SISTEM OPERASI

KEAMANAN SISTEM

Pendahuluan

- Sistem time-sharing dan akses jarak jauh menyebabkan kelemahan komunikasi data dan penyebab masalah keamanan
- Sistem operasi merupakan bagian kecil dari keseluruhan s/w di suatu sistem, tetapi karena peran sistem operasi mengendalikan akses ke sumber daya terhadap s/w lain maka posisinya penting
- Keamanan sistem operasi merupakan bagian masalah keamanan sistem komputer secara total

Keamanan sistem komputer

- Adalah untuk menjamin sumber daya tidak digunakan atau dimodifikasi orang yang tidak diotorisasi
- Pengamanan termasuk masalah :
  - Teknis
  - Manajerial
  - Legalitas
  - Politis

Pembagian Keamanan Sistem

- Keamanan eksternal (external security)
  - Berkaitan dengan pengamanan fasilitas komputer dari penyusup dan bencana seperti kebakaran atau kebanjiran
- Keamanan interface pemakai (user interface security)
  - Berkaitan dengan identifikasi pemakai sebelum pemakai diijinkan mengakses program dan data yang disimpan

- Keamanan internal (internal security)
  - Berkaitan dengan pengamanan beragam kendali yang dibangun pada perangkat keras dan sistem operasi yang menjamin operasi yang handal dan tak terkorupsi untuk menjaga integritas program dan data
- Beda security dan protection

Masalah-masalah Keamanan

- Dua masalah penting pada security:
  - Data Loss (Kehilangan data)
  - Intruder/hacker (penyusup)
- Kehilangan data dapat disebabkan :
  - Bencana
  - Kesalahan perangkat keras dan lunak
  - Kesalahan /kelalaian manusia

Bencana

- Kebakaran
- Banjir
- Gempa bumi
- Perang
- Kerusuhan
- Kerusakan oleh binatang

Kesalahan perangkat keras & lunak

- Disfungsi dari processor
- Disk atau tape yang tidak terbaca
- Kesalahan telekomunikasi
- Kesalahan program (bugs)

Kesalahan / kelalaian manusia

- Kesalahan pemasukkan data
- Memasang tape atau disk yang salah
- Eksekusi program yang salah
- Kehilangan disk atau tape

Cara pencegahan

- Mengelola beberapa backup ,dan backup ditempatkan jauh dari data yang online
- Membuat fasilitas pencegah bencana
  - Racun api
  - Alarm kebakaran
  - Lokasi bebas banjir
  - Training

Intruder (penyusup)

- Penyusup pasif
  - Hanya membaca data yang tak diotorisasi
- Penyusup aktif
  - Membaca dan mengubah data yang tak diotorisasi

Kategori penyusupan

- Lirikan mata pemakai non-teknis
  - (user yang mengakses fasilitas yang bukan haknya >> password)
- Penyadapan oleh orang dalam
- Usaha hacker dalam mencari uang
- Spionase militer/bisnis

Kebutuhan keamanan sistem komputer

- Kerahasiaan (*secrecy)*
  - Keterjaminan bahwa informasi di sistem komputer hanya dapat diakses oleh pihak-pihak yang diotorisasi

- Integritas (*integrity*)
  - Keterjaminan bahwa sumber daya sistem komputer dimodifikasi oleh pihak yang berhak dan tetap menjaga konsistensi dan keutuhan data di sistem

- Ketersediaan (*availability*)
  - Keterjaminan bahwa sumber daya sistem komputer selalu tersedia bagi pihak-pihak yang diotorisasi di saat diperlukan

Ancaman-ancaman keamanan

- Interuption (interupsi)
  - Sumber daya sistem komputer dihancurkan atau menjadi tak tersedia/tidak berfungsi (ancaman bagi availability)
- Contoh
  - Penghancuran perangkat keras (harddisk)
  - Pemotongan kabel komunikasi

- Interception (intersepsi)
  - Pihak yang tak diotorisasi (berupa orang atau program komputer) dapat mengakses sumber daya.
  - Ancaman bagi secrecy
- Contoh :
  - Penyadapan untuk mengambil data rahasia
  - Mengkopi file tanpa otorisasi

- Modification (modifikasi)
  - Pihak tak diotorisasi tidak hanya mengakses tapi juga merusak sumber daya
  - Ancaman terhadap integritas
- Contoh :
  - Mengubah nilai-nilai file data
  - Mengubah kode program
  - Memodifikasi pesan pada jaringan

- Fabrication (fabrikasi)
  - Pihak yang tak diotorisasi menyisipkan/ memasukkan objek-objek palsu ke sistem
  - Ancaman terhadap integritas data
- Contoh:
  - Memasukkan pesan-pesan palsu ke jaringan
  - Penambahan record ke file

Petunjuk Pengamanan Sistem

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

Otentifikasi pemakai

User authentication :

- Sesuatu yang diketahui pemakai
  - Pasword
  - Kombinasi kunci
  - Nickname

- Sesuatu yang dimiliki pemakai
  - Badge
  - Identity card
  - Kunci
- Sesuatu yang menjadi ciri pemakai
  - Sidik jari
  - Sidik suara
  - Foto
  - Tanda tangan

Password

- Upaya pengamanan proteksi password:
  - Salting
  - One-time password
  - 1 daftar panjang pertanyaan dan jawaban
  - Tantangan dan tanggapan

Identifikasi Fisik

- Kartu berpita magnetik
- Sidik fisik
  - Sidik jari, suara, kornea
  - Analisis panjang jari
  - Pengenalan visual dengan kamera
- Analisis tanda tangan
- Analisis suatu yang dipunyai pemakai
- Analisis darah

Pembatasan

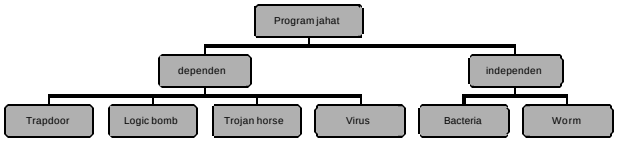
- Pembatasan login
- Pembatasan dengan call-back
- Pembatasan jumlah usaha login

Mekanisme proteksi sistem komputer

- Objek perangkat keras
- Pemroses
- Segment memori
- Terminal
- Disk drive
- Printer

- Objek perangkat lunak
- Proses
- File
- Basisdata
- Semaphore

Program-program jahat



Bacteria

- Program yang mengkonsumsi sumber daya sistem dengan mereplikasi dirinya sendiri
- Bacteria tidak secara eksplisit merusak file
- Dengan cepat mengambil alih seluruh kapasitas pemroses, memori atau ruang disk
- Mengakibatkan penolakan pengaksesan pemakai ke sumber daya

Logic Bomb

- Logik yang ditempelkan pada program komputer agar memeriksa suatu kumpulan kondisi di sistem
- Di-set 'meledak' pada program legal, dan akan akan merusak dengan mengubah,menghapus data, mesin berhenti pada kondisi tertentu misalnya hari/tanggal tertentu

Trapdoor

- Kode yang menerima suatu barisan masukan khusus (ID pemakai)
- Titik masuk tak terdokumentasi rahasia di satu program untuk memberikan akses tanpa metode-metode otentifikasi normal
- Dipakai oleh programmer untuk mencari kesalahan program (error program)

Trojan Horse

- Rutin tak terdokumentasi rahasia yang ditempelkan dalam suatu program berguna dan mengandung kode tersembunyi yang ketika dijalankan melakukan suatu fungsi yang tak diinginkan

Virus

- Kode yang ditempelkan dalam satu program yang menyebabkan pengkopian dirinya disisipkan ke satu program lain atau lebih
- Menular melalui pertukaran disk/ data melalui jaringan

Worm

- Program yang dapat mereplikasi dirinya dan mengirim kopian-kopian dari komputer ke komputer lewat hubungan jaringan
- Contoh : network worm

Virus dan Antivirus

- Virus dapat mencantolkan dirinya ke program lain dan mengeksekusi kodenya secara rahasia setiap kali program induk berjalan
- Masalah: virus sering merusak sistem komputer seperti menghapus file, partisi disk, atau mengacaukan program

Siklus Hidup Virus

- Fase tidur (dormant phase)
  - Virus dalam keadaan menganggur dan dapat aktif pada kondisi tertentu, mis: tgl tertentu, kehadiran file/program tertentu, kapasitas disk yang melewati batas
  - Tidak semua virus memiliki fase ini

- Fase Propagasi (propagation phase)
  - Virus menempatkan kopian dirinya ke program lain atau daerah sistem tertentu di disk.
  - Program yang terinfeksi akan mempunyai kloning virus dan dapat kembali memasuki fase tersebut

- Fase Pemicuan (Triggering Phase)
  - Virus diaktifkan untuk melakukan fungsi tertentu.
  - Disebabkan kondisi tertentu ,seperti penghitungan jumlah kopian, men-delete nya

- Fase Eksekusi (Execution Phase)
  - Virus menjalankan fungsinya, seperti tampilan pesan, merusak program/file data
  - Kebanyakan aktif pada OS/Platform perangkat tertentu
  - Dirancang memanfaatkan kelemahan-kelemahan sistem tertentu

Tipe-Tipe Virus

- **Parasitic Virus**
  - Menyerang file-file .exe
- **Memory Resident Virus**
  - Menyerang memory utama
- **Boot Sector Virus**
  - Menyerang master boot record
- **Stealth Virus**
  - Dapat menyembunyikan diri dari deteksi antivirus
- **Polymorphic Virus**
  - Dapat bermutasi setiap kali menginfeksi

Antivirus

- Antivirus berfungsi untuk mencegah masuknya virus dengan cara :
- Deteksi
  - Mengecek apakah terinfeksi dan mencari lokasinya
- Identifikasi
  - Mengenal ciri-ciri virus
- Penghilangan
  - Menghapus semua jejak virus dari program yang terinfeksi dan kembalikan ke semula

Generasi Antivirus

- Generasi I
  - Sekedar scanner sederhana
- Generasi II
  - Scanner yang pintar (heuristic scanner)
- Generasi III
  - Jebakan-jebakan aktivitas (activity trap)
- Generasi IV
  - Proteksi penuh (full-featured protection)