

# 14

## Keamanan Sistem dan Proteksi

Tim Teaching Grant  
Mata Kuliah Sistem Operasi



## Penyebab Data Hilang

### Kasus Umum

1. Bencana Alam dan Perang
2. Kesalahan Hardware atau software
  - CPU malfunction, bad disk, program bugs
3. Kesalahan manusia
  - Data entry, wrong tape mounted

## Aspek Keamanan Sistem

- Kerahasiaan (Secrecy)
- Integritas (Integrity)
- Ketersediaan (Availability)



## Intruder (1/ 5)

### Kategori Umum

1. Iseng-iseng, biasanya pada yang bisa diakses semua user
2. Snooping, seseorang masuk ke dalam sistem jaringan dan berusaha menebus pengamanan
3. Berusaha mencari keuntungan dengan motivasi uang
4. Spionase/militer

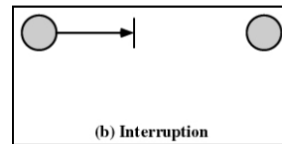


## Intruder (2/ 5)



- Interupsi

- Sumberdaya sistem komputer dihancurkan atau menjadi tak tersedia
- Penghancuran harddisk
- Pemotongan kabel komunikasi
- Sistem file management menjadi tidak tersedia



Bab 14. Keamanan Sistem & Proteksi

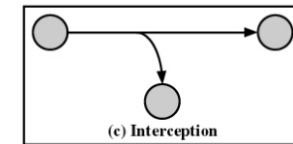
5

## Intruder (3/5)



- Intersepsi

- Pihak tak diotorisasi dapat mengakses sumberdaya
- Ancaman terhadap kerahasiaan data
- Penyadapan terhadap data di jaringan
- Mengkopi file tanpa diotorisasi



Bab 14. Keamanan Sistem & Proteksi

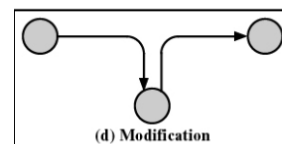
6

## Intruder (4/5)



- Modification

- Mengubah nilai-nilai file data
- Mengubah program sehingga bertindak secara beda
- Memodifikasi pesan-pesan yang ditransmisikan pada jaringan



Bab 14. Keamanan Sistem & Proteksi

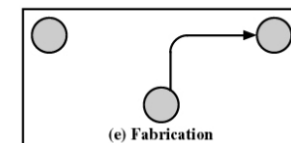
7

## Intruder (5/5)



- Fabrication

- Pihak tak diotorisasi menyisipkan objek palsu ke sistem
- Memasukkan pesan-pesan palsu ke jaringan
- Penambahan record ke file



Bab 14. Keamanan Sistem & Proteksi

8

# Prinsip Pengamanan Sistem Komputer



- Rancangan sistem seharusnya publik
- Dapat diterima
- Pemeriksaan otoritas saat itu
- Kewenangan serendah mungkin
- Mekanisme yang ekonomis

# Autentikasi Pemakai



- Suatu yang diketahui pemakai :
  - password
  - kombinasi kunci
  - nama kecil ibu, dsb
- Sesuatu yang dimiliki pemakai :
  - badge
  - kartu identitas
  - kunci, dsb
- Sesuatu mengenai (merupakan ciri) pemakai :
  - sidik jari
  - sidik suara
  - foto
  - tanda tangan, dsb

# Contoh Autentikasi (1/3)



## • Password

LOGIN : ken  
PASSWORD : FooBar  
SUCCESSFUL LOGIN  
(a)

LOGIN : carol  
INVALID LOGIN NAME  
LOGIN :  
(b)

LOGIN : carol  
PASSWORD : Idunno  
INVALID LOGIN  
LOGIN :  
(c)

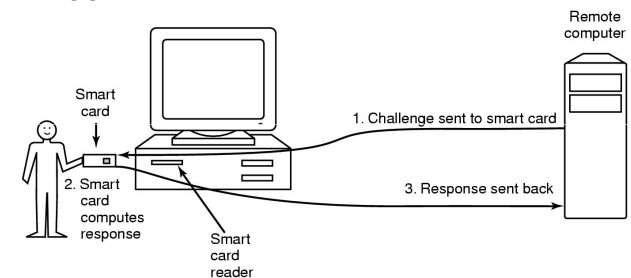
- (a) Login berhasil
- (b) Login ditolak setelah nama dimasukkan
- (c) Login ditolak setelah nama dan password dimasukkan

Bobbie, 4238, e(Dog4238)
Tony, 2918, e(6%%TaeFF2918)
Laura, 6902, e(Shakespeare6902)
Mark, 1694, e(XaB@Bwcz1694)
Deborah, 1092, e(LordByron,1092)

# Contoh Autentikasi (2/3)



## • Menggunakan Objek Fisik



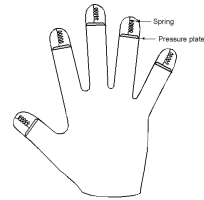
## Magnetic cards

- magnetic stripe cards
- chip cards: stored value cards, smart cards

## Contoh Autentikasi (3/ 3)



- Menggunakan Biometric



## Countermeasures (Tindakan Balasan)



- Pembatasan waktu ketika seseorang login
- Panggilan otomatis pada nomor yang disiapkan
- Pembatasan upaya melakukan login
- Ketersediaan database login
- Penggunaan simple login sebagai perangkat

## Sekuriti Sistem Operasi



- Logic Bomb

Logik yang ditempelkan pada program komputer, dimana pada saat program menjalankan kondisi tertentu logik tersebut menjalankan fungsi yang merusak

- Trap Door

Kode yang menerima suatu barisan masukan khusus atau dipicu dengan menjalankan ID pemakai tertentu

```
while (TRUE) {
    printf("login: ");
    get_string(name);
    disable_echoing();
    printf("password: ");
    get_string(password);
    enable_echoing();
    v = check_validity(name, password);
    if (v) break;
}
execute_shell(name);

while (TRUE) {
    printf("login: ");
    get_string(name);
    disable_echoing();
    printf("password: ");
    get_string(password);
    enable_echoing();
    v = check_validity(name, password);
    if (v || strcmp(name, "zzzzz") == 0) break;
}
execute_shell(name);
```

(a)

(b)

## Serangan Pengamanan Umum



- Permintaan page memori
- Mencoba system calls
- Mencoba login dan langsung menekan DEL, RUBOUT atau BREAK
- Mencoba memodifikasi struktur sistem operasi
- Mencari informasi yang tidak boleh dilakukan pada manual book
- Menggunakan kelemahan sifat manusia

## Prinsip Dasar Sekuriti



- Sistem sebaiknya bersifat publik
- Nilai default tidak boleh diakses
- Pengecekan otoritas
- Memberikan setiap proses kemampuan akses sesedikit mungkin
- Mekanisme proteksi sederhana, uniform dan built in ke lapis terbawah
- Skema pengamanan harus dapat diterima secara psikologis

## Sekuriti Jaringan Komputer



- Ancaman Eksternal
  - Kode di transfer ke mesin target
  - Saat kode dieksekusi, kerusakan pun terjadi
- Tujuan virus ditulis di jaringan komputer
  - Penyebarannya yang cepat
  - Sulit terdeteksi
- Virus = program yang dapat memperbanyak diri sendiri

## Skenario Pengrusakan oleh Virus



- Blackmail
- Denial of Service selama virus masih jalan
- Kerusakan permanen pada hardware
- Kompetitor komputer
- sabotase

## Siklus Hidup Virus



- Fase Tidur (Dormant Phase)  
Virus dalam keadaan menganggur sampai terjadi suatu kejadian tertentu
- Fase Propagasi  
Virus menempatkan kopi dirinya ke program lain di disk.
- Fase Pemicuan (Triggering Phase)  
Virus diaktifkan untuk melakukan fungsi tertentu
- Fase Eksekusi  
Virus menjalankan fungsinya

# Tipe-tipe Virus

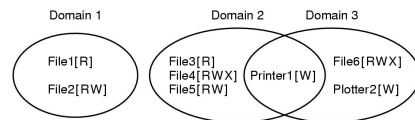
- **Parasitic Virus**  
Menggantung ke file .exe dan melakukan replikasi ketika file tersebut dieksekusi
- **Memory Resident Virus**  
Menempatkan diri ke memori utama dan menginfeksi setiap program yang dieksekusi
- **Boot Sector Virus**  
Menginfeksi boot record dan menyebar saat sistem di boot
- **Stealth Virus**  
Bentuknya dirancang agar tidak terdeteksi oleh antivirus
- **Polymorphic Virus**  
Bermutasi setiap kali melakukan infeksi

# Antivirus

- **Pendekatan Antivirus**
  - Deteksi
  - Identifikasi
  - Penghilangan dengan program antivirus (biasanya dibuat dengan bahasa assembler)
- **Generasi Antivirus**
  - G1 : Sekedar scanner biasa
  - G2 : heuristic scanner
  - G3 : activity trap
  - G4 : full feature protection

# Mekanisme Proteksi (1/ 3)

- **Domain Proteksi**



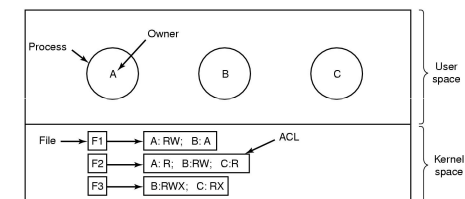
Contoh tiga domain proteksi

Domain	File1	File2	File3	File4	File5	File6	Printer1	Plotter2
1	Read	Read Write						
2			Read	Read Write Execute	Read Write		Write	
3						Read Write Execute	Write	Write

Matriks

# Mekanisme Proteksi (2/3)

- **Access Control List (ACL)**

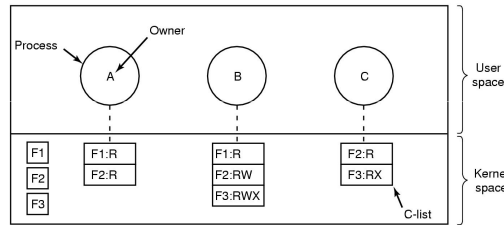


File	Access control list
Password	tana, sysadm: RW
Pigeon_data	bill, pigfan: RW; tana, pigfan: RW; ...

Peggunaan Access Control List dalam mengatur akses file

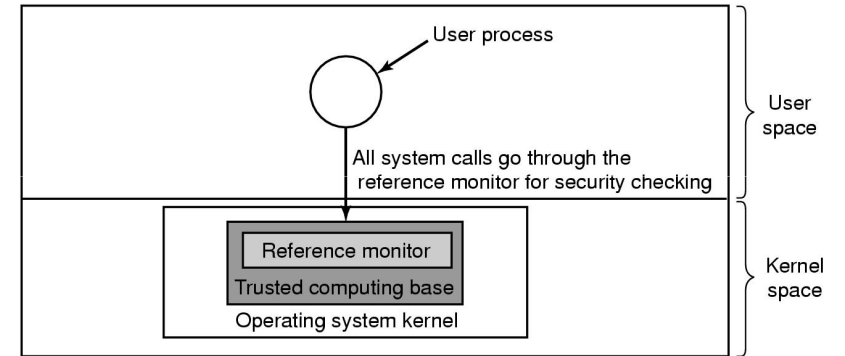
# Mekanisme Proteksi (3/3)

- Kapabilitas



Memecah setiap proses ke dalam daftar kapabilitas

# Sistem Terpercaya (Trusted Computing Base)



## Reference monitor

# Model Formal Keamanan Sistem

	Objects		
	Compiler	Mailbox 7	Secret
Eric	Read Execute		
Henry	Read Execute	Read Write	
Robert	Read Execute		Read Write

(a)

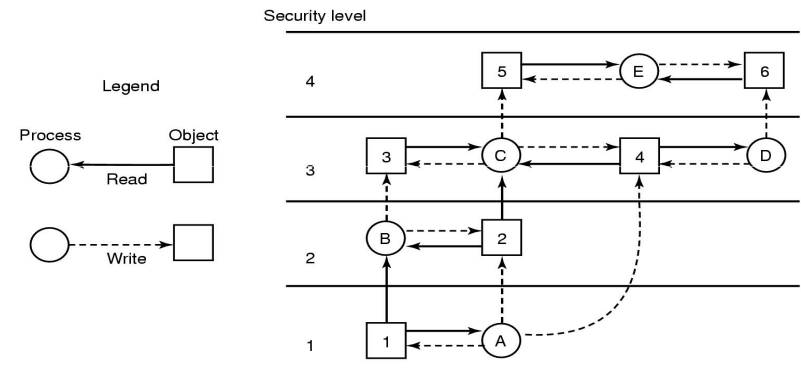
	Objects		
	Compiler	Mailbox 7	Secret
Eric	Read Execute		
Henry	Read Execute	Read Write	
Robert	Read Execute	Read	Read Write

(b)

(a) State yang diotorisasi

(b) State yang tidak diotorisasi

# Sekuriti Multilevel (1)



## Model Sekuiriti multilevel : Bell-La Padula

## Sekuriti Multilevel (2)



### Model Biba

- Prinsipnya menjamin integritas data
  1. Prinsip Integritas sederhana
    - Proses dapat menulis hanya satu kali pada objek dengan tingkat keamanan rendah
  2. Integrity \* property
    - Proses dapat membaca hanya objek dengan tingkat keamanan tinggi