Ir. Budi Rahardjo, M.Sc., Ph.D

Teknik Komputer – STEI ITB

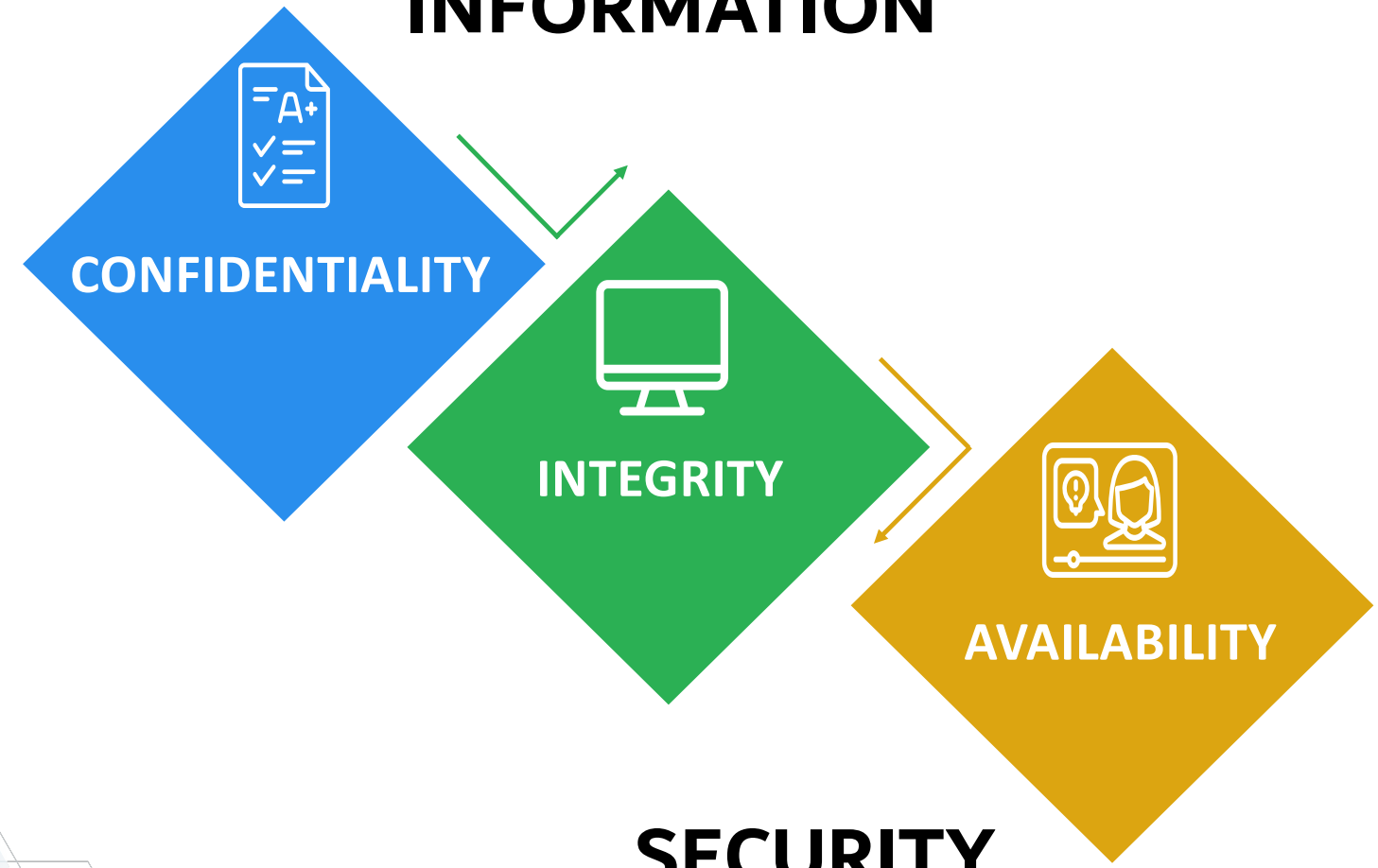
Prinsip Keamanan

II3230 - Keamanan Informasi

Aspek Keamanan | Security Goals | Security Services

(Section 3)

INFORMATION



SECURITY

Confidentiality (Kerahasiaan)

- Data (sistem) tidak boleh (tidak dapat) diakses oleh orang yang tidak berhak
- Perlu mendefinsikan data apa saja yang *confidential*
  - Data pelanggan
  - Data pribadi
  - Data kesehatan
- Bagaimana melakukan kategorisasi data?

Confidentiality

- Serangan
  - Kebocoran data
  - Penyadapan (sniffing)
  - Mengintip (shouldering)
  - Cracking (mencoba memecahkan enkripsi)
  - Social engineering (menipu, mencari-cari kelemahan SOP, membujuk orang untuk membuka data)

Confidentiality

- Perlindungan
  - Memisahkan (separation) jaringan / aplikasi / VLAN
  - Penerapan kriptografi (enkripsi, dekripsi)
  - Memagari (firewall)
  - SOP yang jelas (ketat?)
  - Pemantauan log

Privacy (Privasi)

- Dalam konteks *confidentiality*, kerahasiaan data, jika data yang dilindungi terkait dengan data pribadi disebut *privacy*
  - Data pribadi (*personal data*), termasuk data keluarga
  - Data pelanggan (*customer*)
  - Data kesehatan (*health data*)
  - Data warga
  - Password, PIN

Contoh Kasus

Data Penerima Bansos

- Data penerima bansos (bantuan sosial) ditampilkan secara utuh dalam rangka transparansi dan untuk umpan balik
  - Apakah ada penerima dana yang bukan orang miskin?
  - Apakah semua dana disampaikan (ataukah dikorupsi)?
- Data menampilkan identitas (nama, alamat, NIK) secara lengkap
- Data dapat diabuse oleh pihak lain
  - Untuk ”pembelian suara” dalam pemilihan umum (orang miskin dibeli suaranya)
  - Untuk diskriminasi

Mengapa Perlu Dilindungi

Data pribadi perlu dilindungi dikarenakan

- Aib
- Digunakan oleh pihak lain untuk keuntungan finansial (bisnis), diperjualbelikan, tanpa ijin dari pemilik data
- Menjadi bagian dari otentikasi (*authentication*)
  - Tanggal lahir menjadi bagian dari **password**
  - NIK dianggap sebagai **rahasia**; sesuatu yang hanya diketahui oleh yang bersangkutan, padahal sudah tidak lagi. Asumsi yang salah

Mengapa Perlu Dilindungi

- Data menjadi lepas dari kendali dari kita
  - Bagaimana jika terjadi kesalahan / ketidakakuratan data?
  - Apakah kita memiliki hak untuk memperbaiki data tersebut? Apakah kita dapat menutut pihak lain untuk menghapus data kita?
  - Bagaimana kita tahu pihak mana yang memiliki data kita dan data apa yang mereka miliki?
- Data digunakan tidak semestinya / di luar konteks
  - Tiba-tiba asuransi kesehatan naik
    - Diketahui memiliki penyakit tertentu atau terdapat pandemi di lingkungan sekitar tempat tinggal
  - Diskriminasi
    - Karena memiliki agama yang berbeda atau pilihan (partai politik) yang berbeda

Konteks Pemberian Data

- Data diberikan kepada penyedia jasa / layanan untuk keperluan tertentu
  - Identitas (untuk keperluan otentikasi)
  - Bagaimana jika data digunakan untuk keperluan lain (diperjualbelikan)?
  - Apabila perusahaan bangkrut, bagaimana status data?
- Data apa saja yang dianggap relevan?
  - Apa ukuran secukupnya? Berlebihan?
  - Contoh data Kartu Keluarga (KK) yang diminta oleh operator telekomunikasi termasuk data yang **berlebihan** karena di dalamnya terdapat individu lain yang tidak menggunakan jasa layanan dari penyedia layanan tersebut
- Apa saja yang termasuk bisnis dari penyedia jasa?
  - Apakah data dapat dianggap sebagai aset yang dapat diperjualbelikan?

Keamanan Data di Penyedia Jasa

- Keamanan merupakan **tanggungjawab** dari penyedia jasa
- Kebocoran data (ketidakamanan data) harus mendapatkan hukuman, sanksi, *penalty*
- Untuk memastikan bahwa proses pengamanan dilakukan, penyedia jasa harus melakukan *security audit* secara berkala (misal minimal setahun sekali) yang dilakukan oleh pihak ketiga yang independen
- Adanya peraturan (regulasi) yang secara eksplisit mengatur ini yang diterbitkan oleh instansi terkait

Bagaimana Melindunginya?

- Secara teknis sama dengan perlindungan pada aspek confidentiality
  - Kriptografi (enkripsi, dekripsi)
  - Pemisahan akses (jaringan, aplikasi)
  - Kebijakan tentang akses data
  - ...

Regulasi Terkait Privasi

- Eropa: GDPR (General Data Protection Regulation)
  - https://gdpr-info.eu/
- Indonesia: Telah ada UU 27/2022 tentang PDP (Perlindungan Data Pribadi)
  - https://peraturan.bpk.go.id/Home/Details/229798/uu-no-27-tahun-2022

Integrity (integritas)

- Data (informasi / sistem) tidak dapat diubah oleh pihak yang tidak berhak
- Sebagai contoh
  - Saldo rekening bank kita tidak boleh berubah jika tidak ada transaksi yang sah
  - Pilihan di pemilu (e-voting) harus dapat dipastikan tetap sampai di pusat
  - Nilai mahasiswa di sistem informasi kampus harus benar
- Untuk sistem **transaksi**, aspek integritas ini merupakan aspek yang sangat penting (bahkan lebih penting dari confidentiality)

Integrity

- Serangan
  - Spoofing (pemalsuan)
  - Ransomware (mengubah berkas – dienkripsi – sehingga tidak dapat diakses)
  - Man-in-the-middle (MiTM): mengubah data di tengah perjalanan sehingga data berubah di tujuan

Integrity

- Perlindungan
  - Message authentication code (MAC)
  - Hash function
  - Menggunakan digital signature
  - Blockchain?

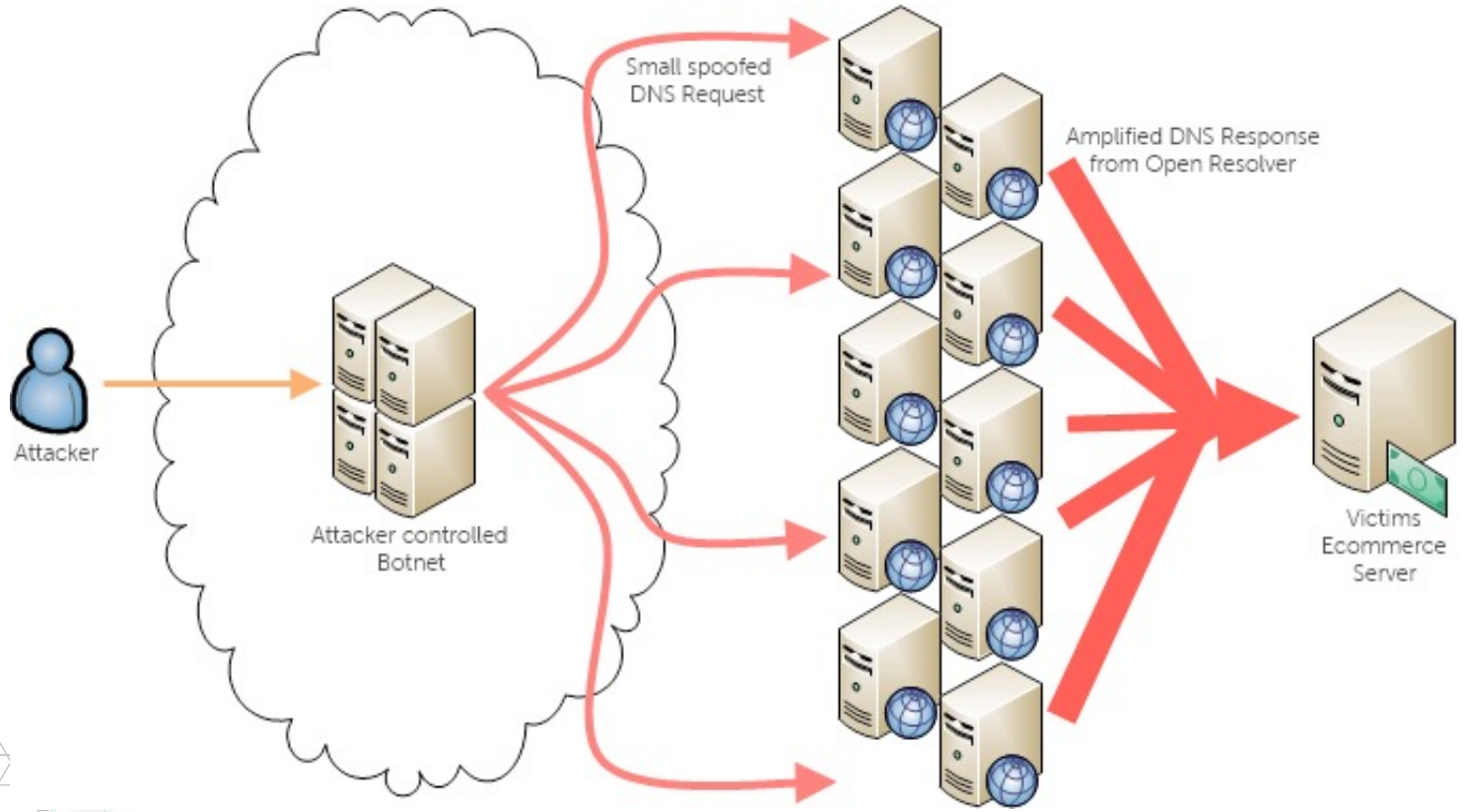
Availability (Ketersediaan)

- Data / informasi / sistem harus tersedia ketika dibutuhkan
- Disebabkan semakin tingginya ketergantungan kepada IT
- Tidak tersedianya data akan mengakibatkan kegagalan bisnis, yang kemudian berdampak kepada aspek finansial

Serangan

- Meniadakan layanan: Denial of Service (DoS)
  - Jaringan
  - Aplikasi
  - Infrastruktur pendukung (misal: listrik)
- Menyerang dari berbagai tempat / lokasi: distributed
  - Distributed Denial of Service (DDoS) attack

DNS DDoS Attack



Perlindungan

- Redundansi, duplikat
  - Server di Data Center (DC) & di Disaster Recovery Center (DRC)
- Backup (& Restore)
- Filtering (network)
- BCP (Business Continuity Planning)
  - Mengamati aspek-aspek yang kritikal terhadap kelangsungan bisnis, baik secara teknis maupun non-teknis
  - DRP: Disaster Recovery Plan
- Cyberdrill

non-repudiation

- Tidak dapat menyangkal (telah melakukan sebuah transaksi)
- Serangan
  - Transaksi palsu, spoofing
  - Menghapus jejak
- Perlindungan
  - message authentication code, hash function
  - digital signature
  - logging

Authentication

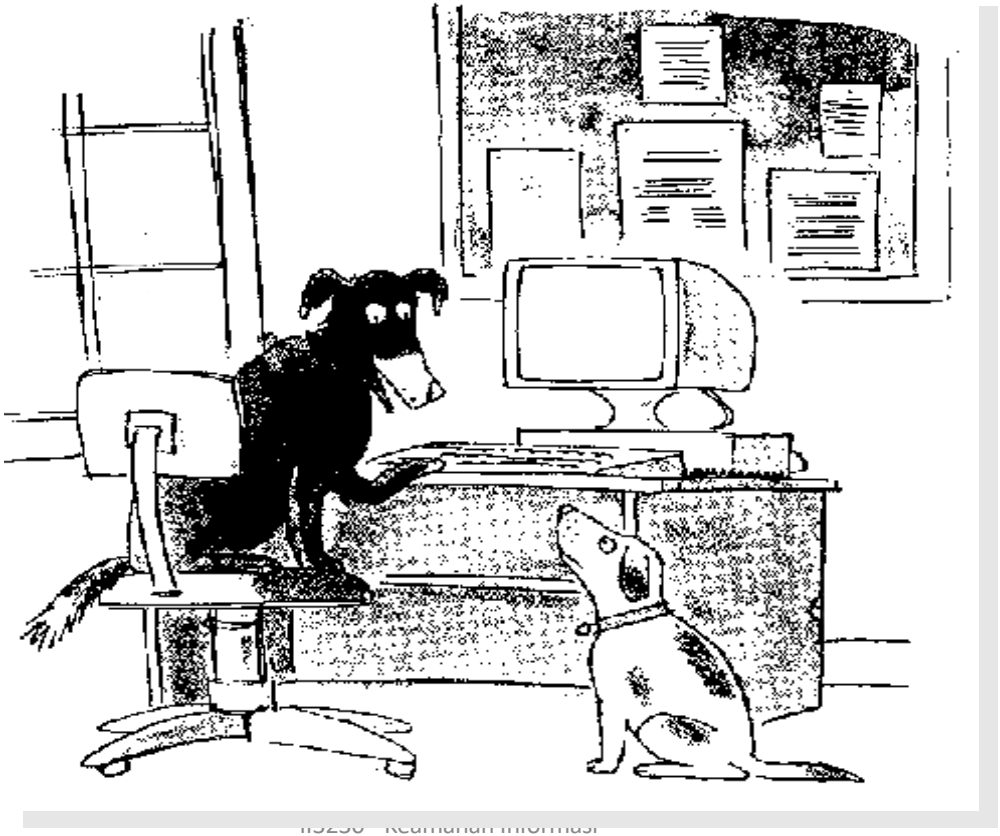
- Meyakinkan keaslian identitas {seseorang / mesin / komputer / server / sumber data}
  - Masalah ketika tidak ada kontak fisik (lack of physical contact)
  - Siapa yang mengakses layanan (internet banking)?
- Faktor otentikasi
  - sesuatu yang dimiliki | **what you have**: kartu identitas, kunci, token, authenticator
  - sesuatu yang diketahui | **what you know**: userid (identitas), password, PIN
  - sesuatu yang melekat | **what you are**: biometric

  - *claimant at a particular place*
  - *authentication is established by trusted third party*

Authentication (2)

- Serangan
  - identitas palsu, KTP palsu
  - terminal palsu, mesin ATM palsu, situs web gadungan (abal-abal, plesetean)
- Perlindungan
  - token (hard token, soft token)
  - OTP (one time password)
  - digital certificates

on the internet, nobody knows you're a dog



Access Control

- Mekanisme untuk mengatur siapa boleh melakukan apa
  - *Roles, separation of duties*
  - Bersama dengan authentication memetakan seseorang ke sebuah *role*
- Adanya kelas / klasifikasi data dan roles, misalnya:
  - *Public*
  - *Private*
  - *Confidential*
  - *Top Secret*

Access Control

- Serangan
  - Menerobos pembatasan
  - Menaikkan tingkat pengguna
  - Cracking, brute force
  - Merusak kendali akses
- Perlindungan
  - Segmentasi jaringan & fisik
  - Membuat daftar siapa/apa yang dapat mengakses, filtering
  - Ilegal access detection
  - Logging