

# TIS13534P KOMUNIKASI DAN KEAMANAN DATA

Minggu 1 - Pengantar

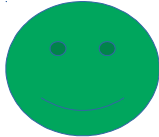

# About Me

- > Nama : Alauddin Maulana Hirzan, S. Kom, M. CS
- > Kota Asal : Semarang
- > Pendidikan Terakhir : S2 (Teknologi Antar Jaringan)
- > Alamat : Jalan Bukit Sambiroto Asri Raya no 271  
RT 10 RW 08 Kelurahan Sambiroto Kecamatan  
Tembalang, Semarang.

## Kontak:

- No. HP (WA) : 085-855-429-229
- E-Mail : [maulanahirzan@yandex.com](mailto:maulanahirzan@yandex.com)

# Perkuliahahan

- Mahasiswa diizinkan terlambat 15 menit
- Makan Permen/Minum Air Botol 
- Makanan Ringan 
- Tugas bisa dikirimkan melalui e-mail

# Persentase Nilai

<b>Jenis</b>	<b>Persentase</b>
Presensi	10
Tugas	10
UTS	35
UAS	45

Semua File Materi Bisa Diakses Di:

- <https://is.gd/kdkd18>

# Outline

- Serangan, Layanan, Mekanisme
- Jenis Serangan Keamanan
  - Serangan Pasif
  - Serangan Aktif
- Layanan Keamanan
  - Kerahasiaan
  - Otentik
  - Integritas
  - Non repudiation
  - Kontrol Access
  - Ketersediaan
- Model Keamanan Jaringan

## **Serangan Keamanan**

Segala perbuatan yang membahayakan informasi yang dimiliki sebuah perusahaan

## **Mekanisme Keamanan**

Segala sesuatu yang dapat mencegah, melindungi, memperbaiki dari serangan.

## **Layanan keamanan**

Sebuah pelayanan yang menambah kuat sistem keamanan dari sebuah serangan

# Lubang Keamanan

- Bersifat Fisik (Hard)
  - Perangkat keras, Tempat Penyimpanan Data (HDD, Flash Drive, CD/DVD)
- Bersifat Non-Fisik (Soft)
  - Data Keamanan Pribadi, (Password, PIN ATM)



# Mungkinkah Aman?

- Tidak ada keamanan 100%, celah itu selalu ada.
- Di tahun 2016 FBI berhasil membobol iPhone tanpa bantuan Apple.
- Komputer yang terhubung dengan internet 24 jam memiliki kemungkinan disusupi Trojan/Worm

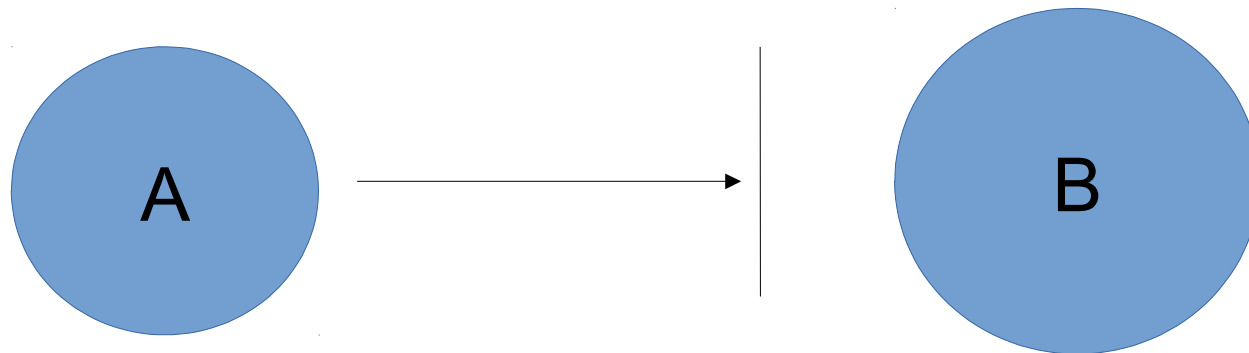
# Jenis-jenis Serangan

- Bagaimana Transmisi Data berjalan secara normal?
- Data mengalir dari A ke B tanpa ada gangguan.



# 1. Interupsi

- Transmisi Data dari A ke B dihentikan oleh orang ke 3

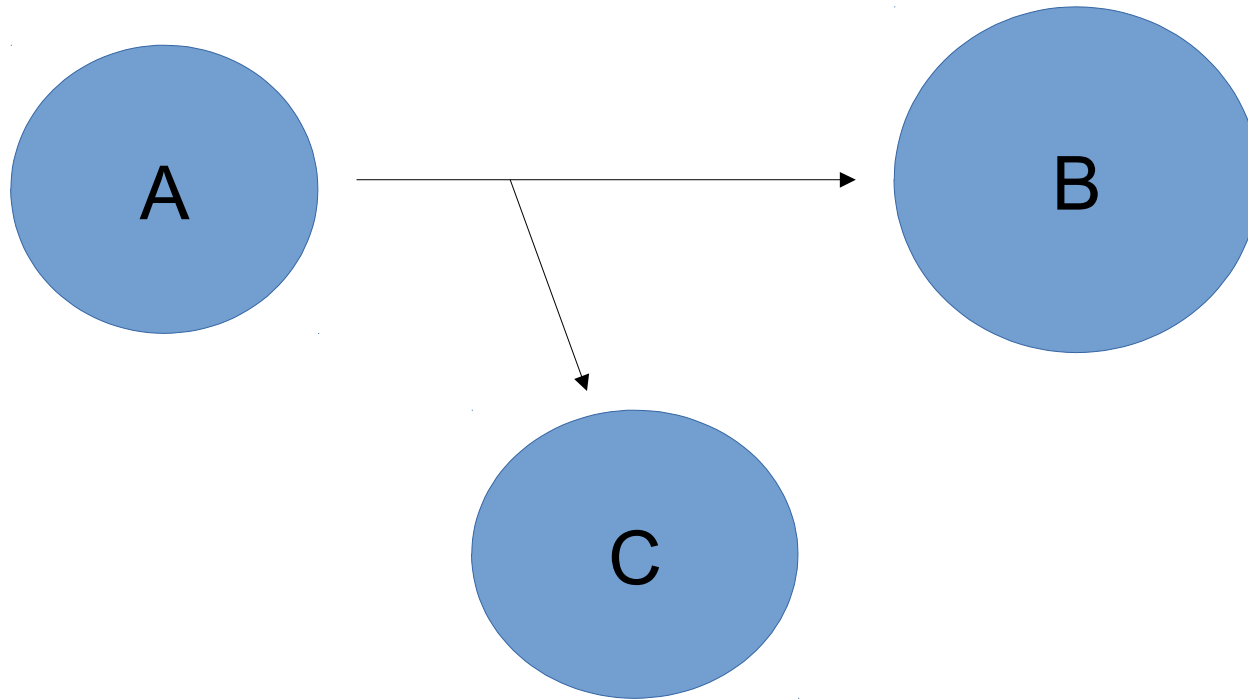


# Serangan Jenis Interupsi

- Denial-of-Service
  - Membanjiri jaringan lokal/internet dengan paket-paket tidak jelas/tidak berguna
  - Sehingga data dari A sulit akan sampai di B
- Ping of Death
  - Menggunakan alat/utiliti lokal untuk melakukan pengecekan waktu yang dibutuhkan untuk mengirim banyak data.
- TCP SYN
  - Membanjiri komputer lain dengan paket TCP yang kacau dan tidak jelas.

## 2. Interception

- Intersepsi menangkap pesan dari A, dan komputer B menerima pesan tersebut secara utuh.

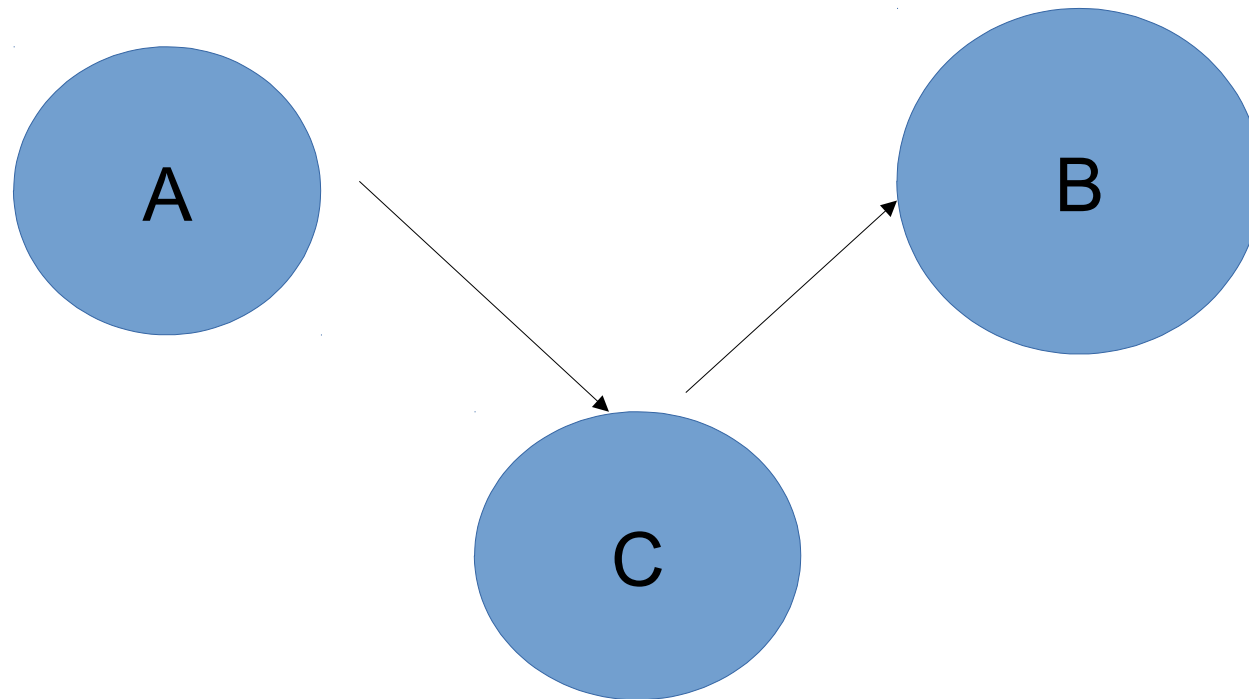


# Serangan Jenis Interception

- Semua software jenis sniffer mampu melakukan ini.
  - Wireshark, TCPDUMP, DSniff, Aircrack-ng, dll
- Serangan ini lebih sering terjadi di area WIFI.
- Karena WIFI menggunakan sistematisa broadcast packet sehingga orang lain yang terhubung bisa membaca paket yang mengalir.

### 3. Modifikasi

- Pesan dari A ditangkap dan dimodifikasi oleh pihak C, yang kemudian pengiriman dilanjutkan ke B



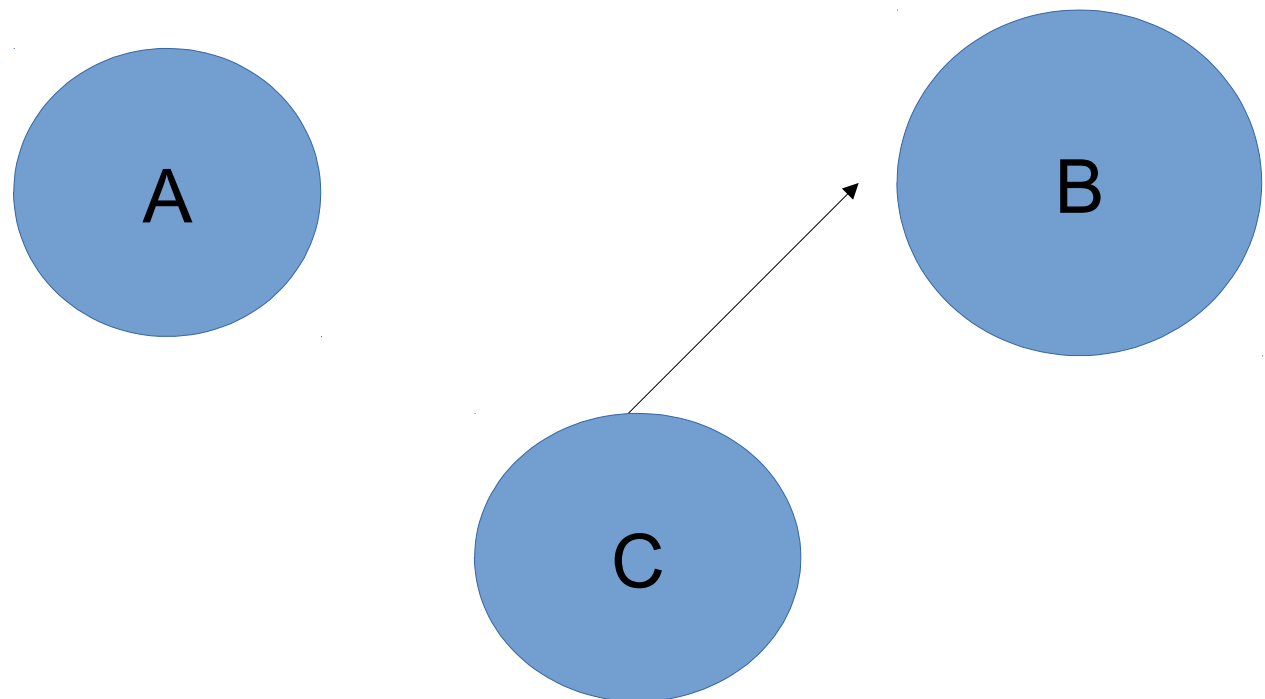
# Serangan Jenis Modifikasi

- SQL Injection, menyisipkan perintah SQL ketika sebuah aplikasi menjalankan statement SQL lain. Hal ini terjadi karena level keamanan web yang tidak sempurna.
- Modifikasi Informasi oleh Virus/Trojan/



## 4. Fabrikasi

- Pihak C memberikan informasi palsu ke pihak B. Mereka ini ingin mencuri informasi rahasia seperti e-mail dan password



# Serangan-Serangan

- Serangan Pasif
  - Serangan yang sifatnya tidak merusak sistem komputer, dan lebih ingin mendapatkan informasi
- Serangan Aktif
  - Serangan yang sifatnya merusak/memodifikasi sistem sehingga dapat membuat komputer berfungsi secara tidak baik

# Serangan Pasif

- Packet Sniffer, Traffic Analysis merupakan serangan pasif yang bertujuan mendapatkan informasi yang mengalir.
  - Contoh: Wireshark

# Serangan Aktif

- Masquerade: Penyerang berpura-pura menjadi user lain untuk mendapatkan informasi, menciptakan data palsu, atau mengambil alih
- Replay: Menangkap data dan memperoleh otorisasi
- Modifikasi: Mengubah pesan yang dikirimkan orang lain
- Denial-of-Service: Membuat server tidak mampu menjalankan layanannya secara baik.

# Layanan Keamanan

## 1. Kerahasiaan (Confidentiality)

Data harus dilindungi (diproteksi) dari serangan dari luar. Perlindungan ini juga harus memasukkan perlindungan dari analisa lalu lintas data.

Caranya? Enkripsi End-to-End jaringan dengan VPN. Teknologi SSL/HTTPS/SFTP.

# Layanan Keamanan #2

## 2. Otentik (Authentication)

Data yang diterima merupakan data yang datang dari sumber yang terpercaya.

- Jika ada data yang datang dari sumber yang tidak bisa dipercaya, ada kemungkinan hal itu merupakan serangan ***Fabrikasi*** atau ***Masquerade***.
- Jika tidak hati-hati, data keamanan bisa dicuri bahkan akses user bisa diambil alih.

# Layanan Keamanan #3

## 3. Integritas (Integrity)

- Data yang baik dikirimkan maupun diterima haruslah asli atau tidak ada perubahan sedikitpun disaat transmisi sedang berlangsung.
- Jika terjadi perubahan, ada kemungkinan bahwa data telah dimodifikasi oleh pihak ketiga, atau
- Terjadi kerusakan disaat transmissi dikarenakan oleh ***noise*** lingkungan.

# Layanan Keamanan #4

## 4. Non-Repudiation

User pengirim maupun penerima dipastikan tidak menolak/menyangkal bahwa dia telah mengirimkan/menerima data. Sehingga bisa diyakinkan bahwa data tersebut datang dari sumber yang bisa dipercaya.



# Layanan Akses #5

## 5. Kontrol Akses (Access Control)

Membatas gerak-gerik pengguna dalam menggunakan sistem atau aplikasi melalui media aplikasi.

Contoh: User yang terkoneksi melalui SSH bisa dibatasi untuk tidak menggunakan akun root (Administrator).

# Layanan Keamanan #6

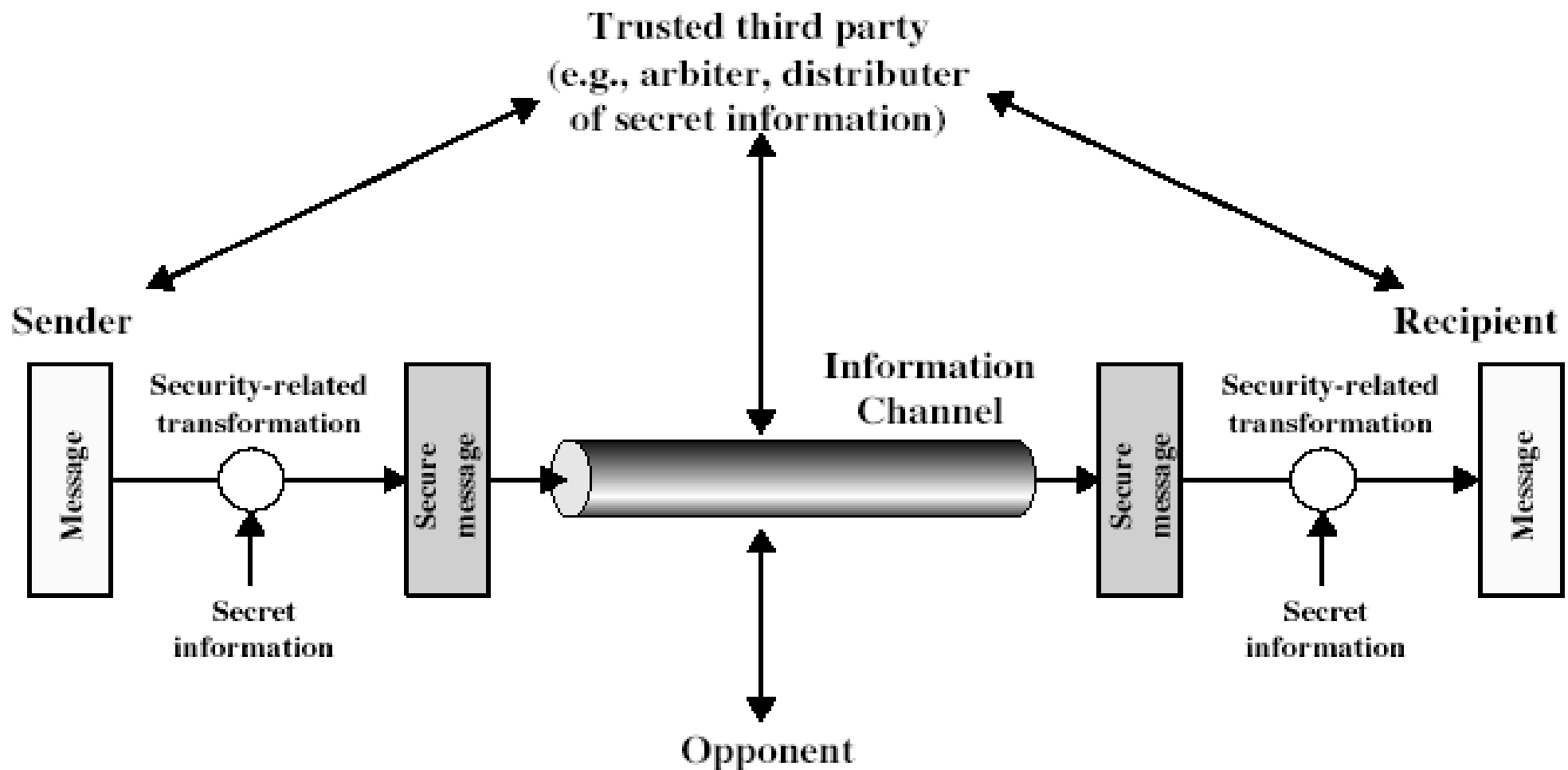
## 6. Ketersediaan (Availability)

Menjaga ketersediaan informasi bagi klien merupakan kewajiban yang harus dilakukan oleh server (biasanya web server).

Ada beberapa jenis serangan yang mengakibatkan server sulit diakses yang mengakibatkan mengurangi ketersediaan untuk klien

Contoh: Denial-of-Service

# Model Untuk Keamanan Jaringan



# Model #1

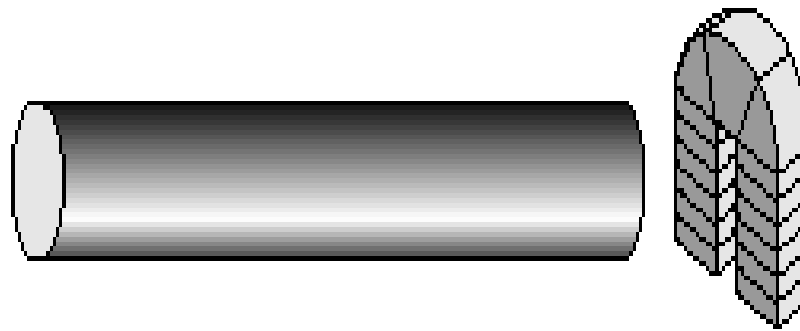
- Jika menggunakan model ini kita diharuskan:
  - Menyiapkan algoritma yang cocok untuk transformasi keamanan
  - Membuat kunci rahasia untuk algoritma
  - Mengembangkan metode untuk pendistribusian data rahasia
  - Mengkhususkan protokol yang digunakan untuk pengiriman data

# Model Keamanan Jaringan #2

Information System

## Opponent

- human (e.g., cracker)
- software  
(e.g., virus, worm)



Access Channel

Gatekeeper  
function

Computing resources  
(processor, memory, I/O)

Data

Processes

Software

Internal security controls

# Model #2

- Untuk model ini kita diharuskan:
  - Mencari penjaga gerbang (gatekeeper) yang sesuai untuk identifikasi user
  - Mengimplementasikan kontrol keamanan dengan hanya mengizinkan user yang memiliki akses di sumber atau informasi tertentu.
  -



To Be Continued....