

KEAMANAN SISTEM INFORMASI

Budi Rahardjo
budi@cert.or.id

Latar Belakang

- ◆ Meningkatnya teknologi komputer dan Internet
 - Mulai digunakan sebagai basis dari bisnis (e-commerce)
 - Mudah membuat identitas, email palsu
 - Meningkatnya jumlah pengguna yang pandai

Beberapa Statistik

- Angka pasti, sulit ditampilkan karena kendala bisnis. Negative publicity.
- **1996**
FBI National Computer Crime Squad, computer fraud detected is less than 15%, of which 10% is reported.
- **1996**
American Bar Association: from 1000 companies, 48% experienced computer fraud in the last 5 years.
- **1996**
England. NCC Information Security Breaches Survey: computer crime increases 200% from 1995 to 1996.
- **1997**
FBI: court case related to computer crime increases 950% from 1996 to 1997, convicted increases to 88%.

Beberapa Statistik

- 1988. Sendmail dieksploitasi oleh R.T. Morris sehingga melumpuhkan Internet. Diperkirakan kerugian mencapai \$100 juta. Morris dihukum denda \$10.000.
- 10 Maret 1997. Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi sebuah airport lokal (Worcester, Mass.) sehingga memutuskan komunikasi di control tower dan menghalau pesawat yang hendak mendarat.
- **1999 Computer Security Institute (CSI) / FBI Computer Crime Survey** menunjukkan beberapa statistik yang menarik, seperti misalnya ditunjukkan bahwa “disgruntled worker” merupakan potensi attack / abuse.
[Http://www.gocsi.com](http://www.gocsi.com)

Beberapa Statistik

- **2000**
Beberapa situs web di Indonesia dijebol. Contoh terakhir: Bank BCA, Bank Lippo, Bank Bali.
Cracker Indonesia ditangkap di Singapura

Mungkinkah Aman?

- Sangat sulit mencapai 100% aman
- Ada timbal balik antara keamanan vs. kenyamanan (security vs convenience)

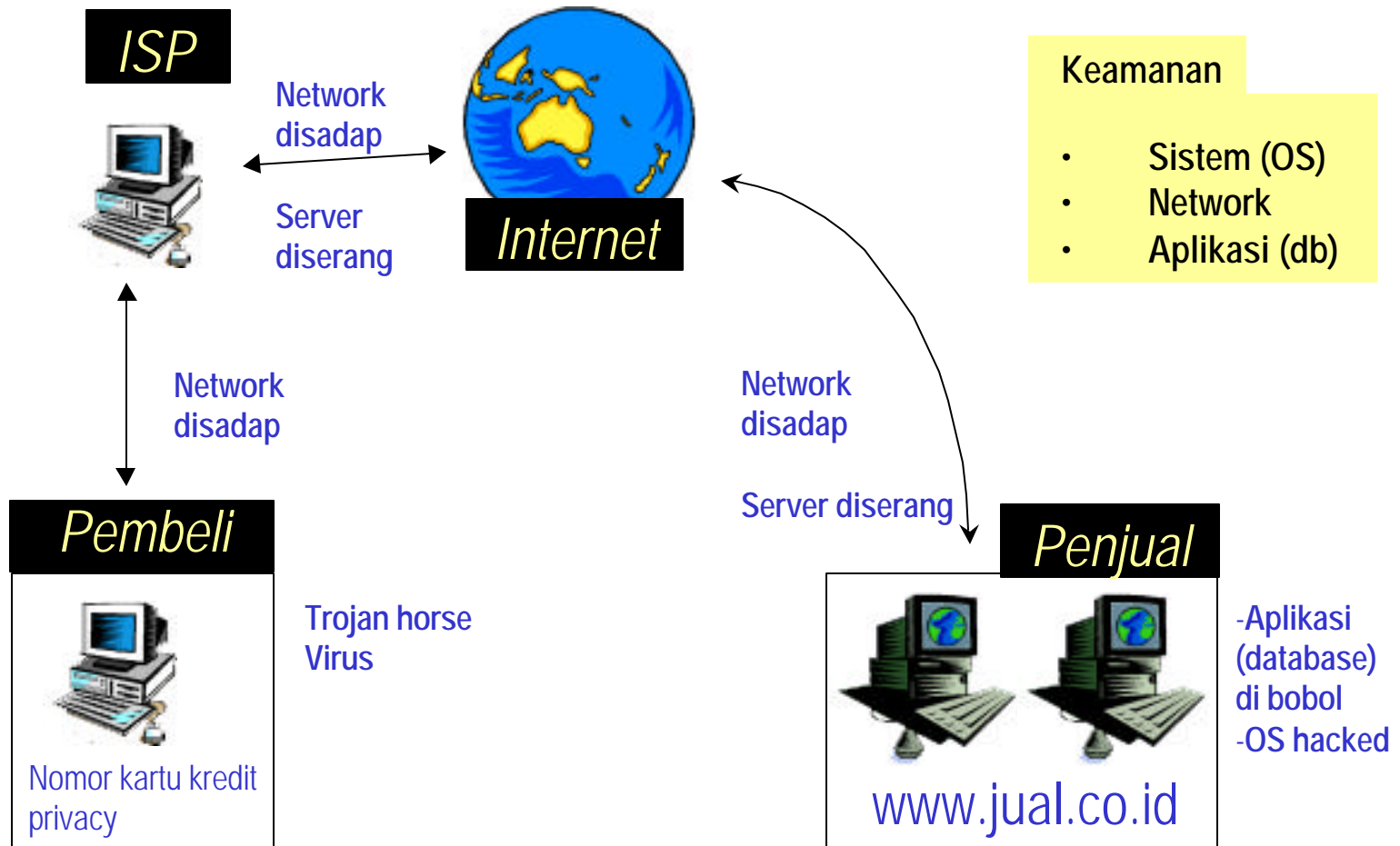
- Definisi computer security:
(Garfinkel & Spafford)

A computer is secure if you can depend on it and its software to behave as you expect

Lubang Keamanan

- Banyak orang menyangka sumber utama lubang keamanan pada network
- Network dapat diamankan dengan menggunakan enkripsi (misal: SSL, SSH, TLS, RSA, ECC dll.) sehingga data susah disadap
- Summary: network dapat diamankan dengan baik

Sumber Lubang Keamanan



Aspek Keamanan

- Privacy / confidentiality
- Integrity
- Authentication
- Availability
- Non-repudiation
- Access control

Privacy / Confidentiality

- Proteksi data [pribadi] yang sensitif
 - Nama, tempat tanggal lahir, agama, hobby, penyakit yang pernah diderita, status perkawinan
 - Data pelanggan
 - Sangat sensitif dalam e-commerce, healthcare
- Serangan: sniffer

Integrity

- Informasi tidak berubah tanpa ijin (tampered, altered, modified)
- Serangan: spoof, virus, trojan horse

Authentication

- Meyakinkan keaslian data, sumber data, orang yang mengakses data, server yang digunakan
 - penggunaan digital signature, biometrics
- Serangan: password palsu

Availability

- Informasi harus dapat tersedia ketika dibutuhkan
 - server dibuat hang, down, crash
- Serangan: Denial of Service (DoS) attack

Non-repudiation

- Tidak dapat menyangkal (telah melakukan transaksi)
 - menggunakan digital signature
 - perlu pengaturan masalah hukum

Access Control

- Mekanisme untuk mengatur siapa boleh melakukan apa
 - biasanya menggunakan password
 - adanya kelas / klasifikasi

Mempelajari Crackers

- Ada baiknya mengerti perilaku perusak.
- Siapakah mereka?
- Apa motifnya?
- Bagaimana cara masuk?
- Apa yang dilakukan setelah masuk?

ID-CERT

- Indonesia Computer Emergency Response Team
- Model: CERT, AUSCERT
- Membutuhkan dukungan
- <http://www.cert.or.id>
- Email: budi@cert.or.id