PENGAMANAN SISTEM OPERASI

Materi :

1. Perancangan sistem operasi yang aman
2. Bentuk serangan terhadap sistem operasi
3. Tinjauan terhadap sistem operasi yang aman

Saat ini sistem komputer yang terpasang makin mudah diakses, sistem time-sharing dana akses jarak jauh menyebabkan kelemahan komuniksai data menjadi pokok masalah keamanan. Terlebih dengan meningkatnya perkembangan jaringan komputer. Kecenderungan lain saat ini adalah memberi tanggungjawab pengelolaan aktivitas pribadi dan bisnis ke komputer, seperti :

- Sistem transfer dana elektronis (electronic fund transfer system) melewatkan uang sebagai aliran bit.
- Sistem kendali lalu-lintas udara (air trafic control system) melakukan banyak kerja yang sebelumnya ditangani pengendali manusia.
- Unit rawat intensif di rumah sakit sudah sangat terkomputerisasi.
- Dan sebagainya.

Implementasi pengamanan sangat penting untuk menjamin sistem tidak diinterupsi dan diganggu. Proteksi dan pengamanan terhadap perangkat keras dan system operasi sama pentingnya. 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.

Pengamanan perangkat lunak cenderung memfokuskan pada pengamanan system operasi, karena perangkat lunak aplikasi juga memberi resiko keamanan.Keamanan sistem operasi merupakan bagian masalah keamanan sistem computer secara total. Pengamanan sistem operasi berarti kecil jika setiap orang dapat melenggang di ruang sistem komputer. Pengamanan secara fisik dengan membatasi pengaksesan fisik secara langsung dengan fasilitas sistem computer harus dilakukan juga.

1. KEAMANAN

Keamanan sistem komputer adalah untuk menjamin sumber daya tidak digunakan atau dimodifikasi orang tak terotorisasi. Pengamanan termasuk masalah teknis, manajerial, legalitas dan politis.

Keamanan sistem terbagi menjadi tiga, yaitu :

1. Keamanan eksternal (external security).
   Berkaitan dengan pengamanan fasilitas komputer dari penyusup (hacker) dan bencana seperti kebakaran dan kebanjiran.
2. Keamanan interface pemakai (user interface security).
   Berkaitan dengan identifikasi pemakai sebelum pemakai diijinkan mengakses program dan data yang disimpan.
3. 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. Istilah keamanan (security) dan proteksi (protection) sering digunakan secara bergantian. Untuk menghindari kesalahpahaman, istilah keamanan mengacu ke seluruh masalah keamanan dan istilah mekanisme proteksi mengacu ke mekanisme sistem yang digunakan untuk memproteksi/melindungi informasi pada sistem komputer.

2. MASALAH-MASALAH KEAMANAN

Terdapat dua masalah penting, yaitu :

a. Kehilangan data (data loss).
   Dapat disebabkan karena :
   a.1. Bencana.
   - o Kebakaran.
   - o Banjir.
   - o Gempa bumi.
   - o Perang.
   - o Kerusuhan.
   - o Binatang.

a.2. Kesalahan perangkat keras dan perangkat lunak.
   - o Ketidak berfungsian pemroses.
   - o Disk atau tape yang tidak terbaca.
   - o Kesalahan telekomunikasi.
   - o Kesalahan program (bugs).

a.3. Kesalahan/kelalaian manusia.

- o Kesalahan pemasukan data.
- o Memasang tape atau disk yang salah.
- o Eksekusi program yang salah.
- o Kehilangan disk atau tape.

Kehilangan data dapat diatasi dengan mengelola beberapa backup dan backup ditempatkan jauh dari data yang online.

b. Penyusup (hacker).
Terdiri dari :
b.1. Penyusup pasif, yaitu yang membaca data yang tak diotorisasi.
b.2 Penyusup aktif, yaitu yang mengubah data yang tak diotorisasi.
Kateogri penyusupan :

- o Lirikan mata pemakai non teknis. Pada sistem time-sharing, kerja pemakai dapat diamati orang sekelilingnya. Bila dengan lirikan itu dapat mengetahui apa yang diketik saat pengisian password, maka pemakai non teknis dapat mengakses fasilitas yang bukan haknya.
- o Penyadapan oleh orang dalam.
- o Usaha hacker dalam mencari uang.
- o Spionase militer atau bisnis.

3. ANCAMAN-ANCAMAN KEAMANAN

Sasaran pengamanan adalah menghindari, mencegah dan mengatasi ancaman terhadap sistem. Kebutuhan keamanan sistem komputer dikategorikan tiga aspek, yaitu :

1. Kerahasiaan (secrecy).
   Adalah keterjaminan bahwa informasi disistem komputer hanya dapat diakses oleh pihak-pihak yang diotorisasi dan modifikasi tetap menjaga konsistensi dan keutuhan data di sistem.
2. Integritas (integrity).
   Adalah keterjaminan bahwa sumber daya sistem komputer hanya dapat dimodifikasi oleh pihak-pihak yang diotorisasi.
3. Ketersediaan (availability).
   Adalah keterjaminan bahwa susmber daya sistem komputer tersedia bagi pihakpihak yang diotorisasi saat diperlukan.

Tipe-tipe ancaman terhadap keamanan sistem dapat dimodelkan dengan memandang fungsi sistem komputer sebagai penyedia informasi.

Berdasarkan fungsi ini, ancaman terhadap sistem komputer dapat dikategorikan menjadi empat ancaman, yaitu :
1. Interupsi (interuption).
Sumber daya sistem komputer dihancurkan atau menjadi tak tersedia atau tak berguna. Interupsi merupakan ancaman terhadap ketersediaan.
Contoh : penghancuran bagian perangkat keras, seperti harddisk, pemotongan kabel komunikasi.
2. Intersepsi (interception).
Pihak tak diotorisasi dapat mengakses sumber daya. Interupsi merupakan ancaman terhadap kerahasiaan. Pihak tak diotorisasi dapat berupa orang atau program komputer.
Contoh : penyadapan untuk mengambil data rahasia, mengetahui file tanpa diotorisasi.
3. Modifikasi (modification).
Pihak tak diotorisasi tidak hanya mengakses tapi juga merusak sumber daya.
Modifikasi merupakan ancaman terhadap integritas.
Contoh : mengubah nilai-nilai file data, mengubah program sehingga bertindak secara berbeda, memodifikasi pesan-pesan yang ditransmisikan pada jaringan.
4. Fabrikasi (fabrication).
Pihak tak diotorisasi menyisipkan/memasukkan objek-objek palsu ke sistem.
Fabrikasi merupakan ancaman terhadap integritas.
Contoh : memasukkan pesan-pesan palsu ke jaringan, penambahan record ke file.

4. PETUNJUK PENGAMANAN SISTEM

Terdapat beberapa prinsip pengamanan sistem komputer, yaitu :
1. Rancangan sistem seharusnya publik.
Keamanan sistem seharusnya tidak bergantung pada kerahasiaan rancangan mekanisme pengamanan. Mengasumsikan penyusup tidak akan mengetahui cara kerja sistem pengamanan hanya menipu/memperdaya perancang sehingga tidak membuat mekanisme proteksi yang bagus.
2. Dapat diterima.
Skema yang dipilih harus dapat diterima secara psikologis. Mekanisme proteksi seharusnya tidak menganggu kerja pemakai dan memenuhi kebutuhan otorisasi pengaksesan. Jika mekanisme tidak mudah digunakan maka tidak akan digunakan atau digunakan secara tak benar.
3. Pemeriksaan otoritas saat itu.

Sistem tidak seharusnya memeriksa ijin dan menyatakan pengaksesan diijinkan, serta kemudian menetapkan terus informasi ini untuk penggunaan selanjutnya. Banyak sistem memeriksa ijin ketika file dibuka dan setelah itu (operasi-operasi lain) tidak diperiksa. Pemakai yang membuka file dan lupa menutup file akan terus dapat walaupun pemilik file telah mengubah atribut proteksi file.

4. Kewenangan serendah mungkin.

Program atau pemakai sistem seharusnya beroperasi dengan kumpulan wewenang serendah mungkin yang diperlukan untuk menyelesaikan tugasnya. Default sistem yang digunakan harus tak ada akses sama sekali.

5. Mekanisme yang ekonomis.

Mekanisme proteksi seharusnya sekecil, sesederhana mungkin dan seragam sehingga memudahkan verifikasi. Proteksi seharusnya dibangun dilapisan terbawah. Proteksi merupakan bagian integral rancangan sistem, bukan mekanisme yang ditambahkan pada rancangan yang telah ada.

5. OTENTIFIKASI PEMAKAI

Kebanyakan proteksi didasarkan asumsi sistem mengetahui identitas pemakai. Masalah identifikasi pemakai ketika login disebut otentifikasi pemakai (user authentication).

Kebanyakan metode otentifikasi didasarkan pada tiga cara, yaitu :

1. Sesuatu yang diketahui pemakai, misalnya :
o Password.
o Kombinasi kunci.
o Nama kecil ibu mertua.
o Dan sebagainya.
2. Sesuatu yang dimiliki pemakai, misalnya :
o Badge.
o Kartu identitas.
o Kunci.
o Dan sebagainya.
3. Sesuatu mengenai (ciri) pemakai, misalnya :
o Sidik jari.
o Sidik suara.
o Foto.
o Tanda tangan.

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 diingat.
Seseorang yang kenal dengan pemakai dapat mencoba login dengan sesuatu yang diketahuinya mengenai pemakai.

Proteksi password dapat ditembus dengan mudah, antara lain :
o 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.
o 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 daftar pertanyaan panjang dan jawabannya. Pertanyaan-pertanyaan dan jawabannya dipilih pemakai sehingga pemakai mudah mengingatnya dan tak perlu menuliskan di kertas.
Pertanyaan berikut dapat dipakai, misalnya :
o Siapa mertua abang ipar Badru ?
o Apa yang diajarkan Pak Harun waktu SD ?
o Di jalan apa pertama kali ditemukan simanis ?

Pada saat login, komputer memilih salah satu dari pertanyaan-pertanyaan secara acak, menanyakan ke pemakai dan memeriksa jawaban yang diberikan.

4. Tantangan tanggapan (chalenge response).
Pemakai diberi kebebasan memilih suatu algoritma, misalnya x3. Ketika pemakai login, komputer menuliskan di layar angka 3. Dalam kasus ini pemakai mengetik angka 27. Algoritma dapat berbeda di pagi, sore, dan hari berbeda, dari terminal berbeda, dan seterusnya.

Identifikasi fisik
Pendekatan lain adalah memberikan yang dimiliki pemakai, seperti :
Kartu berpita magnetik
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 sistem komputer bila memenuhi dua syarat berikut :
o Mempunyai kartu.
o Mengetahui password yang spesifik kartu itu.
ATM merupakan mesin yang bekerja dengan cara ini.
Sidik jari
Pendekatan lain adalah mengukur ciri fisik yang sulit ditiru, seperti :
o Sidik jari dan sidik suara.
o Analisis panjang jari.
o Pengenalan visual dengan menggunakan kamera diterapkan.
o Dan sebagainya.

6. PEMBATASAN
Pembatasan-pembatasan dapat dilakukan sehingga memperkecil peluang penembusan oleh pemakai yang tak diotorisasi, misalnya :

o Pembatasan login.
Login hanya diperbolehkan :
> Pada terminal tertentu.
> Hanya ada waktu dan hari tertentu.
> Pembatasan dengan call-back.
Login dapat dilakukan siapapun. Bila telah sukses login, sistem segera memutuskan koneksi dan memanggil nomor telepon yang telah disepakati.
Penyusup tidak dapat menghubungi lewat sembarang saluran telepon, tapi hanya pada saluran telepon tertentu.

> Pembatasan jumlah usaha login.
Login dibatasi sampai tiga kali dan segera dikunci dan diberitahu ke administrator.
Semua login direkam dan sistem operasi melaporkan informasi-informasi berikut :
>> Waktu, yaitu waktu pemakai login.
>> Terminal, yaitu terminal dimana pemakai login.

Mekanisme proteksi sistem komputer
Pada sistem komputer banyak objek yang perlu diproteksi, yaitu :
1. Objek perangkat keras.
Objek yang perlu diproteksi, antara lain :
o Pemroses.
o Segment memori.
o Terminal.
o Disk drive.
o Printer.
o Dan sebagainya.
2. Objek perangkat lunak.
Objek yang perlu diproteksi, antara lain :
o Proses.
o File.
o Basis data.
o Semaphore.
o Dan sebagainya.

Access Control Matrix
Masalah proteksi adalah mengenai cara mencegah proses-proses mengakses objek-objek yang tidak diotorisasi. Mekanisme ini juga harus memungkinkan membatasi proses-proses ke suatu subset operasi-operasi legal yang diperlukan. Misalnya proses A dapat membaca file F, tapi tidak menulisinya.
Agar dapat menyediakan mekanisme proteksi berbeda dikembangkan berdasar konsep domain. Domain adalah himpunan pasangan (hak, objek). Tiap pasangan menspesifikasikan objek dan suatu subset operasi yang dapat dilakukan terhadapnya. Hak dalam konteks ini berarti ijin melakukan suatu operasi.
Proses berjalan pada suatu domain proteksi, yaitu proses merupakan anggota suatu domain atau beberapa domain. Terdapat kumpulan objek yang dapat diakses proses. Untuk tiap objek, proses mempunyai suatu kumpulan hak

terhadap objek itu. Proses-proses dapat juga beralih dari satu domain ke domain lain selama eksekusi. Aturan peralihan domain ini bergantung pada sistem.
Domain ditetapkan dengan mendaftarkan pemakai-pemakai yang termasuk domain itu. Proses-proses yang dijalankan pemakai adalah proses-proses pada domain itu dan mempunyai hak akses terhadap objek seperti ditentukan domainnya.

Cara penyimpanan informasi anggota domain

Secara konseptual adalah berupa satu matriks besar, dimana :
o Baris menunjukkan domain.
o Kolom menunjukkan objek.
Tiap elemen matriks mendaftar hak-hak yang dimiliki domain terhadap objek. Dengan matriks ini, sistem dapat mengetahui hak pengaksesan terhadap objek. Gambar berikut menunjukkan matriks pengaksesan objek.

	File 1	File 2	Printer 1	Plotter 1	Modem 1
Domain 1	Read	Read Write	Write		
Domain 2	Read			Write	Write
Domain 3		Read Write Execute	Write	Write	Write

Gambar 9.2 : Matriks pengaksesan objek

Untuk sistem-sistem yang mengijinkan peralihan domain dimodelkan dengan menganggap domain sebagai objek, yaitu :
o Jika terdapat operasi enter, berarti mempunyai hak berpindah domain.
Untuk sistem-sistem yang mengijinkan peralihan domain dimodelkan dengan menganggap domain sebagai objek, yaitu :
o Jika terdapat operasi enter, berarti mempunyai hak berpindah domain.

	File 1	File 2	Printer 1	Plotter 1	Modem 1	Domain 1	Domain 1	Domain3
Domain 1	Read	Read Write	Write				Enter	
Domain 2	Read			Write	Write	Enter		
Domain 3		Read Write	Write	Write	Write			

Gambar 9.3 : Matriks pengaksesan objek dengan operasi peralihan domain

Gambar diatas menunjukkan matriks pengaksesan objek dengan operasi pengalihan domain. Proses-proses pada domain 1 dapat berpindah ke domain 2 dan proses pada domain 2 dapat berpindah ke domain 1.

ACL (Access Control List)

Matriks pengaksesan objek akan berbentuk matrik jarang (sparse matrix). Matrik jarang memboroskan ruang penyimpanan dan lambat karena memerlukan ruang besar, Dua alternatif untuk memperbaikinya adalah :

o Menyimpan matriks sebagai perbaris.

o Menyimpan matriks sebagai perkolom.

Teknik yang digunakan adalah mengasosiasikan tiap objek dengan senarai terurut berisi semua domain yang boleh mengakses dan operasi-operasi yang dibolehkan (bagaimana). Temnik ini menghasilkan senarai disebut ACL.

Contoh :

File 1	: (Yani, *, rwx), (Soni, *, rw-)
File 2	: (Yani, system, rwx)
Printer 1	: (Yani, *, -w-), (Elsa, karyawan, -w-)
Plotter 1	: (Yusuf, *, -w-)
Modem 1	: (Yuniar, *, -w-)

Gambar 9.4 : ACL (Access Control List)

Tiap ACL yang disebutkan di kurung menyatakan komponen uid (user ID), gid (group ID) dan hak akses. Dengan ACL, dimungkinkan mencegah uid, gid spesifik mengakses objek sementara mengijinkan yang lain. Pemilik objek dapat mengubah ACL kapanpun.Cara ini untuk mempermudah pencegahan/pelarangan pengaksesan yang sebelumnya diperbolehkan. Penyimpanan dilakukan hanya untuk isian yang tak kosong.

Kapabilitas

Cara lain adalah memecah matrik perbaris. Diasosiasikan tiap proses satu daftar objek yang boleh diakses, bila terdapat tanda operasi yang diijinkan padanya atau domainnya.

Senarai ini disebut senarai kapabilitas (capabilities list). Contoh :

	Tipe	Hak	Objek
0	Berkas	Rwx	Pointer ke file 2
1	Printer	-w-	Pointer ke printer 1
2	Plotter	-w-	Pointer ke plotter 1
3	Modem	-w-	Pointer ke modem 1

Gambar 9.5 : Senarai kapabilitas untuk domain 3 dari gambar 9.2

Ancaman-ancaman canggih terhadap sistem komputer adalah program yang mengeksploitasi kelemahan sistem operasi. Kita berurusan dengan program aplikasi begitu juga program utilitas seperti editor dan kompilator.

Terdapat taksonomi ancaman perangkat lunak atau klasifikasi program jahat (malicious program), yaitu :

1. Program-program yang memerlukan program inang (host program).
Fragmen program tidak dapat mandiri secara independen dari suatu program aplikasi, program utilitas atau program sistem.

2. Program-program yang tidak memerlukan program inang.
Program sendiri yang dapat dijadwalkan dan dijalankan oleh sistem operasi.

Pembagian atau taksonomi menghasilkan tipe-tipe program jahat sebagai berikut :

1. Bacteria.
Bacteria adalah program yang mengkonsumsi sumber daya sistem dengan mereplikasi dirinya sendiri. Bacteria tidak secara eksplisit merusak file. Tujuan program ini hanya satu yaitu mereplikasi dirinya.
Program bacteria yang sederhana bisa hanya mengeksekusi dua kopian dirinya secara simultan pada sistem multiprogramming atau menciptakan dua file baru, masing-masing adalah kopian file program bacteria.
Kedua kopian in kemudian mengkopi dua kali, dan seterusnya.

2. Logic bomb.
Logic bomb adalah logik yang ditempelkan pada program komputer agar memeriksa suatu kumpulan kondisi di sistem. Ketika kondisi-kondisi yang dimaksud ditemui, logik mengeksekusi suatu fungsi yang menghasilkan aksi-aksi tak diotorisasi.
Logic bomb menempel pada suatu program resmi yang diset meledak ketika kondisi-kondisi tertentu dipenuhi. Contoh kondisi-kondisi untuk memicu logic bomb adalah ada atau tudak adanya file-file tertentu, hari tertentu baru minggu atau tanggal, atau pemakai menjalankan aplikasi tertentu.
Begitu terpicu, bomb mengubah atau menghapus data atau seluruh file, menyebabkan mesin terhenti, atau mengerjakan perusakan lain.

3. Trapdoor.
Trapdoor adalah titik masuk tak terdokumentasi rahasia di satu program untuk memberikan akses tanpa metode-metode otentifikasi normal.
Trapdoor telah dipakai secara benar selama bertahun-tahun oleh pemrogram untuk mencari kesalahan program. Debugging dan testing biasanya dilakukan pemogram saat mengembangkan aplikasi. Untuk program yang mempunyai prosedur otentifikasi atau setup lama atau memerlukan pemakai

memasukkan nilai-nilai berbeda untuk menjalankan aplikasi maka debugging akan lama bila harus melewati prosedur-prosedur tersebut.
Untuk debug program jenis ini, pengembang membuat kewenangan khusus atau menghilangkan keperluan setup dan otentifikasi. Trapdoor adalah kode yang menerima suatu barisan masukan khusus atau dipicu dengan menjalankan ID pemakai tertentu atau barisan kejahatan tertentu. Trapdoor menjadi ancaman ketika digunakan pemrogram jahat untuk memperoleh pengkasesan tak diotorisasi. Pada kasus nyata, auditor (pemeriks) perangkat lunak dapat menemukan trapdoor pada produk perangkat lunak dimana nama pencipta perangkat lunak berlakuk sebagai password yang memintas proteksi perangkat lunak yang dibuatnya. Adalah sulit mengimplementasikan kendali-kendali perangkat lunak untuk trapdoor.

4. Trojan horse.
Trojan horse adalah rutin tak terdokumentasi rahasia ditempelkan dalam satu program berguna. Program yang berguna mengandung kode tersembunyi yang ketika dijalankan melakukan suatu fungsi yang tak diinginkan. Eksekusi program menyebabkan eksekusi rutin rahasia ini. Program-program trojan horse digunakan untuk melakukan fungsi-fungsi secara tidak langsung dimana pemakai tak diotorisasi tidak dapat melakukannya secara langsung. Contoh, untuk dapat mengakses file-file pemakai lain pada sistem dipakai bersama, pemakai dapat menciptakan program trojan horse.
Trojan horse ini ketika program dieksekusi akan mengubah ijin-ijin file sehingga file-file dapat dibaca oleh sembarang pemakai. Pencipta program dapat menyebarkan ke pemakai-pemakai dengan menempatkan program di direktori bersama dan menamai programnya sedemikian rupa sehingga disangka sebagai program utilitas yang berguna. Program trojan horse yang sulit dideteksi adalah kompilator yang dimodifikasi sehingga menyisipkan kode tambahan ke programprogram tertentu begitu dikompilasi, seperti program login. Kode menciptakan trapdoor pada program login yang mengijinkan pencipta log ke system menggunakan password khusus.
Trojan horse jenis ini tak pernah dapat ditemukan jika hanya membaca program sumber. Motivasi lain dari trojan horse adalah penghancuran data. Program muncul sebagai melakukan fungsi-fungsi berguna (seperti kalkulator), tapi juga secara diam-diam menghapus file-file pemakai.
Trojan horse biasa ditempelkan pada program-program atau rutin-rutin yang diambil dari BBS, internet, dan sebagainya.

5. Virus.
Virus adalah kode yang ditempelkan dalam satu program yang menyebabkan

pengkopian dirinya disisipkan ke satu program lain atau lebih.
Program menginfeksi program-program lain dengan memodifikasi program-program itu. Modifikasi itu termasuk memasukkan kopian program virus yang kemudian dapat menginfeksi program-program lain. Selain hanya progasi, virus biasanya melakuka fungsi yang tak diinginkan. Seperti virus biologis, pada virus komputer terdapat kode intruksi yang dapat membuat kpian sempurna dirinya.
Ketika komputer yang terinfeksi berhubungan (kontak) dengan perangkat lunak yang belum terinfeksi, kopian virus memasuki program baru. Infeksi dapat menyebar dari komputer ke komputer melalui pemakai-pemakai yang menukarkan disk atau mengirim program melalui jaringan. Pada lingkungan jaringan, kemampuan mengakses aplikasi dan layanan-layanan komputer lain merupakan fasilitas sempurna penyebaran virus.

6. Worm.
Adalah program yang dapat mereplikasi dirinya dan mengirim kopian-kopian dari komputer ke komputer lewat hubungan jaringan. Begitu tiba, worm diaktifkan untuk mereplikasi dan progasai kembali. Selain hanya propagasi, worm biasanya melakukan fungsi yang tak diinginkan. Network worm menggunakan hubungan jaringan untuk menyebar dari sistem ke sistem lain. Sekali aktif di suatu sistem, network worm dapat berlaku seperti virus atau bacteria, atau menempelkan program trojan horse atau melakukan sejumlah aksi menjengkelkan atau menghancurkan. Untuk mereplikasi dirinya, network worm menggunakan suatu layanan jaringan, seperti :
o Fasilitas surat elektronik (electronic mail facility), yaitu worm mengirimkan kopian dirinya ke sistem-sistem lain.
o Kemampuan eksekusi jarak jauh (remote execution capability), yaitu worm mengeksekusi kopian dirinya di sistem lain.
o Kemampuan login jarak jauh (remote login capability), yaitu worm log pada sistem jauh sebagai pemakai dan kemudian menggunakan perintah untuk mengkopi dirinya dari satu sistem ke sistem lain.
Kopian program worm yang baru kemudian dijalankan di sistem jauh dan melakukan fungsi-fungsi lain yang dilakukan di sistem itu, worm terus menyebar dengan cara yang sama. Network worm mempunyai ciri-ciri yang sama dengan virus komputer, yaitu mempunyai fase-fase sama, yaitu :
o Dormant phase.
o Propagation phase.
o Trigerring phase.
o Execution phase.
Network worm juga berusaha menentukan apakah sistem sebelumnya telah

diinfeksi sebelum mengirim kopian dirinya ke sistem itu.

Tipe-tipe virus

Saat ini perkembangan virus masih berlanjut, terjadi perlombaan antara penulis virus dan pembuat antivirus. Begitu satu tipe dikembangkan antivirusnya, tipe virus yang lain muncul. Klasifikasi tipe virus adalah sebagai berikut :

o Parasitic virus.

Merupakan virus tradisional dan bentuk virus yang paling sering.

Tipe ini mencantolkan dirinya ke file .exe. Virus mereplikasi ketika program terinfeksi dieksekusi dengan mencari file-file .exe lain untuk diinfeksi.

o Memory resident virus.

Virus memuatkan diri ke memori utama sebagai bagian program yang menetap. Virus menginfeksi setiap program yang dieksekusi.

o Boot sector virus.

Virus menginfeksi master boot record atau boot record dan menyebar saat system diboot dari disk yang berisi virus.

o Stealth virus.

Virus yang bentuknya telah dirancang agar dapat menyembunyikan diri dari deteksi perangkat lunak antivirus.

o Polymorphic virus.

Virus bermutasi setiap kali melakukan infeksi. Deteksi dengan penandaan virus tersebut tidak dimungkinkan. Penulis virus dapat melengkapi dengan alat-alat bantu penciptaan virus baru (virus creation toolkit, yaitu rutin-rutin untuk menciptakan virus-virus baru). Dengan alat bantu ini penciptaan virus baru dapat dilakukan dengan cepat. Virus-virus yang diciptakan dengan alat bantu biasanya kurang canggih dibanding virus-virus yang dirancang dari awal.

Antivirus

Solusi ideal terhadap ancaman virus adalah pencegahan. Jaringan diijinkan virus masuk ke sistem. Sasaran ini, tak mungkin dilaksanakan sepenuhnya.

Pencegahan dapat mereduksi sejumlah serangan virus. Setelah pencegahan terhadap masuknya virus, maka pendekatan berikutnya yang dapat dilakukan adalah :

o Deteksi.

Begitu infeksi telah terjadi, tentukan apakah infeksi memang telah terjadi dan cari lokasi virus.

o Identifikasi.

Begitu virus terdeteksi maka identifikasi virus yang menginfeksi program.

o Penghilangan.
Begitu virus dapat diidentifikasi maka hilangkan semua jejak virus dari program yang terinfeksi dan program dikembalikan ke semua (sebelum terinfeksi). Jika deteksi virus sukses dilakukan, tapi identifikasi atau penghilangan jejak tidak dapat dilakukan, maka alternatif yang dilakukan adalah menghapus program yang terinfeksi dan kopi kembali backup program yang masih bersih. Sebagaimana virus berkembang dari yang sederhana menjadi semakin canggih, begitu juga paket perangkat lunak antivirus. Saat ini program antivirus semakin kompleks dan canggih.

ACCESS CONTROL
Access control pada system operasi mengatur kemampuan akses user dalam suatu jaringan, computer atau aplikasi. Sistem access control pada jaringan data umumnya menggunakan firewall. Firewall akan bertindak sebagai pelindung atau pembatas terhadap orang-orang yang tidak berhak mengakses jaringan.

Kemampuan-kemampuan firewall :

- IP Hiding/Mapping

  Kemampuan ini mengakibatkan IP address dalam jaringan ditransalasikan ke suatu IP address yang baru. Dengan demikian, IP address dalam jaringan tidak akan dikenali di internet.
- Privilege Limitation

  Dengan kemampuan ini, kita juga bisa membatasi para user jaringan sesuai dengan otorisasi atau hak-hak yang diberikan kepadanya.
- Outside Limitation

  Kemampuan ini, dapat membatasi para user dalam jaringan untuk mengakses ke alamat-alamat tertentu di luar jangkauan kita.
- Inside Limitation

  Kita memperbolehkan orang luar untuk mengakses informasi yang tersedia dalam salah satu computer dalam jaringan kita. Selain itu, tidak diperbolehkan untuk mengakses seluruh computer yang terhubung ke jaringan kita
- Password dan Encrypted Authentication

  Beberapa user di luar jaringan memang diizinkan untuk masuk ke jaringan kita untuk mengakses data, dengan terlebih dahulu harus memasukkan password khusus yang sudah terenkripsi.

Ada 3 macam pembagian firewall berdasarkan cara kerjanya:

1. Internet firewalls

Merupakan system atau grup system yang memberikan kebijakan keamanan pada hubungan antara jaringan korporasi dan internet. Firewall mengatur layanan-layanan apa yang bisa di akses dari luar system. Internet firewall dapat berupa perangkat fisik atau software yang menyaring header paket bergantung pada kebijakan keamanan.

2. Packet filtering firewalls

Merupakan tipe firewall yang melakukan control akses ke dalam maupun keluar jaringan. Packet filter firewalls dapat berupa router maupun switch yang dapat dikonfigurasi dengan access list. Izin maupun penolakan akses didasarkan pada protocol, port asal maupun port tujuan alamat IP asal maupun tujuan.

3. Application/proxy firewalls

Perangkat atau software ini menjamin bahwa resource yang terlindungi tidak bisa diakses oleh sembarang user. Pada saat ini ada beberapa aplikasi firewall yang dapat dipasang di PC diantaranya adalah : McAfee, Personal Firewall, Symantec Norton Personal Firewall 2000, Network ICE Blackice Defender, dll.

Firewall yang tergantung OS

Sistem Operasi	Firewall
SUN-OS/Solaris	Solstice-1, Check Point
Windows NT	Altavista, Borderware
Novell	Intranetware
HP-UX	Borderware, Check Point
Unixware	CyberGuard
IBM AIX	Check Point

Firewall yang bebas

Blackbox Firewall	Vendor
Sunscreen	Sun Microsystem
Instant Internet	Bay Networks
BigFire	NAS Technology
Cisco PIX	Cisco System
Gauntlet	TIS

BENTUK SERANGAN TERHADAP SISTEM OPERASI

Ancaman Sistem Operasi Windows pada saat ini berdasarkan daftar ancaman yang dikeluarkan oleh SANS Institute :

1. Internet Information Services (IIS)
2. Microsoft SQL Server (MSSQL)
3. Windows Authentication (termasuk LM Hashing)
4. Internet Explorer (IE)
5. Windows Remote Access Services (termasuk NetBIOS, Anonymous logon, remote registry, RPC DOM)
6. Microsoft Data Access Components (MDAC)
7. Windows Scripting Host (WSH)
8. Microsoft Outlook & Outlook Express
9. Windows Peer to Peer File Sharing (P2P)
10. Simple Network Management Protocol

Sedangkan ancaman yang terjadi pada Unix berdasarkan daftar ancaman yang dikeluarkan oleh SANS Institute :

1. BIND Domain Name System
2. Remote Procedure Calls (RPC)
3. Apache Web Server
4. General UNIX Authentication Acounts with No Passwords or Weak Passwords
5. Clear Text Services (termasuk FTP, r-service/trust relationship, Line Printer Daemon)
6. Sendmail
7. Simple Network Management Protocol (SNMP)
8. Secure Shell (SSH)
9. Misconfiguration of Enterprise Services NIS/NFS
10. Open Secure Sockets Layer (SSL)

Berdasarkan masalah ancaman pada system operasi ini, dikenal suatu istilah "vulnerabilitas". Vulnerabilitas secara universal adalah keadaan dimana :

- Memungkinkan penyerang mengeksekusi perintah sebagai user lainnya.
- Memungkinkan penyerang untuk mengakses data yang berbeda dengan batasan akses untuk data tersebut.
- Memungkinkan penyerang untuk memalsukan diri sebagai pihak lain
- Memungkinkan penyerang untuk melakukan denial of service.

Selain itu dikenal pula istilah “exposure “, yaitu suatu keadaan dimana :

- Memungkinkan penyerang melakukan aktivitas pengambilan informasi
- Memungkinkan penyerang menyembunyikan aktifitas
- Menyertakan suatu kemampuan yang berperilaku seolah-olah seperti yang diinginkan, tetapi bisa dilakukan compromise dengan mudah
- Merupakan titik masuk utama penyerang bisa melakukan usaha memperoleh akses ke system atau data
- Dianggap sebagai masalah yang berkaitan dengan kebijakan keamanan tertentu.

Contoh vulnerabilitas universal :

- phf (remote command axecution sebagai user “nobody”)
- rpc.ttdbserved (remote command execution sebagai root)
- File password yang writeable secara bebas (modifikasi data penting system.
- Password default (remote command execution atau akses lainnya)
- Permasalahan denial of service yang memungkinkan seorang penyerang untuk menyebabkan blue death screen
- Smurf (denial of service dengan flooding jaringan)

Contoh exposure :

- Menjalankan service semacam finger (berguna untuk mengambil informasi, tapi membuatnya seperti “mengiklankan” system bagi penyerang)
- Setting dan konfigurasi yang tidak tepat pada kebijakan audit Windows NT
- Menjalankan service yang biasa menjadi titik serangan (misal HTTP, FTP, atau SMTP)
- Pemakaian aplikasi atau service yang bisa diserang dengan sukses memakai metode brute force.

KEBIJAKAN KEAMANAN

Suatu system computer bisa dilihat sebagai sekumpulan sumberdaya yang tersedia untuk dipergunakan oleh user yang berhak. Terdapat sejumlah komponen keamanan yang perlu diperhatikan oleh administrator :

1. Availability: Sistem harus tersedia untuk dipergunakan saat user memerlukannya. Serupa dengan itu , data penting harus juga tersedia pada setiap saat.
2. Utility: Sistem dan data pada system harus berguna untuk suatu tujuan
3. Integrity: Sistem dan data harus lengkap dan terbaca
4. Authenticity: Sistem harus mampu memverifikasi identitas dari user, dan user harus bisa memverifikasi identitas system
5. Confidentially: Data pribadi hanya boleh diketahui oleh pemilik data, atau sejumlah pihak terpilih untuk berbagi data
6. Possession: Pemilik dari system harus mampu mengendalikannya. Kehilangan control pada suatu system ke tangan orang yang tidak berhak, akan berdampak pada keamanan system bagi pengguna lainnya.