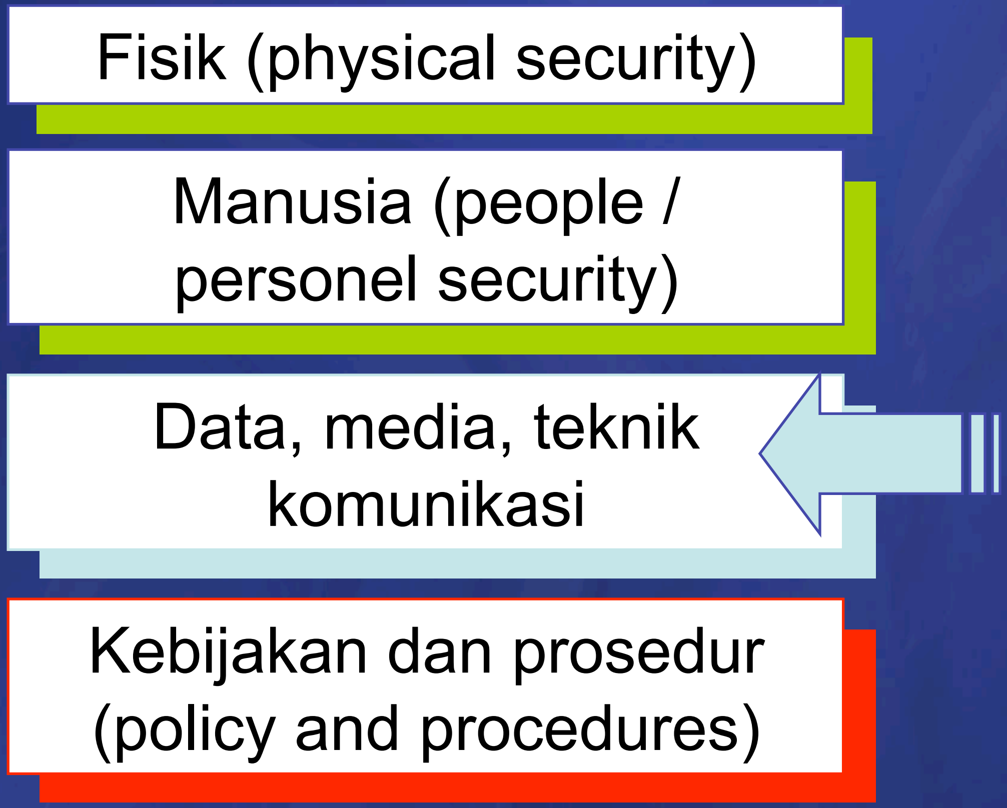
Prinsip Keamanan
-Security Principles-

Klasifikasi Keamanan Sisinfo

[menurut David Icove]



Fisik (physical security)

Manusia (people / personel security)

Data, media, teknik komunikasi

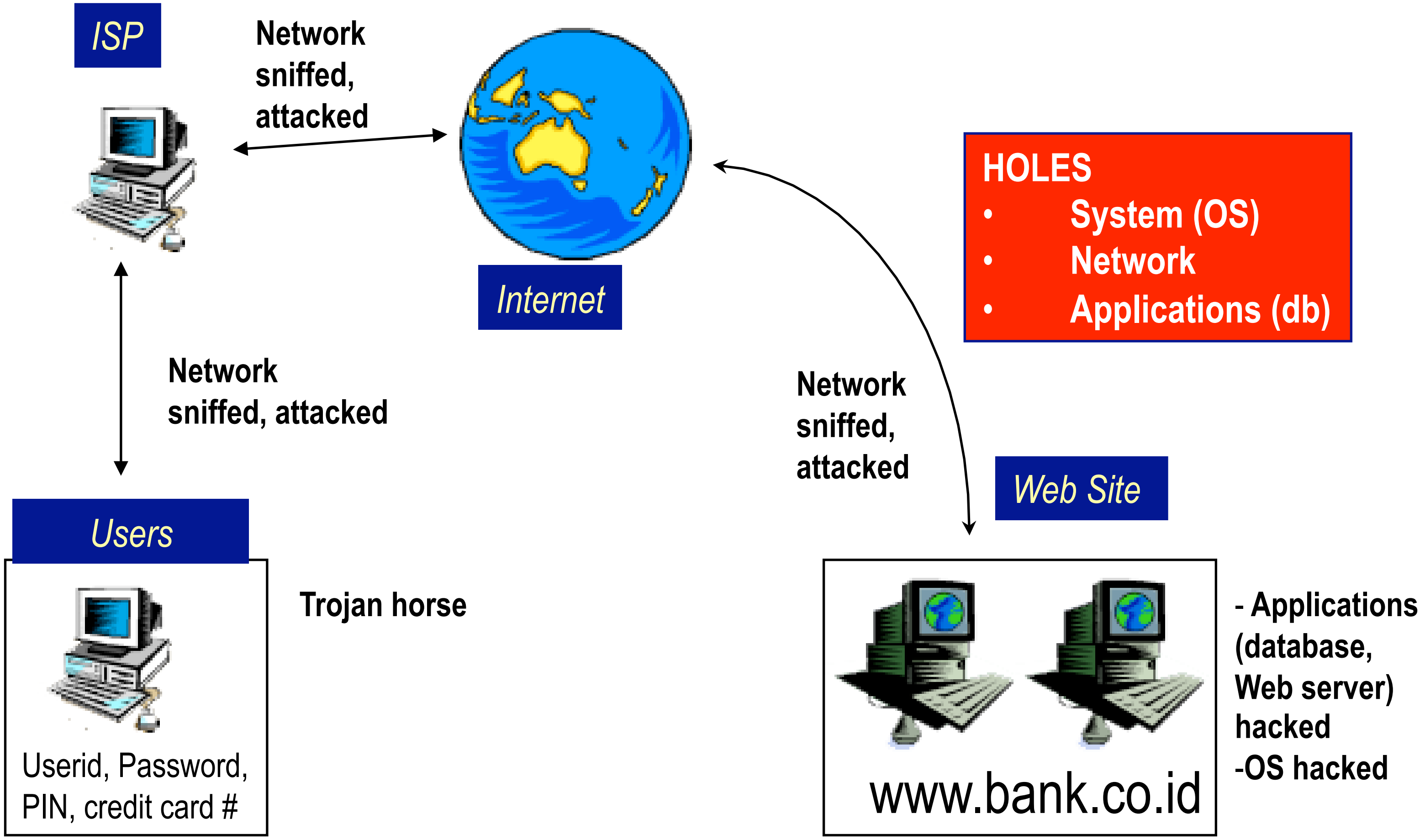
Kebijakan dan prosedur (policy and procedures)

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

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



ISP

Network sniffed, attacked

Internet

HOLES

- System (OS)
- Network
- Applications (db)

Network sniffed, attacked

Network sniffed, attacked

Web Site

Users

Trojan horse

Userid, Password, PIN, credit card #

www.bank.co.id

- Applications (database, Web server) hacked

-OS hacked

Aspek / Servis Keamanan

(Security Control)

- Confidentiality / Privacy
- Integrity
- Availability
- Authentication
- 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 Foundartion http://www.eff.org

Integrity

- Informasi tidak berubah tanpa ijin
  - (*tampered, altered, modified*)

- Serangan:
  - Penerobosan pembatas akses, spoof (pemalsuan), virus (mengubah berkas), trojan horse, *man-in-the-middle attack*

- Proteksi:
  - message authentication code (MAC), (digital) signature, (digital) certificate, hash function

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

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:

  what you have (identity card)

  what you know (password, PIN)

  what you are (biometric identity)

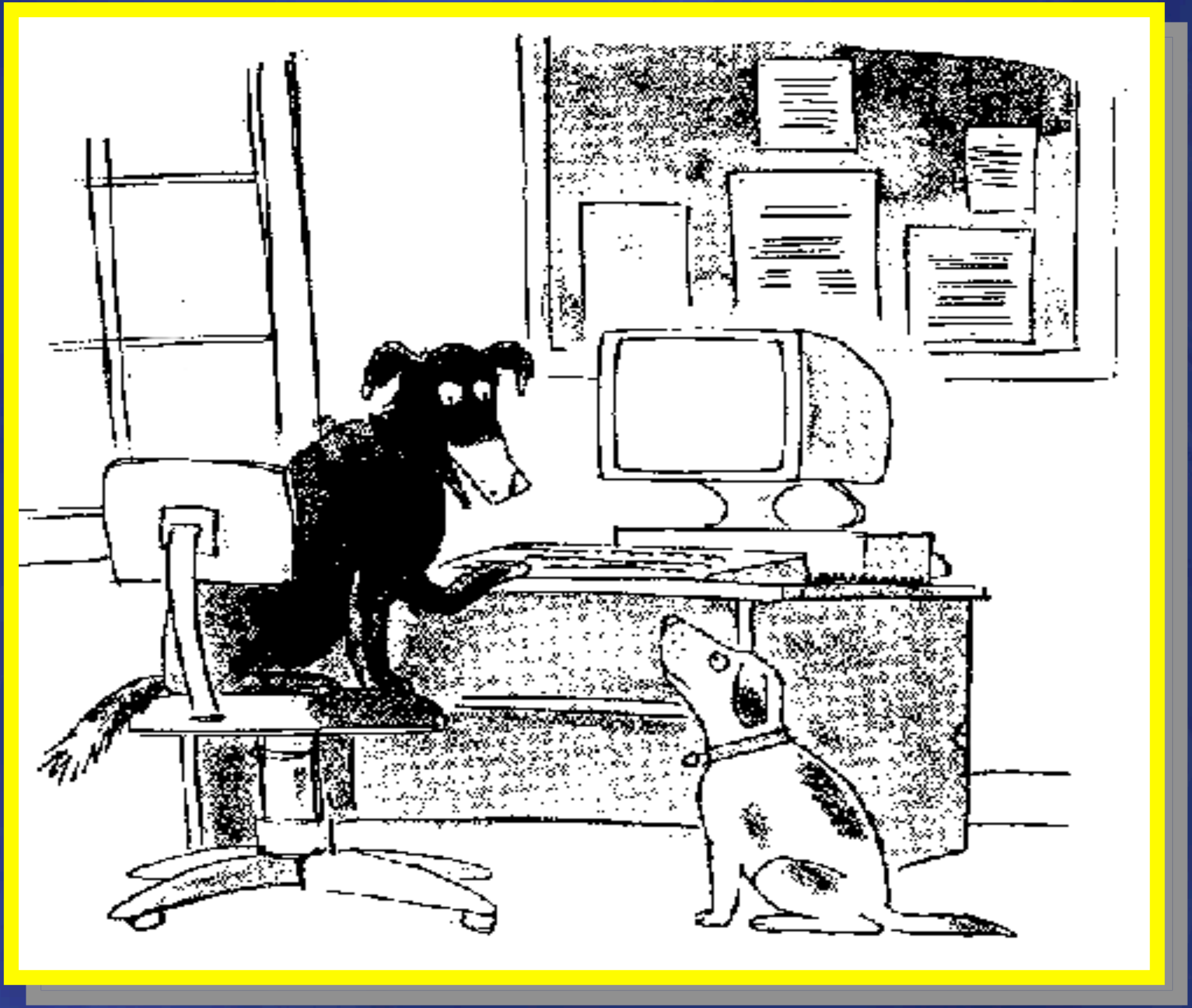
  Claimant is at a particular place (and time)

  Authentication is established by a trusted third party

- Serangan: identitas palsu, password palsu, terminal palsu, situs web gadungan

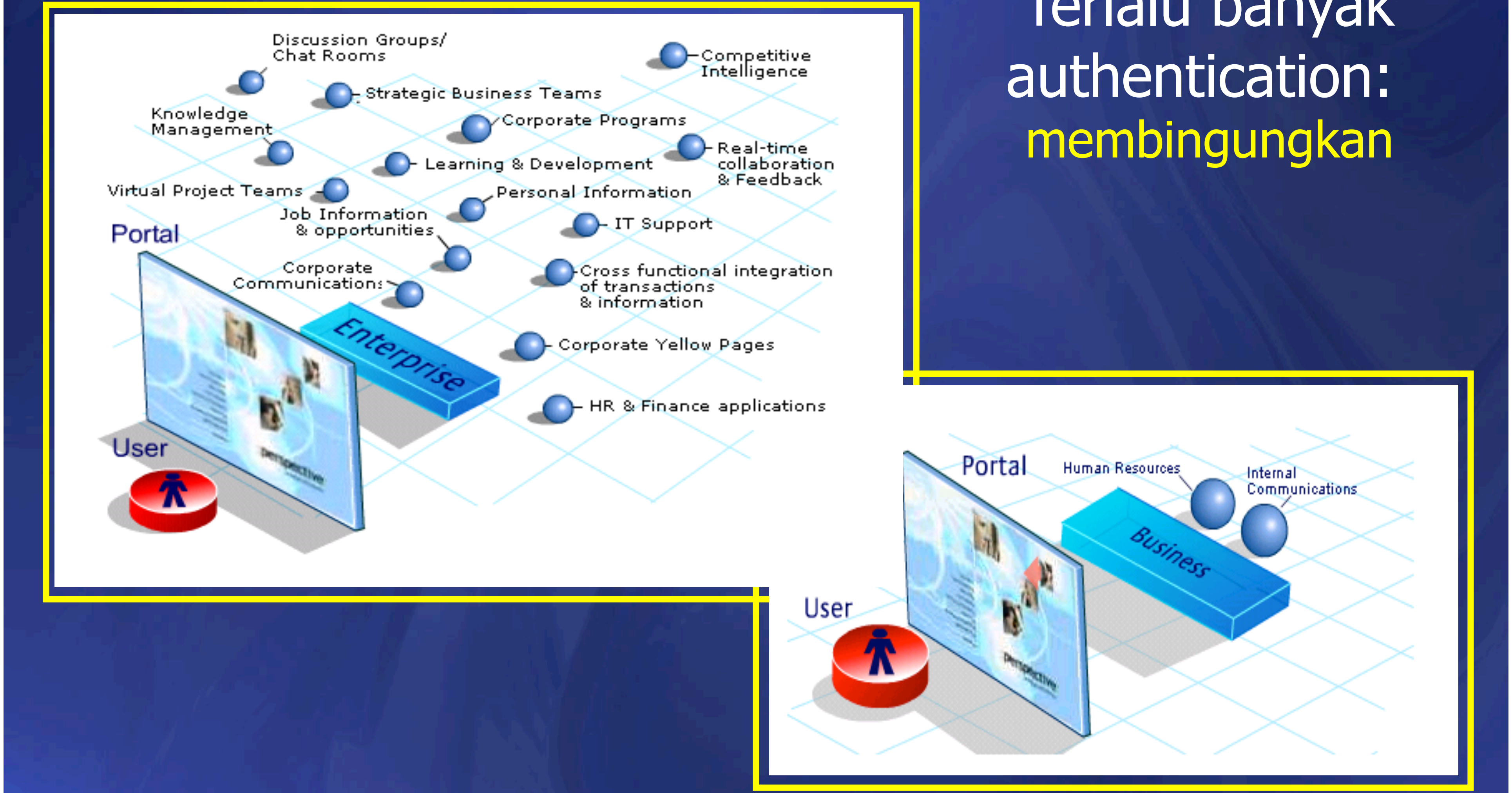
- Proteksi: digital certificates

On the Internet nobody knows you're a dog



Authentication Terpadu

Terlalu banyak authentication: membingungkan



Non-repudiation

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

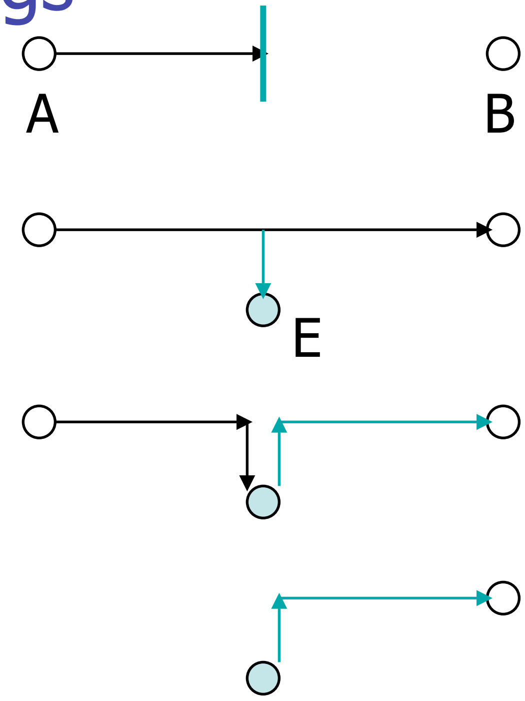
Access Control

- 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**
  spoffed packets



Interruption Attack

- Denial of Service (DoS) attack
  - Menghabiskan bandwith, 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 orginiating 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)

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

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
  - **Tidak semua** dapat diamankan dengan enkripsi!
- Konsep: Private key vs public key
  - Contoh: DES, IDEA, RSA, ECC
- Lebih detail, akan dijelaskan pada bagian terpisah

Security Requirement

- Tidak semua aspek keamanan dibutuhkan
  - Berbeda untuk proses bisnis / aktivitas yang berbeda
  - Berbeda untuk industri yang berbeda
  - Ada prioritas
  - Perlu ditegaskan aspek mana yang harus disediakan

Ancaman (*Security Threats*)

- Perlu diidentifikasi acaman terhadap sistem
  - Darimana saja ancaman tersebut?
    - Dari dalam organisasi (pegawai)?
    - Dari luar organisasi (crackers, kompetitor)?
  - Sumber: oleh manusia (sengaja, tidak sengaja) atau alam (bencana, musibah)?
  - Tingkat kesulitan
  - Probabilitas ancaman menjadi kenyataan

Mempelajari crackers

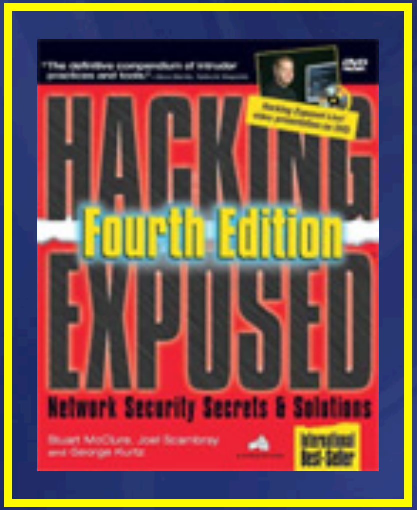
- Mempelajari:
  - Perilaku perusak
  - Siapakah mereka?
  - Apa motifnya?
  - Bagaimana cara masuk?
  - Apa yang dilakukan setelah masuk?
- Tools:
  - honeypot, honeynet

Know Your Enemy

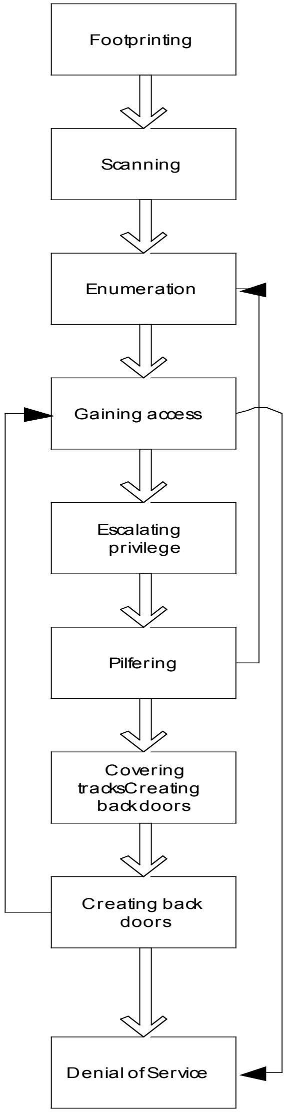
Crackers SOP / Methodology

Dari “Hacking Exposed”:

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

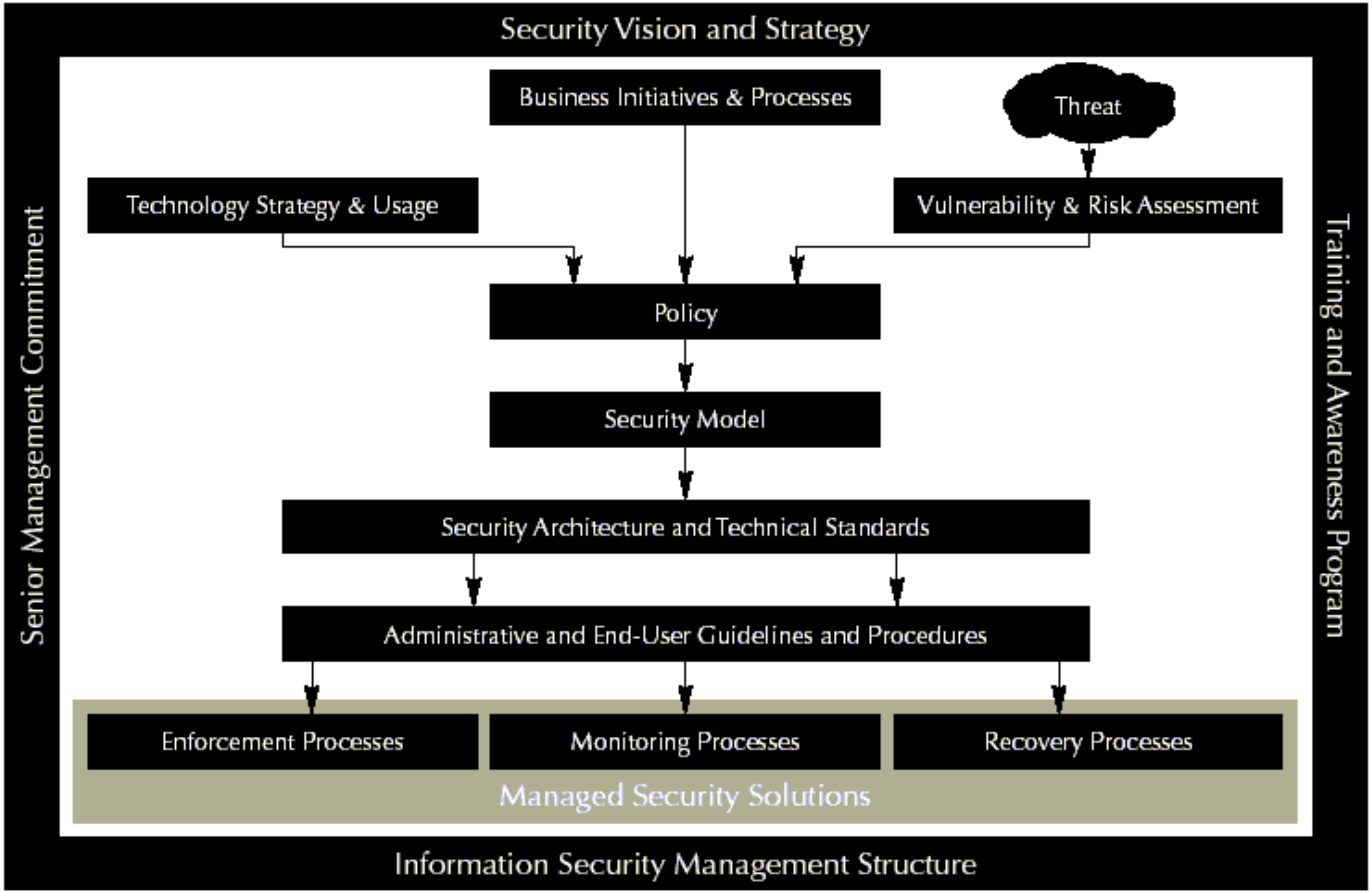

HACKING
Fourth Edition
EXPOSED
Network Security Secrets & Solutions
Stuart McClure, Joel Scambray and George Kurtz
International Best-Seller

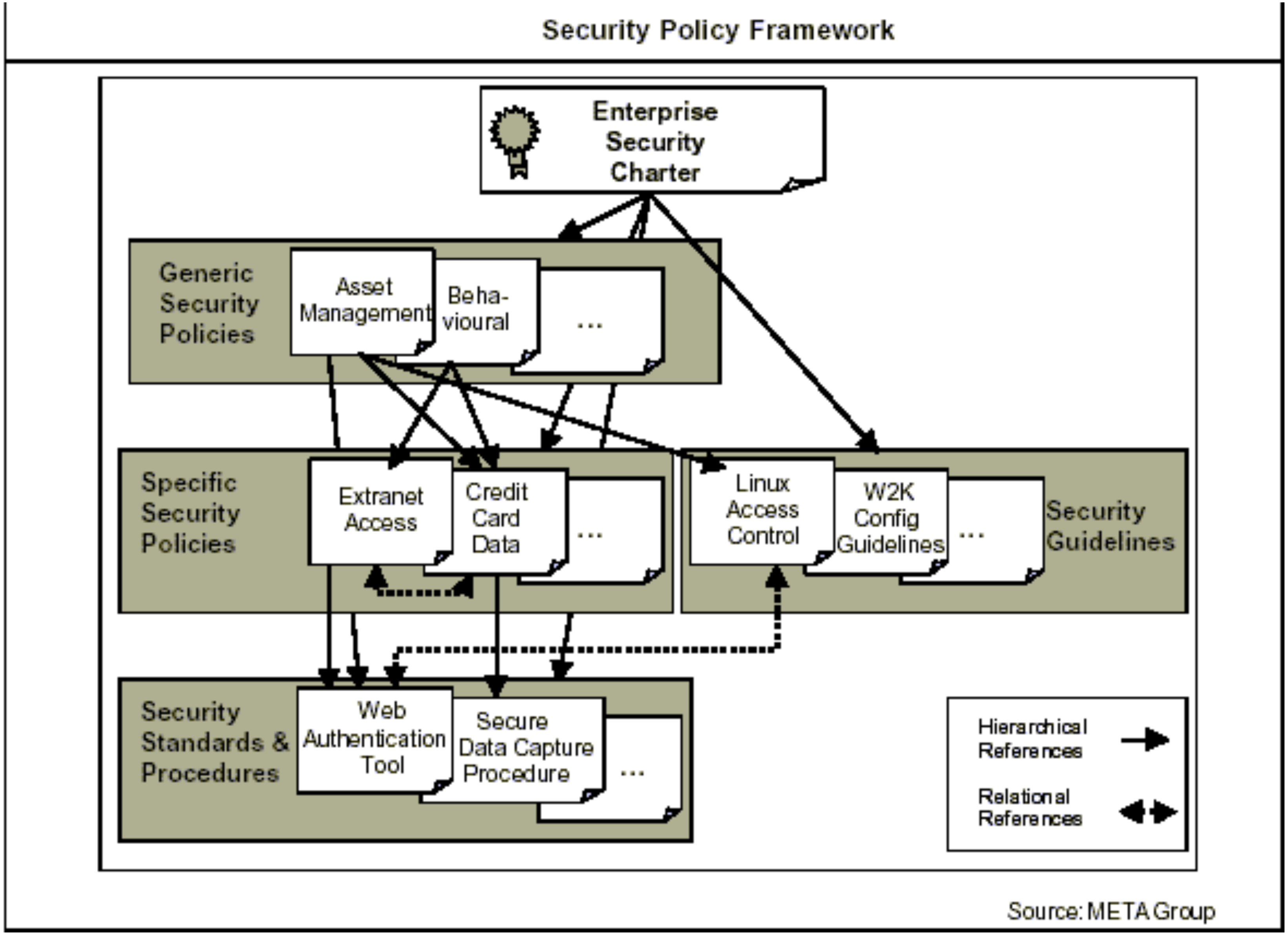
ANATOMY OF A HACK



The Objective	The Methodology	The Techniques	The Tools
Target address range, name space acquisition, and information gathering are essential to a surgical attack. The key here is not to miss any details.	Footprinting	Open source search whois Web interce to whois ARIN whois DNS zone transfer	USENet, search engines, Edgar Any UNIX client http :// www.networksolutions.com/whois http :// www.arin.net/whois dig, nslookup ls -d, Sam Spade
Bulk target assessment and identification of listening services focuses the attacker's attention on the most promising avenues of entry	Scanning	Ping sweep TCP/UDP port OS Detection	fping, icmpenum WS _Ping ProPack nmap, SuperScan, fscan Nmap, queso, siphon
More intrusive probing now begins as attackers begin identifying valid user accounts or poorly protected resource shares.	Enumeration	List user accounts List file shares Identify applications	null sessions, DumpACL, sid 2user, OnSite Admin showmount, NAT, Legion banner grabbing with telnet or netcat, rpcinfo
Enough data has been gathered at this point to make an informed attempt to access the target	Gaining access	Password eavesdropping File share brute forcing Password file grab Buffer overflows	tcpdump, L0phtcrack readsmb NAT, legion tftp, pwdump2 (NT) ttdb, bind, IIS .HTR/ISM .DLL
If only user-level access was obtained in the last step, the attacker will now seek to gain complete control of the system	Escalating privilege	Password cracking Known exploits	john, L0phtcrack lc_messages, getadmin, sechole
The information-gathering process begins again to identify mechanisms to gain access to trusted systems.	Pilfering	Evaluate trusts Search for cleartext passwords	rhosts, LSA Secrets user data, configuration files, Registry
Once total ownership of the target is sesured, hiding this fact from system administrators becomes paramount, lest they quickly end the romp.	Covering tracksCreating backdoors	Clear logs Hide tools	zap EventLog GUI, rootkits, file streaming
Trap doors will be laid in various parts of the system to ensure that priveleged access is easily regained at the whim of the intruder	Creating back doors	Create rouge user accounts Schedule batch jobs Infect startup files Plant remotecontrol services Install monitoring mechanisms Replace apps with Trojans	members of wheel, Administrators cron, AT rc, Startup folder, Registry keys netcat, remote.exe, VNC, BO2K keystroke loggers, add acct. to secadmin mail aliases login, fpnwclnt.dll
If an attacker is unsuccessful in gaining access, they may use readily available exploit code to disable a target as a last resort.	Denial of Service	SYN flood ICMP techniques Identical src /dst SYN requests Overlapping fragment /offset bugs Out of bounds TCP options (OOB) DDoS	synk 4 ping of death, smurf land, latierra teardrop, bonk, newtear supernuke.exe trinoo/TFN/stcheldraht

IT SECURITY FRAMEWORK


Security Vision and Strategy
Business Initiatives & Processes
Threat
Technology Strategy & Usage
Vulnerability & Risk Assessment
Policy
Security Model
Security Architecture and Technical Standards
Administrative and End-User Guidelines and Procedures
Enforcement Processes
Monitoring Processes
Recovery Processes
Managed Security Solutions
Information Security Management Structure
Senior Management Commitment
Training and Awareness Program



Source: META Group

Pengamanan Menyeluruh

- Harus menyeluruh - holistic approach

PEOPLE

- awareness, skill
- ...

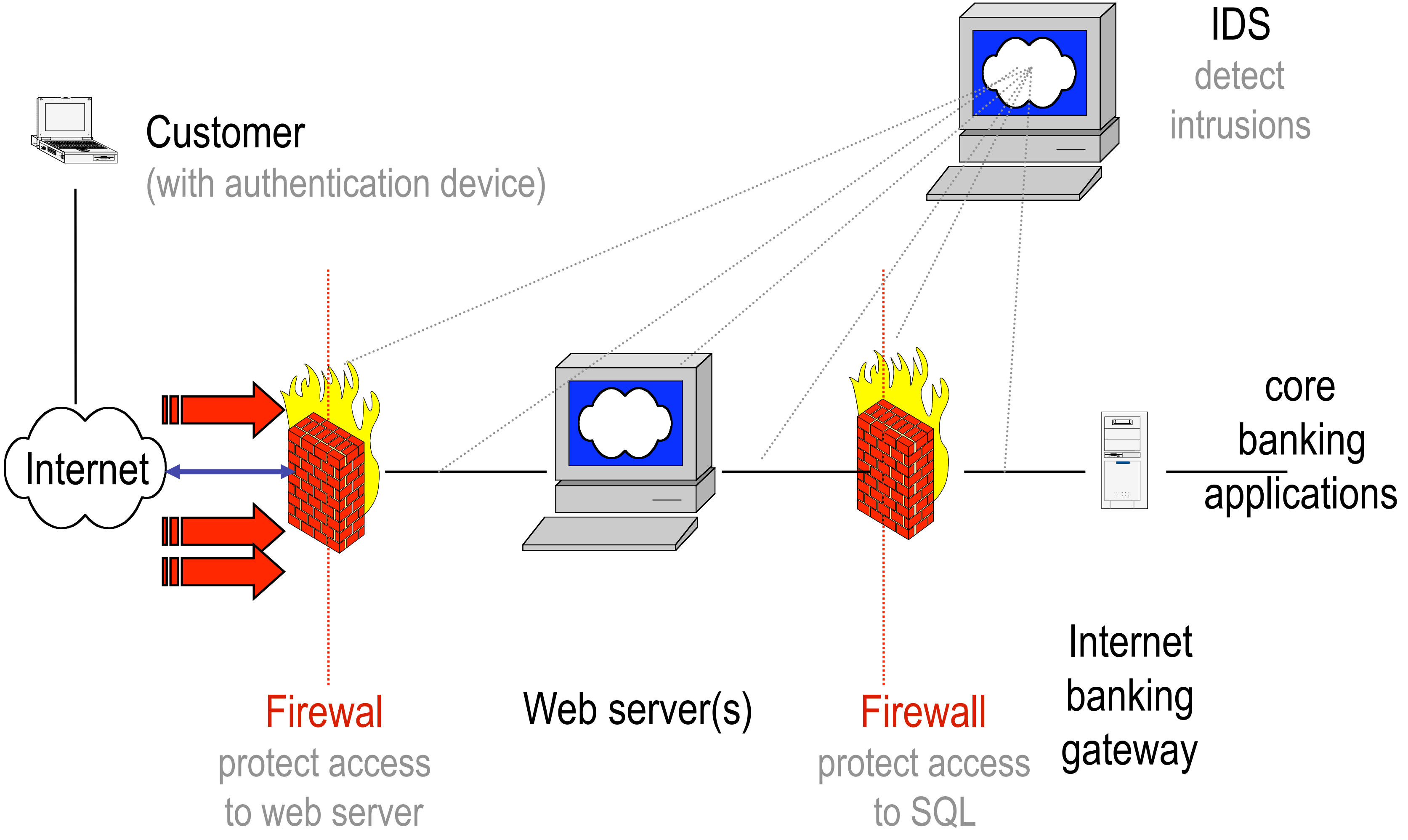
PROCESS

- security as part of business process
- ...

TECHNOLOGY

- implementation
- ...

Pengamanan Berlapis



Customer

(with authentication device)

IDS

detect intrusions

Internet

Firewal

protect access to web server

Web server(s)

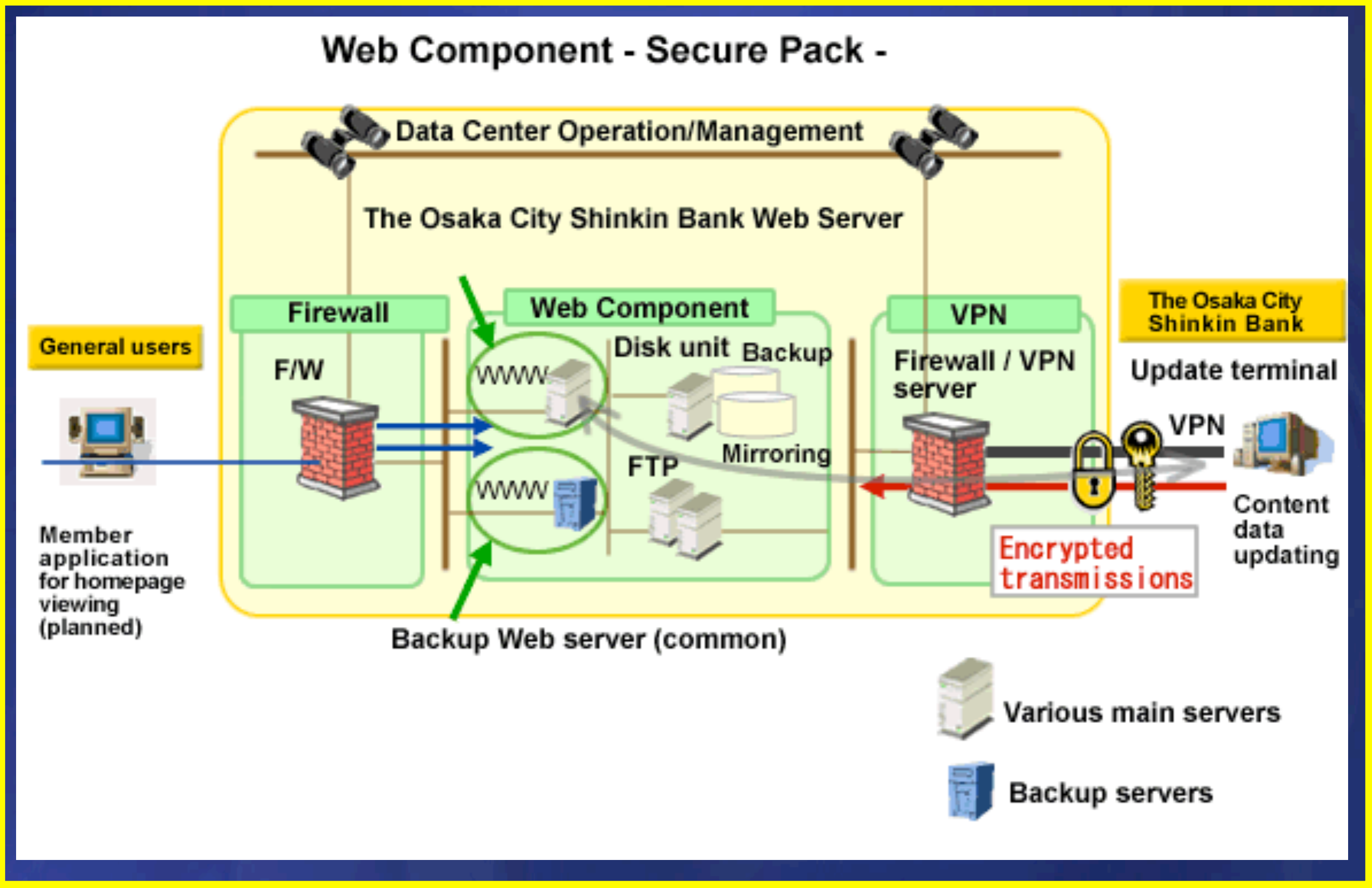
Firewall

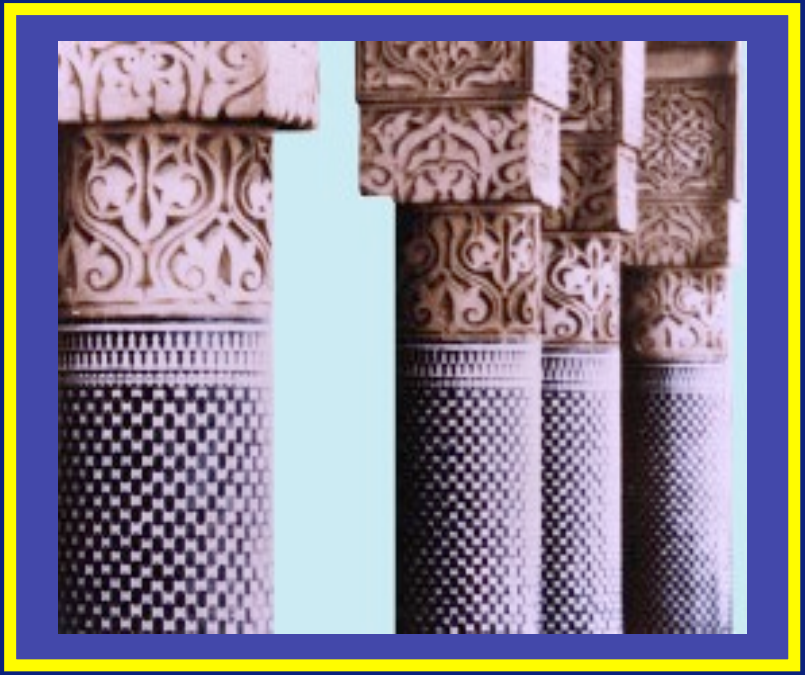
protect access to SQL

Internet banking gateway

core banking applications

Contoh Implementasi:
Osaka Bank


Web Component - Secure Pack -
Data Center Operation/Management
The Osaka City Shinkin Bank Web Server
General users
Firewall
F/W
Web Component
WWW
Disk unit
Backup
Mirroring
FTP
WWW
VPN
Firewall / VPN server
The Osaka City Shinkin Bank
Update terminal
VPN
Content data updating
Encrypted transmissions
Member application for homepage viewing (planned)
Backup Web server (common)
Various main servers
Backup servers



Terima Kasih