PENDAHULUAN

--Dr. Mike Yuliana--

Mata Kuliah : Keamanan Jaringan

Politeknik Elektronika Negeri Surabaya (PENS)

Outline

- Latar belakang
- Prinsip dasar keamanan informasi
- Security attack
- Pemodelan Network Security

Latar Belakang

- Perkembangan Internet yang semakin maju →informasi semakin mudah didapatkan
- Kita semakin mudah membagikan informasi tentang diri kita
- Adanya berbagai kemudahan tersebut memicu timbulnya bahaya → malware, pencurian data
- Bagaimana menangani ancaman tersebut?
  - *Information Security* atau keamanan informasi adalah tentang memahami dan mengontrol ancaman terhadap asset yang kita miliki dan lindungi

Prinsip Dasar Keamanan Informasi

Sumber : opentext.com

Confidentiality

- Artinya kerahasiaan atau hanya pihak yang berhak dan berwenang saja yang dapat mengakses informasi tersebut
- Klasifikasi informasi/data untuk mencapai confidentiality :
  - *Internal use only* → digunakan di internal perusahaan
  - *Public* → disebarkan melalui website atau media sosial
  - *Confidential* → sangat rahasia
- Ancaman yang muncul :
  - *Password strength*
  - *Malware*
  - *Social engineering*
- Cara yang dapat digunakan untuk menjamin tercapainya aspek confidentiality adalah enkripsi pada level media penyimpanan dan transmisi data

Integrity

- Artinya data tidak dirubah dari aslinya oleh orang yang tidak berhak, sehingga konsistensi, akurasi, dan validitas data tersebut masih terjaga.
- Integrity dapat dicapai dengan :
  - *strong encryption* pada media penyimpanan dan transmisi data.
  - *strong authentication* dan *validation* pada setiap akses file/akun login/action yang diterapkan.
  - *access control* yang ketat ke sistem, yaitu setiap akun yang ada harus dibatasi hak aksesnya.

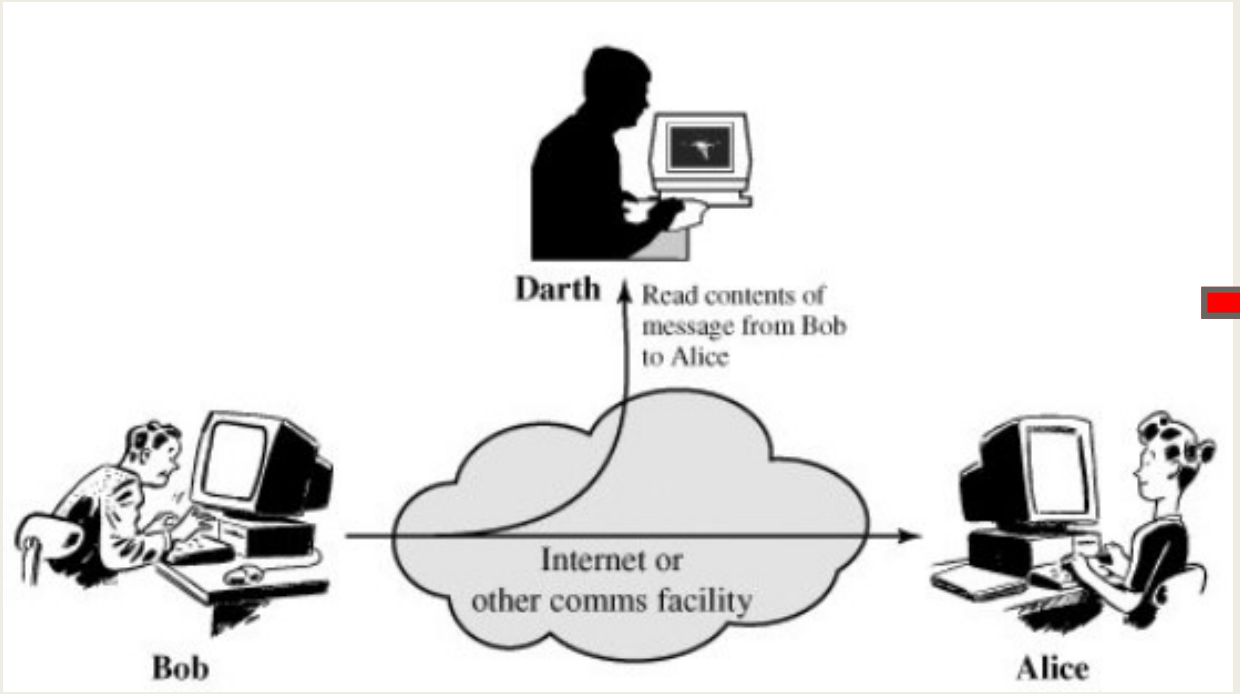
Availability

- Artinya memastikan sumber daya yang ada siap diakses kapanpun oleh user/application/sistem yang membutuhkannya.
- Availability dapat dicapai dengan :
  - *disaster recovery plan* (memiliki cadangan baik tempat dan *resource*, apabila terjadi bencana pada sistem).
  - *redundant hardware* (misal memiliki banyak *power supply*)
  - RAID (salah satu cara untuk menanggulangi *disk failure*)
  - *data backup* (rutin melakukan backup data)

Security Attack

- Adalah setiap tindakan yang membahayakan keamanan informasi yang dimiliki oleh user atau organisasi
- Berdasarkan keterlibatan penyerang dalam komunikasi, terdapat 2 jenis attack yaitu :
  - *Passive attack*
    - Penyerang tidak terlibat dalam komunikasi antara pengirim dan penerima
    - Penyerang hanya melakukan penyadapan untuk memperoleh data atau informasi sebanyak banyaknya
  - *Active attack*
    - Penyerang mengintervensi komunikasi dan ikut mempengaruhi sistem untuk keuntungan dirinya
    - Penyerang mengubah aliran pesan

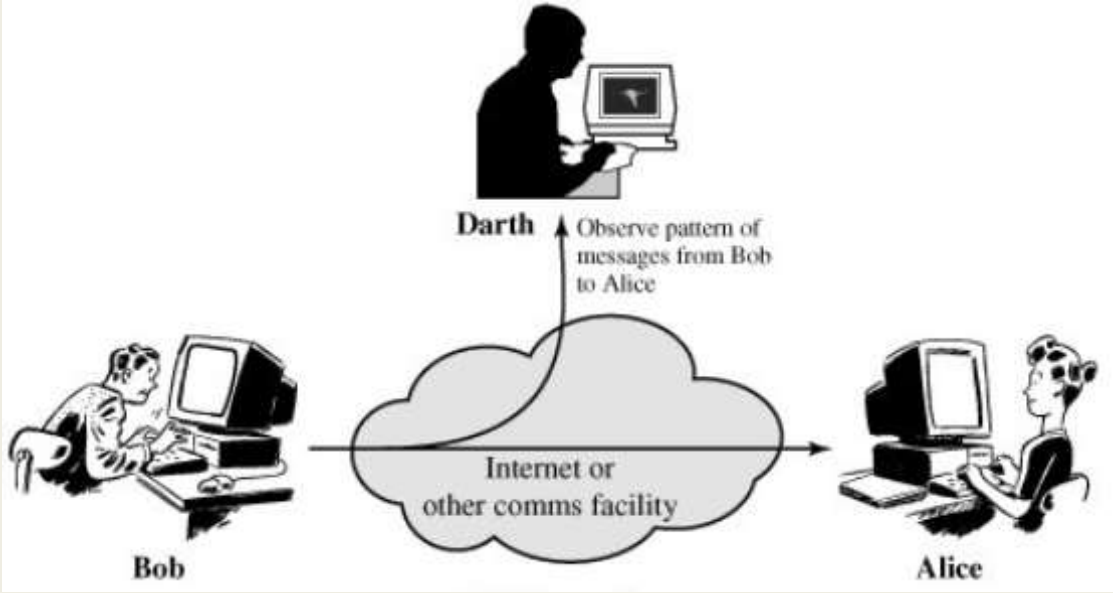
Passive Attack (1)



Release of message content

- Mendapatkan informasi yang dikirim antara kedua pengguna yang sah
- Tidak melakukan perubahan
- Sulit dideteksi

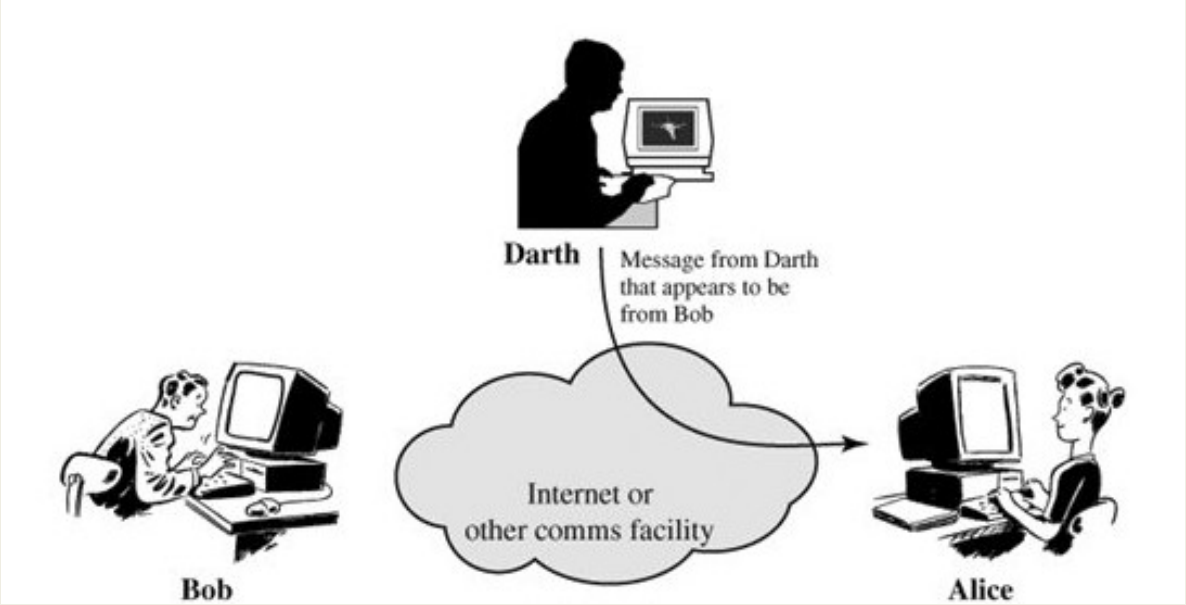
Passive Attack (2)



Traffic analysis

- Mengamati pola pola pesan yang dikirim

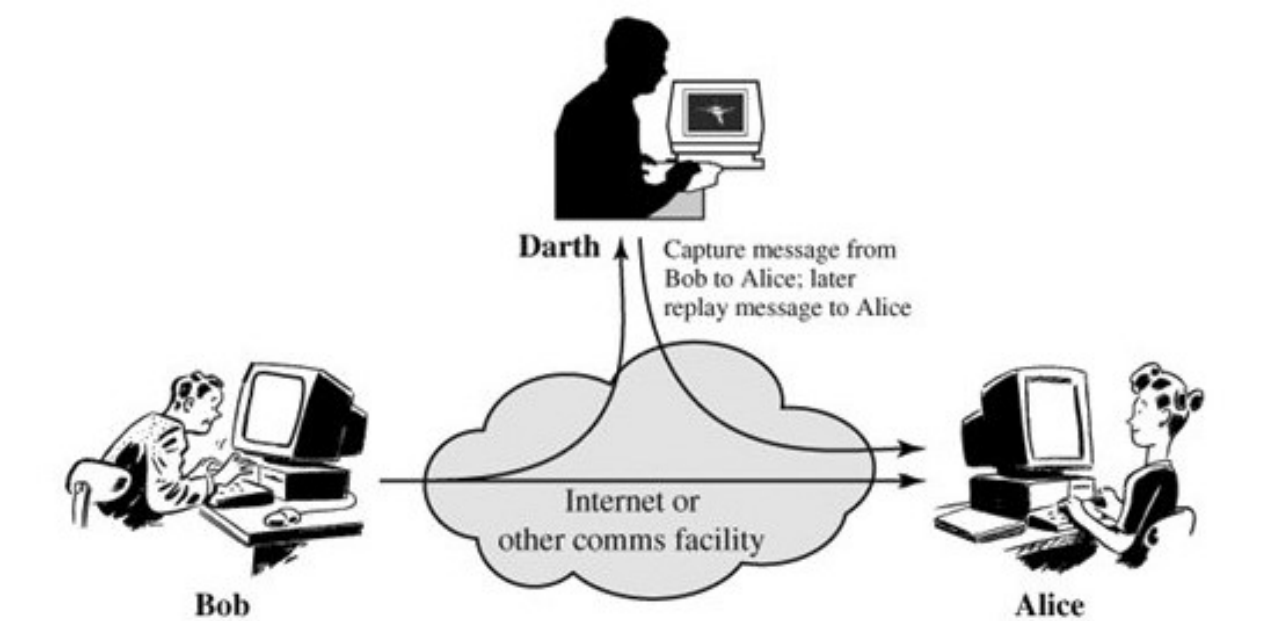
Active Attack (1)



masquerade

- Satu entitas berpura-pura menjadi entitas yang berbeda

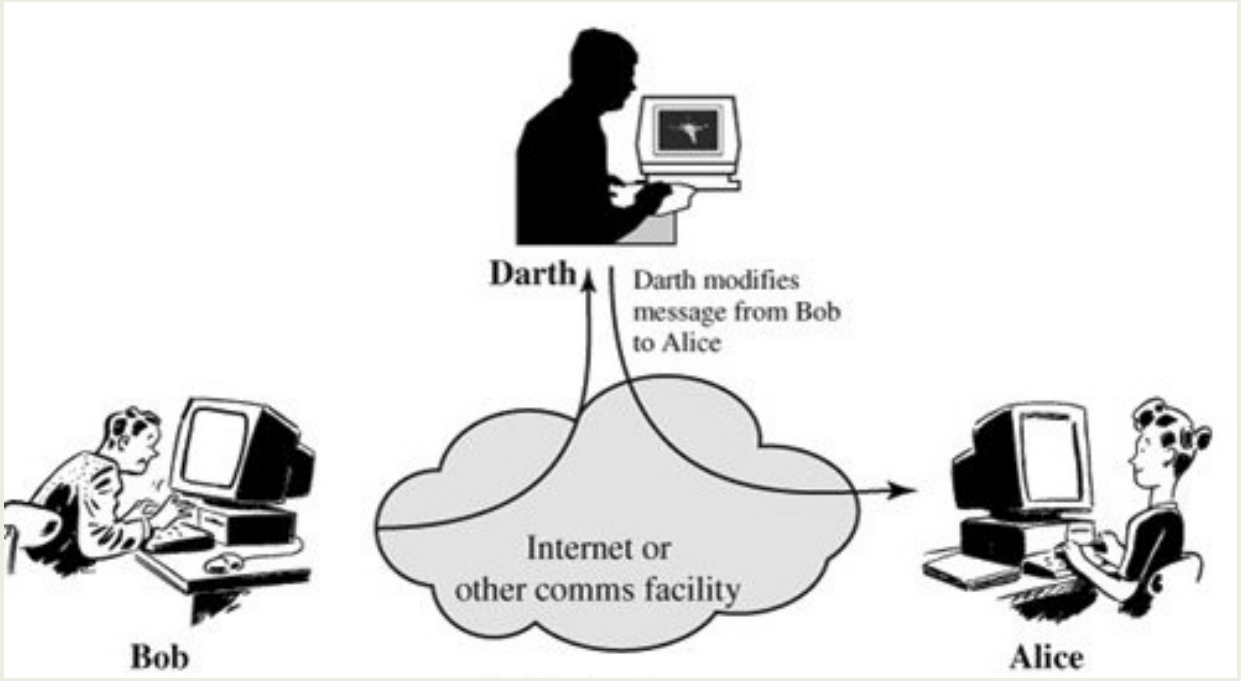
Active Attack (2)



replay

- Mengulang pesan sebelumnya

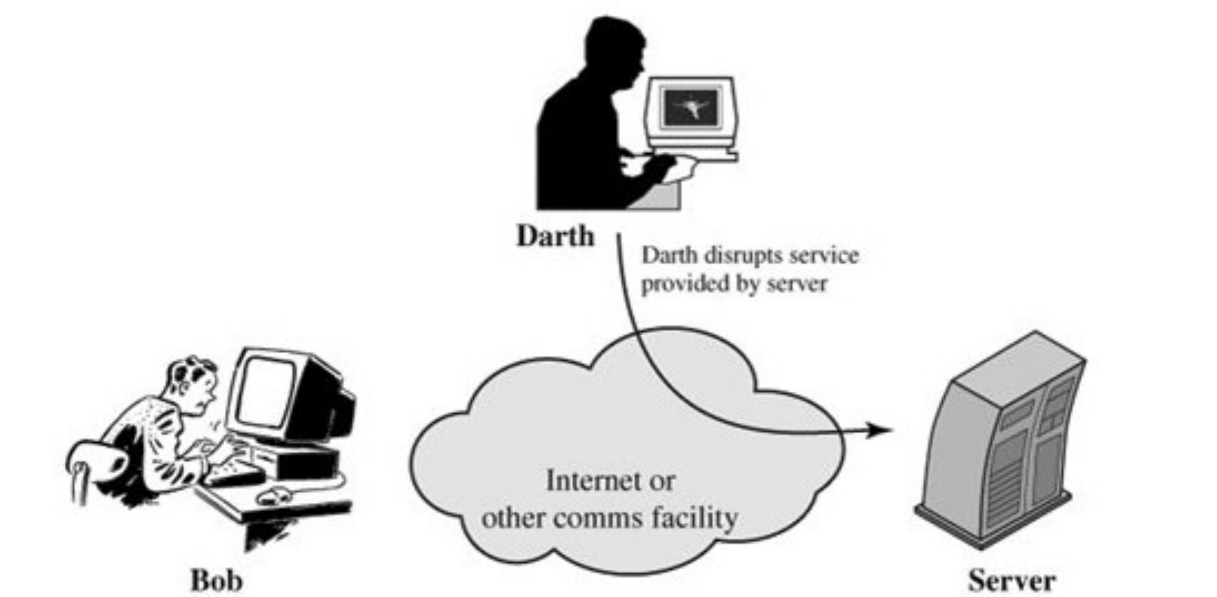
Active Attack (3)



Modifikasi pesan

- Pengubahan beberapa bagian pesan sah

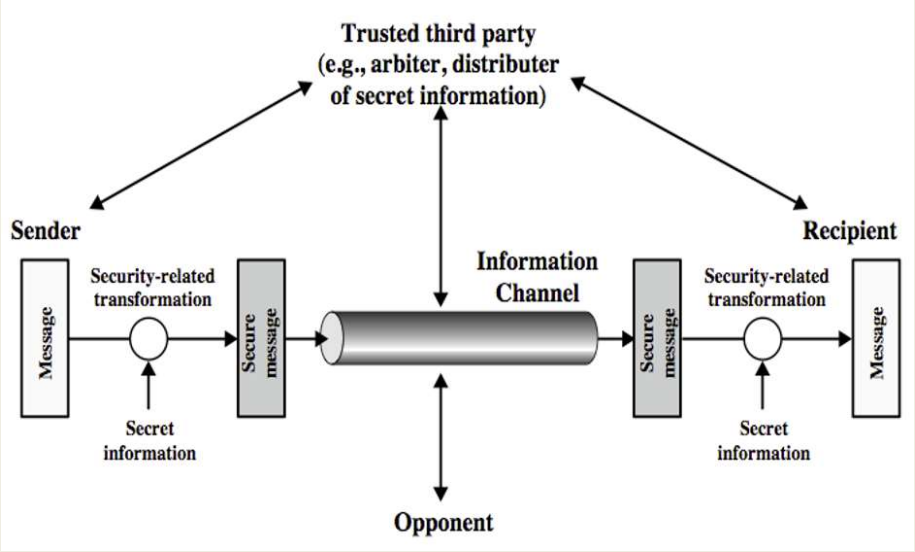
Active Attack (4)



Denial of service

- Mencegah atau menghambat penggunaan secara normal atau pengelolaan fasilitas komunikasi
- Bisa dilakukan dengan flooding packet

Pemodelan Network Security



Langkah-langkah untuk mendesain layanan keamanan :

- Mendesain algoritma yang cocok untuk security
- Membuat secret information yang akan digunakan dalam algoritma tersebut
- Menentukan metode untuk mendistribusikan dan sharing secret information
- Menentukan protokol yang bisa digunakan oleh sender dan receiver sehingga bisa mencapai layanan keamanan tertentu