Keamanan
Jaringan Komputer

Tujuan Keamanan Jaringan Komputer

- Availability / Ketersediaan
- Reliability / Kehandalan
- Confidentiality / Kerahasiaan

- Cara Pengamanan Jaringan Komputer :
  - Autentikasi
  - Enkripsi

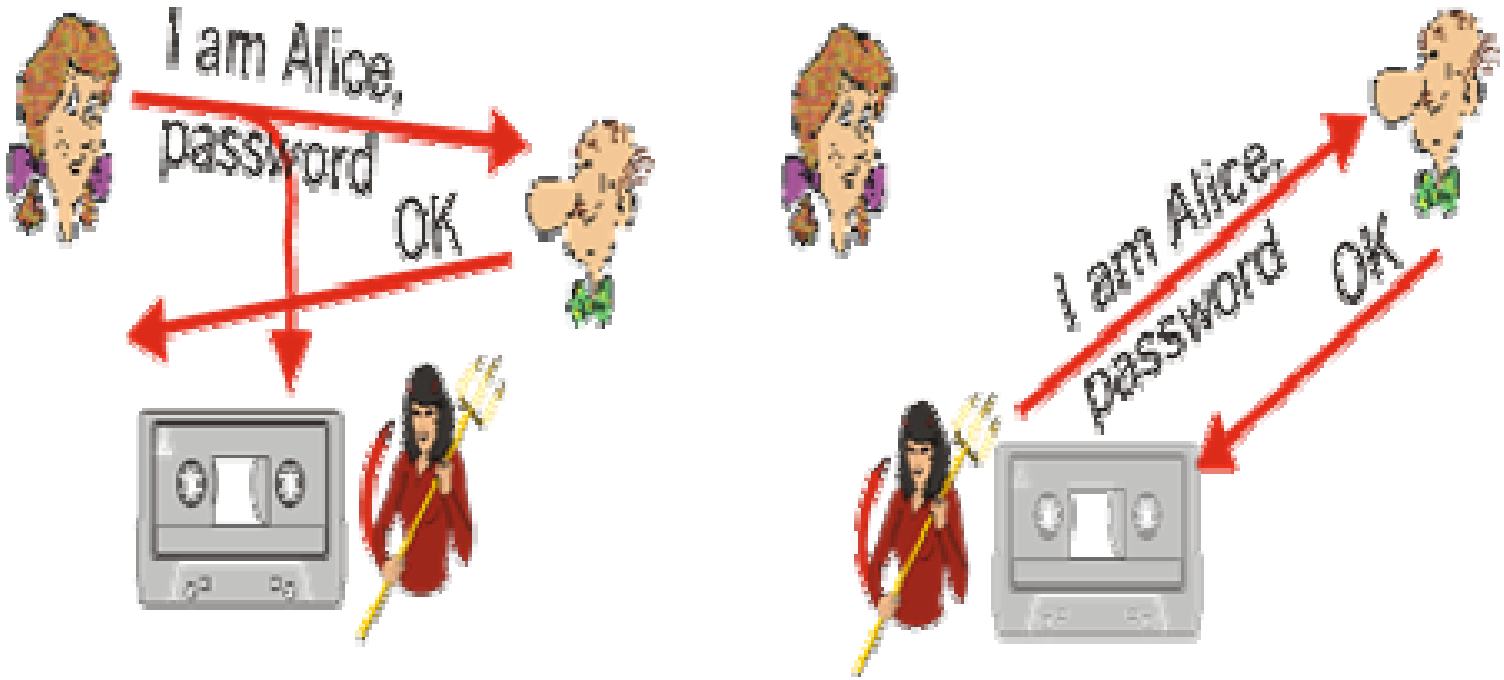
Autentikasi

- 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

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)
4. Autentikasi untuk mengenali user dan aplikasi yang digunakan (application layer)

Resiko yang Muncul Pada Tahapan Autentikasi

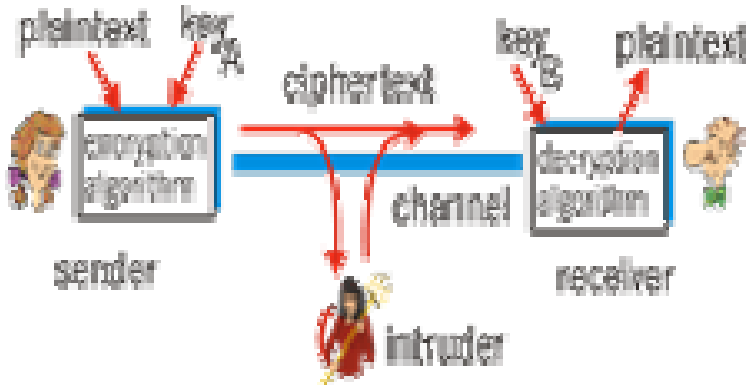


Enkripsi

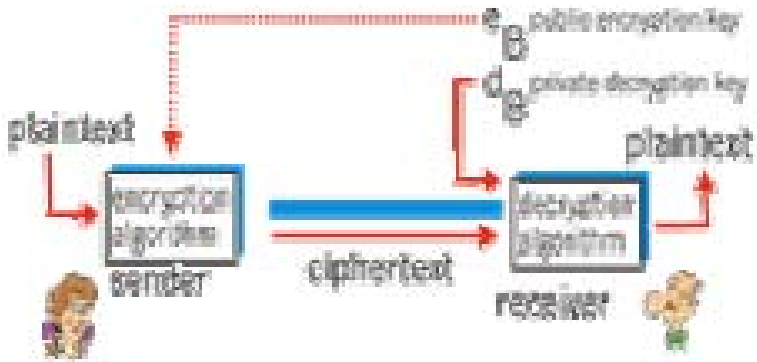
- Teknik pengkodean data yang berguna untuk menjaga data / file baik di dalam komputer maupun pada jalur komunikasi dari pemakai yang tidak dikehendaki
- Enkripsi diperlukan untuk menjaga kerahasiaan data

Teknik Enkripsi

- DES (Data Encription Standard)



- RSA (Rivest Shamir Adelman)



Resiko Jaringan Komputer

Segala bentuk ancaman baik fisik maupun logik yang langsung atau tidak langsung mengganggu kegiatan yang sedang berlangsung dalam jaringan

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 Bentuk Ancaman Jaringan

- **Sniffer**

  Peralatan yang dapat memonitor proses yang sedang berlangsung
- **Spoofing**

  Penggunaan komputer untuk meniru (dengan cara menimpa identitas atau alamat IP.
- **Remote Attack**

  Segala bentuk serangan terhadap suatu mesin dimana penyerangnya tidak memiliki kendali terhadap mesin tersebut karena dilakukan dari jarak jaruh di luar sistem jaringan atau media transmisi
- **Hole**

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

Beberapa Bentuk Ancaman Jaringan

- **Phreaking**
  Perilaku menjadikan sistem pengamanan telepon melemah
- **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
- **Craker**
  – Orang yang secara diam-diam mempelajari sistem dengan maksud jahat
  – Muncul karena sifat dasar manusia yang selalu ingin membangun (salah satunya merusak)

Beberapa Bentuk Ancaman Jaringan

- **Cracker**
  - Ciri-ciri cracker :
    - Bisa membuat program C, C++ atau pearl
    - Memiliki pengetahuan TCP/IP
    - Menggunakan internet lebih dari 50 jam per-bulan
    - Menguasai sistem operasi UNIX atau VMS
    - Suka mengoleksi software atau hardware lama
    - Terhubung ke internet untuk menjalankan aksinya
    - Melakukan aksinya pada malam hari, dengan alasan waktu yang memungkinkan, jalur komunikasi tidak padat, tidak mudah diketahui orang lain

Beberapa Bentuk Ancaman Jaringan

Craker

– Penyebab cracker melakukan penyerangan :
  - spite, kecewa, balas dendam
  - sport, petualangan
  - profit, mencari keuntungan dari imbalan orang lain
  - stupidity, mencari perhatian
  - cruriosity, mencari perhatian
  - politics, alasan politis

Beberapa Bentuk Ancaman Jaringan

Cracker

– Ciri-ciri target yang dibobol cracker :
  - Sulit ditentukan
  - Biasanya organisasi besar dan financial dengan sistem pengamanan yang canggih
  - Bila yang dibobol jaringan kecil biasanya sistem pengamanannya lemah, dan pemiliknya baru dalam bidang internet

– Ciri-ciri target yang “berhasil” dibobol cracker :
  - Pengguna bisa mengakses, bisa masuk ke jaringan tanpa “nama” dan “password”
  - Pengganggu bisa mengakses, merusak, mengubah atau sejenisnya terhadap data
  - Pengganggu bisa mengambil alih kendali sistem
  - Sistem hang, gagal bekerja, reboot atau sistem berada dalam kondisi tidak dapat dioperasikan

Manajemen Resiko

- Pengumpulan Informasi
- Analisis
- Output

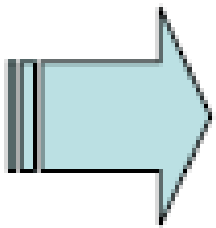
Pengumpulan Informasi

- Identifikasi Assets
  - Perangakat Keras
  - Perangkat Lunak (Sistem Operasi dan Aplikasi)
  - Perangkat Jaringan dan Komunikasi Data
  - Pengguna Jaringan
  - Lingkungan
  - Sarana Pendukung lainnya

Pengumpulan Informasi

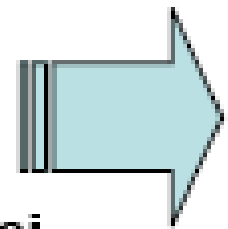
- Penilaian terhadap segala bentuk Ancaman (threat)

– **FISIK**
  - **Hardware**
  - **Perangkat Jaringan**
  - **Perangkat komunikasi data**



- **Pencurian**
- **Kerusakan Fisik**
- **Wiretapping**
- **Bencana Alam**

– **LOGIK**
  - **Aplikasi**
  - **Sistem Operasi**
  - **Data dan Informasi**



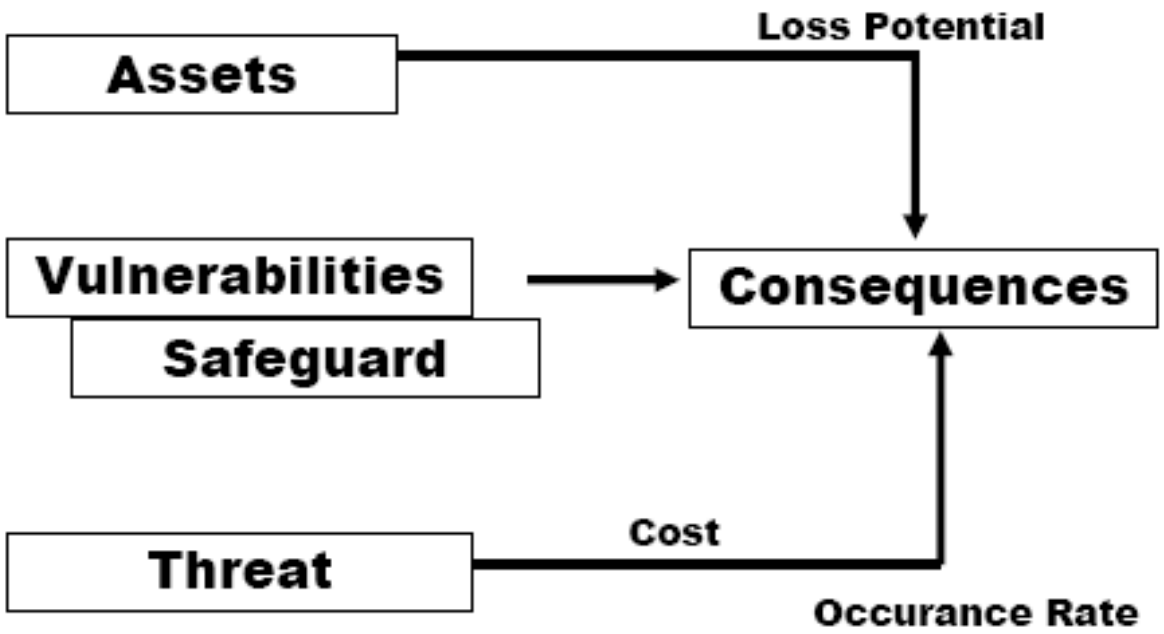
- **Kerusakan Logik**
- **Virus**
- **Sniffing**
- **Denial of Service**

Pengumpulan Informasi

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

Analisis & Output

Analisis



Output

Menjalankan safeguard / risk analysis tools