Pengantar Keamanan Sistem Informasi

Mohammad Iqbal

Materi

1. Mengapa keamanan sistem penting ?
2. Statistik Gangguan Keamanan Sistem Informasi
3. Aspek Keamanan SI
4. Beberapa Jenis Serangan/Ancaman terhadap keamanan sistem informasi
5. Memahami Lingkup Menjaga Keamanan SI
6. Standar Kualitas Keamanan SI
7. Kualifikasi Profesional Keamanan SI

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) $\rightarrow$ 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

Statistik Gangguan Keamanan SI

Trends Gangguan 2010

- Malware, worms, and Trojan horses
  - spread by email, instant messaging, malicious or infected websites
- Botnets and zombies
  - improving their encryption capabilities, more difficult to detect
- Scareware – fake/rogue security software
- Attacks on client-side software
  - browsers, media players, PDF readers, mobile software, etc.
- Ransom attacks
  - malware encrypts hard drives, or DDOS attack
- Social network attacks
  - Users' trust in online friends makes these networks a prime target.
- Cloud Computing - growing use will make this a prime target for attack.
- Web Applications - developed with inadequate security controls
- Budget cuts - problem for security personnel and a boon to cyber criminals.

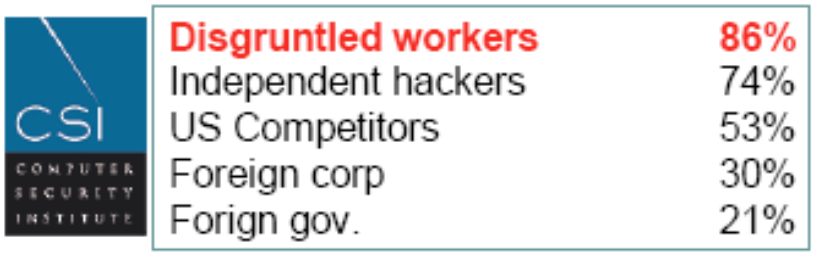
Same list in Oklahoma Monthly Security Tips Newsletter


STEALTH
TERRORISM
DESIGNER
MALWARE
TARGETED
ATTACKS
SPAM
@
SPEAR
PHISHING
@
RANSOMWARE
STEALTH
BLENDED
BOT
SPY
ROOT KIT
SQL INJECTION
TROJAN
STEALTH
TROJAN
ORM
IBM Internet Security Systems
www.iss.net/evolvingthreat

Statistik Gangguan Keamanan SI

Angka pasti, sulit ditampilkan karena kendala bisnis. Negative publicity

- **1996.** **FBI National Computer Crime Squad**, kejahatan komputer yang terdeteksi kurang dari 15%, dan hanya 10% dari angka itu yang dilaporkan.
- **1996.** Di Inggris, **NCC Information Security Breaches Survey**: kejahatan komputer naik 200% dari 1995 ke 1996.
- **1997.** **FBI**: kasus persidangan yang berhubungan dengan kejahatan komputer naik 950% dari tahun 1996 ke 1997, dan yang masuk di pengadilan naik 88%.
- Jumlah kelemahan (vulnerabilities) sistem informasi yang dilaporkan ke **Bugtraq** meningkat empat kali (quadruple) semenjak tahun 1998 sd tahun 2000. Dari 20 laporan perbulan menjadi 80 laporan perbulan.
- **1999.** **Computer Security Institute (CSI) / FBI Computer Crime Survey** menunjukkan beberapa statistik yang menarik, seperti misalnya ditunjukkan bahwa "disgruntled worker" (orang dalam) merupakan potensi attack / abuse. (**http://www.gocsi.com)**



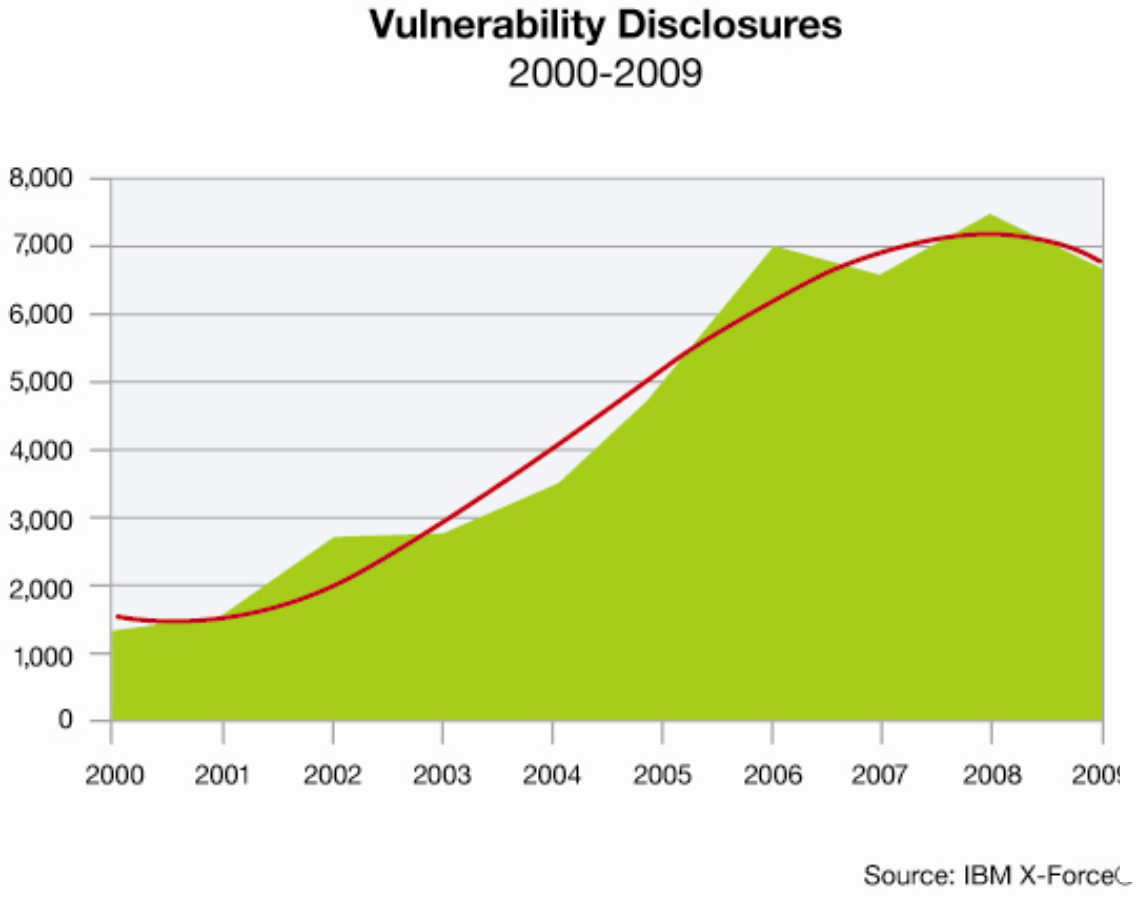
Statistik Gangguan Keamanan SI

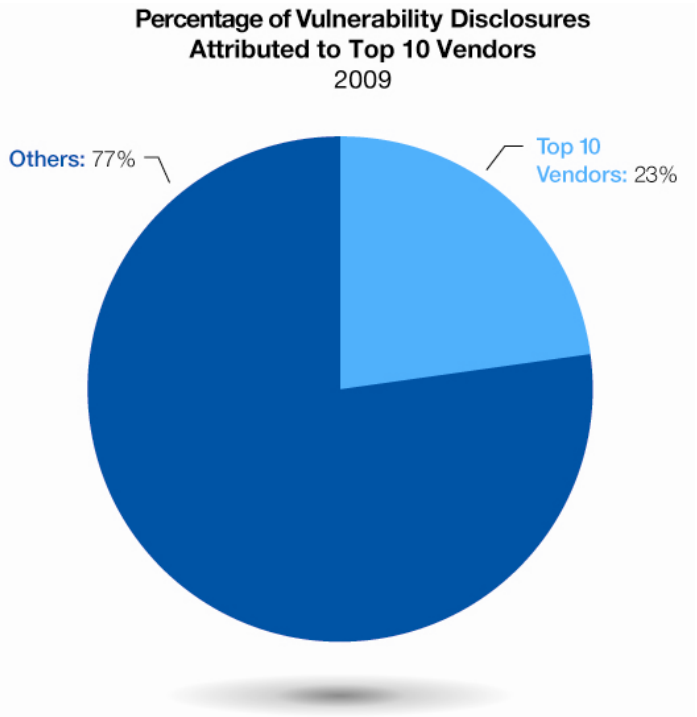
Angka pasti, sulit ditampilkan karena kendala bisnis. Negative publicity

- **7 Februari 2000 s/d 9 Februari 2000**. Distributed Denial of Service (Ddos) attack terhadap Yahoo, eBay, CNN, Amazon, ZDNet, E-Trade.
- **2001.** Virus SirCam mengirimkan file dari harddisk korban. File rahasia bisa tersebar. Worm Code Red menyerang sistem IIS kemudian melakukan port scanning dan menyusup ke sistem IIS yang ditemukannya.
- **2004.** Kejahatan “phising” (menipu orang melalui email yang seolah-olah datang dari perusahaan resmi [bank misalnya] untuk mendapatkan data-data pribadi seperti nomor PIN internet banking) mulai marak - 2004),
- **2004** kejahatan kartu kredit, Indonesia :
  - Nomor #1 dalam persentase (yaitu perbandingan antara transaksi yang baik dan palsu)
  - Nomor #3 dalam volume.
- Akibatnya kartu kredit dan transaksi yang (nomor IP-nya) berasal dari Indonesia secara resmi diblokir di beberapa tempat di Amerika

Statistik Gangguan Keamanan SI

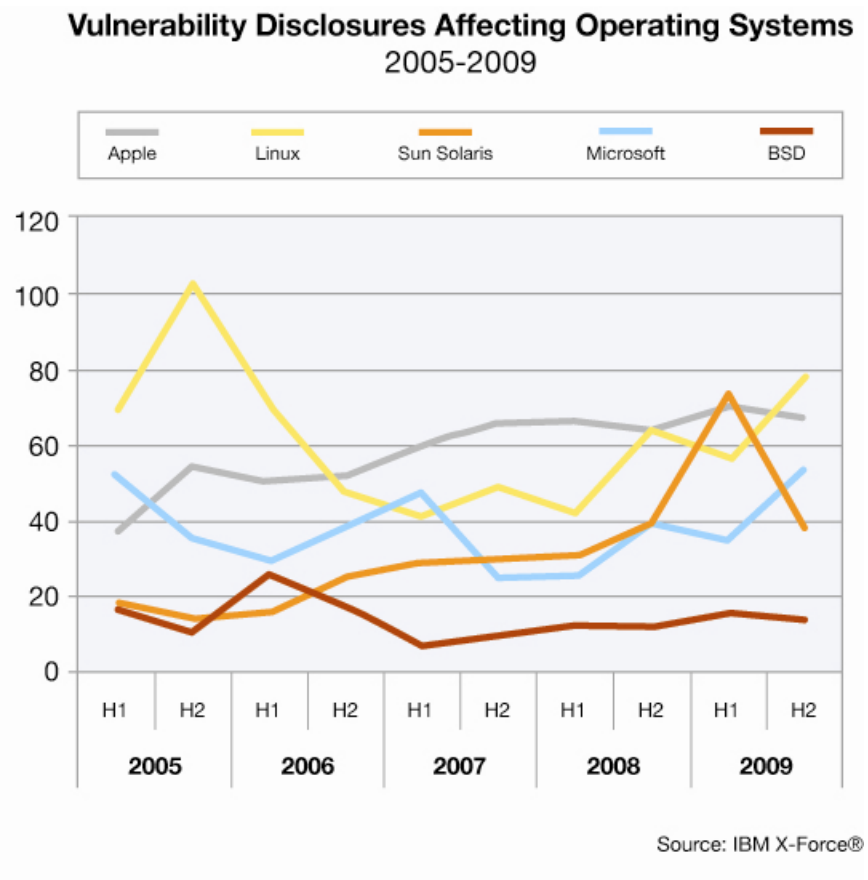
Vulnarabilitas 2000-2009

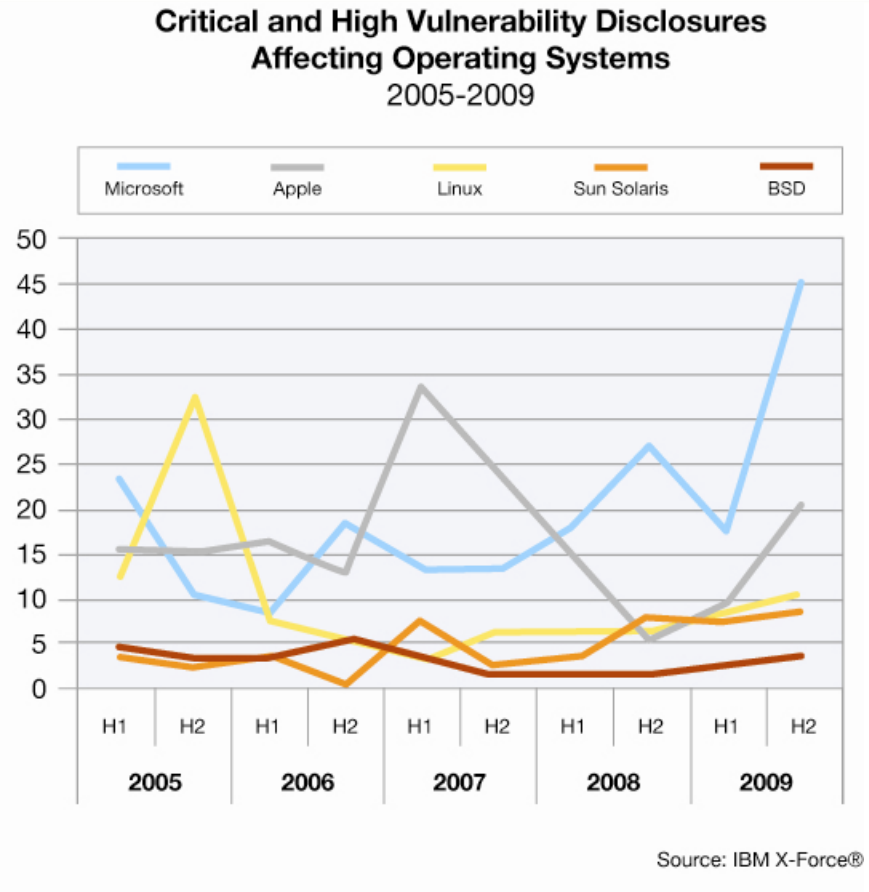




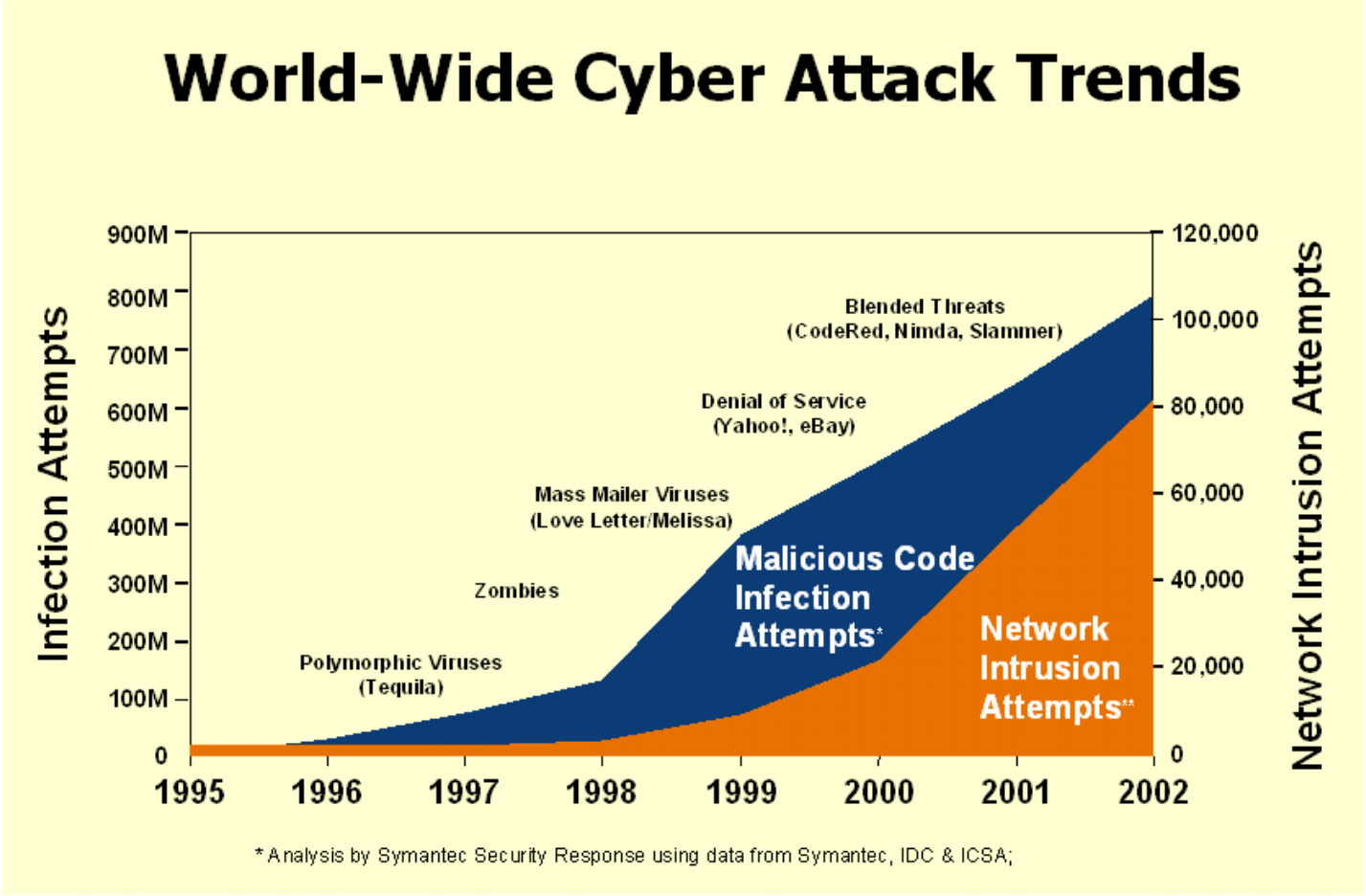
Statistik Gangguan Keamanan SI

Operating system vulnerabilities





Statistik Gangguan Keamanan SI



Statistik Gangguan Keamanan SI

Urutan Negara yang paling banyak mengalami Online fraud

Nir Kshetri, “The Simple Economics of Cybercrimes,” IEEE Security & Privacy, January/February 2006

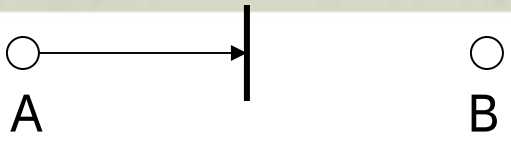
Ukraine
Indonesia
Yugoslavia
Lithuania
Egypt
Romania
Bulgaria
Turkey
Russia
Pakistan
Malaysia
Israel

Aspek-aspek keamanan SI

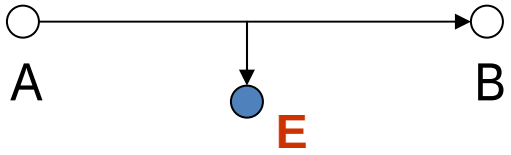
- **Confidentiality**
  Informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang.
- **Integrity**
  Informasi hanya dapat diubah oleh pihak yang memiliki wewenang.
- **Availability**
  Informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan.
- **Authentication**
  Pihak yang terlibat dengan pertukaran informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.
- **Nonrepudiation**
  Pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

Aspek-aspek ketidakamanan (serangan)

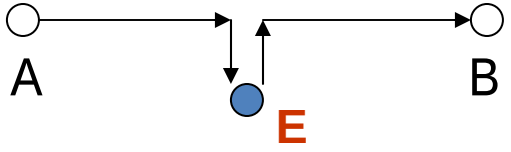
1. **Interruption**
   Suatu aset dari suatu sistem diserang sehingga menjadi tidak tersedia atau tidak dapat dipakai oleh yang berwenang. Contohnya adalah perusakan/modifikasi terhadap piranti keras atau saluran jaringan.



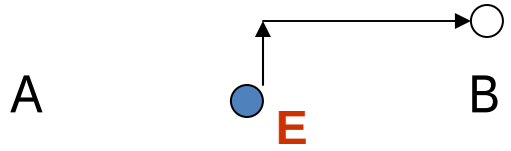
2. **Interception**
   Suatu pihak yang tidak berwenang mendapatkan akses pada suatu aset. Pihak yang dimaksud bisa berupa orang, program, atau sistem yang lain. Contohnya adalah penyadapan terhadap data dalam suatu jaringan.



3. **Modification**
   Suatu pihak yang tidak berwenang dapat melakukan perubahan terhadap suatu aset. Contohnya adalah perubahan nilai pada file data, modifikasi program sehingga berjalan dengan tidak semestinya, dan modifikasi pesan yang sedang ditransmisikan dalam jaringan.

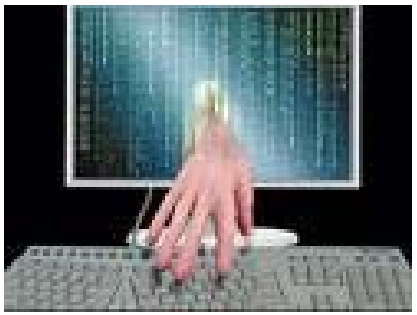


4. **Fabrication**
   Suatu pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem.
   Contohnya adalah pengiriman pesan palsu kepada orang lain.



Beberapa Jenis Serangan/Ancaman

- 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 Jenis Serangan/Ancaman

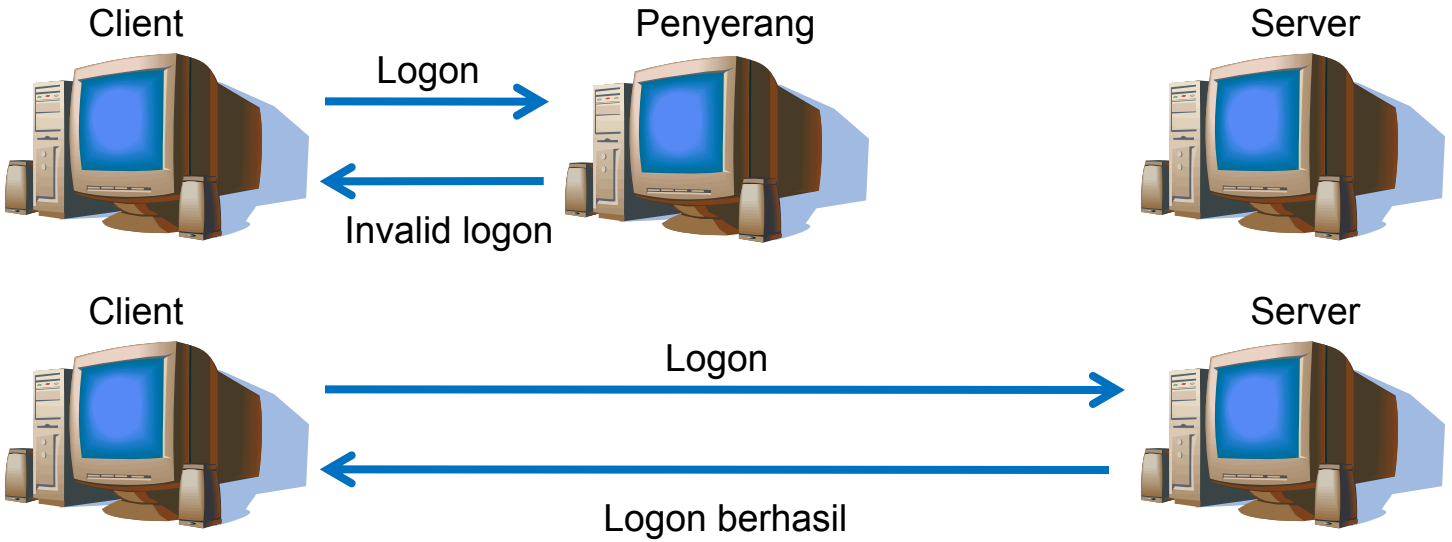
Access Attacks

- 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 Jenis Serangan/Ancaman

Access Attacks

- 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)

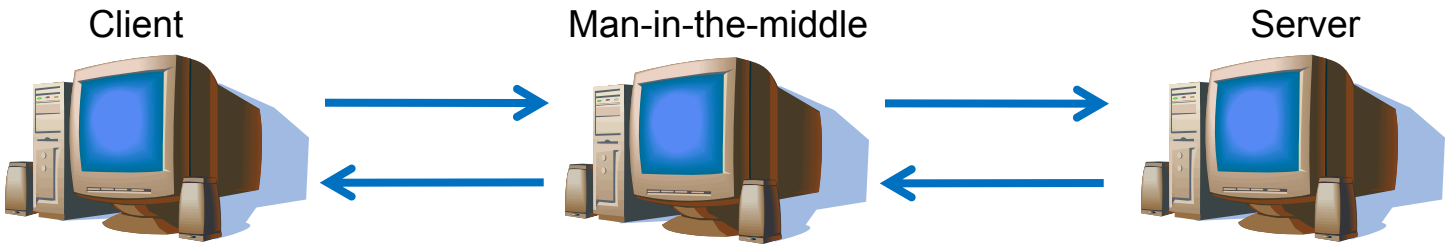


Pada saat ini, penyerang sudah mendapatkan username & password yang sah untuk bisa masuk ke server

Beberapa Jenis Serangan/Ancaman

Access Attacks

- 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 Jenis Serangan/Ancaman

Access Attacks

- 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)

Beberapa Jenis Serangan/Ancaman

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

Beberapa Jenis Serangan/Ancaman

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)

Beberapa Jenis Serangan/Ancaman

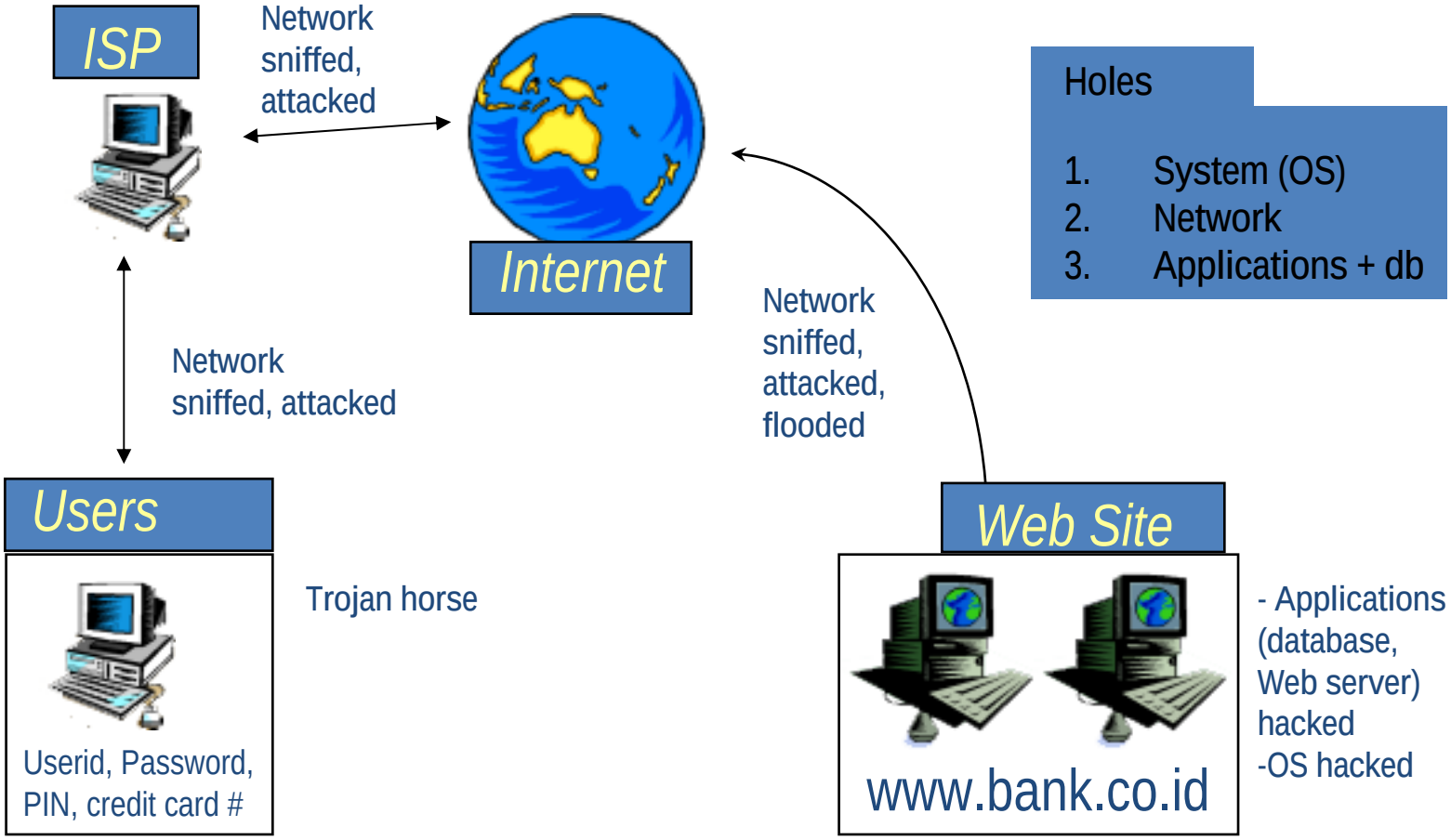
Denial of Service Attacks

- 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)

ANATOMY OF A HACK

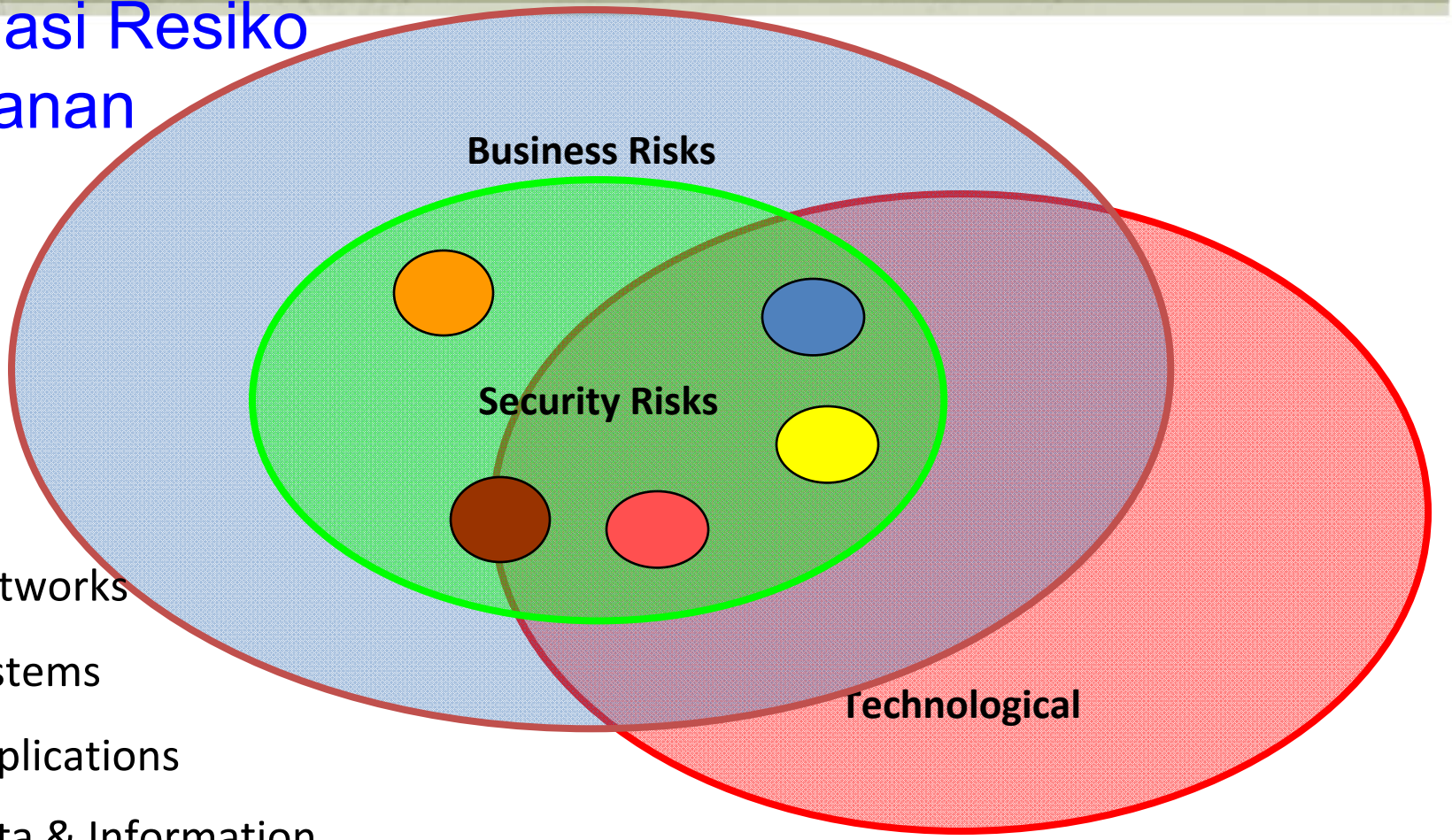
The Objective	The Methodology	The Techniques	The Tools
Target address range, name space acquisition, and information gathering are essential to a surgical attack. The key here is not to miss any details.	Footprinting	Open source search whois Web interce to whois ARIN whois DNS zone transfer	USENet, search 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, sid2user, 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 proccess 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 back doors	Clear logs Hide tools	zap Event Log 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	synk4 ping of death, smurf land, latierra teardrop, bonk, newtear supernuke.exe trinoo/TFN/stcheldraht

Tipologi Lubang Keamanan SI



Memahami Lingkup Menjaga Keamanan SI

1. Situasi Resiko Keamanan



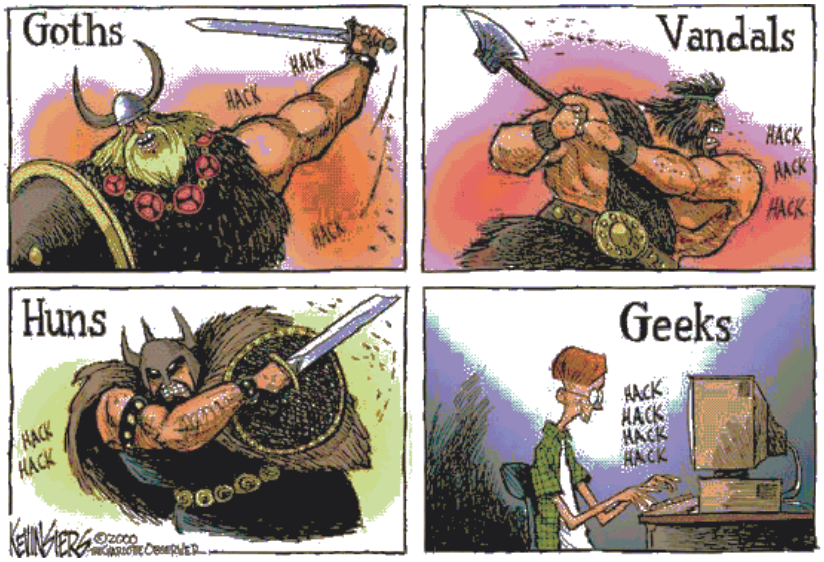
- Networks
- Systems
- Applications
- Data & Information
- People

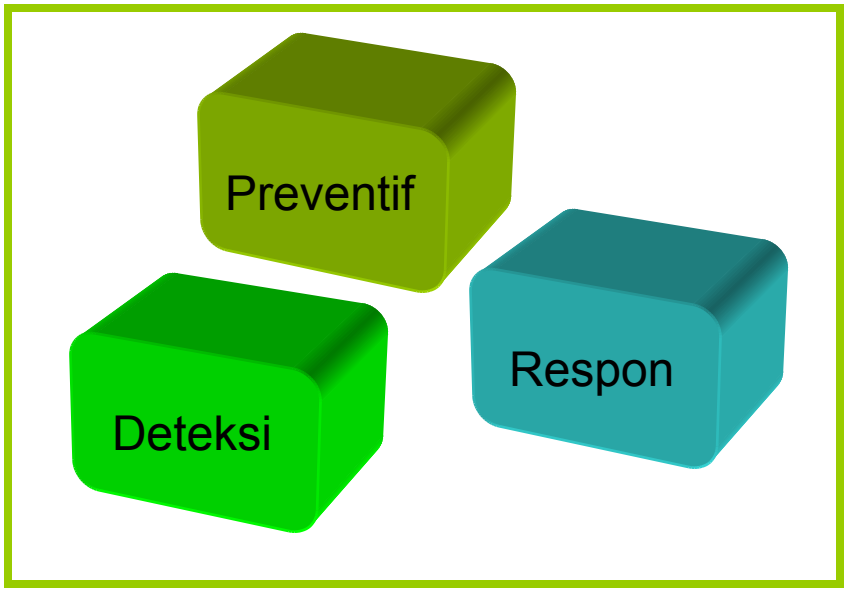
Security ≠ Technological Security
Keamanan itu Socio-technical & Physical!

Memahami Lingkup Menjaga Keamanan SI

2. Perspektif Keamanan

Strategi Keamanan = Preventif + Deteksi + Respon





Memahami Lingkup Menjaga Keamanan SI

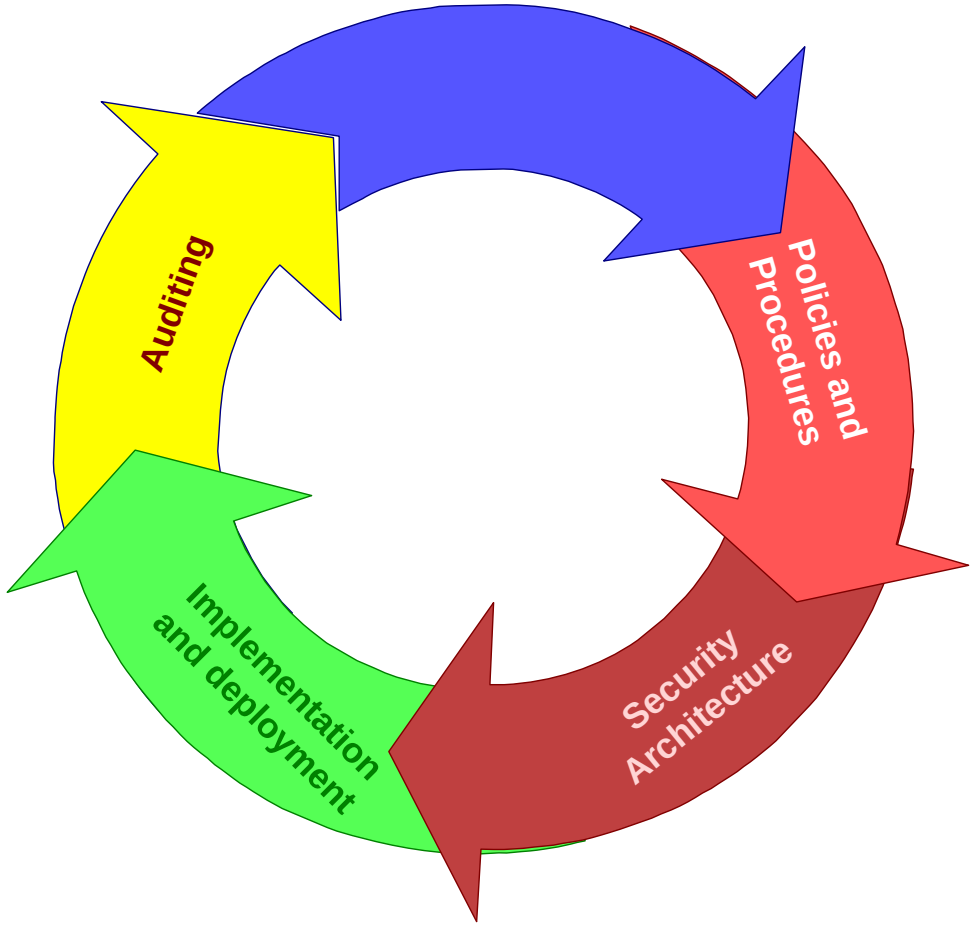
- Preventif
  - Melindungi komputer atau informasi dari pengganggu dan kesalahan.
  - Idealnya prosedur & kebijakan keamanan dapat menutup kesempatan untuk diserang, tapi paling tidak meminimalisasi serangan yang berhasil
- Deteksi
  - Dapat mengukur kapan, bagaimana dan oleh siapa aset dapat dirusak
  - Membutuhkan alat bantu yang rumit atau sekedar file log sederhana yang dapat dianalisa.
- Respon
  - Membangun strategi dan teknik untuk menghadapi serangan atau kehilangan
  - Lebih baik memiliki rencana pemulihan (recovery plan) daripada 'on the fly' atau bagaimana nanti

Memahami Lingkup Menjaga Keamanan SI

- Example: Private Property
  - Prevention: locks at doors, window bars, walls round the property
  - Detection: stolen items are missing, burglar alarms, closed circuit TV
  - Reaction: call the police, replace stolen items, make an insurance claim …
- Example: E-Commerce
  - Prevention: encrypt your orders, rely on the merchant to perform checks on the caller, don't use the Internet (?) …

Memahami Lingkup Menjaga Keamanan SI

3. Keamanan adalah Suatu Proses

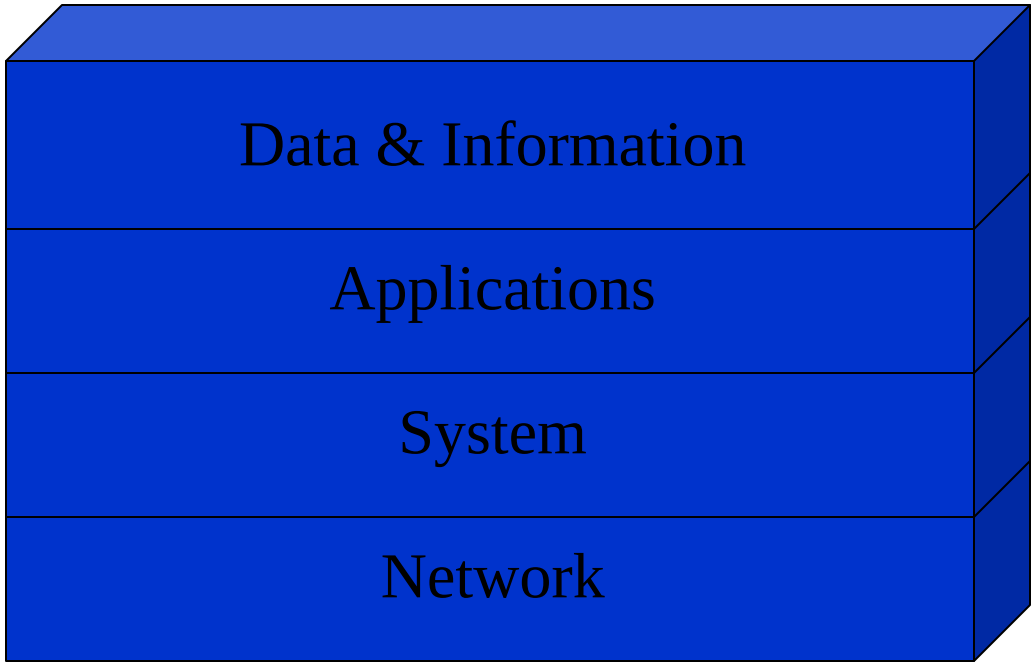


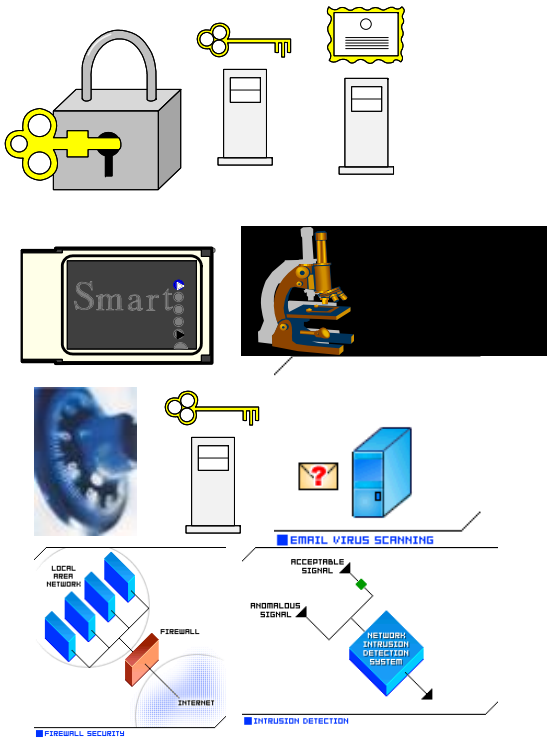
Asses and Risk

Memahami Lingkup Menjaga Keamanan SI

4. Keamanan sistem sebagai satu konsep terpadu

Layer Fisik Keamanan Sistem informasi

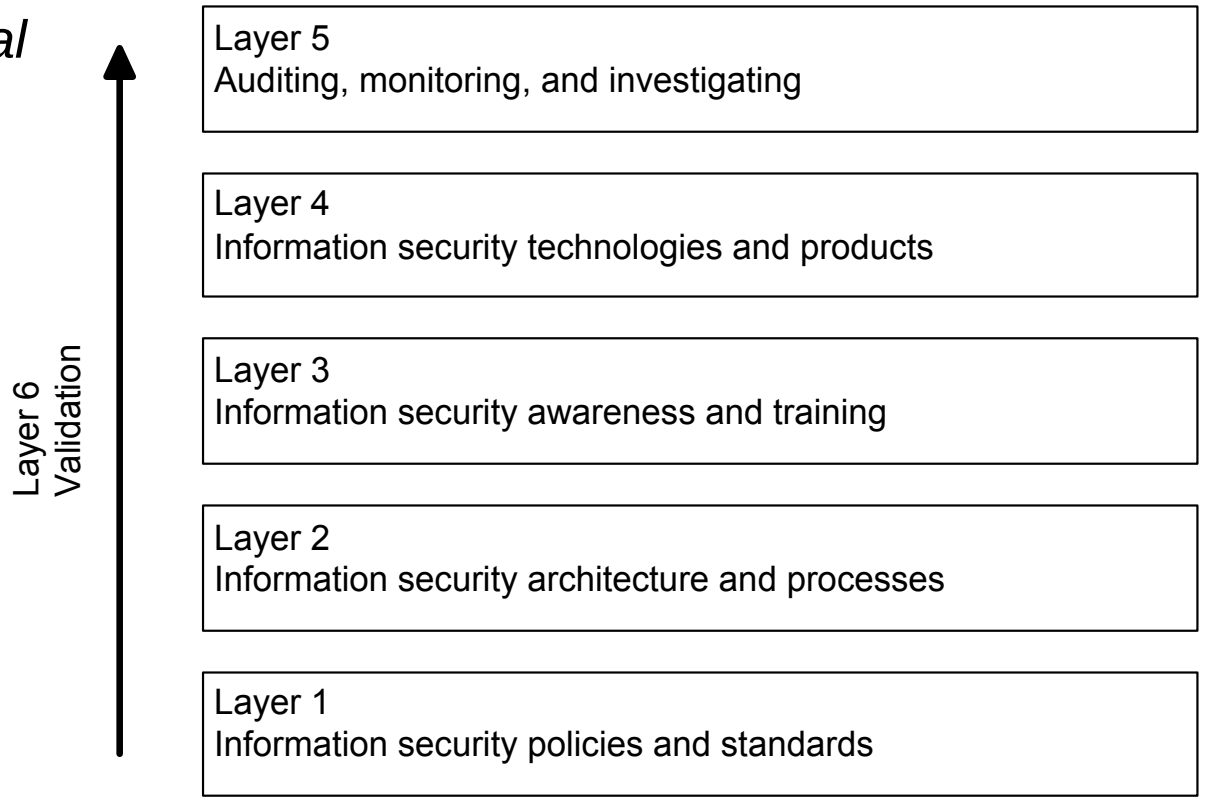




Memahami Lingkup Menjaga Keamanan SI

4. Keamanan sistem sebagai satu konsep terpadu

Layer Operasional Keamanan Sistem informasi

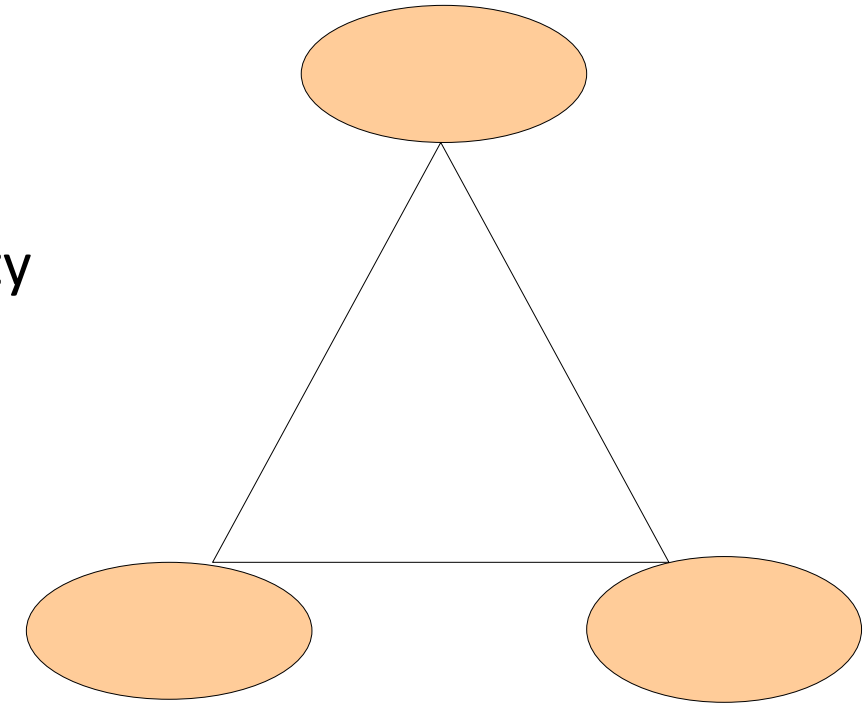


Memahami Lingkup Menjaga Keamanan SI

5. Fokus Utama Keamanan SI

- Tiga Fokus Utama
  a) Physical Security
  b) Operational Security
  c) Management and Policies

- Segitiga Kemanan →



Memahami Lingkup Menjaga Keamanan SI

a) Keamanan Fisik

- Perlindungan aset dan informasi dari akses fisik oleh personal yang tidak diizinkan (unauthorized personnel)
- 3 Komponen :
  - Membuat lokasi fisik tidak menarik dijadikan target serangan
  - Deteksi penetrasi atau pencuri
  - Pemulihan dari pencurian atau kehilangan informasi kritis atau sistem.

Memahami Lingkup Menjaga Keamanan SI

b) Keamanan Operasional

- Bagaimana organisasi memperlakukan komputer, network, sistem komunikasi dan manajemen informasi
- Termasuk *access control, authentication, security topologies, back up* dan *recovery plan*
- Hal efektif untuk meningkatkan operational security $\rightarrow$ pelatihan keamanan SI (security training)

Memahami Lingkup Menjaga Keamanan SI

c) Manajemen dan Kebijakan Keamanan

- Akan menghasilkan tuntunan, aturan dan prosedur untuk implementasi
- Kebijakan agar efektif harus memiliki dukungan penuh dan tidak dapat dikompromikan dari tim manajemen
- Beberapa contoh kebijakan :
  - Administrative policies
  - Design Requirement
  - Disaster Recovery Plan
  - Information Policies
  - Security Policies
  - Usage Policies
  - User Management Policies

Standar Kualitas Keamanan SI

ISO 17799 / 27001 / 27002

- Business Continuity Planning
- System Access Control
- System Development and Maintenance
- Physical and Environmental Security
- Compliance
- Personnel Security
- Security Organization
- Computer & Network Management
- Asset Classification and Control
- Security Policy

Kualifikasi Profesional Keamanan SI

- ***SANS Institute*** *Certified Engineers.*
- ***CISSP Certified*** *and Trained Engineers.*
- ***ISO 27001:2005*** *Lead Auditors.*
- ***Certified Ethical Hackers****.*
- ***Product related engineers*** *with extensive knowledge of various security products.*
- *…dan lain-lain.*

Mau Jadi Satpam SI ?

Modal dasar :

- Mengetahui Bahasa Pemrograman
- Menguasai pengetahuan perangkat keras dan perangkat lunak pengontrolnya (logika interfacing).
- Menguasai pengelolaan instalasi komputer.
- Menguasai dengan baik teori jaringan komputer ; protokol, infrastruktur, media komunikasi.
- Memahami cara kerja sistem operasi.
- Memiliki ‘pikiran jahat’ ;-p

Cara belajar :

- Memantau perkembangan teknologi keamanan komputer :
- Cari buku-buku mengenai keamanan komputer cetakan, e-book, majalah-majalah/tabloid komputer edisi cetak maupun edisi online.
- Akses ke situs-situs review keamanan (contoh: www.cert.org), situs-situs underground (silahkan cari via search engine).
- Pelajari review atau manual book perangkat keras dan perangkat lunak untuk memahami cara kerja dengan baik atau ikuti pelatihan sertifikasi

Selesai dulu untuk hari ini