PERTEMUAN 14:
KEAMANAN SISTEM DAN PROTEKSI

A. TUJUAN PEMBELAJARAN

Pada bab ini akan dijelaskan mengenai jenis-jenis keamanan sistem dan proteksi, Anda harus mampu:

1.1 Penyebab data hilang

1.2 Intruder

1.3 Membedakan keamanan sistem dan proteksi

B. URAIAN MATERI

Tujuan Pembelajaran 1.1:
Penyebab data hilang

Sistem operasi hanya satu bagian kecil dari seluruh perangkat lunak di suatu sistem. Tetapi karena sistem operasi mengendalikan pengaksesan ke sumber daya, dimana perangkat lunak lain meminta pengaksesan sumber daya lewat sistem operasi maka sistem operasi menempati posisi yang penting dalam pengamanan sistem. Adapun yang bisa menyebabkan data hilang, seperti

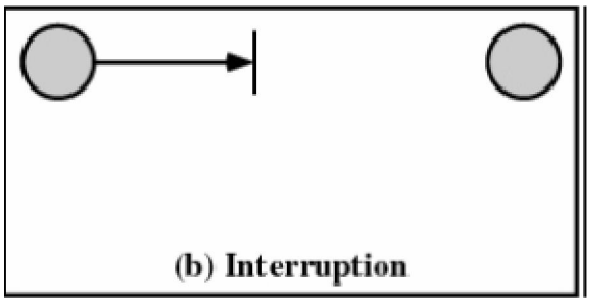
- Bencana alam dan perang
- Kesalahan Hardware atau software, Contohnya CPU malfunction, bad disk, program bugs
- Kesalahan manusia, Contohnya data entry, wrong tape mounted.

Selain itu terdapat ancaman lain pada sistem keamanan komputer yang bisa dikategorikan dalam empat macam Penyusup / Intruder, sehingga sumber daya sistem komputer dihancurkan menjadi tak berguna. Seperti

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

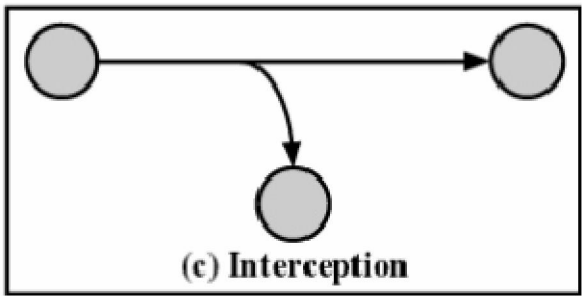
Penyusup / Intruder dikelompokkan menjadi empat bagian:

a. Interupsi, Orang yang tak diotorisasi dapat masuk / mengakses ke sumber daya sistem.
    a. Sumber daya sistem komputer dihancurkan atau menjadi tak tersedia
    b. Penghancuran harddisk
    c. Pemotongan kabel komunikasi
    d. Sistem file management menjadi tidak tersedia



Gambar 14.1 Interupsi

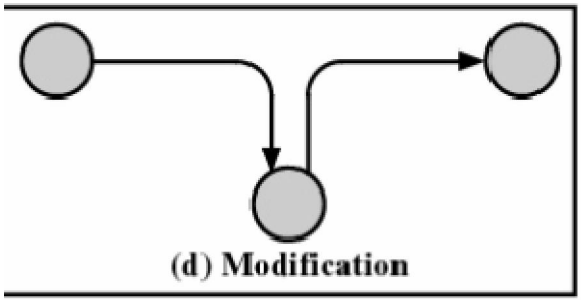
b. Intersepsi
    a. Pihak tak diotorisasi dapat mengakses sumber daya
    b. Ancaman terhadap kerahasiaan data
    c. Penyadapan terhadap data dijaringan
    d. Mengkopi file tanpa diotorisasi



Gambar 14.2 Intersepsi

c. Modification, Orang yang tak diotorisasi tidak hanya dapat mengakses tapi juga mengubah,merusak sumber daya. Ciri – cirinya :
    a. Mengubah nilai-nilai file data

b. Mengubah program sehingga bertindak secara beda
c. Memodifikasi pesan-pesan yang ditransmisikan pada jaringan

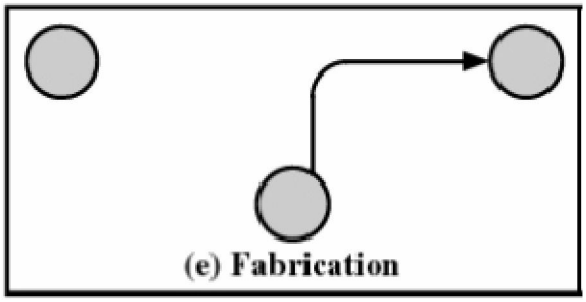


Gambar 14.3 Modification

d. Fabrication, Orang yang tak diotorisasi menyisipkan objek palsu ke dalam sistem.

Ciri-cirinya :

a. Pihak tak diotorisasi menyisipkan objek palsu ke sistem
b. Memasukkan pesan-pesan palsu ke jaringan
c. Penambahan record ke file



Gambar 14.4 Fabrication

Keamanan sistem

Adapun aspek keamanan sistem pada sistem operasi

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

Prinsip Pengamanan Sistem Komputer

a. Rancangan sistem seharusnya publik

b. Dapat diterima
c. Pemeriksaan otoritas saat itu
d. Kewenangan serendah mungkin
e. Mekanisme yang ekonomis

Kebanyakan proteksi didasarkan asumsi sistem mengetahui identitas pemakai. Masalah identifikasi pemakai ketika login disebut autotentikasi pemakai (user authentication). Kebanyakan metode otentifikasi didasarkan pada tiga cara, yaitu :

Autentikasi pemakai, Suatu yang diketahui pemakai, misalnya :

a. passsword
b. kombinasi kunci
c. nama kecil ibu, dsb

Sesuatu yang dimiliki pemakai, misalnya :

a. badge
b. kartu identitas
c. kunci, dsb

Sesuatu mengenai(merupakan ciri) pemakai, misalnya ::

a. sidik jari
b. sidik suara
c. foto
d. tanda tangan, dsb

Contoh Autentikasi

Password

Pemakai memilih satu kata kode, mengingatnya dan mengetikkan saat akan mengakses sistem komputer. Saat diketikkan, komputer tidak menampilkan dilayar. Teknik ini mempunyai kelemahan yang sangat banyak dan mudah ditembus. Pemakai cenderung memilih password yang mudah diingiat. Seseorang yang kenal dengan pemakai dapat mencoba login dengan sesuatu yang diketahuinya mengenai pemakai.

Proteksi password dapat ditembus dengan mudah, antara lain :

- Terdapat file berisi nama depan, nama belakang, nama jalan, nama kota dari kamus ukuran sedang, disertai dengan pengejaan dibalik), nomor plat mobil yang valid, dan string-string pendek karakter acak.
- Isian di file dicocokkan dengan file password. Upaya untuk lebih mengamankan proteksi password, antara lain :

  1. Salting.

     Menambahkan string pendek ke string password yang diberikan pemakai sehingga mencapai panjang password tertentu.

  2. One time password.

     Pemakai harus mengganti password secara teratur. Upaya ini membatasi peluang password telah diketahui atau dicoba-coba pemakai lain. Bentuk ekstrim pendekatan ini adalah one time password, yaitu pemakai mendapat satu buku berisi daftar password. Setiap kali pemakai login, pemakai menggunakan password berikutnya yang terdapat di daftar password Dengan one time password, pemakai direpotkan keharusan menjaga agar buku passwordnya jangan sampai dicuri.

  3. Satu daftar panjang pertanyaan dan jawaban.

     Variasi terhadap password adalah mengharuskan pemakai memberi satu

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

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

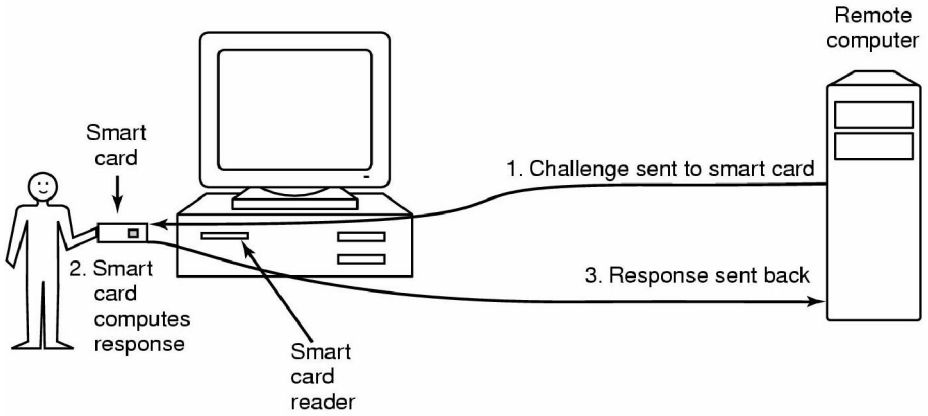
Contoh Autentikasi Menggunakan Objek Fisik

Identifikasi Fisik

Pendekatan lain adalah memberikan yang dimiliki pemakai, seperti :

a. Magnetic cards (Kartu berpita magnetic)

Kartu pengenal dengan selarik pita magnetik. Kartu ini disisipkan ke suatu perangkat pembaca kartu magnetik jika akan mengakses komputer. Teknik ini biasanya dikombinasikan dengan password, sehingga pemakai dapat login system komputer bila memenuhi dua syarat berikut : Mempunyai kartu dan mengetahui password yang spesifik kartu itu. Contohnya ATM, merupakan mesin yang bekerja dengan cara ini.



Gambar 14.5 Objek Fisik

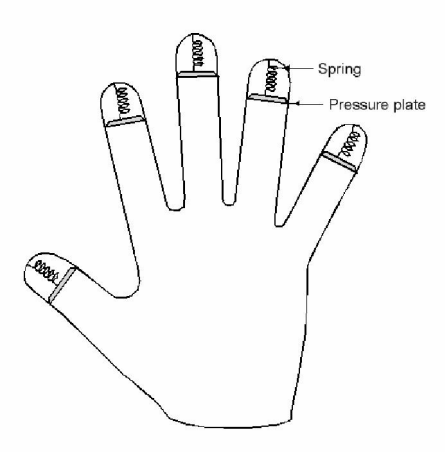
Magnetic cards

a. magnetic stripe cards
b. chip cards: stored value cards, smart cards

b. Autentikasi Menggunakan Biometric (sidik jari)

Pendekatan lain adalah mengukur ciri fisik yang sulit ditiru, seperti :

- Sidik jari dan sidik suara.
- Analisis panjang jari.
- Pengenalan visual dengan menggunakan kamera diterapkan.



Gambar 14.6 Biometric

Countermeasures (Tindakan Balasan)

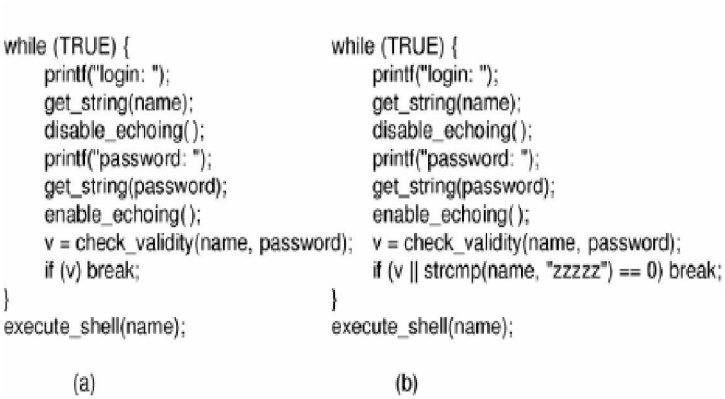
a. Pembatasan waktu ketika seseorang login
b. Panggilan otomatis pada nomor yang disiapkan
c. Pembatasan upaya melakukan login
d. Ketersediaan database login
e. Penggunaan simple login sebagai perangkap

Sekuriti Sistem Operasi

Logic Bomb adalah 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);
```

(a)

```
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);
```

(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 kemamapuan akses sesedikit mungkin
-Mekanisme proteksi sederhana, uniform dan buil in kelapis terbawah
-Skema pengamanan harus dapat diterima secara psikologis

Sekuriti Jaringan Komputer

-Ancaman Eksternal
-Kode ditransfer kemesin target
-Saat kode dieksekusi, kerusakan pun terjadi
-Tujuan virus ditulis dijaringan 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 menganngur sampai terjadi suatu kejadian tertentu

-Fase Propagasi

Virus menempatkan kopi dirinya keprogram lain didisk.

-Fase Pemicuan (Triggering Phase)

Virus diaktifkan untuk melakukan fungsi tertentu

-Fase Eksekusi

Virus menjalankan fungsinya.

Tipe-tipe Virus

-Parasitic Virus

Menggantung kefile .exe dan melakukan replikasi ketika file tersebut dieksekusi

- Memory Resident Virus

Menempatkan diri kemeori utama dan menginfeksi setiap program yang dieksekusi

-Boot Sector Virus

Menginfeksiboot record danmenyebarsaatsistemdiboot

-Stealth Virus

Bentuknyadirancangagar tidakterdeteksiolehantivirus

-Polymorphic Virus

Bermutasi setiap kali melakukan infeksi

Anti virus

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 featue protection

C. SOAL LATIHAN/TUGAS

1. Buatlah contoh Login berhasil?
2. Buatlah contoh Login ditolak setelah nama dimasukkan?
3. Buatlah contoh Login ditolak setelah nama dan password ?

D. DAFTAR PUSTAKA

Buku

Bambang Hariyanto. 1997. Sistem Operasi, Bandung:Informatika Bandung.

Dali S. Naga. 1992. Teori dan Soal Sistem Operasi Komputer,Jakarta: Gunadarma.

Silberschatz Galvin. 1995. 4 Edition Operating System Concepts: Addison Wesley.

Sri Kusumadewi. 2000. Sistem Operasi. Yogyakarta: J&J Learning.

Tanenbaum, A.1992. Modern Operating Systems.New York: Prentice Hall

Link and Sites:

http://www.ilmukomputer.com
http://vlsm.bebas.org
http://www.wikipedia.com