COMPUTER SECURITY

ARTIKEL



OLEH :

NIM	**: 120010150**
Nama	**: I Gede Yudita Eka Prasetya**
Jurusan	**: S1 - Sistem Komputer**
Angkatan	**: 2012**

Sekolah Tinggi Manajemen Informatika dan Teknik Komputer

(STMIK) STIKOM BALI

2014

Uraian:
Mata Kuliah ini memberikan pengetahuan kepada mahasiswa tentang penjelasan pengertian sekuriti dan privacy serta hubungan yang terjadi, masalah-masalah yang dapat menghambat pengoperasi sekuriti, pertimbangan-pertimbangan dalam sistem sekuriti dan rencana-rencana pengimplementasiannya.

Sasaran:
Membekali pengetahuan kepada mahasiswa tentang konsep keamanan pada komputer serta dampak-dampak yang dapat terjadi

Materi:
1. Konsep Dasar Keamanan Komputer
2. Keamanan computer secara fisik
3. Keamanan Komputer secara Operating System
4. Keamanan Komputer di dalam jaringan
5. Administrasi Keamanan Komputer
6. Cryptography; Etika di dalam keamanan komputer.

Daftar Pustaka:
1. P.Pleeger, Charles, Lawrence Pleeger Sari, "Security in Computing", 3rd Edition, Prentice Hall, New Jersey, 2003
2. Staling, William, "Cryptography and Network Security: Principles & Practices", Third Edition, Prentice Hall, New Jersey, 2003
3. Russell, Deborah and Gangemi Sr., G.T., "Computer Security Basics", 3rd Edition, O'Reilly & Associates, USA, July 1992.

DAFTAR ISI

DAFTAR ISI ..... **II**

BAB 1 KONSEP DASAR KEAMANAN KOMPUTER **1**

1. PENGERTIAN KEAMANAN COMPUTER 1
2. ATTACKS 1
3. COMPUTER CRIMINAL 1
4. METHODS OF DEFENSE 1
5. ENCRYPTION, HARDWARE, SOFTWARE AND HUMAN CONTROL IN SECURITY 1

BAB 2 KEAMANAN COMPUTER SECARA FISIK **2**

1. NATURAL DISASTER ..... **ERROR! BOOKMARK NOT DEFINED.**
2. HARDWARE ..... **ERROR! BOOKMARK NOT DEFINED.**
3. HUMAN VANDALS ..... **ERROR! BOOKMARK NOT DEFINED.**
4. INTERCEPTION OF SENSITIVE INFORMATION ..... **ERROR! BOOKMARK NOT DEFINED.**
5. LOCKS AND KEY ..... **ERROR! BOOKMARK NOT DEFINED.**
6. BIOMETRICS ..... **ERROR! BOOKMARK NOT DEFINED.**

BAB 3 KEAMANAN KOMPUTER SECARA OPERATING SYSTEM **8**

1. CONTROL OF ACCESS TO GENERAL OBJECT 8
2. ACCESS CONTROL MATRIX 9
3. PROCEDURE ORIENTED ACCESS CONTROL 24
4. USER AUTHENTICATION 29
5. AUTHENTICATION PROCESS 30
6. SENSITIVE DATA 38
7. ACCESS DECISION 38
8. DIRECT ATTACK 42
9. INDIRECT ATTACT 50

BAB 4 KEAMANAN KOMPUTER DIDALAM JARINGAN **51**

1. ENCRYPTION 51
2. CRYPTOGRAPHIC 58
3. THREATS IN NETWORKS 58
4. NETWORK SECURITY CONTROL 58
5. FIREWALLS 58

BAB 5 ADMINISTRASI KEAMANAN KOMPUTER **65**

1. PERENCANAAN SEKURITI 65
2. ANALISA RESIKO 70
3. KEBIJAKAN KEAMANAN ORGANISASI 72

BAB 6 CRYPTOGRAPHY **74**

2. LATAR BELAKANG MATEMATIKA 74
3. SYMETRIC ENCRYPTION 76
4. SISTEM ENKRIPSI PUBLIC KEYS 76
5. QUANTUM CRYPTOGRAPHY 81

BAB 7 ETIKA DIDALAM KEAMANAN COMPUTER **81**

1. PROTEKSI TERHADAP PROGRAM DAN DATA 81
2. HUKUM DAN INFORMASI DIDALAM COMPUTER SEKURITI 82
3. RIGHTS OF EMPLOYEES AND EMPLOYERS 84
4. SOFTWARE FAILURE 86
5. COMPUTER CRIME 87

DAFTAR ACUAN **91**

BAB 1

Konsep Dasar Keamanan Komputer

1. *Pengertian keamanan computer*

Sekuriti : Segala sesuatu yang mengenai keamanan
Komputer : Suatu sistem yang meliputi CPU (Prosesor), Memori, I/O Device, dll
Sekuriti Komputer : Segala sesuatu yang mengenai keamanan bagi Sistem Komputer

Filosofi (dasar pemikiran) Keamanan Komputer
Agar dapat mengamankan sistem komputer dengan benar, maka kita harus tahu karakteristik penganggu yang akan mendatangi sistem komputer kita.

Komponen sistem Komputer :
Perangkat Keras (Hardware)
Misalnya : dari pencurian, dll
Perangkat Lunak (Software)
Misalnya : dari serangan virus, harckres, dll
Perangkat Manusia (Brainware)
Pembajakan tenaga kerja

Ada 2 pihak yang terkait

Pihak yang diganggu (Sistem Komputer)	**Pihak yang mengganggu**
• Perangkat lunak • Perangkat keras • Perangkat manusia • Manajemen • Basis Data • Operasional • Fisik	• Lingkungan • Fisika • Kimia • Manajemen • Organisasi • Perangkat Lunak • Perangkat Keras • Sistem Operasi • Telekomunikasi

2. *Attacks*
3. *Computer Criminal*
4. *Methods Of Defense*
5. *Encryption, Hardware, Software and Human Control in security*

BAB 2

Keamanan Computer Secara Fisik

SISI LINGKUNGAN

Dari sisi lingkungan yang perlu diwaspadai adalah :

- Manusia
- Binatang
- Tumbuhan
- Cuaca
- Iklim
- Bencana Alam

MANUSIA

- Mencuri
    - Mengambil barang (fisik)
        - Mencuri perangkat keras komputer
    - Mencuri data (logic)
        - Menyadap
            - Mendengar
            - Melihat
            - Media transmisi
        - Mengcopy data
        - Memotret
- MERUSAK
    - Mengakibatkan sebagian atau keseluruhan sistem tidak berfungsi
- MENGGANGGU
    - Sebagian atau seluruh sistem terganggu

PENANGGULANGAN

- Dengan membuat area yang terbatas, terutama ruang server
- Melindungi sebagian peralatan komputer dengan kerangka besi

BINATANG

- Tikus : mengerat, sarang, urine, kotoran, bangkai
- Cicak : telur, urine, kotoran, bangkai
- Kecoa : mengerat, telur, urine, kotoran, bangkai
- Laba-laba : sarang, telur, urine, kotoran, bangkai
- Rayap : mengerat, sarang, urine, kotoran, bangkai
- Ngengat : telur, urine, kotoran, bangkai
- Semut : sarang, urine, kotoran, bangkai
- Lalat : urine, kotoran, bangkai
- Tawon : sarang, telur, urine, kotoran, bangkai
- Nyamuk : urine, kotoran, bangkai

Yang berbahaya dari binatang adalah :

- Keratan, urine, kotoran, bangkai, sarang
- Yang paling berbahaya yaitu urine, Karena mengandung zat-zat yang bersifat asam. Urine dapat melarutkan materi yang bersifat logam yang tidak tahan asam,misalnya Tembaga (Cu), Besi (Fe), Emas (Au)
- Bahan yang digunakan pada *motherboard* adalah tembaga dan emas, sehingga dapat ikut larut bila terkena zat yang bersifat asam.

PENANGGULANGAN

- Menjaga kebersihan komputer
- Menghalangi jalan masuk ke dalam dengan kasa
- Membunuh atau menangkap serangga dengan alat
- Jangan menggunakan kapur barus, karena kapur barus akan menyublim pada udara bebas. Gas yang dihasilkan dapat menempel pada benda lain dan mengkristal, misalnya pada permukaan head baca tulis, sehingga akan menganggu proses baca tulis.

TUMBUHAN

Ada 3 jenis tumbuhan yang perlu diwaspadai, yaitu :

- Jamur
- Lumut
- Ganggang Biru

Ketiganya akan mudah tumbuh pada lingkungan yang kelembabannya tinggi.

PENANGGULANGAN

- Gunakan Air Conditioning (AC) untuk ruang kerja
- Gunakan Silica Gel untuk tempat penyimpanan

  Baik AC maupun Silica Gel berfungsi untuk membuat ruangan atau tempat penyimpanan.

CUACA

Yang termasuk cuaca antara lain :

- Kelembaban
  - Kadar air di udara
  - Satuannya : %
  - Diukur dengan Hygrometer
  - Udara yang lembab dapat menyebabkan tumbuhnya jamur, lumut dan ganggang biru.

  PENANGGULANGAN
  - Gunakan AC untuk ruang kerja komputer
  - Gunakan Silica Gel untuk tempat penyimpanan

- Angin
    - Udara yang bergerak
    - Dapat membawa debu, materi-materi kecil
    - Dapat membuat kabel komunikasi bergetar, sehingga mengganggu pengiriman data.

    PENANGGULANGAN
    - Bersihkan komputer secara berkala

- Debu
    - Debu yang lembab cenderung bersifat konduktor.
    - Dapat mengakibatkan hubungan singkat
    - Bila menempel pada head baca tulis, permukaan disket, pita magnetic ataupun CDROM dapat mengganggu proses baca tulis.

    PENANGGULANGAN
    - Ruangan harus selalu dijaga kebersihannya
    - Gunakan penghisap debu
    - Bersihkan komputer secara berkala
    - Simpan media penyimpanan pada tepat yang tertutup
    - Setelah selesai bekerja dengan komputer, tutuplah komputer dengan penutup khusus.

- Mendung
    - Mengakibatkan temperatur meningkat

    PENANGGULANGAN
    - Gunakan AC untuk mengatur suhu udara

- Hujan
    - Mengakibatkan kelembaban udara meningkat

    PENANGGULANGAN
    - Gunakan AC untuk mengurangi kelembaban udara

- Petir
    - Cenderung menyambar sesuatu yang relatif paling tinggi

    PENANGGULANGAN
    - Gunakan penangkal petir yang baik
    - Arde (ground) yang benar, ditanam sampai ke air tanah
    - Hindari pemasangan kabel dari logam di udara, misalnya , dll

- Iklim
    - Yang perlu diwaspadai adalah daerah yang mempunyai 4 musim, karena perbedaan antara siang dan malam sangat tinggi.
    - Pada suhu panas, material akan memuai dan suhu dingin akan menyusut.
    - Pemuaian dan penyusutan dapat merusak komponen komputer

    PENANGGULANGAN
    - Gunakan AC untuk mengatur suhu ruangan

BENCANA ALAM

- Yang termasuk bencana alam antara lain
    - Gempa Bumi
    - Banjir
    - Kebakaran

PENANGGULANGAN

- Buat supaya ruangan lebih tahan gempa
- Jangan letakkan komputer pada lantai dasar, untuk menghindari banjir
- Siapkan alat pemadam kebakaran

SISI FISIKA dan KIMIA

Yang termasuk gangguan dari sisi fisika :

PANAS

- Dapat terjadi dari dalam komputer, ruangan dan luar ruangan
    - Dari dalam komputer disebabkan karena komponen elektronik dialiri arus listrik
    - Dari ruangan disebabkan karena alat pemanas, seperti pemanas air, kompor
    - Dari luar ruangan lebih disebabkan dari panas matahari.

PENANGGULANGAN

- Gunakan kipas angin (fan) atau heat sink pada komponen yang mudah panas.
- Gunakan kaca film atau Gordeyn, untuk menghindari masuknya sinar matahari.
- Gunakan AC untuk mengatur suhu udara ruangan

LISTRIK

- Kelebihan voltase
    - Dapat merusak komponen elektronik
- Kekurangan voltase
- Mati Listrik
    - Sering membuat sistem operasi rusak

PENANGGULANGAN

- Gunakan stabilizer untuk menstabilkan voltase
- Gunakan UPS

MAGNET

- Dapat merusak media penyimpangan yang dibuat dari bahan mylar, misalnya disket, tape, kaset lagu/video.
- Dapat mempengaruhi head pada disk drive

PENANGGULANGAN

- Jauhkan dari magnet

- **SUARA**
    - Getaran suara dapat mempengaruhi head dari disk

PENANGGULANGAN

- Jauhkan dari sumber bunyi-bunyian yang kuat

- **KIMIA**
    - Salah satunya adalah kebocoran baterai
    - Bahan kimia yang keluar dari baterai yang bocor dapat merusak motherboard

PENANGGULANGAN

- Lakukan pemeriksaan komputer secara berkala

SISI PERANGKAT KERAS

PERANGKAT KERAS Komputer dibagi menjadi 3 kategori :

- Mililiter (-40^0 s/d 120^0 C)
    - Digunakan oleh pemerintahan
- Industri (Normal s/d 90^0 C s/d 100^0 C)
    - Komputer yang bermerek
- Jangkrik (normal s/d 60^0 C s/d 70^0C)
    - Komputer rakitan

SISI MANAJEMEN

MANAJEMEN

- Pemberian otoritas (hak pakai) kepada user
    - Setiap user akan mempunyai otoritas sesuai dengan pekerjaannya.
- Pemberian kata sandi / password
    - Setiap user / account **harus** diberikan kata sandi atau password
    - Sering kali password dilakukan dengan cara mengetik pada keyboard
    - Sekuriti paling lemah
    - Mudah disadap oleh orang lain
    - Mudah dilihat apa yang ketik oleh orang pada keyboard

    Solusinya :
        - Password tidak harus diketik melalui keyboard
        - Ada cara lain untuk menggantikan pengetikan di keyboard

Password dapat dengan menggunakan

- Sinyal suara
    - Pada awalnya semua suara kita direkam terlebih dahulu
    - Diproses lalu hasilnya disimpan
- Sidik jari / telapak tangan
    - Pada awalnya sidik jari atau telapak tangan di scan
    - Diproses lalu hasilnya disimpan
- Retina mata
    - Pada awalnya mata kita direkam pola retinanya
    - Diproses lalu hasilnya disimpan
- Tanda tangan
    - Dilihat dari penekanan pada waktu tanda tangan
- Wajah
    - Pada awalnya wajah direkam terlebih dahulu
    - Diproses lalu hasilnya disimpan
- Kartu magnetik
    - Dapat menyimpan data pada magnetic stripe
- Bar code
    - Berupa garis-garis
    - Sering kali dipergunakan pada barang-barang yang dijual
- Kartu Chip
    - Biasanya dipergunakan sebagai ATM Bank, Kartu Telpon, dll
- Micro chip
    - Dapat menyimpan identitas manusia
    - (Rencananya) akan ditanam dalam tubuh manusia

BAB 3
Keamanan Komputer Secara Operating System

1. Control Of Access to General Object

Control Access

Classification of Information Assets

a. Siapa yang mempunyai hak akses dan untuk apa?
b. Level akses yang diberikan
c. Siapa yang bertanggungjawab untuk menentukan hak akses dan level akses
d. Persetujuan apa yang diperlukan untuk melakukan akses?

What is access control?

- Access control adalah jantungnya security
- Definisi:
  - Kemampuan untuk memberikan ijin hanya kepada orang yang berhak atau mempunyai auhthorized (otoritas) terhadap program atau sistem proses atau mengakses sumber data
  - Memberikan hak (grant) atau menghapus hak (deny), sesuai dengan security model khusus, yang mempunyai ijin (permission) pasti untuk mengakses sumber data
  - Sekumpulan prosedur yang dibentuk oleh h/w, s/w dan administrator, untuk memonitor akses, mengidentifikasi user yang meminta akses, mencatat record yang diakses dan memberikan akses grant atau deny berdasarkan aturan yang sudah ditetapkan.

Controls

- Kendali: mengurangi resiko/kerugian
  - Preventive: mencegah terjadinya insiden
  - Detective: mendeteksi terjadinya insiden
  - Correctice: memperbaiki (restoration) jika terjadi insiden
- Implementasi:
  - Administrative Control: policies, prosedur, security awareness/training, supervisi, dll.
  - Logical/Technical Control: pembatasan akses ke sistem dan teknik proteksi yang digunakan, mis. Smart cards, enkripsi dll.
  - Physical Control: penjagaan fisik, mis. Biometric door lock, secured area utk server, deadman door dll.

Logical Access Controls

- Akses kontrol infrastruktur TI dapat dilakukan pada berbagai tingkat
  - Front end (user) & Back end (server)
  - Bagaimana jaringan terbagi dan perlindungan akses ke sumber informasi
- Paths of Logical Access
  - Point umum dari entry
    - Network connectivity
    - Remote access
    - Operator console
    - Online workstations or terminals

Logical Access Controls: Protection

- Logical Access Control Software
  - Cegah akses dan modifikasi data sensitif organisasi dari orang yang tidak mempunyai otorisasi dan penggunaan fungsi sistem kritis
  - Semua layer: network, operating systems, databases & application systems
  - Fungsi software:
    - Identifikasi dan otentikasi
    - Otorisasi akses
    - Monitor: Logging aktifitas user, reporting
  - Implementasi paling efektif: tingkat networks dan operating system (membatasi privileges pada low level)

Logical Access Controls: Software

- Logical Access Control Software Functionality
  - Secara umum fungsi akses kontrol sistem operasi meliputi:
    - Mekanisasi identifikasi dan otentikasi user
    - Restricted logon IDs
    - Aturan akses untuk sumber informasi yang spesifik
    - Create individual accountability and auditability
    - Create or change user profile
    - Log events
    - Log user activities
    - Report capabilities
- Logical Access Control Software
  - Fungsi akses kontrol basis data dan/atau level aplikasi meliputi:
    - Create or change data files and database profiles
    - Verify user authorization at the application and transaction levels
    - Verify user authorization within the application
    - Verify user authorization at the field level for changes within a database
    - Verify subsystem authorization for the user at the file level
    - Log database/data communications access activities for monitoring access violations

2. Access Control Matrix

Transaksi yang aman tetap dipertanyakan karena tidak yakin apakah e-mail purchase order yang diterima benar-benar otentik, apakah transfer bonus anggota tidak diubah-ubah.

Persepsi menghadapi pertanyaan:

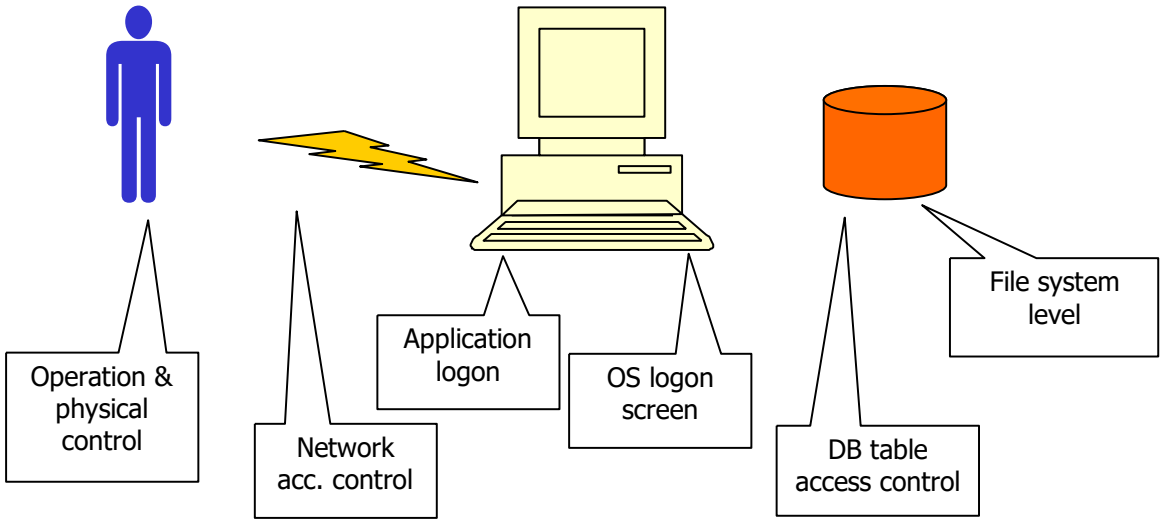
- Bagaimana caranya supaya website saya tidak di-hack orang?
- Bagaimana caranya agar data kartu kredit saya tidak dibaca orang lain?
- Bagaimana caranya agar kita yakin bahwa e-mail purchase order yang kita terima benar-benar otentik?
- Bagaimana caranya agar yakin bahwa nilai 100 juta dalam fund transfer tidak diubah-ubah?

Untuk meyakinkan hal ini maka dipelajari Security Architecture & Models.

Security Architecture & Models

Tujuan

- Mempelajari berbagai konsep, prinsip dan standar untuk merancang dan mengimplementasikan aplikasi, sistem operasi, dan sistem yang aman.
  Untuk lebih jelas maka akan dijabarkan dimana pengamanannya yaitu:



Tempat pengamanan pada Security Architecture & Models

Prinsip-prinsip keamanan

- **Least previlage**: artinya setiap orang hanya diberi hak akses tidak lebih dari yang dibutuhkan untuk menjalankan tugasnya. Seorang staf umum dan gudang hanya mendapat hak akses untuk menjalankan aplikasi administrasi gudang. Seorang staf penanganan anggota hanya mendapat hak akses untuk menjalankan aplikasi administrasi Seorang staf pemasaran hanya mendapat hak akses untuk menjalankan aplikasi administrasi pemasaran dan penjualan. Seorang staf kepegawaian hanya mendapat hak akses untuk menjalankan aplikasi administrasi kepegawaian. Seorang manajer mendapat hak akses untuk membaca dan menjalankan aplikasi departemen yang dibawahinya dan dapat membaca file yang dimiliki oleh stafnya. Seorang direktur dapat memonitor seluruh pekerjaan yang dilakukan oleh manajer yang ada dibawahnya.
- **Defense in Depth**: gunakan berbagai perangkat keamanan untuk saling membackup. Misalnya dapat dipergunakan multiple screening router, mirroring harddisk pada server, dua CDRW untuk satu kali backup data yaitu dua kali sehari (setiap pagi dan sore) pada masing-masing departemen sehingga kalau satu dijebol, maka yang satu lagi masih berfungsi.
- **Choke point**: semua keluar masuk lewat satu (atau sedikit) gerbang. Syaratnya tidak ada cara lain keluar masuk selain lewat gerbang.
- **Weakest link**: "a chain is only as strong as its weakest link". Oleh karena itu kita harus tahu persis dimana weakest link dalam sistem sekuriti organisasi kita. Kelemahan jaringan di dalam sistem sekuriti organisasi yang perlu diawasi adalah bila ada virus baru yang tidak terdeteksi. Oleh karena itu update anti virus pada server dan client harus selalu dilakukan dan tidak boleh diabaikan.

- **Fail-Safe Stance**: maksudnya kalau suatu perangkat keamanan rusak, maka secara default perangkat tersebut settingnya akan ke setting yang paling aman. Misalnya: kapal selam di Karibia kalau rusak mengapung, kunci elektronik kalau tidak ada power akan unlock, packet filtering kalau rusak akan mencegah semua paket keluar-masuk. Bila packet filtering pada firewall modem router ADSL rusak maka semua paket keluar-masuk akan dicegah.
- **Universal participation**: semua orang dalam organisasi harus terlibat dalam proses sekuriti. Setiap tiga bulan sekali dilakukan pelatihan untuk menyegarkan kembali ingatan akan pentingnya mengamankan perangkat keamanan komputer. Di dalamnya dilakukan evaluasi untuk peningkatan efisiensi kinerja proses keamanan komputer.
- **Diversity of Defense**: mempergunakan beberapa jenis sistem yang berbeda untuk pertahanan. Maksudnya, kalau penyerang sudah menyerang suatu jenis sistem pertahanan, maka dia tetap akan perlu belajar sistem jenis lainnya.
- **Simplicity**: jangan terlalu kompleks, karena sulit sekali mengetahui salahnya ada di mana kalau sistem terlalu kompleks untuk dipahami. Untuk mempermudah mengetahui bila terjadi kesalahan maka setiap data yang disimpan dalam server akan teridentifikasi siapa yang menyimpan berdasarkan user name dan passwordnya, kapan tanggal dan waktunya, dari workstation yang mana, dan apa aksi yang dilakukan. Bila user tidak mempunyai hak untuk menambah dan mengubah data pada sistem aplikasi tertentu tersebut maka akan ada trigger yang memberitahu bahwa sistem menolak adanya perubahan data.

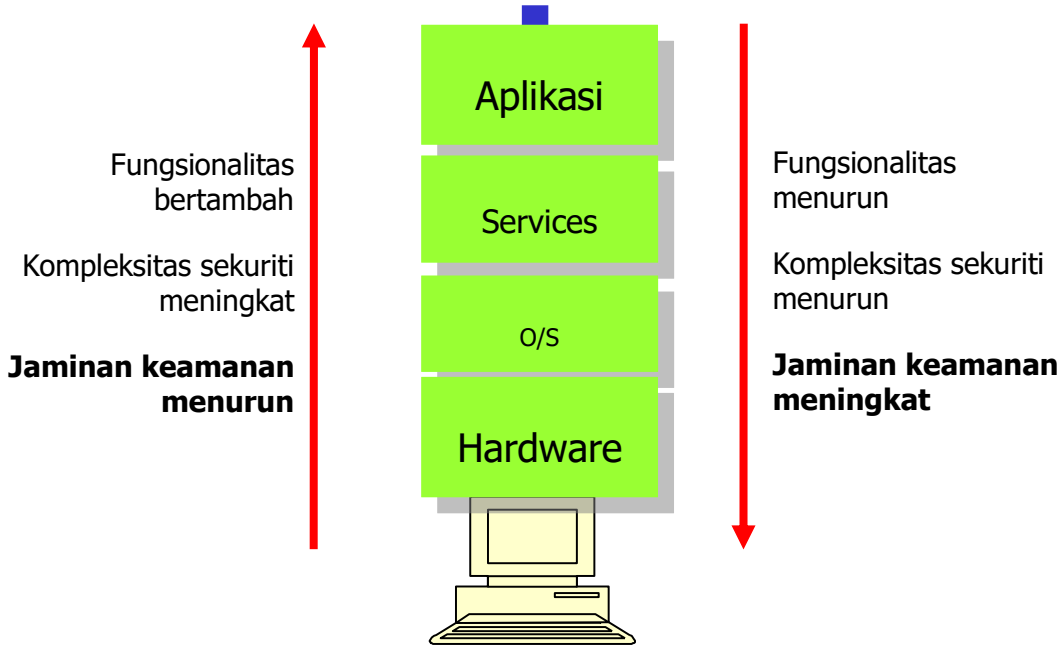
Proteksi Lapis Bawah (Low Level)

- Pengamanan yang lebih ke arah hardware
- Lebih Sederhana
- Melebar
- Tidak fleksibel
- Misalnya: write-protect pada USB drive, IP restriction

Proteksi Lapis Atas (High Level)

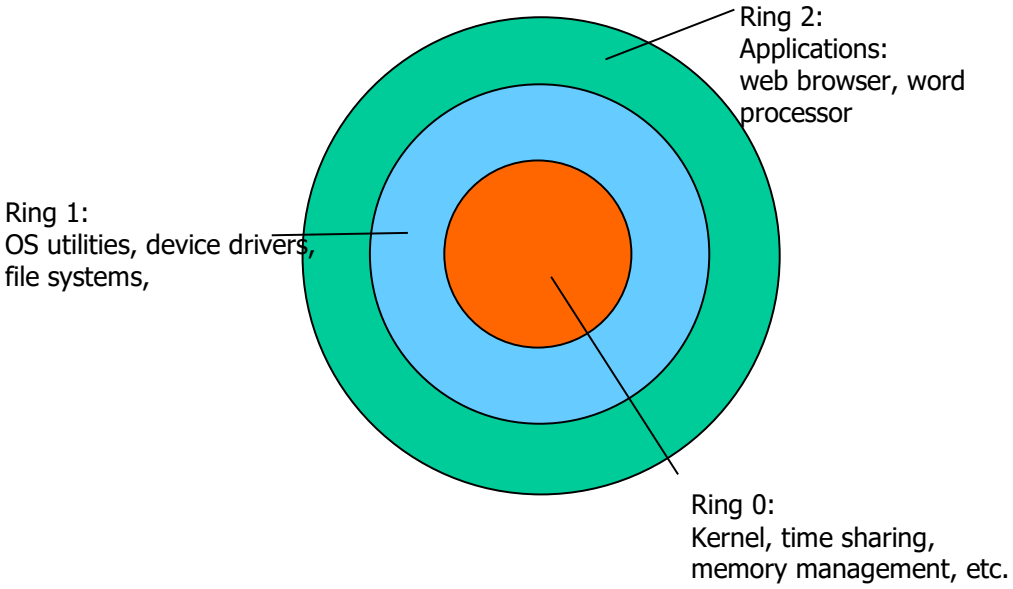
- Lebih rumit/kompleks
- Bisa pada aplikasi atau sistem prosedur
- Lebih fleksibel dan lebih detail kendalinya
- Mengakibatkan menurunnya jaminan mekanisme keamanan
- Karena butuh ekstra untuk install, testing/pengujian dan pemeliharaan
- Misalnya: akses kontrol tabel database & aplikasi

Tingkatan jaminan keamanan



System Architecture Security

Contoh pada operating systems



Trusted Computing Base (TCB)

- Kombinasi keseluruhan dari mekanisme pengamanan dalam sebuah sistem komputer
- Mencakup: hardware, software, dan firmware
- Komponen yang masuk TCB harus teridentifikasi dan kemampuannya terdefinisi dgn jelas.
- TCB mengikuti standar *security rating* tertentu seperti **Orange Book** (akan dijelaskan)
- Perihal tingkat **kepercayaan** (bukan keamanan)

Security Perimeter

- Semua komponen yang tidak masuk dalam TCB.
- Harus ada standar komunikasi, yakni melalui interface yang sudah *defined.*
- Contoh:
  - Anda membuat program dengan bahasa Java, belum tentu anda berhak mendapatkan hak akses untuk manipulasi data pada memori secara langsung. Pembuatan dan manipulasi data dilakukan melalui objek-objek dan interface Java Virtual Machine.

Security Models

Security model adalah representasi simbolik dari kebijakan, yang harus dilaksanakan oleh sistem komputer, apa yang boleh dan tidak secara teknis. Tujuannya yaitu untuk memformalkan kebijakan keamanan organisasi.

Security Models

- Untuk memformalkan kebijakan keamanan organisasi
- Representasi simbolik dari kebijakan, yang harus dilaksankan oleh sistem komputer
- Security policy sifatnya lebih abstrak dan lebar, security model adalah apa yang boleh dan tidak secara teknis
  - Analogi: kalau dokter bilang kita harus hidup sehat, ini adalah "policy". Tapi kalau dokter memberikan wejangan: makan secukupnya, rajin olah raga, jangan suka marah, ini "teknisnya"

Security Models

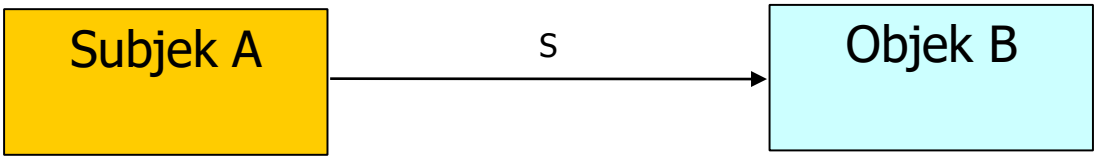
- Access Control Matrix Models
- Bell-LaPadula Model
- Biba
- Clark-Wilson Model
- Information Flow Model

Access Matrix Model

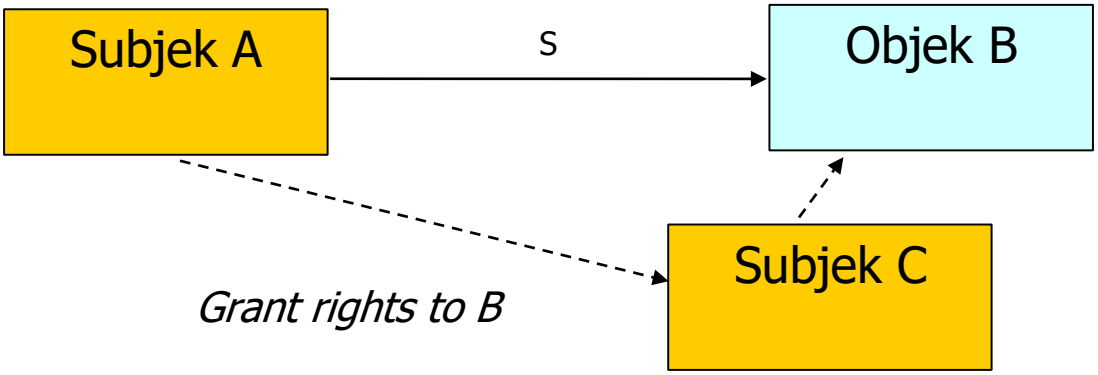
	File: Income	File: Salaries	Process: Deductions	Print Server
Joe	R	R/W	X	W
Jane	R/W	R	-	W
Checking prog.	R	R	X	-
Tax Prog.	R/W	R/W	X	W

Take-Grant Model

- Menggunakan directed graph untuk mentransfer hak ke subjek lain
- Misalnya A punyak hak S, termasuk untuk hak mentransfer, pada objek B



- Subjek A bisa memberikan haknya kepada Subjek C, sehingga memiliki hak atas objek B



Bell-LaPadua Model

- Dibuat tahun 1970-an, untuk militer Amerika Serikat, untuk pengamanan kerahasiaan informasi
- Menggunakan lattice, tingkatan keamanan militer yakni:
  - Top Secret
  - Secret
  - Sensitive but unclassified
  - Unclassified
- Fokus pada confidentiality

Yang dimaksud dengan model adalah sistem yaitu kumpulan subject, object dan access control matrix. Adapun tingkat atau level security, setiap subject, object berada pada tingkat tersebut. Access right untuk subject adalah read-only, append, execute, read-write.

Formal modelnya adalah state transitions yaitu:

a. State awal dari system adalah secure (aman)

b. Selama perubahan state, transition dapat menjaga system tetap aman sehingga state berikutnya tetap secure.

c. System state secure merupakan operasi dan izin mengikuti aturan (access control) sesuai dengan spesifik policy keamanan untuk system tersebut.

d. Mode akses dari subject terhadap object yaitu:

   i. Izin terhadap subject tertentu dibandingkan dengan tingkat klasifikasi keamanan dari suatu object.

   ii. Berdasarkan penjelasan diatas, ditentukan tingkat otorisasi bagi subject tersebut untuk mode akses yang akan dilakukan.

Untuk menjaga kerahasiaan informasi maka secure state kerahasiaannya adalah multilevel properties yaitu:

a. Simple Security Property (SS Property) – no read up. Artinya membaca informasi oleh subject yang lebih rendah tidak diperbolehkan.

b. * Star Security Property – no write down. Artinya menulis informasi oleh subject pada level lebih rendah tidak diperbolehkan.

c. Discretionary SS – access matrix untuk flexibilitas control.

Sebagai tambahan maka Trusted subject dapat secara sah diberikan untuk dispensasi aturan diatas.

Model rulenya yaitu:

a. Higher-level subject selalu dapat membaca (read down) object yang berada pada level yang sama atau dibawahnya.

b. Lower-level subject tidak berhak membaca (read up) object yang berada pada level diatasnya.

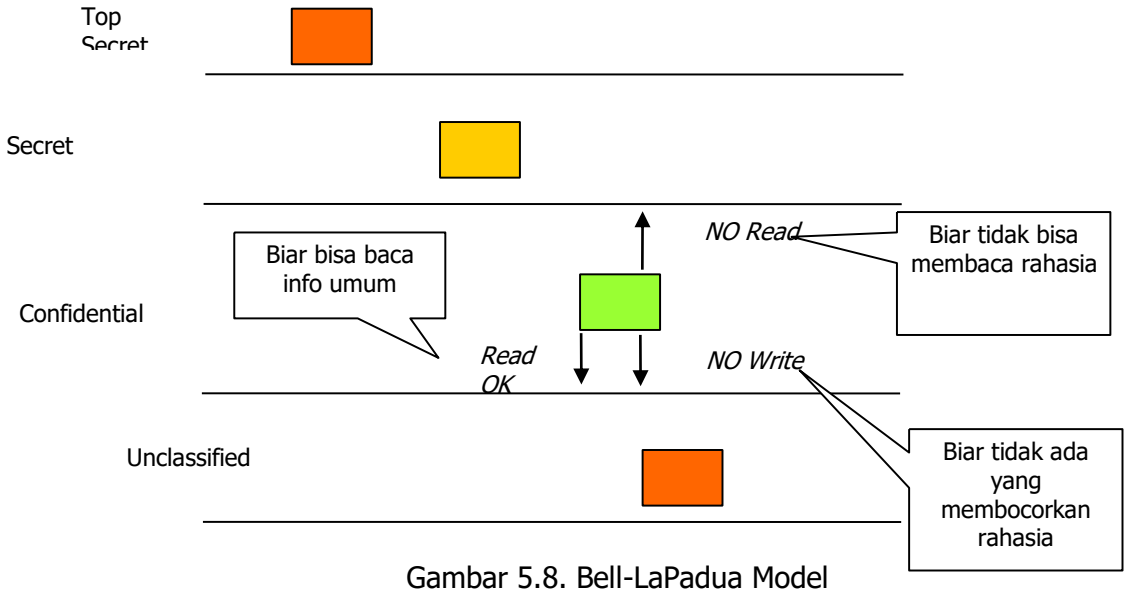
c. Subject mempunyai: read-write akses untuk object yang setingkat.

d. Subject pada lower-level dapat melakukan update (append) object yang berada pada tingkat atas.

e. Subject pada higher-level tidak dapat menulis (write down) pada object lower level karena kemungkinan terjadi kebocoran informasi (lower level tidak cukup aman utuk menangani informasi dari upper level).

Implikasi model pada security informasi yaitu "No read-up, no write down" pada setiap tingkat (level) security.

Bell-LaPadua



Gambar 5.8. Bell-LaPadua Model

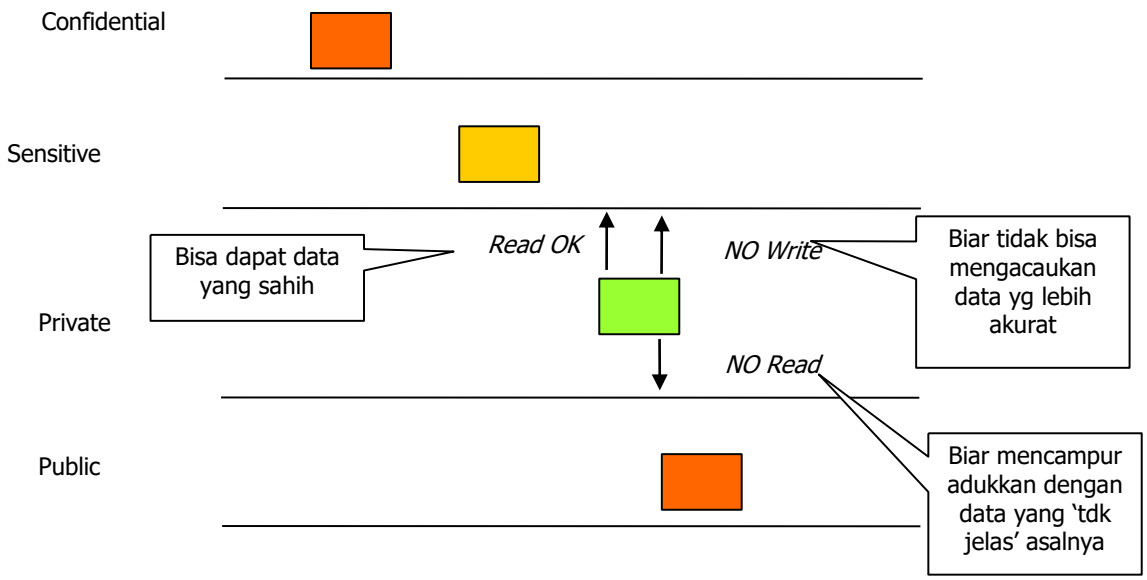
Biba Model

Biba yang menjamin integritas data dibuat tahun 1977. Untuk integritas informasi ditambahkan aturan "lower level" tidak dapat mengupdate higher-level object. Fungsinya yaitu untuk mencegah kontaminasi informasi dari object yang kurang aman. Misalnya, akuntan lebih ingin agar data keuangan akurat, dan

tidak ingin data menjadi corrupt gara-gara aplikasi/operator tidak bekerja seperti semestinya (misalnya: pembulatan, salah ketik, penambahan digit, dsb.)

Implikasi model pada security informasinya yaitu ”No write up, no append up”. Bahkan untuk akuntan yang lebih ingin agar data keuangan akurat, dan tidak ingin data menjadi corrupt gara-gara aplikasi/operator tidak bekerja seperti semestinya (misalnya: pembulatan, salah ketik, penambahan digit, dsb.) maka dilakukan enkripsi sebagai perlindungan datanya.

Biba Model

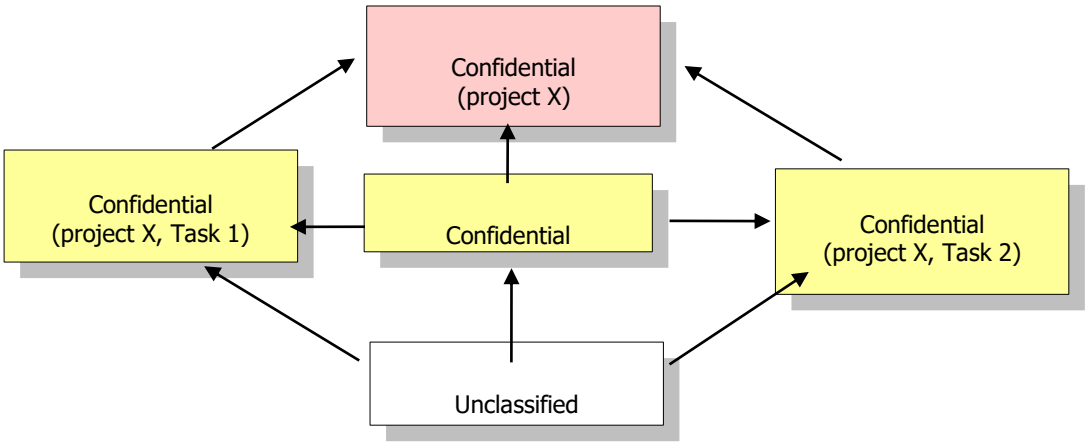


Clark-Wilson Model

- User tidak bisa akses objek langsung, tapi harus lewat suatu program
- File tidak bisa dibuka sembarangan program (notepad.exe, misalnya), tapi harus lewat aplikasi khusus
- Bisa menerapkan *separation of duties,* misalnya orang yang melakukan entri data (Write) dan yang membuat laporan (Read), orangnya berbeda

Information Flow Model

- Tiap objek diberikan *security class* dan mungkin nilai.
- Informasi hanya bisa mengalir sesuai kebijakan yang ditetapkan
- Contoh:



Orange Book

- DoD Trusted Computer System Evaluation Criteria, DoD 5200.28-STD, 1983
- Provides the information needed to classify systems (A,B,C,D), defining the degree of trust that may be placed in them
- For stand-alone systems only
- Windows NT has a C2 utility, it does many things, including disabling networking

Orange book levels

- A - Verified protection
  - A1
  - Boeing SNS, Honeywell SCOMP
- B - MAC
  - B1/B2/B3
  - MVS w/ s, ACF2 or TopSecret, Trusted IRIX
- C - DAC
  - C1/C2
  - DEC VMS, NT, NetWare, Trusted Solaris
- D - Minimal security. Systems that have been evaluated, but failed
  - PalmOS, MS-DOS

Problems with the Orange Book

- Based on an old model, Bell-LaPadula
- Stand alone, no way to network systems
- Systems take a long time (1-2 years) to certify
  - Any changes (hot fixes, service packs, patches) break the certification
- Has not adapted to changes in client-server and corporate computing
- Certification is expensive
- For the most part, not used outside of the government sector

Red Book

- Used to extend the Orange Book to networks
- Actually two works:
  - Trusted Network Interpretation of the TCSEC (NCSC-TG-005)
  - Trusted Network Interpretation Environments Guideline: Guidance for Applying the Trusted Network Interpretation (NCSC-TG-011)

Sertifikasi vs. Akreditasi

- Sertifikasi
  - evaluasi teknis untuk keperluan akreditasi
  - evaluasi menggunakan prosedur baku
- Akreditasi
  - persetujuan resmi bahwa sistem yang disertifikasi dapat dipercaya.

Sistem Terbuka vs. Tertutup

- Sistem Terbuka
  - spesifikasi terbuka sesuai bakuan/standar industri tertentu
  - pihak ketiga dapat berpartisipasi
- Sistem Tertutup
  - spesifikasi khusus dan tertutup
  - tanpa pihak ketiga

Keamanan Jaringan

Keamanan jaringan pada PT. MASS-NET dilakukan untuk menjaga agar resource digunakan sebagaimana mestinya oleh pemakai yang berhak. Pemakaian alat (termasuk program) dapat menyebabkan kerusakan baik disengaja atau tidak. Pembatasan pemakaian bukan untuk mempersulit tetapi supaya efisien dan tidak merusak. Oleh karena itu untuk meyakinkan keamanan jaringannya maka dilakukan perlindungan yaitu:

1. **authentication**: pemakai harus dapat membuktikan dirinya yang ditandai dengan usernamenya dan passwordnya. Dalam jaringan ditambahkan sumber akses (komputer yang digunakan) dengan asumsi bahwa pada satu saat satu orang hanya dapat/boleh bekerja dengan satu komputer yang sama.
2. **gateway**: gerbang masuk menuju sistem dengan firewall modem router ADSL
3. **attack**: serangan terhadap system dilindungi dengan firewall modem router ADSL dan intrusion detection systems (IDS).
4. **authorization**: pemakai diperbolehkan menggunakan pelayanan dan resource sesuai dengan haknya.
5. **Monitoring**: pengawasan terhadap jaringan dilakukan dengan software khusus untuk monitoring jaringan dan menulis catatan pada sistem.
6. **Komunikasi terenkripsi**: menggunakan enkripsi agar data tak dapat diintip

Authentication. Database tentang user.

Dibawah ini merupakan informasi umum tentang pemakai yang disimpan di file /etc/passwd sebagai penjelasan yang lebih rinci dari keamanan jaringan.

```
Enter command # more /etc/passwd
root:*:0:0:Bozz:/root:/bin/sh
toor:*:0:0:Bourne-again Superuser:/root:
daemon:*:1:1:Owner of many system processes:/root:/sbin/nologin
--- dipotong ---
www:*:10000:65533:WebMaster:/nonexistent:/sbin/nologin
nobody:*:65534:65534:Unprivileged user:/nonexistent:/sbin/nologin
gatut:*:21001:21001:Gatut:/home2/gatut:/usr/local/bin/tcsh
wardojo:*:1004:20:Wardojo:/home2/wardojo:/usr/local/bin/tcsh
ari:*:1005:20:Ari Nurcahyo:/home1/ari:/usr/local/bin/tcsh
tres:*:1006:20:Theresia Maria Sri Prihatiningsih:/home2/tres:/usr/local/bin/tcsh
--- dipotong ---
```

Pada contoh diatas yang digunakan adalah utilitas LINUX: finger. Dimana defaultnya, menampilkan daftar nama pemakai yang sedang aktif atau informasi lain tentang pemakai tertentu. Dibawah ini berikut contoh untuk penggunaan finger.

```
[gatut@bsd02 gatut]$ finger
[gatut@bsd02 gatut]$ finger gatut
Login    Name               TTY  Idle  Login Time   Office  Phone
gatut    V Gatut Harijoso    p0         Wed    00:13 PUSKOM
```

Untuk utilitas LINUX: w dan who, fungsinya adalah mengetahui pemakai yang sedang aktif. Berikut ini bentuk contoh untuk penggunaan utilitas LINUX: w dan who.

```
[gatut@bsd02 gatut]$ w
[gatut@bsd02 gatut]$ who
```

Untuk utilitas LINUX: last, fungsinya adalah menampilkan daftar pemakai terakhir. Berikut ini bentuk contoh untuk penggunaan utilitas LINUX: last.

```
[gatut@bsd02 gatut]$ last
pemake   ttyp0    10.210.2.51      Tue Jun 29 23:50 - 00:02  (00:11)
yuser    ttyp9    167.205.136.3    Tue Jun 29 23:37 - 23:39  (00:02)
7397023  ttyp1    10.210.2.48      Tue Jun 29 23:07 - 23:24  (00:16)
--- dst -- dipotong --
```

Pemakai harus selalu memperhatikan pesan "last login from:" pada saat login agar dapat segera diketahui apabila terdapat pemakai lain yang menggunakan user-id tersebut. Authentikasi melalui sistem (yaitu, password) yang sesungguhnya disimpan dalam bentuk ter-enkripsi dalam file yang tak dapat dilihat oleh pemakai biasa, biasanya /etc/master.passwd atau /etc/shadow.

Authorization

Untuk authorization sebagai bagian dari keamanan jaringan maka pemakai yang sudah terbukti mendapatkan haknya dapat dilayani dan dapat menggunakan resource yang sesuai dengan levelnya. Pemakai memiliki hak penuh atas file yang dimilikinya, maka pemakai harus mengatur sendiri datanya.

Untuk utilitas LINUX: chmod, fungsinya adalah menentukan hak akses file dan directory. Berikut ini bentuk contoh untuk penggunaan utilitas LINUX: chmod.

```
.[gatut@bsd02 gatut]$ chmod
[gatut@bsd02 /home]$ ls -l
total 4
drwxr-xr-x  26 gatut    staff        2048 Jun 30 00:03 gatut
drwxr-xr-x   9 pemake   user         1024 May  8 09:41 pemake
drwxr-xr-x   2 noone    nobody       1024 Apr 16 11:53 noone
[gatut@bsd02 /home]$ chmod 0711 gatut
[gatut@bsd02 /home]$ ls -l
total 4
drwx--x--x  26 gatut    staff        2048 Jun 30 00:03 gatut
drwxr-xr-x   9 pemake   user         1024 May  8 09:41 pemake
drwxr-xr-x   2 noone    nobody       1024 Apr 16 11:53 noone
[gatut@bsd02 /home]$
```

Ada banyak aplikasi yang bekerja di server bekerja atas nama super-user, misalnya agar dapat membaca file password atau menulis data ke dalam sistem (lihat kembali perintah "ps aux"). Semakin kompleks aplikasi, semakin besar kemungkinan terdapat kesalahan (bug). Program yang berjalan atas nama super-user dan salah bisa berakibat fatal. Oleh sebab itu, biasanya aplikasi client-server sebisa mungkin memisahkan akses yang menuntut hak super-user.

Gateway

Gateway yang menghubungkan sistem ke luar dapat menjadi gerbang ke dalam, sehingga ada resiko perusakan atau pencurian data oleh publik yang jauh lebih luas. Firewall (dinding api) gateway yang menjaga keamanan sistem.

1. Penyaringan packet: hanya paket dari dan ke host, tcp, udp tertentu yang boleh berkomunikasi. Program melakukan pemeriksaan dan penyaringan sehingga hanya pelayanan yang diketahui dan benar yang boleh lewat.
2. Gateway aplikasi: pengiriman dan penerimaan mail gateway untuk mempermudah pemeriksaan dan mengurangi beban jaringan.

Attack

Kejadian yang sering menyebabkan data disadap atau tercuri bahkan terkena virus adalah akibat password terbuka karena adanya pencurian, catatan yang tercecer, pengamatan (cara mengetik, mengintip paket). Oleh karena itu cara yang dapat dilakukan adalah dengan membelokkan akses yaitu dengan mengganti ip, dns, atau route membelokkan akses ke server palsu untuk menjebak password.

Serangan yang terjadi kadangkala juga disebabkan karena kesalahan program. Seperti pepatah yang mengatakan tak ada gading yang tak retak. Oleh karena itu diberikan kebijakan keamanan jaringan yaitu dilarang menjalankan program yang tak diketahui karena penyebaran virus dapat dengan mudah melalui email, java script, vb script akibatnya membebani server dengan akses yang besar.

Cara penyerangan yang juga perlu diwaspadai adalah batu loncatan. Biasanya akses dari komputer yang terletak di intranet kurang dibatasi. Apabila akses ke komputer di intranet terbuka, maka pemakai internet dapat masuk ke dalam komputer di intranet, kemudian menggunakan komputer tersebut sebagai batu loncatan. Oleh karena itu pembatasan pemakaian komputer terhadap orang yang tidak berwenang dilakukan dengan mengunci pintu ruangan setiap keluar dan masuk ruangan.

Monitoring

Untuk mengamankan jaringan maka penting sekali dilakukan monitoring. Karena monitoring merupakan cara untuk mengetahui apa yang terjadi sebagai tindakan preventif dengan membaca catatan system. Karena server menggunakan LINUX maka dapat dilihat catatan systemnya yang biasanya disimpan dalam directory /var/log.

/var/log/messages Pesan-pesan dari sistem
/var/log/maillog Transaksi email (SMTP)

Komunikasi Terenkripsi

Komunikasi melalui jaringan publik memungkinkan adanya penyadap ikut mendengarkan percakapan oleh karena itu jalur komunikasi harus dienkripsi. Namun ada konsekuensi akibat enkripsi yaitu data yang dipertukarkan lebih besar. Dibawah ini merupakan beberapa software yang menjadi pilihan agar komunikasi dapat terenkripsi sehingga dapat diyakinkan keamanan jaringannya yaitu:

- ☑ Secure Shell: pengganti telnet dengan enkripsi
- ☑ HTTPS: secure HTTP

3. Procedure Oriented Access Control

DATA ACCESS : PERLINDUNGAN TERHADAP DATA

Yang perlu diperhatikan terhadap pengaturan akses terhadap data yang disimpan adalah :

- **Siapa yang boleh membaca file Anda**
- **Siapa yang boleh merubah file Anda**
- **Dapatkan data Anda di-share dengan user lain**

Kondisi ini hanya berlaku pada komputer yang mendukung multi user.

Control: Models

- ☐ Akses kontrol "subject" (aktif:mis. Proses, user) terhadap "objet" (pasif mis. File) berdasarkan setting "rule" (aturan)
- ☐ Rule dapat dikategorikan tiga model:
  - ■ Mandatory Access Control
  - ■ Discretionary Access Control
  - ■ Non-Discretionary Access Control

Mandatory Access Control

- ☐ Setiap data/resource yang akan di-share dengan membandingkan sensitivitas object tersebut terhadap "dearance" yang diberikan untuk "subject"
- ☐ Pemberian label dari level sensitivitas untuk semua data berdasarkan klasifikasi
- ☐ Hanya user dengan clearance utk level tsb yg dpt mengakses: need to know basis
- ☐ Hanya administrator, owner tidak boleh, yg dpt merubah object level
- ☐ Semua keputusan akses ditentukan oleh sistem
- ☐ Lebih komplek bila dibandingkan dengan DAC
- ☐ Khusus digunakan untuk proses data yang sensitif
- ☐ Misalnya : informasi pemerintah atau perusahaan.
- ☐ Digunakan dalam sistem dimana security adalah hal yang kritis, cth., militer

Discretionary Access Control

- ■ Access Control merupakan otorisasi yang diberikan oleh owner dari data / resources

- Harus mematuhi security policies, tapi lebih flexible; - misalkan mandatory => apa yang tidak tercantum adalah dilarang sedangkan discretionary => owner dapat memberikan penilaian otorisasi
- Contoh: Access Control List => daftar apa saja permission yang diberikan oleh owner dari data/resources

Non-Discretionary Access Control

- Penjabaran kebijakan, jabatan, tugas dalam organisasi: "role based"
- Access control tidak tergantung pada individu tapi fungsi dan perorangan individu tersebut

DISCRETIONARY ACCES CONTROL (DAC)

- Pembatasan akses terhadap file, direktori, device berdasarkan user dan/atau group
- Pengaturan akses dilakukan oleh pemilik file
- Ada 3 tipe dasar dari pengaksesan data
    - Read
    - Write
    - Execute

JENIS-JENIS PEMBATALAN AKSES KONTROL

- **OWNERSHIP**
    - Pembuat File adalah si pemilik file
    - Login atau beberapa pengenal disimpan dalam file
    - Jika kita pemilik dari file, maka dapat membaca dan merubah isi file
    - Jika kita bukan pemilik file, maka kita tidak dapat mengakses file tersebut
    - Administrator dapat mengakses file ini.

FILE TYPES and FILE PROTECTION CLASSES

- **Lebih baik daripada metode Ownership**
- **Sebuah file dapat didefinisikan sebagai public, semi public atau private file.**
- **Contoh :**
- **Sebuah user dapat membaca atau menulis ke file yang bersangkutan.**

- **Sebuah file diberi atribut Blank --> Publik**
- **Semua user dapat membaca atau menulis ke file yang bersangkutan**
- **Sebuah file diberi atribut Execute-only ----> Semi Public**
- **Semua user dapat menjalankan file tersebut**
- **Hanya pemilik file dari Administrator yang dapat merubah isi file**

- **Sebuah file diberi atribut Read-only -> Semi Public**
  - **Semua user dapat membaca dan menjalankan file**
  - **Hanya pemilik dari file Administrator yang dapat merubah isi file**
- **Sebuah file diberi atribut Private --> Private**
  - **Hanya pemilik file dan Administractor yang dapat membaca, merubah dan menjalankan file.**

- **Pengelompokan file-file berdasarkan kelas-kelas**
  - **Contoh : Administrator men-setup sistem sehingga hanya user yang memiliki akses klas P yang dapat mengakses program PAYROLL.**

SELF/GROUP/PUBLIC CONTROLS

- **Dibagi dalam 3 kategori**
- **Beberapa sistem menyebutnya sebagai pengontrolan self/group/public**
- **Dalam UNIX disebut user/group/other (UGO)**
  - **Self Anda – Pembuat/pemilik file**
  - **Group Sekelompok user**
  - **Public User yang tidak termasuk di atas**
- **Setiap file mempunyai sekumpulan bit-bit yang disebut permissions**
- **Contoh :**
- **-rw-rw-r-- 1 budi staff 81904 nov 7 13:25 berkas**

- **- rw – rw – r –**
-
- **X S G P**
- **Tanda (-) menunjukkan bahwa user tidak mempunyai hak**
- **Abaikan tanda (-) pertama**

- **Pemilik file (budi) dapat membaca dan menulis/mengubah file berkas (rw-)**
- **Anggota group file (staff) dapat membaca dan menulis/mengubah file berkas (rw-)**
- **Sedangkan user yang lainnya hanya dapat membaca file berkas (r--)**A
- **Contoh :**

  Bila terdapat 3 buah group dengan anggotanya masing-masing dalam suatu sistem oprasi, misalnya :

Manager	Operator	Staff
Budi	**ani**	**ali**
Amir	**joni**	**joko**
Melati	**amir**	**tia**

  Bila diketahui suatu direktori Sbb :

-rwxr-xr--	**budi**	**oprator**	**berkas.soal**
----rwx---	**joni**	**staff**	**hasil.ujian**
-rx---rwx	**melati**	**staff**	**nilai.ujian**
-r--r-x--x	**joko**	**manager**	**soal.ujian**

  Penjelasan:

- **User budi mempunyai hak terhadap file berkas.soal : rwx**
- **User ani mempunyai hak terhadap file berkas.soal : rx**
- **User joko mempunyai hak terhadap file berkas.soal : r**
- **User joni mempunyai hak terhadap file hasil.ujian : -**
- **User joko mempunyai hak terhadap file hasil.ujian : rwx**
- **User melati mempunyai hak terhadap file hasil.ujian : -**
- **User melati mempunyai hak terhadap file nilai.ujian : rx**
- **User tia mempunyai hak terhadap file nilai.ujian : x**
- **User budi mempunyai hak terhadap file nilai.ujian : rwx**
- **User ami mempunyai hak terhadap file soal.ujian : rx**
- **User joko mempunyai hak terhadap file soal.ujian : r**
- **User ali mempunyai hak terhadap file soal.ujian : rwx**

- Yang dapat merubah file permissions adalah pemilik dari file dan Administrator.
- Pasa UNIX, untuk merubah file permissions, instruksinya adalah **chmod**
- Syntax :

  Chmod <a|u|g|o><+|-><r|w|x> namafile

  a - all + - Menambahkan

  u – user - - Mengurangi/menghilangkan

  g – group

  o – other r – Read

  w – Write

  x – eXecute

-rwxr-xr	**budi**	**operator**	**berkas.ujian**
----rwx---	joni	staff	hasil.ujian
-rx---rwx	melati	staff	nilai.ujian
-r--r-x--x	joko	manager	soal.ujian

- Contoh :

  Chmod u + r hasil.ujian

  -**r--**rwx--- joni staff hasil.ujian

  Chmod g + rwx nilai.ujian

  -r-x**rwx**rwx melati staff nilai.ujian

  Chmod go + w berkas.soal

  -rwxr**w**xr**w**- budi operator berkas.soal

-rwxr-xr	**budi**	**operator**	**berkas.soal**
----rwx---	joni	staff	hasil.ujian
-rx---rwx	melati	staff	nilai.ujian
-r--r-x--x	joko	manager	soal.ujian

  Chmod a + w soal.ujian

  -r**w--**r**w**x-**w**x joko manager soal.ujian

  Chmod u-rwx berkas.soal

-rwxrw budi operator berkas.soal

Chmod ug-r hasil.ujian

-----wx--- joni staff hasil.ujin

Chmod a-rwx berkas.soal

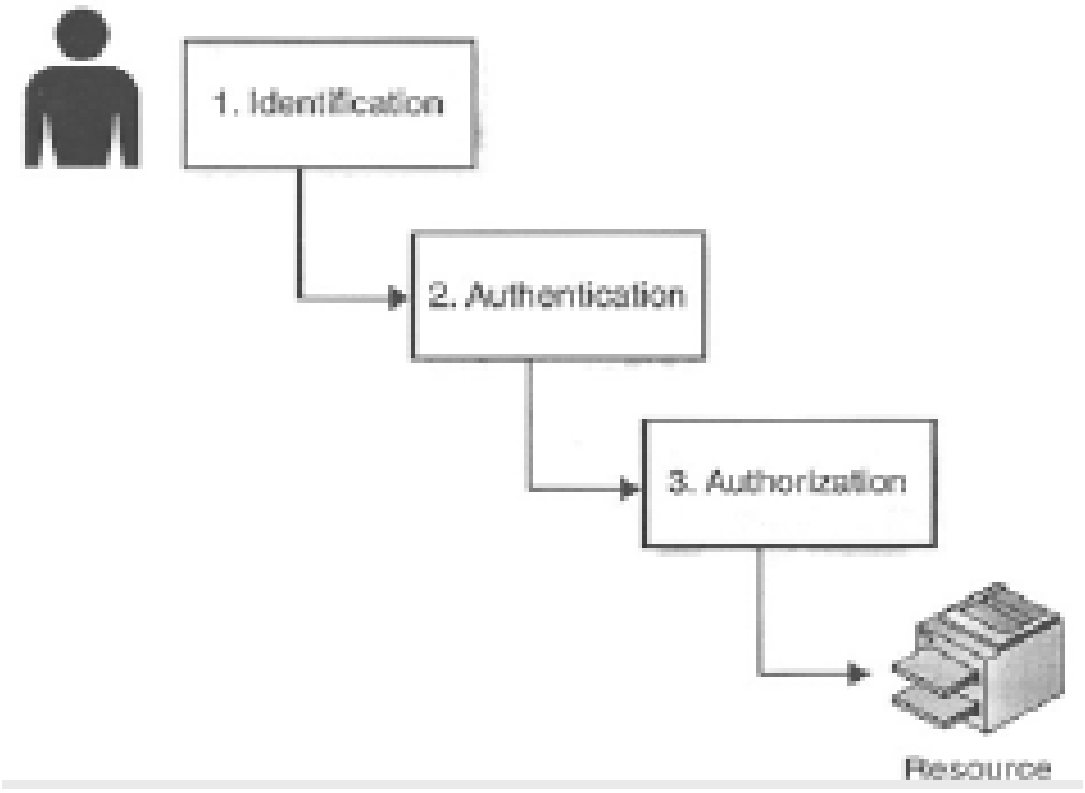
ACCESS CONTROL LIST

- **Suatu daftar user-user dan group-group dengan haknya masing-masing.**
- **Lebih fleksibel dibandingkan dengan sebelumnya**
- **Contoh :**
    - **File PAYROLL akan dilindungi dengan ACL dalam bentuk :**
    - **<john.acct,r>**
    - **<jane.pay, rw>**
    - **Dimana :**
- **John dan jane adalah user yang dapat mengakses file PAYROLL**
- **Acct dan pay adalah group id dari user**
- **r dan w menunjukkan jenis akses**
- **r berarti user dapat membaca file, w berarti user dapat merubah file**

4. User Authentication

Identification & Authentication (1/2)

- Identification and authentication
    - Logon-ids and passwords
        - Bentuk tampilan dan ukuran password
        - Aturan format / sintaks password
    - Token devices – one time passwords
    - Biometric
    - Umumnya access control bertumpu pada:
    - Identifikasi dan Otentifikasi



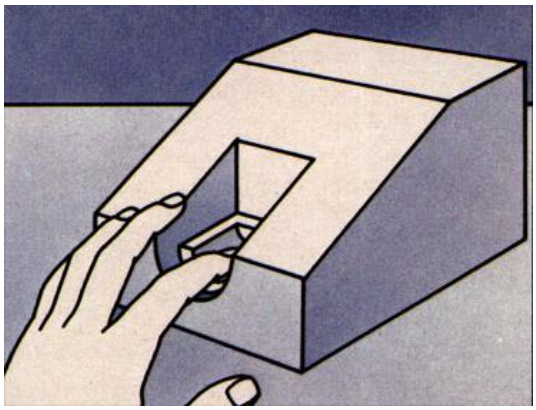
Umumnya access control bertumpu pada:
Identifikasi dan Otentifikasi

5. Authentication Process

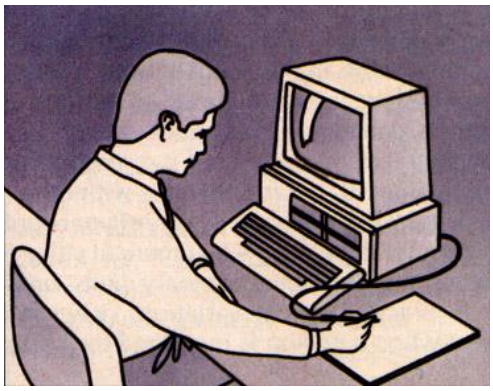
Identification

- Identifikasi:
  - Proses atau aksi yang dilakukan oleh user untuk membuktikan siapa (identitas) dirinya kepada sistem.
  - Misalkan: log-on ke sistem
- Otentikasi:
  - Verifikasi user tersebut sesuai dengan identitas yang diberikan
  - Logical access control akan dilakukan sesuai dengan hasil verifikasi tersebut.
  - Berdasarkan tiga faktor: what you know (mis.: PIN, password), what you have (mis. Card), what you are (mis. Fingerprint)

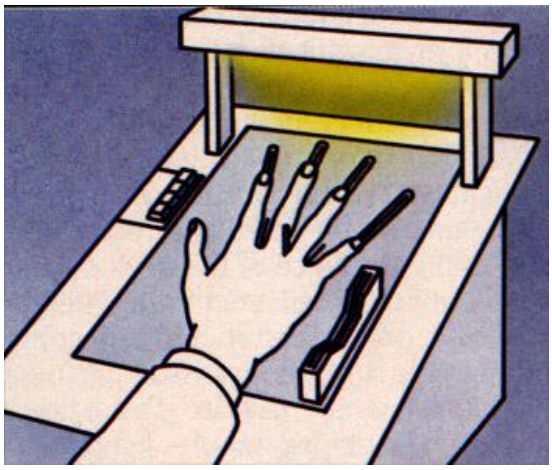
Identifikasi Fisik Manusia



Fingerprint scan



Hand Signature



Hand Geometry

Authentication: Variant



1. Memasukkan kartu identifikasi (what you have)
2. Mengetikkan 12 digit angka rahasia (what you know)
3. Komputer secara acak akan memilihkan kata-kata yang harus diucapkan ulang (who you are)

Authentication: Factors
- Umum: otentikasi makin banyak faktor (kombinasi) makin baik
- Two-Factor Authentication:
  - Diperlukan dua faktor otentikasi (dari 3 variant) yang ada
  - Misalkan: ATM menggunakan two-faktor, yakni ATM card dan PIN yang rahasia yang hanya diketahui user

Ada 2 langkah dalam proses login :

- Identifikasi

  Proses untuk memberitahu kepada sistem bahwa Anda mau login.

  Contoh :

  F : \ LOGIN > LOGIN

  Username : **BUDI**

- Otentikasi

  Proses membuktikan bahwa yang mau login benar-benar Anda.

  F : \ LOGIN > LOGIN

  Username : **BUDI**

  Password : XXXXXXXXXXX

Ada 3 cara otentikasi, yaitu :

- Sesuatu yang Anda tahu, misalnya Password
  - Secara teori, yang mengetahui password adalah pemiliknya sendiri, namun dalam prakteknya terdapat beberapa permasalahan
    - Diberikan ke orang lain lalu orang lain itu memberitahukan ke orang lain
    - Dicuri orang lain

    - Dituliskan di suatu tempat
    - Terlalu mudah ditebak
- Sesuatu yang Anda miliki, misalnya kunci, tanda pengenal, smart card
    - Secara teori, yang punya kunci atau dipinjam ke seseorang lalu diduplikasi.
    - Masalahnya :
        - Kunci hilang/terkunci atau dipinjam ke seseorang lalu diduplikasi

- Sesuatu yang Anda punya di tubuh, misalnya sidik jari, telapak tangan, pola retina, suara, tanda tangan, pola ketik di keyboard.
- Keamanan password menjadi tanggung jawab dari setiap pemiliknya
- Password itu seperti sikat gigi
    - Dipergunakan tiap hari
    - Diganti secara periode
    - Jangan digunakan oleh orang lain

PETUNJUK PROTEKSI DENGAN PASSWORD

- Jangan biarkan user / account tanpa password
    - Jika Anda seorang administrator sistem, pastikan setiap account punya password.
    - Gunakan software untuk memeriksa account /user yang tidak menggunakan password
- Jangan membiarkan password awal yang berasal dari sistem
    - Setelah menginstall sistem operasi, ubah segera semua password dari user **root, supervisor atau administrator**
- Jangan pernah biarkan seseorang
    - Password jangan diberitahukan ke orang lain, kecuali bila terpaksa sekali
- **Jangan menulis password Anda di terminal komputer, sekitar meja kerja atau di buku harian.**
    - **Dapat dibaca oleh orang lain**

    - **Jika pernah melakukan hal tersebut, jangan identifikasikan bahwa itu adalah password.**
- **Jangan mengetik password, sementara orang lain mengawasai dari belakang.**
    - **Sebelum mengetik password, alangkah baiknya kita melihat di sekitar kita, apakah ada yang mengawasi kita atau tidak.**

- **Jangan merekam password secara online atau mengirim ke suatu tempat via e-mail**
    - **Ada suatu program yang dapat men-scan isi –mail yang terdapat kata password.**
- Jangan membuat situasi semakin memburuk
    - Jika password Anda bocor, baik sengaja mau tidak sengaja segera langsung diubah
- Jangan menggunakan password sebelumnya
    - Apa lagi bila password itu pernah tercuri.

PETUNJUK MEMILIH PASSWORD

- **Jika diperbolehkan untuk mengubah password, pilihlah password yang sukar untuk ditebak.**
- **Ada beberapa saran untuk memilih password yang baik**
    - **Jangan menggunakan nama-nama seperti :**
        - **Nama sendiri**
        - **Nama anak**
        - **Nama pasangan (Suami/Istri/Pacar)**
        - **Nama pahlawan fiktif**
        - **Anggota keluarga**
        - **Binatang piaraan**
        - **Nama mobil**
        - **Dll**
- **Jangan menggunakan kata dalam bahasa Inggris**

- **Ada banyak file yang berisi kata-kata dalam bahasa Inggris, dimana kata-kata tersebut sering dipakai orang sebagai password.**
- **Dengan file tersebut orang akan coba-coba untuk menerka password**

- **Gunakan gabungan huruf dan angka**
  - **Misalnya : batman2001**
- **Jangan menggunakan seluruhnya berupa angka**
  - **Misalnya : nomor telpom, tanggal lahir**
  - **Kombinasi yang terjadi n^{10}**

- **Hati-hati dengan penggunakan spesial karakter**
  - **Beberapa spesial karakter mempunyai arti khusus bagi sofware emulasi**
  - **Contoh : Ctrl-S, Ctrl-H, Ctrl-/**
- **Pilihlah password yang panjang**
  - **Bila hanya beberapa huruf, maka akan mudah ditemukan dengan mencoba semua kombinasi**
  - **Gunakan minimal 6 – 8 karakter**
- **Password yang terbaik terdiri dari huruf kapital, huruf kecil dan minimal sebuah angka dan/atau spesial karakter.**
  - **Misalnya : BatmaN95**
- **Bedakan password antara host yang satu yang lainnya**
  - **Bila account satu host kebobolan, maka host yang lainnya setidaknya masih aman.**
- **Jangan menggunakan password sebelumnya**
  - **Apa lagi bila password itu pernah tercuci**
- **Boleh juga menggunakan kata-kata yang tidak ada artinya**
  - **Misalnya 8Bektang atau s1 (z/a%zo2**

PENGONTROLAN LOGIN / PASSWORD

- **Membatasi kesalahan login**

- **Kesalahan login harus dibatasi untuk menghindari login dengan coba-coba.**
- **Contoh : Pada ATM Bank, bila salah memasukkan PIN 3 x, maka kartu ATM akan "ditelan" atau nomer account akan diblokir.**

- **Periode waktu login setiap user dibatasi**
  - **Waktu login seorang user harus dibatasi**
- **Munculkan pesan login terakhir**
  - **Agar tahu kapan dan dimana terakhir kita login**
- **User dapat merubah password**
  - **User diberi hak untuk merubah password**
- **Password disediakan oleh sistem**
- **Password diberi batas waktu**
  - **Hal ini berguna agar user harus merubah password secara periodik**
- **Berikan panjang minimum dari password**
  - **Agar seorang user tidak membuat password dengan hanya beberapa huruf saja.**
- **Diperlukan 2 password (primary dan secondary) untuk login.**

Password (PIN etc.)

- Mekanisme yang paling umum untuk otentikasi
- Problems? Rawan!
  - Statik (digunakan berulang) => idealnya "one time password" hanya dapat digunakan sekali saja.
  - Mudah ditebak (singkat, kode) => passphrase (urutan strings/karakter panjang)
  - Penyimpanan (storages)/transmissions salah satu target dari hacker => harus dienkripsi (disandikan)
- Improvements dgn menggunakan "token"
  - Smartcard (processor+memori) yang dapat men-generate password (mis. One time password)

Passwords + Token

- Token: what you have!
- Dynamic passwords token
  - Token: generate password unik pada fixed time intervals (sumber: time-of-day dan disandikan dengan secret key token user)
  - Password tsb disubmit ke sistem + PIN user

- Sistem: otentikasi PIN user => secret key token user => decode password => time-of-day: valid untuk time window tersebut (one time only)

- Challenge-Response token
  - Sistem: challenge string/bilangan
  - Token: memproses challenge string + PIN dari user => response (dikirimkan ke sistem)
  - Sistem: verifikasi response sesuai atau tidak

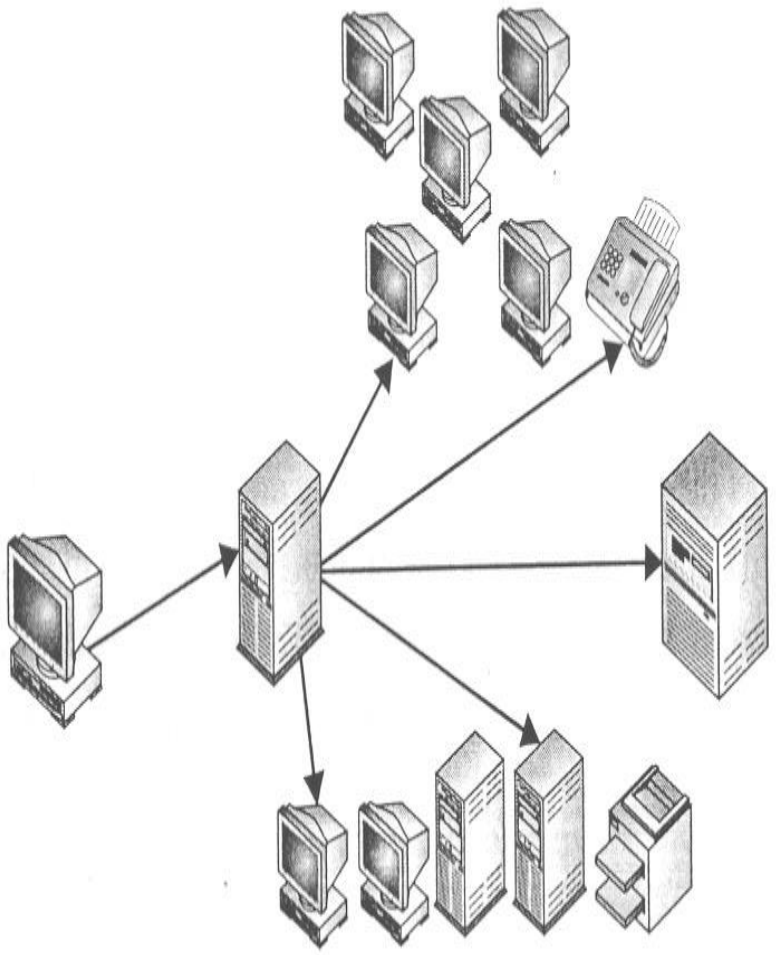
Typical Access Rights
- ✓ Read, inquiry or copy only
- ✓ Write, create, update or delete only
- ✓ Execute only
- ✓ A combination of the above

6. Sensitive Data

Biometric
- Pilihan lain selain passwords: something you are
  - Contoh: fingerprints, retina, hand geometry, voice.
- Verifikasi berdasarkan atribut (fisik atau kebiasaan) dari user:
  - Umumnya identifikasi user tersimpan, selanjutnya biometric mencocokkan klaim identitas user tersebut.
- Ukuran:
  - False Rejection Rate (FRR): valid subject => but reject
  - False Acception Rate (FAR): invalid subject => accepted
  - Crossover Error Rate (CER): FRR = FAR

7. Access Decision

Single Sign-on (SSO)
- Bagaimana mengontrol akses untuk multiple recources tersebar dijaringan komputer?
  - Setiap recource memanage access control => multiple passwords, tokens, etc.
- SSO melakukan konsolidasi proses administrasi otentikasi dan otorisasi terpusat (centralized administrative function):
  - Client-server and distributed systems
  - Mainframe systems
  - Network security including remote access mechanisms



Single sign-on technology enables a user to enter credentials one time to be able to access all resources within the domain.

Single sign-on (SSO) advantages

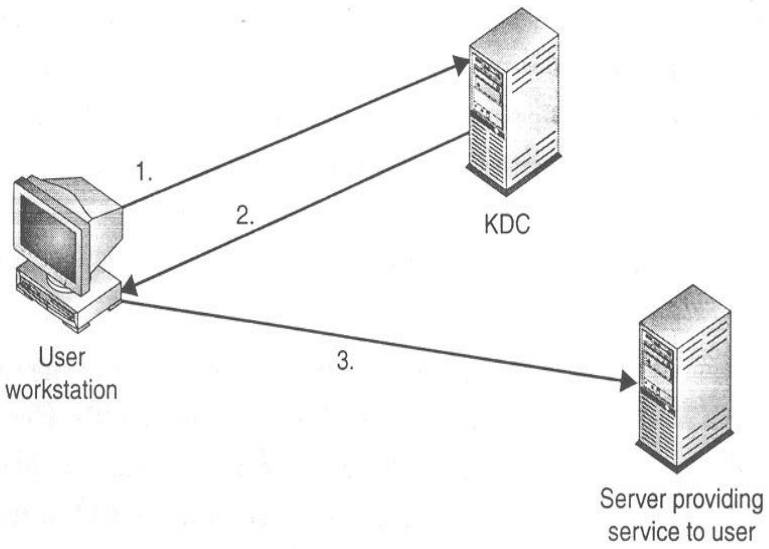
- ✓ Multiple passwords are no longer required, therefore, whereby a user may be more inclined and motivated to select a stronger password
- ✓ It improves an administrator's ability to manage users' accounts and authorizations to all associates systems
- ✓ It reduces administrative overhead in resetting forgotten passwords over multiple platforms and applications
- ✓ It reduces the time taken by users to log into multiple applications and platforms

Single sign-on (SSO) disadvantages

- ✓ Support for all major operating system environments is difficult
- ✓ The costs associated with SSO development can be significant when considering the nature and extent of interface development and maintenance that may be necessary
- ✓ The centralized nature of SSO presents the possibility of a single point of failure and total compromise of an organization's information assets

Key Distribution Centre

(gambaran umum)



1. User requests access to service running on a different server.
2. KDC authenticates user and sends a ticket to be used between the user and the service on the server.
3. User's workstation sends ticket to service to authenticate and use the requested service.

Figure 4-6 The user needs to receive a ticket from the KDC before being able to use requested resource.

Untung rugi KDC

- Keuntungan:
  - kalau ada user baru, tinggal menambahkan di KDC
  - kalau seorang user ter-*compromised*, tidak semua node akan tercompromised
- Kerugiannya:
  - KDC bisa memalsukan jati diri orang lain
  - KDC ada titik lemah dari sistem
  - Performa KDC bisa berkurang kalau banyak sekali orang berhubungan ke KDC pada waktu yang bersamaan.

Contoh KDC: Kerberos 5

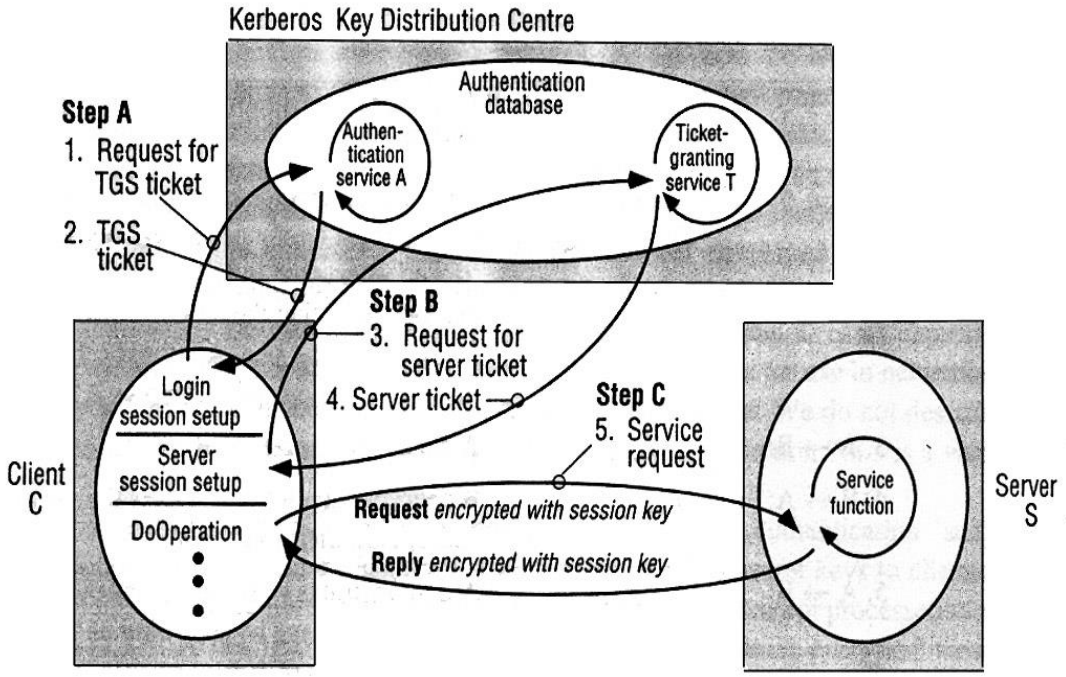
- Dimuat dalam RFC 1510 oleh Kohl dan Neuman pada tahun 1993, dan source code-nya bisa diambil dari http://web.mit.edu.
- Produk yang menggunakan antara lain OSF Distributed Computing Environment (DCE) dan Windows 2000.

Objek Kerberos

- Authentication: Token yang dibuat oleh client dan dikirim ke server untuk membuktikan jati diri user
- Ticket: diterbitkan oleh TGS (ticket granting service), yang dapat "ditunjukkan" oleh klien kepada suatu server layanan tertentu (misalnya database server).
- Session key: kunci random yang dibuat oleh Kerberos dan diberikan kepada klien saat ingin berkomunikasi dengan server tertentu.

Catatan:

- Klien membutuhkan 'ticket' dan session key untuk berhubungan dg server tertentu, dimana ticket tersebut memiliki periode pemakaian beberapa jam



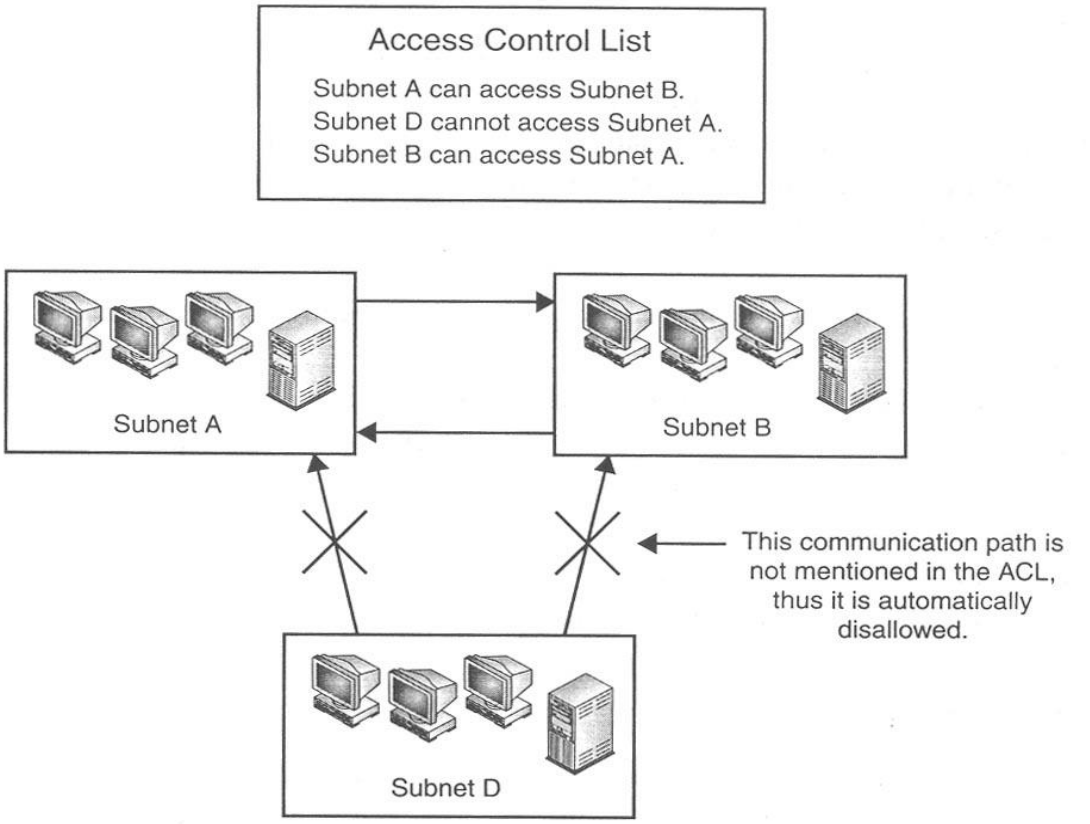


Figure 4-5 What is not explicitly allowed should be disallowed.

8. Direct Attack

PROGRAM YANG BERKELAKUAN JAHAT

- **Ada banyak program yang mempunyai kelakuan jahat, misalnya :**
  - **Virus**
  - **Worm**
  - **Trojan Horse**
  - **Bomb**
  - **Trap Door atau Back Door**
  - **Spoof**
  - **Bacteria**
  - **Rabbits**
  - **Crabs**
  - **Creepres**

  - **Salamis**
  - **Dll**
- **Saat ini di Indonesia yang paling banyak adalah Virus**

VIRUS

- **Sebuah program yang mempunyai kemampuan memecahkan diri dan meng-copy- ke dalam program/sistem lainnya.**
- **Biasanya dalam lingkungan satu istem operasi, walaupun ada yang beda sistem operasi**
- **Akan aktif bila sesuatu yang mengandung virus dijalankan**
- **Bergantung pada program yang lainnya**
- **Menginfeksi :**
  - **Memori**
  - **Disket**
  - **Harddisk,**
  - **Tape**
  - **Atau tempat penyimpanan lainnya**
- **Jenis virus menurut cara penyebarannya :**
  - Virus boot sektor / partisi
  - **Virus file**
  - Virus hybrid

Virus Boot Sektor / Boot Record atau Tabel Partisi

- **Bila disket telah diformat, maka secara logik akan terbagi dalam 4 area/daerah :**
  - **Boot Sektor/Boor Record**
  - **File Allocation Table (FAT)**
  - **Root Directory**
  - **Data Area**
- **Proses booting dengan menggunakan disket :**
  - **Komputer dihidupkan**
  - **ROM BIOS memperiksa peripheral**

- **ROM BIOS membaca Boot Record**
- **Boot Record membaca sistem operasi**
- **Komputer siap dipergunakan**

- **Bila harddisk telah diformat, maka secara logik akan terbagi dalam 5 area/daerah :**
  - **Tabel Partisi**
  - **Boot sektor / Boot Record**
  - **File Allocation Table (FAT)**
  - **Root Directory**
  - **Data Area**
- **Proses booting dengan menggunakan harddisk**
  - **Komputer dihidupkan**
  - **ROM BIOS memperiksa peripheral**
  - **ROM BIOS membaca Tabel Partisi**
  - **Tabel Partisi membaca Boot Record**
  - **Boot Record membaca sistem operasi**
  - **Komputer siap dipergunakan**
- **Pada virus jenis boot sektor/tabel partisi, virus ini memanfaatkan daerah Boot Sektor atau Boot Record atau Tabel Partisi untuk menyimpan program virus.**
- **Boot Sektor/Boot Record atau Tabel Partisi yang asli disimpan di tempat yang lain.**
- **Sehingga pada saat proses booting, yang pertama kai dibaca adalah Boot record atau Tabel Partisi yang mengandung virus**
- **Contoh virus jenis adalah :**
  - **(C) Brain**
  - **Stoned/Marijuana**
  - **Ping Pong/Bouncing Ball**
  - **Michelangelo**
  - **Denzuko**
  - **N250**

- **Supernova**
- **Dll**

- **Proses booting dengan menggunakan disket yang mengandung virus :**
  - **Komputer dihidupkan**
  - **ROM BIOS memperiksa peripheral**
  - **ROM BIOS membaca Boot Record (mengandung virus)**
  - **Boot record yang mengandung virus membaca Boot record yang asli**
  - **Komputer siap dipergunakan**
- **Proses booting dengan menggunakan harddisk yang mengandung virus :**
  - **Komputer dihidupkan**
  - **ROM BIOS memperiksa peripheral**
  - **ROM BIOS membaca Tabel Partisi (mengandung Virus)**
  - **Tabel Partisi yang mengandung virus membaca Tabel Partisi yang asli**
  - **Tabel Partisi yang asli membaca Boot record**
  - **Boot record membaca sistem operasi**
  - **Komputer siap dipergunakan**

Virus File

- **Pada virus jenis file, virus ini memanfaatkan file untuk tempat menyimpan program virusnya**
- **Pada awalnya virus ini menyerang file.EXE dan .COM**
- **Dibuat dengan bahasa Rakitan**
- **Saat ini, dapat menyerang file documen, seperti .DOC, .XLS, .PPT, dll**
  - **Termasuk juga file NORMAL.DOT**
- **Dibuat dengan bahasa Visual Basic**
- **Contoh virus jenis ini adalah :**
  - **Black Friday**
  - **Rontok/Falling Tears**
  - **UFO-4**
  - **Indonesia Emas**
  - **Virus Macro**

Virus Hybrid

- **Merupakan gabungan antara virus boot sektor dengan virus file**
- **Contoh :**
    - **Liberty/Mystic**

- **Jenis virus menurut tingkat keganasannya :**
    - **Virus jinak**
    - **Virus ganas**
    - **Virus mematikan**

Virus Jinak

- **Tidak berbahaya**
- **Biasanya hanya menampilkan namanya, nama perusahan, dll**
- **Contoh :**
    - **Virus Denzuko**
    - **Virus Indonesia Emas**
    - **Virus Ping Pong**

Virus Ganas

- **Virus ini merusak, tapi masih dapat diperbaiki kembali**
- **Contoh :**
    - **Virus Supernova**

Virus Mematikan

- **Virus ini merusak dan tidak dapat diperbaiki lagi**
- **Contoh :**
    - **Virus Michelangelo**
    - **Virus CIH**

- **Jenis virus menurut tujuan virus :**
    - **Untuk popularitas**
    - **Untuk tujuan proteksi**
    - **Untuk tujuan sabotase**

Untuk Popularitas

- **Bisanya hanya memunculkan nama pembuat, nama perusahaan, nama kampus.**

Untuk Proteksi

- **Digunakan untuk melindungi program dari pembajakan**

Untuk Sabotase

- **Digunakan oleh orang untuk menghancurkan komputer orang lain/lawannya yang tidak disukai.**

WORM

- **Tidak bergantung dengan suatu program**
- **Memperbanyak dirinya dengan cara mencopy dirinya sendiri dari 1 komputer ke komputer yang lainnya**
- **Biasanya melalui jaringan/network**
- **Tidak menyerang program**
- **Tidak merubah suatu program**
- **Tidak merusak data**
- **Tetapi berbahaya**
- **Memanfaatkan sumber daya jaringan**
- **Dengan dibuat menjadi macet dan sering kali membuat jaringan menjadi down.**

TROJAN HORSE

- **Suatu penggalan program yang bersembunyi di dalam program dan mempunyai suatu fungsi yang khusus.**
- **Sering disembunyikan di dalam program yang menarik user**
- **Misalnya suatu program yang menarik, permainan yang baru**
- **Biasanya digunakan untuk menyadap password seseorang**
- **Program Trojan Horse yang cerdik :**
    - **Tidak meninggalkan jejak kehadirannya**
    - **Tidak dapat dideteksi**
    - **Diprogram agar dapat menghancurkan dirinya sendiri sebelum terdeteksi**
    - **Untuk tujuan proteksi**
    - **Untuk tujuan sabotase**

BOMB

- **Sejenis Trojan Horse**
- **Seringkali digabung dengan virus**
- **Bekerja berdasarkan tanggal, jam atau kondisi tertentu**
- **Ada 2 macam bomb : time dan logic**
- **Yang bekerja berdasarkan waktu tertentu disebut bomb (bom waktu)**
- **Yang bekerja berdasarkan kejadian/kondisi tertentu disebut logic bomb (bom logik)**
- **Contoh**
    - **Virus Michel Angelo, akan meledak bomnya setiap tanggal 6 Maret**
    - **Virus CIH, akan menghapus Flash ROM setiap tanggal 27 April**

TRAP DOOR (atau BACK DOOR)

- **Suatu teknik yang digunakan oleh si programer untuk masuk ke suatu sistem**
- **Merupakan jalan rahasia untuk masuk ke suatu sistem**
- **Fungsinya untuk memberikan kepada si programer untuk masuk ke suatu sistem lewat "pintu belakang"**
- **Kadangkala programer membiarkan trap door di dalam program untuk pengentasan program atau memonitor suatu operasi.**

SPOOF

- **Nama umum yang diberikan untuk program yang melakukan suatu trik dengan memberikan hak-hak istimewa kepada user.**
- **Contohnya : Trojan Horse Login**

BACTERIA

- **Suatu program yang tidak melakukan apapun, tetapi memperbanyak dirinya sendiri**
- **Biasanya beralokasi di memori, disk atau media penyimpanan lainnya**

RABBITS

- **Nama lain dari program yang memproduksi dirinya sendiri dengan cepat sekali**

CRABS

- **Suatu program yang menyerang/mengganggu tampilan data di layar monitor**

CREEPERS

- **Suatu program, seperti worm, yang menyebar dari terminal ke terminal lainnya di dalam jaringan ARPANET (1970an) sambil menampilkan pesan "I'm the crreper, catch me if you can' sampai nantinya program ini dibasmi** oleh **"The Reaper"**

SALAMIS

- **Suatu program yang menyerang nilai-nilai uang dari file transaksi di bank, terutama nilai pecahan**
- **Nilai pecahan (sen) dari bunga diambil dan dipindahkan ke rekening orang lain**

PETUNJUK UNTUK PERLINDUNGAN TERHADAP PROGRAM YANG BERSIFAT JAHAT

- **Boot dengan disket (jangan dari Hard Disk) dikenak, baik dan diprotek.**
    - **Bila harddisk terkena virus, maka untuk proses booting sebaiknya menggunakan disket.**
- **Install software dengan menggunakan yang aslinya**
    - **Sebaik mempunyai sofware yang asli, jangan yang bajakan.**
    - **Software bajakan tidak dijamin bebas dari virus**
- **Simpan software asli pada tempat yang aman**
- **Jangan gunakan software yang dipesan bila tiba dalam keadaan terbuka**
- **Jangan menginstal software yang dipinjam dari kantor ke komputer di rumah**
- **Install hanya sofware yang dibutuhkan saja.**
- **Hati-hati dengan program baru yang bersifat public-domain dan shareware.**
    - **Software semacam ini yang didapat dari internet, tidak dijamin bebas dari virus.**

- **Jangan pinjamkan software ke orang lain tanpa persetujuan Administrator**
- **Jangan menjadi pencoba pertama suatu program**
    - **Untuk menghindari bila terjadi hal yang tidak diinginkan.**
- **Bila terpaksa, periksa program ini dengan serum**
    - **Gunakan serum produksi luar negeri dan dalam negeri**
    - **Seringkali serum produksi luar negeri tidak dapat menghapus viru-virus lokal, begitu pula sebaliknya**
- **Pastikan backup seluruh data**
    - **Proses backup lakukan setiap hari**
- **Pastikan bahwa data yang dibackup tidak terinfeksi virus**
    - **Gunakan serum untuk memeriksa**

9. Indirect Attact

BAB 4 Keamanan Komputer Didalam Jaringan

1. Encryption

a.

PARITAS (PARITY)

- **Suatu teknik pemeriksaan apakah data yang dikirim antar komputer telah berubah atau tidak**
- **Dapat juga digunakan untuk memeriksa apakah data yang disimpan ke dalam tempat penyimpangan telah berubah atau tidak**
- **Dengan menambah sebuah bit (Parity bit)**

1100101	01100101

- **Ada 2 cara metoda paritas :**
    - **Paritas Genap (Even Parity)**
    - **Paritas Ganjil (Odd Parity)**

PARITAS GENAP

- **Apabila jumlah bit 1 adalah genap, maka paritas bit diberi nilai 0**
- **Apabila jumlah bit 1 adalah ganjil, maka paritas bit diberi nilai 1**

1100101	01100101

PARITAS GANJIL

- **Apabila jumlah bit 1 adalah ganjil, maka paritas bit diberi nilai 0**
- **Apabila jumlah bit 1 adalah genap, maka paritas bit diberi nilai 1**

1100101	01100101

- **Digunakan juga dala komunikasi antar modern**
- **Bila menggunakan paritas genap dan jumlah bit 1 dari data yang diterima adalah ganjil, maka berarti data terebut berubah demikian sebaliknya**
- **Contoh :**
    - **Serangkaian bit yang akan dikirim : 10110011**
    - **Metoda paritas yang digunakan paritas genap : 110110011**

  - **Bila sampai di tujuan adalah : 110110011 maka data dianggap benar**
  - **Bila sampai di tujuan adalah : 111111011 maka data dianggap salah**
- **Masalahnya adalah bila yang berubah 2 buah bit**
- **Misalnya bila sampai di tujuan adalah : 110011011 maka data dianggap benar, padahal salah**
- **Ada teknik lain, yaitu rangkaian bit tersebut dibuat dalam bentuk matrik**
- **Paritas bit dihitung secara horizontal dan vertikal**
- **Contoh bila menggunakan paritas genap**

11011	**11011**
01001 bilan sampai ditujuan	**00011 maka data dianggap salah**
10100	**10100**
10110	**10110**

CHECK SUM

- **Dapat juga digunakan sebagai pemeriksaan dari suatu data yang dikirim atau yang disimpan, apakah telah berubah atau tidak.**
- **Dengan menjumlahkan seluruh karakter yang dikirim atau yang disimpan, lalu dimodulus suatu bilangan.**
- **Contoh :**
  - **Bila ada sebuah string mau dikirim, misalnya "ABC"**
  - **Setiap karakter (kode ASCII) diakumulasikan, sehingga didapat suatu nilai**
  - **Nilai ini akan dikirim bersamaan dengan string "ABC"**
  - **Setelah sampai di tujuan, string "ABC" ini akan dihitung kembali dan dibandingkan dengan nilai tersebut.**
  - **Bila hasilnya sama, maka data dianggap benar, tapi bila hasilnya beda maka data yang dikirim dianggap salah.**
- **Masalahnya adalah bila data yang akan dikirim atau disimpan sangat besar, maka nilai check sum akan besar sekali.**
- **Untuk menghindari nilai yang benar ini, maka nilai check sum itu dimodulus dengan suatu bilangan.**
- **Biasanya 256 (8-bit), 65536 (16-bit)**

- **Bila dimodulus dengan 356, maka check sum akan berukuran 8-bit**
- **Bila dimodulus dengan 65536, maka check sum akan berukuran 16-it**

CHECK DIGIT

- **Suatu teknik pemeriksaan apakah data yang dimasukan sah atau tidak**
- **Check digit didapat dari menjumlahkan seluruh karakter, lalu dimodulus suatu biangan.**
- **Biasanya bilangan modulusnya adalah bilangan prima**
- **Check digit biasanya ditambahkan pada akhir data yang dimasukan**
- **Biasanya digunakan pada NIM, Nomer Account Bank, Nomer Kartu Kredit, dll**
- **Contoh**

3095062141
345-1369022

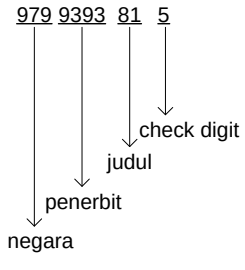
- **Contoh pada Nomer Account Bank**
- **Misalkan ada sebuah Nomer Rekening 001-034410**
- **Angka 0 terakhir merupakan check digit**
- **Contoh cara menghitung check digit.**

0 * 16 (2^4) = 0
3 * 8 (2^3) = 24
4 * 4 (2^2) = 16
4 * 2 (2^1) = 8
1 * 1 (2^0) = 1 +
49

- **Bilangan pem-modulusnya adalah 7**
- **Nilai 49 dimodulus dengan 7 = 0**
- **Sehingga nomer rekeningnya menjadi : 001-034410**

Contoh Check Digit dalam ISBN
Check digit ini tujuannya untuk memeriksa atau menguji validitas angka. Apabila angka tersebut dimasukkan tidak sesuai dengan angka aslinya maka angka akan dimunculkan sebagai hal yang salah.

Cara kerja check digit ini adalah:
Nomor ISBN yang ditetapkan terdiri dari empat kelompok dengan total digit sebanyak 10 digit, yang masing-masing dapat dipisahkan oleh tanda hubung atau spasi.



Kelompok angka pertama (tiga angka pertama) adalah nomor yang diberikan untuk suatu Negara. Angka untuk Indonesia adalah 979.
Kelompok angka kedua adalah kode penerbit.
Kelompok ketiga adalah nomor judul.
Kelompok terakhir terdiri dari satu check digit mulai dari 1 sampai dengan X yang menunjukkan angka sepuluh.

Untuk mengetahui apakah nomor ISBN tersebut sah (valid) maka digit pertama hingga kesepuluh masing-masing dikalikan dengan angka 10, 9, 8 dan seterusnya sampai angka 1. Untuk dapat dikatakan sah maka jumlah hasil perkaliannya harus habis dibagi sebelas.

Contoh hasil perhitungan dengan check digit ISBN adalah:

9	7	9	9	3	9	3	8	1	5		
10	9	8	7	6	5	4	3	2	1		
90	63	72	63	18	45	12	24	2	5	X	= 394

394 dibagi 11 = 35 sisa 9. Karena angka 394 tidak habis dibagi sebelas maka nomor ISBN ini tidak sah. Untuk mendapatkan nomor ISBN yang sah maka check digitnya harus diganti dengan nilai yang bila dijumlah nilainya habis dibagi sebelas.
Untuk penyelesaian contoh diatas adalah:
Lihat sisa dari jumlah hasil perkalian 394 adalah 9, supaya jumlah hasil perkaliannya habis dibagi sebelas maka kekurangannya adalah 11 – 9 = 2.
Nilai ini kemudian ditambahkan ke jumlah hasil perkalian mula-mula: 394 + 2 = 396 sehingga jumlah hasil perkaliannya menjadi 396.
396 dibagi 11 adalah 36 sisa 0 jadi karena 396 habis dibagi 11 maka supaya nomor ISBN menjadi sah, angka check digit harus ditambahkan 2 juga.

- **Contoh**

5439 7280 0153 3142
1234 5678 9abc defg

1 = kode kartu (5 = MC, 4 = Visa)
2,3,4,5 = kode Bank
6,7,8 = ditentukan oleh Bank, misalnya untuk pembagian type gold/silver
9,a = biasanya berisi 00
b,c,d,e,f = Nomer pelanggan CC
g = Check digit

- **Sehingga nomer kartu kredit setelah nomer di atas adalah :**

5439 7280 0153 315x

ENKRIPSI / DEKRIPSI

- **Enkripsi adalah suatu cara untuk mengkodekan data asli yang akan dikirim ke luar dari komputer**
- **Agar orang yang tidak berwenang, tidak dapat membaca data tersebut**
- **Deskripsi adalah suatu cara untuk mengembalikan data yang telah di enkripsi**
- **Banyak metode enkripsi, yang paling sederhana adalah Vernam Clipher**
- **Caranya :**
- **Data asli (Plain Text) diubah ke dalam bentuk biner**
- **Dikenal operasi XOR dengan kunci (Key Text)**
- **Hasilnya disebut Cipher Text**
- **Contoh :**
- **Data asli :** BUDI LUHUR

B – 01000010 **L – 01001100**
U – 01010101 **U – 01010101**
D – 01000100 **H – 01001000** ⇐ **Kode ASCII**
I – 01001001 **U – 01010101**
<blank> - 00100000 **R – 01010010**

- **Kunci :** 1234567890

1 – 00110001 **6 – 00110110**
2 – 00110010 **7 – 00110111**
3 – 00110011 **8 – 00111000** ⇐ **Kode ASCII**
4 – 00110100 **9 – 00111001**
5 – 00110101 **0 – 00110000**

- **Tiap-tiap karakter dari data asli di XOR dengan tiap-tiap karakater dari kunci**
- **Caranya : tiap-tiap bit dari sebuah karakter dari data asli di XOR dengan tiap-tiap bit dari karakater kunci**

B --> 01000010
1 --> 00110001 xor
s --> 01110011

U --> 01010101

2 --> 00110010 xor

g --> 01100111

D --> 01000100

3 --> 00110011 xor

w --> 01110111

I --> 01001001

4 --> 00110100 xor

} --> 01110101

dst….

KOMPRESI

- **Berguna untuk memanfaatkan file**
- **Banyak algoritma yang digunakan untuk mengkompres data, antara lain : Ascii (?), Huffman, Lempel-Ziv dan kombinasinya dll.**
- **Metoda ASCII digunakan pada file teks dengan cara menghilangkan bit ke-8 dari setiap bytenya. Pada file teks, bit ke-8 dari setiap bytenya pasti 0**
- **Contoh : String : ABCD (ada 32 bit)**

A --> 0**1000001**
B --> 0**1000010** ⟸ **Kode ASCII**
C --> 0**1000011**
D --> 0**1000100**

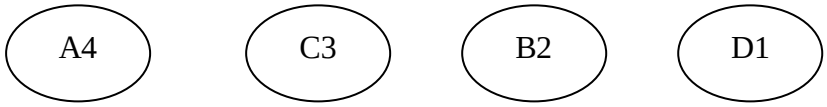
- **Bit yang dicetak tebal (bit ke-8) dihilangkan, sehingga menjadi :**

10000011000010100000111000100 (28-bit)

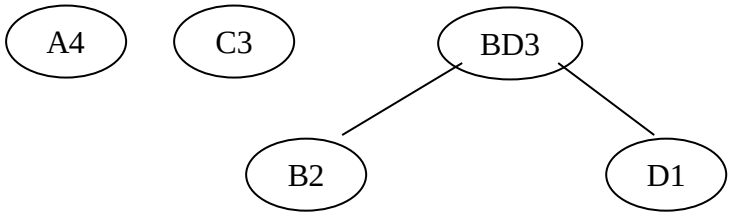
KOMPRESI

- **Metoda Huffman lebih baik dibanding dengan metoda diatas**
- **Jumlah karakter yang sama dihitung**
- **Contoh : String ABCDACCABA (ada 80-bit)**
- **A – ada 4 buah**
- **B – ada 2 buah**
- **C – ada 1 buah**
- **D – ada 1 buah**

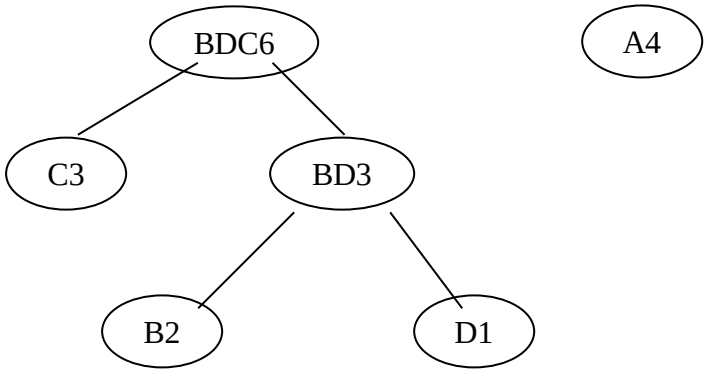
- **Urutan karakter tersebut dari jumlah yang besar ke jumlah yang kecil**



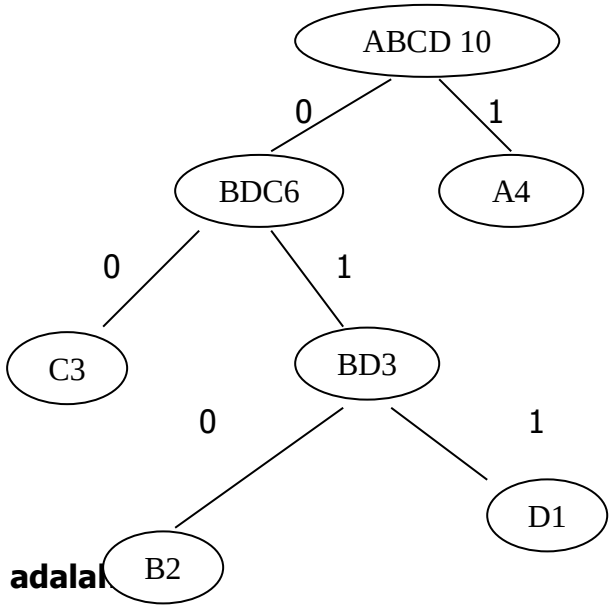
- **Gabungkan 2 yang terkecil, lalu urutkan kembali dari besar ke kecil**



- **Gabungkan 2 yang terkecil, lalu urutkan kembali dari besatr ke kecil**



- **Gabungkan 2 yang terkecil, lalu urutkan kembali dari besar ke kecil**



- **Hasilnya adalah**

A dapat diwakili dengan bit 1
B dapat diwakili dengan bit 010
C dapat diwakili dengan bit 00
D dapat diwakili dengan bit 011

- **Sehingga hasil kompresnya menjadi :**

1010000111000010101 (19-bit)

2. Cryptographic

3. Threats in Networks

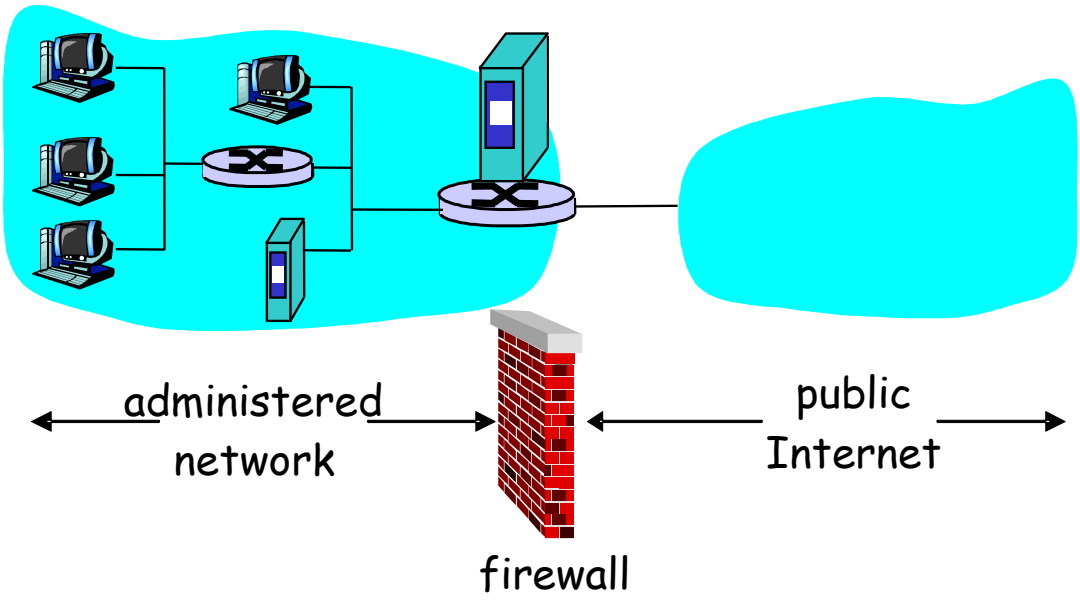
4. Network Security Control

5. Firewalls

Firewalls

- **Basic problem – many network applications and protocols have security problems that are fixed over time**
  - Sulit untuk implementasi pd tingkat users dan sejumlah host yg banyak (control & managed)
  - Solution
    - Administrators limit access to end hosts by using a firewall
    - Firewall is kept up-to-date by administrators
- **Firewall**
  - Router diprogram khusus yg membatasi "site" dan eksternal network
    - Router => connect & forward paket
    - Filter => membatasi paket yang dapat di forward (drop)

Firewall
isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.

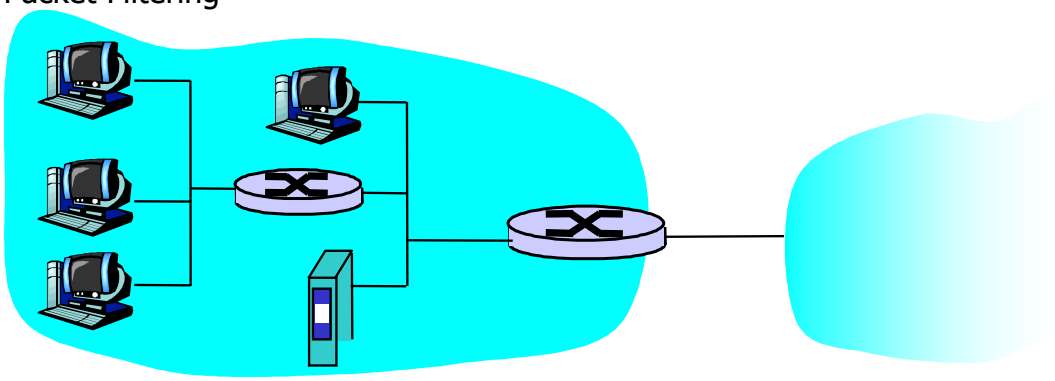


- **Contoh:**
  - Firewall membuang paket IP dgn address tertentu (source, destination) atau TCP port number (services yg dibatasi)
- **A firewall is like a castle with a drawbridge**
  - Hanya satu titik akses ke jaringan internal
  - This can be good or bad (Why?)
- **Can be hardware or software**
  - Ex. Some routers come with firewall functionality

Firewall Types

- **Packet Filtering**
- **Application Level Firewalls**
  - Tingkat aplikasi, sering disebut sbg proxy server.
  - Tidak ada hubungan langsung antara client & server.
  - Hanya firewall/proxy yg ter-expose ke pihak eksternal.
- **Stateful Inspection Firewalls**
  - Melakukan tracking status dan konteks dari data paket.
  - Pemeriksaan paket yg diterima apakah sesuai dgn konteks koneksi yg ada (list address yg valid)
- **Dynamic Packet Filtering Firewalls**

Packet Filtering



- **Internal network connected to Internet via router firewall**
- **Router filters packet-by-packet, decision to forward/drop packet based on:**
  - source IP address, destination IP address
  - TCP/UDP source and destination port numbers
  - ICMP message type
  - TCP SYN and ACK bits

Application Gateway

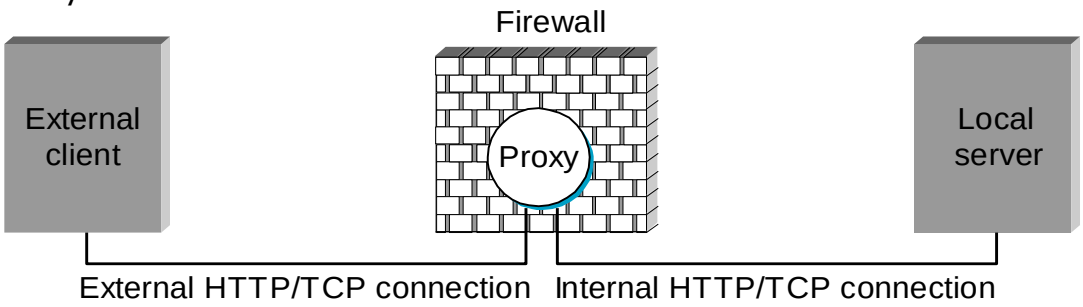
- **Proxy:**
  - Istilah umum pd teknik jaringan => proses yang berada antara client dan server proses.

- Dari sisi client => proxy mewakili server
  Dari sisi server => proxy mewakili client
- Umumnya proxy => terkait dengan konteks aplikasi:
  - Mampu melakukan intrepetasi pada tingkat aplikasi (mis. Cache proxy => request file di lokal cache, walaupun URL ke external networks).
- Security: proxy dpt menerapkan (enforce) kebijakan keamanan dalam memberikan services dari suatu aplikasi.

Example

- Misalkan: kebijakan utk membatasi akses ke direktori tertentu (file) di Web-server untuk user tertentu/remote site.
  - Menggunakan filter port 80, tidak efektif karena melakukan blok pd keseruhan akses.
  - Deny utk URL tertentu tidak dapat diterapkan pada "packet filtering".
- HTTP proxy:
  - Remote user establish HTTP/TCP connection to the proxy.
  - Proxy check the URL: allowed/deny for the source host.
  - If allowed, proxy established a second HTTP/TCP connection to the server.
  - If deny, proxy returns error to the remote user.

Proxy: extend connections



Firewall Security Systems

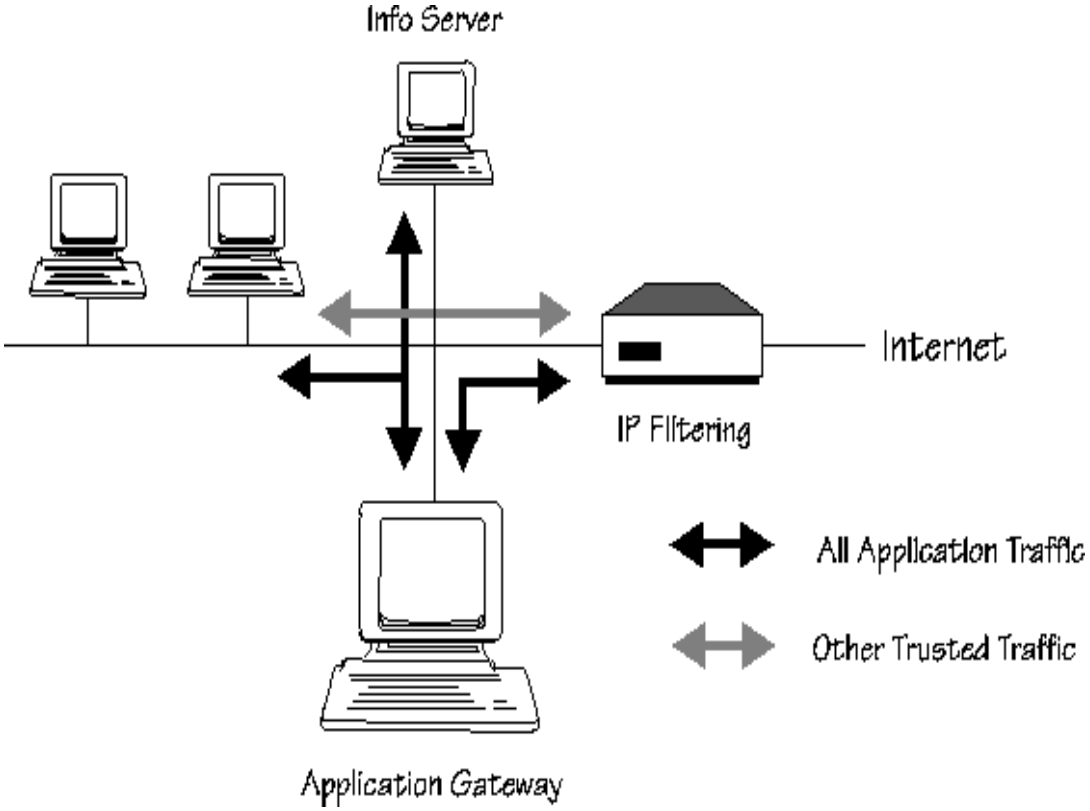
- **Examples of firewall implementations**
  - Screened-host firewall
  - Dual-homed firewall
  - Demilitarized zone (DMZ)

Firewall Implementations

- **Network address translation (NAT)**
  - Internal addresses unreachable from external network
- **DMZ - De-Militarized Zone**
  - Hosts that are directly reachable from untrusted networks
- **Choke, Choke router**
  - A router with packet filtering rules (ACLs) enabled
- **Gate, Bastion host, Dual Homed Host**
  - A server that provides packet filtering and/or proxy services

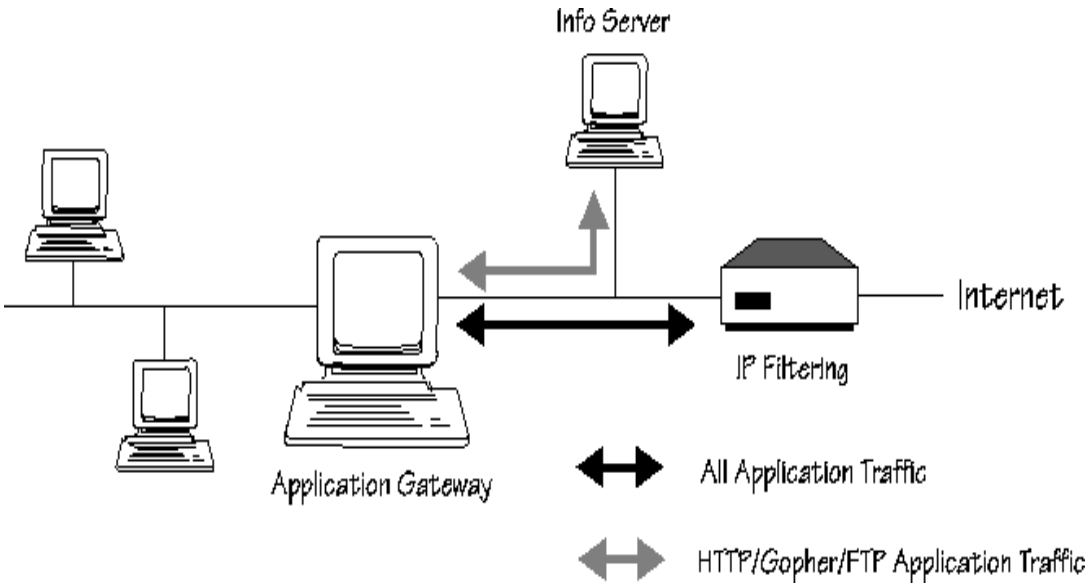
- **proxy server**
  - A server that provides application proxies

Screened-Host Firewall

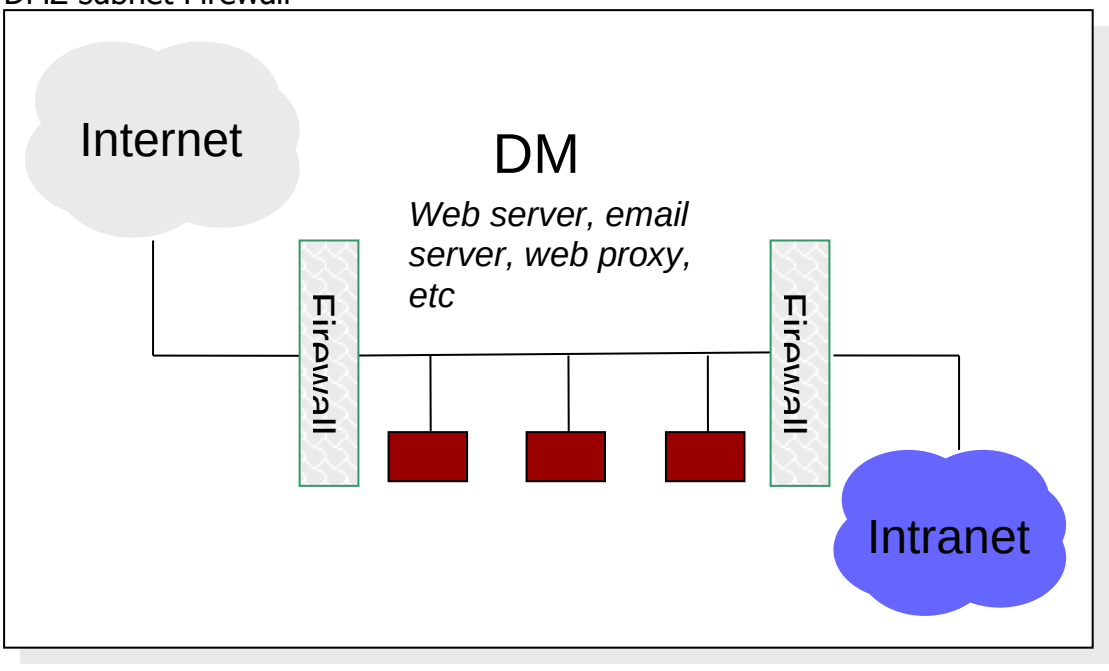


Router: filtering rule: IP untuk server aplikasi (Info Server) diberikan ke proxy (application gateway)

Dual-Homed Firewall



Intranet & Internet dipisahkan oleh
proxy (application gateway)
DMZ subnet Firewall



Limitations

- **Keterbatasan Firewalls**
  - Fokus pd ancaman eksternal => membatasi akses dari luar. Bagaimana dengan user internal?
    - Program dpt masuk melalui "mobile" computer dan berada di internal networks.
    - Email messages => expode pada jaringan internal.

- Wireless LANs => interkoneksi berbagai devices (eksternal komputer), termasuk area jangkauan, dapat menggunakan akses dari remote host melalui firewall.

Intrusion Detection Systems (IDS)

Another element to securing networks complementing firewall implementations is an intrusion detection system (IDS). An IDS works in conjunction with routers and firewalls by monitoring network usage anomalies. It protects a company's information systems resources from external as well as internal misuse.

An IDS operates continuously on the system, running in the background and notifying administrators when it detects a perceived threat. For example, an IDS detects attack patterns and issues an alert. Broad categories of intrusion detection systems include:

- Network-based IDSs—They identify attacks within the monitored network and issue a warning to the operator. If a network-based IDS is placed between the Internet and the firewall, it will detect all the attack attempts, whether or not they enter the firewall. If the IDS is placed between a firewall and the corporate network, it will detect those attacks that enter the firewall (it will detect intruders). The IDS is not a substitute for a firewall, but it complements the function of a firewall.
- Host-based IDSs—They are configured for a specific environment and will monitor various internal resources of the operating system to warn of a possible attack. They can detect the modification of executable programs, detect the deletion of files and issue a warning when an attempt is made to use a privileged command.

Intrusion Detection Systems (IDS)

- **An IDS works in conjunction with routers and firewalls by monitoring network usage anomalies.**
  - Network-based IDSs
  - Host-based IDS
- **Components:**
  - Sensors that are responsible for collecting data
  - Analyzers that receive inputo from sensors and determine intrusive activity
  - An administration console: warning & alarm
  - A user interface

Intrusion Detection Systems (IDS)

- **Types include:**
  - Signature-based:
    - Proteksi dengan melakukan deteksi thp pola (signature) serangan tertentu.
  - Statistical-based
    - Prediksi serangan dengan membandingkan gejala yg lengkap dan "expected behaviour" sistem.
  - Neural networks
    - Self learning?

Types of IDSs include:

- Signature-based—These IDS systems protect against detected intrusion patterns. The intrusive patterns they can identify are stored in the form of signatures.
- Statistical-based—These systems need a comprehensive definition of the known and expected behavior of systems.
- Neural networks—An IDS with this feature monitors the general patterns of activity and traffic on the network and creates a database. This is similar to the statistical model but with added self-learning functionality.
- Signature-based IDSs will not be able to detect all types of intrusions due to the limitations of the detection rules. On the other hand, statistical-based systems may report many events outside of defined normal activity but which are normal activities on the network. A combination of signature- and statistical-based models provides better protection.

IDS: Limitations

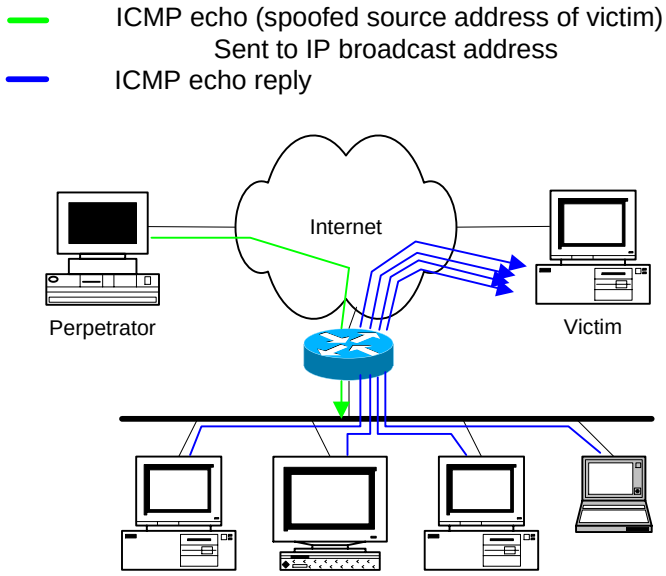
- **Can only detect "pattern" of attack we know about**
  - Sering ancaman yg berbahaya belum ada signaturenya
- **Weaknesses in the policy definition**
  - Bagaimana cara respond, mekanisme review (update)
- **False-positive attacks**
  - Sering sulit membedakan pola attack yg sebenarnya atau kejadian kebelulan => generate false alarm yg banyak dan akhirnya diabaikan oleh operator.
- **Application-level vulnerabilities**
  - Sulit untuk dideteksi, pola seperti keadaan normal

Limitations

An IDS cannot help with the following weaknesses:

- Weaknesses in the policy definition
- Application-level vulnerabilities
- Backdoors into applications
- Weaknesses in identification and authentication schemes

Denial of Service



Tipe Denial of Service

- Yang umum
  - filling up the targets hard drive using email attachments or large transfers
  - sending a message, which resets a targets host's subnet mask.
  - using up all of a targets resources to accept network connections, resulting in additional requests to be denied.

Tipe Denial of Service (2)

- Buffer overflow-when a process receives more data than expected and has no way to deal with the excess data
- SYN attack – when an attacker floods a target with SYNs, but it does not respond when a target system sends an ACK back from those requests. This causes the target system to "time out" while waiting for the proper response.
- Teardrop attack-Consists of modifying the length and fragmentation offset fields in sequential IP packets. The target system becomes confused and crashes after it receives contradictory instructions on how the fragments are offset on these packets.

Tipe Denial of Service (3)

- **Smurf** -Uses a combo of IP spoofing and ICMP to saturate a target network with traffic. It consists of 3 elements. The source site, the bounce site, and the target site. The attacker (source site) sends a spoofed ping packet to the broadcast address of a large network (bounce site). This modified packet contains the address of the target site. This causes the bounce site to broadcast the misinformation to all of the devices on it's local network. All of these devices now respond with a reply to the target system which is then saturated with those replies.

BAB 5 Administrasi Keamanan Komputer

1. Perencanaan Sekuriti

Latar Belakang

- What is Security Management?
  - Q: Apa yang anda lakukan jika enemukan disk dengan label "confidential" berada di meja makan?
  - Q: Apakah anda pernah mendapatkan user ID dan password superisor?
  - Q: Apakah orang luar dapat menggunakan PC dan mencoba log-on ke sistem komputer?
  - Q: Apa yang harus dilakukan jika laptop perusahaan hilang?
  - Q: Apa yang harus dilakukan jika saya ingin mengirimka data "confidential" ke kantor cabang melalui e-mail?
- Security Management
  - Proses manajemen dalam melindungi informasi dan IT Services pada tingkatan keamanan tertentu.
  - Identifikasi aset dan pengembangan keamanan dalam implementasi kebijakan, standard, guidelines dan prosedur

- ❑ Praktik manajemen: analisa resiko dan klasifikasi data/aset TI

Security Management: Issues

- Security Management IT => part of manager's job
  - ❑ Bertanggung-jawab dalam melindungi insiden keamanan
  - ❑ Berhubungan dengan kebijakan/strategi dan operasional => bagian dari quality (assurance) management
- Issues :

- Insiden: event yang dapat terjadi baik disengaja atau tidak yang merugikan nilai dari informasi
- Meniadakan insiden? Sulit dilakukan!
  Mencapai "acceptable level" dari resiko.
- Faktor penting perlindungan nilai dari informasi:
  Kerahasiaan, Integritas dan Ketersediaan informasi

Information Security

- Information security merupakan metode & teknologi untuk melindungi informasi:
  - Confidentially (privacy),
  - Integrity, and
  - Availability
- Kategori utama: Big Three (C.I.A)

- Tolak ukur terhadap: perlindungan (safeguard), ancaman (threat), kerawanan (vulnerability) dan proses manajemen keamanan.

Confidetiality (Kerahasiaan)

- What information needs to be kept secret?
- Kerahasiaan:

- Pencegahan terhadap usaha yang disengaja atau tidak yang melanggar otorisasi untuk mengakses/menyebarkan informasi

- How much protection is needed?
- For how long must the information be kept secret?

Integrity (Keutuhan)

- Information that cannot be trusted is worse than useless – it costs money and time to create and store, but provides no benefit.
- Integrity:
  - ❑ Pencegahan terhadap modifikasi data oleh orang yang tidak berhak atau perubahan yang tidak di-otorisasi.
  - ❑ Konsistensi data/informasi: eksternal dan internal.
  - ❑ Who create/send the information?
  - ❑ Can we prove who create the data?
  - ❑ We know the information is not changed or altered by "unauthorized personnel"

Availability (Ketersediaan)

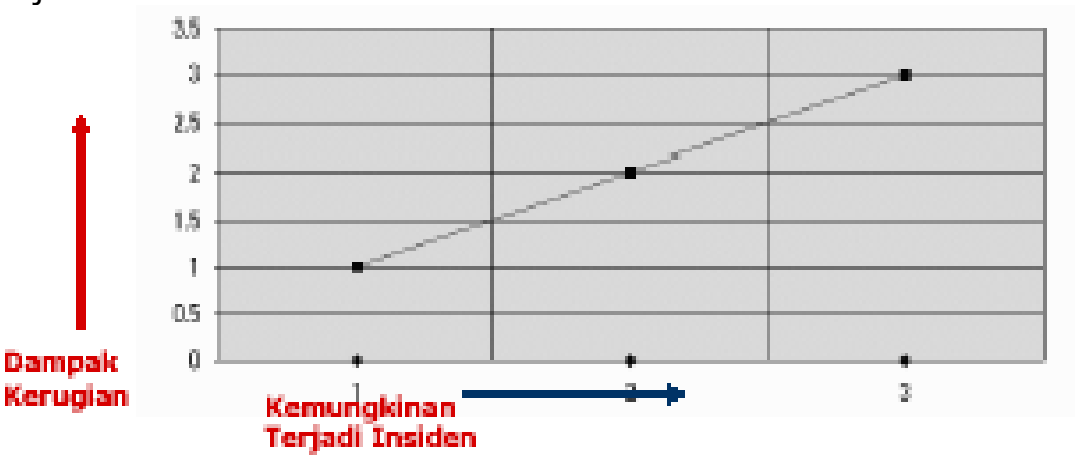
- Information which is not available when required is of no use, even if its confidentiality is secure and its integrity intact
- Availability:
  - ❑ Menjamin informasi/services tetap ada saat diperlukan
- What information must we have readily available?

- How readily must be able to access the information?
- Days?, Hours?; Minutes or seconds?

Important Concepts

- Identification
- Authentication
- Accountability
- Authorization
- Privacy
- Non Repudiation

Objectives

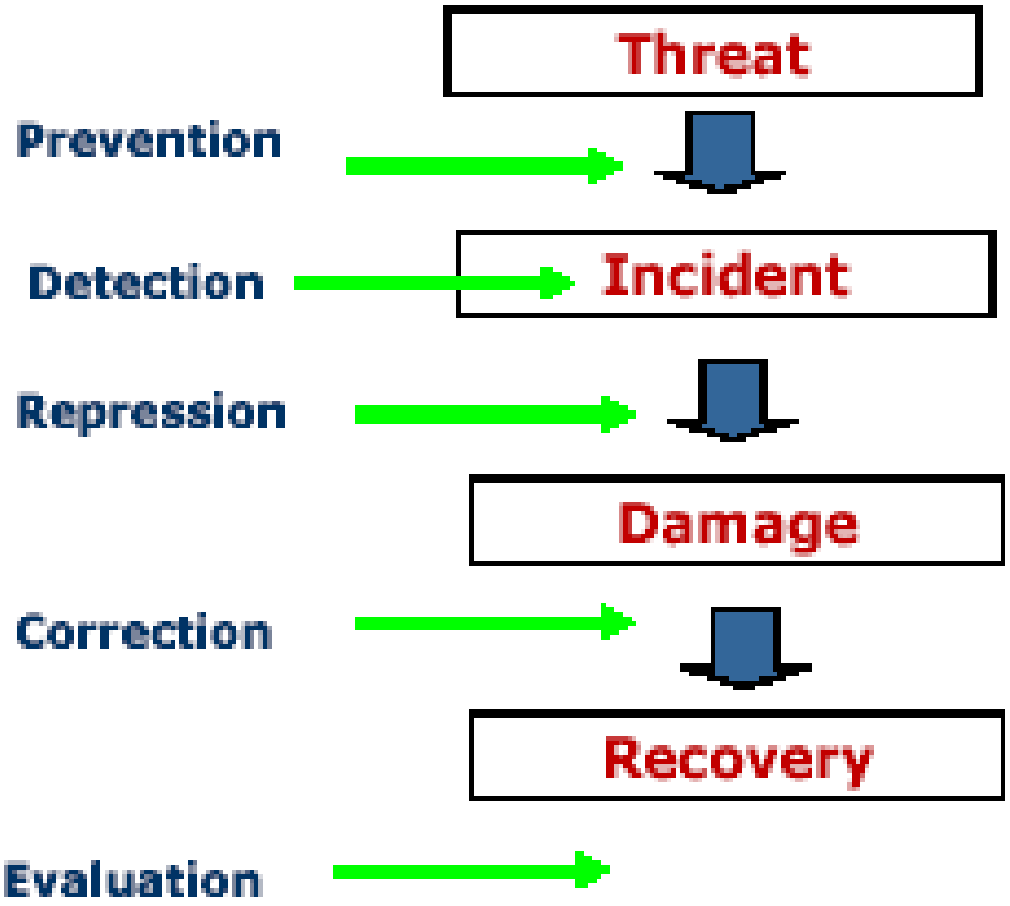


- Security Controls:
  - Sulit untuk ancaman dan dampak kerugian
  - Feasible: mengurangi atau menurunkan dampak kerugian maupun kemungkinan terjadi insiden
  - Sebagai contoh: objektif dari security control dapat menurunkan matrix diatas dari titik 3, ke titik 2 atau ke titik 1.
  - Matrix ini dapat digunakan untuk melakukan evaluasi penerapan security control.

Security Measures (1)

- Tindakan Keamanan
  - Tidak semua informasi sama penting/bernilai => perlu klasifikasi jenis aset (informasi + services) yang perlu dilindungi.
  - Manajemen: pertimbangan faktor cost (waktu, SDM dan biaya) dalam melindungi informasi
  - Required resources vs tingkat proteksi yang diperlukan
- Insiden => Tindakan Keamanan yang diperlukan
  - Mencegah dan menangani insiden yang dapat terjadi pada setiap tahapan

Security Measures (2)



Discussion

- Berikan contoh tindakan keamanan dalam kategori?
  - Ancaman
  - Kerawanan
  - Resiko
  - Deteksi
  - Represi (pengurangan)
  - Pencegahan/Perbaikan

Example: Threat

Table 3-1 Relationship of Threat Agents, Vulnerabilities and Risks

Threat Agents	**Can Exploit This Vulnerability**	**Resulting in This Risk**
Virus	Lack of antivirus software	Virus Infection
Hacker	Powerful services running on a server	Unauthorized access to confidential information
Users	Misconfigured parameter in the operating system	System malfunction

Fire	Lack of fire extinguishers	Facility and computer damage, and possibly loss of life
Employee	Lax access control mechanisms	Damaging mission-critical information
Contractor	Lax access control mechanisms	Stealing trade secrets
Attacker	Poorly written application	Conducting a buffer overflow
Intruder	Lack of security guard	Breaking windows and stealing computers and devices
Employee	Lack of auditing	Altering data inputs and outputs from data processing applications
Attacker	Lack of stringer firewall settings	Conducting a denial of service attack

Classification

- Klasifikasi informasi/data
  - Sesuai dengan sifat organisasi: sensitivitas, dampak kerugian yang dapat ditimbulkan.
  - Penentuan klasifikasi data penting untuk menentukan kontrol akses dan menjamin data yang penting aman.
- Contoh DoD – pemerintah mempunyai klasifikasi sbb:
  - Top Secret
  - Secret
  - Confidential
  - Unclassified

Classification: General

- Klasifikasi yang umum:
  - Confidential: rahasia, internal use only; kerahasiaan merupakan hak dan kritis untuk operasi dan strategi bisnis perusahaan. Sering mempunyai dampak langsung pada bisnis atau masalah hukum, jika tidak dilindungi.
  - Private: informasi yang hanya untuk akses internal saja. Distribusi keluar dapat menimbulkan kerugian besar dan kredibilitas perusahaan.
  - Sensitive: perlu proteksi terhadap akses dan perubahan yang tidak ter-otorisasi.
  - Public: informasi umum, semua data yang tidak masuk dalam kategori di atas.

Classification: Roles

- Peranan (roles) dalam prosedur klasifikasi
  - Owner: pemilik data/informasi (mis. Manajer dari bisnis unit)
    - Tanggung-jawab akhir terhadap proteksi data/informasi
    - Paling mengetahui dalam menentukan klasifikasi data/informasi

- Custodian
  - Penjaga/proteksi data secara operasional
  - Umumnya didelegasikan oleh owner, mis. Staf TI.
  - Contoh operasionil: penyandian data, backup data dsb.
- User: pemakai data/informasi

2. Analisa resiko

Risk Management (1)

- General Approach
  - Threat – possible (event) attacks on the system
  - Vulnerability – weakness that may be exploited to cause loss or harm
  - Risk – probability of loss actually occuring, due to realization of threat.
  - Protection – measure to reduce risk, by reducing the probability of a threat being realized, reducing the loss if a threat is realized or both
- Risk only exist if there is a threat than can exploit the actual vulnerability and the go adversely impact the asset value

Risk

- Risk Category
  - Damage – Result in physical loss of an asset or the inability to access the asset, such as as cutting a network cable
  - Disclosure – Disclosing critical information regardless of where or how it was disclosed
  - Losses – these might be permanent or temporary, including the altering of data or the inability to access data
- Risk Factor
  - Physical damage: i.e. natural disasters, power loss or vandalism.
  - Malfunction: the failure of systems, networks, or peripherals.
  - Attacks: inside or outside, virus, i.e. unauthorized disclosure,
  - Human or Application errors: accidental incidents

Risk Analysis (1/3)

- Proses:
  - Melakukan analisa resiko, dan justifikasi cost/benefit jika dilakukan proteksi.
  - Kuantifikasi (besaran, benchmark) – dampak ancaman jika terjadi.
  - Implementasi dan review proteksi
- Definisi & Terminologi:
  - Asset – resource, proses, produk, infrastruktur TI yang perlu dilindungi. Ancaman terhadap asset dapat memberikan dampak terhadap C.I.A dari sistem informasi.
  - Exposure Factore (EF) – presentase kerugian jika insiden ancaman terjadi pada asset tertentu. Misalkan presentase kecil jika hanya satu modul software yang rusak, tapi besar jika mencakup semua software di server.

Risk Analysis (2/3)

- Quantitative
  - Pendekatan secara finansial: nilai ($) dlm melakukan analisa resiko dan cost

- Qualitative
  - Pendekatan menggunakan "scoring system": rank ancaman dan efektivitas "counter measures" relatif terhadap sistem & lingkungannya.
- Analisa kuantitatif:
  - Lebih sulit dilakukan
  - Dapat mendukung perencanaan budgets dan mampu memberikan informasi kepada manajemen

Risk Analysis (3/3)

- Identifikasi asset-asset perusahaannya
- Berikan nilai pada asset
- Identifikasi resiko dan ancaman yang langsung terkait dengan setiap asset
- Estimasi potensial loss dari resiko atau ancaman
- Estimasi berapa sering kemungkinan munculnya ancaman
- Hitung biaya resiko
- Rekomendasi ukuran atau aktivitas yang muncul

Single Loss Expectancy (SLE)

- Kerugian financial yang muncul jika terjadi sekali (1) bencana
- SLE = Asset Value x Exposure Factor
  - Exposure Factor: 0%-100%, yakni besarnya prosentasi kerugian yang diderita dalam satu bencana
- Misal:
  - Dalam suatu bencana banjir, akan menyebabkan ATM terendam di 30% lokasi di Jakarta. Replacement cost ATM = Rp. 100 juta/ATM. Total ATM yang dimiliki 200 unit
  - SLE = Rp. 100 juta x 30% x 200 = Rp. 6 milyar

Threat Frequency

- Seberapa sering ancaman itu terjadi? Misalnya:
  - Kebakaran besar: 1 dalam 40 tahun
  - Banjir besar: 1 dalam 6 tahun
  - System crash: 1 dalam 6 bulan
  - Unauthorized access: 2 dalam bulan
- Dihitung dalam Annualized Rate of Occurance (ARO):
  - Kebakaran: 1/40
  - Banjir besar: 1/6
  - System crash: 2
  - Unauthorized access: 2 x 2 = 24

Annualized Loss Expectancy (ALE)

- Annualized rate of occurrence (ARO)
  - On an annualized basis, the frequency with which a threat is expected to occur
- Annualized loss expectancy (ALE)
  - Single loss expectance x annualized rate of occurance = ALE
- ALE = Single Loss Expectancy x Annualized Rate of Occurance
- Contoh:
  - Dalam kasus ATM, SLE = Rp. 6 milyar dan ARO = 1/6, maka ALE = Rp. 6 milyar x 1/6 = Rp. 1 milyar

- Dibaca: "Setiap tahunnya diperkirakan akan ada biaya ATM yang harus diperbaiki/diganti akibat sebesar Rp. 1 milyar"

Cost/benefit analysis

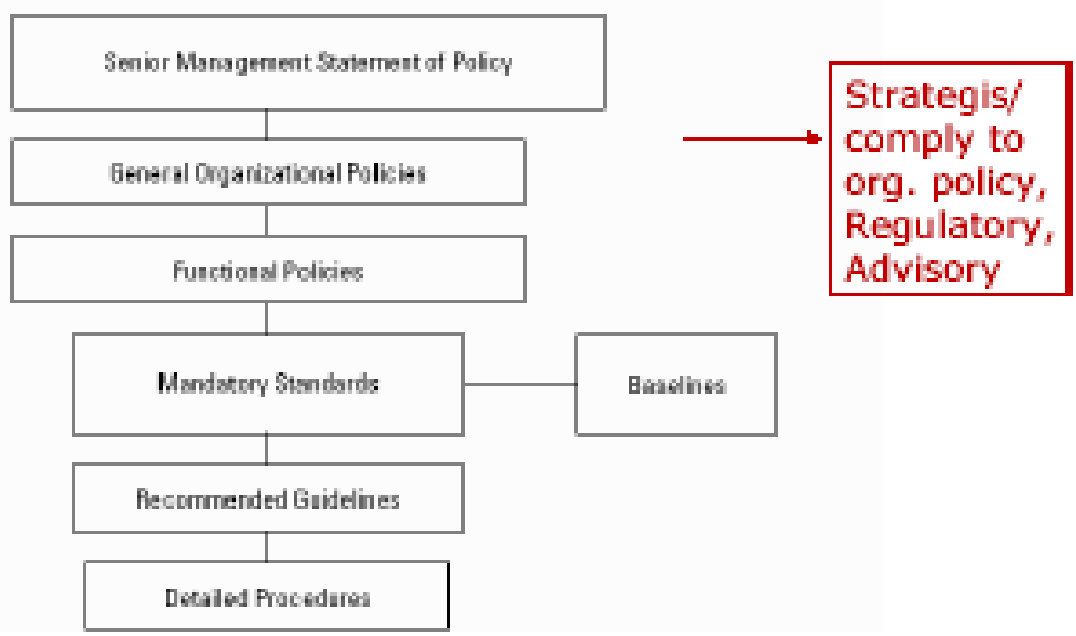
- Cost of a loss
  - Seringkali sulit untuk menentukan secara akurat
- Cost of prevention
  - Jangka panjang / jangka pendek
- Adding up the numbers
  - Output yang berasal dari listing asset di spreadsheet Excel, resiko-resiko dan kemungkinan kehilangan
  - Untuk setiap kehilangan, perlu diketahui kemungkinan, prediksi kehilangan dan jumlah uang yang dibutuhkan untuk mempertahankan keadaan setelah kehilangan

3. Kebijakan keamanan organisasi

Business Perspectives

- Organisasi dan implementasi: tanggung-jawab tugas dsb
  - Traceable to business needs: value of information
- Umumnya disusun dalam bentuk abstraksi:
  - Kebijakan (policy): "which objective we aiming for?"
  - Proses: "What has to happen to achieve those objectives?"
  - Prosedur/standard/guidelines: who does, what and when
- Pendekatan "top-down"
  - Pengembangan mulai dari security policy: "blue print" untuk perencanaan dan implementasi

Policy Hierarchy



Information security policies

- Components of an effective policy:
  - Title
  - Purpose
  - Authorizing individual
  - Author/sponsor
  - Reference to other policies
  - Scope
  - Measurement expectations
  - Exception process
  - Accountability
  - Effective/expiration dates
  - Definitions

No procedures, techniques or methods
Policy is the approach
The spesific details & implementations should be in another document

Information security policies

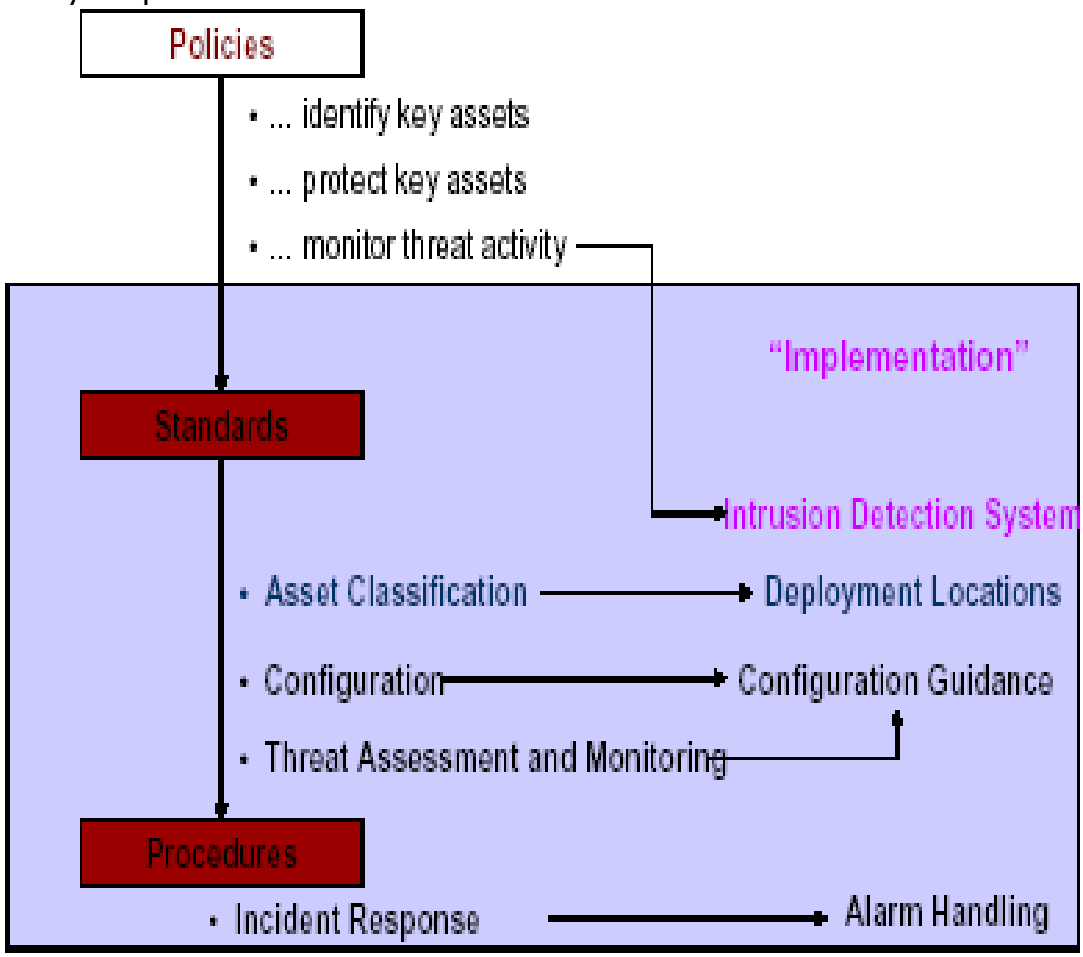
- How to ensure that policies are understood:
  - Jargon free/non-technical language
  - Rather then, "when creating software authentication codes, users must endeavor to use codes that do not facilitate nor submit the company to vulnerabilities in the event that external operatives break such codes", use "password that are guessable should not be used".
  - Focused
  - Job position independent
  - No procedures, techniques or methods
    - Policy is the approach. The spesific details & implementations should be in another document
  - Responsibility for adherence
    - Users must understand the magnitude & significance of the policy. "I thought this policy didn't apply to me" should never be heard.

Standard & Guidelines

- Implementasi policy
- Standard:
  - Terdapat unsur keharusan
  - Petunjuk penerapan dalam lingkup/sistem tertentu
  - Uniform untuk seluruh organisasi dan mencakup spesifik teknologi.
  - Contoh: standard manajemen password, standard firewall dll.
- Guidelines:
  - Rekomendasi dan relatif lebih flexible (evolusi menjadi standard)
  - Contoh: guidelines keamanan password untuk seluruh client dan server.
- Procedures:
  - Rincian tahapan/aksi untuk melakukan task tertentu dikaitkan dengan standard yang akan diterapkan

- Contoh: prosedur perubahan/pembuatan password, prosedur setup firewall

Policy: Implementations



BAB 6 Cryptography

2. Latar Belakang Matematika

Untuk memastikan bahwa data aman maka pengamanan yang dilakukan terhadap data adalah:

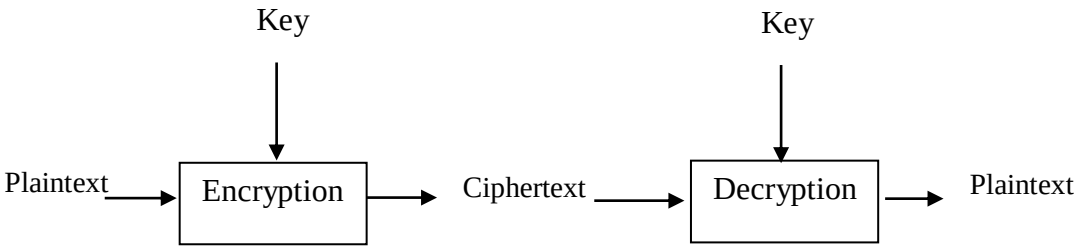
1. Melakukan enkripsi (penyandian) untuk menjamin informasi rahasia (confidentiality) yaitu monitoring stok gudang pada aplikas administrasi gudang, administrasi penggajian (payroll).

2. Menggunakan algoritma fungsi hash satu arah untuk menjamin keutuhan (integrity) atas data-data pembayaran yaitu data yang terdapat pada aplikasi akuntansi seperti general ledger, account payable, account receivable, dan laporan keuangan.
3. Menggunakan password atau sertifikat digital untuk menjamin identitas dan keabsahan (authenticity) dari pihak-pihak yang melakukan transaksi yaitu dalam pembuatan purchase order, pembuatan delivery order, pembuatan report stok opname yang ada dalam aplikasi administrasi gudang serta pembuatan sales order, pembuatan laporan penjualan yang ada dalam aplikasi administrasi pemasaran dan penjualan.
4. Menggunakan tanda tangan digital untuk menjamin keotentikan data transaksi agar transaksi dapat dijadikan sebagai barang bukti yang tidak bias disangkal (non-repudiation) yaitu yang terdapat pada aplikasi administrasi gudang, aplikasi pemasaran dan penjualan, aplikasi administrasi keanggotaan.

Semua yang bersifat mengamankan data menggunakan metode tertentu merupakan inti dari cryptography yaitu menjamin kerahasiaan (confidentiality) informasi dengan melakukan enkripsi (penyandian). Keutuhan (integrity) atas data-data pembayaran dilakukan dengan fungsi hash satu arah. Jaminan atas identitas dan keabsahan (authenticity) pihak-pihak yang melakukan transaksi dilakukan dengan menggunakan password atau sertifikat digital. Sedangkan keotentikan data transaksi dapat dilakukan dengan tanda tangan digital. Transaksi dapat dijadikan barang bukti yang tidak bisa disangkal (non-repudiation) dengan memanfaatkan tanda tangan digital dan sertifikat digital.

Tujuan dari cryptography adalah mempelajari berbagai metode dan teknik penyembunyian data menggunakan kriptografi. Adapun makna kriptografi adalah: ⋯⋯ + ⋯⋯ = secret + writing. Jadi cryptography: ilmu untuk membuat sebuah pesan menjadi aman Untuk membuat pesan menjadi aman maka diperlukan kunci (key) supaya mempermudah pemakaian dalam mengirim pesan. Karena bila menggunakan algoritma rahasia terdapat kesulitan yaitu harus selalu membuat yang baru setiap kali akan mengirim pesan. Analoginya adalah dalam penggunaan gembok yang menggunakan kode-kode angka untuk membuka atau mengunci gemboknya putar saja kode-kode angkanya ke posisi yang tepat. Jadi kuncinya hanya bisa diputar oleh orang yang tahu urutan kode yang benar.

Proses Kriptografis



Gambar 5.1. Proses Kriptografis

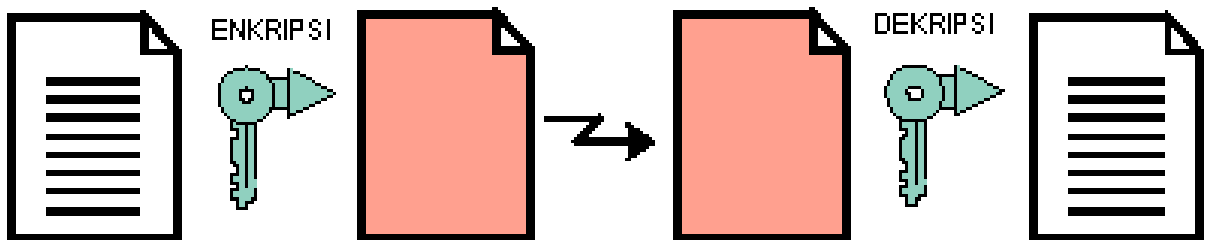
Cipher adalah fungsi matematika yang dipergunakan untuk enkripsi & dekripsi. Enkripsi adalah suatu cara untuk mengkodekan data asli yang akan dikirim ke komputer lain dengan menggunakan kunci (key). Tujuannya adalah agar orang yang tidak berwenang tidak dapat membaca data tersebut. Deskripsi adalah suatu cara untuk mengembalikan data yang telah di enkripsi. Plaintext adalah data asli. Sedangkan Ciphertext adalah hasil dari enkripsi.

Proses kriptografisnya adalah dari data asli (plain text) diubah bentuknya menjadi data acak (cipher text) menggunakan key. Cara ini disebut enkripsi. Data yang sudah di enkripsi dikirim ke orang yang sudah ditentukan bersama dengan kuncinya. Data yang diterima dikembalikan ke bentuknya yang semula dengan menggunakan key yang sudah dikirim bersama. Cara ini disebut dengan dekripsi.

3. Symetric Encryption

Symetric Cryptography

Metode cryptography yang biasa digunakan adalah symmetric cryptography dimana sebuah kunci yang dipakai bersama-sama oleh pengirim pesan dan penerima pesan. Contoh: DES, TripleDES, AES, Blowfish. Dalam pendistribusian kunci rahasia diberikan dalam pesan yang dimasukkan ke dalam amplop yang tidak bisa dibuka.



Gambar 5.2. Symetric Criptography

4. Sistem Enkripsi Public Keys

Public Key Cryptography

Metode cryptography yang dipergunakan adalah public key cryptography. Kegunaan yang mendasar pada public key crytogragraphy adalah :

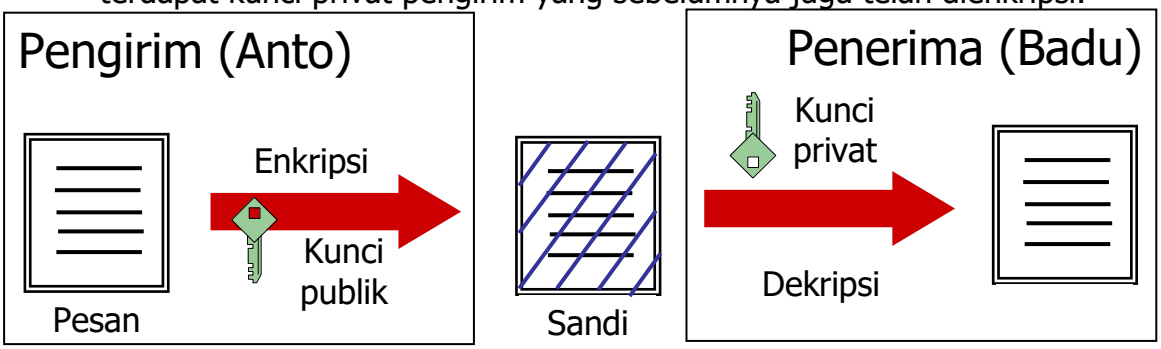
- ☑ Menandatangani pesan
- ☑ Mengirim surat rahasia dalam amplop yang tidak bisa dibuka orang lain

Ada sepasang kunci untuk setiap orang (entitas):

- ☑ kunci publik (didistribusikan kepada khalayak ramai / umum)
- ☑ kunci privat (disimpan secara rahasia, hanya diketahui diri sendiri)

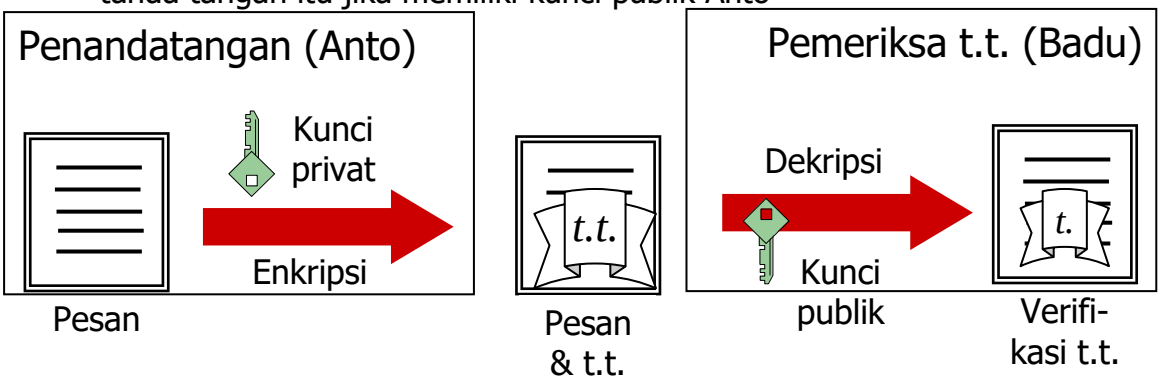
Analoginya adalah:

- ☑ Semua orang bisa (Anto, Chandra, Deni) mengirim surat ke "Penerima" (Badu) dan hanya "penerima" yang bisa membuka surat. Pengirim mengenkripsi pesan menggunakan kunci publik penerima yang didalamnya terdapat kunci privat pengirim yang sebelumnya juga telah dienkripsi.



Membungkus Pesan

- ☑ Hanya pemilik kunci privat (penandatangan, Anto) saja yang bisa membuat tanda tangan digital. Semua orang (Badu, Chandra, Deni) bisa memeriksa tanda tangan itu jika memiliki kunci publik Anto

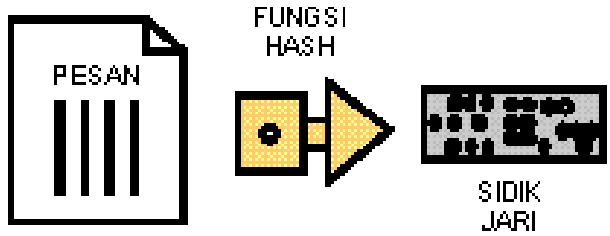


Menandatangani pesan dengan public key cryptography

Fungsi Hash

Fungsi Hash disebut juga sidik jari (fingerprint), message integrity check, atau manipulation detection code untuk integrity-check bila dokumen/pesan yang diubah 1 titik saja, sidik jarinya akan sangat berbeda. Contoh Algoritma Hash adalah Message

Digest (MD) series: MD-2, MD-4, MD-5. 128-bit, dan Secure Hash Algorithm (SHA), termasuk SHA-1. 160-bit

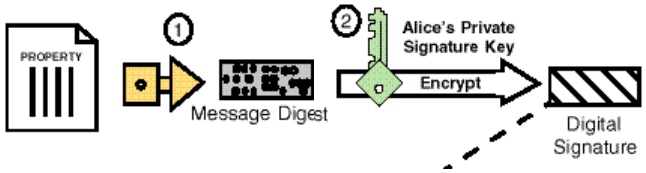


Gambar 5.5. Fungsi Hash

Mekanisme fungsi hash adalah pesan dibubuhi sidik jari dimana sidik jarinya sudah dimanipulasi menggunakan kode pendeteksi tertentu sehingga keabsahannya dapat dipercaya. Fungsi hash ini digunakan untuk pembuatan kontrak perjanjian kerja pegawai maupun perjanjian keanggotaan baru pada PT. MASS-NET. Juga dipergunakan sebagai data pembayaran pada aplikasi akuntansi PT. MASS-NET.

Tanda Tangan Digital

Tanda tangan digital atau digital signature adalah tanda tangan yang telah dienkripsi menggunakan kunci publik seseorang yang sudah memiliki sertifikat digital. Didalam tanda tangan ini sebenarnya terdapat pesan penting dan rahasia yang hanya dapat diketahui bila memiliki kunci kode pendeteksi fungsi hash.



Gambar 5.6. Tanda tangan digital

Sifat tanda tangan digital:

1. Otentik, dapat dijadikan alat bukti di peradilan (kuat)
2. hanya sah untuk dokumen (pesan) itu saja, atau kopinya. Dokumen berubah satu titik, tanda tangan jadi invalid!
3. dapat diperiksa dengan mudah oleh siapapun, bahkan oleh orang yang belum pernah bertemu (dgn sertifikat digital tentunya)

Sertifikat Digital

Sertifikat digital atau yang sering disebut dengan digital certificate berisi kunci public seseorang yang telah mendaftarkan dirinya pada perusahaan sertifikasi. Sertifikat digital ini menyakinkan kepada khalayak umum / ramai bahwa tanda tangan digital yang ada adalah benar merupakan data yang dapat dipercaya. Bahkan dapat dipergunakan sebagai pengganti orang tersebut seperti halnya surat kuasa.
Keuntungan sertifikat digital:

1. bisa membuat "pipa komunikasi" tertutup antara 2 pihak
2. bisa dipergunakan untuk mengotentikasi pihak lain di jaringan (mengenali jati dirinya)
3. bisa dipakai untuk membuat dan memeriksa tanda tangan
4. bisa dipakai untuk membuat surat izin "digital" untuk melakukan aktifitas tertentu, atau identitas digital
5. bisa untuk off-line verification

Transaksi Aman Yang Umum
Transaksi aman yang dipergunakan adalah seperti gambar dibawah ini. Gambar ini mengilustrasikan pengiriman informasi rahasia dari komputer Alice ke komputer Bob yang telah dienkripsi dan bagaimana bob melakukan dekripsi data.

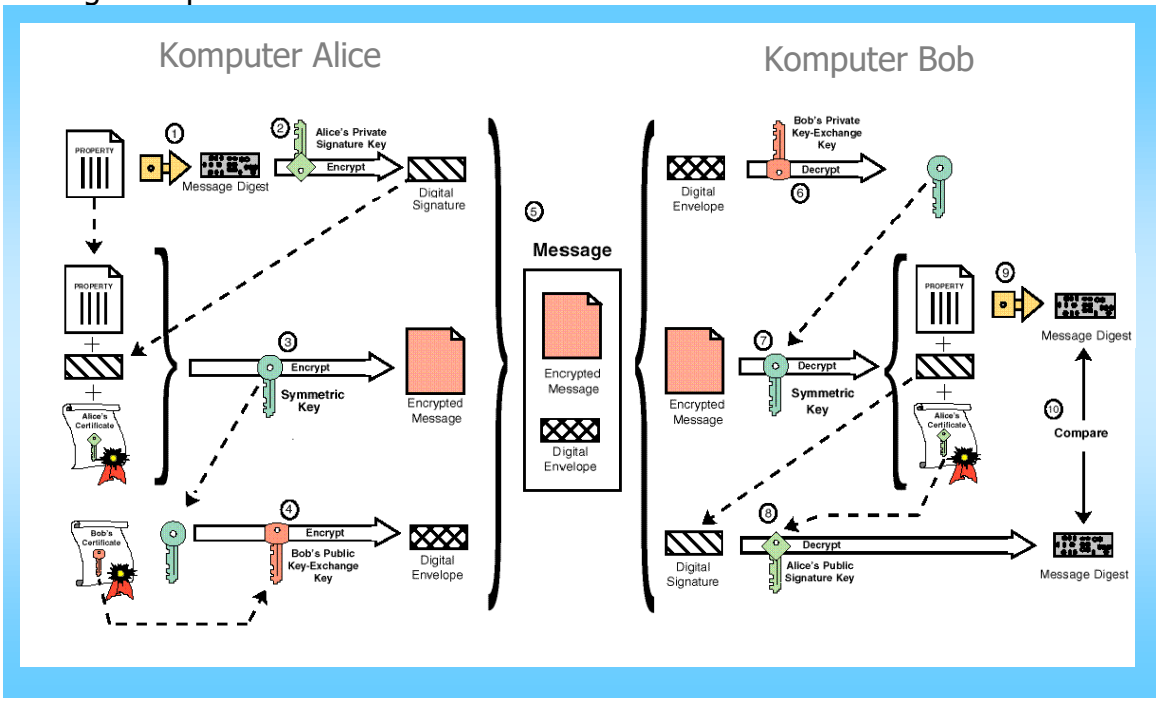
Untuk proses pengiriman dari komputer Alice yaitu:

1. (Property) pesan asli telah dibubuhi sidik jari yang dimanipulasi dengan kode tertentu menggunakan fungsi hash sehingga menjadi message digest.
2. Message digest kemudian dienkripsi menggunakan kunci privat kepunyaan Alice sehingga menjadi tanda tangan digital (digital signature).
3. (Property) pesan asli, tanda tangan digital (digital signature) dan sertifikat digital kepunyaan Alice (Alice's certificate) yang berisi kunci public kepunyaan Alice kemudian semuanya dienkripsi menggunakan kunci simetrik (symmetric key) sehingga menjadi pesan yang terenkripsi (encrypted message).
4. Kunci simetrik (symmetric key) dienkripsi menggunakan kunci publik kepunyaan Bob yang diketahui berdasarkan sertifikat digital kepunyaan Bob (Bob's certificate) sehingga menjadi digital envelope (amplop digital yang tidak dapat dibuka).
5. Pesan yang terenkripsi (encrypted message) dan digital envelope (amplop digital yang tidak dapat dibuka) merupakan pesan (message) yang dikirimkan kepada Bob.

Bob yang menerima pesan kemudian melakukan dekripsi. Adapun prosesnya adalah sebagai berikut:

6. Digital envelope (amplop digital yang tidak dapat dibuka) pertama kali didekripsi menggunakan kunci privat kepunyaan Bob sehigga didapat sebuah kunci. Kunci ini adalah kunci simetrik (symetric key) yang fungsinya untuk membuka pesan yang terenkripsi.
7. Pesan yang terenkripsi (encrypted message) kemudian didekripsi menggunakan kunci simetrik (symetric key) sehingga menghasilkan (property) pesan asli, tanda tangan digital (digital signature) dan sertifikat digital kepunyaan Alice (Alice's certificate).

8. Tanda tangan digital (digital signature) kemudian didekripsi menggunakan kunci public kepunyaan Alice yang berada didalam sertifikat digital kepunyaan Alice (Alice's certificate). Hasilnya adalah message digest.
9. (property) pesan asli didekripsi menggunakan fungsi hash yang telah diketahui oleh Alice dan Bob. Hasilnya adalah message digest.
10. Kedua message digest kemudian dibandingkan kebenarannya. Keabsahan data ini meyakinkan bahwa (property) pesan asli yang dikirim adalah benar dan tidak mengalami perubahan sama sekali.



Transaksi aman yang umum

Transaksi ini dipergunakan untuk mengamankan:

1. Browser, terutama secure website dengan SSL yang dipergunakan khususnya bagi manajer yang menggunakan fasilitas internet dan bagi anggota yang ingin melihat bonus bulanan yang diterimanya.
2. Payment system, SET yang dipergunakan untuk data pembayaran yang ada di PT. MASS-NET yang dilakukan oleh staf keuangan.
3. Secure E-mail (S/MIME, PGP) yang dipergunakan untuk keamanan pada data stok gudang yang biasa dikirim dalam bentuk text kepada supplier bila melakukan pembuatan purchase order.
4. Document signing dan kontrak digital ini sangat penting baik bagi downline (anggota baru) maupun bagi supplier untuk memperpanjang kontrak perjanjian kerjasama.
5. VPN, Intranet yang ada dalam lingkungan PT MASS-NET juga memerlukan pengamanan data khususnya untuk data transaksi.
6. Secure wireless network (termasuk WAP) dipergunakan bagi para manajer, direktur dan komisaris bahkan orang lain yang menggunakan laptop agar tidak sembarangan mengambil data.
7. Smartcard applications dipergunakan sebagai bukti tanda keanggotaan yang sah.

8. Timestamping service dan digital notary dipergunakan pada saat pembuatan purchase order, pembuatan delivery order, pembuatan sales order, kontrak perjanjian kerjasama.

5. Quantum Cryptography

BAB 7 Etika Didalam Keamanan Computer

Tujuan

- Mempelajari berbagai jenis aturan yang terkait dengan kejahatan komputer dan legalitas transaksi elektronik, serta membahas masalah etika dalam dunia komputer.

1. Proteksi terhadap program dan data

Technology Trends

Trend	Impact
Moore's Law: Computing power doubles every 18 months	More organization depend on computers for critical operations
Rapidly declining data storage costs	Organizations can easily maintain detailed database on individuals
Datamining advances	Companies can analyze vast quantities of data gathered on individuals to develop detailed profiles of individuals behaviour
Ease of networking	Copying data from one location to another and accessing data from remote locations will be easier

Do you think this is a problem?

Profiling…

- The use of computers to combine data from multiple sources and create electronic dossier of detailed information on individuals
- What technologies can be used to create information of an individual behavior?
  - credit & debit cards
  - Internet proxies
  - cookies

2. Hukum dan Informasi didalam computer sekuriti

Ethical & Social Impact of Information Systems

- Objective
  - To provide a basic understanding of ethical & social problems in the information society
  - To provide background issues for further discussions on later weeks

Discussion Topics

- Opening topic: the Internet
- Understanding ethics
- Ethics in information society
- Moral dimensions of information systems
  - Information rights
  - Intellectual property
  - Accountability, Liability & Control
  - System Quality
  - Quality of Life

The Internet

- The Internet
- Tell me both pros & cons of the Internet!
- How about cell phones & SMS?

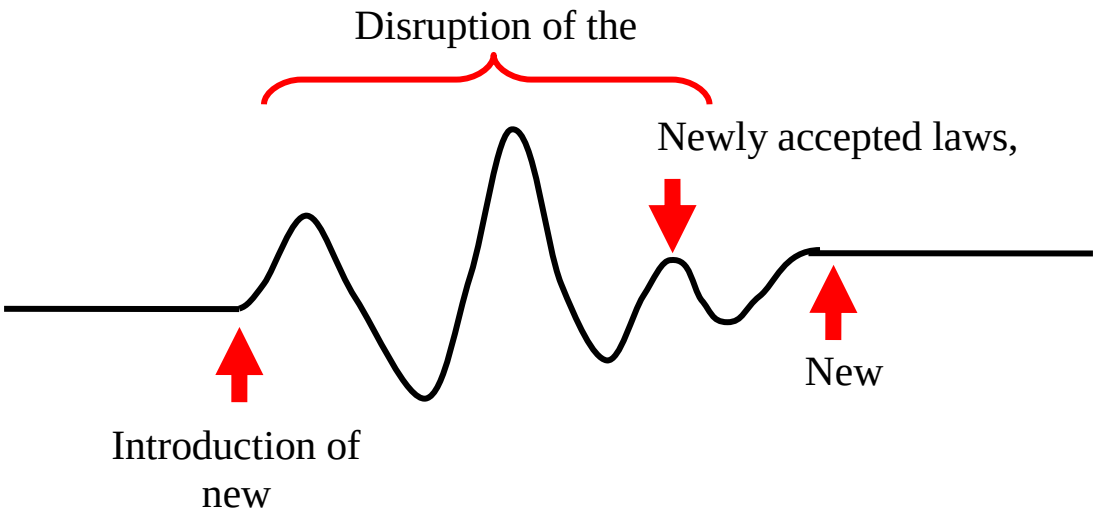
So?

- Technology is a double edged sword

Ethics

- Principles of right & wrong that can be used by individuals acting as a moral agents to make choices to guide their behavior
- IT can be used to achieve social progress (e.g. economic development, healthier environment, better understanding among cultures)
- But IT can also be used to commit crimes!

Equilibrum of the Society



Ethics in an Information Society

- Basic Concepts:
  - **Responsibility**
    - accepting the potential cost, duties, & obligations for the decisions one makes
  - **Accountability**
    - the mechanism to determine who took responsible action, and who is responsible (who took what action)
  - **Liability**
    - the existence of laws that permit individuals to recover the damages done to them by other person

Ethical Analysis of Information Systems

- Computers do not act by themselves. "Impacts" are products of individual or organizational actions/behavior
- Responsibility for the consequence of technology falls to the user of the technology
- "Victims" can recover damages done to them

Ethical Analysis Methodology

- Identify & describe clearly the facts
- Define the conflict dilemma and identify the higher order values involved
- Identify the stakeholders
- Identify the options that you can take reasonably
- Identify the potential consequence of your opinion

Candidate Ethical Principles

- **Golden Rule**. Do to the others as you would do to them. (Do not do to the others) as you (do not want others) to do to you
- **Kant's Categorical Imperative**. If an action is not right for everyone to take, then it is not right for everyone

- **Descartes' rule of change**. If an action can not be taken repeated, then it is not right to be taken in any time
- **Utilitarian principle**. One could put values in rank order an understand the consequence of various courses of action.
- **Risk Aversion principle**. Action taken should produce the least harm or incures the least cost.
- **No "Free Lunch" principle**. Assume that all objects (tangible & intangible) are owned by someone unless there is a specific declaration. Assume the creator wants compensation for this work.

Professional Code of Conduct

- Promulgated by professional associations
  - Doctors
  - Association of Computing Machinery
  - Certified IS Auditors

Some Cases

- Downsizing with technology: employee layoffs
- Electronic profiling at the airport
- Employee monitoring on the Internet
- What do you think?

3. Rights of Employees and Employers

Moral Dimensions of Computers
Privacy
Information Rights

- Privacy:
  - claim of individuals to be left alone, free from surveillance or interference from other individuals, organization or state
- Why do some culture value privacy more than the others?
- Historical background:
  - freedom of religious interpretation
  - America: land of freedom
  - "it is none of your business"

FIB: Fair Information Practice

- Written in 1973 by federal committee
- Based on "mutual interest" between record holder & the individual

FIP Principles (1)

- No personal record systems is secret
- Individuals have the right to access, inspect, review, and amendment to systems that contain information about them
- There must be no use of personal information other than those for which it was gathered without prior consent

FIP Principles (2)

- Managers of information systems are responsible and can be held accountable and liable for the damage done by systems

- Governments have the right to intervene in the information relationships among private parties

Internet Challenges to Privacy

- Record on-line activities: Amazon.com
- Cookies

Spamming

- The practice of sending unsolicited e-mail and other electronic communication
- Options:
  - unsubscribe
  - filter
- Used by marketing companies, the collect e-mails from the Internet:
  - mailing list
  - web pages

Issues

- Do we have to inform customers that we are monitoring their behavior?
- Are we allowed to use health records to screen insurance applicants?
- What do we consider private territory?
- What about secure transmissions & wiretapping? SSL 1028 bit?

Property Rights:

Intellectual Property

- Intangible property created by individuals or corporations that is subject to protections under trade secret, copyright and patent law.
- For instance:
  - Trade Secrets
  - Copyright
  - Patent

Trade Secrets

- Any intellectual work or product used for a business purpose that can be classified as belonging to that business, provided it is not based on information in the public domain
- Protects the main idea, the "engine", the "how it works" of the software
- Requires employees' non disclosure agreement
- When the software is widely used and disassembled, the "engine" could be known by public

Copyright

- Statutory grant that protects creators of intellectual property against copying by others for any purpose for a certain period.
- Books, lectures, dramas, musical composition, computer software
- Intention of copyright laws: creative people receive financial & other benefits from their work.
- Benefit: protection against illegal copying
- Drawbacks: the idea is not protected, only its manifestation

Patents

- A legal document that grants the owner an exclusive monopoly on the ideas behind an invention for several years

- Designed to ensure that inventors of new machines or methods are rewarded for their labor while making wire spread use of their inventions
- Requires originality, novelty & invention
- Strength: monopoly of the underlying ide, while the ide is known to the public
- However, the ide must pass stringent criteria at the Patent Office

Challenges to
Intellectual Property Rights

- Digital media: ease of copying (theft)
- Case: Sim Lim at Singapore
- Allowing citizens to keep up with technology?
- Case: MP3, Napster, Gnutella (source code)
- Web framing

Accountability, Liability & Control

- ATMs of a bank is out of order for one day
- Customers can not withdraw any money
- Who is liable for the loss?
    - The bank
    - The ATM vendor

Managing Risk

- The use of risk management is important
- Service providers must have disaster recovery plan (DRP).
- Also called "Business Continuity Plan" (BCP)
- BCP includes legal matters and customer response guidelines during disaster

Case: Network Service Provider

- Would ISP be liable for:
    - spamming?
    - Trojan horse & Internet virus?
    - Pornography?

4. Software failure

System Quality:
Data Quality & System Errors

- Impossible to create "zero defect" softwares
- The importance of testing (remember debugging & testing in Java?)
- Formal methods: can significantly decrease defects (still can not achieve 0% defect)
- Perfect software >> never be released >> no sales >> no money!

Data Quality

- System should ensure data in the computers are accurate
- Some "computer errors" are actually made by human
- Case: Fraud in Universities

Standards

- Should there be IT Management standards?
- Example:
    - Control Objectives for IT Governance
    - ISO 17799 IT Management Security

- Software Quality Assurance

Quality of Life: Rapidity of Change

- Information technology creates a very efficient market
- Information pours like water
- Company must adjust fast to competition, based on the information
- What are the impact to the employees:
  - stress
  - just in time workplace

Nomadic Computing

- The danger of ubiquitous computing & telecommunication
- Where is the family & work boundaries?
- Pros:
  - supports the idea of "knowledge workers"
  - be close to family
  - saves energy, less pollution
- Cons:
  - no private time
  - home but "not at home"

Digital Divide

- The right for information access
- Is it an already a real problem in Indonesia?
- What do you think you can achieve by narrowing the digital divide?

Techno-stress

- Induced by computer used
- Human expects fast response, because of their interaction with computers
- Will get impatient when confronted with slow response system, or with other "slow reacting" human/institutions!

5. Computer Crime

Computer Crime

- Case & Example
- Definition
- Computer Crime Modus

Computer Crime Definitions

- Encyclopedia of Crime & Justice, "*any illegal act requiring knowledge of computer technology for its perpetration, investigation or prosecution*"

Classic Case: BNI 1987

- Fund transfer of US$ 9 million from BNI New York to foreign bank accounts
- Used remote access from a hotel, with stolen password
- Was a new case at that time for Indonesia!

Recent Case

- Wendy Setiawan (15) hacked Data Storage Institute website, Singapore, from an Internet Café in Singapore
- Liable on conviction to a fine $5000, 3 years in prison (max)

Forms of Computer Crime

- According to Stair (1986)

- deletion, addition & modification part of whole data in a computer system
- modify/develop programs for criminal purpose
- use computer for criminal purpose

Computer Crime Modus (1)

- Data diddling: modifying data as they being entered into computer (low-tech!)
- Trojan horse
- Salami technique/rounding down
- Viruses (inserted to other programs)
- Worms (do not change other program)
- Data leakage: stealing computer generated reports...

Computer Crime Modus (2)

- Piggybacking: following a person, or an acceptable/valid data packet
- Impersonation: being someone else, in the real world or electronically
  - spoofing: IP, e-mail
- DoS: Denial of service
- Computer shut down
- Wire-tapping: eavesdropping over telecommunication line

Computer Crime Modus (3)

- Logic bombs, by disgruntled employees
- War dialing: finding a modem pool from a telephone book
- Spamming
- E-mail flaming
- Scavenging, from deleted(!) files

Targets

- Competitors
- Financial institutions
- Government & military agencies
- Enemy
- Well know portals/websites
- Anything (for fun)

Impacts

- Financial loss: direct or indirect
- Legal repercussions: breach of law (by being ignorant of security)
- Loss of credibility: case of kilkbca.com
- Blackmail: threatening someone
- Industrial espionage
- Disclosure of information
- Sabotage

Violators

- Crackers
- Employees
- IS personnel
- End users
- Former employees
- Interested or educated outsiders
- Part-time & temporary staffs

- Vendors & consultants
- Accidental ignorant

Controling Crimes

- Preventive: do not allow access for guest into data centre
- Detective: always use anti virus programs
- Curative: system backups

Publish or Not to Publish

- Reasons to keep vulnerabilities secret
  - to enhance security
- Reasons to dislose vulnerabilities
  - to enhance security…!
  - Why?
  - Eventually the bad guys will know the vulnerabilities. It is better the good guys to know the vulberabilities first!

Attack or Defend?

- If a cracker is known to enter a computer system, there are two options to consider:
  - Protect & proceed
  - Pursue & prosecute

Reasons for Protect & Proceed

- the computer system was not actually protected before
- if not protected, financial loss will be staggering
- cost for prosecution is expensive
- legitimate users in the network would face considerable threat.
- if the business is vulberable to lawsuits from the users or customers.
- the legal infrastructure is still weak

Reasons for Pursue & Prosecute

- the network & computer system had already been well protected
- the system had already been struck several times before
- the attack is/was concentrated
- the computer system is highly popular/visible
- while tracking the attacker, don't mind the attacker use a few computer resource (as long as considered not yet dangerous)
- attacker's access can be limited
- tools to monitor the attacker are sufficient
- the network administrator is sufficiently clever
- the managers are willing to press charges
- know what kind of evidence would lead to prosecution
- a system & data backup exist
- a working law exist, including knowledgeable law enforcement
- if not punished, the attacker will re-attack

Personnel Security

- Human is the most vulnerable part in computer security
- Screening employees
- Segregation of jobs of IS personnel
- Job rotation

- Termination of access rights of after termination
- Employee awareness program

New Topics

- Password sharing?
- Cyber-squatters
- Framing
- Typo-squatters

Indonesian Laws

- UU no.36/1999 Telekomunikasi h(http://bebas.vlsm.org/v01/RI/uu/1999/uu-1999-036.txt)
- RUU Informasi & Transaksi Elektronik

DAFTAR ACUAN

Suyatmi dan Sukiyo, 2005, *Laporan Kuliah Kerja Praktek (K.K.P) Rancangan Sistem Informasi Perpustakaan Pada PERSERO PT. Virama Karya*, Jakarta: Fakultas Teknologi Informasi, Universitas Budi Luhur.

Husnan, Suad dan Mulyanto, Sri, 2004, *Risalah Rapat Umum Pemegang Saham Luar Biasa PT (Persero) Virama Karya tentang Pengesahan Rencana Jangka Panjang Perusahaan Periode tahun 2004 – 2008*, Jakarta: Persero PT Virama Karya Konsultan Teknik dan Manajemen.

Ward, John and Joe Peppard, 2003, *Strategic Planning for Information Sistems,* 3rd Edition, John Wiley & Son Ltd.: West Sussex.

Atmaja, Wahyu H. K., M. Kom., 2002, *Tesis: Penyusunan Metodologi Perencanaan Strategis Sistem Informasi Berbasis Value Bisnis (Be Vista Planning) dalam rangka Meningkatkan Peran Strategis Sistem Informasi pada Suatu Organisasi*, Jakarta: Magister Teknologi Informasi, Program Pascasarjana, Fakultas Ilmu Komputer, Universitas Indonesia.

Defriansyah, Denny, M.Kom., 2002, *Tesis: Perencanaan Strategis Sistem Informasi Studi Kasus: PT. Dataprima GrahaPratama*, Jakarta: Magister Teknologi Informasi, Program Pascasarjana, Fakultas Ilmu Komputer, Universitas Indonesia.

Sulistijo, Budi, 2001, *Tesis: Pengukuran Nilai Ekonomis Proyek Intranet Virtual Private Network dan Sistem Informasi Eksekutif pada Industri Asuransi Kerugian dengan Metodologi Information Economics (Studi Kasus PT Jasa Raharja)*, Jakarta: Kekhususan Teknologi Informasi, Program Studi Ilmu Komputer, Program Pasca Sarjana, Universitas Indonesia.

Rangkuti, F., 2001, *Analisis SWOT Teknik membedah Kasus Bisnis*, 7th Edition, Jakarta: PT. Gramedia Pustaka Umum.

Indrajit, R.E., 2000, *Pengantar Konsep Dasar Manajemen Sistem Informasi dan Teknologi Informasi*, 1st Edition, Jakarta: PT. Elex Media Komputindo.

Satrio, Ir., dan Alambai, Syarifuddin, Ir., 1999, *Rencana Jangka Panjang Persero PT Virama Karya Tahun 1999 – 2003*, Jakarta: Persero PT. Virama Karya Konsultan Teknik dan Manajemen.

Applegate, McFarlan, McKenney, 1999, *Corporate Information Systems Management: Text and Cases*, 5th Edition, Singapore: Mc Graw Hill.

Callon, D.J., 1996, *Competitive Advantage Through Information Technology*, International Edition, Singapore: Mc Graw Hill.

Waterhouse, Price, 1996, *System Management Methodology Strategic Information Systems Planning (SISP)*, version 2.1, Inc.: Price Waterhouse World Firm Services BV.

Ward, J & Griffiths, P., 1996, *Strategic Planning for Information Systems*, 2nd Edition, New York: John Wiley & Sons.

Tozer, E. E., 1996, *Strategic IS/IT Planning*, Professional Edition, Boston: Butterworth-Heinemann.

Parker, Marilyn, 1996, *Strategic Transformation and IT*, Prentice Hall.

Remenyi Dan et al, 1995, *Effective Measurement and Management of IT Costs and Benefits*, Butterworth Heinemann.

Gitman, L.J., 1991, *Principles of Management Finance*, 6th Edition, New York: Harper Collins Publishers.

Earl, M.J., 1989, *Management Strategies For Information Technology*, 1st Edition, London: Prentice Hall.

Parker, Marilyn et al, 1988, *Information Economics*, Linking Business Performance to IT, Prentice Hall.

Channon, D. F., 1986, *Encyclopedic Dictionary of Strategic Management*, International Edition, England: Blackwell Business.