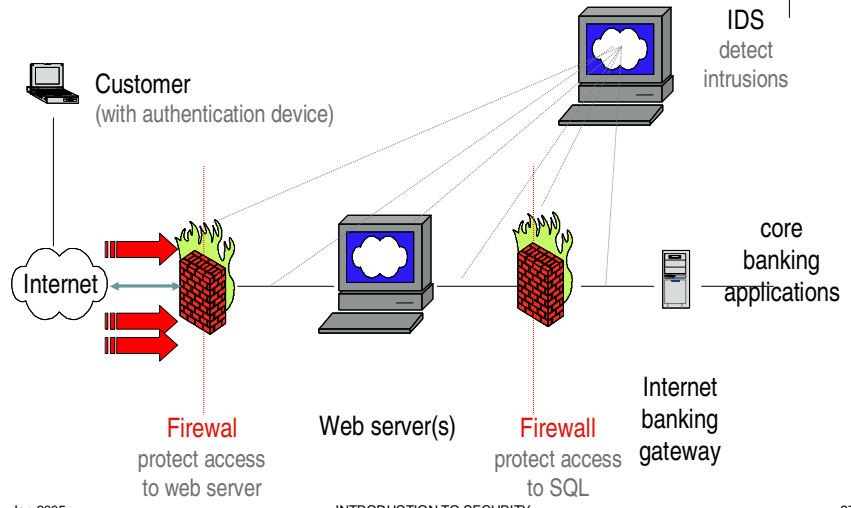
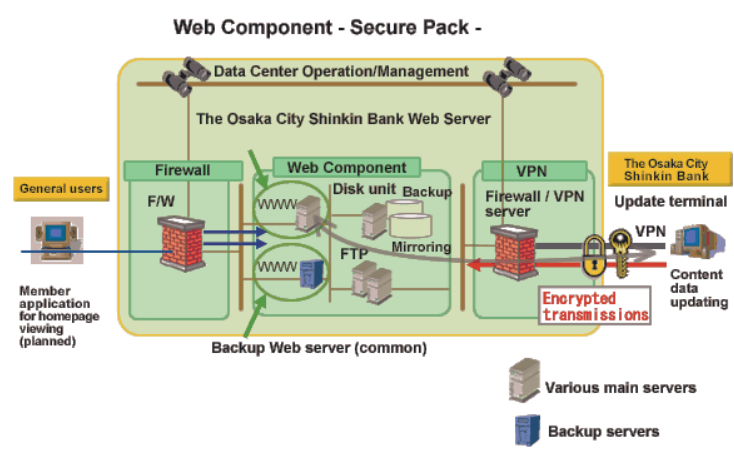
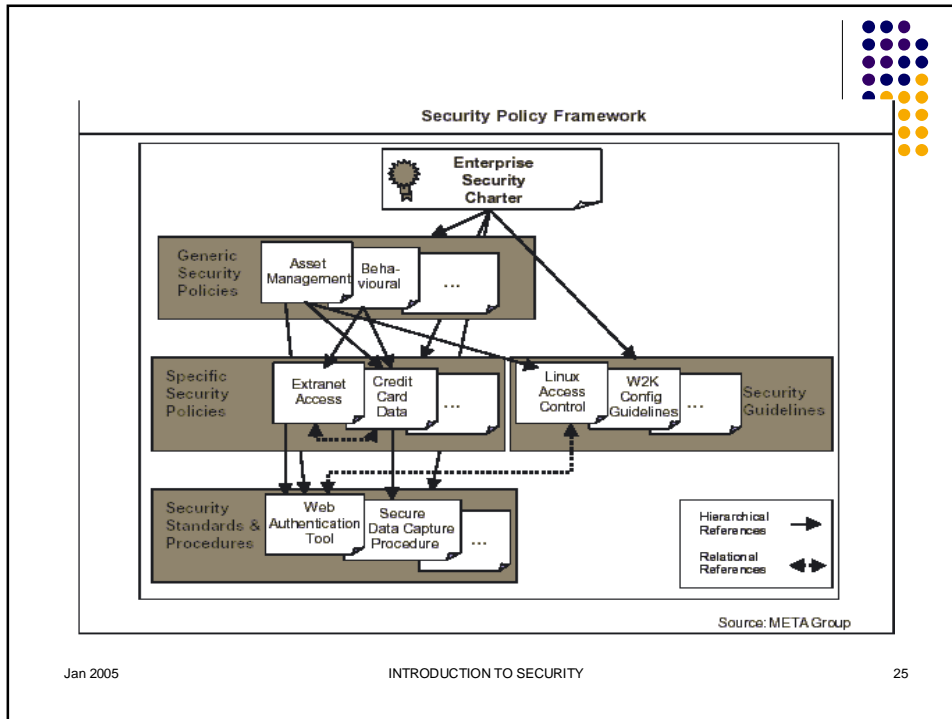


Pengamanan Berlapis



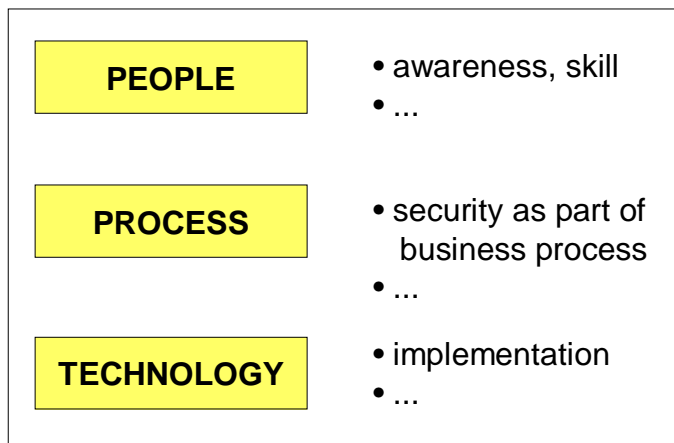
Contoh Implementasi: Osaka Bank





Pengamanan Menyeluruh

- Harus menyeluruh - holistic approach



Mempelajari crackers



- Mempelajari:
 - Perilaku perusak
 - Siapakah mereka?
 - Apa motifnya?
 - Bagaimana cara masuk?
 - Apa yang dilakukan setelah masuk?
- Tools: honeypoy, honeynet

Know Your Enemy

Crackers SOP / Methodology



Dari “Hacking Exposed”:

- Target acquisition and information gathering
- Initial access
- Privilege escalation
- Covering tracks
- Install backdoor
- Jika semua gagal, lakukan DoS attack



More on Interruption Attack (cont.)



- Distributed Denial of Service (DDoS) attack
 - Flood your network with spoofed packets from many sources
 - Based on SubSeven trojan, “phone home” via IRC once installed on a machine. Attacker knows how many agents ready to attack.
 - Then, ready to exhaust your bandwidth
 - See Steve Gibson’s paper <http://grc.com>

Teknologi Kriptografi



- Penggunaan enkripsi (kriptografi) untuk meningkatkan keamanan
- Private key vs public key
- Contoh: DES, IDEA, RSA, ECC
- Lebih detail, akan dijelaskan pada bagian terpisah

Modification Attack



- Modify, change information/programs
- Examples: Virus, Trojan, attached with email or web sites
- Protection: anti virus, filter at mail server, integrity checker (eg. tripwire)

Fabrication Attack



- Spoofing address is easy
- Examples:
 - Fake mails: virus sends emails from fake users (often combined with DoS attack)
 - spoofed packets
- Tools: various packet construction kit
- Protection: filter outgoing packets at router

Interruption Attack



- Denial of Service (DoS) attack
 - Menghabiskan bandwidth, network flooding
 - Memungkinkan untuk spoofed originating address
 - Tools: ping broadcast, smurf, synk4, macof, various flood utilities
- Proteksi:
 - Sukar jika kita sudah diserang
 - Filter at router for outgoing packet, filter attack originating from our site

Interception Attack



- Sniffer to capture password and other sensitive information
- Tools: tcpdump, ngrep, linux sniffer, dsniff, trojan (BO, Netbus, Subseven)
- Protection: segmentation, switched hub, promiscuous detection (anti sniff)

Access Control



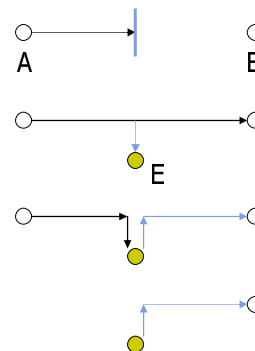
- Mekanisme untuk mengatur siapa boleh melakukan apa
 - biasanya menggunakan password, token
 - adanya kelas / klasifikasi pengguna dan data, misalnya:
 - Publik
 - Private
 - Confidential
 - Top Secret

Jenis Serangan (attack)



- Menurut W. Stallings

- Interruption
DoS attack, network flooding
- Interception
Password sniffing
- Modification
Virus, trojan horse
- Fabrication
spoofed packets



Availability



- Informasi harus dapat tersedia ketika dibutuhkan
 - Serangan terhadap server: dibuat hang, down, crash, lambat
 - Biaya jika server web (*transaction*) down di Indonesia
 - Menghidupkan kembali: Rp 25 juta
 - Kerugian (*tangible*) yang ditimbulkan: Rp 300 juta
- Serangan: Denial of Service (DoS) attack
- Proteksi: backup, redundancy, DRC, BCP, IDS, filtering router, firewall untuk proteksi serangan

Non-repudiation



- Tidak dapat menyangkal (telah melakukan transaksi)
 - menggunakan digital signature / certificates
 - perlu pengaturan masalah hukum (bahwa digital signature sama seperti tanda tangan konvensional)



On the Internet nobody knows you're a dog



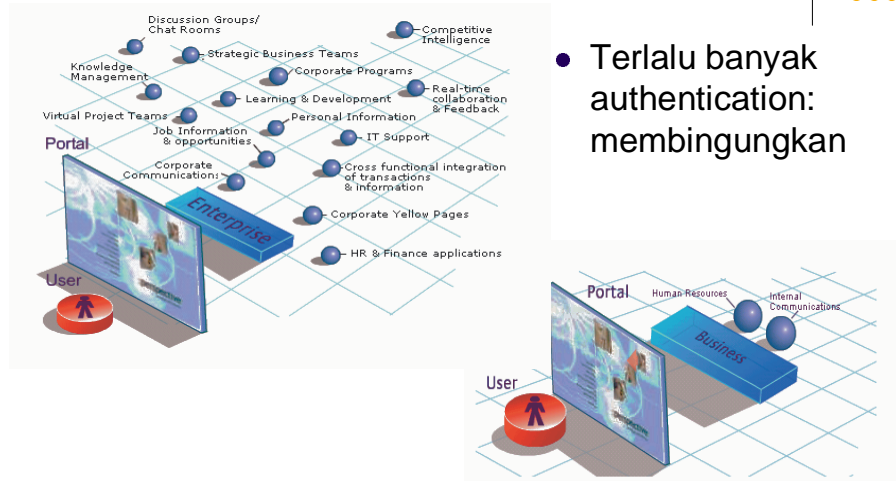
Jan 2005

INTRODUCTION TO SECURITY

9



Authentication Terpadu



- Terlalu banyak authentication: membingungkan

Jan 2005

INTRODUCTION TO SECURITY

10

Integrity



- Informasi tidak berubah tanpa ijin (tampered, altered, modified)
- Serangan:
 - spoof (pemalsuan), virus (mengubah berkas), trojan horse, *man-in-the-middle attack*
- Proteksi:
 - message authentication code (MAC), (digital) signature, (digital) certificate, hash function

Authentication



- Meyakinkan keaslian data, sumber data, orang yang mengakses data, server yang digunakan
 - Bagaimana mengenali nasabah bank pada servis Internet Banking? *Lack of physical contact*
 - Menggunakan:
 1. *what you have (identity card)*
 2. *what you know (password, PIN)*
 3. *what you are (biometric identity)*
 4. *Claimant is at a particular place (and time)*
 5. *Authentication is established by a trusted third party*
- Serangan: identitas palsu, password palsu, terminal palsu, situs web gadungan
- Proteksi: digital certificates

Aspek / Servis Keamanan (Security Control)



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

Privacy / confidentiality



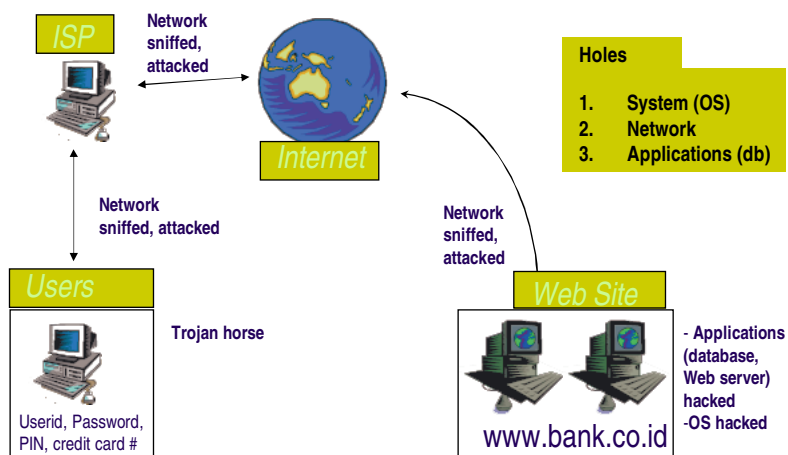
- Proteksi data [hak pribadi] yang sensitif
 - Nama, tempat tanggal lahir, agama, hobby, penyakit yang pernah diderita, status perkawinan, nama anggota keluarga, nama orang tua
 - Data pelanggan. Customer Protection harus diperhatikan
 - Sangat sensitif dalam e-commerce, *healthcare*
- Serangan: sniffer (penyadap), keylogger (penyadap kunci), social engineering, kebijakan yang tidak jelas
- Proteksi: firewall, kriptografi / enkripsi, policy
- Electronic Privacy Information Center <http://www.epic.org>
Electronic Frontier Foundation <http://www EFF.org>

Klasifikasi Berdasarkan Elemen Sistem



- Network security
 - fokus kepada saluran (media) pembawa informasi
- Application security
 - fokus kepada aplikasinya sendiri, termasuk di dalamnya adalah database
- Computer security
 - fokus kepada keamanan dari komputer (end system), termasuk operating system (OS)

Letak potensi lubang keamanan



Prinsip Keamanan

Security Principles



Klasifikasi Keamanan Sisinfo

[menurut David Icove]



Fisik (physical security)

Manusia (people /
personel security)

Data, media, teknik
komunikasi

Kebijakan dan prosedur
(policy and procedures)

Biasanya orang
terfokus kepada
masalah data,
media, teknik
komunikasi.
Padahal kebijakan
(policy) sangat
penting!