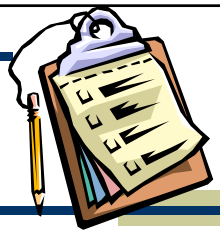
Dasar Keamanan Jaringan Komputer

Topik…



- Kerapuhan Sistem (Vulnerabilities)
- Ancaman (Threats)
- Penyelesaian (Solutions)
- Pertahanan (Defence)

Mungkinkah Aman?

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

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

  Keamanan merupakan sebuah proses, bukan sebuah produk akhir. (*Security is a process, not an end product*.)

Jenis Serangan

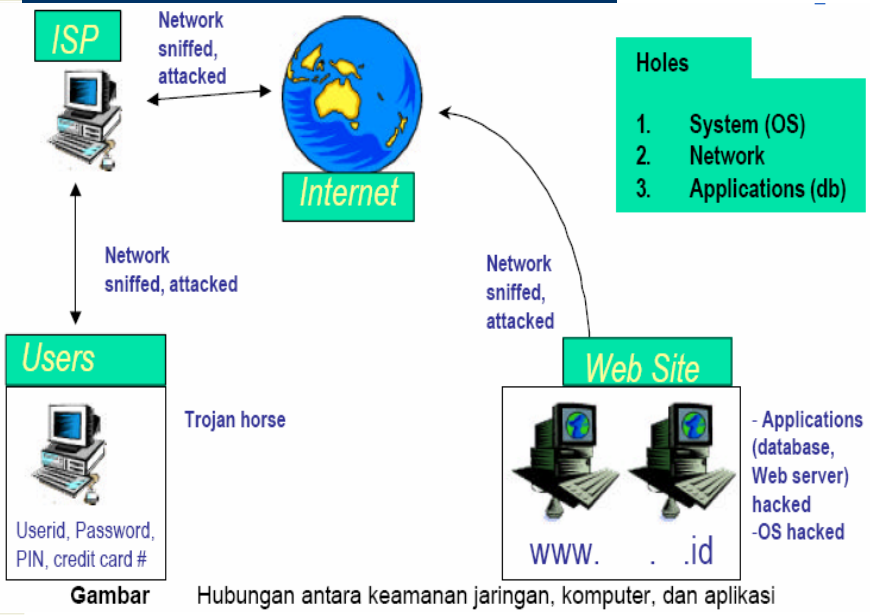
- Interupsi : sebuah system yang dirusak sebelum sampai ketujuan.
- Interception : user yang tidak berhak (anauthorized) mendapatkan akses file.
- Modifikasi : user yang tidak berhak tidak hanya mendapatkan akses tetapi juga dapat merubahnya.
- Fabrication : user yang tidak berhak memasukkan atau menyelipkan obyek kedalam system.

Jenis-Jenis Penyerang

- Joyriders.
- Vandals.
- Score Keepers.
- Spies (Industrial & Otherwise).
- Stupidity & Accidents.

KLASIFIKASI KEAMANAN SISTEM INFORMASI

- **Network security**: fokus kepada media pembawa informasi/data, seperti jaringan komputer
- **Computer security**: fokus kepada komputer (server, workstation, terminal), termasuk di dalamnya masalah yang berhubungan dengan operating system
- **Application security**: fokus kepada program aplikasi (software) dan database.



Gambar Hubungan antara keamanan jaringan, komputer, dan aplikasi

ASPEK KEAMANAN

1. Privacy / confidentiality
2. Intergrity
3. Authentication
4. Availability
5. Access control

Privacy/Confidentially

- Interception (sniffer)
- Virus (Virus SirCam)
- Trojan Horse→ Remote Access

Biasanya mengambil userid dan password

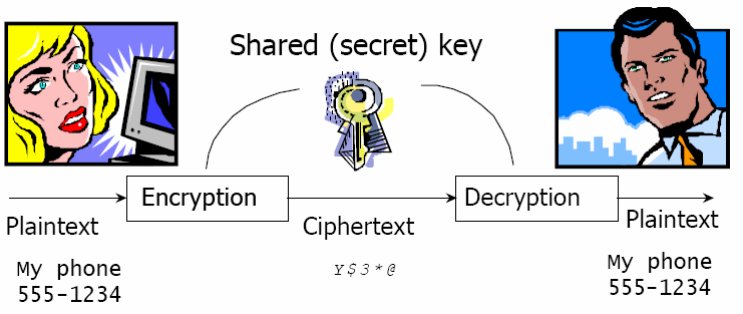
TELNET → ssh (Secure Shell)

FTP → scp (Secure Copy)

Privacy/Confidentially (sambungan)

Pencegahan :

Kriptografi



Integrity (keutuhan)

- Data atau informasi tidak boleh berubah (*tampered, altered, modified*) tanpa ijin dari pemilik.
- Serangan : virus, trojan horse, *man in the middle attack*
- Pengamanan terhadap aspek ini adalah dengan menggunakan *(digital) signature, checksum, hash algorithm*, dan teknik-teknik lain.

Authentication

- Digunakan untuk meyakinkan keaslian data, sumber data, orang yang mengakses data, dan server yang digunakan.
- Implementasi menggunakan :

  tanda pengenal, password, digital signature, dan biometrics.

Availability

- Menjamin bahwa data dan informasi harus dapat tersedia ketika dibutuhkan
- Serangan :
  - DOS (Denial of Service)
  - DDOS (Distributed Denial of Service)

Availability (sambungan)

- Pengamanan :
  - *Intrusion Detection System (*IDS),
  - Backup,
  - *Audit trail*,
  - *Dissaster recovery*,
  - Pembuatan mirror dari sistem di tempat lain.

Access Contol

- Membatasi atau mengatur siapa boleh melakukan apa. Biasanya akses ke suatu data atau sistem memiliki tingkat (level, jenjang).
- Pengamanan :
  - Menggunakan password
  - penggunaan biometrik (tangan, sidik jari jempol, mata)

Aspek Keamanan yang Harus Dipertimbangkan

→ Implementasi bergantung kepada tingkat keamanan yang diinginkan, budget, dan ketersediaan teknologi.

- **Kebijakan dan Prosedur Keamanan (Security Policies and Procedures)**
- **Keamanan Aplikasi**
- **Mengevaluasi Desain Jaringan**
- **Implementasi Firewall**
- **Implementasi Intrusion Detection System (IDS)**
- **Implementasi Network Management**
- **Pemasangan Anti virus**
- **Desain dan Implementasi Backup System & Dissaster Recovery Plan**
- **Desain dan Implementasi Audit Trail**

Kebijakan dan Prosedur Keamanan (Security Policies and Procedures)

- merupakan komponen penting sebab dia yang menjadi perantara antara sistem keamanan dengan manusia pengguna sistem informasi tersebut.
- sejalan dengan asas atau kebijakan yang mengatur semua aktivitas.
- harus ada dan dimengerti oleh semua pengguna dan pengelola sistem informasi

Inti dari kebijakan dan prosedur keamanan adalah:

- Membuat setiap pengguna bertanggung jawab (*accountable*) terhadap perilakunya (*actions*, *behaviors*).
- Mendesain sistem sedemikian rupa sehingga untuk melakukan kejahatan (*crime*, *fraudulent act*) dibutuhkan lebih dari satu orang.

Keamanan Aplikasi

Klasifikasi	Definisi
Public	Informasi yang secara eksplisit dinyatakan untuk publik. Informasi ini dapat dikomunikasikan melalui terbitan konvensional (majalah, surat kabar, newsletter) dan/atau WWW
Internal	Informasi yang tidak/belum boleh diketahui oleh umum tapi sudah diketahui di dalam (internal). Informasi ini dapat dijadikan publik apabila sudah mendapat persetujuan. Informasi ini juga dapat tetap menjadi internal.
Confidential	Informasi yang bilamana bocor dapat memberikan impak negatif yang berat terhadap institusi, pekerjanya, dan pihak-pihak yang terkait. Informasi ini dapat diketahui oleh pekerja internal namun tidak diperuntukan untuk publik.
Restricted	Informasi yang bilaman bocor dapat memberikan dampak negatif yang sangat kritis terhadap masalah finansial, hukum (legal), regulatory, atau reputasi dari institusi, pekerjanya, dan pihak yang terkait. Informasi ini hanya diketahui oleh orang-orang tertentu saja.

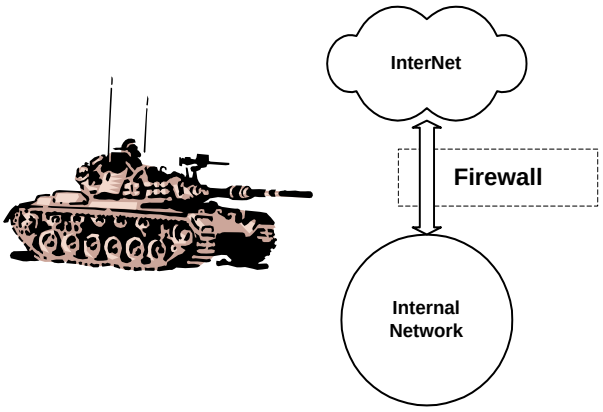
Mengevaluasi Desain Jaringan

- melakukan evaluasi terhadap desain, baik untuk intranet maupun hubungan ke Internet.
- melakukan segmentasi dan menggunakan perangkat yang memiliki tingkat keamanan yang lebih tinggi (misal menggunakan switch sebagai pengganti hub biasa).

Implementasi Firewall

- Firewall merupakan pengaman yang memisahkan jaringan internal dengan jaringan Internet. Jika dianalogikan dengan rumah, maka firewall merupakan pagar yang melindungi rumah. Tamu harus melalui pagar (firewall) dulu sebelum masuk ke rumah.
- Ada beberapa jenis firewall. Pemilihan firewall yang tepat membutuhkan pengkajian yang lebih mendalam.

Layout Firewall



Implementasi Intrusion Detection System (IDS)

- IDS mendeteksi adanya intrusion (tamu yang tidak diundang). Jika dianalogikan dengan rumah, maka IDS mirip dengan sistem alarm.
- Jenis IDS, yaitu network-based IDS dan host-based IDS.
  - Network-based IDS mengamati jaringan untuk mendeteksi adanya kelainan (anomali). → network flooding atau port scanning, usaha pengiriman virus melalui email
  - Host-based IDS dipasang pada host untuk mendeteksi kelainan pada host tersebut (misalnya ada proses yang semestinya tidak jalan akan tetapi sekarang sedang jalan, adanya virus di workstation).

Implementasi Network Management

- Pengelola dapat memantau penggunaan jaringan untuk mendeteksi adanya masalah (jaringan tidak bekerja,lambat, dan seterusnya).
- Implementasi dari network management dapat bervariasi. Standar yang sering digunakan saat ini adalah SNMP (Simple Network Management Protokol).

Pemasangan Anti virus

- Penggunaan anti virus yang up-to-date
- Anti virus ini harus dipasang pada setiap workstation dan server yang ada di jaringan sistem informasi

Tools Security Jaringan

- NET TOOLS