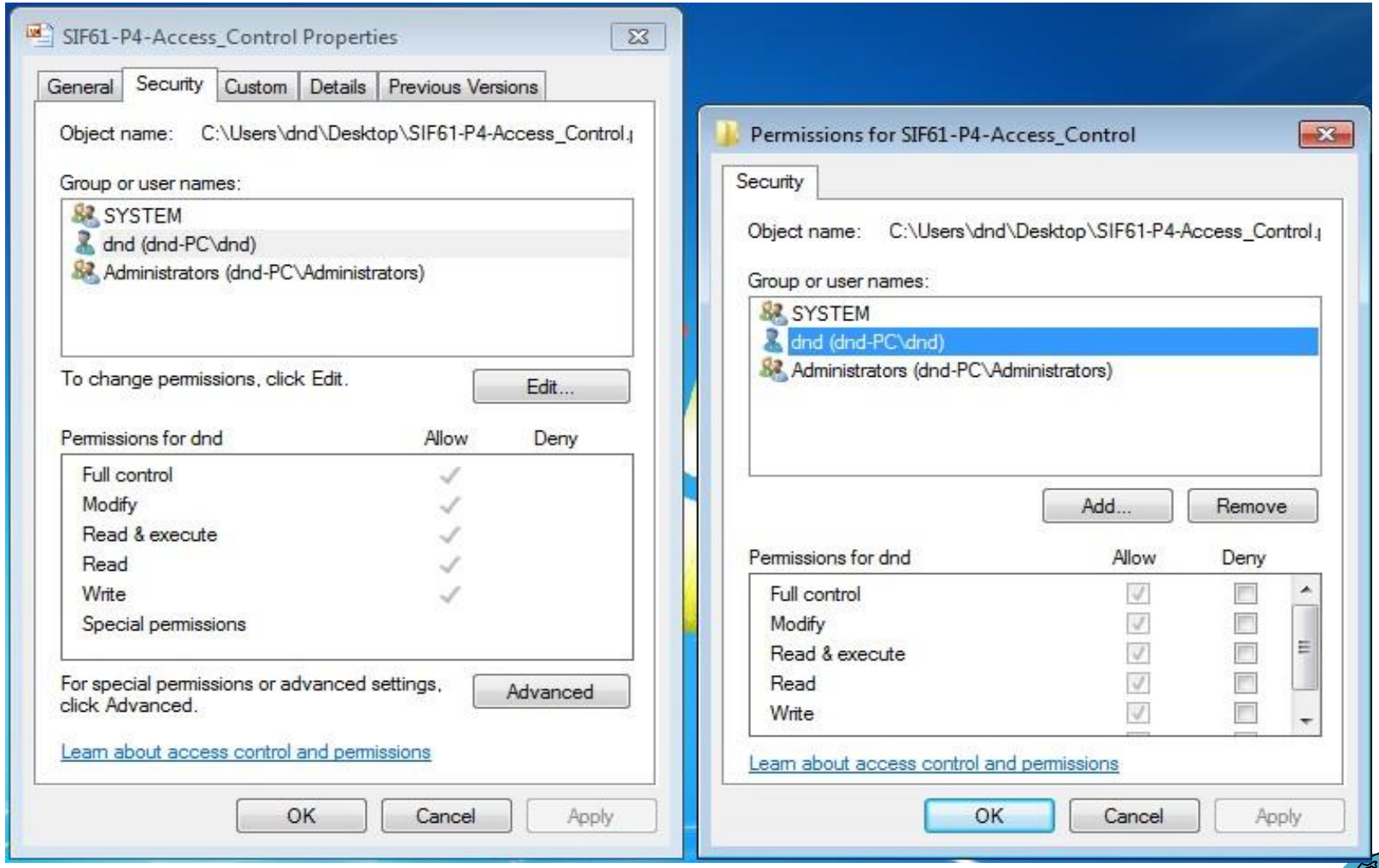
- contoh lain :

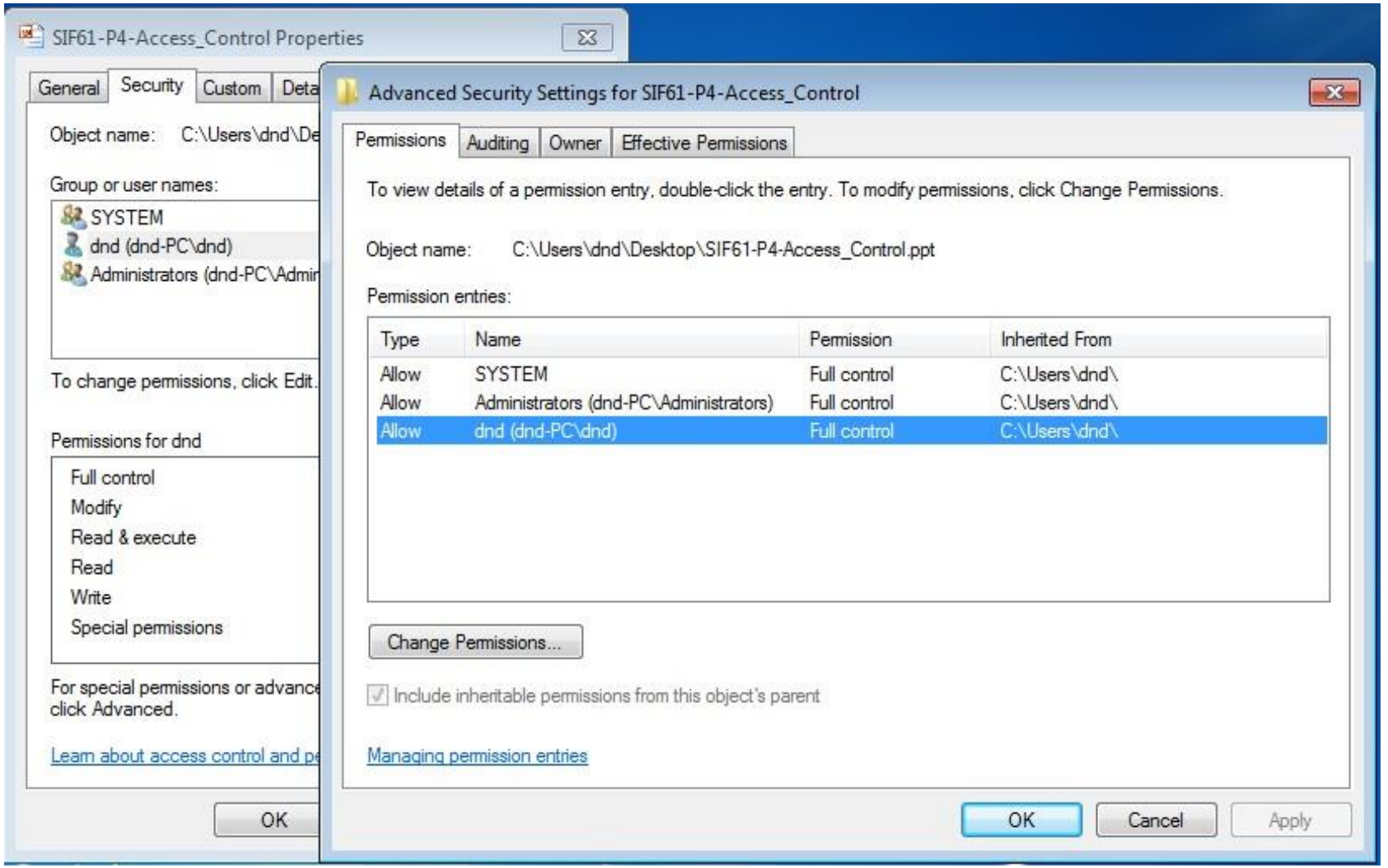
ACL	Keterangan
-rwxrwxrwx	a file that everyone can read, write and execute (and delete).
-rw-------	a file that only the owner can read and write - no-one else can read or write and no-one has execution rights (e.g. your mailbox file).

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)




SIF61-P4-Access_Control Properties
General
Security
Custom
Deta
Object name: C:\Users\dnd\De
Group or user names:
SYSTEM
dnd (dnd-PC\dnd)
Administrators (dnd-PC\Admir
To change permissions, click Edit.
Permissions for dnd
Full control
Modify
Read & execute
Read
Write
Special permissions
For special permissions or advance
click Advanced.
Learn about access control and pe
OK
Advanced Security Settings for SIF61-P4-Access_Control
Permissions
Auditing
Owner
Effective Permissions
To view details of a permission entry, double-click the entry. To modify permissions, click Change Permissions.
Object name: C:\Users\dnd\Desktop\SIF61-P4-Access_Control.ppt
Permission entries:
Type
Name
Permission
Inherited From
Allow
SYSTEM
Full control
C:\Users\dnd\
Allow
Administrators (dnd-PC\Administrators)
Full control
C:\Users\dnd\
Allow
dnd (dnd-PC\dnd)
Full control
C:\Users\dnd\
Change Permissions...
Include inheritable permissions from this object's parent
Managing permission entries
OK
Cancel
Apply

- 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

STMIK Amik Riau

- 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.

STMIK
Amik Riau

Administrative Controls

Preventive Administrative Controls

STMIK Amik Riau

- 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

STMIK Amik Riau

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

Summary

STMIK Amik Riau

- PHYSICAL CONTROLS
- Preventive

•Backup files and documentation

•Fences

•Security guards

•Badge systems

•Locks and keys

•Backup power

•Biometric access controls

•Site selection

•Fire extinguishers

- Detective

•Motion detector

•Smoke & Fire detector

•Closed circuit television monitoring

•Sensors and alarm

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

STMIK Amik Riau

- 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

Referensi

- 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/Intrusion_detection_system
- http://en.wikipedia.org/wiki/Access_control_list
- http://en.wikipedia.org/wiki/Filesystem_permissions
- https://helgeklein.com/blog/2009/03/permissions-a-primer-or-dacl-sacl-owner-sid-and-ace-explained/

REFERENSI UTAMA :

>> Michael Felderer , Riccardo Scandariato (editor) - Exploring Security in Software Architecture and Design, 2018.

>> Nancy R. Mead, Carol Woody - Cyber Security Engineering_ A Practical Approach for Systems and Software Assurance-Addison-Wesley Professional (2016)

>> James Helfrich - Security for Software Engineers-CRC Press (2019)

>> Pete Loshin - Simple Steps to Data Encryption_ A Practical Guide to Secure Computing-Syngress (2013)

>> Tevfik Bultan,Fang Yu,Muath Alkhalaf,Abdulbaki Aydin (auth.) - String Analysis for Software Verification and Security (2017)

THANKS!