

PERTEMUAN 16: KEAMANAN JARINGAN KOMPUTER

A. TUJUAN PEMBELAJARAN

Pada bab ini akan dijelaskan mengenai keamanan sistem operasi jaringan,
Anda harus mampu:

- 1.1 Keamanann jaringan komputer
- 1.2 Tujuan keamanan jaringan
- 1.3 Karakteristik pengganggu

B. URAIAN MATERI

| |
|--------------------------|
| Tujuan Pembelajaran 1.1: |
|--------------------------|

| |
|-------------------------|
| Sistem Operasi Jaringan |
|-------------------------|

Keamanan Jaringan Komputer

Keamanan Komputer seperti yang dikatakan oleh John D. Howard, seorang Analisis Of Security Incidents On The Internet pada tahun 1989-1995, mengatakan bahwa :

“ Computer Security is preventing attackers form achieving objectives through unathorized access or unauthorized use of computers & Networks ” . Yaitu proses

pencegahan yang dilakukan oleh penyerang untuk terhubung ke dalam jaringan komputer melalui akses yang tidak sah, atau penggunaan secara ilegal dari komputer dan jaringan.

Tujuan Keamanan Jaringan Komputer

- Availability / Ketersediaan,
- Reliability / Keandalan, dan
- Confidentiality / Kerahasiaan.

Karakteristik pengganggu yang sering dijumpai pada sistem komputer, antara lain :

1. Lingkungan atau alam
2. Faktor Fisika
3. Kimia
4. Perangkat Keras
5. Perangkat Lunak
6. Sistem Operasi
7. Manajemen
8. Organisasi
9. Telekomunikasi

Salah Satu Pengamanan dari Faktor Lingkungan atau Alam Yaitu :

✓ Sistem Operasi

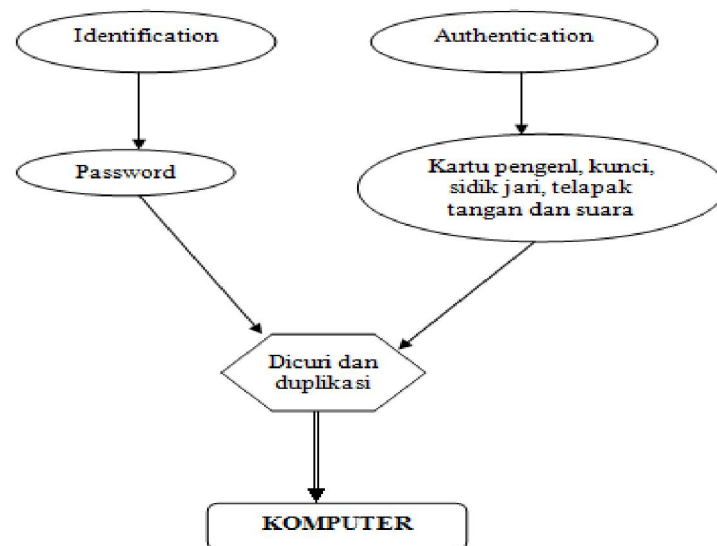
Penggunaan Sistem operasi dimaksudkan untuk memudahkan interaksi antara manusia dengan komputer, dan pada sistem operasi yang berbasis jaringan berfungsi untuk memudahkan hubungan antarkomputer yang satu dengan yang lain. Dalam penggunaan sistem operasi, Kita akan dicek oleh sistem operasi tersebut atau yang dikenal dengan Identification dan Authentication. Keduanya berfungsi untuk memberitahukan kepada sistem tentang siapa kita. Identification atau dikenal dengan pembuatan password pada umumnya digunakan untuk memastikan sistem operasi apakah kita yang berwenang atau tidak. Authentication pada umumnya menggunakan media pengenalan, seperti kunci, tanda pengenalan, sidik jari, telapak tangan, suara dan lain – lain. Kerusakan komputer yang diakibatkan oleh sistem operasi, banyak disebabkan faktor manusianya antara lain :

- Memberikan password kepada orang lain.
- Orang lain memberikan kepada orang lain lagi (Pihak Ketiga)
- Password ditulis pada media dan dibaca oleh orang lain.
- Terlalu mudah ditebak password-nya.
- Dicurunya kunci dan tanda pengenalan atau kunci dan tanda pengenalan tersebut dipinjam orang dan dibuat duplikat.

- Dibuatnya suatu alat yang membuat duplikat dari sidik jari, telapak tangan, dan suara.

Bila Kejadian tersebut terjadi, komputer dapat dibuka atau dijalankan oleh orang yang telah membuat duplikatnya, sehingga keamanan komputer sudah tidak terjamin lagi.

Untuk lebih jelasnya, lihat gambar berikut ini :



Beberapa Ancaman dan Serangan

Tujuan utama dengan adanya keamanan adalah untuk membatasi akses informasi dan sumber hanya untuk pemakai yang memiliki hak akses.

Ancaman keamanan :

- Leakage (Kebocoran) : Pengambilan informasi oleh penerima yang tidak berhak
- Tampering : Pengubahan informasi yang tidak legal
- Vandalism (perusakan) : Gangguan operasi sistem tertentu. Si pelaku tidak mengharap keuntungan apapun.
- Serangan pada sistem terdistribusi tergantung pada pengaksesan ke saluran komunikasi yang ada atau membuat saluran baru yang menyamarkan (masquerade) sebagai koneksi legal

- Penyerangan Pasive, Hanya mengamati komunikasi atau data
- Penyerangan Aktif, Secara aktif memodifikasi komunikasi atau data
- Pemalsuan atau pengubahan Email
- TCP/IP Spoofing

Faktor- Faktor Penyebab Resiko Dalam Jaringan Komputer :

- Kelemahan manusia (human error)
- Kelemahan perangkat keras komputer
- Kelemahan sistem operasi jaringan
- Kelemahan sistem jaringan komunikasi

Ancaman Jaringan Komputer :

√ FISIK

- Pencurian perangkat keras komputer atau perangkat jaringan
- Kerusakan pada komputer dan perangkat komunikasi jaringan
- Wiretapping
- Bencana alam

√ LOGIK

Kerusakan pada sistem operasi atau aplikasi

Virus

Sniffing

Beberapa Metode Penyerangan

- Eavesdropping, mendapatkan duplikasi pesan tanpa ijin
- Masquerading, Mengirim atau menerima pesan menggunakan identitas lain tanpa ijin mereka
- Message tampering, Mencegat atau menangkap pesan dan mengubah isinya sebelum dilanjutkan ke penerima sebenarnya. “man-in-the-middle attack” adalah bentuk message tampering dengan mencegat pesan pertama pada pertukaran kunci enkripsi pada pembentukan suatu saluran yang aman.

Penyerang menyisipkan kunci lain yang memungkinkan dia untuk mendekrip pesan berikutnya sebelum dienkrip oleh penerima

- Replaying, menyimpan pesan yang ditangkap untuk pemakaian berikutnya.
- Denial of Service, membanjiri saluran atau sumber lain dengan pesan yang bertujuan untuk menggagalkan pengaksesan pemakai lain

Beberapa Bentuk Ancaman Jaringan :

Ø Sniffer

Peralatan yang dapat memonitor proses yang sedang berlangsung

Ø Spoofing

Penggunaan komputer untuk meniru (dengan cara menimpa identitas atau alamat IP)

Ø Phreaking

Perilaku menjadikan sistem pengamanan telepon melemah

Ø Remote Attack

Segala bentuk serangan terhadap suatu mesin dimana penyerangnya tidak memiliki kendali terhadap mesin tersebut karena dilakukan dari jarak jauh di luar sistem jaringan atau media transmisi.

Ø Hole

Kondisi dari software atau hardware yang bisa diakses oleh pemakai yang tidak memiliki otoritas atau meningkatnya tingkat pengaksesan tanpa melalui proses otorisasi

Ø Hacker

Orang yang secara diam-diam mempelajari sistem yang biasanya sukar dimengerti untuk kemudian mengelolanya dan men-share hasil ujicoba yang dilakukannya. Hacker tidak merusak sistem

Ø Craker

Orang yang secara diam-diam mempelajari sistem dengan maksud jahat Muncul karena sifat dasar manusia yang selalu ingin membangun (salah satunya merusak)

Manajemen Resiko :


- Pengumpulan Informasi
- Analisis
- Output

Pengumpulan Informasi


- Identifikasi Assets
 - Perangkat Keras
 - Perangkat Lunak (Sistem Operasi dan Aplikasi)
 - Perangkat Jaringan dan Komunikasi Data
 - Pengguna Jaringan
 - Lingkungan
 - Sarana Pendukung lainnya
- Pencurian
- Kerusakan Fisik
- Wiretapping
- Bencana Alam

Penilaian terhadap segala bentuk Ancaman (threat) :

– FISIK

- | | | |
|-----------------------------|---|-------------------|
| • Hardware |  | • Pencurian |
| | | • Kerusakan Fisik |
| | | • Wiretapping |
| | | • Bencana Alam |
| • Perangkat Jaringan | | |
| • Perangkat komunikasi data | | |

– LOGIK

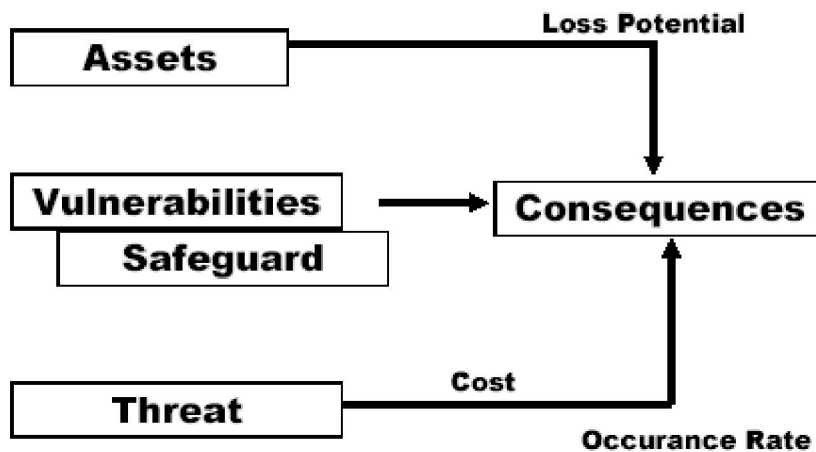
- | | | |
|------------------|---|-------------------|
| • Aplikasi |  | • Kerusakan Logik |
| • Sistem Operasi | | • Virus |
| | | • Sniffing |

- Denial of Service
- Data dan Informasi

Pengumpulan Informasi

- Penilaian terhadap bagian yang berpotensi terkena gangguan (vulnerability)
- Penilaian terhadap perlindungan yang efektif (safeguard)
 - keamanan fasilitas fisik jaringan
 - keamanan perangkat lunak
 - keamanan pengguna jaringan
 - keamanan komunikasi data
 - keamanan lingkungan jaringan

Analisis



Output

- Menjalankan safeguard / risk analysis tools

Pengamanan Komputer dari Faktor sistem Operasi

Pengganggu komputer dari faktor sistem operasi banyak terjadi karena faktor manusia, yaitu Identification dan Authentication. Untuk mengamankan keduanya, Kita dapat mengikuti cara berikut ini :

1. Identification

Password dapat diibaratkan seperti sikat gigi yang digunakan setiap hari. Oleh Karena itu, harus mengganti password tersebut secara periode dan

jangan digunakan oleh orang lain. Password menjadi tanggung jawab setiap orang (Pemilik), sehingga kita dapat mengikuti cara – cara di bawah ini agar password lebih terjamin.

- Jangan biarkan login tanpa password, Jika kita bekerja dengan jaringan dan kita adalah seorang administrator sistem, pastikan setiap account mempunyai password
- Jangan pernah membiarkan seseorang menggunakan password kita, Jika kita sudah terlanjur memberitahukan kepada orang lain, segeralah mengganti password dengan yang baru.
- Janganlah menulis password pada layar monitor, meja, atau sekitar ruang kerja.
- Jangan mengetik password, sementara di belakang atau sekeliling komputer kita ada orang lain yang mengawasi.
- Jangan mengirimkan password secara online ke suatu tempat melalui e-mail, karena ada kemungkinan orang lain akan menyadap saluran e-mail anda.

Apabila anda diperbolehkan memilih password, pilihlah password yang sukar ditebak. Dibawah ini saran – saran untuk menentukan nama password, yaitu :

- Jangan menggunakan kata – kata dalam bahasa Inggris.
- Jangan menggunakan nama – nama, seperti nama sendiri atau keluarga, pahlawan fiktif, anggota keluarga, hewan piaraan dan lain – lain.
- Boleh juga menggunakan kata – kata yang tidak mempunyai arti, misalnya Jt93gpy
- Sebaiknya gunakan gabungan huruf dan angka.
- Jangan menggunakan nomor telepon anda.
- Pilih Password yang panjang, karena jika password anda hanya beberapa huruf atau angka atau kombinasi keduanya, akan mudah ditemukan. Gunakan minimal 6 – 8 karakter.
- Apabila anda bekerja dengan jaringan, sebaiknya bedakan password antara host (Komputer) yang satu dengan yang lain.

- Password yang baik adalah yang menggunakan kombinasi huruf besar dan kecil.

2. Authentication

- Proses pengenalan peralatan, sistem operasi, kegiatan, aplikasi dan identitas user yang terhubung dengan jaringan komputer
- Autentikasi dimulai pada saat user login ke jaringan dengan cara memasukkan password
- Jangan pernah meninggalkan kartu pengenalan atau kunci di tempat terbuka, walaupun hanya sebentar.
- Tempatkan kartu pengenalan atau kunci pada tempat yang sulit dijangkau oleh orang lain, atau letakkan pada tempat yang dapat anda kunci dari luar.
- Pada beberapa negara maju pengamanan komputer telah menggunakan sensor untuk mengamankan komputer. Oleh karena itu, jangan pernah merekam sidik jari atau telapak tangan atau suara pada komputer anda karena akan mudah bagi orang lain untuk membuat duplikatnya.

Bila anda seorang administrator sistem, sebaiknya anda membagi file – file tersebut menjadi beberapa tingkatan, yaitu :

- Siapa yang boleh membaca file anda.
- Siapa yang boleh mengubah file anda.
- Data anda di share (mendapat bagian yang sama) dengan user yang lain.

Dalam pengaturan akses terhadap file – file terdapat 2 tipe, yaitu :

1. Discretionary Access Control (DAC)

Pembatasan akses terhadap file, directory dan device berdasarkan user atau group. Pengaturan akses ini dilakukan oleh pemiliknya. Pembahasan dengan tipe ini dibagi menjadi 3 bagian yang mendasar, yaitu Read, Write, dan Execute.

Pembatasan akses kontrol dengan tipe Discretionary Access Control mempunyai beberapa jenis, yaitu :

a. Ownership

- Pembuatan file dilakukan oleh pemilik.
- Login atau beberapa pengenalan disimpan dalam file.
- Apabila anda pemilik file tersebut, anda dapat membaca dan mengubah isi file.
- Jika anda bukan pemilik file tersebut, anda tidak dapat mengakses file-nya.

b. File Types and File Protection Classes

- Metode ini lebih baik dibandingkan metode Ownership.
- Sebuah file dapat didefinisikan sebagai public, semipublic atau private file. Untuk mendefinisikan, anda dapat menggunakan beberapa kode, yaitu :

- o Blank

Digunakan untuk mendefinisikan Public, yaitu semua user dapat membaca atau menulis ke dalam file yang bersangkutan.

- o @

Digunakan untuk mendefinisikan Execute Only, yaitu hanya pemilik file, Administrator System dan semua user saja dapat menjalankan file dan mengubah isi file.

- o S

Digunakan untuk mendefinisikan Read Only, yaitu semua user dapat membaca dan menjalankan file, namun hanya pemilik file dan Administrator System yang dapat mengubah file.

- o #

Digunakan untuk mendefinisikan Private, yaitu hanya pemilik file dan Administrator System yang dapat membaca, mengubah dan menjalankan file.

- o A – Z

Digunakan untuk mendefinisikan System Dependent, yaitu Administrator System dapat mensetting sistem sehingga user yang mempunyai kelas tertentu yang dapat mengakses file tertentu pula, Misalnya kelas A dapat mengakses program Akuntansi, Kelas P dapat mengakses program Payroll dan lain – lain

c. Self/Group/Public Controls

- Pengaturannya menggunakan 3 kategori, yaitu :
 - Self, digunakan oleh anda sendiri sebagai pembuat atau pemilik file.
 - Group, digunakan oleh sekelompok user.
 - Public, digunakan yang tidak termasuk self dan group.
- Cara seperti ini digunakan pada sistem operasi UNIX, yang dikenal dengan nama UGO (User / Group / Other).
- Setiap file mempunyai sekumpulan bit – bit yang disebut dengan file permissions.

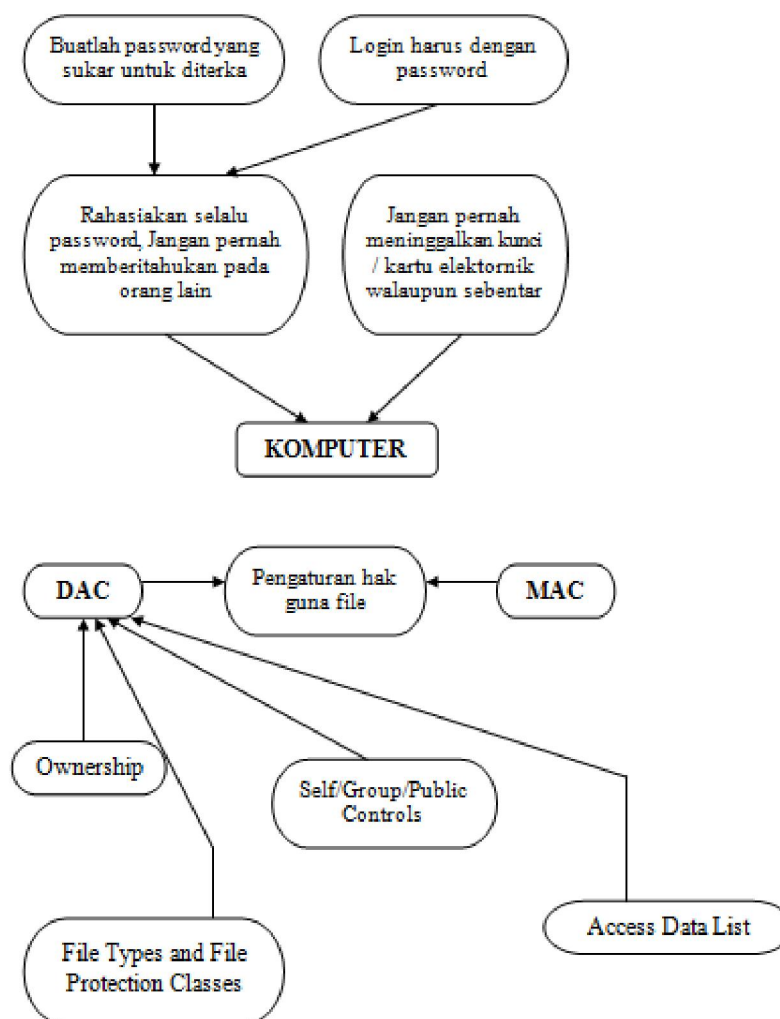
d. Access Data List

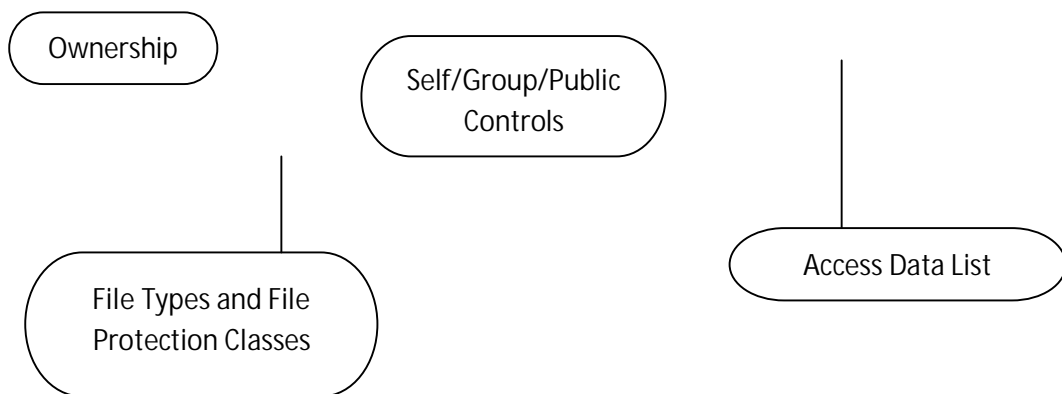
- Pembatasan file dengan cara membuat daftar user – user dan group – group dengan haknya masing – masing.
- Cara ini lebih fleksibel dibandingkan dengan cara – cara sebelumnya.

2. Mandatory Access Control (MAC)

Pembatasan akses yang ditentukan oleh sistem. Pengaturan akses dengan menggunakan Mandatory Access Control lebih kompleks dibandingkan dengan menggunakan Discretionary Access Control. Pada umumnya, penggunaan dengan tipe ini dilakukan untuk memproses data yang bersifat sensitif, misalnya informasi pemerintah atau swasta, informasi badan intelejen, dan lain – lain.

Untuk lebih jelasnya, lihat gambar berikut ini :

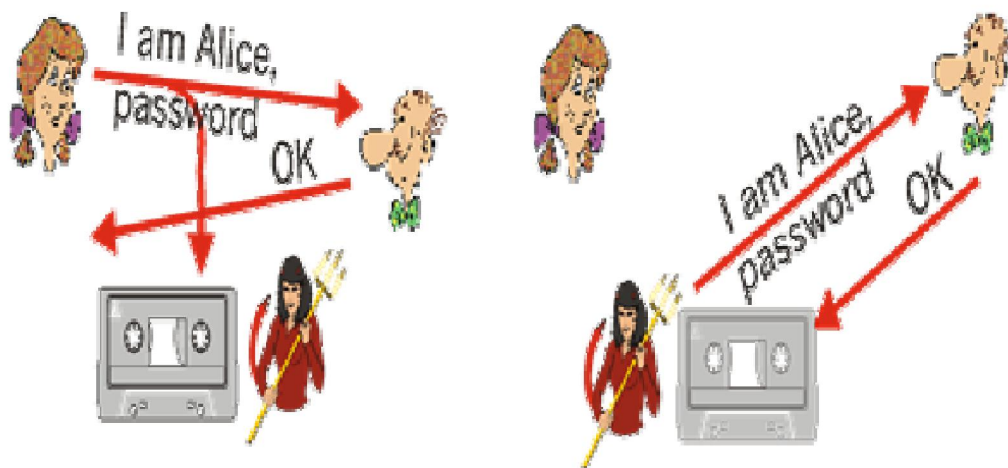




Tahapan Autentikasi :

1. Autentikasi untuk mengetahui lokasi dari peralatan pada suatu simpul jaringan (data link layer dan network layer)
2. Autentikasi untuk mengenal sistem operasi yang terhubung ke jaringan (transport layer)
3. Autentikasi untuk mengetahui fungsi/proses yang sedang terjadi di suatu simpul jaringan (session dan presentation layer)

Resiko yang Muncul Pada Tahapan Autentikasi



Kebijakan dan Mekanisme Keamanan

Pemisahan antara kebijakan dan mekanisme keamanan akan membantu memisahkan kebutuhan implementasinya :

- Kebijakan menspesifikasikan kebutuhan
- Mekanisme menerapkan spesifikasi kebijakan tersebut

Berdasar spesifikasi dari OSI, sebuah layanan (kebijakan) keamanan meliputi :

- Access Control, Perlindungan terhadap pemakaian tak legak
- Authentication, Menyediakan jaminan identitas seseorang
- Confidentiality (kerahasiaan), Perlindungan terhadap pengungkapan identitas tak legak
- Integrity, Melindungi dari pengubahan data yang tak legak
- Non-repudiation (penyangkalan), Melindungi terhadap penolakan komunikasi yang sudah pernah dilakukan

Untuk mencapai layanan keamanan tersebut, mekanisme-mekanisme yang dapat diterapkan :

Ø Enkripsi

§ proses pengkodean pesan untuk menyembunyikan isi

§ Digunakan untuk menyediakan kerahasiaan, dapat menyediakan authentication dan perlindungan integritas

§ Algoritma enkripsi modern menggunakan kunci (key).

- Pesan M (plaintext) di encodekan dengan fungsi E dan sebuah kunci K untuk menjadi ciphertext.

$$E(K,M) = \{M\}_K$$

- Pesan didekripsi dengan menggunakan fungsi D dan kunci L

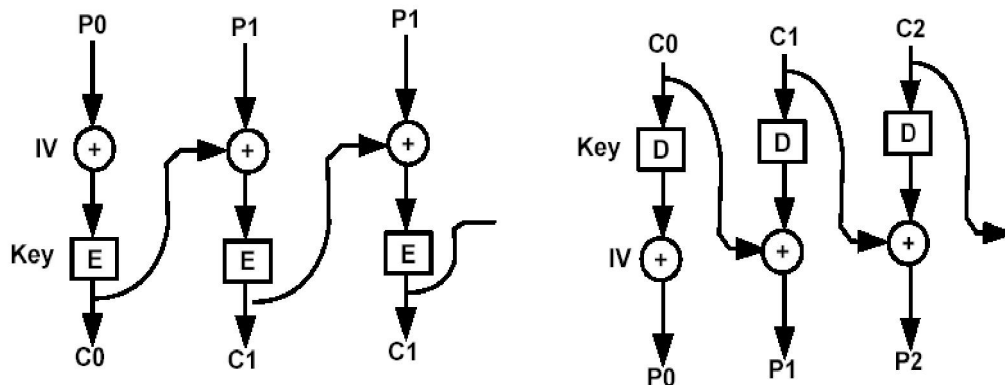
$$D(K,E(K,M)) = M$$

Ø Kunci kriptografi adalah parameter yang digunakan dalam algoritma enkripsi dimana hasil enkripsi tidak dapat didekripsi jika tanpa kunci yang sesuai

Berikut beberapa mode Cipher :

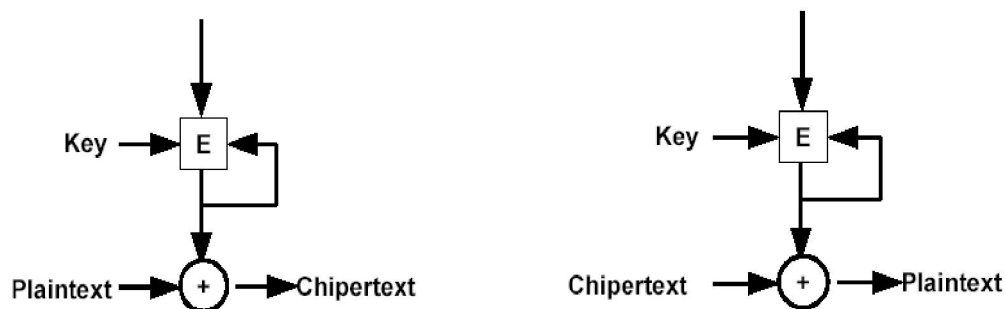
✓ Cipher Block Chaining

- Untuk ukuran block data yang tetap, yang populer adalah 64 bit
- Pesan dibagi ke dalam block, dan block terakhir di padding ke ukuran standard yang digunakan, dan setiap block dienkrip secara independent
- Block pertama tersedia untuk transmisi setelah enkripsi selesai



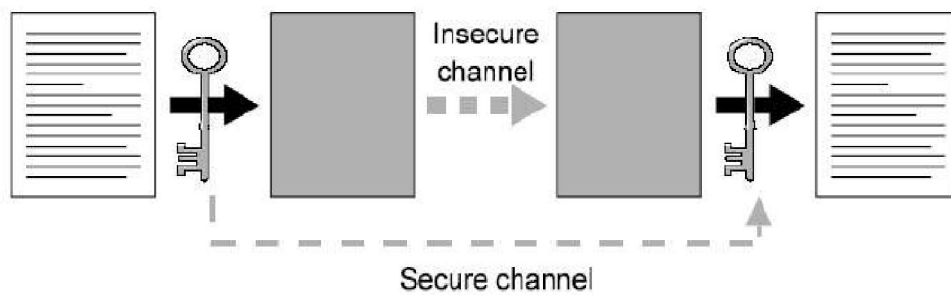
✓ Stream Cipher

- menghasilkan keystream dari setiap enkripsi kunci dengan initialization vector (IV)



Ada dua tipe algoritma enkripsi :

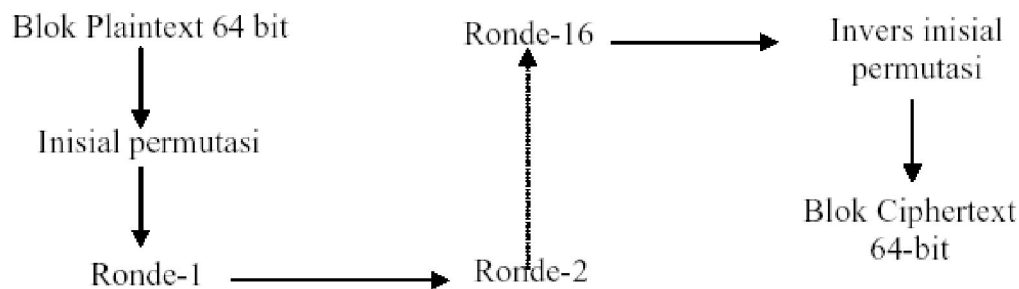
- Symmetric (secret-key)
 - Pengirim dan penerima harus berbagi kunci dan tidak diberikan kepada orang lain.
 - One-way function.



- Contoh : DES (Data Encryption Standard), Triple DES

Proses Kerja DES

Cara kerja DES secara sederhana dapat digambarkan sebagai berikut :



- AES (Advanced Encryption Standard) yang disponsori oleh NIST (National Institute of Standards and Technology) menetapkan beberapa algoritma enkripsi AES :
 - § Rijndael (Joan Daemen dan Vincent Rijmen)
 - § Serpent (Ross Anderson, Eli Biham, Lars Knudsen)
 - § Twofish (dari Bruce Schneier)
 - § RC6 (dari RSA Laboratories)
 - § MARS (dari IBM)
- Algoritma AES harus memenuhi :
 - § symmetric block chiper
 - § panjang kunci 128, 192 dan 256
 - § dimungkinkan implementasi pada software maupun hardware
 - § Algoritma harus umum atau berlisensi tanpa persyaratan yang diskriminatif

Berikut contoh program untuk melakukan enkripsi dan dekripsi DES :

```
import java.security.*;
import javax.crypto.*;

public class EnDeDES {
    public static void main(String[] args) {
        Cipher ecipher;
        Cipher dcipher;
        String teks = args[0];
        try {
            //menghasilkan kunci temporary
            SecretKey key =
                KeyGenerator.getInstance("DES").generateKey();
            ecipher = Cipher.getInstance("DES");
            ecipher.init(Cipher.ENCRYPT_MODE, key);
            dcipher = Cipher.getInstance("DES");
            dcipher.init(Cipher.DECRYPT_MODE, key);
            // Enkripsi dimulai
            byte[] enc = ecipher.doFinal(teks.getBytes());
            String teksEnc =
                new sun.misc.BASE64Encoder().encode(enc);
            System.out.println("Hasil enkripsi DES '" +
                teks + "' adalah " + teksEnc);
            // Dekripsi dimulai
            byte[] dec = dcipher.doFinal(enc);
            System.out.println("Hasil dekripsi DES '" +
                teksEnc + "' adalah " + new String(dec));
        } catch (Exception e) {
        }
    }
}
```

Hasil eksekusi adalah sebagai berikut :

```
$ java EnDeDES "Ini percobaan saja dari Budsus"
```

Hasil enkripsi DES 'Ini percobaan saja dari Budsus'

adalah y4OhBZX/T923EdH07f1x9kf65l6jE38Q0dq9fabwucE=

Hasil dekripsi DES

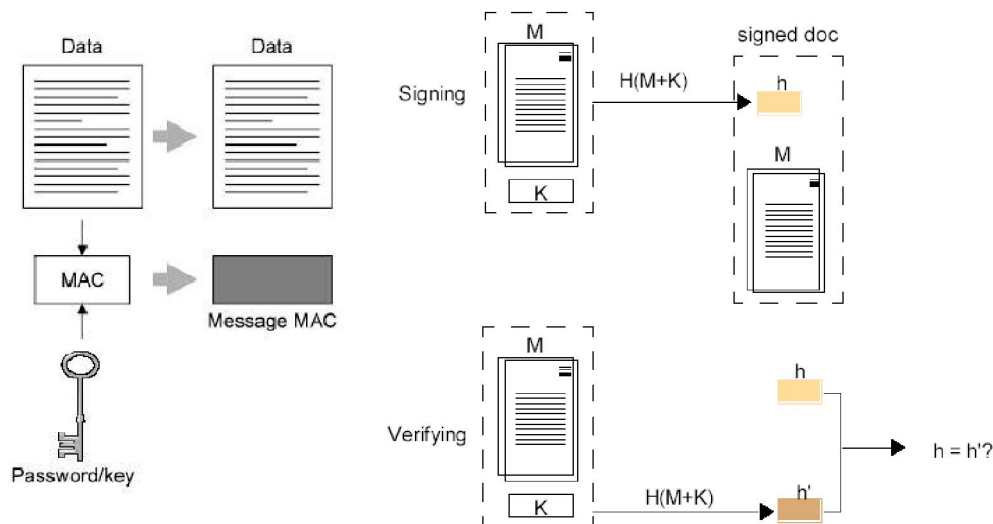
'y4OhBZX/T923EdH07f1x9kf65l6jE38Q0dq9fabwucE=' adalah

Ini percobaan saja dari Budsus

- Asymmetric (public-key)
 - Pengirim pesan menggunakan public key (kunci yang dipublikasikan ke penerima) untuk mengenkrip pesan
 - Penerima menggunakan private key yang cocok (miliknya) untuk mendekrip pesan.
 - Pola public key dimunculkan pertama oleh Diffie Hellman (1976)
 - Dasar public key : trap-door function adalah one-way function yang dapat dibalikkan dengan hanya adanya secret key
 - contoh : RSA

MAC (Message Authentication Code)

- Menghasilkan random password/key untuk suatu hash
- Hanya pemegang password yang dapat menghasilkan MAC



Beberapa fungsi Digest :

§ MD5 (Message Digest 5) oleh Rivest (1991)

- Dapat ditemukan di RFCs 1319-1321
- Panjang digest : 128 bit

§ SHA (Secure Hash Algorithm)

- Panjang digest : 160 bit
- Didasarkan pada algoritma MD4

Perangkat Lunak

Tidak semua perangkat lunak dibuat untuk kebaikan, ada pula yang dibuat untuk merusak software yang lain yang telah ada, misalnya virus komputer. Virus yang ada hingga kini lebih dari 15.000 jenis dan jenis yang lain terus bermunculan seiring dengan perkembangan software yang ada. Pembuatan virus komputer memang disengaja untuk memodifikasi program orang lain, sehingga program tersebut menjadi kacau dan tidak dapat digunakan kembali. Ada pula yang membuat virus komputer untuk popularitas dan komersial, misalnya dengan adanya virus komputer tersebut, banyak perusahaan baru yang membuat pembasmi virus atau disebut antivirus.

C. SOAL LATIHAN/TUGAS

1. Apa yang dimaksud dengan Sistem operasi jaringan ?
2. Sebutkan jenis-jenis sistem operasi jaringan berbasis Windows, linux dan Unix ?
3. Apa yang dimaksud dengan sistem operasi router ?
4. Sebutkan beberapa fitur yang terdapat pada sistem operasi router ?

D. DAFTAR PUSTAKA

Buku

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

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

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

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

Setiawan Agung. 2005, Pengantar Sistem Komputer Edisi Revisi, Bandung: Informatika

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

Link and Sites:

Unswagati. 2010. Keamanan Jaringan Komputer.

http://unswagati-crb.ac.id/component/option,com_phocadownload/Itemid,73/download,55/id,11/view,category/ . Tanggal akses 10 November 2012.

<http://www.ilmukomputer.com>

<http://vlsm.bebas.org>

<http://www.wikipedia.com>