PROGRAM STUDI

S1 SISTEM KOMPUTER

UNIVERSITAS DIPONEGORO

Pengantar Keamanan Sistem Informasi

By: Rinta Kridalukmana, S. Kom, MT
Email: kridalukmana@undip.ac.id

Materi

- Mengapa keamanan sistem penting ?
- Contoh-contoh gangguan/serangan/ancaman terhadap keamanan sistem informasi
- Pengamanan sistem
- Beberapa teknik dan *tools* untuk mengamankan sistem

Pentingnya Keamanan Sistem

- Mengapa keamanan sistem informasi diperlukan ?
  - Teknologi komunikasi modern (mis: Internet) membawa beragam dinamika dari dunia nyata ke dunia virtual
    - Dalam bentuk transaksi elektronis (mis: e-banking) atau komunikasi digital (mis: e-mail, messenger)
    - Membawa baik aspek positif maupun negatif (contoh: pencurian, pemalsuan, penggelapan, …)
  - Informasi memiliki “nilai” (ekonomis, politis) → obyek kepemilikan yang harus dijaga
    - Kartu kredit
    - Laporan keuangan perusahaan
    - Dokumen-dokumen rancangan produk baru
    - Dokumen-dokumen rahasia kantor/organisasi/perusahaan

Pentingnya Keamanan Sistem

- Mengapa sistem informasi rentan terhadap gangguan keamanan
  - Sistem yg dirancang untuk bersifat “terbuka” (mis: Internet)
    - Tidak ada batas fisik dan kontrol terpusat
    - Perkembangan jaringan *(internetworking)* yang amat cepat
  - Sikap dan pandangan pemakai
    - Aspek keamanan belum banyak dimengerti
    - Menempatkan keamanan sistem pada prioritas rendah
  - Ketrampilan *(skill)* pengamanan kurang

Beberapa Jenis Serangan/Gangguan

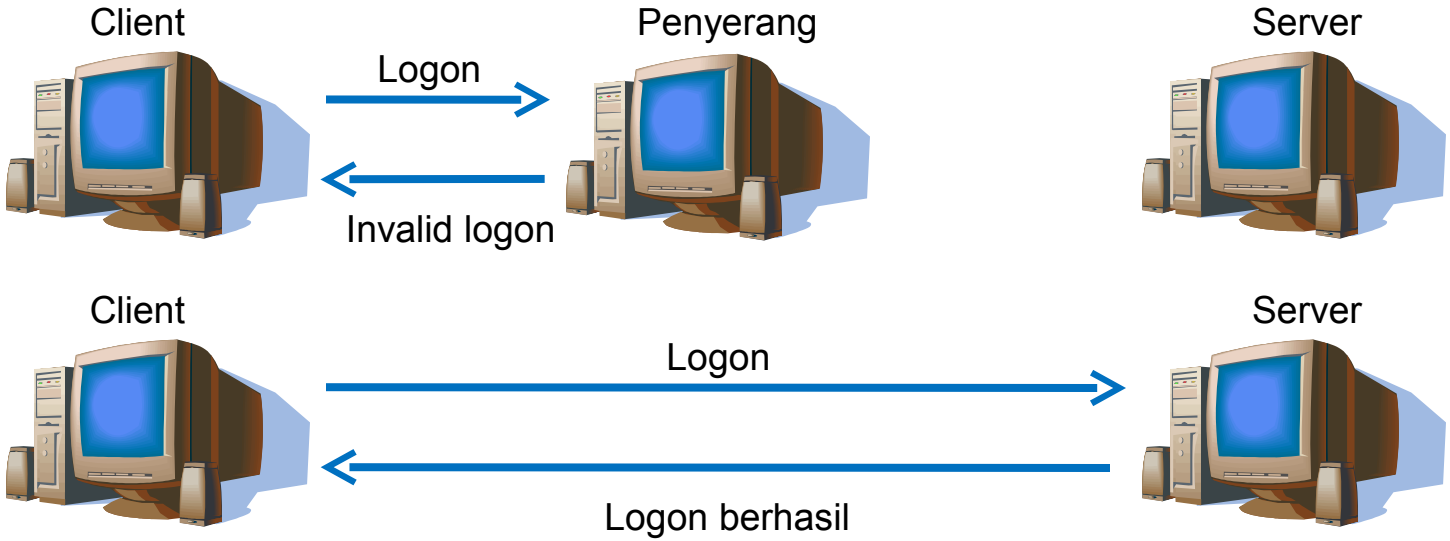
- Serangan untuk mendapatkan akses *(access attacks)*
  - Berusaha mendapatkan akses ke berbagai sumber daya komputer atau data/informasi
- Serangan untuk melakukan modifikasi *(modification attacks)*
  - Didahului oleh usaha untuk mendapatkan akses, kemudian mengubah data/informasi secara tidak sah
- Serangan untuk menghambat penyediaan layanan *(denial of service attacks)*
  - Menghambat penyediaan layanan dengan cara mengganggu jaringan komputer

Beberapa Cara Melakukan Serangan

- Sniffing
  - Memanfaatkan metode broadcasting dalam LAN
  - “Membengkokkan” aturan Ethernet, membuat network interface bekerja dalam mode *promiscuous*
  - Contoh-contoh sniffer: Sniffit, TCP Dump, Linsniffer
  - Mencegah efek negatif sniffing
    - Pendeteksian sniffer (local & remote)
    - Penggunaan kriptografi (mis: ssh sbg pengganti telnet)

Beberapa Cara Melakukan Serangan

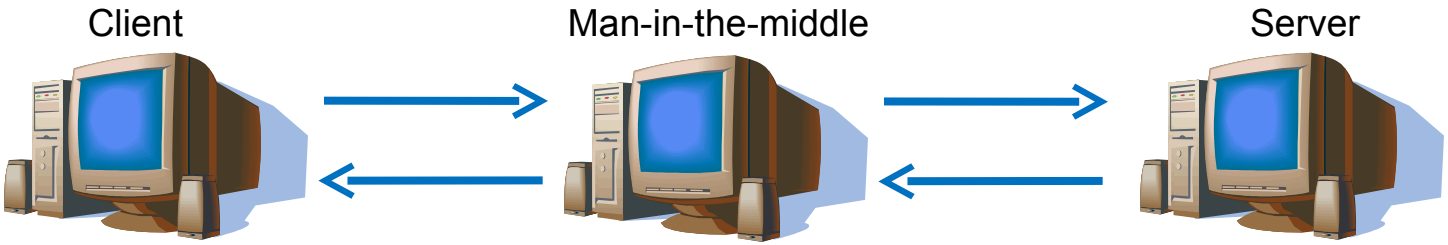
- Spoofing
  - Memperoleh akses dengan acara berpura-pura menjadi seseorang atau sesuatu yang memiliki hak akses yang valid
  - Spoofer mencoba mencari data dari user yang sah agar bisa masuk ke dalam sistem (mis: username & password)



Pada saat ini, penyerang sudah mendapatkan username & password yang sah untuk bisa masuk ke server

Beberapa Cara Melakukan Serangan

- Man-in-the-middle
  - Membuat client dan server sama-sama mengira bahwa mereka berkomunikasi dengan pihak yang semestinya (client mengira sedang berhubungan dengan server, demikian pula sebaliknya)



Beberapa Cara Melakukan Serangan

- Menebak password
  - Dilakukan secara sistematis dengan teknik brute-force atau dictionary
  - Teknik brute-force: mencoba semua kemungkinan password
  - Teknik dictionary: mencoba dengan koleksi kata-kata yang umum dipakai, atau yang memiliki relasi dengan user yang ditebak (tanggal lahir, nama anak, dsb)

Modification Attacks

- Biasanya didahului oleh access attack untuk mendapatkan akses
- Dilakukan untuk mendapatkan keuntungan dari berubahnya informasi
- Contoh:
  - Pengubahan nilai kuliah
  - Penghapusan data utang di bank
  - Mengubah tampilan situs web

Denial of Service Attacks

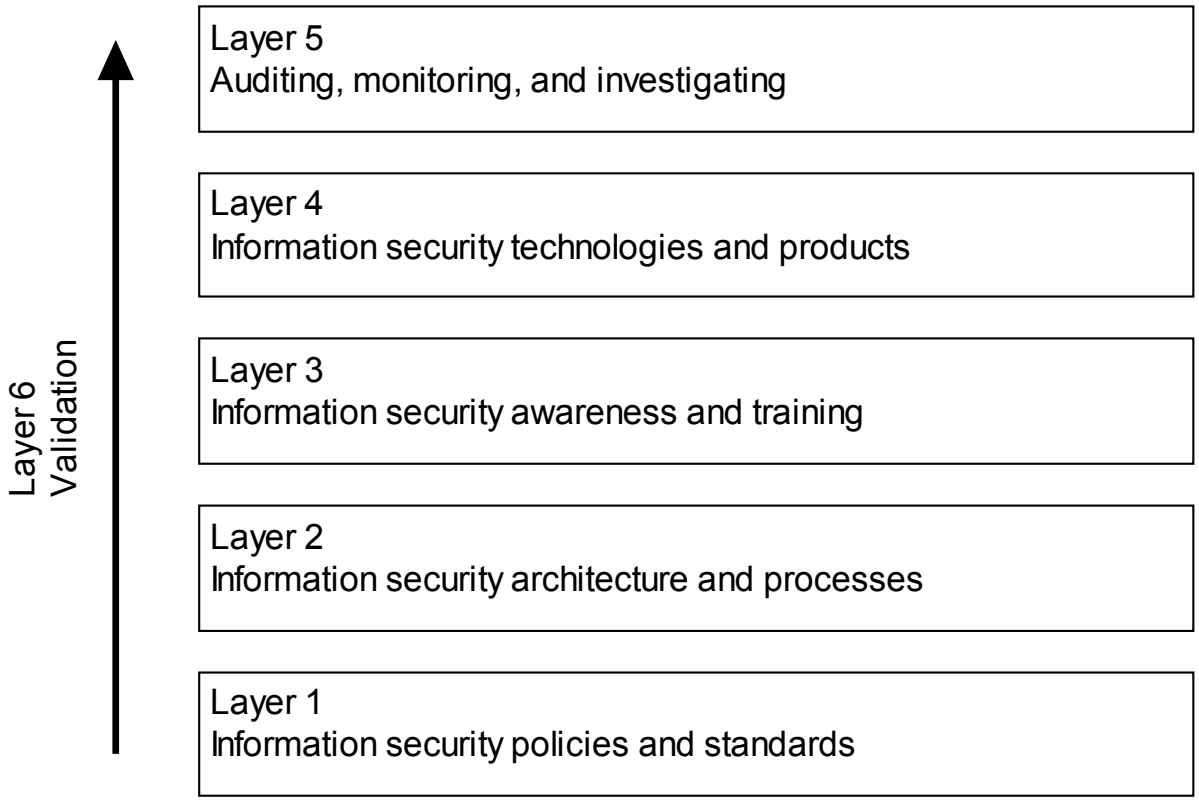
- Berusaha mencegah pemakai yang sah untuk mengakses sebuah sumber daya atau informasi
- Biasanya ditujukan kepada pihak-pihak yang memiliki pengaruh luas dan kuat (mis: perusahaan besar, tokoh-tokoh politik, dsb)
- Teknik DoS
  - Mengganggu aplikasi (mis: membuat webserver down)
  - Mengganggu sistem (mis: membuat sistem operasi down)
  - Mengganggu jaringan (mis: dengan TCP SYN flood)

Denial of Service Attacks

- Contoh: MyDoom worm email (berita dari F-Secure, 28 Januari 2004) http://www.f-secure.com/news/items/news_2004012800.shtml
  - Ditemukan pertama kali 26 Januari 2004
  - Menginfeksi komputer yang diserangnya. Komputer yang terinfeksi diperintahkan untuk melakukan DoS ke www.sco.com pada tanggal 1 Februari 2004 jam 16:09:18
  - Pada saat itu, diperkirakan 20-30% dari total lalulintas e-mail di seluruh dunia disebabkan oleh pergerakan worm ini
  - Penyebaran yang cepat disebabkan karena:
    - "Penyamaran" yang baik (tidak terlihat berbahaya bagi user)
    - Penyebaran terjadi saat jam kantor
    - Koleksi alamat email sasaran yang agresif (selain mengambil dari address book di komputer korban, juga membuat alamat email sendiri)

Pengamanan Sistem Informasi

Keamanan sistem sebagai satu konsep terpadu

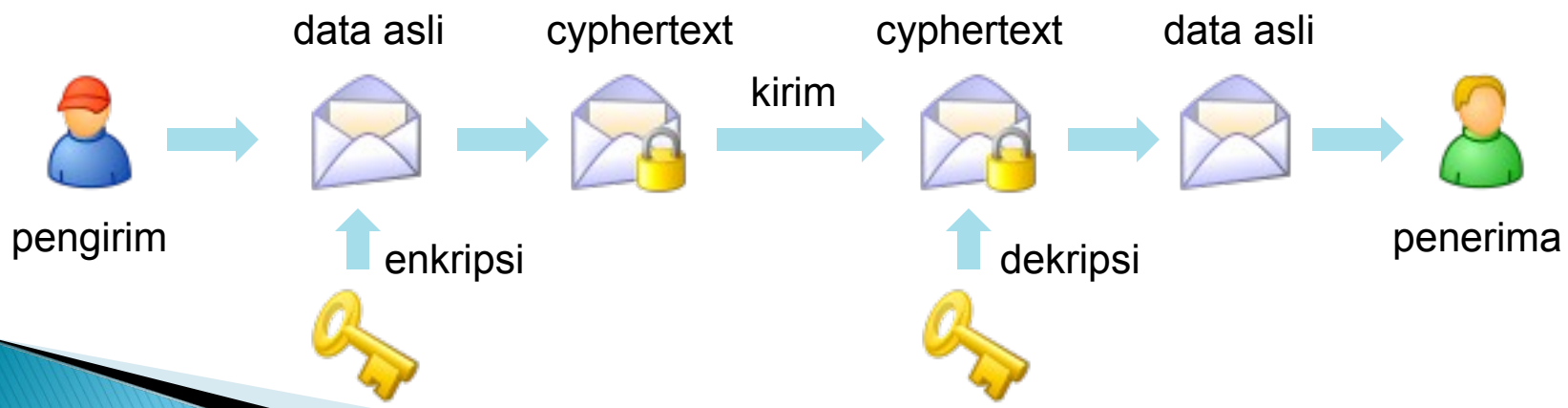


Kriptografi

- Studi tentang enkripsi dan dekripsi data berdasarkan konsep matematis
- Meningkatkan keamanan data dengan cara menyamarkan data dalam bentuk yang tidak dapat dibaca
  - enkripsi: data asli → bentuk tersamar
  - dekripsi: data tersamar → data asli
- Komponen sistem kriptografi:
  - fungsi enkripsi & dekripsi
  - kunci

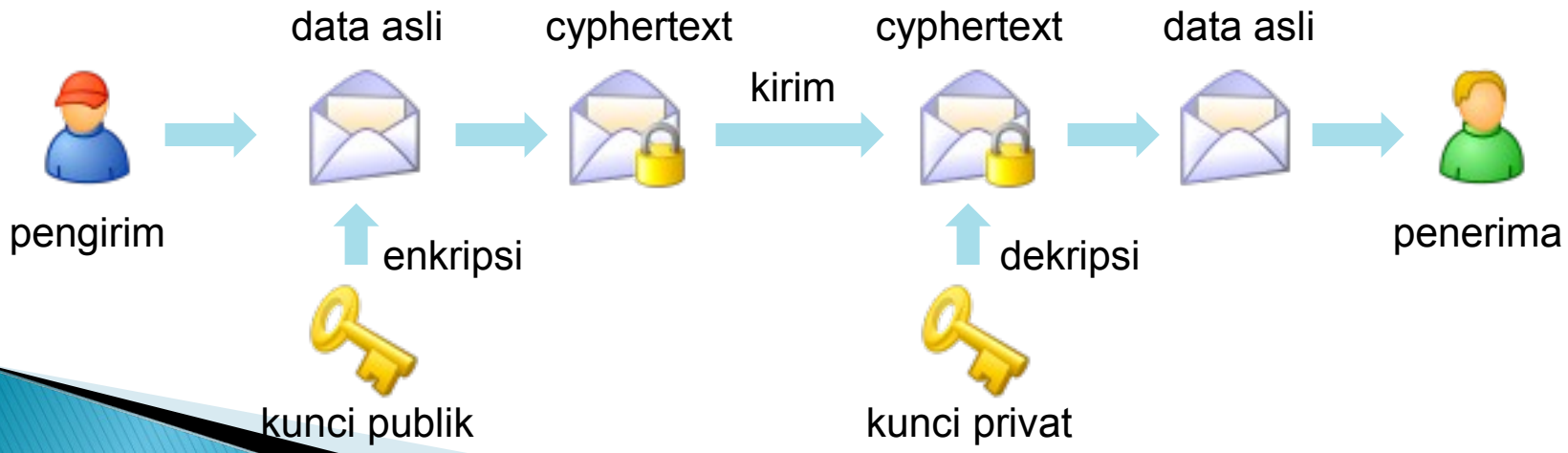
Kriptografi Simetris

- Kunci yang sama untuk enkripsi & dekripsi
- Problem
  - Bagaimana mendistribusikan kunci secara rahasia ?
  - Untuk n orang pemakai, diperlukan n(n-1)/2 kunci → tidak praktis untuk pemakai dalam jumlah banyak



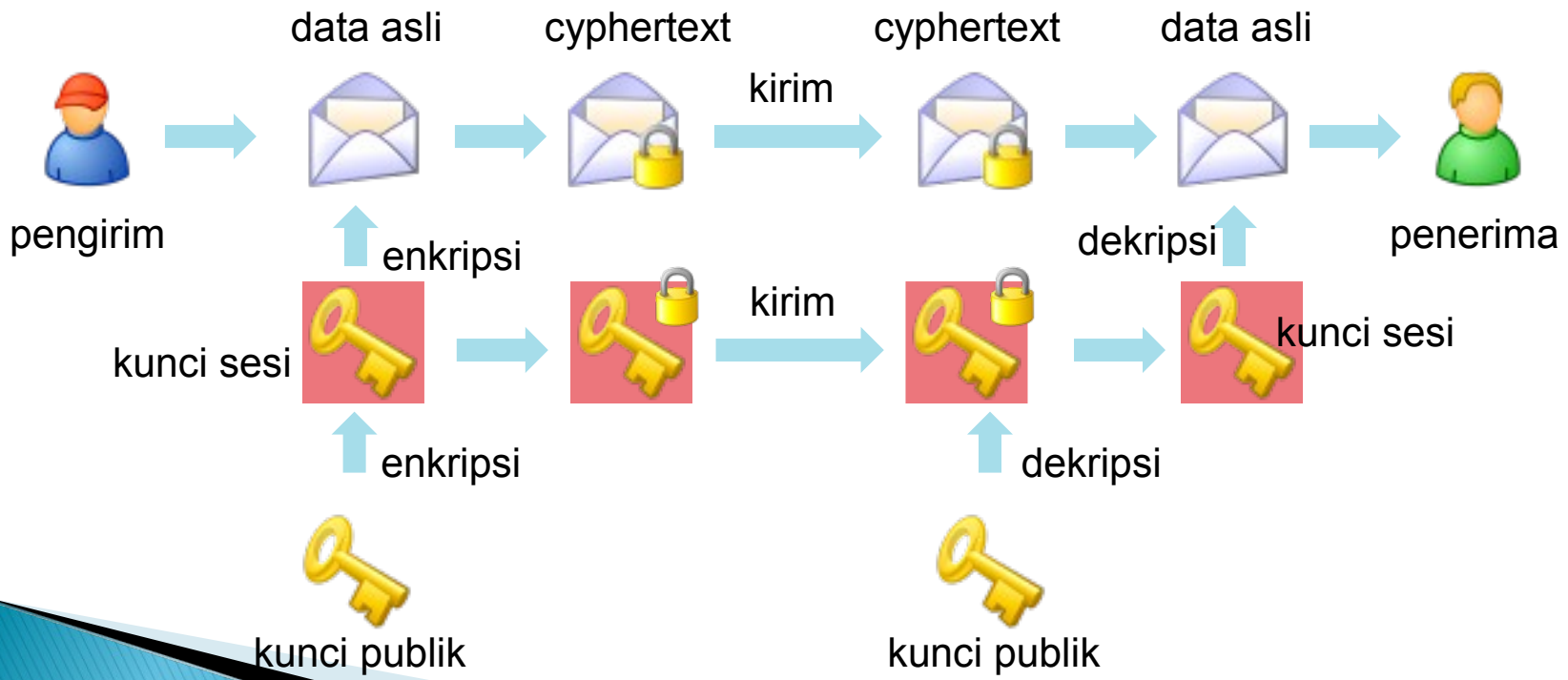
Kriptografi Asimetris

- Kunci enkripsi tidak sama dengan kunci dekripsi. Kedua kunci dibuat oleh penerima data
  - enkripsi → kunci publik
  - dekripsi → kunci privat



Kriptografi Hibrid

- Menggabungkan antara kriptografi simetris dan asimetris → mendapatkan kelebihan kedua metode



Infrastruktur Kunci Publik

- Pengamanan komunikasi data untuk keperluan publik (antar institusi, individu-institusi, individu-individu, dsb)
  - Kebutuhan komunikasi yang aman
  - Heterogenitas pemakai
  - Jaringan komunikasi yang kompleks
- Komponen infrastruktur kunci publik:
  - Tandatangan digital (digital signature): untuk menjamin keaslian dokumen digital yang dikirim
  - Otoritas Sertifikat (certificate authority): lembaga yang mengeluarkan sertifikat digital sebagai bukti kewenangan untuk melakukan transaksi elektronis tertentu

Infrastruktur Kunci Publik

- Mengapa diperlukan ?
  - Kasus KlikBCA beberapa tahun yang lalu
    - Ada orang yang meniru persis situs netbanking Bank BCA, dengan URL yang mirip
    - Situs tersebut menerima informasi login dari nasabah BCA (userID dan password)
    - Apa yang terjadi jika informasi login nasabah disalahgunakan ?
  - Semakin banyaknya transaksi elektronis yang memerlukan legalitas secara elektronis juga
    - Dokumen kontrak
    - Perjanjian jual beli