



MODUL PERKULIAHAN

Keamanan Jaringan

Pendahuluan

Fakultas Fasilkom	Program Studi Teknik Informatika	TatapMuka 01	Kode MK MK:15020	Di susun Oleh Tim Dosen
----------------------	-------------------------------------	------------------------	---------------------	----------------------------

Abstract

Keamanan jaringan ([Bahasa Inggris: Network Security](#)) dalam [jaringan komputer](#) sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah.

Kompetensi

Setelah membaca modul ini diharapkan mahasiswa :

- Mampu memahami konsep dasar keamanan jaringan dan Infrastruktur Perusahaan.
- Mampu menjelaskan jenis aspek security, ancaman dan kelemahan secara umum

Konsep Keamanan Jaringan

Keamanan jaringan ([Bahasa Inggris: Network Security](#)) dalam [jaringan komputer](#) sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah.

- Satu hal yang perlu diingat bahwa tidak ada jaringan yang anti sadap atau tidak ada jaringan komputer yang benar-benar aman. Sifat dari jaringan adalah melakukan komunikasi. Setiap komunikasi dapat jatuh ke tangan orang lain dan disalahgunakan.
- Sistem keamanan membantu mengamankan jaringan tanpa menghalangi penggunaannya dan menempatkan antisipasi ketika jaringan berhasil ditembus
- Pastikan bahwa user dalam jaringan memiliki pengetahuan yang cukup mengenai keamanan dan pastikan bahwa mereka menerima dan memahami rencana keamanan yang di buat .

Modal dasar untuk pembelajaran :

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

Cara belajar :

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

Mengapa di butuhkan?

- “**information-based society**”, menyebabkan nilai informasi menjadi sangat penting dan menuntut kemampuan untuk mengakses dan menyediakan informasi secara cepat dan akurat menjadi sangat

- esensial bagi sebuah organisasi,
- **Infrastruktur Jaringan komputer**, seperti LAN dan Internet, memungkinkan untuk menyediakan informasi secara cepat, sekaligus membuka potensi adanya lubang keamanan (*security hole*)

Mengapa Kejahatan IT Semakin Meningkat?

1. Aplikasi bisnis berbasis TI dan jaringan komputer meningkat : online banking, e-commerce, Electronic data Interchange (EDI).
2. Desentralisasi server.
3. Transisi dari single vendor ke multi vendor.
4. Meningkatnya kemampuan pemakai (user).
5. Kesulitan penegak hukum dan belum adanya ketentuan yang pasti.
6. Semakin kompleksnya system yang digunakan, semakin besarnya source code program yang digunakan.
7. Berhubungan dengan internet.

Elemen Utama:

Ada dua elemen utama pembentuk keamanan jaringan :

1. **Tembok pengamanan**, baik secara fisik maupun maya, yang ditaruh diantara piranti dan layanan jaringan yang digunakan dan orang-orang yang akan berbuat jahat.
2. **Rencana pengamanan**, yang akan diimplementasikan bersama dengan user lainnya, untuk menjaga agar sistem tidak bisa ditembus dari luar.

Resiko

Menurut David Icove [John D. Howard, "An Analysis Of Security Incidents On The Internet 1989 - 1995," PhD thesis, Engineering and Public Policy, Carnegie Mellon University, 1997.] berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu:

1. **Keamanan yang bersifat fisik (physical security)**: termasuk akses orang ke gedung, peralatan, dan media yang digunakan.

Contoh :

- **Wiretapping** atau hal-hal yang ber-hubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini.
- **Denial of service**, dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya jumlah pesan).
- **Syn Flood Attack**, dimana sistem (*host*) yang dituju dibanjiri oleh permintaan sehingga dia menjadi ter-lalu sibuk dan bahkan dapat berakibat macetnya sistem

(hang).

2. Keamanan yang berhubungan dengan orang (personel),

Contoh :

- Identifikasi user (username dan password)
- Profil resiko dari orang yang mempunyai akses (pemakai dan pengelola).

3. Keamanan dari data dan media serta teknik komunikasi (*communications*).

4. Keamanan dalam operasi: Adanya prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga ter-masuk prosedur setelah serangan (*post attack recovery*).

Karakteristik Penyusup :

- 1 **The Curious** (Si Ingin Tahu) - tipe penyusup ini pada dasarnya tertarik menemukan jenis sistem dan data yang anda miliki.
- 2 **The Malicious** (Si Perusak) - tipe penyusup ini berusaha untuk merusak sistem anda, atau merubah web page anda, atau sebaliknya membuat waktu dan uang anda kembali pulih.
- 3 **The High-Profile Intruder** (Si Profil Tinggi) - tipe penyusup ini berusaha menggunakan sistem anda untuk memperoleh popularitas dan ketenaran. Dia mungkin menggunakan sistem profil tinggi anda untuk mengiklankan kemampuannya.
- 4 **The Competition** (Si Pesaing) - tipe penyusup ini tertarik pada data yang anda miliki dalam sistem anda. Ia mungkin seseorang yang beranggapan bahwa anda memiliki sesuatu yang dapat menguntungkannya secara keuangan atau sebaliknya.

Istilah bagi penyusup :

- 1 **Mundane** ; tahu mengenai hacking tapi tidak mengetahui metode dan prosesnya.
- 2 **Iamer** (script kiddies) ; mencoba script2 yang pernah dibuat oleh aktivis hacking, tapi tidak paham bagaimana cara membuatnya.
- 3 **wannabe** ; paham sedikit metode hacking, dan sudah mulai berhasil menerobos sehingga berfalsafah ; HACK IS MY RELIGION.
- 4 **larva** (newbie) ; hacker pemula, teknik hacking mulai dikuasai dengan baik, sering bereksperimen.
- 5 **hacker** ; aktivitas hacking sebagai profesi.
- 6 **wizard** ; hacker yang membuat komunitas pembelajaran di antara mereka.
- 7 **guru** ; master of the master hacker, lebih mengarah ke penciptaan tools-tools yang powerfull yang salah satunya dapat menunjang aktivitas hacking, namun

lebih jadi tools pemrograman system yang umum.

Mungkinkah Aman?

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

Aspek-Tujuan Keamanan Jaringan

Menurut Garfinkel [Simson Garfinkel, "PGP: Pretty Good Privacy," O'Reilly & Associates, Inc., 1995.]

1. Privacy / Confidentiality

Defenisi : menjaga informasi dari orang yang tidak berhak mengakses.

Privacy : lebih kearah data-data yang sifatnya privat , Contoh : e-mail seorang pemakai (user) tidak boleh dibaca oleh administrator.

Confidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.

Contoh : data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya.

Bentuk Serangan : usaha penyadapan (dengan program *sniffer*).

Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

2. Integrity

Definisi : informasi tidak boleh diubah tanpa seijin pemilik informasi.

Contoh : e-mail di *intercept* di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang dituju.

Bentuk serangan : Adanya virus, *trojan horse*, atau pemakai lain yang mengubah informasi tanpa ijin, "man in the middle attack" dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

3. Authentication

Definisi : metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.

Dukungan :

Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking(untuk menjaga "*intellectual property*", yaitu dengan menandai dokumen atau hasil karya dengan "tanda tangan" pembuat) dan digital signature.

Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

4. Availability

Definisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan.

Contoh hambatan :

“*denial of service attack*” (DoS attack), dimana server dikirim permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down, hang, crash*.

mailbomb, dimana seorang pemakai dikirim e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.

5. Access Control

Definisi : cara pengaturan akses kepada informasi. berhubungan dengan masalah authentication dan juga privacy

Metode : menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain.

6. Non-repudiation

Definisi : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.

Security Attack Models

Menurut W. Stallings [William Stallings, “*Network and Internetwork Security*,” Prentice Hall, 1995.] serangan (*attack*) terdiri dari :

- **Interruption:** Perangkat sistem menjadi rusak atau tidak tersedia. Serangan ditujukan kepada ketersediaan (*availability*) dari sistem. Contoh serangan adalah “*denial of service attack*”.
- **Interception:** Pihak yang tidak berwenang berhasil mengakses asset atau informasi. Contoh dari serangan ini adalah penyadapan (*wiretapping*).
- **Modification:** Pihak yang tidak berwenang tidak saja berhasil mengakses, akan tetapi dapat juga mengubah (*tamper*) aset. Contoh dari serangan ini antara lain adalah mengubah isi dari web site dengan pesan-pesan yang merugikan pemilik web site.
- **Fabrication:** Pihak yang tidak berwenang menyisipkan objek palsu ke dalam sistem. Contoh dari serangan jenis ini adalah memasukkan pesan-pesan palsu seperti e-mail palsu ke dalam jaringan komputer.

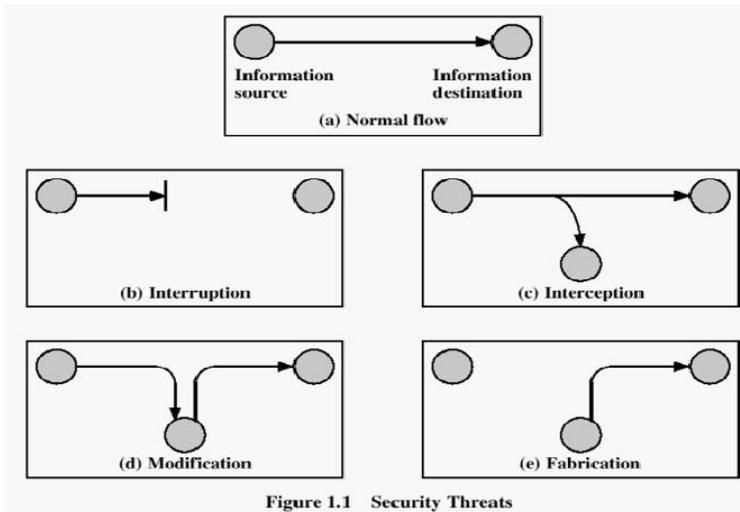


Figure 1.1 Security Threats

Contoh:

1996	U.S. Federal Computer Incident Response Capability (FedCIRC) melaporkan bahwa lebih dari 2500 "insiden" di sistem komputer atau jaringan komputer yang disebabkan oleh gagalnya sistem keamanan atau adanya usaha untuk membobol sistem keamanan
1996	FBI National Computer Crimes Squad, Washington D.C., memperkirakan kejadian komputer yang terdeteksi kurang dari 15%, dan hanya 10% dari angka itu yang dilaporkan
1997	Penelitian Deloitte Touche Tohmatsu menunjukkan bahwa dari 300 perusahaan di Australia, 37% (dua diantara lima) pernah mengalami masalah keamanan sistem komputernya.
1996	Inggris, NCC Information Security Breaches Survey menunjukkan bahwa kejadian komputer menaik 200% dari tahun 1995 ke 1996. Kerugian rata-rata US \$30.000 / insiden.
1998	FBI melaporkan bahwa kasus persidangan yang berhubungan dengan kejadian komputer meroket 950% dari tahun 1996 ke tahun 1997, dengan penangkapan dari 4 ke 42, dan terbukti (convicted) di pengadilan naik 88% dari 16 ke 30 kasus. Dan lain-lain. Dapat dilihat di www.cert.org

Contoh akibat dari jebolnya sistem keamanan, antara lain:

1988	Keamanan sistem mail sendmail dieksloitasi oleh Robert Tapan Morris sehingga melumpuhkan sistem Internet. Kegiatan ini dapat diklasifikasikan sebagai "denial of service attack". Diperkirakan biaya yang digunakan untuk memperbaiki dan hal-hal lain yang
------	--

	hilang adalah sekitar \$100 juta. Di tahun 1990 Morris dihukum (convicted) dan hanya didenda \$10.000.
10 Maret 1997	<p>Seorang hacker dari Massachusetts berhasil mematikan sistem telekomunikasi di sebuah airport local (Worcester, Massachusetts) sehingga mematikan komunikasi di control tower dan menghalau pesawat yang hendak mendarat.</p> <p>Dia juga mengacaukan sistem telepon di Rutland, Massachusetts.</p> <p>http://www.news.com/News/Item/Textonly/0,25,20278,00.html?pfv</p>
1990	Kevin Poulsen mengambil alih system komputer telekomunikasi di Los Angeles untuk memenangkan kuis di sebuah radio local.
1995	Kevin Mitnick, mencuri 20.000 nomor kartu kredit, menyalin system operasi DEC secara illegal dan mengambil alih hubungan telpon di New York dan California.
1995	Vladimir Levin membobol bank-bank di kawasan Wallstreet, mengambil uang sebesar \$10 juta.
2000	Fabian Clone menjebol situs aetna.co.id dan Jakarta mail dan membuat directory atas namanya berisi peringatan terhadap administrator situs tersebut.
2000	Beberapa web site Indonesia sudah dijebol dan daftarnya (beserta contoh halaman yang sudah dijebol) dapat dilihat di koleksi < http://www.2600.com >
2000	Wenas, membuat server sebuah ISP di singapura down

PRINSIP DASAR PERANCANGAN SISTEM YANG AMAN

- Mencegah hilangnya data
- Mencegah masuknya penyusup

Security Policy

Sebelum melanjutkan implementasi ke tingkat yang lebih jauh sebaiknya ditentukan dulu apa yang hendak dilindungi dan dilindungi dari siapa. Beberapa pertanyaan berikut dapat membantu penentuan kebijakan keamanan yang diambil.

1. Informasi apa yang dianggap rahasia atau sensitif ?
2. Anda melindungi sistem anda dari siapa ?
3. Apakah anda membutuhkan akses jarak jauh?
4. Apakah password dan enkripsi cukup melindungi ?
5. Apakah anda butuh akses internet?

6. Tindakan apa yang anda lakukan jika ternyata sistem anda dibobol?
- Kebijaksanaan keamanan tergantung sebesar apa anda percaya orang lain, di dalam ataupun di luar organisasi anda. Kebijakan haruslah merupakan keseimbangan antara mengijinkan user untuk mengakses informasi yang dibutuhkan dengan tetap menjaga keamanan sistem.

LAPISAN KEAMANAN :

1. Lapisan Fisik :

- Membatasi akses fisik ke mesin :
 - Akses masuk ke ruangan komputer
 - penguncian komputer secara hardware
 - keamanan BIOS
 - keamanan Bootloader
- Back-up data :
 - pemilihan piranti back-up
 - penjadwalan back-up
- Mendeteksi gangguan fisik :

log file : Log pendek atau tidak lengkap, Log yang berisikan waktu yang aneh, Log dengan permisi atau kepemilikan yang tidak tepat, Catatan pelayanan reboot atau restart, Log yang hilang, masukan su atau login dari tempat yang janggal mengontrol akses sumber daya.

2. Keamanan lokal

Berkaitan dengan user dan hak-haknya :

- Beri mereka fasilitas minimal yang diperlukan.
- Hati-hati terhadap saat/dari mana mereka login, atau tempat seharusnya mereka login.
- Pastikan dan hapus account mereka ketika mereka tidak lagi membutuhkan akses.

3. Keamanan Root

- Ketika melakukan perintah yang kompleks, cobalah dalam cara yang tidak merusak dulu, terutama perintah yang menggunakan globbing: contoh, anda ingin melakukan "rm foo*.bak", pertama coba dulu: "ls foo*.bak" dan pastikan anda ingin menghapus file-file yang anda pikirkan.
- Beberapa orang merasa terbantu ketika melakukan "touch /-i" pada sistem mereka. Hal ini akan membuat perintah-perintah seperti : "rm -fr *" menanyakan apakah anda benar-benar ingin menghapus seluruh file. (Shell anda menguraikan "-i" dulu, dan memberlakukannya sebagai option -i ke rm).
- Hanya menjadi root ketika melakukan tugas tunggal tertentu. Jika anda berusaha mengetahui bagaimana melakukan sesuatu, kembali ke shell pemakai normal hingga

anda yakin apa yang perlu dilakukan oleh root.

- Jalur perintah untuk pemakai root sangat penting. Jalur perintah, atau variabel lingkungan PATH mendefinisikan lokasi yang dicari shell untuk program. Cobalah dan batasi jalur perintah bagi pemakai root sedapat mungkin, dan jangan pernah menggunakan '.', yang berarti 'direktori saat ini', dalam pernyataan PATH anda. Sebagai tambahan, jangan pernah menaruh direktori yang dapat ditulis pada jalur pencarian anda, karena hal ini memungkinkan penyerang memodifikasi atau menaruh file biner dalam jalur pencarian anda, yang memungkinkan mereka menjadi root ketika anda menjalankan perintah tersebut.
- Jangan pernah menggunakan seperangkat utilitas rlogin/rsh/rexec (disebut utilitas r) sebagai root. Mereka menjadi sasaran banyak serangan, dan sangat berbahaya bila dijalankan sebagai root. Jangan membuat file .rhosts untuk root.
- File /etc/securetty berisikan daftar terminal-terminal tempat root dapat login. Secara baku (pada RedHat Linux) diset hanya pada konsol virtual lokal (vty). Berhati-hatilah saat menambahkan yang lain ke file ini. Anda seharusnya login dari jarak jauh sebagai pemakai biasa dan kemudian 'su' jika anda butuh (mudah-mudahan melalui ssh atau saluran terenkripsi lain), sehingga tidak perlu untuk login secara langsung sebagai root.
- Selalu perlakukan dan berhati-hati ketika menjadi root. Tindakan anda dapat mempengaruhi banyak hal. Pikir sebelum anda mengetik!

4. Keamanan File dan system file

- Directory home user tidak boleh mengakses perintah mengubah sistem seperti partisi, perubahan device dan lain-lain.
- Lakukan setting limit system file.
- Atur akses dan permission file : read, write, execute bagi user maupun group.
- Selalu cek program-program yang tidak dikenal

5. Keamanan Password dan Enkripsi

- Hati-hati terhadap bruto force attack dengan membuat password yang baik.
- Selalu mengenkripsi file yang dipertukarkan.
- Lakukan pengamanan pada level tampilan, seperti screen saver.

6. Keamanan Kernel

- selalu update kernel sistem operasi.
- Ikuti review bugs dan kekurang-kekurangan pada sistem operasi.

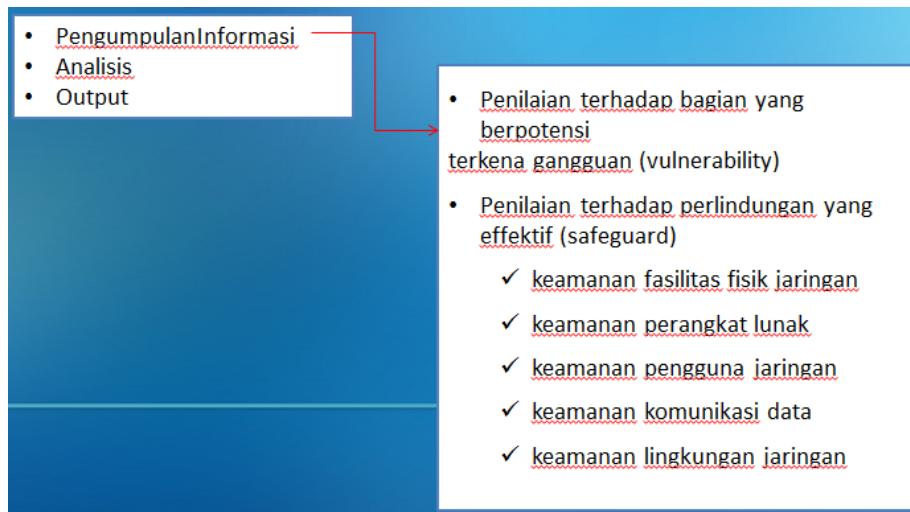
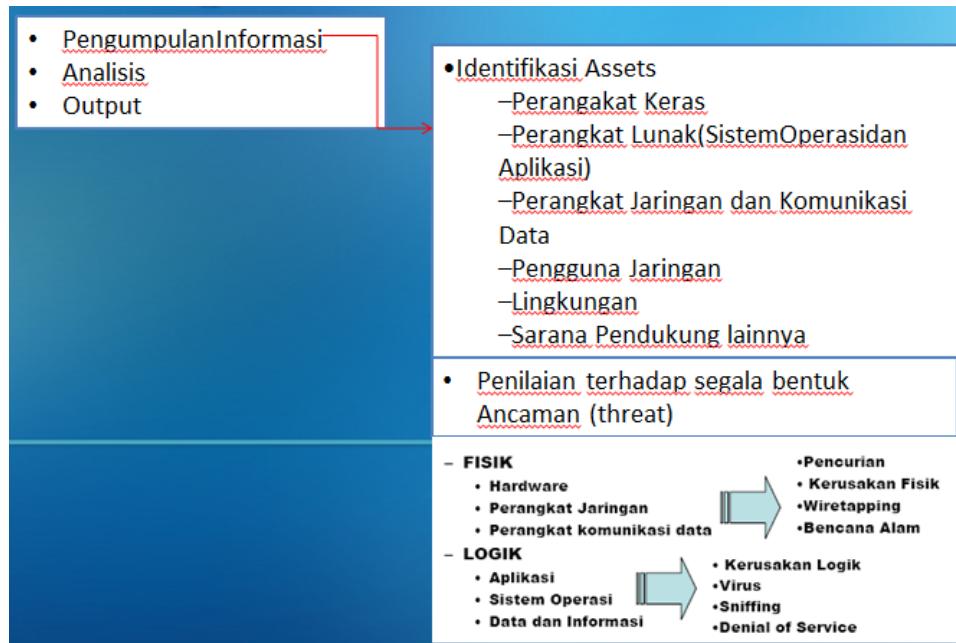
7. Keamanan Jaringan

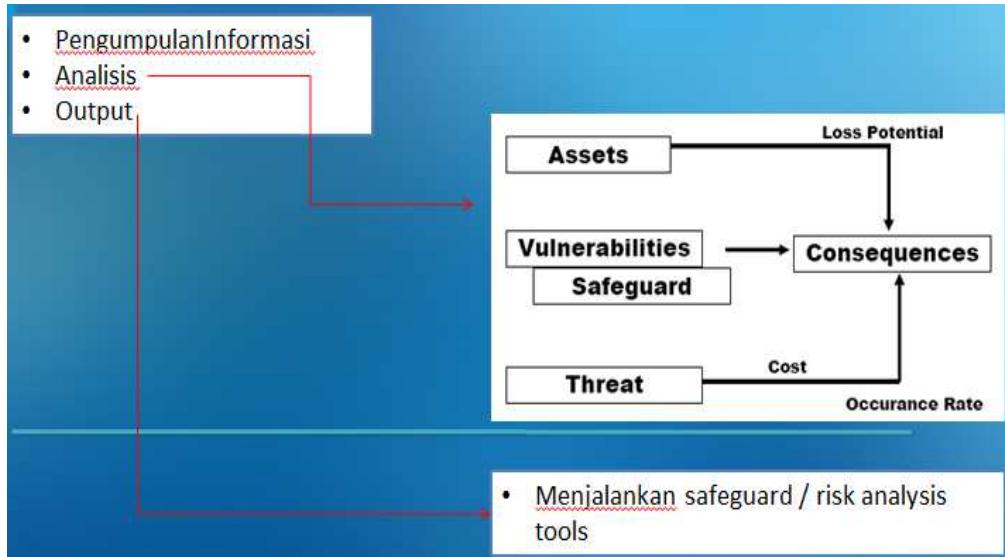
- Waspadai paket sniffer yang sering menyadap port Ethernet.

- Lakukan prosedur untuk mengecek integritas data
- Verifikasi informasi DNS
- Lindungi network file system

Gunakan firewall untuk barrier antara jaringan privat dengan jaringan eksternal

Management Resiko







MODUL PERKULIAHAN

Keamanan Jaringan

Kriptografi, Enkripsi & Steganografi

Fakultas
Fasilkom

Program Studi
Teknik Informatika

TatapMuka
02

Kode MK
MK:15020

Di susun Oleh
Tim Dosen

Abstract

Keamanan jaringan (Bahasa Inggris: Network Security) dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah.

Kompetensi

Setelah membaca modul ini diharapkan mahasiswa :

- Memahami konsep dasar peningkatan keamanan jaringan
- Mampu menjelaskan teknik keamanan jaringan secara umum, autentifikasi, Kriptografi, Steganografi

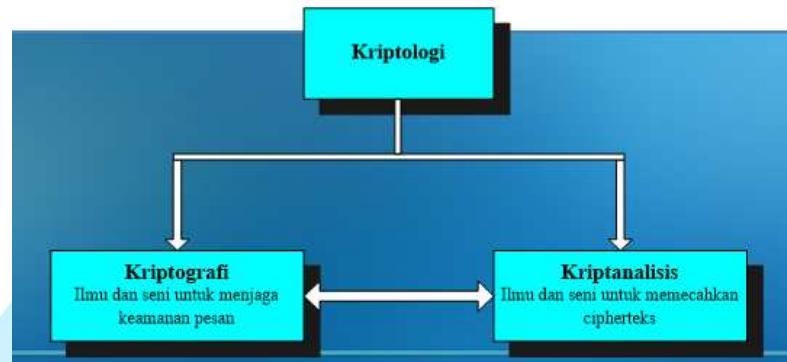
Terminologi

- **Kriptografi** (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. “*Crypto*” berarti “*secret*” (rahasia) dan “*graphy*” berarti “*writing*” (tulisan).
- Para pelaku atau praktisi kriptografi disebut **cryptographers**.
- Sebuah algoritma kriptografik (*cryptographic algorithm*), disebut **cipher**, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi.
- **Enkripsi** merupakan proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*)
- **Ciphertext** adalah pesan yang sudah tidak dapat dibaca dengan mudah.
- **Dekripsi** merupakan proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*.
- **Cryptanalysis** adalah seni dan ilmu untuk memecahkan *ciphertext* tanpa bantuan kunci.
- *Cryptanalyst* adalah pelaku atau praktisi yang menjalankan *cryptanalysis*.
- **Penyadap** (*eavesdropper*): orang yang mencoba menangkap pesan selama ditransmisikan.

Nama lain: *enemy, adversary, intruder, interceptor, bad guy*

- Ron Rivest (pakar kriptografi): “*cryptography is about communication in the presence of adversaries*”
- **Steganography** adalah seni dan ilmu untuk menyembunyikan pesan didalam pesan lainnya dengan sedemikian rupa sehingga orang lain yang melihatnya tidak menyadari bahwa ada suatu pesan rahasia didalam teks tersebut
- steganography itu sendiri berasal dari bahasa yunani *steganos* yang artinya ” tersembunyi/terselubung sedangkan *graphien* artinya ” menulis ” sehingga dapat disimpulkan bahwa *steganography* artinya tulisan yang tersembunyi.

Kriptologi (*cryptology*): studi mengenai kriptografi dan kriptanalisis.



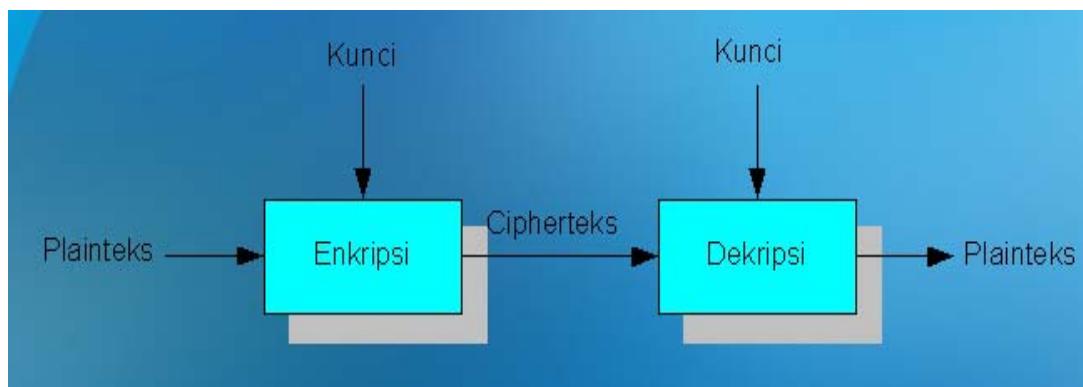
- Persamaan kriptografer dan kriptanalisis:
→ Keduanya sama-sama menerjemahkan cipherteks menjadi plainteks

- Perbedaan kriptografer dan kriptanalisis:
 - Kriptografer bekerja atas legitimasi pengirim atau penerima pesan
 - Kriptanalisis bekerja tanpa legitimasi pengirim atau penerima pesan.

Enkripsi

- Enkripsi digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak.
- Dengan enkripsi data anda disandikan (*encrypted*) dengan menggunakan sebuah kunci (*key*).
- Untuk membuka (*decrypt*) data tersebut digunakan juga sebuah kunci yang dapat sama dengan kunci untuk mengenkripsi (untuk kasus *private key cryptography*) atau dengan kunci yang berbeda (untuk kasus *public key cryptography*).
 - saat ini enkripsi telah digunakan pada sistem secara luas, seperti [Internet e-commerce](#), jaringan [Telepon bergerak](#) dan [ATM](#) pada bank.

- **Proses Enkripsi**



Secara matematis, proses atau fungsi enkripsi (E) dapat dituliskan sebagai:

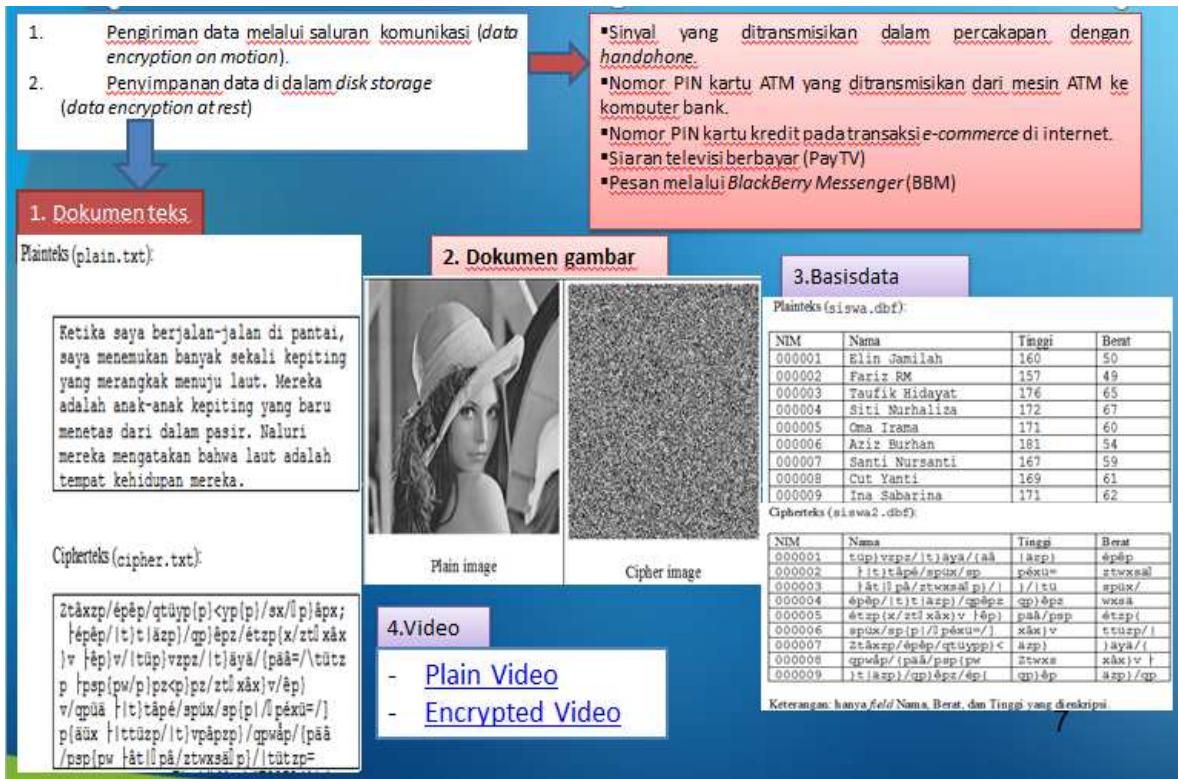
$$E(M) = C$$

dimana: M adalah *plaintext (message)* dan C adalah *ciphertext*.

Proses atau fungsi dekripsi (D) dapat dituliskan sebagai:

$$D(C) = M$$

Aplikasi Enkripsi – Dekripsi



Sejarah

- Kriptografi mempunyai sejarah yang panjang.
- Tercatat Bangsa Mesir 4000 tahun yang lalu menggunakan *hieroglyph* yang tidak standard untuk menulis pesan
- Jaman dahulu orang Yunani menggunakan tool yang disebut *Scytale* untuk membantu mengenkripsi pesan yang akan mereka kirimkan. Mereka akan membungkus silinder dengan kertas, menulis pesan dan mengirimkannya.
- Metode enkripsi ini sangat mudah dipecahkan, tidak mengherankan karena ini adalah enkripsi pertama di dunia yang digunakan di dunia nyata.

Teknik Dasar Kriptografi

- Substitusi**
- Blocking**
- Permutasi**
- Ekspansi**
- Pemampatan**
- Substitusi**
 - Langkah pertama adalah membuat suatu tabel substitusi. Tabel substitusi dapat dibuat sesuka hati, dengan catatan bahwa penerima pesan memiliki tabel yang sama untuk keperluan dekripsi.
 - Bila tabel substitusi dibuat secara acak, akan semakin sulit pemecahan cipherteks oleh

orang yang tidak berhak.

Contoh :

- Tabel subsitusi
- Caesar Chipher
- ROT 13

Tabel Subtitusi

A-B-C-D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y-Z-1-2-3-4-5-6-7-8-9-0-.,,

B-F-1-K-Q-G-A-T-P-J-6-H-Y-D-2-X-5-M-V-7-C-8-4-I-9-N-R-E-U-3-L-S-W-,-.-O-Z-0

Contoh :

SISTEM

7P7CQY (TABEL SUBSITUSI)

VLVWHP (CAESAR CHIPHER)

FVFGRZ (ROT13)

- **Caesar Cipher**

Metode Caesar Cipher yang digunakan oleh Julius Caesar. Pada prinsipnya, setiap huruf digantikan dengan huruf yang berada tiga (3) posisi dalam urutan alfabet.

Sebagai contoh huruf “a” digantikan dengan huruf “D” dan seterusnya.

Transformasi yang digunakan adalah:

plain : a b c d e f g h i j k l m n o p q r s t u v w x y z

cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Contoh:

WINPOIN maka dituliskan ZLQSRLQ.

- **ROT13**

Pada sistem ini sebuah huruf digantikan dengan huruf yang letaknya 13 posisi darinya.

Sebagai contoh, huruf “A” digantikan dengan huruf “N”, huruf “B” digantikan dengan huruf “O”, dan seterusnya.

Secara matematis, hal ini dapat dituliskan sebagai:

$$C \text{ ROT13} = (M)$$

Untuk mengembalikan kembali ke bentuk semulanya dilakukan proses enkripsi ROT13 dua kali.

$$M = \text{ROT13}(\text{ROT13}(M))$$

- **Blocking**

• Sistem enkripsi terkadang membagi plaintext menjadi blok-blok yang terdiri dari

beberapa karakter yang kemudian dienkripsi secara independen.

- Dengan menggunakan enkripsi blocking dipilih jumlah lajur dan kolom untuk penulisan pesan. Jumlah lajur atau kolom menjadi kunci bagi kriptografi dengan teknik ini.
- Plaintext dituliskan secara vertikal ke bawah berurutan pada lajur, dan dilanjutkan pada kolom berikutnya sampai seluruhnya tertulis. Ciphertext-nya adalah hasil pembacaan plaintext secara horizontal berurutan sesuai dengan blok-nya.

Jika plaintext adalah 5 TEKNIK DASAR KRIPTOGRAFI maka hasil ciphertext) .

Jika menggunakan teknik blocking dengan 1blok berisi 4 karakter.

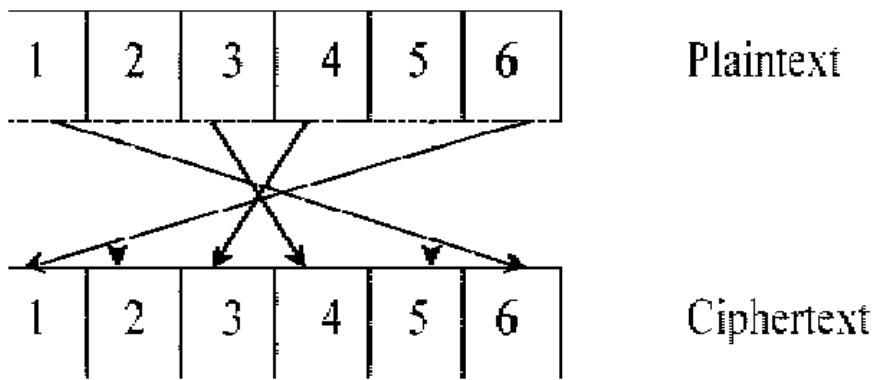
5	K		G		BLOK 1
		K	R		BLOK 2
T	D	R	A		BLOK 3
E	A	I	F		BLOK 4
K	S	P	I		BLOK 5
N	A	T			BLOK 6
I	R	O			BLOK 7

Jadi ciphertext yang dihasilkan dengan teknik ini adalah

"5K G KRTDRAEAIFKSPINAT IRO".

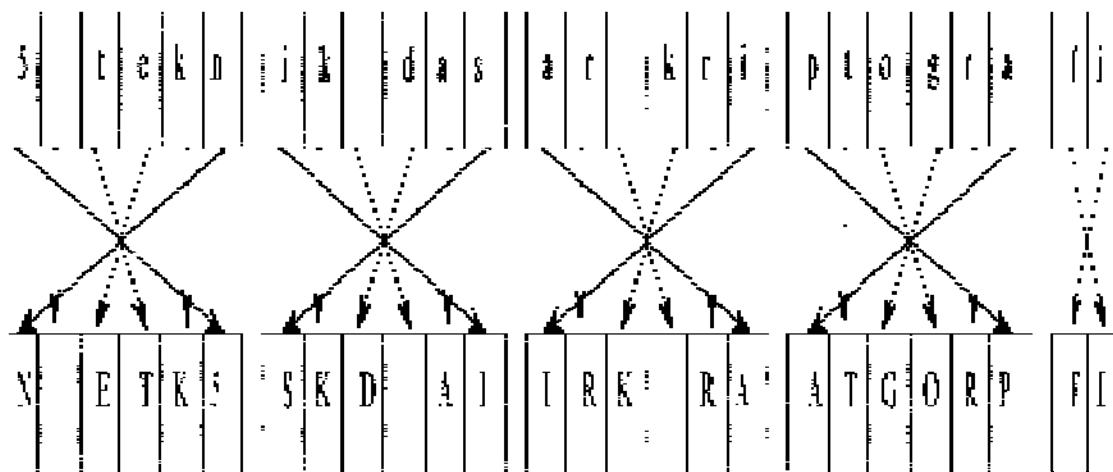
Plaintext dapat pula ditulis secara horizontal dan ciphertextnya adalah hasil pembacaan secara vertikal.

- **Permutasi**
- Salah satu teknik enkripsi yang terpenting adalah permutasi atau sering juga disebut transposisi. Teknik ini memindahkan atau merotasikan karakter dengan aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi.
- Dalam teknik substitusi, karakter berada pada posisi yang tetap tapi identitasnya yang diacak. Pada teknik permutasi, identitas karakternya tetap, namun posisinya yang diacak.
- Sebelum dilakukan permutasi, umumnya plaintext terlebih dahulu dibagi menjadi blok-blok dengan panjang yang sama.
- Untuk contoh diatas, plaintext akan dibagi menjadi blok-blok yang terdiri dari 6 karakter, dengan aturan permutasi sebagai berikut :



- **Permutasi**

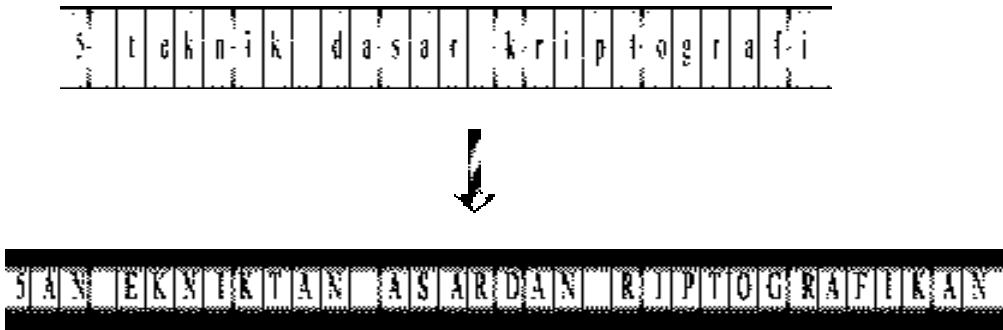
Dengan menggunakan aturan diatas, maka proses enkripsi dengan permutasi dari plaintext adalah sebagai berikut :



Ciphertext yang dihasilkan dengan teknik permutasi ini adalah "N ETK5 SKD AIIRK RAATGORP FI".

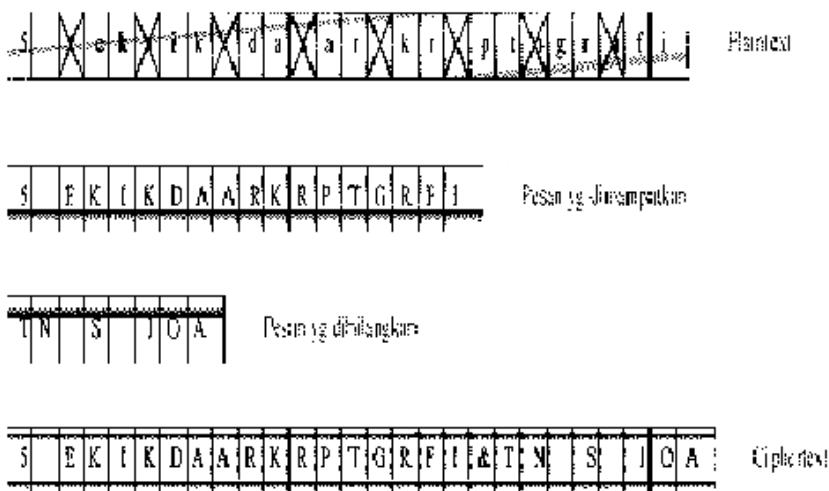
- **Ekspansi**

- Suatu metode sederhana untuk mengacak pesan adalah dengan memelarkan pesan itu dengan aturan tertentu.
- Salah satu contoh penggunaan teknik ini adalah dengan meletakkan huruf konsonan atau bilangan ganjil yang menjadi awal dari suatu kata di akhir kata itu dan menambahkan akhiran "an".
- Bila suatu kata dimulai dengan huruf vokal atau bilangan genap, ditambahkan akhiran "i".
- Proses enkripsi dengan cara ekspansi terhadap plaintext terjadi sebagai berikut :



Ciphertextnya adalah
"5AN EKNIKTAN ASARDAN RIPTOGRAFIKAN".

- Pemampatan
- Mengurangi panjang pesan atau jumlah bloknya adalah cara lain untuk menyembunyikan isi pesan. Contoh sederhana ini menggunakan cara menghilangkan setiap karakter ke-tiga secara berurutan.
- Karakter-karakter yang dihilangkan disatukan kembali dan disusulkan sebagai "lampiran" dari pesan utama, dengan diawali oleh suatu karakter khusus, dalam contoh ini digunakan "&".
- Proses yang terjadi untuk plaintext kita adalah :



Teknik Dasar Kriptografi

• Penggunaan Kunci

- Salah satu cara untuk menambah tingkat keamanan sebuah algoritma enkripsi dan dekripsi adalah dengan menggunakan sebuah kunci (*key*) yang biasanya disebut *K*.
- Sehingga persamaan matematisnya menjadi:

$$EK(M) = C$$

$$DK(C) = M$$

- Atau:

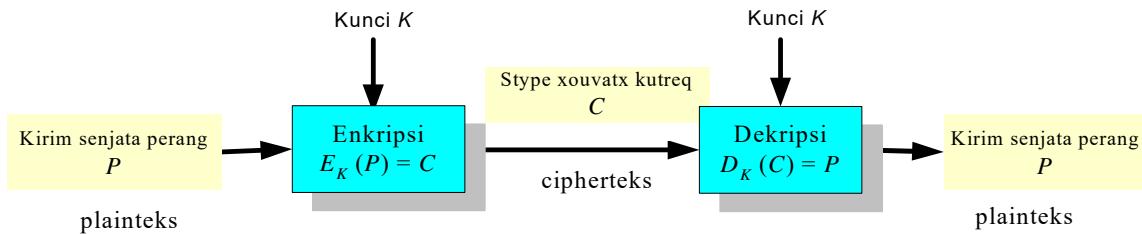
Enkripsi: $E_K(P) = C$

Dekripsi: $D_K(C) = P$

Harus dipenuhi: $D_K(E_K(P)) = P$

- Terdapat 2 macam kunci :

1. Algoritma Simetris
2. Algoritma Asimetris



Algoritma kriptografi berdasarkan jenis kunci yang digunakan:

- Algoritma *simetris*

Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi adalah kunci yang sama

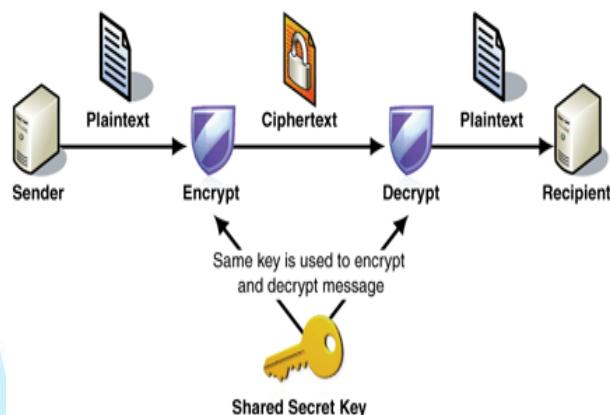
- Algoritma *asimetris*

Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi menggunakan kunci yang berbeda.

- Algoritma simetris (*symmetric algorithm*)** adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm*.

Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini disebut juga algoritma kunci rahasia (*secret-key algorithm*).

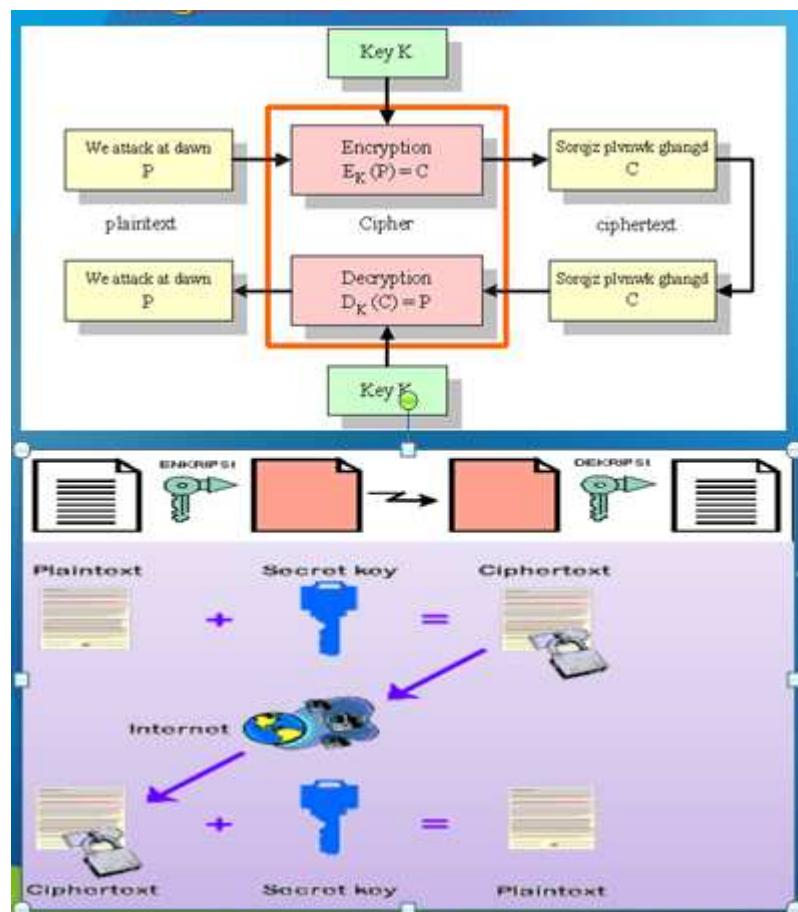
Metode : DES (*Data Encryption Standard*)



Alice menaruh sebuah pesan rahasia di dalam kotak dan mengunci kotak menggunakan

gembok dan ia memiliki kuncinya. Kemudian dia mengirimkan kotak ke Bob melalui surat biasa. Ketika Bob menerima kotak, ia menggunakan kunci salinan sama persis yang dimiliki Alice untuk membuka kotak dan membaca pesan. Bob kemudian dapat menggunakan gembok yang sama untuk membalas pesan rahasia.

Algoritma Simetris



Contoh algoritma simetris:

- **DES (Data Encryption Standard)**
- **Rijndael**
 - **Blowfish**
 - **IDEA**
 - **GOST**
 - **Serpent**
 - **RC2, RC4, Rc5, dll**

- **Algoritma ASimetris**

Algoritma asimetris (*asymmetric algorithm*) adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi.

Pada algoritma ini menggunakan dua kunci yakni kunci publik (*public key*) dan kunci privat (*private key*).

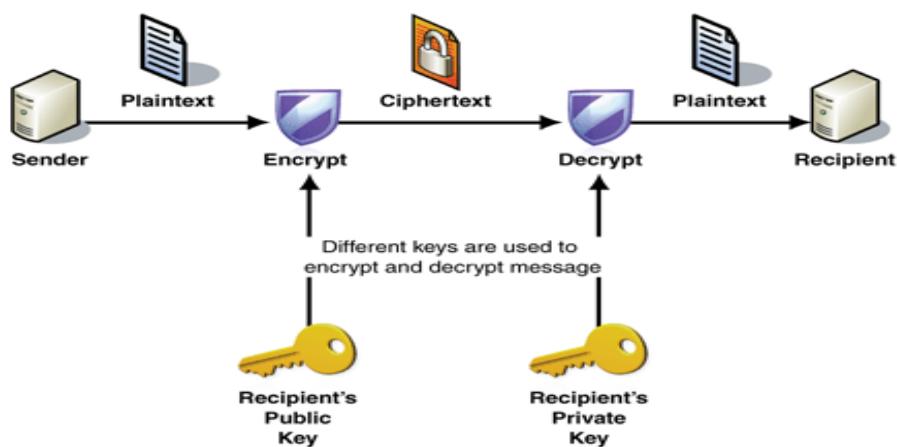
Kunci publik disebarluaskan secara umum sedangkan kunci privat disimpan secara rahasia

oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan.

Metode : RSA (Rivest, Shamir, Adleman)

Contoh algoritma nirsimetri/Asimetris:

- RSA
- ElGamal
- Rabin
- Diffie-Hellman Key Exchange
- DSA
- dll



- Pertama Alice meminta Bob untuk mengirim gembok yang terbuka melalui surat biasa, sehingga ia tidak membagikan kuncinya. Ketika Alice menerimanya, ia menggunakannya untuk mengunci sebuah kota yang berisi pesan dan mengirimkan kotak dengan gembok terkunci tadi ke Bob. Bob kemudian membuka kotak dengan kunci yang ia pegang karena itu gembok miliknya untuk membaca pesan Alice. Untuk membalasnya, Bob harus meminta Alice untuk melakukan hal yang sama.
- Keuntungan dari metode asymmetric key adalah Bob dan Alice tidak pernah berbagi kunci mereka. Hal ini untuk mencegah pihak ketiga agar tidak menyalin kunci atau memata-matai pesan Alice dan Bob. Selain itu, jika Bob ceroboh dan membiarkan orang lain untuk menyalin kuncinya, pesan Alice ke Bob akan terganggu, namun pesan Alice kepada orang lain akan tetap menjadi rahasia, karena orang lain akan memberikan gembok milik mereka ke Alice untuk digunakan.

Berdasarkan besar data yang diolah dalam satu kali proses

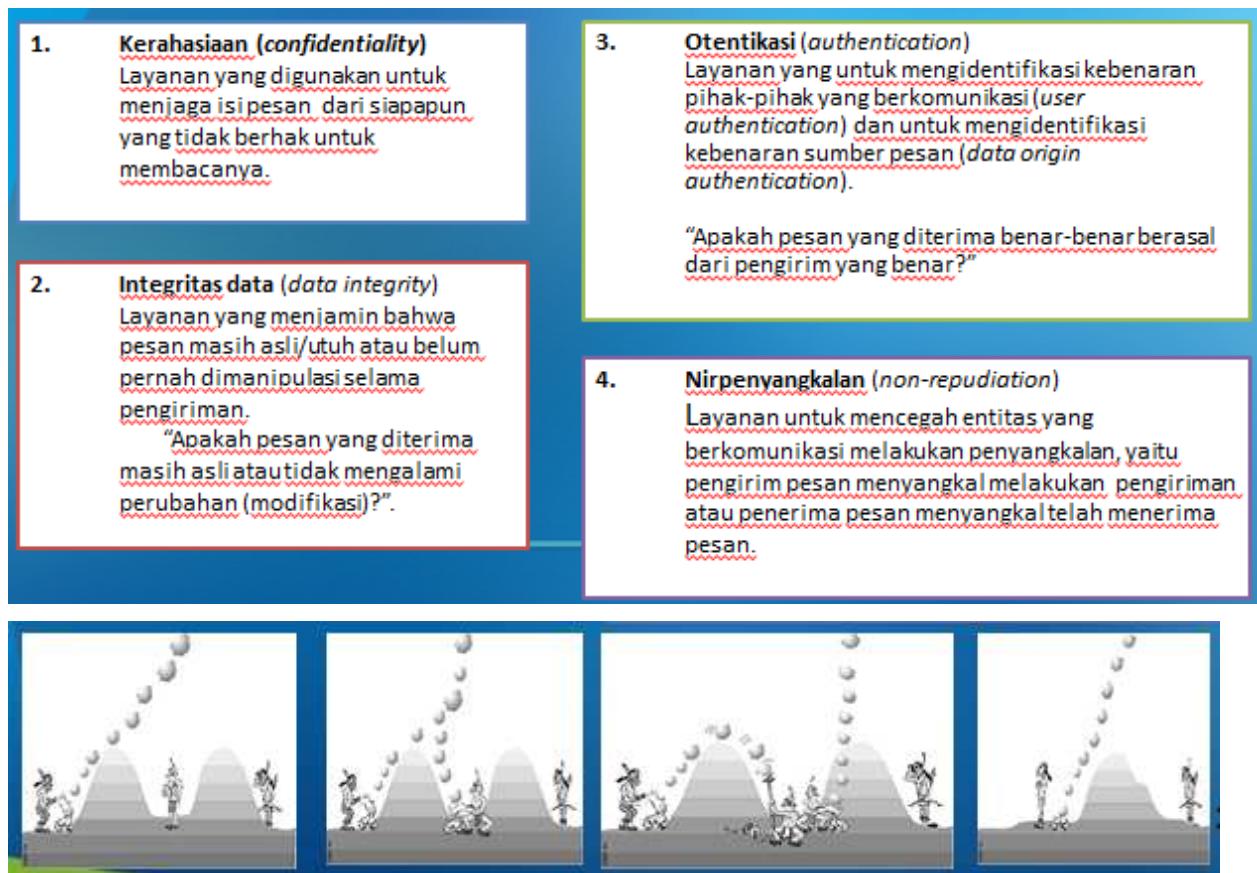
- **Algoritma *block cipher***

Informasi/data yang hendak dikirim dalam bentuk blok-blok besar (misal 64-bit) dimana blok-blok ini dioperasikan dengan fungsi enkripsi yang sama dan akan menghasilkan informasi rahasia dalam blok-blok yang berukuran sama.

- **Algoritma *stream cipher***

Informasi/data yang hendak dikirim dioperasikan dalam bentuk blok-blok yang lebih kecil (byte atau bit), biasanya satu karakter persatuan persatuan waktu proses, Penggunaan transformasi enkripsi yang berubah setiap waktu.

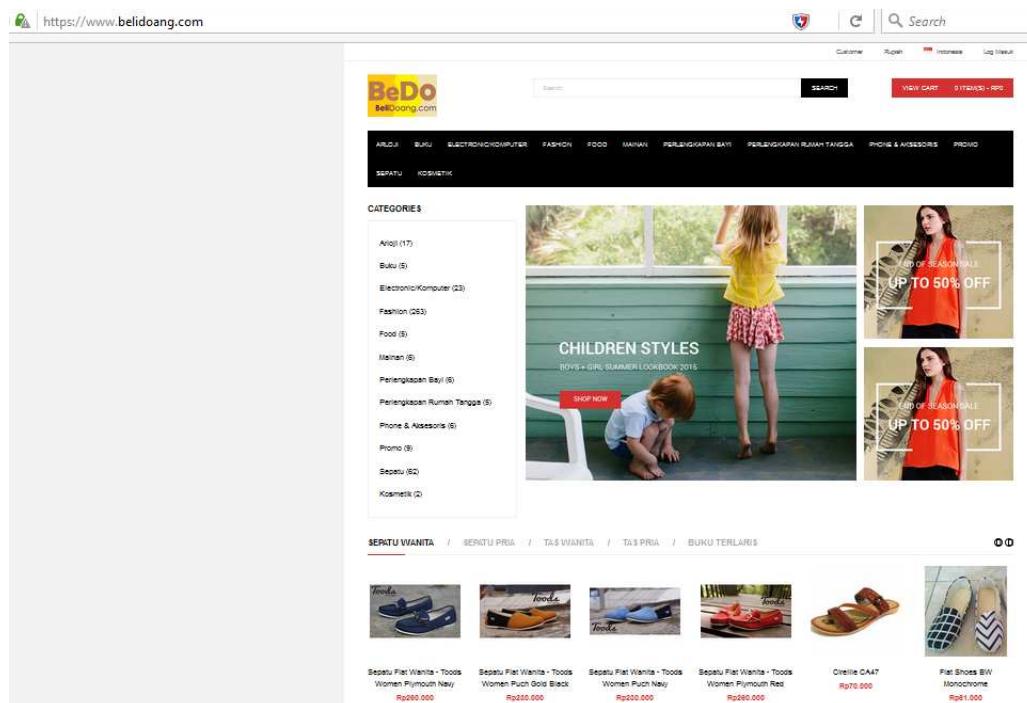
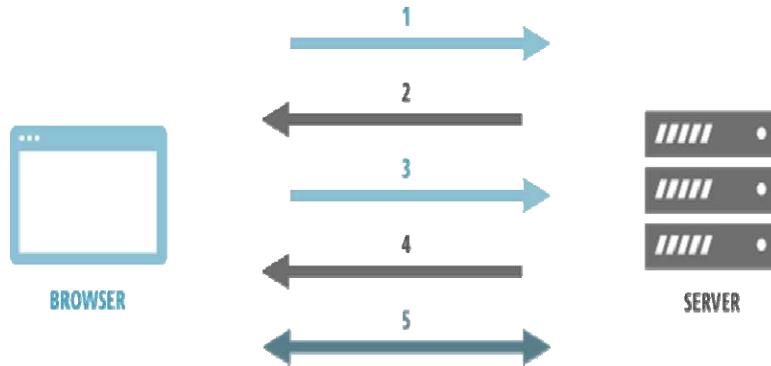
Layanan Kriptografi



Keamanan Enkripsi di Bidang Web

- Selama bertahun-tahun, protokol SSL (Secure Sockets Layer) telah mengamankan transaksi web menggunakan enkripsi antara web browser dan web server, melindungi kamu dari siapa pun yang mengintai kamu.
- SSL sendiri memiliki konsep yang sederhana. Dimulai ketika browser meminta halaman yang aman (biasanya https://).
- Web server mengirimkan kunci publik dengan sertifikat.
- Browser memeriksa sertifikat yang dikeluarkan oleh pihak terpercaya (biasanya CA), bahwa sertifikat tersebut masih berlaku dan sertifikat masih berkaitan dengan web tersebut.
- Browser kemudian menggunakan kunci publik untuk mengenkripsi kunci symmetric secara acak dan mengirimkannya ke server dengan URL terkenkripsi, membutuhkan juga enkripsi http data.
- Web server mendekripsi enkripsi symmetric key menggunakan kunci pribadi dan menggunakan kunci sysmmetric untuk mendekripsi URL dan http data.
- Web server mengirimkan kembali permintaan dokumen html dan enkripsi http data

dengan browser symmetric key. Browser mendekripsi http data dan dokumen html menggunakan symmetric key dan menampilkan informasi.



Steganography

- **Steganography** adalah seni dan ilmu untuk menyembunyikan pesan didalam pesan lainnya dengan sedemikian rupa sehingga orang lain yang melihatnya tidak menyadari bahwa ada suatu pesan rahasia didalam teks tersebut.
- kata steganography itu sendiri berasal dari bahasa yunani *steganos* yang artinya ” tersembunyi/terselubung sedangkan *graphien* artinya ” menulis “ sehingga dapat disimpulkan bahwa *steganography* artinya tulisan yang tersembunyi.
 - *Tujuan dari steganography* adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi.
 - *Kelebihan steganography* jika dibandingkan dengan cryptography adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam crytography yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganography dan crptography digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.
- Dalam praktiknya, kebanyakan pesan disembunyikan dengan membuat perubahan tipis

terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya. Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.

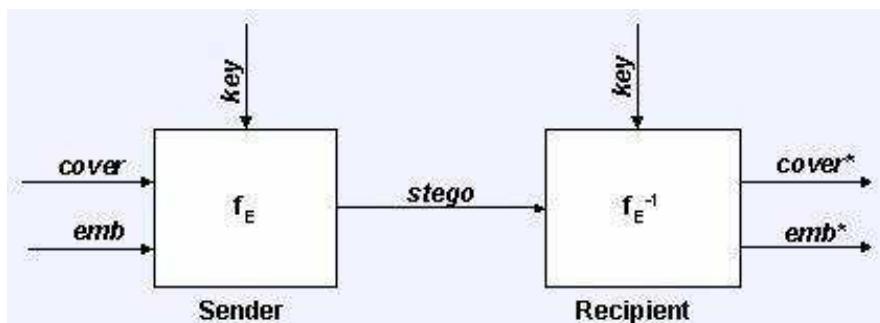
- Pada metode steganografi cara ini sangat berguna jika digunakan pada cara steganografi komputer karena banyak format berkas digital yang dapat dijadikan media untuk menyembunyikan pesan. Format yang biasa digunakan di antaranya:

Format *image* : bitmap (bmp), gif, pcx, jpeg, dll.

Format audio : wav, voc, mp3, dll.

Format lain : teks file, html, pdf, dll.

Gambaran Sistem



Gambar. menunjukkan sebuah sistem steganography umum dimana di bagian pengirim pesan (**sender**), dilakukan proses embedding (**fe**) pesan yang hendak dikirim secara rahasia (**emb**) ke dalam data cover sebagai tempat meyimpannya (**cover**), dengan menggunakan kunci tertentu (**key**), sehingga dihasilkan data dengan pesan tersembunyi di dalamnya (**stego**). Di bagian penerima pesan (**recipient**), dilakukan proses extracting (**fe-1**) pada stego untuk memisahkan pesan rahasia (**emb**) dan data penyimpan (**cover**) tadi dengan menggunakan kunci yang sama seperti pada proses embedding tadi. Jadi hanya orang yang tahu kunci ini saja yang dapat mengekstrak pesan rahasia tadi.

Ada 4 metode dalam steganography diantaranya :

1. Least Significant Bit Insertion (LSBI)
2. Algorithms and Transformation
3. Redundant Pattern Encoding
4. Spread Spectrum Method

Least Significant Bit Insertion (LSBI)

- Dengan cara memanipulasi LSB dari suatu image.
- Untuk image dengan 24 bit color dapat digunakan 3 bit per pixel untuk dimanipulasi, untuk 8 bit color hanya 1 bit per pixel saja yang dapat dimanipulasi.
- Jika Stego dilakukan kompresi, maka harus menggunakan Lossless Compression

- supaya data tidak hilang.
- Berfungsi sangat baik ketika image yang digunakan dalam format grayscale karena perubahannya akan sulit dideteksi oleh mata.
 - Contohnya, pada berkas image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data pixel yang menyusun file tersebut. Pada berkas bitmap 24 bit, setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian, pada setiap pixel berkas bitmap 24 bit kita dapat menyisipkan 3 bit data

Least Significant Bit Insertion (LSBI)

- Kekurangan dari LSB Insertion: Dapat diambil kesimpulan dari contoh 8 bit pixel, menggunakan LSB Insertion dapat secara drastis mengubah unsur pokok warna dari pixel. Ini dapat menunjukkan perbedaan yang nyata dari *cover image* menjadi *stego image*, sehingga tanda tersebut menunjukkan keadaan dari steganografi. Variasi warna kurang jelas dengan 24 bit image, bagaimanapun file tersebut sangatlah besar. Antara 8 bit dan 24 bit *image* mudah diserang dalam pemrosesan *image*, seperti *cropping* (kegagalan) dan *compression* (pemampatan).
- Keuntungan dari LSB Insertion : Keuntungan yang paling besar dari algoritma LSB ini adalah cepat dan mudah. Dan juga algoritma tersebut memiliki *software* steganografi yang mendukung dengan bekerja di antara unsur pokok warna LSB melalui manipulasi *palette* (lukisan).

Algorithms and Transformation

Algoritma *compression* adalah metode steganografi dengan menyembunyikan data dalam fungsi matematika.

Dua fungsi tersebut adalah *Discrete Cosine Transformation* (DCT) dan *Wavelet Transformation*.

Fungsi DCT dan Wavelet yaitu mentransformasi data dari satu tempat (domain) ke tempat (domain) yang lain.

Fungsi DCT yaitu mentransformasi data dari tempat spatial (*spatial domain*) ke tempat frekuensi (*frequency domain*).

Redundant Pattern Encoding

Redundant Pattern Encoding adalah menggambar pesan kecil pada kebanyakan gambar.

Keuntungan dari metode ini adalah dapat bertahan dari *cropping* (kegagalan). Kerugiannya yaitu tidak dapat menggambar pesan yang lebih besar.

Spread Spectrum method

Spread Spectrum steganografi terpencar-pencar sebagai pesan yang diacak (*encrypted*) melalui gambar (tidak seperti dalam LSB).

Untuk membaca suatu pesan, penerima memerlukan algoritma yaitu *crypto-key* dan *stego-key*.

Metode ini juga masih mudah diserang yaitu penghancuran atau pengrusakan dari kompresi dan proses *image*.

Steganalisis dan Stegosystem

- Seperti Kriptografi dan Kriptanalisis, Steganalisis didefinisikan sebagai suatu seni dan ilmu dalam mendeteksi informasi tersembunyi. Sebagai tujuan dari steganografi adalah untuk merahasiakan keberadaan dari sebuah pesan rahasia, satu keberhasilan penyerangan pada sebuah sistem steganografi terdiri dari pendekripsi bahwa sebuah berkas yang diyakini berisikan data terselubung. Seperti dalam Kriptanalisis, diasumsikan bahwa sistem steganografi telah diketahui oleh si penyerang. Maka dari itu, keamanan dari sistem steganografi bergantung hanya pada fakta bahwa kunci rahasia tidak diketahui oleh si penyerang.
- *Stegosystem* di sini berisi tentang penyerangan-penyerangan yang dilakukan terhadap suatu sistem steganografi, sebuah perbedaan penting harus dibuat di antara penyerangan-penyerangan pasif di mana penyerang hanya dapat memotong data, dan penyerangan-penyerangan aktif di mana penyerang juga dapat memanipulasi data.

Penyerangan-penyerangan berikut memungkinkan dalam model dari stegosistem ini:

- *Stego-Only-Attack* (Penyerangan hanya Stego). Penyerang telah menghalangi stego data dan dapat menganalisisnya.
- *Stego-Attack* (Penyerangan Stego). Pengirim telah menggunakan *cover* yang sama berulangkali untuk data terselubung. Penyerang memiliki berkas stego yang berasal dari *cover file* yang sama. Dalam setiap berkas stego tersebut, sebuah pesan berbeda disembunyikan.
- *Cover-Stego-Attack* (Penyerangan selubung Stego). Penyerang telah menghalangi berkas stego dan mengetahui *cover file* mana yang digunakan untuk menghasilkan berkas stego ini. Ini menyediakan sebuah keuntungan melalui penyerangan *stego-only* untuk si penyerang.
- *Manipulating the stego data* (Memanipulasi data stego). Penyerang memiliki kemampuan untuk memanipulasi data stego. Jika penyerang hanya ingin menentukan sebuah pesan disembunyikan dalam berkas stego ini, biasanya ini tidak memberikan sebuah keuntungan, tapi memiliki kemampuan dalam memanipulasi data stego yang berarti bahwa si penyerang mampu memindahkan pesan rahasia dalam data stego (jika ada).
- *Manipulating the cover data* (Memanipulasi data terselubung). Penyerang dapat memanipulasi data terselubung dan menghalangi hasil data stego. Ini dapat membuat tugas dalam menentukan apakah data stego berisikan sebuah pesan rahasia lebih mudah bagi si penyerang.

Penggunaan:

- Digunakan untuk informasi penjelasan yang menyertai sebuah gambar (seperti catatan dokter yang menyertai sebuah X-ray)
 - Menanamkan data yang dapat memperbaiki audio atau image pada kerusakan yang terjadi dari koneksi atau transmisi yang jelek.
 - Komunikasi private peer-to-peer
 - Mengirimkan komunikasi rahasia pada web untuk menghindari penyebaran
 - Perlindungan hak cipta
 - Menyembunyikan data pada jaringan untuk menghindari pelanggaran.
- **Contoh:**
- **Dari Iringan Air Mata**
 - **Jiwa Nona Gadis Anak Nirwana**
 - **Bicara Ingin Cinta Andai Rasanya Ada**
 - Mudah sekali kan menebak pesan tersembunyi diatas, caranya adalah dengan mengambil huruf pertama pada teks diatas. Dan pesan tersembunyi tersebut adalah “ **DIAM JANGAN BICARA**

Daftar Pustaka

- http://www.academia.edu/6124616/Rinaldi_Munir_IF5054_Kriptografi_1_Bahan_Kuliahan_ke-10_IF5054_Kriptografi
- <https://shineofscience.wordpress.com/2013/09/30/kiptografi-sistem-keamanan-komputer/>
- <http://ditonugroh08.blogspot.co.id/2012/09/keamanan-jaringan-komputer-menggunakan.html>



MODUL PERKULIAHAN

Keamanan Jaringan

Resiko Keamanan, Jenis Serangan & Malware

Fakultas
Fasilkom

Program Studi
Teknik Informatika

TatapMuka
03

Kode MK
MK:15020

Di susun Oleh
Tim Dosen

Abstract

Keamanan jaringan (Bahasa Inggris: Network Security) dalam jaringan komputer sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah.

Kompetensi

Setelah membaca modul ini diharapkan mahasiswa :

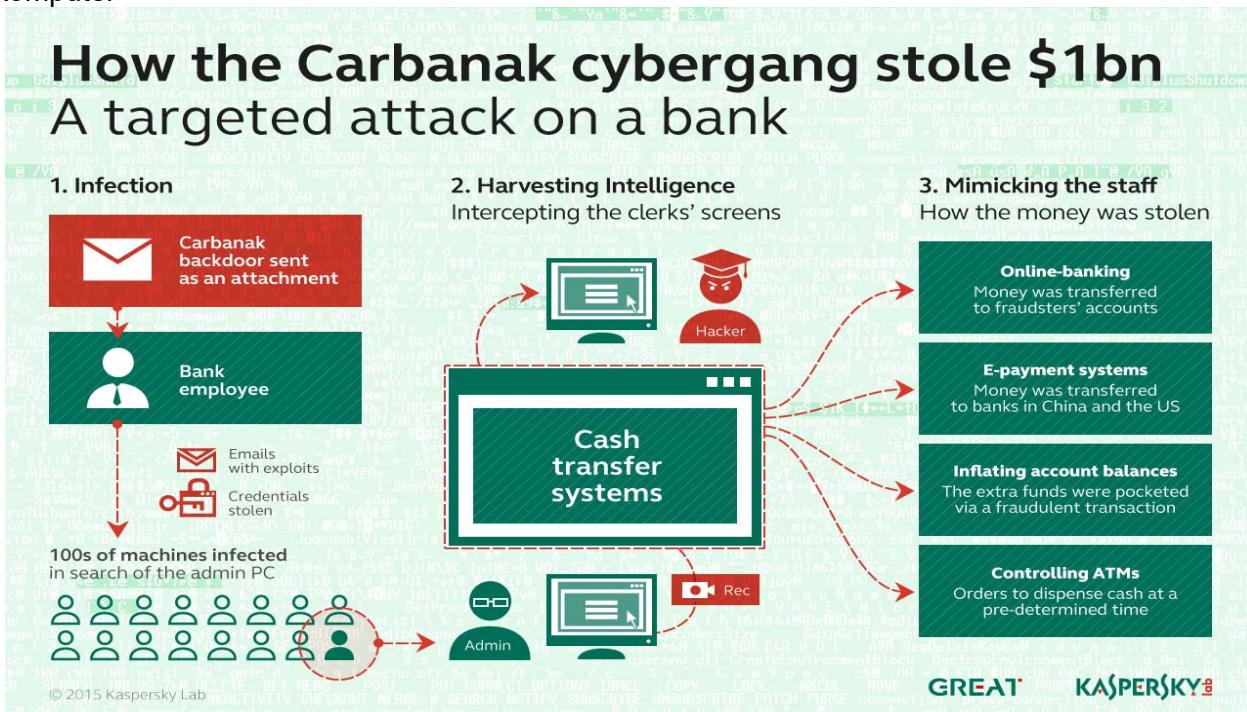
- Memahami identifikasi resiko keamanan jaringan
- Identifikasi serangan & Malware

Identifikasi:

- Loss Potensial:



Sumber: <http://www.slideshare.net/jagoanilmu/modul-1-pendahuluan-keamanan-jaringan-komputer>

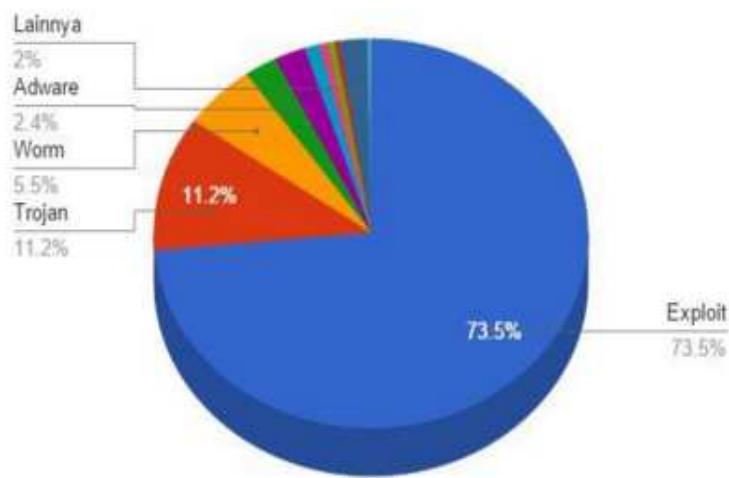


<https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/>

Kuartal pertama 2015, penyebaran malware di Indonesia di dominasi oleh malware yang melakukan eksplorasi atas celah keamanan sebanyak 73,5 % , diikuti oleh trojan 11,2 % dimana salah satunya adalah trojan yang melakukan penyerangan atas situs internet banking. Peringkat 3 dan 4 masing-masing ditempati oleh jagoan lama worm sebanyak 5,5 % dan Adware sebanyak

2,44 %. Dari insiden malware di kuartal pertama 2015 beberapa hal penting yang perlu menjadi perhatian para pengguna internet Indonesia adalah kesadaran untuk melakukan patching atau penambalan atas celah keamanan dari piranti lunak yang digunakan, salah satunya dengan cara memproteksi komputernya dengan pengamanan bank guard dan anti exploit serta menghindari situs freeware yang banyak mengandung adware / PUP seperti Softonic, Brothersoft dan Cnet.

STATISTIK MALWARE INDONESIA Q1 2015



Sumber: <http://www.vaksin.com/0415-statistik-malwareq1>

Review- Aspek Keamanan Jaringan Komputer

ASPEK KEAMANAN JARINGAN KOMPUTER :

Menurut Garfinkel [Simson Garfinkel, "PGP: Pretty Good Privacy," O'Reilly & Associates, Inc., 1995.]

1. Privacy / Confidentiality

Defenisi : menjaga informasi dari orang yang tidak berhak mengakses.

Privacy : lebih kearah data-data yang sifatnya privat , Contoh : e-mail seorang pemakai (*user*) tidak boleh dibaca oleh administrator.

Confidentiality : berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu dan hanya diperbolehkan untuk keperluan tertentu tersebut.

Contoh : data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) harus dapat diproteksi dalam penggunaan dan penyebarannya.

Bentuk Serangan : usaha penyadapan (dengan program *sniffer*).

Usaha-usaha yang dapat dilakukan untuk meningkatkan privacy dan confidentiality adalah dengan menggunakan teknologi kriptografi.

Integrity

Defenisi : informasi tidak boleh diubah tanpa seijin pemilik informasi.

Contoh : e-mail di *intercept* di tengah jalan, diubah isinya, kemudian diteruskan ke alamat yang

dituju.

Bentuk serangan : Adanya virus, *trojan horse*, atau pemakai lain yang mengubah informasi tanpa ijin, **“man in the middle attack”** dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

Authentication

Defenisi : metoda untuk menyatakan bahwa informasi betul-betul asli, atau orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud.

Dukungan :

- Adanya Tools membuktikan keaslian dokumen, dapat dilakukan dengan teknologi watermarking(untuk menjaga “*intellectual property*”, yaitu dengan menandai dokumen atau hasil karya dengan “tanda tangan” pembuat) dan digital signature.
- Access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. User harus menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya.

Review- Aspek Keamanan Jaringan Komputer

Availability

Defenisi : berhubungan dengan ketersediaan informasi ketika dibutuhkan.

Contoh hambatan :

- **“Denial of service attack” (DoS attack)**, dimana server dikirimi permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down, hang, crash*.
- **mailbomb**, dimana seorang pemakai dikirimi e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya.
- **Access Control**
- **Defenisi** : cara pengaturan akses kepada informasi. berhubungan dengan masalah
- authentication dan juga privacy
- **Metode** : menggunakan kombinasi userid/password atau dengan menggunakan mekanisme lain.
- **Non-repudiation**
- **Defenisi** : Aspek ini menjaga agar seseorang tidak dapat menyangkal telah melakukan sebuah transaksi. Dukungan bagi electronic commerce.

Perangkat perusak

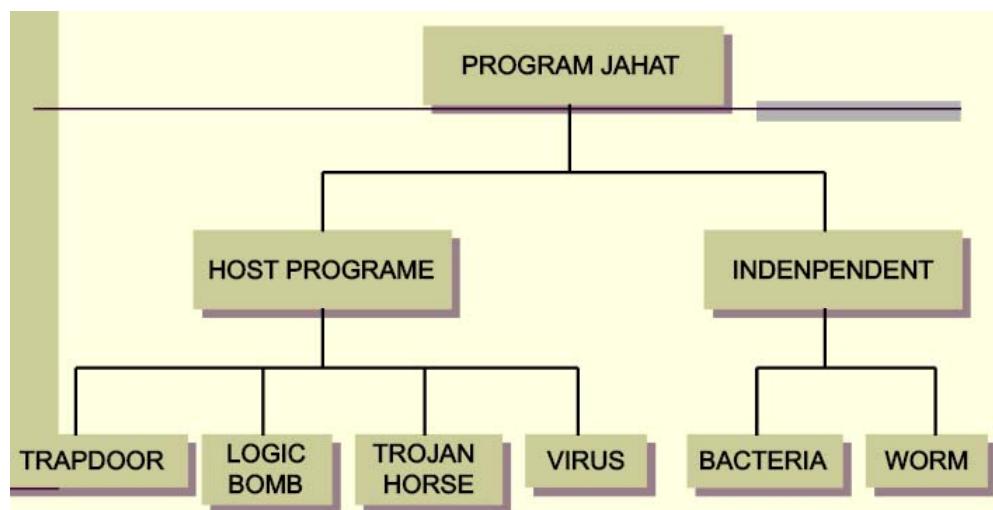
Perangkat perusak ([bahasa Inggris](#): *malware*, berasal dari kata **malicious** dan **software**) adalah [perangkat lunak](#) yang diciptakan untuk menyusup atau merusak sistem komputer, [peladen](#) atau jejaring komputer tanpa izin termaklum (*informed consent*) dari pemilik. Istilah ini adalah istilah umum yang dipakai oleh pakar komputer untuk mengartikan berbagai

macam perangkat lunak atau kode perangkat lunak yang mengganggu atau mengusik.

Ancaman canggih terhadap system computer adalah program yang mengeksplorasi kelemahan system komputasi

Taksonomi ancaman perangkat lunak / klasifikasi program jahat (malicious program):

- Program-program yang memerlukan program inang (host program). Fragmen program tidak dapat mandiri secara independen dari suatu program aplikasi, program utilitas atau program sistem.
- Program-program yang tidak memerlukan program inang. Program sendiri yang dapat dijadwalkan dan dijalankan oleh sistem operasi.



Tipe-tipe program jahat (Taksonomi Bowles)

1. **Bacteria :**

- program yang mengkonsumsi sumber daya sistem dengan mereplikasi dirinya sendiri. Bacteria tidak secara eksplisit merusak file.
- Tujuan program ini hanya satu yaitu mereplikasi dirinya.
- Program bacteria yang sederhana bisa hanya mengeksekusi dua kopian dirinya secara simultan pada sistem multiprogramming atau menciptakan dua file baru, masing-masing adalah kopian file program bacteria. Kedua kopian ini kemudian mengkopi dua kali, dan seterusnya.

2. **Logic bomb :**

- logik yang ditempelkan pada program komputer agar memeriksa suatu kumpulan kondisi di sistem. Ketika kondisi-kondisi yang dimaksud ditemui, logik mengeksekusi suatu fungsi yang menghasilkan aksi-aksi tak diotorisasi.
- Logic bomb menempel pada suatu program resmi yang diset meledak ketika kondisi-kondisi tertentu dipenuhi.
- Contoh kondisi-kondisi untuk memicu logic bomb adalah ada atau tidak adanya file-file

tertentu, hari tertentu dari minggu atau tanggal, atau pemakai menjalankan aplikasi tertentu. Begitu terpicu, bomb mengubah atau menghapus data atau seluruh file, menyebabkan mesin terhenti, atau mengerjakan perusakan lain.

3. Trapdoor :

- Titik masuk tak terdokumentasi rahasia di satu program untuk memberikan akses tanpa metode-metode otentifikasi normal.
- Trapdoor telah dipakai secara benar selama bertahun-tahun oleh pemogram untuk mencari kesalahan program. Debugging dan testing biasanya dilakukan pemogram saat mengembangkan aplikasi. Untuk program yang mempunyai prosedur otentifikasi atau setup lama atau memerlukan pemakai memasukkan nilai-nilai berbeda untuk menjalankan aplikasi maka debugging akan lama bila harus melewati prosedur-prosedur tersebut. Untuk debug program jenis ini, pengembang membuat kewenangan khusus atau menghilangkan keperluan setup dan otentifikasi.
- Trapdoor adalah kode yang menerima suatu barisan masukan khusus atau dipicu dengan menjalankan ID pemakai tertentu atau barisan kejahatan tertentu. Trapdoor menjadi ancaman ketika digunakan pemrogram jahat untuk memperoleh pengkasesan tak diotorisasi.
- Pada kasus nyata, auditor (pemeriksa) perangkat lunak dapat menemukan trapdoor pada produk perangkat lunak dimana nama pencipta perangkat lunak berlakuk sebagai password yang memintas proteksi perangkat lunak yang dibuatnya. Adalah sulit mengimplementasikan kendali-kendali perangkat lunak untuk trapdoor.

4. Trojan horse :

- Rutin tak terdokumentasi rahasia ditempelkan dalam satu program berguna. Program yang berguna mengandung kode tersembunyi yang ketika dijalankan melakukan suatu fungsi yang tak diinginkan. Eksekusi program menyebabkan eksekusi rutin rahasia ini.
- Program-program trojan horse digunakan untuk melakukan fungsi-fungsi secara tidak langsung dimana pemakai tak diotorisasi tidak dapat melakukannya secara langsung. Contoh, untuk dapat mengakses file-file pemakai lain pada sistem dipakai bersama, pemakai dapat menciptakan program trojan horse.
- Trojan horse ini ketika program dieksekusi akan mengubah ijin-ijin file sehingga file-file dapat dibaca oleh sembarang pemakai. Pencipta program dapat menyebarkan ke pemakai-pemakai dengan menempatkan program di direktori bersama dan menamai programnya sedemikian rupa sehingga disangka sebagai program utilitas yang berguna.
- Program trojan horse yang sulit dideteksi adalah kompilator yang dimodifikasi sehingga menyisipkan kode tambahan ke program-program tertentu begitu dikompilasi, seperti program login. Kode menciptakan trapdoor pada program login yang mengijinkan pencipta log ke sistem menggunakan password khusus. Trojan horse jenis ini tak pernah dapat

ditemukan jika hanya membaca program sumber. Motivasi lain dari trojan horse adalah penghancuran data. Program muncul sebagai melakukan fungsi-fungsi berguna (seperti kalkulator), tapi juga secara diam-diam menghapus file-file pemakai.

- Trojan horse biasa ditempelkan pada program-program atau rutin-rutin yang diambil dari BBS, internet, dan sebagainya.

5. **Virus :**

- Kode yang ditempelkan dalam satu program yang menyebabkan pengkopian dirinya disisipkan ke satu program lain atau lebih, dengan cara memodifikasi program-program itu.
- Modifikasi dilakukan dengan memasukkan kopian program virus yang dapat menginfeksi program-program lain. Selain hanya progasi, virus biasanya melakukan fungsi yang tak diinginkan.
- Di dalam virus komputer, terdapat kode intruksi yang dapat membuat kopian sempurna dirinya. Ketika komputer yang terinfeksi berhubungan (kontak) dengan perangkat lunak yang belum terinfeksi, kopian virus memasuki program baru. Infeksi dapat menyebar dari komputer ke komputer melalui pemakai-pemakai yang menukar disk atau mengirim program melalui jaringan. Pada lingkungan jaringan, kemampuan mengakses aplikasi dan layanan-layanan komputer lain merupakan fasilitas sempurna penyebaran virus.
- Masalah yang ditimbulkan virus adalah virus sering merusak sistem komputer seperti menghapus file, partisi disk, atau mengacaukan program.

6. **Worm :**

- Program yang dapat mereplikasi dirinya dan mengirim kopian-kopian dari komputer ke komputer lewat hubungan jaringan. Begitu tiba, worm diaktifkan untuk mereplikasi dan progasai kembali. Selain hanya propagasi, worm biasanya melakukan fungsi yang tak diinginkan.
- Network worm menggunakan hubungan jaringan untuk menyebar dari sistem ke sistem lain. Sekali aktif di suatu sistem, network worm dapat berlaku seperti virus atau bacteria, atau menempelkan program trojan horse atau melakukan sejumlah aksi menjengkelkan atau menghancurkan.
- Untuk mereplikasi dirinya, network worm menggunakan suatu layanan jaringan, seperti : Fasilitas surat elektronik (electronic mail facility), yaitu worm mengirimkan kopian dirinya ke sistem-sistem lain.
- Kemampuan eksekusi jarak jauh (remote execution capability), yaitu worm mengeksekusi kopian dirinya di sistem lain.
- Kemampuan login jarak jauh (remote login capability), yaitu worm log pada sistem jauh sebagai pemakai dan kemudian menggunakan perintah untuk mengkopi dirinya dari satu sistem ke sistem lain. Kopian program worm yang baru kemudian dijalankan di sistem jauh

dan melakukan fungsi-fungsi lain yang dilakukan di sistem itu, worm terus menyebar dengan cara yang sama.

- Network worm mempunyai ciri-ciri yang sama dengan virus komputer, yaitu mempunyai fase-fase sama, yaitu : Dormant phase, Propagation phase, Trigerring phase, Execution phase.
- Network worm juga berusaha menentukan apakah sistem sebelumnya telah diinfeksi sebelum mengirim kopian dirinya ke sistem itu.

7. Spam

- Spam adalah sejenis komersial email yang menjadi sampah mail (junkmail). Para spammer dapat mengirim jutaan email via internet untuk kepentingan promosi produk/info tertentu. Efeknya sangat mengganggu kenyamanan email pengguna dan berpotensi juga membawa virus/worm/trojan.

8. Spyware

- Spyware adalah suatu program dengan tujuan menyusupi iklan tertentu (adware) atau mengambil informasi penting dikomputer pengguna. Spyware berpotensi mengganggu kenyamanan pengguna dan mencuri data-data tertentu dikomputer pengguna untuk dikirim ke hacker. Efek spyware akan menkonsumsi memory computer sehingga computer menjadi lambat atau hang.

Siklus hidup Virus melalui empat fase (tahap), yaitu :

1. **Fase tidur (dormant phase).** Virus dalam keadaan menganggur. Virus akan tiba-tiba aktif oleh suatu kejadian seperti tibanya tanggal tertentu, kehadiran program atau file tertentu, atau kapasitas disk yang melewati batas. Tidak semua virus mempunyai tahap ini.
2. **Fase propagasi (propagation phase).** Virus menempatkan kopian dirinya ke program lain atau daerah sistem tertentu di disk. Program yang terinfeksi virus akan mempunyai kloning virus. Kloning virus itu dapat kembali memasuki fase propagasi.
3. **Fase pemicuan (triggering phase).** Virus diaktifkan untuk melakukan fungsi tertentu. Seperti pada fase tidur, fase pemicuan dapat disebabkan beragam kejadian sistem termasuk penghitungan jumlah kopian dirinya.
4. **Fase eksekusi (execution phase).** Virus menjalankan fungsinya, fungsinya mungkin sepele seperti sekedar menampilkan pesan dilayar atau merusak seperti merusak program dan file-file data, dan sebagainya. Kebanyakan virus melakukan kerjanya untuk suatu sistem operasi tertentu, lebih spesifik lagi pada platform perangkat keras tertentu. Virus-virus dirancang memanfaatkan rincian-rincian dan kelemahan-kelemahan sistem tertentu.

Klasifikasi:

Klasifikasi tipe virus :

1. **Parasitic virus.** Merupakan virus tradisional dan bentuk virus yang paling sering. Tipe ini mencantolkan dirinya ke file .exe. Virus mereplikasi ketika program terinfeksi dieksekusi dengan mencari file-file .exe lain untuk diinfeksi.
2. **Memory resident virus.** Virus memuatkan diri ke memori utama sebagai bagian program yang menetap. Virus menginfeksi setiap program yang dieksekusi.
3. **Boot sector virus.** Virus menginfeksi master boot record atau boot record dan menyebar saat sistem diboot dari disk yang berisi virus.
4. **Stealth virus.** Virus yang bentuknya telah dirancang agar dapat menyembunyikan diri dari deteksi perangkat lunak antivirus.
5. **Polymorphic virus.** Virus bermutasi setiap kali melakukan infeksi. Deteksi dengan penandaan virus tersebut tidak dimungkinkan. Penulis virus dapat melengkapi dengan alat-alat bantu penciptaan virus baru (virus creation toolkit, yaitu rutin-rutin untuk menciptakan virus-virus baru). Dengan alat bantu ini penciptaan virus baru dapat dilakukan dengan cepat. Virus-virus yang diciptakan dengan alat bantu biasanya kurang canggih dibanding virus-virus yang dirancang dari awal.

Program Anti virus

Perkembangan program antivirus dapat diperiode menjadi empat generasi, yaitu :

1. **Generasi pertama** : sekedar scanner sederhana. Antivirus menscan program untuk menemukan penanda (signature) virus. Walaupun virus mungkin berisi karakter-karakter varian, tapi secara esensi mempunyai struktur dan pola bit yang sama di semua kopiannya. Teknis ini terbatas untuk deteksi virus-virus yang telah dikenal. Tipe lain antivirus generasi pertama adalah mengelola rekaman panjang (ukuran) program dan memeriksa perubahan panjang program.
2. **Generasi kedua** : scanner yang pintar (heuristic scanner). Antivirus menscan tidak bergantung pada penanda spesifik. Antivirus menggunakan aturan-aturan pintar (heuristic rules) untuk mencari kemungkinan infeksi virus. Teknik yang dipakai misalnya mencari fragmen- fragmen kode yang sering merupakan bagian virus. Contohnya, antivirus mencari awal loop enkripsi yang digunakan polymorphic virus dan menemukan kunci enkripsi. Begitu kunci ditemukan, antivirus dapat mendeskripsi virus untuk identifikasi dan kemudian menghilangkan infeksi virus. Teknik ini adalah pemeriksanaan integritas. Checksum dapat ditambahkan di tiap program. Jika virus menginfeksi program tanpa mengubah checksum, maka pemeriksaan integritas akan menemukan perubahan itu. Untuk menanggulangi virus canggih yang mampu mengubah checksum saat

menginfeksi program, fungsi hash terenkripsi digunakan. Kunci enkripsi disimpan secara terpisah dari program sehingga program tidak dapat menghasilkan kode hash baru dan mengenkripsinya. Dengan menggunakan fungsi hash bukan checksum sederhana maka mencegah virus menyesuaikan program yang menghasilkan kode hash yang sama seperti sebelumnya.

3. Generasi ketiga : jebakan-jebakan aktivitas (activity trap). Program antivirus merupakan program yang menetap di memori (memory resident program). Program ini mengidentifikasi virus melalui aksi-aksinya bukan dari struktur program yang diinfeksi. Dengan antivirus semacam ini tak perlu mengembangkan penanda-penanda dan aturan-aturan pintar untuk beragam virus yang sangat banyak. Dengan cara ini yang diperlukan adalah mengidentifikasi kumpulan instruksi yang berjumlah sedikit yang mengidentifikasi adanya usaha infeksi. Kalau muncul kejadian ini, program antivirus segera mengintervensi.

4. Generasi keempat : proteksi penuh (full featured protection). Antivirus generasi ini menggunakan beragam teknik antivirus secara bersamaan. Teknik-teknik ini meliputi scanning dan jebakan-jebakan aktivitas. Antivirus juga mempunyai senarai kapabilitas pengaksesan yang membatasi kemampuan virus memasuki sistem dan membatasi kemampuan virus memodifikasi file untuk menginfeksi file. Pertempuran antara penulis virus dan pembuat antivirus masih berlanjut. Walau beragam strategi lebih lengkap telah dibuat untuk menanggulangi virus, penulis virus pun masih berlanjut menulis virus yang dapat melewati barikade-barikade yang dibuat penulis antivirus. Untuk pengaman sistem komputer, sebaiknya pengaksesandan pemakaian komputer diawasi dengan seksama sehingga tidak menjalankan program atau memakai disk yang belum terjamin kebersihannya dari infeksi virus. Pencegahan terbaik terhadap ancaman virus adalah mencegah virus memasuki sistem disaat yang pertama.

Anti virus

- Solusi ideal terhadap ancaman virus adalah **pencegahan**. Jaringan tidak ijinkan virus masuk ke sistem. Sasaran ini, tak mungkin dilaksanakan sepenuhnya. Pencegahan dapat mereduksi sejumlah serangan virus.

Setelah pencegahan terhadap masuknya virus, maka pendekatan berikutnya yang dapat dilakukan adalah :

1. **Deteksi.** Begitu infeksi telah terjadi, tentukan apakah infeksi memang telah terjadi dan cari lokasi virus.
2. **Identifikasi.** Begitu virus terdeteksi maka identifikasi virus yang menginfeksi

program.

3. **Penghilangan.** Begitu virus dapat diidentifikasi maka hilangkan semua jejak virus dari program yang terinfeksi dan program dikembalikan ke semua (sebelum terinfeksi). Jika deteksi virus sukses dilakukan, tapi identifikasi atau penghilangan jejak tidak dapat dilakukan, maka alternatif yang dilakukan adalah menghapus program yang terinfeksi dan kopi kembali backup program yang masih bersih.

Daftar Pustaka

- <http://www.infokom.id/2016/01/identifikasi-resiko-keamanan-jaringan.html>
- <http://www.slideshare.net/jagoanilmu/modul-1-pendahuluan-keamanan-jaringan-komputer>
- https://id.wikipedia.org/wiki/Perangkat_perusak
- <http://tamrenata.blogspot.co.id/2013/09/inilah-berbagai-jenis-virus-komputer.html>



MODUL PERKULIAHAN

Keamanan Jaringan

Evaluasi Keamanan WAN

Fakultas
Fasilkom

Program Studi
Teknik Informatika

TatapMuka
04

Kode MK
MK:15020

Di susun Oleh
Tim Dosen

Abstract

Keamanan jaringan ([Bahasa Inggris: Network Security](#)) dalam [jaringan komputer](#) sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah.

Kompetensi

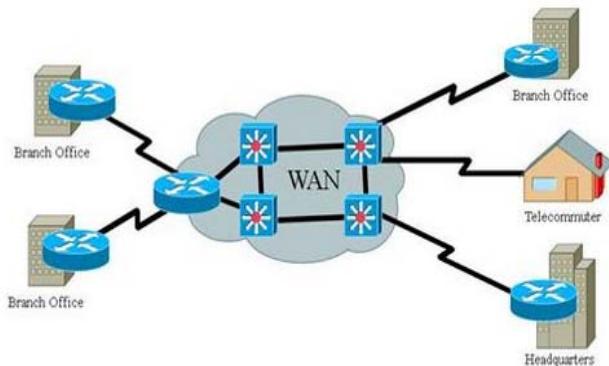
Setelah membaca modul ini diharapkan mahasiswa :

- [**Evaluasi Keamanan WAN/Sistem Informasi**](#)
- [**Sumber Lubang\(Hole\) keamanan pada WAN/Sistem informasi**](#)

WAN (Wide Area network)

A **wide area network (WAN)** is a telecommunications **network** or computer **network** that extends over a large geographical distance. **Wide area networks** are often established with leased telecommunication circuits.

WAN Definition



- Mencakup daerah geografis yang luas, sertingkali mencakup sebuah negara atau benua. Dan memiliki banyak elemen switching
- Dengan sistem jaringan ini, pertukaran data antar kantor dapat dilakukan dengan cepat serta dengan biaya yang relatif murah.
- Sistem jaringan ini dapat menggunakan jaringan Internet yang sudah ada, untuk menghubungkan antara kantor pusat dan kantor cabang atau dengan PC Stand Alone/Notebook yang berada di lain kota ataupun negara.

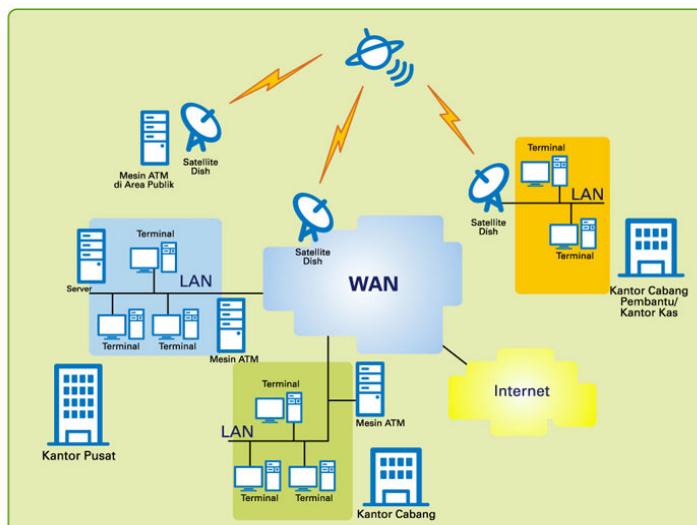
Keuntungan Jaringan WAN.

- Server kantor pusat dapat berfungsi sebagai bank data dari kantor cabang.
- Komunikasi antar kantor dapat menggunakan E-Mail & Chat.
- Dokumen/File yang biasanya dikirimkan melalui fax ataupun paket pos, dapat dikirim melalui E-mail dan Transfer file dari/ke kantor pusat dan kantor cabang dengan biaya yang relatif murah dan dalam jangka waktu yang sangat cepat.
- Pooling Data dan Updating Data antar kantor dapat dilakukan setiap hari pada waktu yang ditentukan.



Konsep Jaringan WAN

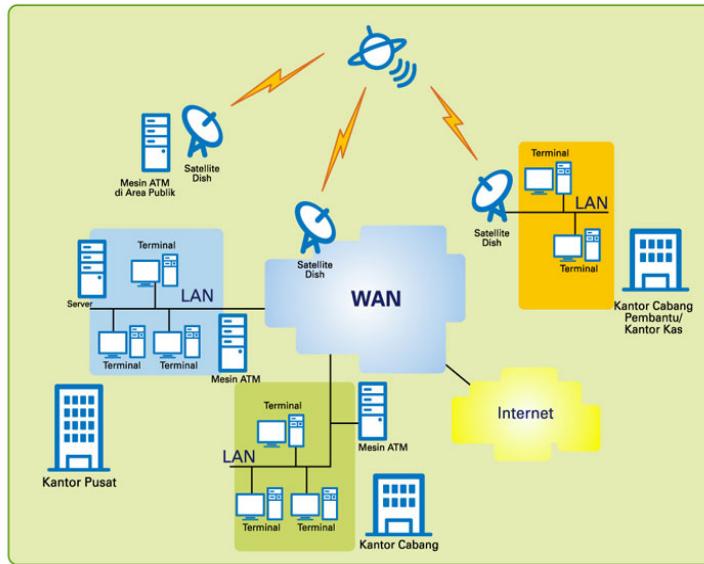
- Untuk mengoneksikan jaringan WAN kita harus menggunakan alat khusus yang bekerja sebagai pusat layanan, misalnya satelit VSAT.
- VSAT merupakan jaringan atau sistem komunikasi satelit yang terdiri atas sejumlah stasiun remote (terminal VSAT) dengan menggunakan antena parabola berdiameter lebih kecil dibandingkan dengan komunikasi satelit lainnya, menggunakan sebuah atau sebagian transponder satelit sebagai pengulang (repeater) dengan didukung peralatan pada stasiun dan sebuah stasiun bumi utama.
- Di sini VSAT berperan sebagai media penghubung antara suatu jaringan LAN.



- Pada sistem WAN dengan media VSAT maka selain server pada tiap jaringan LAN-nya masih ada server lain yang lebih besar yang berada pada stasiun Hub.
- Server ini akan mengontrol komunikasi antar terminal VSAT yang berada di bawahnya. Server yang berada pada stasiun terminal hanya menampung data dari workstation-workstation yang ada di bawahnya.
- Sistem kerja dari WAN adalah seperti halnya jaringan LAN hanya jika diinginkan transfer data dari user di terminal VSAT yang lain maka server yang berada pada terminal VSAT tersebut akan menghubungi stasiun Hub dan stasiun Hub akan menghubungkan dengan

terminal VSAT yang diinginkan sehingga transfer data yang diinginkan dapat terjadi.

- Selain digunakan untuk transfer data jaringan VSAT pada konfigurasi WAN juga dapat digunakan untuk transfer video maupun voice.



Infrastruktur Jaringan WAN

Seperti LAN (Local Area Network), Terdapat sejumlah perangkat yang melewatkkan aliran informasi data dalam sebuah WAN. Penggabungan perangkat tersebut akan menciptakan infrastruktur WAN. Perangkat-perangkat tersebut adalah :

- **Router**

Router adalah peningkatan kemampuan dari bridge. Router mampu menunjukkan rute/jalur (route) dan memfilter informasi pada jaringan yang berbeda. Beberapa router mampu secara otomatis mendeteksi masalah dan mengalihkan jalur informasi dari area yang bermasalah.

- **ATM Switch**

Switch ATM menyediakan transfer data berkecepatan tinggi antara LAN dan WAN.

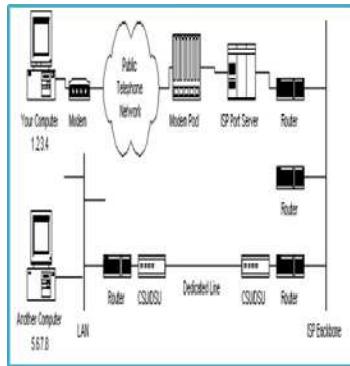
- ***Modem and CSU/DSU***

Modem mengkonversi sinyal digital dan analog. Pada pengirim, modem mengkonversi sinyal digital ke dalam bentuk yang sesuai dengan teknologi transmisi untuk dilewatkan melalui fasilitas komunikasi analog atau jaringan telepon (public telephone line).

Di sisi penerima, modem mengkonversi sinyal ke format digital kembali.

- ***CSU/DSU (Channel Service Unit / Data Service Unit)***

CSU/DSU sama seperti modem, hanya saja CSU/DSU mengirim data dalam format digital melalui jaringan telephone digital. CSU/DSU biasanya berupa kotak fisik yang merupakan dua unit yang terpisah : CSU atau DSU.



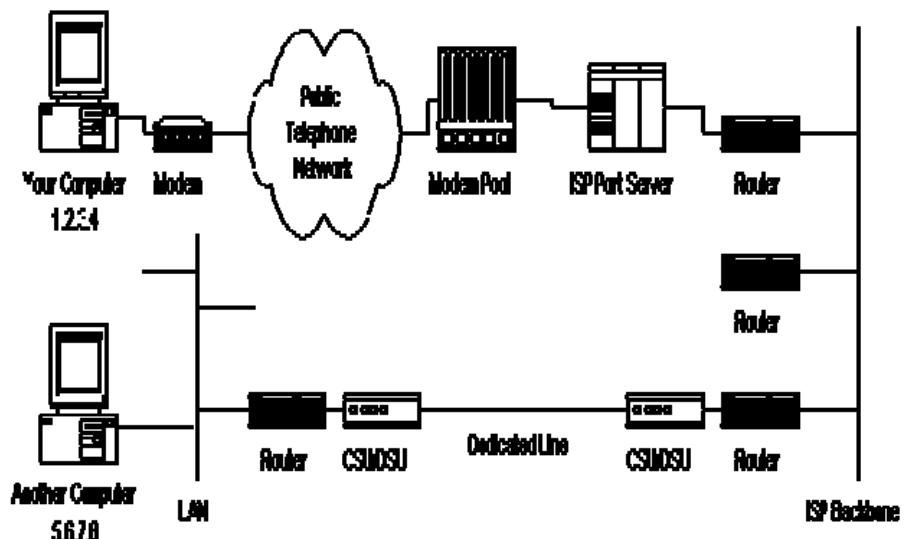
Seperti LAN (Local Area Network), Terdapat sejumlah perangkat yang melewatkkan aliran informasi data dalam sebuah WAN. Penggabungan perangkat tersebut akan menciptakan infrastruktur WAN. Perangkat-perangkat tersebut adalah :

Communication Server

Communication Server adalah server khusus dial in/out, bagi pengguna untuk dapat melakukan dial dari lokasi remote sehingga dapat terhubung ke LAN.

- **X.25/Frame Relay Switches**

Switch X.25 dan Frame Relay menghubungkan data lokal/private melalui jaringan data, menggunakan sinyal digital. Unit ini sama dengan switch ATM, tetapi kecepatan transfer datanya lebih rendah dibanding dengan ATM.



<http://klinikschool-konsepjaringanwan.blogspot.com>

Internet

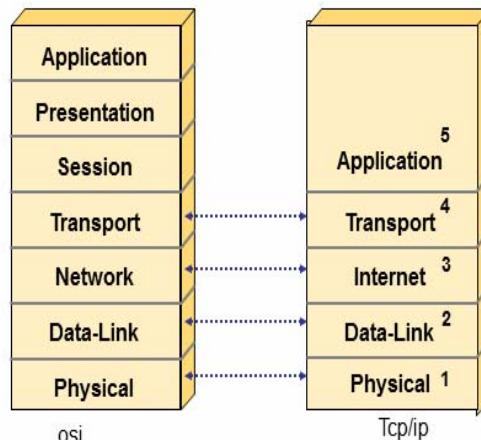
The **internet** is an informal term for the world-wide communication network of computers.

The internet is used to send information quickly between computers around the world. It has millions of smaller domestic, academic, business, and government networks and websites, which together carry many different kinds of information (facts and details) and services. So in other words, the Internet is a network of networks

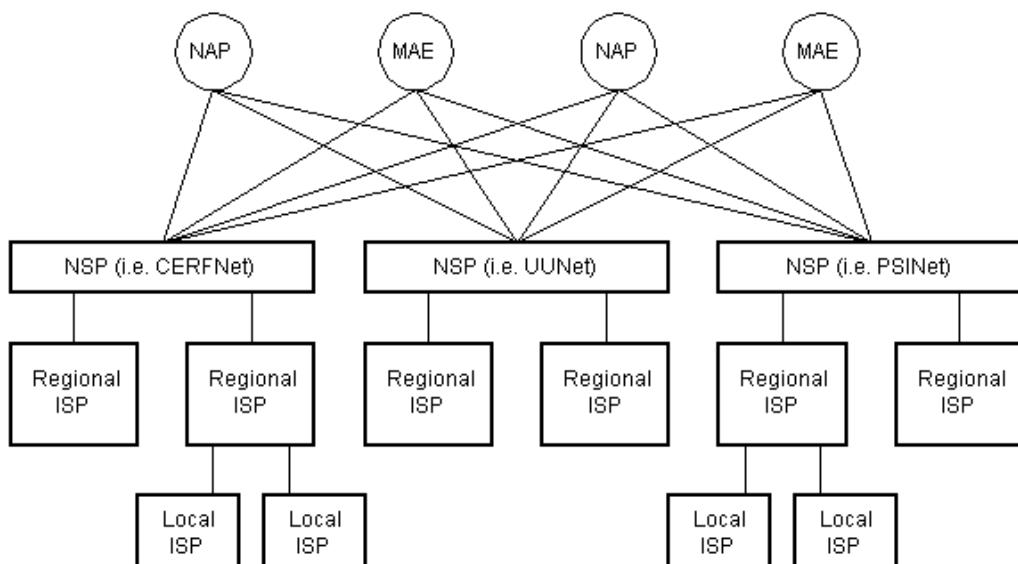
- **Internet** adalah sekumpulan komputer atau server yang saling terhubung satu sama lain melalui berbagai macam media (kabel, radio, satelit dll). Komputer-komputer tersebut letaknya tersebar di seluruh belahan dunia sehingga memungkinkan terbentuknya suatu jaringan informasi global.
- Sekumpulan komputer di suatu tempat memiliki jenis dan karakteristik yang tidak sama dengan tempat-tempat lain, namun semuanya dihubungkan oleh suatu protokol standard yang sama yang disebut TCP/IP (*Transfer Control Protocol/Internet Protocol*).
- TCP/IP ini dapat diumpamakan sebagai bahasa yang dimengerti oleh semua jenis komputer yang terhubung ke Internet. Tanpa mengikuti protokol standard ini, komputer kita tidak akan mampu berkomunikasi dengan komputer-komputer lain di Internet

Protocol TCP/IP

• Protocol Standar Internet



Internet Infrastructure

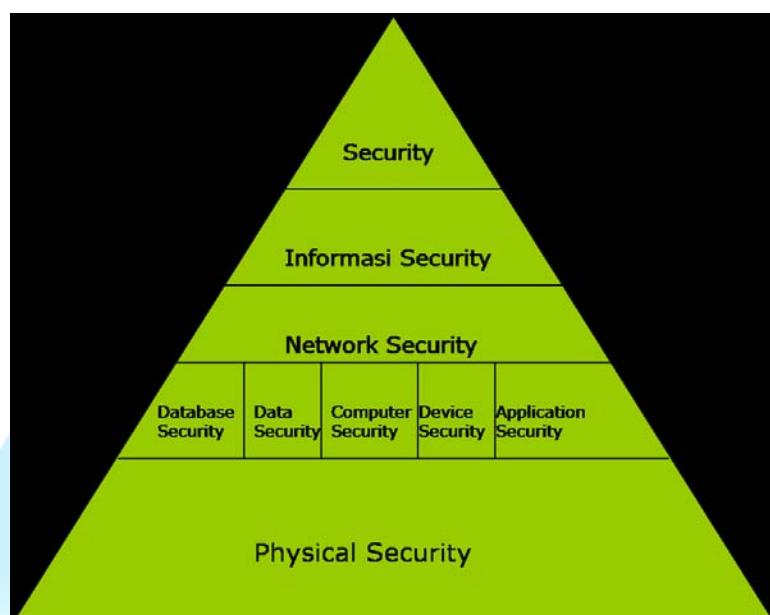


The Internet backbone is made up of many large networks which interconnect with each

other. These large networks are known as **Network Service Providers** or **NSPs**. Some of the large NSPs are UUNet, CerfNet, IBM, BBN Planet, SprintNet, PSINet, as well as others. These networks **peer** with each other to exchange packet traffic. Each NSP is required to connect to three **Network Access Points** or **NAPs**. At the NAPs, packet traffic may jump from one NSP's backbone to another NSP's backbone. NSPs also interconnect at **Metropolitan Area Exchanges** or **MAEs**. MAEs serve the same purpose as the NAPs but are privately owned. NAPs were the original Internet interconnect points. Both NAPs and MAEs are referred to as Internet Exchange Points or **IXs**. NSPs also sell bandwidth to smaller networks, such as ISPs and smaller bandwidth providers

<https://web.stanford.edu/class/msande91si/www-spr04/readings/week1/InternetWhitepaper.htm>

Evaluasi Keamanan



Evaluasi & Sumber

Pentingnya Evaluasi

- Lubang keamanan diketemukan hampir setiap hari.
 - Perangkat lunak dan perangkat keras biasanya sangat kompleks sehingga tidak mungkin untuk diuji seratus persen. Kadang-kadang ada lubang keamanan yang ditimbulkan oleh kecerobohan implementasi.
- Kesalahan konfigurasi bisa terjadi.
 - Kadang-kadang karena lalai atau alpa, konfigurasi sebuah sistem kurang benar sehingga menimbulkan lubang keamanan. Misalnya mode (permission atau kepemilikan) dari berkas yang menyimpan password (/etc/passwd di sistem UNIX) secara tidak sengaja diubah sehingga dapat diubah atau ditulis oleh orang-orang yang tidak berhak.
- Penambahan perangkat baru yang mengubah konfigurasi yang sudah ada.
 - Operator dan administrator harus belajar lagi. Dalam masa belajar ini banyak hal yang jauh dari sempurna, misalnya server atau software masih menggunakan konfigurasi awal dari vendor (dengan password yang sama)

Sumber Lubang Keamanan

1. Salah Disain (design flaw)

- Umumnya jarang terjadi. Akan tetapi apabila terjadi sangat sulit untuk diperbaiki. Akibat disain yang salah, maka biarpun dia diimplementasikan dengan baik, kelemahan dari sistem akan tetap ada.

Contoh :

- Lemah disainnya algoritma enkripsi ROT13 atau Caesar cipher, dimana karakter digeser 13 huruf atau 3 huruf. Meskipun diimplementasikan dengan programming yang sangat teliti, siapapun yang mengetahui algoritmanya dapat memecahkan enkripsi tersebut.
- Kesalahan disain urutan nomor (sequence numbering) dari paket TCP/IP. Kesalahan ini dapat dieksplorasi sehingga timbul masalah yang dikenal dengan nama **“IP spoofing”** (sebuah host memalsukan diri seolah-olah menjadi host lain dengan membuat paket palsu setelah engamati urutan paket dari host yang hendak diserang).

2. Implementasi kurang baik

- Banyak program yang diimplementasikan secara terburu-buru sehingga kurang cermat dalam pengkodean.
- Akibat tidak adanya cek atau testing implementasi suatu program yang baru dibuat.

Contoh:

- Tidak memperhatikan batas (“bound”) dari sebuah “array” tidak dicek sehingga

- terjadi yang disebut out-of-bound array atau buffer overflow yang dapat dieksplorasi (misalnya overwrite ke variable berikutnya).
- Kelelahan memfilter karakter-karakter yang aneh-aneh yang dimasukkan sebagai input dari sebuah program sehingga sang program dapat mengakses berkas atau informasi yang semestinya tidak boleh diakses.

3. Salah konfigurasi

Contoh :

- Berkas yang semestinya tidak dapat diubah oleh pemakai secara tidak sengaja menjadi "writeable". Apabila berkas tersebut merupakan berkas yang penting, seperti berkas yang digunakan untuk menyimpan password, maka efeknya menjadi lubang keamanan. Kadangkala sebuah komputer dijual dengan konfigurasi yang sangat lemah.
- Adanya program yang secara tidak sengaja diset menjadi "setuid root" sehingga ketika dijalankan pemakai memiliki akses seperti super user (root) yang dapat melakukan apa saja.

4. Salah menggunakan program atau sistem

Contoh :

- Kesalahan menggunakan program yang dijalankan dengan menggunakan account root (super user) dapat berakibat fatal.

Penguji Keamanan Sistem

Untuk memudahkan administrator dari sistem informasi membutuhkan "automated tools", perangkat pembantu otomatis, yang dapat membantu menguji atau meng-evaluasi keamanan sistem yang dikelola.

Contoh Tools Terintegrasi:

Perangkat lunak bantu	Sistem Operasi
Cops	UNIX
Tripwire	UNIX
Satan/Saint	UNIX
SBScan: localhost security scanner	UNIX
Ballista < http://www.secnet.com >	Windows NT
Dan sebagainya... (cari sendiri!)	

Contoh Tools Pengujian yang dibuat para hacker :

Tools	Kegunaan
Crack	program untuk menduga atau memecahkan password dengan menggunakan sebuah atau beberapa kamus (dictionary). Program crack ini melakukan brute force cracking dengan mencoba mengenkripsi sebuah kata yang diambil dari kamus, dan kemudian membandingkan hasil enkripsi dengan password yang ingin dipecahkan.
land latierra	sistem Windows 95/NT menjadi macet (hang, lock up). Program ini mengirimkan sebuah paket yang sudah di"spoofed" sehingga seolah-olah paket tersebut berasal dari mesin yang sama dengan menggunakan port yang terbuka
Ping-o-death	sebuah program (ping) yang dapat meng-crash-kan Windows 95/NT dan beberapa versi Unix.
Winuke	program untuk memacetkan sistem berbasis Windows
Dan sebagainya... (cari sendiri!)	

Probing Services

- Defenisi Probing : “probe” (meraba) servis apa saja yang tersedia. Program ini juga dapat digunakan oleh kriminal untuk melihat servis apa saja yang tersedia di sistem yang akan diserang dan berdasarkan data-data yang diperoleh dapat melancarkan serangan.
- Servis di Internet umumnya dilakukan dengan menggunakan protokol TCP atau UDP. Setiap servis dijalankan dengan menggunakan port yang berbeda, misalnya:
 - ❖ SMTP, untuk mengirim dan menerima e-mail, TCP, port 25
 - ❖ POP3, untuk mengambil e-mail, TCP, port 110
- Contoh di atas hanya sebagian dari servis yang tersedia. Di system UNIX, lihat berkas /etc/services dan /etc/inetd.conf untuk melihat servis apa saja yang dijalankan oleh server atau komputer yang bersangkutan.
- Untuk beberapa servis yang berbasis TCP/IP, proses probe dapat dilakukan dengan menggunakan program telnet.
 - ❖ Misalnya untuk melihat apakah ada servis e-mail dengan menggunakan SMTP digunakan telnet ke port 25 dan port 110.
 - ✓ unix% telnet target.host.com 25

- ✓ unix% telnet localhost 110
- ❖ Dengan mengamati entry di dalam berkas log, dapat diketahui adanya probing.

Contoh : root# tail /var/log/syslog

May 16 15:40:42 epson tcplogd: "Syn probe"

notebook[192.168.1.4]:[8422]-

epson[192.168.1.2]:[635]

Dari contoh diatas diketahui IP : 192.168.1.4 melakukan probing.

Program penguji probing (penguji semua port otomatis) :

Paket probe untuk sistem UNIX

- nmap
- strobe
- tcpprobe

Probe untuk sistem Window

- NetLab
- Cyberkit
- Ogre

Program yang memonitor adanya probing ke system

Probing biasanya meninggalkan jejak di berkas log di system anda. Dengan mengamati entry di dalam berkas log dapat diketahui adanya probing. Selain itu, ada juga program untuk memonitor probe seperti paket program courtney, portsentry dan tcplogd.

OS Finger Printing

- Mengetahui operating system (OS) dari target yang akan diserang merupakan salah satu pekerjaan pertama yang dilakukan oleh seorang cracker. Setelah mengetahui OS yang dituju, dia dapat melihat database kelemahan sistem yang dituju.
- Fingerprinting merupakan istilah yang umum digunakan untuk menganalisa OS sistem yang dituju.

Metode Fingerprinting :

Cara yang paling konvensional :

- Service telnet ke server yang dituju, jika server tersebut kebetulan menyediakan servis telnet, seringkali ada banner yang menunjukkan nama OS beserta versinya.
- Service FTP di port 21. Dengan melakukan telnet ke port tersebut dan memberikan perintah "SYST" anda dapat mengetahui versi dari OS yang digunakan.

Melakukan finger ke Web server, dengan menggunakan program netcat (nc).

- Cara fingerprinting yang lebih canggih adalah dengan menganalisa respon sistem terhadap permintaan (request) tertentu. Misalnya dengan menganalisa nomor urut packet

TCP/IP yang dikeluarkan oleh server tersebut dapat dipersempit ruang jenis dari OS yang digunakan. Ada beberapa tools untuk melakukan deteksi OS ini antara lain:

- nmap
- queso

Penggunaan program penyerang

- Untuk mengetahui kelemahan sistem informasi adalah dengan menyerang diri sendiri dengan paket-paket program penyerang (attack) yang dapat diperoleh di Internet.
- Selain program penyerang yang sifatnya agresif melumpuhkan sistem yang dituju, ada juga program penyerang yang sifatnya melakukan pencurian atau penyadapan data.
- Untuk penyadapan data, biasanya dikenal dengan istilah “sniffer”. Meskipun data tidak dicuri secara fisik (dalam artian menjadi hilang), sniffer ini sangat berbahaya karena dia dapat digunakan untuk menyadap password dan informasi yang sensitif. Ini merupakan serangan terhadap aspek privacy.

Contoh program penyadap (sniffer) antara lain:

- pcapture (Unix)
- sniffit (Unix)
- tcpdump (Unix)
- WebXRay (Windows)

Penggunaan sistem pemantau jaringan

- Sistem pemantau jaringan (network monitoring) dapat digunakan untuk mengetahui adanya lubang keamanan.

Misalnya apabila anda memiliki sebuah server yang semetinya hanya dapat diakses oleh orang dari dalam, akan tetapi dari pemantau jaringan dapat terlihat bahwa ada yang mencoba mengakses melalui tempat lain. Selain itu dengan pemantau jaringan dapat juga dilihat usaha-usaha untuk melumpuhkan sistem dengan melalui denial of service attack (DoS) dengan mengirimkan packet yang jumlahnya berlebihan.

- Network monitoring biasanya dilakukan dengan menggunakan protokol SNMP (Simple Network Management Protocol).

Program network monitoring / management :

- Etherboy (Windows), Etherman (Unix)
- HP Openview (Windows)
- Packetboy (Windows), Packetman (Unix)
- SNMP Collector (Windows)
- Webboy (Windows)

Program pemantau jaringan yang tidak menggunakan SNMP :

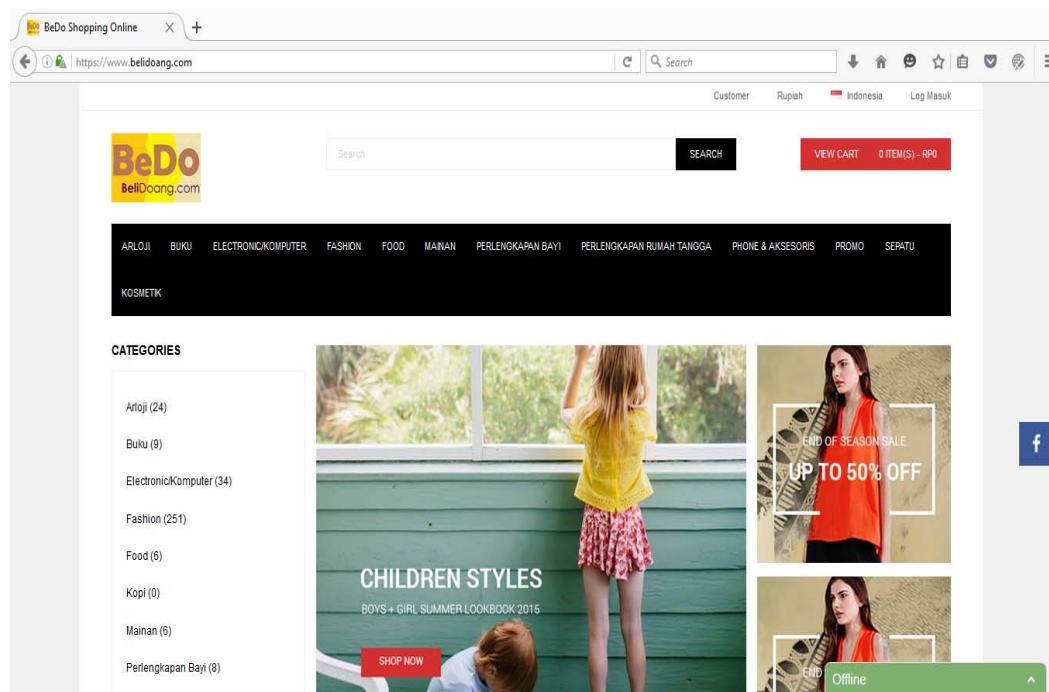
- iplog, icmplog, updlog, yang merupakan bagian dari paket iplog untuk memantau paket IP,

ICMP, UDP.

- iptraf, sudah termasuk dalam paket Linux Debian netdiag
- netwatch, sudah termasuk dalam paket Linux Debian netdiag
- ntop, memantau jaringan seperti program top yang memantau proses di sistem Unix
- trafshow, menunjukkan traffic antar hosts dalam bentuk text-mode.

Samples:

- Keamanan Sistem World Wide Web



WORLD WIDE WEB

- Merupakan sekumpulan dokumen multimedia yang saling terkoneksi, yang memudahkan perpindahan dari dokumen satu ke dokumen lainnya.
- Pada dasarnya suatu web, situs, atau homepage adalah bagian dari www.
- Untuk menampilkan www, kita membutuhkan web browser seperti internet explorer atau mozilla firefox. WWW bekerja dengan menggunakan teknologi yang disebut **hypertext**. Teknologi ini kemudian dikembangkan menjadi protokol aplikasi bernama hypertext transfer protocol (HTTP). Hypertext ini akan menggabungkan beberapa jenis representasi dan metode pengaksesan informasi dan menyajikan dalam beragam bentuk informasi seperti teks, suara, animasi, video dan lain sebagainya.

Keamanan Server WWW

- Keamanan server WWW biasanya merupakan masalah dari seorang **administrator**. Dengan memasang server WWW di sistem anda, maka anda membuka akses (meskipun

secara terbatas) kepada orang luar. Apabila server anda terhubung ke Internet dan memang server WWW anda disiapkan untuk publik, maka anda harus lebih berhati-hati sebab anda membuka pintu akses ke seluruh dunia.

- Membatasi akses melalui Kontrol Akses Sebagai penyedia informasi (dalam bentuk berkas-berkas), sering diinginkan pembatasan akses. Misalnya, diinginkan agar hanya orang-orang tertentu yang dapat mengakses berkas (informasi) tertentu. Pada prinsipnya ini adalah masalah kontrol akses.
- Keamanan yang paling mudah digunakan adalah authentikasi yang menggunakan user dan password. Banyak sekali ditemukan para admin atau web master menggunakan user dan password standar atau tidak dirubah sama sekali, dimana user dan password tersebut masih menggunakan default dari vendor pembuatnya.
- Baik password default untuk di perangkat jaringan atau password default untuk di aplikasi webbased. Sebut saja solusi Content
- Management Systems (CMS) seperti pembangunan sebuah web/portal dengan solusi CMS ini, banyak sekali masih menggunakan user dan password default dari opencart/mamboo/joomla/drupal/Aura/ dan lain-lain.
- **Password default**
 - Terutama web yang dibangun dengan CMS
 - Penanganan
 - Atur direktori administrator
 - Buat policy tentang password
 - Update patch CMS yang digunakan

The image shows a login form with the following fields and buttons:

- A header message: **Silahkan masukkan rincian login anda.**
- A "Nama Pengguna" field with a placeholder "Nama Pengguna".
- A "Kata Sandi" field with a placeholder "Kata Sandi".
- A blue link labeled **Lupa Kata Sandi**.
- A blue button labeled **Log Masuk**.

SSL (Secure Socket Layer)

- SSL merupakan salah satu metode enkripsi dalam komunikasi data yang dibuat oleh Netscape Communication Corporation. Sebagaimana yang dijelaskan dalam SSL Protocol

Internet Draft (The SSL Protocol, Version 3.0 oleh ALAN O. FREIER dan PAUL C. KOCHER, dapat Anda buka di <http://home.netscape.com/eng/ssl3/ssl-toc.html>.

- SSL adalah Protokol berlapis. Dalam tiap lapisannya, sebuah data terdiri dari panjang, deskripsi dan isi. SSL mengambil data untuk dikirimkan, dipecahkan kedalam blok-blok yang teratur, kemudian dikompres jika perlu, menerapkan MAC, dienkripsi, dan hasilnya dikirimkan. Di tempat tujuan, data didekripsi, verifikasi, dekompres, dan disusun kembali. Hasilnya dikirimkan ke klien di atasnya. (terjemahan bebas).
- SSL hanya mengenkripsi data yang dikirim lewat http. Bagaimana SSL berjalan dapat digambarkan sebagai berikut :
 - Pada saat koneksi mulai berjalan, klien dan server membuat dan mempertukarkan kunci rahasia, yang dipergunakan untuk mengenkripsi data yang akan dikomunikasikan. Meskipun sesi antara klien dan server diintip pihak lain, namun data yang terlihat sulit untuk dibaca karena sudah dienkripsi.
 - SSL mendukung kriptografi public key, sehingga server dapat melakukan autentikasi dengan metode yang sudah dikenal umum seperti RSA dan Digital Signature Standard (DSS).
 - SSL dapat melakukan verifikasi integritas sesi yang sedang berjalan dengan menggunakan algoritma digest seperti MD5 dan SHA. Hal ini menghindarkan pembajakan suatu sesi.

HTML dan URL

- Hypertext Markup Language (HTML) adalah perintah atau bahasa terformat yang digunakan untuk membuat halaman web pada internet. Ketika membuka sebuah halaman Web, browser menginterpretasikan perintah HTML pada halaman tersebut dalam bentuk teks dan grafik Universal resource locator (URL) adalah alamat internet, diterjemahkan dari umum ke khusus.

Contohnya seperti <https://www.belidoang.com>.

Pada penggunaan WWW, penunjukkan sumber informasi dengan metode URL merupakan konsep penanaman lokasi standar dari suatu file, direktori, komputer, lokasi komputernya dan metode yang dipakai.

Browser and Search Engine

- Browser adalah interface visual yang menginterpretasikan hypertext link dan dipakai untuk memandu dari satu situs ke situs lain.
- Search engine adalah program pencari dokumen berdasar kata tertentu, daftar dokumen yang ditampilkan akan berisi kata yang dimaksud. Biasanya, mesin pencari ini bekerja dengan mengirimkan sebuah bot atau spider untuk mendapatkan dokumen sebanyak mungkin. Kemudian program indeker, membaca dokumen tersebut dan membuat indeks berdasar kata yang

ditunjuk.

INTERNET AND WEB DEVELOPMENT

Interface Web memberikan kemudahan interaksi dengan sistem internet. Akses internet yang terbuka dan mudah mempercepat arus informasi.

Real-Time Interaction

- Merupakan istilah untuk menggambarkan sejumlah fitur komputer. Sistem operasi ini dapat segera merespon masukan begitu diberikan. Dalam animasi grafik, program ini menampilkan obyek bergerak dengan kecepatan yang normal.
- Basisdata waktu menyimpan data persis seperti keadaan dunia nyata dari waktu ke waktu. Real-time Interaction telah mengalami kemajuan seperti peluncuran stasiun radio berbasis internet, promosi iklan dan pemutaran film, peragaan online, menyampaian berita dan hiburan elektronik, pendidikan dan pelatihan online, serta teleconference.

HTML Authoriting and Java

- Dikembangkan oleh Sun Microsystem Corp. Bahasa ini memiliki kemampuan dan keunggulan seperti object-orientedprogramming, mendukung konsep sistem terbuka, mendukung pemakaian terdistribusi, baik dalam jaringan maupun internet,menghasilkan sistem yang aman, serta performasi tinggi dan dinamis. Dalam dunia Internet, Java digunakan untuk menyusun dan mengembangkan dokumen web yang menarik dan interaktif. Dengan Java, berbagai program aplikasi, animasi, multimedia dan database dapat dimasukkan dalam dokumen web.
- Dengan kemampuan tersebut, Java menjadi populer dan dimanfaatkan para pengembang sistem maupun para pengguna Internet. Apabila mengakses suatu alamat web berbasis bahasa Java, kita dapat menggunakan browser HotJava untuk memperoleh tampilan menarik, seperti animasi ataupun suara hasil pemograman Java.

Keamanan client WWW

- Dalam bagian terdahulu dibahas masalah yang berhubungan dengan server WWW. Dalam bagian ini akan dibahas masalah-masalah yang berhubungan dengan keamanan client WWW, yaitu pemakai (pengunjung) biasa.
- Keamanan di sisi client biasanya berhubungan dengan masalah privacy dan penyisipan virus atau trojan horse.

Berhubungan dengan masalah privacy

- Cookies untuk tracking kemana saja browsing
- Pengiriman informasi pribadi

Attack (via active script, javascript, java)

- Pengiriman data-data komputer (program apa yang terpasang, dsb.)
- DoS attack (buka windows banyak)
- Penyusupan virus, trojan horse, spyware

Daftar Pustaka

- <http://narudesign.blogspot.co.id/2012/09/kegunaan-software-putty.html>
- <http://narudesign.blogspot.co.id/2011/10/th3hack3rcom-site-komunitas-download.html>
- <https://citrabagus.wordpress.com/keamanan-jaringan-komputer/>
- <http://www.listpdf.com/si/sistem-keamanan-jaringan-wan-pdf.html>
- <https://sani97854.wordpress.com/2011/07/17/arsitektur-jaringan/>
- <http://ilmukomputer.org/2013/01/31/konsep-jaringan-wan/>
- <http://www.webopedia.com/TERM/S/SSL.html>



MODUL PERKULIAHAN

Keamanan Jaringan

Top 10 WAN Security Risk

Fakultas
Fasilkom

Program Studi
Teknik Informatika

TatapMuka
05

Kode MK
MK:15020

Di susun Oleh
Tim Dosen

Abstract

Keamanan jaringan ([Bahasa Inggris: Network Security](#)) dalam [jaringan komputer](#) sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah.

Kompetensi

Setelah membaca modul ini diharapkan mahasiswa :

- Mampu memahami konsep WAN & Infrastructure Internet dari sisi keamanan

Top 10 WAN Security Risk

Defining Terms – What are patches?

Patch Signature

A small "pattern-matching" file, necessary for detecting whether a specific patch is needed by a machine.

Patch Package

A larger file containing the actual payload, necessary for deploying the patch to a machine.

Importance of Patches

Security – A really important patch
Non-Security – A really important patch
OS Patch – A really important patch
App Patch – A really important patch
Critical – A really important patch
Recommended – A really important patch

Quite often these are meaningless distinctions. For instance Microsoft considers Operating System Service Packs as Application Patches! They also frequently mark Security fixes as non-Security patches!

Dell World User Forum



1. Un-patched Servers

- ✓ Server utk menangani internal
- ✓ Server utk menangani eksternal
- ✓ Banyak IT staf mengklaim sering patch, namun hampir tidak mungkin mem-patch seluruh server dg segera

2. Un-patched Client Software

- ✓ Banyak software yg gratisan (misalnya bawaan dari OS seperti IE dan OE) memiliki banyak bug .
- ✓ Malware seperti worm sering memanfaatkan celah ini
- ✓ Web browser dan email client harus sering dipatch
- ✓ Gunakan anti-virus yg menangani internet security

The screenshot shows a detailed patch report from QualysGuard Enterprise Suite. The main interface is titled 'Patch Report' and includes a 'Report Summary' section with statistics: Total Patches (155), Hosts Requiring Patches (14), and Vulnerabilities Addressed (318). The report is organized into three main sections: OPERATING SYSTEMS, PATCHES, and HOSTS.

- OPERATING SYSTEMS:** This section lists various Windows versions and their patch status. For example, Windows 2000 Service Pack 3-4 has 4 hosts requiring patches, while Windows 7 has 6 hosts requiring patches.
- PATCHES:** This section provides a detailed list of individual patches. One highlighted patch is MS10-012, which is a Microsoft SMB Server Remote Code Execution vulnerability. It was published 109 days ago and affects 4 hosts.
- HOSTS:** This section lists hosts that require specific patches. For instance, host 10.10.24.32 requires the MS10-012 patch. Another section shows hosts requiring the Microsoft SMB Server Remote Code Execution vulnerability, with host 10.10.24.48 requiring the MS08-022 patch.

Annotations with numbers 1 through 8 highlight specific items in the report, likely corresponding to numbered points in the accompanying text.

3. Insecure peer-to-peer sharing

- ✓ Banyak komputer mengijinkan file dan printer sharing
- ✓ Pertimbangkan folder apa yg boleh dishare
- ✓ OS pada W/S lebih longgar keamanannya dibanding OS utk Server
- ✓ Worm dan virus yg network-aware dapat memanfaatkan ini.

4. Insecure Password

- ✓ Password harus sulit ditebak
- ✓ Tidak boleh diletakkan ditempat yg mudah dilihat
- ✓ Password policy: panjang dan kombinasi password, jam kerja, akses tertentu
- ✓ Harus dihapus bila user tidak ada lagi
- ✓ Username pada server harus dirahasiakan

5. Dial-up Connection

- ✓ User dg internet account utk rumahan dapat mengakses komputernya di kantor dari rumah
- ✓ Dapat menyebabkan banyak virus dan worm mengancam jaringan di kantor .

6. Residential High-Speed Internet Connection

- ✓ Cable dan ADSL memiliki resiko yg sama dengan dial-up
- ✓ Kecenderungan utk selalu-on menjadikan resiko lebih tinggi
- ✓ Bila kecepatan di rumah tinggi dan di kantor rendah, ada kecenderungan utk downlod di rumah dan dibawa ke kantor .

7. Corporate Owned Laptops

- ✓ Sifat laptop yg portabel membuatnya memiliki banyak setting untuk koneksi di berbagai jaringan
- ✓ HD, RAM, CPU speed yg terbatas membuat agak sulit mem-patch agar tetap up-to-date

8. Employee Owned Laptops

- ✓ Resikonya sama dengan milik corporate, dg tambahan bhw tidak ada kontrol terhadap software yg diinstal
- ✓ Tidak ada jaminan pula bahwa laptop2 ini di-patch dan memiliki anti virus.

9. Network Devices

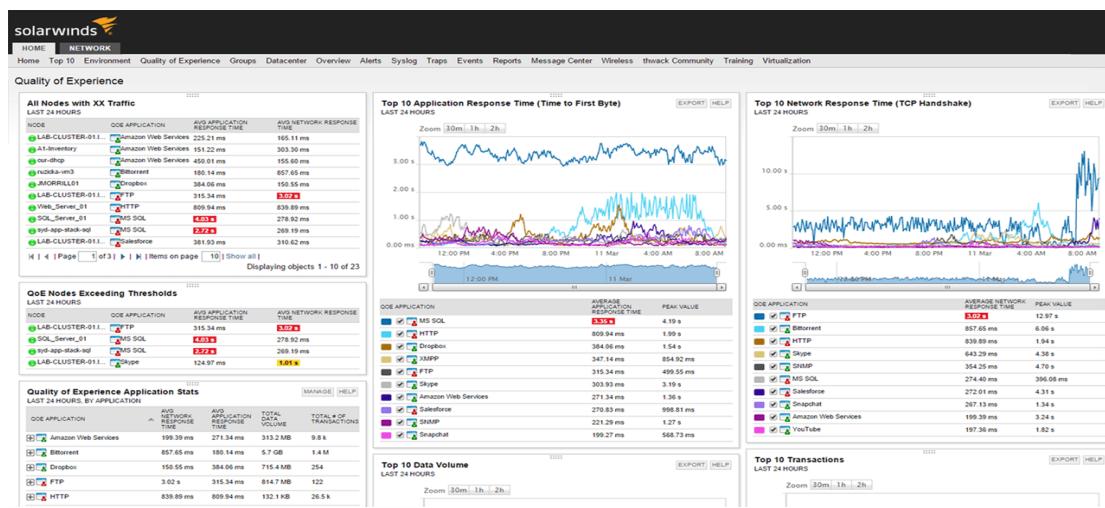
- ✓ Default Settings – Juga berlaku pd OS
- ✓ Keterbaruan peralatan jaringan
- ✓ Bila memungkinkan: upgrade firmware

10. Physical Access

- ✓ Jalur penarikan kabel
- ✓ Pertimbangan Line of Sight pada wireless
- ✓ Penempatan peralatan jaringan

Sistem Monitoring

- **Monitoring jaringan** adalah salah satu fungsi dari management yang berguna untuk menganalisa apakah jaringan masih cukup layak untuk digunakan atau perlu tambahan kapasitas.
- Hasil monitoring juga dapat membantu jika admin ingin mendesain ulang jaringan yang telah ada. Banyak hal dalam jaringan yang bisa dimonitoring, salah satu diantaranya load traffic jaringan yang lewat pada sebuah router atau interface komputer.
- Monitoring dapat dilakukan dengan standar SNMP, selain load traffic jaringan, kondisi jaringan pun harus dimonitoring, misalnya status up atau down dari sebuah peralatan jaringan.



- Sebuah sistem monitoring melakukan proses pengumpulan data mengenai dirinya sendiri dan melakukan analisis terhadap data-data tersebut dengan tujuan untuk memaksimalkan seluruh sumber daya yang dimiliki.
- Data yang dikumpulkan pada umumnya merupakan data yang real-time, baik data yang diperoleh dari sistem yang hard real-time maupun sistem yang soft real-time.
- Sistem yang real-time merupakan sebuah sistem dimana waktu yang diperlukan oleh sebuah komputer didalam memberikan stimulus ke lingkungan eksternal adalah suatu hal yang vital.
- Waktu didalam pengertian tersebut berarti bahwa sistem yang real-time menjalankan suatu pekerjaan yang memiliki batas waktu (deadline).
- Di dalam batas waktu tersebut suatu pekerjaan mungkin dapat terselesaikan dengan benar atau dapat juga belum terselesaikan.
- Sistem yang real-time mengharuskan bahwa suatu pekerjaan harus terselesaikan dengan benar.

Secara garis besar tahapan dalam sebuah sistem monitoring terbagi ke dalam tiga proses besar, yaitu:

1. Proses di dalam pengumpulan data monitoring,

2. Proses di dalam analisis data monitoring,
3. Proses di dalam menampilkan data hasil monitoring.

Proses di dalam sistem monitoring

- Sumber data dapat berupa network traffic, informasi mengenai hardware, dan lain sebagainya.
- Proses dalam analisis data dapat berupa pemilihan data dari sejumlah data yang telah terkumpul atau bisa juga berupa manipulasi data sehingga diperoleh informasi yang diharapkan.
- Sedangkan tahap menampilkan data hasil monitoring menjadi informasi yang berguna di dalam pengambilan keputusan atau kebijakan terhadap sistem yang sedang berjalan dapat berupa sebuah tabel, gambar, kurva, atau animasi.
- Aksi yang terjadi diantara proses-proses yang ada di dalam sebuah sistem monitoring adalah berbentuk service, yaitu suatu proses yang terus-menerus berjalan pada interval waktu tertentu.
- Proses yang dijalankan dapat berupa pengumpulan data dari objek yang di-monitor atau melakukan analisis data yang telah diperoleh dan menampilkannya.
- Proses yang terjadi tersebut bisa saja memiliki interval waktu yang berbeda.

Contoh interval

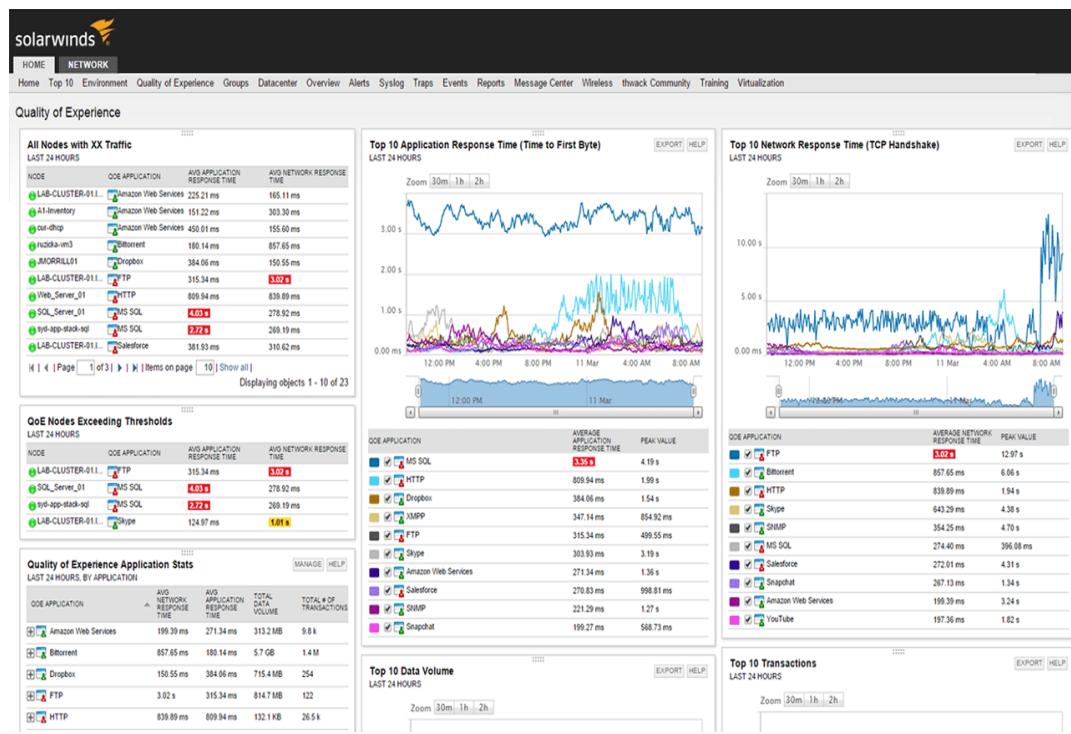
- Waktu didalam pengumpulan data dapat terjadi tiap lima menit sekali. Namun pada proses analisis data terjadi tiap satu jam sekali untuk menghasilkan informasi yang diharapkan membutuhkan lebih dari satu sampel data.
- **The Best Free Network Monitoring Tools**

<http://www.dnsstuff.com/free-network-monitoring-software>

Posted on November 25th, 2015

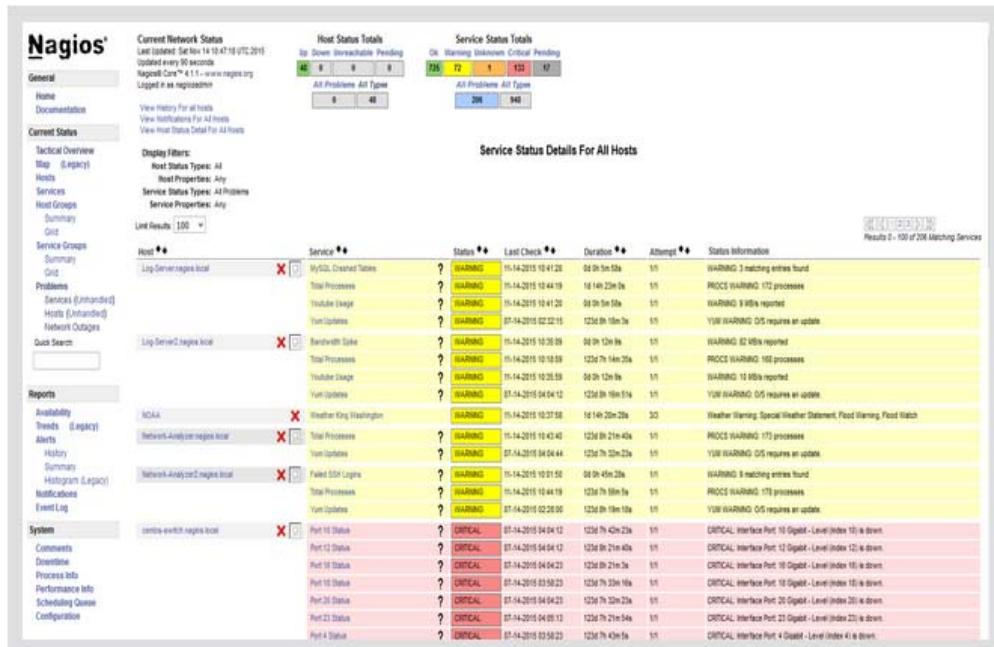
1.Solarwinds

When we need a monitoring tool that is easy to install, supports monitoring and reporting out of the box, we like [SolarWinds® Network Performance Monitor](#) (NPM). NPM acts as a single pane of glass to provide complete and comprehensive network monitoring capabilities that complement some of the essential free tools you may already use.



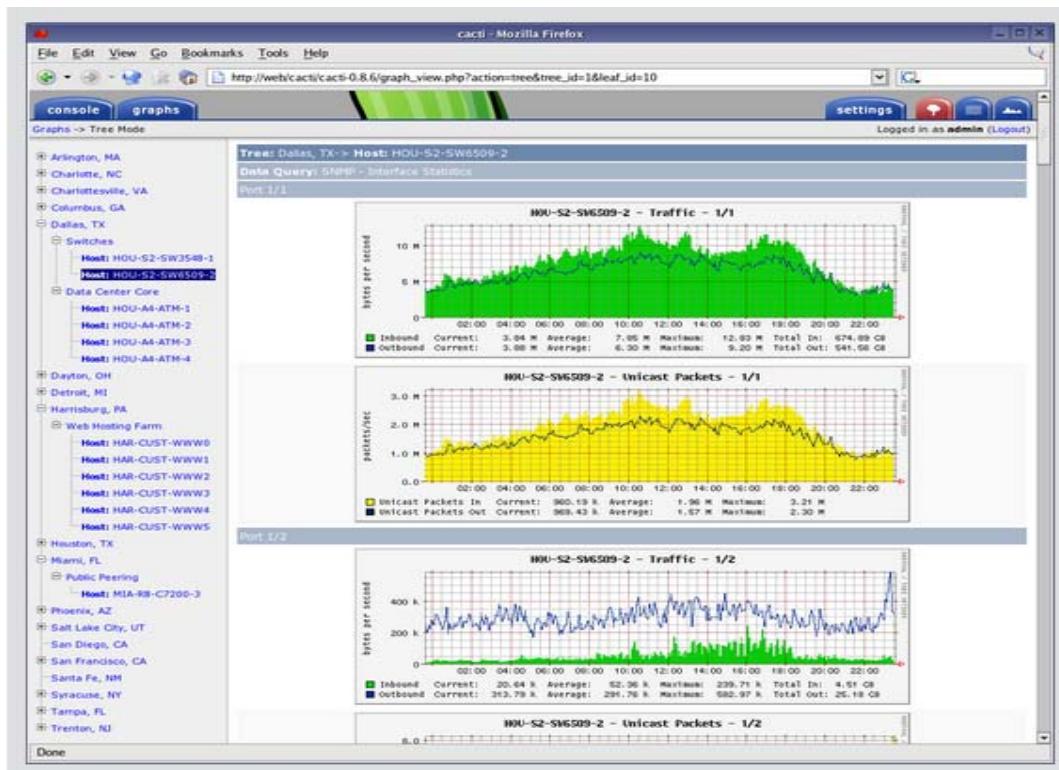
2. Nagios® is one of the most popular and widely used free network monitoring tools.

Network admins like Nagios because it does everything. Whatever it doesn't have can be built, or has been built by the Nagios community.

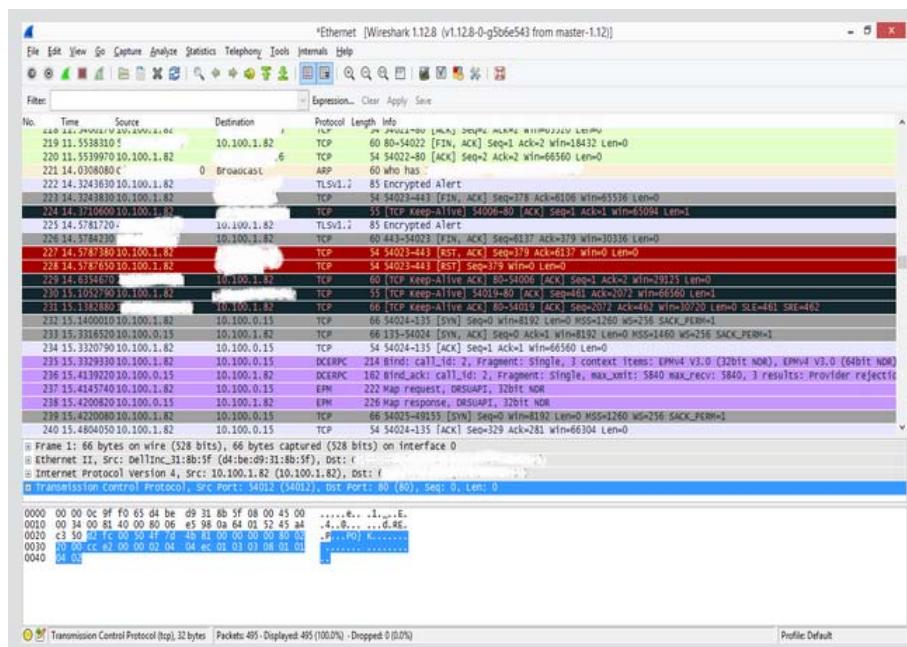


3.Cacti® is a network monitoring tool that allows you to collect data from almost any

network element, including routing and switching systems, firewalls, load balancers, and servers, and put that data into robust graphs. If you have a device, it's possible that Cacti's active community of developers has created a monitoring template for it.



4.Wireshark® is an open-source packet analyzer that uses libpcap (*nix) or winpcap (Windows®) to capture packets and display them on its graphical front end, while also providing good filtering, grouping, and analysis capabilities. It lets users capture traffic at wire speed, or read from packet dumps and analyze details at microscopic levels. Wireshark supports almost every protocol, and has functionalities that filter based on packet type, source, destination, etc. It has the ability to analyze VoIP calls, plot IO graphs for all traffic from an interface, decrypt many protocols, export the output, and lots more.



5.Zabbix® comes with a simple and clean GUI that makes it easy to manage, once you get the hang of it. Zabbix supports agent-less monitoring using technologies such as SNMP, ICMP, Telnet, SSH, etc., and agent-based monitoring for all Linux® distros, Windows® OS, and Solaris®. It supports a number of databases, including MySQL®, PostgreSQL™, SQLite, Oracle®, and IBM® DB2®. Zabbix's VMware® monitoring capabilities allow you to customize using any scripting or programming language, which is widely regarded as its best feature.

The screenshot shows the Zabbix Personal Dashboard with the following sections:

- Status of Zabbix:**

Parameter	Value	Details
Zabbix server is running	Yes	localhost:10051
Number of hosts (monitored/not monitored/templates)	85	47 / 0 / 38
Number of items (monitored/disabled/not supported)	503	493 / 0 / 9
Number of triggers (enabled/disabled) [problem/ok]	291	291 / 0 [10 / 281]
Number of users (online)	2	1
Required server performance, new values per second	7.7	-
- System status:**

Host group	Disaster	High	Average	Warning	Information	Not classified
Business System	0	0	0	0	0	0
Cloud	0	0	0	0	0	0
Database services	0	0	0	0	0	0
JBoss instances	0	0	0	3	0	0
Network Device	0	0	0	0	0	0
Private Cloud	0	0	0	5	0	0
Web servers	0	0	0	0	0	0
Zabbix services	0	0	0	2	0	0
- Host status:**

Host group	Without problems	With problems	Total
Business System	17	0	17
Cloud	2	0	2
Database services	2	0	2
JBoss instances	0	3	3
Network Devices	13	0	13
Private Cloud	0	5	5
Web servers	1	0	1
Zabbix services	3	1	4
- Last 20 issues:**

Host	Issue	Last change	Age	Info	Ack	Actions
Zabbix server	More than 100 items having missing data for more than 10 minutes	Dec 16th, 2013 03:17:51 AM	23d 23h 25m	0	0	
38host 302	Lack of free swap space on 38host 302	Nov 12th, 2013 12:03:59 PM	1m 27d 14h	0	0	

SNMP (Simple Network Management Protocol)

- SNMP adalah sebuah protokol yang dirancang untuk memberikan kemampuan kepada pengguna untuk memantau dan mengatur jaringan komputernya secara sistematis dari jarak jauh atau dalam satu pusat kontrol saja.
- Dengan menggunakan protokol ini kita bisa mendapatkan informasi tentang status dan keadaan dari suatu jaringan.
- Pengolahan ini dijalankan dengan menggumpulkan data dan melakukan penetapan terhadap variabel-variabel dalam elemen jaringan yang dikelola.
- Kebutuhan akan Simple Network Management Protocol pada sebuah sistem monitoring disebabkan oleh kebutuhan akan pemerolehan data monitoring dari sumber daya komputer lain.
- SNMP pada awalnya hanya dikhususkan pada manajemen jaringan TCP/IP, yaitu untuk melakukan manajemen informasi yang berkaitan dengan IP dan TCP, seperti pengubahan dari IP address ke suatu alamat fisik, jumlah data incoming dan outgoing IP datagram, atau tabel informasi mengenai koneksi TCP yang mungkin terjadi.
- Namun selanjutnya berkembang dengan memberikan dukungan informasi pada berbagai protokol jaringan, seperti DECnet, AppleTalk, dan NetWare IPX/SPX. Dukungan SNMP juga sampai pada berbagai fungsi yang terdapat di dalam sebuah multiprotocol routers.

SNMP key elements:

- Management station
 - Management agent
 - Management information base
 - Network Management protocol
- Get, Set and Notify
- Sebuah managed device adalah sebuah node di jaringan yang berisi agen SNMP yang berada di jaringan yang dapat di manage. Managed device akan mengumpulkan dan menyimpan informasi manajemen dan membuat informasi ini tersedia bagi NMS menggunakan SNMP. Managed device, kadang kala di sebut elemen jaringan, dapat berupa router dan akses server, switch dan bridge, hub, host komputer atau printer.
 - Agen adalah sebuah modul software network manajemen yang berada di dalam managed device. Agen ini mengetahui tentang informasi manajemen dan dalam menterjemahkan ke informasi yang kompatibel dengan SNMP
 - Aplikasi NMS menjalankan aplikasi yang dapat memonitor dan mengontrol managed device. NMS memberikan resource memory dan prosesor yang dibutuhkan untuk manajemen network. Satu atau lebih NMS harus ada dalam sebuah jaringan yang di manage.

Ada beberapa versi SNMP, diantaranya yaitu :

- **SNMP versi 1 (SNMPv1)** adalah implementasi awal dari protokol SNMP. SNMPv1 beroperasi di atas protokol lain, seperti, User Datagram Protocol (UDP), Internet Protocol (IP), OSI Connectionless Network Service (CLNS), AppleTalk Datagram-Delivery Protocol (DDP), dan Novell Internet Packet Exchange (IPX). SNMPv1 banyak digunakan dan menjadi de-facto protokol untuk manajemen jaringan di komunitas Internet. Beberapa RFC pertama untuk SNMP, yang sekarang di kenal sebagai Simple Network Management Protocol versi 1, muncul di tahun 1998

2. SNMP Versi 2, Versi 2 tidak di adopsi secara luas karena ke tidak sepakatan mengenai kerangka keamanan di dalam standard. Simple Network Management Protocol versi 2 (RFC 1441–RFC 1452), yang juga di kenal sebagai SNMP v2 atau SNMP v2p, merevisi versi 1 dan memasukan beberapa perbaikan masalah performance, keamanan, kerahasiaan, dan komunikasi antar manager. SNMP v2 memperkenalkan GETBULK, sebuah alternatif dari iterasi GETNEXT untuk data manajemen dalam jumlah besar melalui satu perintah saja. Akan tetapi, kebanyakan melihatnya terlalu rumit, sehingga tidak secara luas di adopsi

3. SNMP versi 3, IETF mengakui Simple Network Management Protocol versi 3 seperti di definisikan oleh RFC 3411–RFC 3418 (juga di kenal sebagai STD0062) sebagai standard SNMP

sejak 2004.

SNMPv3 memberikan tiga (3) servis yang penting, yaitu, **authentikasi, privasi dan access control**.

SNMP (Simple Network Management Protocol)

Comparison of SNMPv1 and SNMPv2

PDU	SNMPv1 PDU	SNMPv2 PDU	Direction	Description
GetRequest	GetRequest	GetRequest	Manager to agent	Request value for each listed object
GetRequest	GetRequest	GetRequest	Manager to agent	Request next value for each listed object
-----	GetBulkRequest	GetBulkRequest	Manager to agent	Request multiple values
SetRequest	SetRequest	SetRequest	Manager to agent	Set value for each listed object
-----	InformRequest	InformRequest	Manager to manager	Transmit unsolicited information
GetResponse	Response	Response	Agent to manager or Manager to manager(SNMPv2)	Respond to manager request
Trap	SNMPv2-Trap	Trap	Agent to manager	Transmit unsolicited information

SNMP operates in the [Application Layer](#) of the [Internet Protocol Suite \(Layer 7 of the OSI model\)](#). The SNMP agent receives requests on UDP port 161. The manager may send requests from any available source port to port 161 in the agent. The agent response will be sent back to the source port on the manager. The manager receives notifications ([Traps](#) and [InformRequests](#)) on port 162. The agent may generate notifications from any available port. When used with [Transport Layer Security](#) or [Datagram Transport Layer Security](#) requests are received on port 10161 and traps are sent to port 10162

SNMPv3 STD0062

	Communications protocol
OSI layer	Application
Port(s)	161, 162 (Trap)
RFC(s)	3411 – 3418

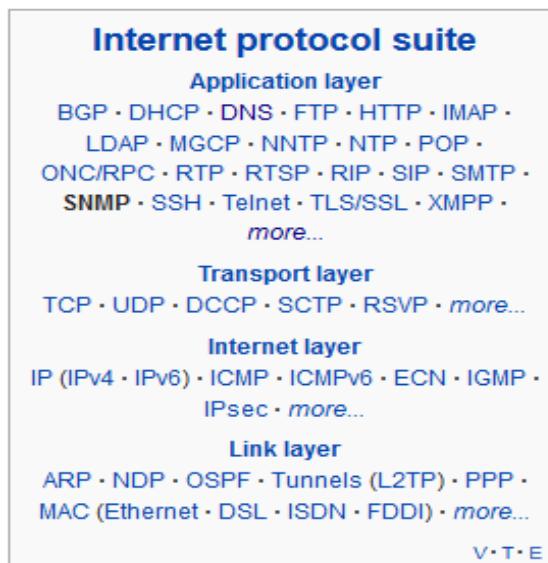
Secure SNMP

	Communications protocol
OSI layer	Application
Port(s)	10161, 10162 (Trap)
RFC(s)	6353

IETF([Internet Engineering Task Force](#)) menganggap versi sebelumnya sebagai "Obsolete" atau "Historical".

Di sisi praktis, implementasi SNMP biasanya memberikan dukungan bagi banyak versi, terutama SNMPv1, SNMPv2c, dan SNMPv3.

Ada baiknya membaca RFC 3584 "Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework".

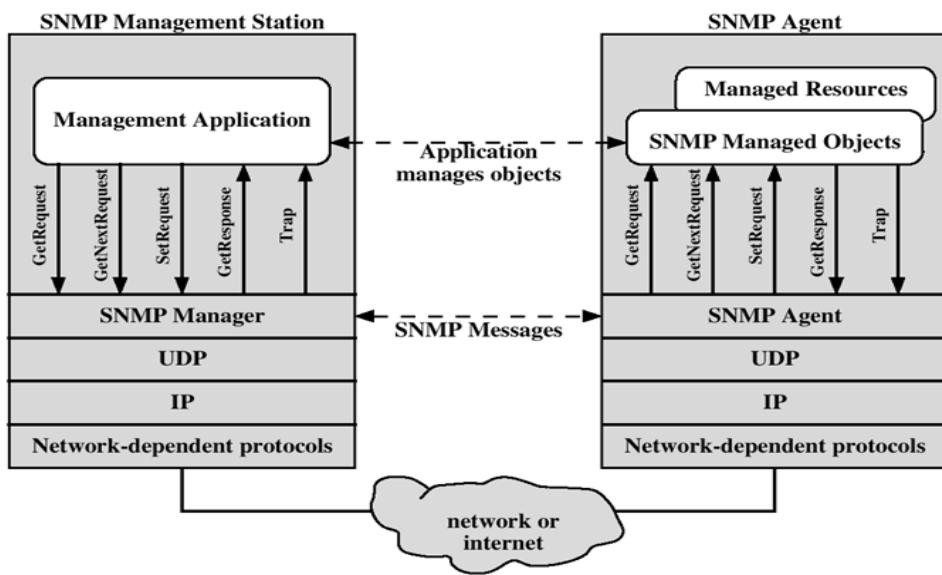


Protocol context of SNMP

Protocol context of SNMP

Protocol context of SNMP

Protocol context of SNMP



Protocol context of SNMP

All SNMP PDUs are constructed as follows:

IP header	UDP header	version	community	PDU-type	request-id	error-status	error-index	variable bindings
-----------	------------	---------	-----------	----------	------------	--------------	-------------	-------------------

The **seven SNMP** protocol data unit (PDU) types are as follows:

1. **GetRequest** A *manager-to-agent* request to retrieve the value of a variable or list of variables. Desired variables are specified in variable bindings (values are not used). Retrieval of the specified variable values is to be done as an [atomic operation](#) by the agent. A *Response* with current values is returned.
2. **SetRequest** A *manager-to-agent* request to change the value of a variable or list of variables. Variable bindings are specified in the body of the request. Changes to all specified variables are to be made as an atomic operation by the agent. A *Response* with (current) new values for the variables is returned.
3. **GetNextRequest** A *manager-to-agent* request to discover available variables and their values. Returns a *Response* with variable binding for the lexicographically next variable in the MIB. The entire MIB of an agent can be walked by iterative application of *GetNextRequest* starting at OID 0. Rows of a table can be read by specifying column OIDs in the variable bindings of the request.

4. GetBulkRequest Optimized version of *GetNextRequest*. A *manager-to-agent* request for multiple iterations of *GetNextRequest*. Returns a *Response* with multiple variable bindings walked from the variable binding or bindings in the request. PDU specific *non-repeaters* and *max-repetitions* fields are used to control response behavior. *GetBulkRequest* was introduced in SNMPv2.

5. Response Returns variable bindings and acknowledgement from *agent to manager* for *GetRequest*, *SetRequest*, *GetNextRequest*, *GetBulkRequest* and *InformRequest*. Error reporting is provided by *error-status* and *error-index* fields. Although it was used as a response to both gets and sets, this PDU was called *GetResponse* in SNMPv1.

6. Trap Asynchronous notification from *agent to manager*. SNMP traps enable an agent to notify the management station of significant events by way of an unsolicited SNMP message. Includes current *sysUpTime* value, an OID identifying the type of trap and optional variable bindings. Destination addressing for traps is determined in an application-specific manner typically through trap configuration variables in the MIB. The format of the trap message was changed in SNMPv2 and the PDU was renamed *SNMPv2-Trap*. While in classic communication the client always actively requests information from the server, SNMP allows the additional use of so-called "traps". These are data packages that are sent from the SNMP client to the server without being explicitly requested.

7. InformRequest Acknowledged asynchronous notification. This PDU was introduced in SNMPv2 and was originally defined as *manager to manager* communication.^[4] Later implementations have loosened the original definition to allow *agent to manager* communications.^{[5][6][7]} Manager-to-manager notifications were already possible in SNMPv1 (using a *Trap*), but as SNMP commonly runs over UDP where delivery is not assured and dropped packets are not reported, delivery of a *Trap* was not guaranteed. *InformRequest* fixes this by sending back an acknowledgement on receipt

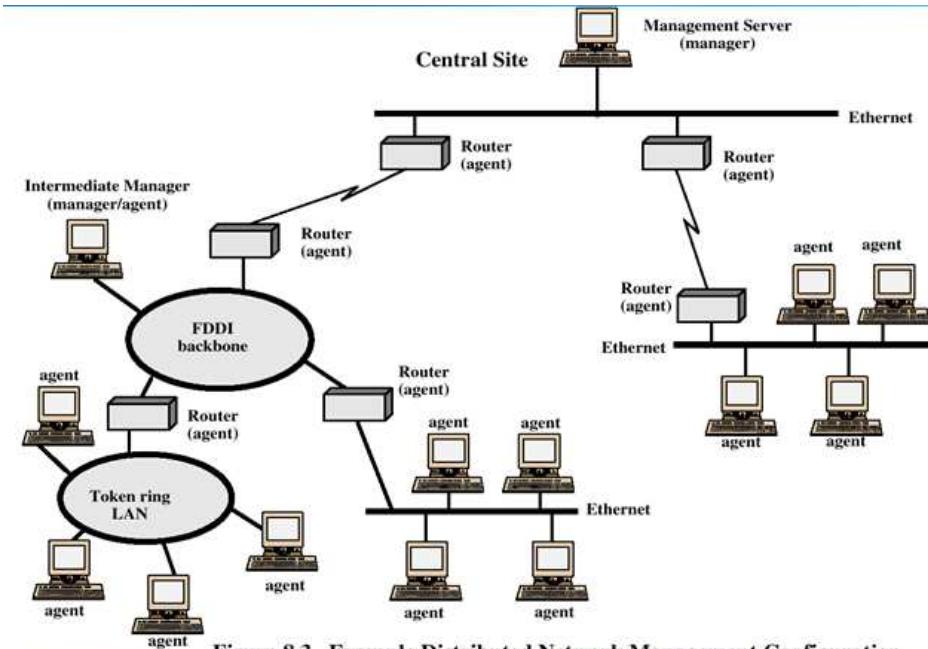
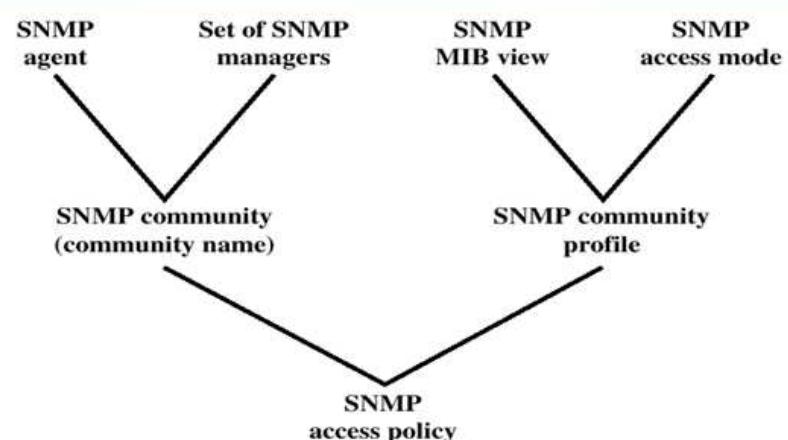


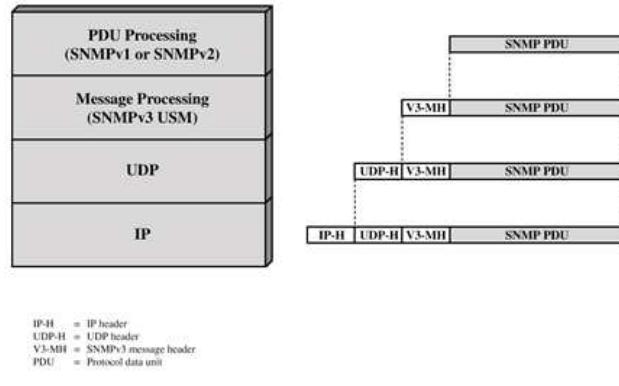
Figure 8.3 Example Distributed Network Management Configuration

SNMPv1 Administrative Concepts

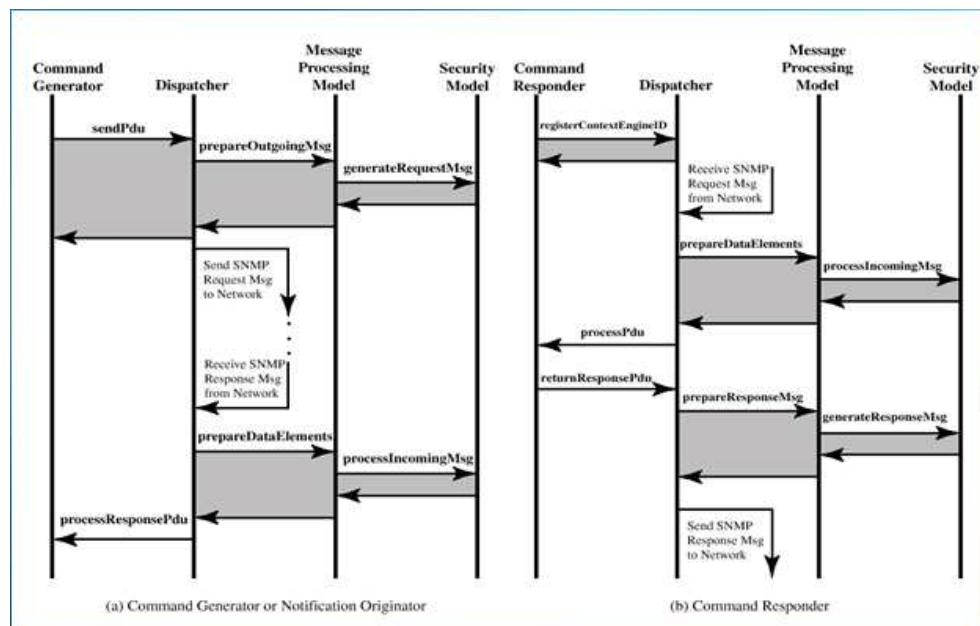


SNMPv3

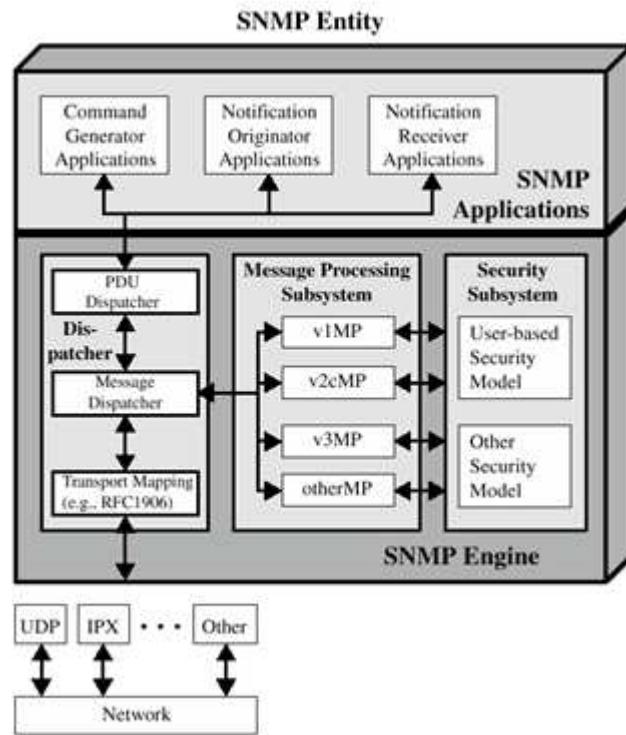
- SNMPv3 defines a security capability to be used in conjunction with SNMPv1 or v2



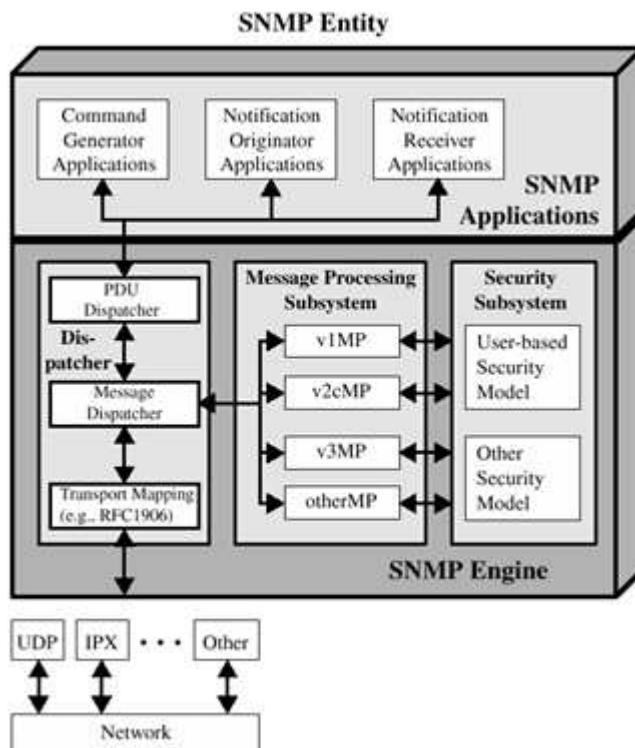
SNMPv3 Flow



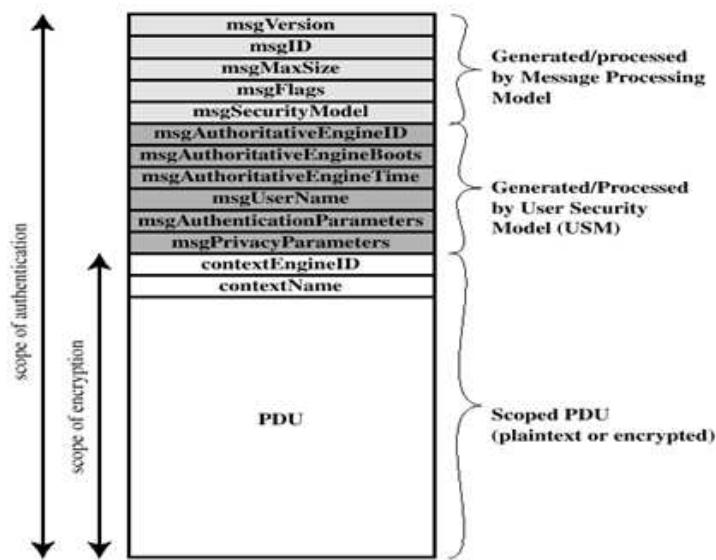
Traditional SNMP Manager



Traditional SNMP Agent



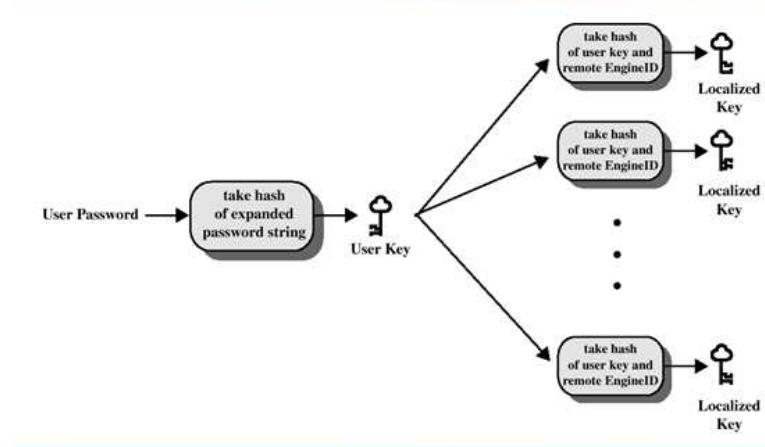
SNMP3 Message Format with USM



User Security Model (USM)

- Designed to secure against:
 - Modification of information
 - Masquerade
 - Message stream modification
 - Disclosure
- Not intended to secure against:
 - Denial of Service (DoS attack)
 - Traffic analysis

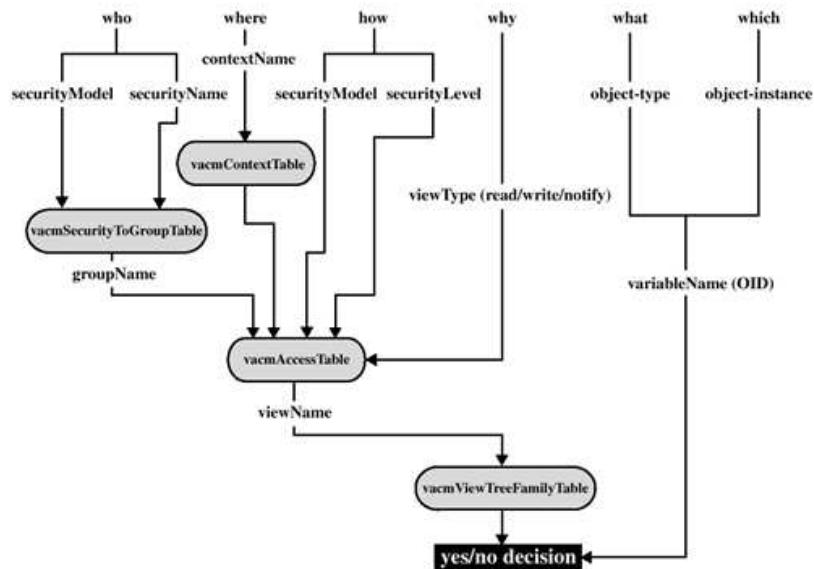
Key Localization Process



View-Based Access Control Model (VACM)

- VACM has two characteristics:
 - Determines whether access to a managed object should be allowed.
 - Make use of an MIB that:
 - Defines the access control policy for this agent.
 - Makes it possible for remote configuration to be used.

Access control decision



Daftar Pustaka

- https://en.wikipedia.org/wiki/Simple_Network_Management_Protocol
- Henric Johnson, Blekinge Institute of Technology, Sweden
- <http://www.its.bth.se/staff/hjo/henric.johnson@bth.se>



MODUL PERKULIAHAN

Keamanan Jaringan

Konsep Monitoring Network

Fakultas
Fasilkom

Program Studi
Teknik Informatika

TatapMuka
06

Kode MK
MK:15020

Di susun Oleh
Tim Dosen

Abstract

Keamanan jaringan ([Bahasa Inggris: Network Security](#)) dalam [jaringan komputer](#) sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah.

Kompetensi

Setelah membaca modul ini diharapkan mahasiswa :

- Mampu menyebutkan konsep network monitoring, serta menyebutkan tipe tool monitoring.

Konsep Network Monitoring

Network Monitoring

Network Monitoring System(NMS) menggambarkan sebuah sistem yang terus menerus memonitor jaringan komputer sehingga jika terjadi gangguan dapat secepatnya melakukan notifikasi kepada seorang network administrator atau system administrator.

Sebagai contoh untuk mengetahui status dari sebuah webserver, software monitoring secara periodik mengirim request http; atau untuk email server, pesan tes di kirimkan melalui sebuah SMTP untuk kemudian di ambil melalui IMAP ataupun POP3.



Network & Server Monitoring

Monitor packet loss, response time, and performance metrics of devices such as routers, switches, servers, VMs.

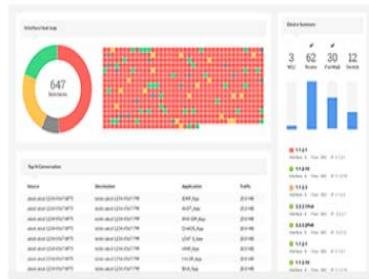
- Yang biasa dijadikan variabel dalam NMS ini adalah waktu respon dan ketersediaan (uptime), dan konsistensi serta reliability juga di perhatikan.
- Status request yang failure, seperti ketika koneksi tidak bisa berhubungan (established), yang kemudian terputus, yang kemudian sistem monitoring menghasilkan suatu pesan/notifikasi, notifikasi ini bermacam-macam:
- Sebuah alarm suara mungkin di kirimkan kepada seorang net/sys admin.
- Network Monitoring penggunaan tool pencatatan dan analisis yang secara akurat menentukan arus trafik, penggunaan, dan indikator kinerja di jaringan lainnya.
- Tool monitoring yang baik memberi anda baik angka maupun representasi grafik dari kondisi jaringan. Ini menolong anda untuk menvisualisasikan secara akurat apa yang terjadi, agar anda tahu di mana perlu dilakukan penyesuaian.



Network & Server Monitoring

Monitor packet loss, response time, and performance metrics of devices such as routers, switches, servers, VMs.

https://www.manageengine.com/network-monitoring/?gclid=CJ3hvqGj_8sCFdWGAAodrRUFmg



Bandwidth Analysis

Analyze bandwidth consumed by users & apps via NetFlow, sFlow, jFlow, IPFIX, etc. and shape traffic.



Firewall Log Management

Collect, analyze, and archive firewall logs for security and compliance. Fix security loop holes instantly.

Ada beberapa keuntungan melakukan sistem monitor yang baik untuk jaringan anda:

1. Anggaran jaringan dan sumber daya di justifikasi.

Tool monitor yang baik bisa memperlihatkan tanpa ragu-ragu bahwa infrastruktur jaringan (bandwidth, hardware, dan software) cocok dan bisa menangani kebutuhan pengguna jaringan.

2. Penyusup jaringan dideteksi dan disaring.

Dengan menonton trafik jaringan anda, anda bisa mendeteksi penyerang dan mencegah akses ke server dan layanan yang penting.

3. Virus jaringan dengan mudah dideteksi.

- Anda akan diberitahu akan adanya virus jaringan, dan melakukan tindakan sebelum mereka memakan bandwidth Internet dan mendestabilisasi jaringan anda.

4. Troubleshooting masalah jaringan sangat disederhanakan.

- Daripada mencoba untuk men-debug masalah jaringan, anda dengan segera bisa diberitahukan mengenai masalah spesifik. Beberapa masalah bahkan bisa diperbaiki secara otomatis.

5. Kinerja jaringan bisa sangat di optimisasi.

- Tanpa monitoring efektif, mustahil untuk mengkonfigurasi alat dan protokol anda untuk mencapai kinerja yang terbaik.

6. Perencanaan kapasitas lebih mudah.

- Dengan catatan kinerja sejarah, anda tidak harus "mengira-ngira" berapa banyak bandwidth yang anda perlukan sewaktu jaringan anda bertambah besar.

7. Penggunaan jaringan secara layak bisa ditekankan.

- Ketika bandwidth adalah sumber daya yang susah didapat, satu-satunya cara untuk menjadi adil kepada semua user adalah menjamin kalau jaringan dipakai sesuai dengan maksudnya.

Tipe Tool Monitoring

Kita sekarang akan melihat beberapa kelas **tool monitoring**.

1. **Tool pendeksi jaringan** memperhatikan beacon yang dikirim oleh akses point nirkabel, dan menampilkan informasi seperti nama jaringan, kekuatan signal yang didapat, dan channel.
2. **Tool spot check** di disain untuk troubleshooting dan biasanya dikelola secara interaktif selama periode waktu yang singkat. Program seperti **ping** mungkin dianggap sebagai tool spot check aktif, karena dia mengeluarkan trafik dan melakukan polling ke mesin tertentu. Tool spot check pasif termasuk **protokol analyzer**, yang memeriksa setiap paket di jaringan dan menyediakan perincian secara detail mengenai percakapan jaringan (termasuk alamat sumber dan tujuan, informasi protokol, dan bahkan data aplikasi).
3. **Tool trending** menjalankan monitor tanpa operator dalam periode lama, dan biasanya menyiapkan hasil menjadi grafik.
4. **Tool monitor** realtime menjalankan monitor yang sama, tetapi segera memberitahu administrator jika mereka mengetahui masalah.
5. **Tool penguji throughput** memberitahu anda bandwidth sebenarnya yang ada di antara dua ujung di jaringan.
6. **Tool Intrusion detection** mengamati trafik jaringan yang tidak diinginkan, dan mengambil keputusan yang tepat (biasanya menolak akses dan/atau memberitahu seorang network administrator).
7. **Tool benchmarking** memperkirakan kinerja maksimum dari sebuah layanan atau sambungan jaringan.

Tool monitor nirkabel yang paling sederhana hanya memberikan daftar jaringan yang tersedia, di dampingi oleh informasi dasar (seperti kekuatan sinyal dan kanal).

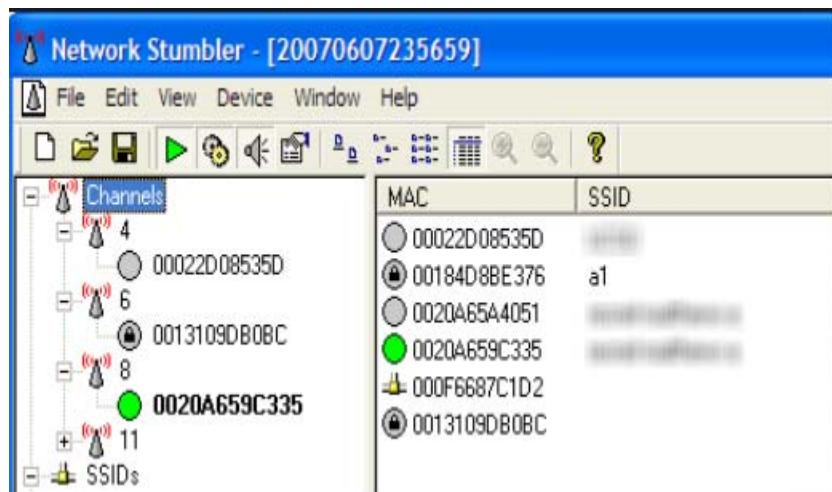
Mereka memungkinkan anda mendeksi jaringan yang dekat dengan cepat dan menentukan bila mereka ada dalam jangkauan atau mengakibatkan gangguan.

1. **Built-in client.**

- Semua sistem operasi modern mempunyai built-in support untuk jaringan nirkabel. Ini biasanya termasuk kemampuan untuk scan jaringan yang tersedia, membantu user untuk memilih sebuah jaringan dari daftar. Hampir semua alat nirkabel biasanya mempunyai alat scan sederhana, fungsi bisa berbeda di setiap implementasi. Alat-alat ini biasanya hanya berguna untuk mengatur sebuah komputer di konfigurasi rumah atau kantor. Mereka biasanya hanya menyediakan sedikit informasi selain dari nama jaringan dan sinyal yang tersedia sampai dengan akses point yang sedang dipakai.

2. **Netstumbler (<http://www.netstumbler.com/>).**

- Ini adalah tool yang paling populer karena mendeteksi jaringan nirkabel menggunakan Microsoft Windows.
 - Dia mendukung beberapa jenis wireless card, dan sangat mudah digunakan.
 - Dia akan mendeteksi jaringan-jaringan yang terenkripsi dan yang terbuka, tetapi tidak bisa mendeteksi jaringan-jaringan nirkabel “tertutup”.
 - Dia juga menampilkan kekuatan sinyal / noise dan menggambarkan sinyal yang diterima sebagai fungsi waktu.
 - Dia juga dapat berintegrasi dengan beberapa jenis GPS, untuk mencatatkan informasi lokasi dan kekuatan sinyal secara tepat. Ini membuat Netstumbler menjadi sebuah alat berguna untuk site survey informal.



3. Ministumbler (<http://www.netstumbler.com/>).

- Dari pembuat Netstumbler, Ministumbler memberikan fungsi yang sama dengan versi Windows nya, tapi bekerja di Pocket PC Ministumbler nyaman digunakan di handheld PDA dengan sebuah wireless card untuk mendeteksi akses point.

Ministumbler

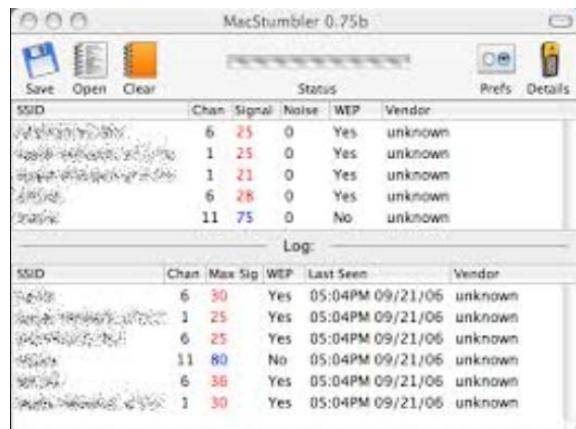
The screenshot shows the Ministumbler software interface. At the top, it says 'Ministumbler' and shows the time as 12:09. Below is a table of detected wireless access points (APs). The table has columns 'MAC', 'Chan', 'SSID', and 'SNR'. The data is as follows:

MAC	Chan	SSID	SNR
0090D100BF6C	11	WLAN	5
0090D100B93B	11	WLAN	
0090D100CC6F	11+	WLAN	10
0090D100BEC5	6	WLAN	
004033AFC3D1	10	Wireless	
0090D100CAA5	11	WLAN	17
0090D100BE02	1	WLAN	

At the bottom, there's a toolbar with icons for File, View, Options, and other functions. It also shows 'Ready', '3 APs', 'GPS Off', and '7/7'.

4. Macstumbler (<http://www.macstumbler.com/>).

- Biarpun tidak terkait langsung dengan Netstumbler, Macstumbler memberi banyak fungsi yang sama tetapi untuk platform Mac OSX.
- Dia bekerja dengan semua Apple Airport cards.



5. Wellenreiter (<http://www.wellenreiter.net/>).

- Wellenreiter adalah sebuah pendeteksi jaringan nirkabel grafik untuk Linux.
- Dia membutuhkan Perl dan GTK, dan menyokong port Prism2, Lucent, dan Cisco wireless cards.



- Penggunaan sistem yg secara terus-menerus mengawasi jaringan komputer
 - Yg diawasi: komponen-komponen yg lambat dan yg gagal menjalankan fungsinya, server yg crash atau overload, masalah koneksi, dll.
 - Idealnya admin kemudian akan diberitahu lewat email, pager, sms, atau yang lainnya
 - Bagian dari Network Management
 - Biasanya yg diukur ialah *response time* dan *availability* (atau *uptime*)
 - Response Time atau waktu tanggap ialah waktu yg dibutuhkan oleh komponen jaringan (atau suatu layanan - server) untuk merespon permintaan. Response time diukur dalam μ s

- Availability atau ketersediaan ialah tingkat ketersediaan (ada atau tidaknya) komponen atau layanan dalam menangani request.
- Availability diukur dalam % waktu

$$A = \frac{E[\text{Uptime}]}{E[\text{Uptime}] + E[\text{Downtime}]}$$

Hal lain yg biasanya juga diukur ialah:

- **Consistency dan reliability**
- Netmon biasanya bereaksi terhadap:
 - kegagalan permintaan status, kegagalan koneksi, time-out, paket yg tidak dapat diteruskan, dll
- Tindakan yg dapat diambil antara lain: automatic failover system, load balancing untuk mengantikan posisi server yg failed dg backup-nya

Contoh:

- Untuk mengawasi status dari webserver, monitoring system dpt mengirimkan paket *http_request* kecil secara berkala
- Bila tidak ada *http_response*, berarti ada masalah
- Paket *http_request* dapat dimodifikasi untuk informasi lain, tergantung kolaborasi dengan web server
- Untuk layanan lain seperti email, kurang lebih sama

Administrator Jaringan

Administrator Jaringan Komputer adalah sebuah jenis pekerjaan yang banyak dibutuhkan saat ini terutama pada perusahaan/instansi yang telah mengimplementasikan teknologi komputer dan internet untuk menunjang pekerjaan.

- Penggunaan sistem jaringan komputer dalam skala kecil maupun luas akan membutuhkan pengaturan-pengaturan mulai dari tingkat fisik maupun non fisik. Pengaturan-pengaturan tersebut melibatkan proses pengontrolan.
- Ada beberapa definisi mengenai administrasi jaringan ini antara lain :
 - controlling corporate strategic (assets)
 - controlling complexity
 - improving service
 - balancing various needs
 - reducing downtime
 - controlling costs
- Pada intinya administrator network bertugas mengelola serta menjaga seluruh sumber

daya pada sistem jaringan agar kinerja jaringan lebih efektif dan efisien dilihat dari fungsi, struktur dan keamanan jaringan itu sendiri.

Sebelum berbicara tugas dan tanggung jawab berikut beberapa hal umum **yang harus di kuasai** seorang network administrator ;

- Pengetahuan dasar tentang komputer teori maupun praktek, hal ini sangat penting karena tidak mungkin menjadi seorang administrator jaringan komputer namun bagaimana kerja sistem komputer sendiri tidak dikuasai dengan baik.
- Pengetahuan tentang berbagai perangkat keras jaringan komputer seperti ; repeater, switch, router, antena, kabel dan berbagai perangkat pendukung lainnya, pemahaman meliputi cara kerja, pemasangan dan konfigurasi.
- Pemahaman tentang routing

Pemahaman tentang routing teori maupun konfigurasi harus di kuasai dengan baik agar mampu membangun jaringan dengan baik hal ini sangat diperlukan terutama jika komputer ataupun sub organisasi perusahaan sangat banyak.

- Pengetahuan tentang sistem keamanan komputer terutama jaringannya (network security) akan sangat membantu dan memberikan nilai lebih.
- Selain kemampuan teori maupun praktek yang harus dikuasai dengan baik hal lain adalah memiliki etika profesional, tanpa etika dan sikap seorang profesional yang baik maka semua kemampuan teori maupun praktek yang dikuasai tidak akan berarti banyak.

Fungsi dan Tugas Network Administrator

Ada beberapa fungsi dan kerja administrator, namun secara garis besar dapat dinyatakan dari irisan antara network, hardware, dan application.

Tugas dari administrator jaringan adalah:

- Security management: menitik beratkan kerja mencakup masalah network administrator keamanan , mencakup hal-hal berikut:
 - Firewall adalah sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalulintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalulintas yang dianggap tidak aman.
 - Username: username akan digunakan sebagai informasi log in password control: yaitu pengendalian pasword yang dimiliki oleh sebuah sistem.
 - Resource access: network admin mampu melakukan pembatasan penggunaan sumber daya sesuai dengan hak akses yang diberikan.

Keamanan Jaringan

1. Membatasi Akses ke Jaringan

A. Membuat tingkatan akses :

- Pembatasan-pembatasan dapat dilakukan sehingga memperkecil peluang penembusan

oleh pemakai yang tak diotorisasi, misalnya :

- ✓ Pembatasan login. Login hanya diperbolehkan :
 - ✓ Pada terminal tertentu.
 - ✓ Hanya ada waktu dan hari tertentu.
- Pembatasan dengan call-back

(Login dapat dilakukan siapapun. Bila telah sukses login, sistem segera memutuskan koneksi dan memanggil nomor telepon yang telah disepakati, Penyusup tidak dapat menghubungi lewat sembarang saluran telepon, tapi hanya pada saluran telepon tertentu).

- Pembatasan jumlah usaha login.
 - Login dibatasi sampai tiga kali dan segera dikunci dan diberitahu ke administrator.
 - Semua login direkam dan sistem operasi melaporkan informasi-informasi berikut :

Waktu, yaitu waktu pemakai login.

Terminal, yaitu terminal dimana pemakai login.

Tingkat akses yang diizinkan (read / write / execute / all)

B. Mekanisme kendali akses :

- Masalah identifikasi pemakai ketika login disebut otentifikasi pemakai (user authentication). Kebanyakan metode otentifikasi didasarkan pada tiga cara, yaitu :

1. Sesuatu yang diketahui pemakai, misalnya :

Password.

Kombinasi kunci.

Nama kecil ibu mertua.

Dan sebagainya.

2. Sesuatu yang dimiliki pemakai, misalnya :

Badge.

Kartu identitas.

Kunci.

Dan sebagainya.

3. Sesuatu mengenai (ciri) pemakai, misalnya :

Sidik jari.

Sidik suara.

Foto.

Tanda tangan.

C. Waspada terhadap Rekayasa sosial :

- Mengaku sebagai eksekutif yang tidak berhasil mengakses, menghubungi administrator via telepon/fax.
- Mengaku sebagai administrator yang perlu mendiagnosa masalah network, menghubungi end user via email/fax/surat.

- Mengaku sebagai petugas keamanan e-commerce, menghubungi customer yang telah bertransaksi untuk mengulang kembali transaksinya di form yang disediakan olehnya.
- Pencurian surat, password.
- Penyuapan, kekerasan.

D. Membedakan Sumber daya internal dan Eksternal :

- Memanfaatkan teknologi firewall yang memisahkan network internal dengan network eksternal dengan rule tertentu.

E. Sistem Otentikasi User :

Def : adalah proses penentuan identitas dari seseorang yang sebenarnya, hal ini diperlukan untuk menjaga keutuhan (integrity) dan keamanan (security) data, pada proses ini seseorang harus dibuktikan siapa dirinya sebelum menggunakan layanan akses.

Upaya untuk lebih mengamankan proteksi password, antara lain :

1. **Salting.**
2. Menambahkan string pendek ke string password yang diberikan pemakai sehingga mencapai panjang password tertentu.

2. One time password.

- Pemakai harus mengganti password secara teratur. Upaya ini membatasi peluang password telah diketahui atau dicoba-coba pemakai lain.
- Bentuk ekstrim pendekatan ini adalah one time password, yaitu pemakai mendapat satu buku berisi daftar password. Setiap kali pemakai login, pemakai menggunakan password berikutnya yang terdapat di daftar password.
- Dengan one time password, pemakai direpotkan keharusan menjaga agar buku passwordnya jangan sampai dicuri.

3. Satu daftar panjang pertanyaan dan jawaban.

- Variasi terhadap password adalah mengharuskan pemakai memberi satu daftar pertanyaan panjang dan jawabannya. Pertanyaan-pertanyaan dan jawabannya dipilih pemakai sehingga pemakai mudah mengingatnya dan tak perlu menuliskan di kertas.
- Pertanyaan berikut dapat dipakai, misalnya :
 - Siapa mertua abang ipar Badru ?
 - Apa yang diajarkan Pak Harun waktu SD ?
 - Di jalan apa pertama kali ditemukan simanis ?
- Pada saat login, komputer memilih salah satu dari pertanyaan-pertanyaan secara acak, menanyakan ke pemakai dan memeriksa jawaban yang diberikan.

4. Tantangan tanggapan (challenge response).

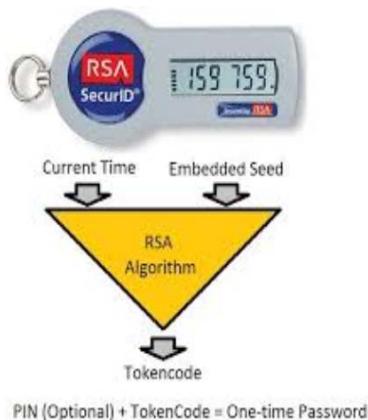
- Pemakai diberi kebebasan memilih suatu algoritma, misalnya x3.

- Ketika pemakai login, komputer menuliskan di layar angka 3. Dalam kasus ini pemakai mengetik angka 27. Algoritma dapat berbeda di pagi, sore, dan hari berbeda, dari terminal berbeda, dan seterusnya.

Contoh Produk Otentikasi User, antara lain :

1. Secureid ACE (Access Control Encryption)

- System token hardware seperti kartu kredit berdisplay, pemakai akan menginput nomor pin yang diketahui bersama, lalu memasukkan pascode bahwa dia pemilik token.

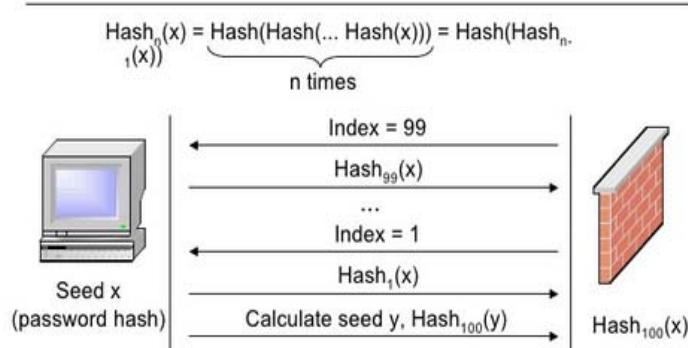


Contoh Produk Otentikasi User, antara lain :

2. S/key (Bellcore)

System software yang membentuk one time password (OTP) berdasarkan informasi login terakhir dengan aturan random tertentu.

S/Key Authentication



- "y = MakeSeed(time(NULL))"
- Attack: brute force

T. Lopatic, J. McDonald, D. Song, "A Stateful Inspection of FireWall-1", Black Hat Briefings 2000

23

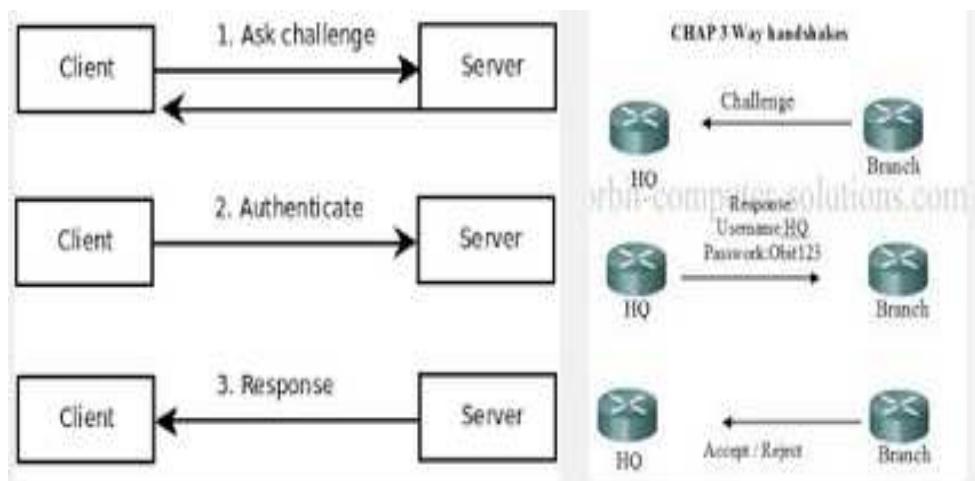
3. Password Authentication Protocol (PAP)

Protokol dua arah untuk PPP (Point to point Protocol). Peer mengirim pasangan user id dan password, authenticator menyetujuinya.



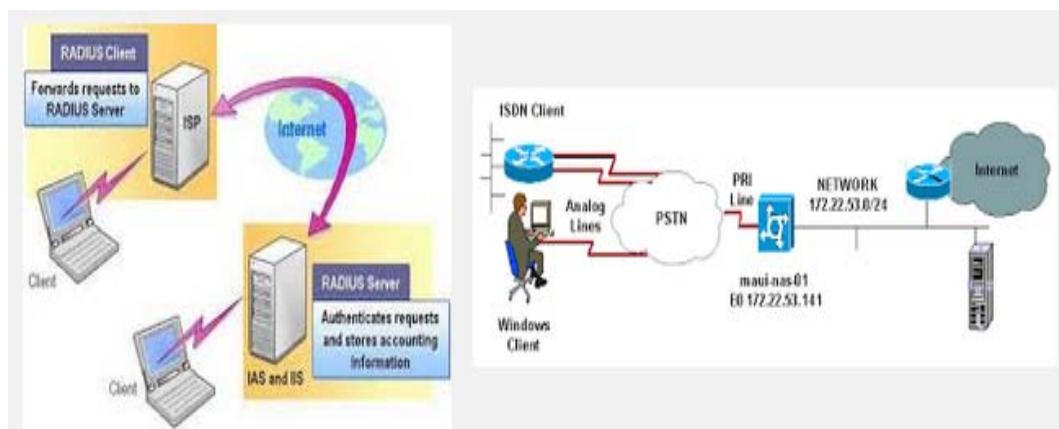
Contoh Produk Otentikasi User, antara lain :

- 4. Challenge Handshake Authentication Protocol (CHAP)
- S/key pada PAP, protocol 3 arah, authenticator mengirim pesan tantangan ke peer, peer menghitung nilai lalu mengirimkan ke authenticator, authenticator menyetujui otentifikasi jika jawabannya sama dengan nilai tadi.



5. Remote Authentication Dial-in User Service (RADIUS)

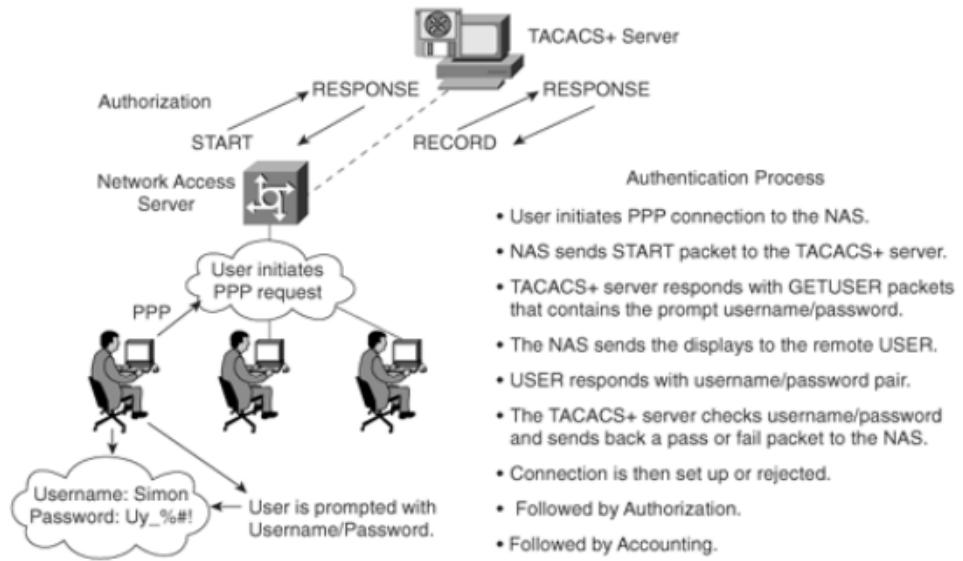
- Untuk hubungan dial-up, menggunakan network access server, dari suatu host yang menjadi client RADIUS, merupakan sistem satu titik akses.



6. Terminal Access Controller Access Control System (TACACS)

- Protokol keamanan berbasis server dari CISCO System. Security Server terpusat dengan file password UNIX, database otentikasi, otorisasi dan akunting, fungsi digest (transmisi

password yang tidak polos)



2. Melindungi Aset Organisasi

A. Secara Adminsistratif / fisik

- Rencana kemungkinan terhadap bencana
- Program penyaringan calon pegawai system informasi
- Program pelatihan user
- Kebijakan akses network

B. Secara Teknis

Daftar Pustaka

- Cisco.com
- [https://www.manageengine.com/network-](https://www.manageengine.com/network-monitoring/)
- <http://www.netstumbler.com/>



MODUL PERKULIAHAN

Keamanan Jaringan

Study Kasus & Presentasi

Fakultas
Fasilkom

Program Studi
Teknik Informatika

TatapMuka

Kode MK
MK:15020

Di susun Oleh
Tim Dosen

07

Abstract

Keamanan jaringan ([Bahasa Inggris: Network Security](#)) dalam [jaringan komputer](#) sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah.

Kompetensi

Setelah membaca modul ini diharapkan mahasiswa :

- **Mampu membuat proposal mengenai paparan security hole dan solusinya**

Contoh Study Kasus Keamanan Jaringan

1. Kartu Kredit Pelanggan Zalora Dibobol Rp 14 Juta

Adi Fida Rahman - detikinet

Senin, 11/04/2016 15:13 WIB

- Perusahaan e-commerce yang berpusat di Singapura ini langsung menangani masalah tersebut.

"Saat ini sudah 8 order yang berhasil dibatalkan. Tinggal satu lagi masih menunggu notifikasi. Saya masih mempercayakan ke pihak Zalora untuk proses tersebut," terang Sulaiman.

Ia berharap Zalora dan e-commerce lain menerapkan verifikasi 3D dengan OTP jika pembayaran dengan KK. Sebab tidak ada jaminan server tidak di-hack dan terjadi pencurian user name.

- 2. <http://inet.detik.com/read/2016/03/31/150945/3176775/1205/belanja-online-aman-dengan-kartu-kredit-begini-caranya>
- **Jakarta** - Penipuan kartu kredit makin sering terjadi seiring meluasnya penggunaan internet dan kartu kredit. Tak sedikit konsumen yang terkaget-kaget karena tiba-tiba tagihan kartu kreditnya membengkak padahal ia tidak belanja, atau kartu kreditnya dipakai untuk membayar tagihan lain yang bukan miliknya.

Kasus seperti ini terjadi karena adanya pencurian identitas. Pelaku membuat software berbahaya untuk mencuri informasi akun dan password pengguna internet saat sedang belanja online, melakukan transaksi perbankan atau merespon email palsu yang meminta konfirmasi nomor rekening.

3. <http://sharingvision.com/2013/04/studi-kasus-indonesia-keamanan-layana-finansial-eletronic-data-capture/>

- **Studi Kasus Indonesia: Keamanan Layanan Finansial (Eletronic Data Capture)**

Satu lagi kejadian yang dapat menyerang teknologi transaksi finansial, yaitu serangan terhadap Eletronic Data Capture (EDC). Serangan tersebut pernah terjadi di Eropa pada tahun 2008. Pelaku mengakses EDC dalam jalur *supply chain*. Setelah membongkar, memasang alat tambahan di EDC dan mengembalikannya seperti semula, pelaku membaca serta merekam detail account pembeli dan PIN. Lalu pelaku mengirimkan data melalui jaringan telepon seluler jaringan bawah tanah di Pakistan.

(sumber : sharingvision.com)

Serangan terhadap EDC juga pernah terjadi di Indonesia. Tahun 2011 Aparat Reserse Resmob/Tanahabang Direktorat Reserse Kriminal Umum Polda Metro Jaya mengungkap pembobolan kartu kredit senilai Rp. 80 miliar lebih. Kejadian itu dilakukan oleh komplotan

penjahat kartu kredit yang otak pelakunya adalah mantan pegawai salah satu bank swasta dan menjabat sebagai investigator kartu kredit. Pelaku mengetahui seluk-beluk cara mengambil dan mengkloning data Terminal ID (T.ID) dan Merchant ID (M.ID) dari terminal EDC.

Pada Umumnya bank sudah menerapkan pengamanan berlapis hingga ke jaringan corenya juga adanya sistem deteksi terjadinya transaksi yang tidak sah. Seperti kasus diatas, serangan dapat dilakukan oleh orang dalam. Namun resiko ini bisa dikatakan minim, mengingat berbagai sangsi yang akan diterima jika ketahuan seperti pemecatan, sangsi pidana dan lain.lain. Namun dampaknya bisa besar jika menyerang nasabah yang *highly valuable*.

EDC: Identifikasi Ancaman Keamanan



- September 2000. Polisi mendapat banyak laporan dari luar negeri tentang adanya user Indonesia yang mencoba menipu user lain pada situs web yang menyediakan transaksi lelang (auction) seperti eBay.

- 24 Oktober 2000. Dua warung Internet (Warung) di Bandung digrebeg oleh Polisi (POLDA Jabar) dikarenakan mereka meningkatnya Kejahatan Komputer Jumlah kejahatan komputer (computer crime), terutama yang berhubungan dengan sistem informasi, akan terus meningkat dikarenakan beberapa hal, antara lain:

- Aplikasi bisnis yang menggunakan (berbasis) teknologi informasi dan jaringan komputer semakin meningkat. Sebagai contoh saat ini mulai bermunculan aplikasi bisnis seperti online banking, electronic commerce (e-commerce), Electronic Data Interchange (EDI), dan masih banyak lainnya. Bahkan aplikasi e-commerce akan menjadi salah satu aplikasi pemicu di Indonesia (melalui "Telematika Indonesia" [48] dan Nusantara 21). Demikian pula di berbagai penjuru dunia aplikasi ecommerce terlihat mulai meningkat.

Juni 2001. Seorang pengguna Internet Indonesia membuat beberapa situs yang mirip (persis sama) dengan situs klikbca.com, yang digunakan oleh BCA untuk memberikan layanan Internet banking. Situs yang dia buat menggunakan nama domain yang mirip dengan klikbca.com, yaitu kilkbca.com (perhatikan tulisan "kil" yang sengaja salah ketik), wwwklikbca.com (tanpa titik antara kata "www" dan "klik"), clikbca.com, dan klickbca.com. Sang user mengaku bahwa dia mendapat memperoleh PIN dari beberapa nasabah BCA yang salah mengetikkan nama situs layanan Internet banking tersebut.

Beberapa Contoh Kasus Serangan terhadap Sistem Informasi beserta Dampaknya

Beberapa Contoh Umum

- Situs FPI menjadi Target Serangan CRACKER Massal .**FBI News**, Pasca Penolakan Kedatangan Pengurus Pusat FPI(Forum Pembela Islam) ke Kalimantan Tengah oleh masyarakat setempat membangkitkan sentimen serupa di pelosok tanah air sehingga menginspirasi munculnya gerakan indonesia tanpa fpi di jantung ibukota jakarta yang kegiatannya dimulai dari situs jaring sosial seperti facebook dan twitter yang mengkristal menjadi gerakan moral turun ke jalan oleh beberapa aktifis humanis dan beberapa seniman.Gerakan Moral selain di situs jaring sosial dan aksi turun ke jalan juga dilakukan dengan serangan dunia maya(cracking)yang ditujukan kepada official website FPI <http://www.fpi.or.id> oleh hacker yang menggunakan id sn0wman yang memperkenalkan dirinya di sebuah blogmiliknya di <http://www.hack4down.wordpress.com>"dalam perkenalan singkatnya tanggal 17 februari 2012 sn0wman mengatakan bahwa dia membuat blog itu hanya sebagai pembelajaran dalam berpikir simple bahwa segala sesuautunya mesti ada keseimbangan baik dan buruk semua harus seimbang dan juga mengatakan "perang gerilya" selalu menang melawan pasukan yang bersenjata lengkap sembari mengklaim bahwa situs fpi sudah jadi targetnya dan sudah diserang yang dimulai tanggal 17 februari dengan program yang dibuatnya sendiri. keesokan harinya sn0wman juga mengajak dan mengajarkan cara menyerang situs fpi sembari membuka program yang digunakannya untuk bisa digunakan untuk umum sekaligus memberi tahu langkah2nya.Sampai berita ini diturunkan situs resmi FPI sepertinya masih down. Sumber
- 7 Februari 2000 s/d 9 Februari 2000. Distributed Denial of Service (Ddos) attack terhadap Yahoo, eBay, CNN, Amazon, ZDNet, E- Trade.
- 2001. Virus SirCam mengirimkan file dari harddisk korban. File rahasia bisa tersebar. Worm Code Red menyerang sistem IIS kemudian melakukan port scanning dan menyusup ke sistem IIS yang ditemukannya.
- 2004. Kejahatan “phising” (menipu orang melalui email yang seolah-olah datang dari perusahaan resmi [bank misalnya] untuk mendapatkan data-data pribadi seperti nomor PIN internet banking) mulai marak.

Dec
9

Beberapa Contoh Kasus Serangan terhadap Sistem Informasi beserta Dampaknya

Beberapa Contoh Umum

- Situs FPI menjadi Target Serangan CRACKER Massal .**FBINews**, Pasca Penolakan Kedatangan Pengurus Pusat FPI(Forum Pembela Islam) ke Kalimantan Tengah oleh masyarakat setempat membangkitkan sentimen serupa di pelosok tanah air sehingga menginspirasi munculnya gerakan indonesia tanpa fpi di jantung ibukota jakarta yang kegiatannya dimulai dari situs jaring sosial seperti facebook dan twitter yang mengkristal menjadi gerakan moral turun ke jalan oleh beberapa aktifis humanis dan beberapa seniman.Gerakan Moral selain di situs jaring sosial dan aksi turun ke jalan juga dilakukan dengan serangan dunia maya(cracking)yang ditujukan kepada official website FPI <http://www.fpi.or.id> oleh hacker yang menggunakan id sn0wman yang memperkenalkan dirinya di sebuah blogmiliknya di <http://www.hack4down.wordpress.com>"dalam perkenalan singkatnya tanggal 17 februari 2012 sn0wman mengatakan bahwa dia membuat blog itu hanya sebagai pembelajaran dalam berpikir simple bahwa segala sesuautunya mesti ada keseimbangan baik dan buruk semua harus seimbang dan juga mengatakan "perang gerilya" selalu menang melawan pasukan yang bersenjata lengkap sembari mengklaim bahwa situs fpi sudah jadi targetnya dan sudah diserang yang dimulai tanggal 17 februari dengan program yang dibuatnya sendiri. keesokan harinya sn0wman juga mengajak dan mengajarkan cara menyerang situs fpi sembari membuka program yang digunakannya untuk bisa digunakan untuk umum sekaligus memberi tahu langkah2nya.Sampai berita ini diturunkan situs resmi FPI sepertinya masih down. [Sumber](#)
- 7 Februari 2000 s/d 9 Februari 2000. Distributed Denial of Service (Ddos) attack terhadap Yahoo, eBay, CNN, Amazon, ZDNet, E- Trade.
- 2001. Virus SirCam mengirimkan file dari harddisk korban. File rahasia bisa tersebar. Worm Code Red menyerang sistem IIS kemudian melakukan port scanning dan menyusup ke sistem IIS yang ditemukannya.
- 2004. Kejahatan “phising” (menipu orang melalui email yang seolah-olah datang dari perusahaan resmi [bank misalnya] untuk mendapatkan data-data pribadi seperti nomor PIN internet banking) mulai marak. [Sumber](#)

Beberapa Peristiwa di Indonesia

- **Pencurian dan penggunaan account Internet milik orang lain** . Salah satu kesulitan dari sebuah ISP (Internet Service Provider) adalah adanya account pelanggan mereka yang “dicuri” dan digunakan secara tidak sah. Berbeda dengan pencurian yang dilakukan secara fisik, “pencurian” account cukup menangkap “userid” dan “password” saja. Hanya informasi yang dicuri. Sementara itu orang yang kecurian tidak merasakan hilangnya “benda” yang dicuri. Pencurian baru terasa efeknya jika informasi ini digunakan oleh yang tidak berhak. Akibat dari pencurian ini, penggunaan dibebani biaya penggunaan account tersebut. Kasus ini banyak terjadi di ISP. Namun yang pernah diangkat adalah penggunaan account curian oleh dua Warnet di Bandung.
- **Membajak situs web** . Salah satu kegiatan yang sering dilakukan oleh cracker adalah mengubah halaman web, yang dikenal dengan istilah deface. Pembajakan dapat dilakukan dengan mengeksplorasi lubang keamanan. Sekitar 4 bulan yang lalu, statistik di

Indonesia menunjukkan satu (1) situs web dibajak setiap harinya. Hukum apa yang dapat digunakan untuk menjerat cracker ini?

- **Probing dan port scanning** . Salah satu langkah yang dilakukan cracker sebelum masuk ke server yang ditargetkan adalah melakukan pengintaian. Cara yang dilakukan adalah dengan melakukan “port scanning” atau “probing” untuk melihat servis-servis apa saja yang tersedia di server target. Sebagai contoh, hasil scanning dapat menunjukkan bahwa server target menjalankan program web server Apache, mail server Sendmail, dan seterusnya. Analogi hal ini dengan dunia nyata adalah dengan melihat-lihat apakah pintu rumah anda terkunci, merek kunci yang digunakan, jendela mana yang terbuka, apakah pagar terkunci (menggunakan *firewall* atau tidak) dan seterusnya. Yang bersangkutan memang belum melakukan kegiatan pencurian atau penyerangan, akan tetapi kegiatan yang dilakukan sudah mencurigakan. Apakah hal ini dapat ditolerir (dikatakan sebagai tidak bersahabat atau *unfriendly* saja) ataukah sudah dalam batas yang tidak dapat dibenarkan sehingga dapat dianggap sebagai kejahatan? Berbagai program yang digunakan untuk melakukan probing atau portscanning ini dapat diperoleh secara gratis di Internet. Salah satu program yang paling populer adalah “nmap” (untuk sistem yang berbasis UNIX, Linux) dan “Superscan” (untuk sistem yang berbasis Microsoft Windows). Selain mengidentifikasi port, nmap juga bahkan dapat mengidentifikasi jenis operating system yang digunakan.
- **Virus** . Seperti halnya di tempat lain, virus komputer pun menyebar di Indonesia . Penyebaran umumnya dilakukan dengan menggunakan email. Seringkali orang yang sistem emailnya terkena virus tidak sadar akan hal ini. Virus ini kemudian dikirimkan ke tempat lain melalui emailnya. Kasus virus ini sudah cukup banyak seperti virus Mellisa, I love you, dan SirCam. Untuk orang yang terkena virus, kemungkinan tidak banyak yang dapat kita lakukan. Akan tetapi, bagaimana jika ada orang Indonesia yang membuat virus (seperti kasus di Filipina)? Apakah diperbolehkan membuat virus komputer?
- **Denial of Service (DoS) dan Distributed DoS (DDos) attack** . DoS attack merupakan serangan yang bertujuan untuk melumpuhkan target (hang, crash) sehingga dia tidak dapat memberikan layanan. Serangan ini tidak melakukan pencurian, penyadapan, ataupun pemalsuan data. Akan tetapi dengan hilangnya layanan maka target tidak dapat memberikan servis sehingga ada kerugian finansial. Bagaimana status dari DoS attack ini? Bayangkan bila seseorang dapat membuat ATM bank menjadi tidak berfungsi. Akibatnya nasabah bank tidak dapat melakukan transaksi dan bank (serta nasabah) dapat mengalami kerugian finansial. DoS attack dapat ditujukan kepada server (komputer) dan juga dapat ditargetkan kepada jaringan (menghabiskan bandwidth). Tools untuk melakukan hal ini banyak tersebar di Internet. DDoS attack meningkatkan serangan ini

dengan melakukannya dari berberapa (puluhan, ratusan, dan bahkan ribuan) komputer secara serentak. Efek yang dihasilkan lebih dahsyat dari DoS attack saja.

- **Kejahatan yang berhubungan dengan nama domain** . Nama domain (domain name) digunakan untuk mengidentifikasi perusahaan dan merek dagang. Namun banyak orang yang mencoba menarik keuntungan dengan mendaftarkan domain nama perusahaan orang lain dan kemudian berusaha menjualnya dengan harga yang lebih mahal. Pekerjaan ini mirip dengan calo karcis. Istilah yang sering digunakan adalah cybersquatting. Masalah lain adalah menggunakan nama domain saingen perusahaan untuk merugikan perusahaan lain. (Kasus: mustika-ratu.com) Kejahatan lain yang berhubungan dengan nama domain adalah membuat “domain plesetan”, yaitu domain yang mirip dengan nama domain orang lain. (Seperti kasus klikbca.com) Istilah yang digunakan saat ini adalah typosquatting.
- **IDCERT (Indonesia Computer Emergency Response Team)**. Salah satu cara untuk mempermudah penanganan masalah keamanan adalah dengan membuat sebuah unit untuk melaporkan kasus keamanan. Masalah keamanan ini di luar negeri mulai dikenali dengan munculnya “sendmail worm” (sekitar tahun 1988) yang menghentikan sistem email Internet kala itu. Kemudian dibentuk sebuah Computer Emergency Response Team (CERT). Semenjak itu di negara lain mulai juga dibentuk CERT untuk menjadi *point of contact* bagi orang untuk melaporkan masalah kemanan. IDCERT merupakan CERT Indonesia .
- **Sertifikasi perangkat security** . Perangkat yang digunakan untuk menanggulangi keamanan semestinya memiliki peringkat kualitas. Perangkat yang digunakan untuk keperluan pribadi tentunya berbeda dengan perangkat yang digunakan untuk keperluan militer. Namun sampai saat ini belum ada institusi yang menangani masalah evaluasi perangkat keamanan di Indonesia. Di Korea hal ini ditangani oleh Korea Information Security Agency.

Beberapa Cracker terkenal di Dunia

- “Seorang pria yang baik di siang hari dan nampak jahat di malam hari”, begitulah yang dapat menggambarkan pemuda yang satu ini. Poulsen adalah seorang penjahat cyber paling terkenal di Amerika yang pernah ada. Untuk menjadi seorang peretas, Poulsen belajar sendiri secara otodidak. Salah satu aksi terbaik yang pernah dilakukannya adalah mengambil alih saluran telepon yang menuju stasiun radio Los Angeles KIIS-FM. Poulsen ditangkap oleh FBI akibat beberapa akun yang ia retas termasuk mail, kawat dan penipuan komputer, pencucian uang dan penggangguan pengadilan dan dihukum 51 bulan penjara dengan biaya \$ 56.000 sebagai biaya kompensasi

- Albert Gonzalez, lahir pada tahun 1981. Adalah seorang hacker komputer dan criminal computer yang dituduh mendalangi pencurian kombinasi kartu kredit dan kemudian dijual kembali lebih dari 170 juta kartu kredit dan nomor ATM dari 2005 hingga 2007, dan menjadi penipuan terbesar dalam sejarah. Gonjalez dan komplotannya menggunakan teknik injeksi SQL untuk membuat backdoor malware pada beberapa sistem perusahaan untuk meluncurkan paket sniffing yang digunakan untuk mencuri data komputer dari jaringan internet perusahaan. Gonzalez memiliki tiga dakwaan federal. Dan pada tanggal 25 Maret 2010, Gonzalez dijatuhi hukuman 20 tahun penjara federal
- Levin terkenal pada 1990-an atas upaya hacking yang terkena kerentanan situs perusahaan yang populer, salah satu yang paling terkenal dalam hal ini menjadi Citibank. Levin, pada tahun 1994, mampu mengakses rekening Citibank milik pelanggan berbagai perusahaan. Dia menggunakan layanan dial-up wire transfer dan berhasil mentransfer uang dari rekening tersebut ke rekening yang terletak di Israel, Jerman, Amerika Serikat, Finlandia, dan Belanda. Levin memiliki kaki tangan di masing-masing lokasi. Namun, 3 dari antek-anteknya diawasi ketika mereka mencoba untuk menarik uang. Mereka ditangkap dan mereka semua memberi tanda-tanda yang menunjuk keberadaan Levin. Pada tahun 1995, Levin ditangkap.
- Pada akhir semua itu, Levin bisa berhasil, tetapi secara curang mentransfer sekitar \$ 10,7 dolar dari rekening Citibank ke akun yang telah dia buat. Pada tahun 1997 dia dibawa ke Amerika Serikat dan mengaku bersalah atas konspirasi untuk menipu serta mencuri \$ 3,7 juta. Dia dimasukkan ke dalam penjara selama 3 tahun dan diperintahkan untuk membayar \$ 240.015.
- Pada November 1988, sebuah program jahat menyebar ke sekitar 6.000 mesin komputer berbasis Unix. Komputer yang jadi korban menjadi sangat lambat dan tidak bisa digunakan. Kerugiannya ditaksir mencapai jutaan dolar. Kejadian itu kemudian dikenang sebagai The Great Worm, The Great Worm of 1988 memiliki dampak besar pada ranah cyber. Bukan hanya sebagai worm yang awal menyebar di dunia, tapi juga karena membelalakkan mata dunia – terutama masyarakat non-TI pada sebuah bentuk “ancaman jahat” baru. Di balik worm itu adalah seorang brilian bernama Robert Tappan Morris. Ketika itu Morris masih bersekolah di Cornell University, alhasil worm itu pun dinamai sesuai nama belakangnya: Morris Worm. Kengerian yang ditimbulkan akibat Morris Worm diperburuk dengan tindakan yang oleh banyak kalangan dinilai berlebihan terhadap Robert Morris. RTM, demikian ia kadang disebut, menjadi orang pertama yang dihukum dalam Undang-Undang Computer Fraud and Abuse (Penyalahgunaan dan Penipuan dengan Komputer). Dia mendapatkan hukuman 3 tahun masa percobaan dan 4.000 jam layanan masyarakat. Selain itu, Morris juga harus membayar denda dan biaya-biaya lain yang totalnya hingga mencapai US\$ 10.000. Kiprah Morris di dunia akademis

menunjukkan potret seorang yang cukup brilian. Sebagai lulusan terbaik di Sekolah Menengah Atas, ia telah mencicipi tiga kampus mentereng di Amerika Serikat. Morris pertama kali kuliah di Harvard, lalu melanjutkan ke Cornell dan kembali ke Harvard sebelum akhirnya, hingga saat ini, menjadi Profesor di MIT.

- Michael Calce adalah seorang anak siswa SMA dari Westland, Quebec. Sejak muda ia sudah disebut seorang hacker tepatnya pada umur 15 tahun. Ketika ia sedang melakukan aksinya ia menyamarkan namanya menjadi "MafiaBoy". Alasan mengapa dia disebut seorang hacker karena dia pernah meluncurkan serangan 9 dari 13 root server nama, namun gagal. Dan aksi terheboh nya pada tahun 2000, dia pernah mencoba menargetkan sasarannya terhadap situs-situs komersial besar seperti Yahoo, Ebay, CNN, Amazon.com, Dell, Inc, dan E-Trade, tetapi aksinya terhenti saat ia ditangkap sedang mengacak-acak situs-situs besar tersebut.
- Ketenaran Smith adalah karena menjadi pencipta virus e-mail terkenal, Melissa. Smith mengklaim bahwa virus Melissa tidak pernah dimaksudkan untuk menyebabkan kerusakan, tetapi cara sederhana propagasi (masing-masing komputer yang terinfeksi mengirim email yang terinfeksi)membuat kelebihan beban sistem komputer dan server di seluruh dunia.Virus Smith mengambil gilirannya tidak lazim karena pada awalnya tersembunyi dalam file yang berisi password untuk 80 situs porno terkenal. Nama Melissa berasal dari seorang penari yang dikenal Smith saat dalam perjalanan di Florida. Meskipun lebih dari 60.000 pc terinfeksi virus email dalam melakukan pengiriman, Smith adalah satu-satunya orang yang ditahan meski dia hanya mengirim 1email.
- Adrian Lamo adalah seorang analis ancaman virus dan “grey hat” hacker. Dia pertama kali mendapat perhatian media adalah saat merusak beberapa profil jaringan komputer tinggi, termasuk The New York Times, Yahoo, dan Microsoft, yang berpuncak pada tahun 2003 penangkapannya. Pada tahun 2010, Lamo menjadi terlibat dalam skandal yang melibatkan WikiLeaks Bradley Manning, yang ditangkap setelah Lamo dilaporkan kepada otoritas federal bahwa Manning telah membocorkan ratusan ribu dokumen pemerintah AS yang sensitif. Pada bulan Februari 2002 ia masuk ke jaringan komputer internal dari The New York Times, menambahkan namanya ke database internal sumber ahli, dan menggunakan kertas account LexisNexis untuk melakukan penelitian tentang profil tinggi subyek. Tahun 2004, dia membobol New York Times untuk mendapatkan info personal dan beberapa security number dan membobol Microsoft. Dia akhirnya didenda 65.000 dollar AS. Saat ini dia jadi pembicara di beberapa acara seminar
- Hacker yang sebelumnya membuat gempar dunia dengan membuka kunci (unlock) Apple iPhone pada 2007 silam, kini pria berusia 20 tahun itu mengungkapkan dirinya berhasil meng-hack Sony PlayStation 3 (PS3).George Hotz, pria 20 tahun asal Amerika yang telah membobol celah keamanan PS3 yang disebut-sebut sangat sulit untuk ditembus.

Pembongkaran PS3 ini, diakui Hotz, adalah "prakarya" terbarunya. Menurut laporan BBC, dia akan mempublikasi temuannya dengan rinci secara online, dalam waktu dekat. "PlayStation 3 seharusnya unhackable (tak bisa dihack). Tetapi, kini tidak ada lagi yang unhackable," ujar Hotz, yang dikenal dengan nama maya 'Geohot'. Dia sendiri menyadari perbuatannya bisa mengakibatkan orang-orang untuk memainkan software PS3 bajakan. Namun, Hotz merasa tidak ada niat khusus untuk memasyarakatkan software bajakan. Motivasi utama Hotz adalah rasa ingin tahu, dan bagaimana membuka platform yang selama ini di rasan aman kepada BBC. Sebelumnya, nama Hotz juga sempat populer, pada 2007, karena di usianya saat itu 17 tahun, ia berhasil meng-unlock iPhone, yang saat itu dikunci hanya bisa beroperasi dengan layanan operator AT & T. Diperkirakan akibat ulahnya ada Hacker masuk ke PlayStation Network dan mencuri informasi pribadi dari 77 juta pengguna. Namun, Hotz membantah bertanggung jawab atas serangan itu, dan menambahkan "Bisa Menjalankan keamanan homebrew dan menembus skuritas pada perangkat Anda adalah keren; hacking ke server orang lain dan mencuri database dari info pengguna.adalah tidak keren. "

- James yang nama lengkapnya Joseph Jonathan James lahir di Miami Florida 12 Desember 1983 merupakan hacker yang sangat muda. Saat usia 16 tahun harus masuk penjara . Hacker yang dia lakukan adalah menginstal backdoor untuk membobol server Badan Pengurangan Ancaman Pertahanan. DTRA merupakan lembaga Departemen Pertahanan dibebankan dengan mengurangi ancaman terhadap AS dan sekutunya dari senjata nuklir, biologi, kimia, konvensional dan khusus.James juga masuk ke dalam komputer NASA, mencuri software bernilai sekitar \$ 1,7 juta.Namun,James kemudian melanggar masa percobaan bahwa ketika ia dites positif untuk penggunaan narkoba dan yang kemudian ditahan oleh Amerika Serikat Marshall Layanan dan diterbangkan ke Alabama federal. Namun, enam bulan di penjara atas pelanggaran dia memperoleh pembebasan bersyarat. James menegaskan bahwa dia jera dan mungkin memulai sebuah perusahaan keamanan komputer.Pada tanggal 18 Mei 2008, Jonathan James ditemukan tewas dari luka tembak , diduga bunuh diri.
- Gary McKinnon, hacker yang pernah membobol 97 komputer NASA, Pentagon dan Dephan Kam pada 2001-2002 silam.Kelahiran Inggris berusia 41 tahun yang bekerja sebagai computer system administrator di sebuah perusahaan ini punya "achievement" yang mencengangkan: meng-hack komputer dengan tingkat security paling ketat di dunia.Alasan Gary (online nickname: Solo) hanya satu: ia ingin tahu bahwa memang ada proyek pemerintah USA terhadap UFO yang selama ini ditutup-tutupi, dan menurut pengakuan Gary, ia berhasil melihat satu image semacam aircraft yang pastinya bukan buatan bumi. Sayangnya ada suatu "kekonyolan" bahwa ia lupa meng-save image tersebut karena dalam sesaat ia lupa fungsi save pada software RemotelyAnywhere yang

ia pakai untuk meng-hack.Gary muda sangat menggemari fiksi ilmiah dan UFO. Gary termotivasi dengan sang ayah tirinya yang pernah berkata kepadanya bahwa ayah tirinya pernah melihat sebuah UFO terbang di atas Bonnybridge, dekat Falkirk. Bonnybridge merupakan salah satu ibukota UFO di dunia. Disebut begitu karena penampakan UFO di sana tertinggi dari wilayah manapun di dunia. Gary juga mengaku menyusun daftar orang-orang di bumi yang bukan human beings. Kata Gary, meski mereka ETs, mereka sudah sangat menyerupai manusia. Sayangnya daftar tersebut ada di dalam komputernya yang disita oleh kepolisian Inggris.Gary terancam dihukum 7 tahun penjara atas kelakukannya dan denda US\$250,000. Ia membuat US Government harus mengeluarkan dana sebesar US\$700,000 untuk memperbaiki tingkat security sistemnya.Gary mesti mendekam selama tiga tahun di Inggris sebelum rencana ekstradisi ke AS. Bahkan kabarnya penjara Guantanamo sudah menantinya. Namun pada akhir Juli lalu the British House of Lord (semacam MPR (?), di atas House of Commons) bersedia untuk mendengarkan kasus ini, memberi harapan bagi Gary untuk mendapatkan semacam perlindungan. Namun jadwal hearing/pertemuan belum diketahui dengan pasti.

Daftar Pustaka

- <http://blogbriyann.blogspot.co.id/2013/10/contoh-kasus-keamanan-sistem-informasi.html>
- <http://ardirnccnetrekti.blogspot.co.id/2012/12/beberapa-contoh-kasus-serangan-terhadap.html>
- <http://siskaseptia.blogspot.co.id/2015/03/contoh-kasus-keamanan-sistem-komputer.html>



MODUL PERKULIAHAN

Keamanan Jaringan

Hardening

Fakultas
Fasilkom

Program Studi
Teknik Informatika

TatapMuka
9

Kode MK
MK:15020

Di susun Oleh
Tim Dosen

Abstract

Keamanan jaringan ([Bahasa Inggris: Network Security](#)) dalam [jaringan komputer](#) sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah.

Kompetensi

Setelah membaca modul ini diharapkan mahasiswa :

- **Mampu Hardening**

Hardening adalah proses untuk menilai atau menimbang arsitektur keamanan sistem operasi, serta proses auditing (memeriksa kembali) apakah sistem operasi yang sudah terpasang berjalan dengan baik atau tidak. Hal ini untuk mengantisipasi beberapa jenis serangan yang dapat dilakukan terhadap sistem operasi tersebut. Serangan tersebut bisa dilakukan oleh attacker apabila banyak kesalahan (vulnerable) yang dijumpai didalam sistem operasi.

System Hardening kurang lebihnya dapat disimpulkan sebagai langkah awal untuk bertahan dan mengevaluasi dari serangan yang dilakukan terhadap sistem operasi (komputer), hal ini meliputi:

- Pengecekan setelah proses instalasi awal
- Pengoptimalan sistem operasi sebelum dilakukan hubungan ke internet
- Pengecekan secara rutin apabila perlu dilakukan patching (tambahan) terhadap fasilitas pendukung yang ada didalam sistem operasi dan aplikasinya.
- Penghapusan terhadap kesalahan (vulnerabilities) yang ditemukan.

Why Hardening

1. Karena sistem operasi yang ada sekarang ini banyak terjadi kesalahan dan cenderung tidak aman (insecure configuration) secara default.
2. Untuk menerapkan standar keamanan (security policy) dari sistem operasi.
3. Menemukan lubang keamanan (security vulnerabilities) dan mencegah beberapa serangan dari akibat ditemukannya 'exploit' baru.
4. Karena perkembangan dari sistem operasi yang cenderung dinamis, proses analisa, auditing selalu diperlukan.

Where Starting Hardening

1. Kenali sistem operasi yang anda gunakan, hal ini meliputi dari struktur sistem operasi, karakteristik sistem operasi, jenis paket pendukung, dan stabilitas dari sistem operasi tersebut.
2. Pelajari bagaimana cara mengkonfigurasi sistem operasi, hal ini meliputi standar keamanan yang harus dimengerti terkait dengan sistem operasi tersebut, dan pelajari hal-hal yang berkaitan dengan kesalahan (vulnerabilities) sebelumnya dari sistem operasi tersebut, dan segera lakukan tambahan (patching) dari kesalahan yang ada.
3. Perlunya dipahami bahwa tidak semua 'services' atau packages yang anda install adalah layak digunakan (perlu digunakan). Idealnya haruslah membuang paket paket yang tidak perlu dan mengoptimalkan services standar yang dibutuhkan oleh sistem operasi tersebut sebelum terhubung dengan internet.

The three basic areas of hardening

1. Operating system

2. Application,

3. Network.

1. Operating system hardening

includes :

- configuring log files and auditing, changing default administrator account names and default passwords, and the institution of account lockout and password policies to guarantee strong passwords that can resist brute-force attacks.
- File-level security and access control mechanisms serve to isolate access attempts within the operating system environment.

Disabling Unnecessary Services

Some of the more attack-prone services include IIS, FTP, and other common web technologies. Make sure these services are disabled if they aren't needed, and keep them up-to-date with the most recent security and service packs.

Here are some tips:

- File and Print Servers
 - Vulnerable to DoS and access attacks. Make sure these servers run only the protocols needed to support the network.
- Networks with PC-Based Systems
 - Make sure NetBIOS services are disabled (ports 135, 137, 138, and 139) on servers or that an effective firewall is in place between the server and the Internet. On Unix, disable port 111, the Remote Procedure Call.
- Directory Sharing
 - Limit directory sharing to what is essential. Make sure root directories are hidden from browsing. Do not share the root directory.
- Root Directories
 - If an attacker penetrates the root directory, all the subdirectories under that directory are vulnerable.

➤ OS Hardening

Protecting Management Interfaces and Applications

- Administrator dapat melakukan perubahan konfigurasi pada sistem (s) dan mengubah pengaturan. Untuk melindungi terhadap ini, akses ke antarmuka administrasi manajemen / harus dibatasi untuk hanya mereka administrator yang membutuhkannya.
- Group Policy dapat digunakan untuk kemudahan administrasi dalam mengelola lingkungan pengguna. Hal ini dapat mencakup menginstal perangkat lunak dan pembaruan atau mengendalikan apa yang akan muncul di desktop berdasarkan fungsi

pekerjaan pengguna dan tingkat pengalaman. Objek kebijakan grup (GPO) yang digunakan untuk menerapkan kebijakan grup untuk pengguna dan komputer.

- Kebijakan kelompok memungkinkan Anda untuk mengatur standar keamanan umum yang konsisten untuk kelompok tertentu komputer dan menegakkan komputer dan pengguna konfigurasi umum. Hal ini juga menyederhanakan konfigurasi komputer dengan mendistribusikan aplikasi dan membatasi distribusi aplikasi yang mungkin memiliki lisensi terbatas.
- Keamanan template set konfigurasi yang mencerminkan peran tertentu atau standar yang ditetapkan melalui standar industri atau dalam suatu organisasi, yang ditugaskan untuk memenuhi tujuan tertentu.

• **Password Protection**

Password harus panjang dan serumit mungkin. Kebanyakan vendor menyarankan Anda menggunakan karakter nonalphabetic seperti #, \$, dan% password Anda(Strong password)

• **Disabling Unnecessary Accounts**

account diaktifkan yang tidak diperlukan pada sistem, menyediakan pintu di mana penyerang dapat memperoleh akses.

Anda harus menonaktifkan semua akun yang tidak diperlukan segera, pada server dan workstation. Berikut ini adalah beberapa jenis account Anda harus menonaktifkan:

- Karyawan yang telah meninggalkan perusahaan
- Pegawai tidak Tetap
- Tamu account default - target kemungkinan untuk hacker.

Application Hardening

- All applications and services installed on network based host systems must be included in the security hardening process to ensure that they do not provide a weak link in the security defenses.
- A number of common operating system based services are installed by default and need to be reviewed.

Application hardening

Terdiri dari:

- Default application administration accounts,
- standard passwords, and common services and protocols installed by default.
- They should be reviewed and changed or disabled as required.
- Applications must be maintained in an updated state through the regular review of hotfixes, patches, and service packs.
- **Fuzzing** Sebagian besar aplikasi yang ditulis untuk menerima input mengharapkan jenis tertentu dari data yang akan diberikan seperti nilai-nilai string, nilai numerik, dll **Fuzzing**

adalah teknik memberikan nilai yang tak terduga sebagai masukan untuk aplikasi untuk mencoba untuk membuatnya rusak/crash. Sebuah metode yang umum adalah untuk membanjiri input dengan aliran bit acak

- **(Cross-Site Request Forgery)** dikenal sebagai CSRF, sesi berkuda, dan satu-klik serangan, melibatkan perintah yang tidak sah yang datang dari pengguna terpercaya untuk website, sering tanpa sepengetahuan pengguna dan mempekerjakan beberapa jenis rekayasa sosial.
- Dengan meningkatnya penggunaan Internet Relay Chat (IRC), jenis serangan bisa terjadi di mana saja satu pengguna dapat berbicara dan berinteraksi dengan pengguna lain. Karakteristik umum untuk serangan ini termasuk memastikan identitas pengguna, mengeksplorasi kepercayaan mereka (sering oleh tipu daya), dan menggunakan permintaan HTTP. Keterbatasan utama dari serangan ini adalah bahwa korban harus terpikat.

Web Servers

- For non-public sites authentication methods should be put in place and for sites that are only to be accessible by internal users
- Intranet approach should be used so that external access is prevented by a firewall
- Secure web based transactions - SSL communication
- Web server logs should be reviewed routinely for suspicious activity. Any attempts to access unusual URLs on the web server typically indicate an attempt to exploit problems in outdated or Unpatched web servers
- Latest vendor supplied patches

Email Servers

- Unneeded configuration options of the mail server software are disabled
- All the latest vendor supplied updates are applied
- Relay prevention options should be activated
- Authentication must be used to ensure that only authorized users are able to send and receive email messages

FTP Servers

- The purpose of the File Transfer Protocol (FTP) is to allow files to be downloaded from and uploaded to remote servers.

Access can be in the form of:

- ▶ Anonymous FTP
- ▶ Authenticated FTP

Anonymous FTP accounts should be used with caution and monitored regularly.

In the case of authenticated FTP it is essential that Secure FTP be used so that login and password credentials are encrypted, rather than transmitted in plain text.

DNS Servers

- Domain Name Servers (DNS) provide the translation of human friendly names for network destination (such as a web site URL) to the IP addresses understood by routers and other network devices.
- Steps should be taken to ensure DNS software is updated regularly and that all access to servers is authenticated to prevent unauthorized zone transfers.
- Access to the server may be prevented by blocking port 53, or restricted by limiting access to the DNS server to one or more specified external systems.

Network Hardening

■ Updating Software and Hardware

- ▶ Ongoing process
- ▶ All networking software together with the firmware in routers are updated with the latest vendor supplied patches and fixes

■ Password Protection

- ▶ Routers and wireless should be protected with strong passwords

■ Disable and remove unnecessary Protocols and Services –

- ▶ For example, in a pure TCP/IP network environment it makes no sense to have AppleTalk protocols

■ Ports

- ▶ Unneeded ports blocked by a firewall and associated services disabled on any hosts within the network
- ▶ For example, a network in which none of the hosts acts as a web server does not need to allow traffic for port 80 to pass through the firewall

■ Wireless Security

- ▶ Wireless networks must be configured to highest available security level.
- ▶ For older access points WEP security should be configured with 128-bit keys.

Newer routers should implement WPA security measures.

■ Restricted Network Access

- ▶ There should be a firewall between the network and the internet.
- ▶ Other options include the use of Network Address Translation (NAT) and access control lists (ACLs).
- ▶ Authorized remote access should be enabled through the use of secure tunnels and virtual private networks.

■ Contoh:

Operating System Security Hardening for SAP HANA

Peter Schinagl

Technical Architect Global SAP Alliance

peters@suse.com



Markus Görtler

Architect & Technical Manager SAP Linux Lab

mguertler@suse.com

<http://www.slideshare.net/snoopy1710/os-security-hardeningforsaphana>

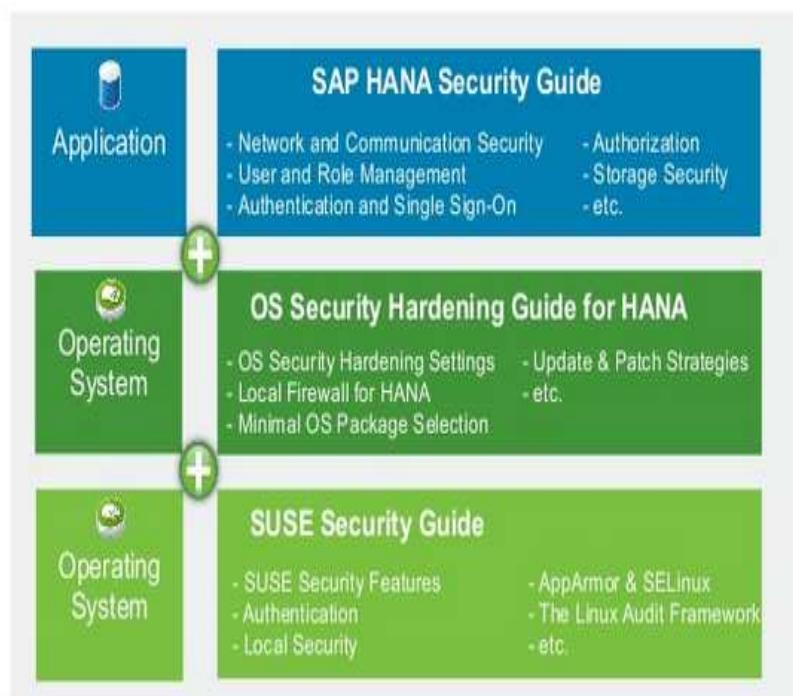
SUSE Linux Enterprise Server Security Components



Classification of the Hardening Guide



Content of the Security Guides



Customized OS Security Hardening for SAP HANA



Security Hardening Settings

Categories

- Authentication Settings
 - User login restrictions, password policy, etc.
- System Access Settings
 - Local and remote access restrictions
- Networking Settings
 - i. e. behavior of the Linux IP stack
- Linux Service permissions
 - i. e. disallow of 'at'-jobs
- File permissions
 - Access rights of security-critical files
- Logging and Reporting
 - Behavior of the system logging, security reports, etc.





Security Hardening Settings

Examples

- Prohibit root login via ssh
- Setup password strengthening
- Adjust sysctl variables (i. e. network settings)
- Adjust default umask
- Change permissions of certain system files
- Forwarding of syslog files to a central syslog server
- Configure user login restrictions via access.conf
- etc.



Security Hardening Settings

Detailed Example: Prohibit login as root via ssh

Description

By default, the user "root" is allowed to remotely log in via ssh. This has two disadvantages: First, root logins are logged, but cannot be associated with a particular user. This is especially a disadvantage if more than one system administrator makes changes on the system. Second, a stolen root password allows an attacker to login directly to the system. Instead of logging in as a normal user first, then doing "su" or a "sudo," an attacker just requires the root password.

Procedure

Edit /etc/ssh/sshd.conf and set parameter

PermitRootLogin no

Impact

Root no longer can be used to login remotely, so that users are required to use "su" or "sudo" to gain root access when using ssh.

Priority: high





SUSE Firewall for SAP HANA

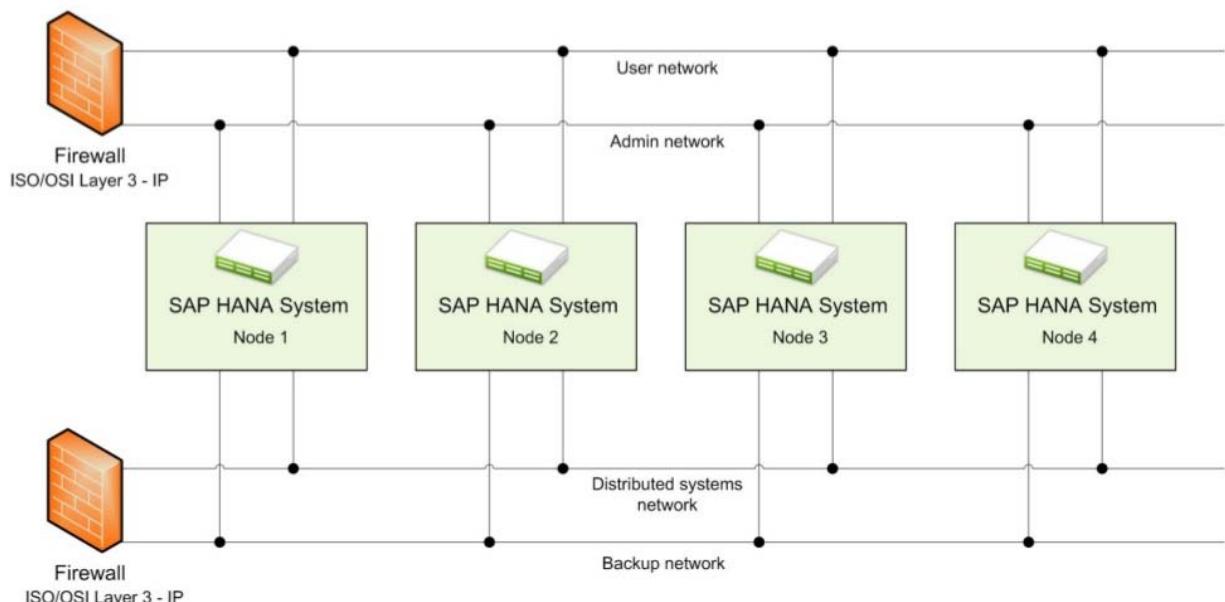
Overview

- Local firewall dedicated for SAP HANA
- Predefined service definitions according to "SAP HANA Master Guide"
- Automatic calculation of ports according to SAP HANA Instance Numbers
- Supports multiple HANA systems & instances on one system
- Dropped packages can be logged via syslog
- Easy configuration
→ via the file `/etc/sysconfig/hana_firewall`
- Available as RPM package



SUSE Firewall for SAP HANA

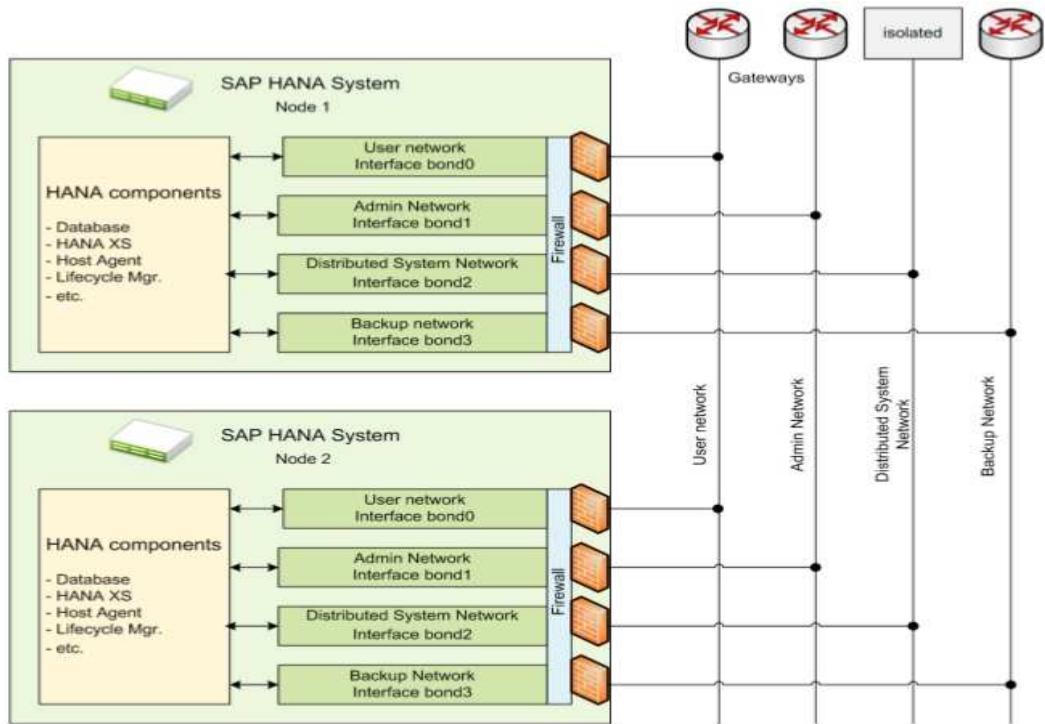
Example of a Logical Network Diagram with External Firewalls





SUSE Firewall for SAP HANA

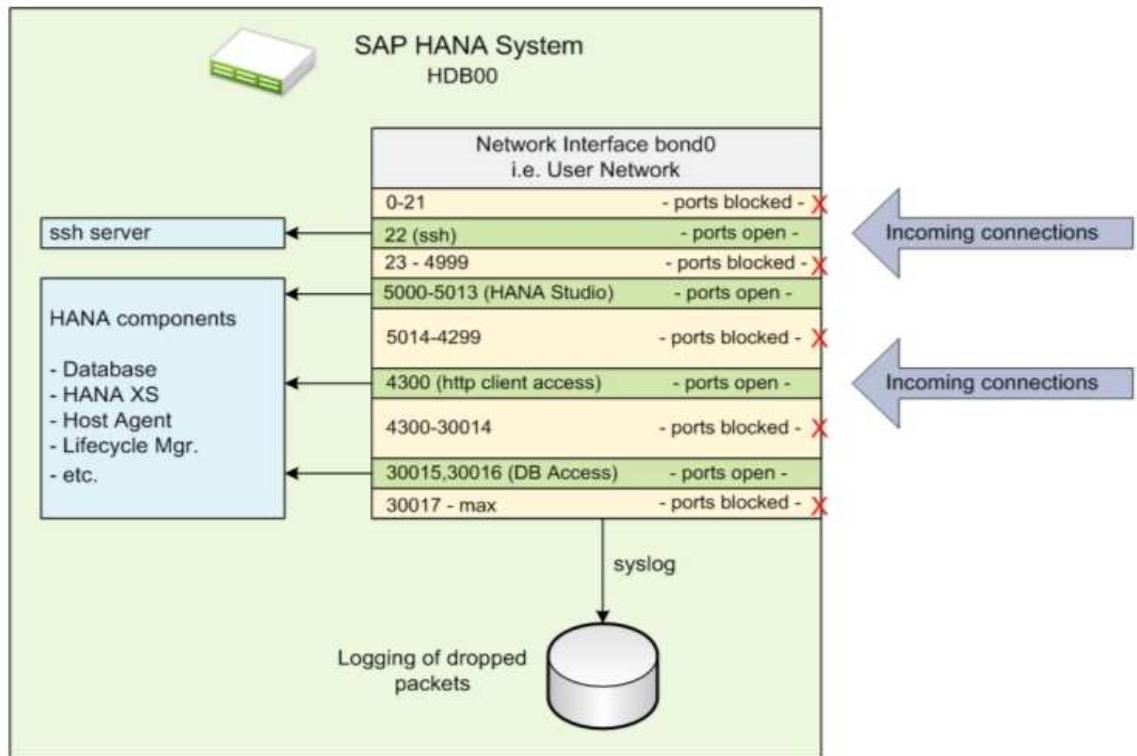
Example of a Physical Network Diagram





SUSE Firewall for SAP HANA

Traffic Flow Example



Minimal OS Package Selection

Overview

- The fewer OS packages a HANA system has installed, the less possible security holes it might have
- Just enough Operating System (JeOS) approach not perfect for HANA
- Approached based on middle ground
 - Installation patterns “Base System” + “Minimal System” + some additional packages
- Amount of packages reduced to ~550 from ~1200 (SLES standard installation)
- Described in SAP Note #1855805



SUSE Security Updates

- Security vulnerabilities are found almost every day;
Most of them are reported & fixed very quickly
- SUSE constantly provides security updates & patches
- Security updates & patches can be received via the
SUSE Linux Enterprise Server update channels
 - We generally recommend to configure update channels
- Comparison between certain update & patch strategy
 - Best update & patch strategy: Selective installation of only
security updates on a regular basis + installation of remaining
updates during maintenance windows

Daftar Pustaka

1. <http://www.fahmi.my.id/mengenal-system-hardening.html>
2. <http://www.slideshare.net/snoopy1710/os-security-hardeningforsaphana>
3. <http://slideplayer.com/slide/6283047/>
4. Nishi kumar, wwwowasp.org

5. <https://wikis.utexas.edu/display/ISO/Windows+Server+2012+R2+Hardening+Checklist>



MODUL PERKULIAHAN

Keamanan Jaringan

Ancaman Fisik & Ancaman Logik,
Identifikasi Aset Network Policy.

Fakultas
Fasilkom

Program Studi
Teknik Informatika

TatapMuka

10

Kode MK
MK:15020

Di susun Oleh
Tim Dosen

Abstract

Keamanan jaringan ([Bahasa Inggris: Network Security](#)) dalam [jaringan komputer](#) sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah.

Kompetensi

Setelah membaca modul ini diharapkan mahasiswa :

- Mampu identifikasi asset network policy, ancaman fisik & ancaman logic.

PRINSIP DASAR PERANCANGAN SISTEM YANG AMAN

- Mencegah hilangnya data
- Mencegah masuknya penyusup

Security Policy

Sebelum melanjutkan implementasi ke tingkat yang lebih jauh sebaiknya ditentukan dulu apa yang hendak dilindungi dan dilindungi dari siapa. Beberapa pertanyaan berikut dapat membantu penentuan kebijakan keamanan yang diambil.

1. **Informasi apa yang dianggap rahasia atau sensitif ?**
2. **Anda melindungi sistem anda dari siapa ?**
3. **Apakah anda membutuhkan akses jarak jauh?**
4. **Apakah password dan enkripsi cukup melindungi ?**
5. **Apakah anda butuh akses internet?**
6. **Tindakan apa yang anda lakukan jika ternyata sistem anda dibobol?**

Kebijakan keamanan tergantung sebesar apa anda percaya orang lain, di dalam ataupun di luar organisasi anda. Kebijakan haruslah merupakan keseimbangan antara mengijinkan user untuk mengakses informasi yang dibutuhkan dengan tetap menjaga keamanan sistem.

Lapisan Keamanan.

Terdiri dari:

1. Lapisan Fisik :

- Membatasi akses fisik ke mesin :
 - Akses masuk ke ruangan komputer
 - penguncian komputer secara hardware
 - keamanan BIOS
 - keamanan Bootloader
- Back-up data :
 - pemilihan piranti back-up
 - penjadwalan back-up
- Mendeteksi gangguan fisik :

log file : Log pendek atau tidak lengkap, Log yang berisikan waktu yang aneh, Log dengan permisi atau kepemilikan yang tidak tepat, Catatan pelayanan reboot atau restart, Log yang hilang, masukan su atau login dari tempat yang janggal mengontrol akses sumber daya.

2. Keamanan lokal

Berkaitan dengan user dan hak-haknya :

- Beri mereka fasilitas minimal yang diperlukan.
- Hati-hati terhadap saat/dari mana mereka login, atau tempat seharusnya mereka login.

- Pastikan dan hapus account mereka ketika mereka tidak lagi membutuhkan akses.

3. Keamanan Root

- Ketika melakukan perintah yang kompleks, cobalah dalam cara yang tidak merusak dulu, terutama perintah yang menggunakan globbing: contoh, anda ingin melakukan "rm foo*.bak", pertama coba dulu: "ls foo*.bak" dan pastikan anda ingin menghapus file-file yang anda pikirkan.
- Beberapa orang merasa terbantu ketika melakukan "touch /-i" pada sistem mereka. Hal ini akan membuat perintah-perintah seperti : "rm -fr *" menanyakan apakah anda benar-benar ingin menghapus seluruh file. (Shell anda menguraikan "-i" dulu, dan memberlakukannya sebagai option -i ke rm).
- Hanya menjadi root ketika melakukan tugas tunggal tertentu. Jika anda berusaha mengetahui bagaimana melakukan sesuatu, kembali ke shell pemakai normal hingga anda yakin apa yang perlu dilakukan oleh root.
- Jalur perintah untuk pemakai root sangat penting. Jalur perintah, atau variabel lingkungan PATH mendefinisikan lokasi yang dicari shell untuk program. Cobalah dan batasi jalur perintah bagi pemakai root sedapat mungkin, dan jangan pernah menggunakan '.', yang berarti 'direktori saat ini', dalam pernyataan PATH anda. Sebagai tambahan, jangan pernah menaruh direktori yang dapat ditulis pada jalur pencarian anda, karena hal ini memungkinkan penyerang memodifikasi atau menaruh file biner dalam jalur pencarian anda, yang memungkinkan mereka menjadi root ketika anda menjalankan perintah tersebut.
- Jangan pernah menggunakan seperangkat utilitas rlogin/rsh/rexec (disebut utilitas r) sebagai root. Mereka menjadi sasaran banyak serangan, dan sangat berbahaya bila dijalankan sebagai root. Jangan membuat file .rhosts untuk root.
- File /etc/securetty berisikan daftar terminal-terminal tempat root dapat login. Secara baku (pada RedHat Linux) diset hanya pada konsol virtual lokal (vty). Berhati-hatilah saat menambahkan yang lain ke file ini. Anda seharusnya login dari jarak jauh sebagai pemakai biasa dan kemudian 'su' jika anda butuh (mudahan-mudahan melalui ssh atau saluran terenkripsi lain), sehingga tidak perlu untuk login secara langsung sebagai root.
- Selalu perlahan dan berhati-hati ketika menjadi root. Tindakan anda dapat mempengaruhi banyak hal. Pikir sebelum anda mengetik!

4. Keamanan File dan system file

- ❖ Directory home user tidak boleh mengakses perintah mengubah system seperti

partisi, perubahan device dan lain-lain.

- ❖ Lakukan setting limit system file.
- ❖ Atur akses dan permission file : read, write, execute bagi user maupun group.
- ❖ Selalu cek program-program yang tidak dikenal

5. Keamanan Password dan Enkripsi

- ❖ Hati-hati terhadap bruto force attack dengan membuat password yang baik.
- ❖ Selalu mengenkripsi file yang dipertukarkan.
- ❖ Lakukan pengamanan pada level tampilan, seperti screen saver.

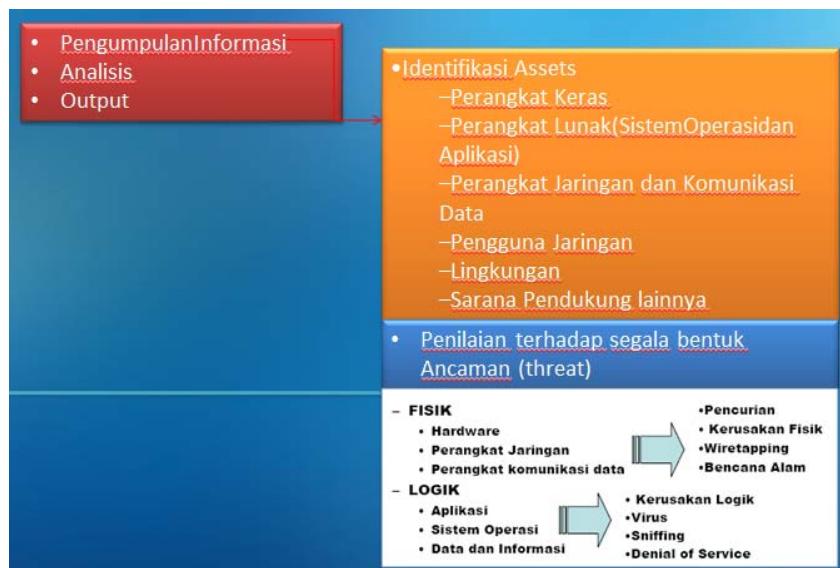
6. Keamanan Kernel

- ❖ Selalu update kernel system operasi.
- ❖ Ikuti review bugs dan kekurang-kekurangan pada system operasi.

7. Keamanan Jaringan

- ❖ Waspadai paket sniffer yang sering menyadap port Ethernet.
- ❖ Lakukan prosedur untuk mengecek integritas data
- ❖ Verifikasi informasi DNS
- ❖ Lindungi network file system
- ❖ Gunakan firewall untuk barrier antara jaringan privat dengan jaringan eksternal

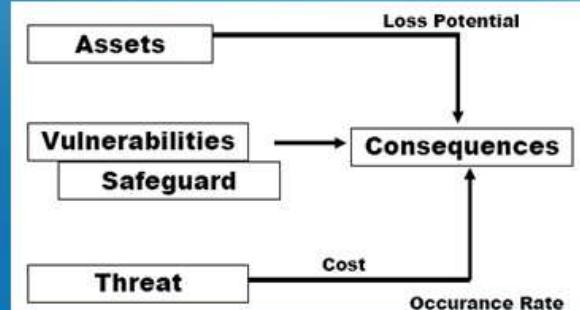
Management Resiko



- Pengumpulan Informasi
- Analisis
- Output

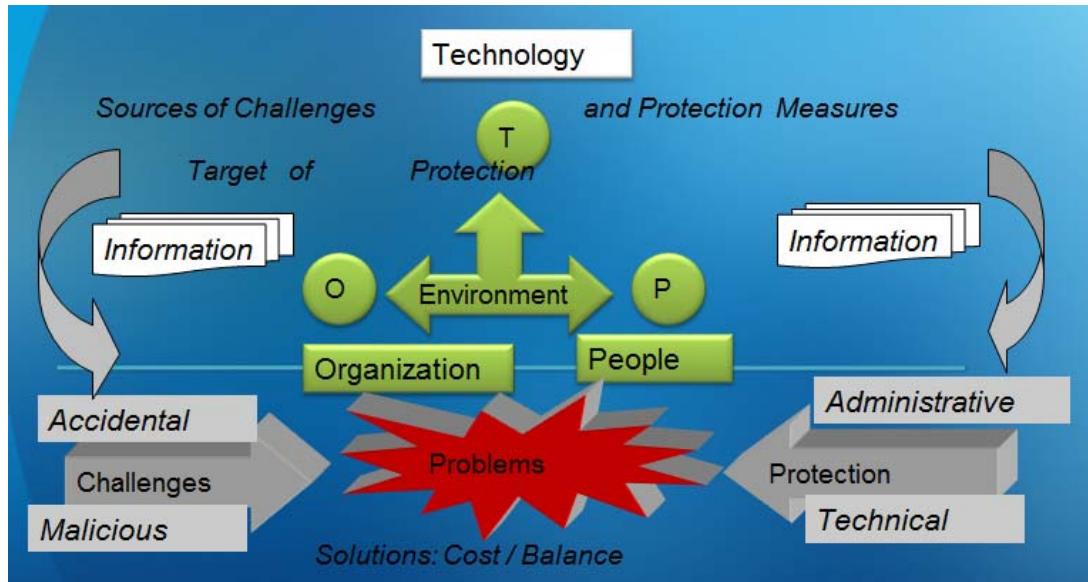
- Penilaian terhadap bagian yang berpotensi terkena gangguan (vulnerability)
- Penilaian terhadap perlindungan yang effektif (safeguard)
 - ✓ keamanan fasilitas fisik jaringan
 - ✓ keamanan perangkat lunak
 - ✓ keamanan pengguna jaringan
 - ✓ keamanan komunikasi data
 - ✓ keamanan lingkungan jaringan

- Pengumpulan Informasi
- Analisis
- Output



- Menjalankan safe guard / risk analysis tools

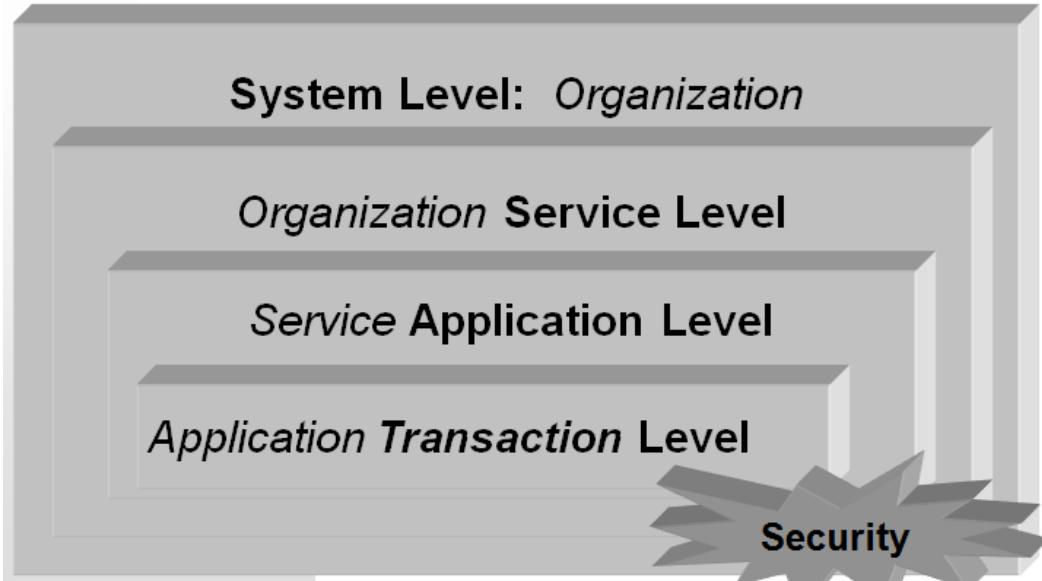
Network Security Profile



Basic Levels



SubLevels



Security Problems

Problem	Description
Accessibility	Who access: system / service.
Availability	System / service readiness.
Reliability	Identity / repudiation / legal information
Integrity	Alteration / loss of information (&SW)
Confidentiality	Disclosure of private information.
Trust	Disaster recovery.
“Cost”	“Challenges” versus “Protection”

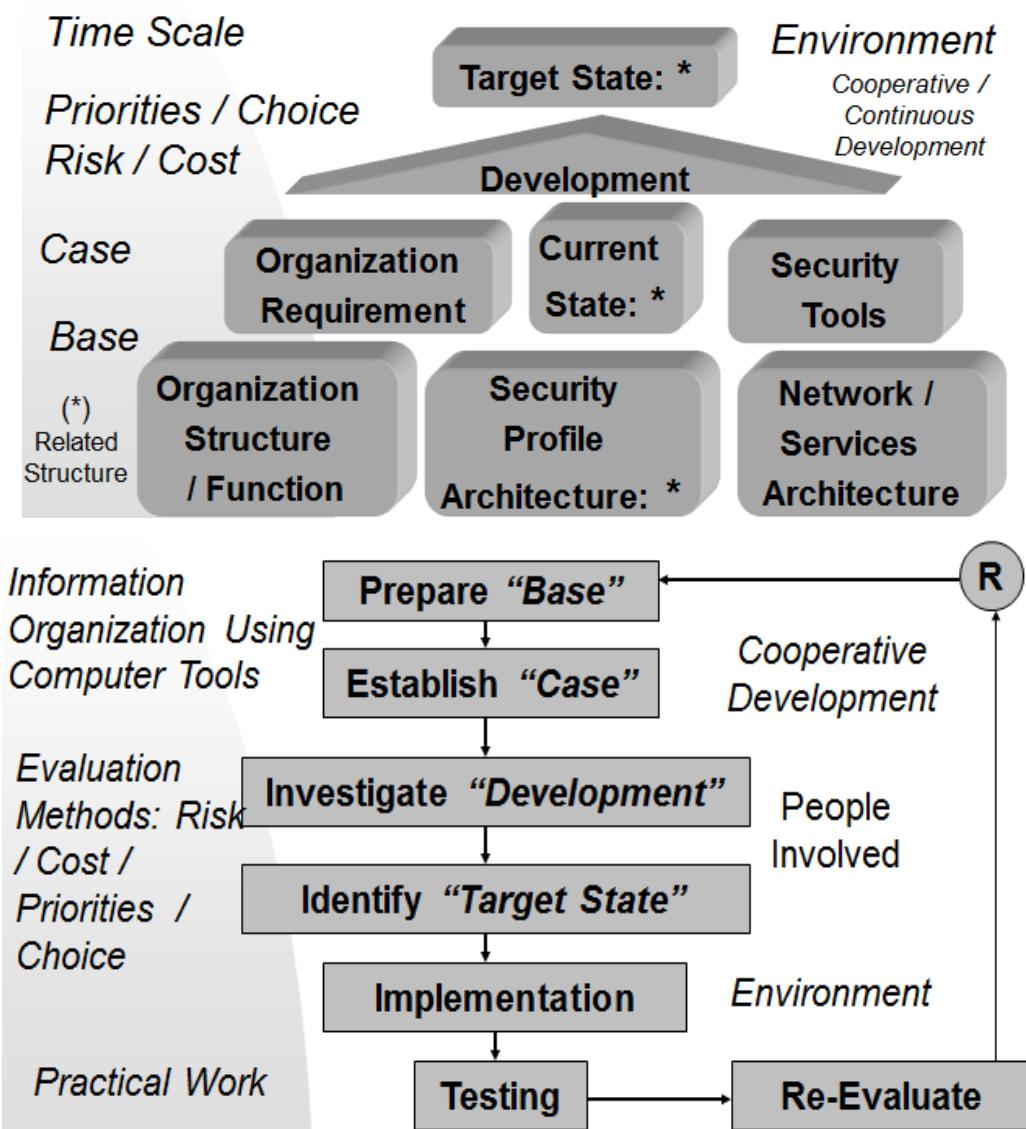
Challenges / Problems / Protection

Issues	Challenges	Protection	Security
Technology	Design Management	Quality Systems Access Systems Anti-Virus Firewalls Traffic Control Cryptographic Systems Standby Systems	Accessibility Availability Reliability Integrity Confidentiality Trust
Organization / People	Illegal Access Viruses Repudiation Cryptanalysis Theft Destruction	Awareness / Rights / Practice Policy / Management	“Risk / Cost”
Environment	Natural Professional	Laws / Regulations: Cyber-Crime Rules	

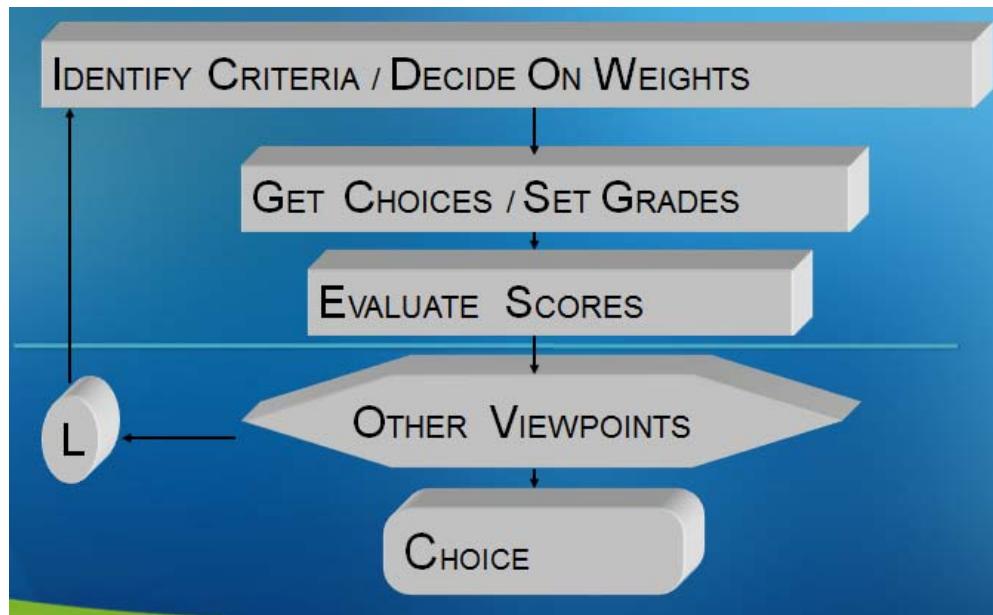
Cryptography Systems

Cryptography	Security
Symmetric Secret Key / Public-Private Keys	
Management: <i>Key Distribution / Key Agreement</i>	Confidentiality
Hash Function: <i>Message Testing</i>	Integrity
Digital Signature: <i>Authentication of Identity</i>	
Time-Stamping: <i>Non-Repudiation (Proof of Transaction)</i>	Reliability
Public Key Infrastructure: <i>Digital Certificates</i>	All the above
Security Protocols: <i>Applications</i>	

Policy Development Framework



Process: Choosing from Alternative



Process: *Risk / Cost Examples*

Issue	Fact
Virus Damage	The damage of the “I Love Virus” (May 2000) was estimated to be “\$ 10-15 billion” with the majority of the damage done in the first few hours. (The virus destroyed files and sent itself to others through MS Outlook Address Book)
Spending on Data Security	Estimated by “IDC” (International Data Corporation). “\$ 6.2 billion” (1999) / “\$ 14.8 billion” (2003)
Building a “Digital Certificate Infrastructure”	Estimated by “Identrus” (Consortium of Global Financial Companies) for financial organizations to provide trusted B-to-B e-Commerce. “\$ 5 – 10 million”

Important “Security” Webs (1/3)

Subject	Web
RSA Algorithm	www.rsasecurity.com
PGP (Pretty Good Privacy): MIT P-K “Web of Trust”	Web.mit.edu/network/pgp.html
Time-stamping	www.authentidate.com
US Legislation in Information Security	www.itaa.org/infosec
Certification Authorities	www.verisign.com www.thawte.com

Important “Security” Webs (2/3)

Subject	Web
Netscape SSL: Secure Socket Layer	www.netscape.com/security/index.html developer.netscape.com/tech/security/ss1/protocol.html
PCI: Peripheral Component Interconnect cards	www.phobos.com/products/infamily.htm
SET: Secure Electronic Transaction	www.setco.org www.visa.com www.visa.com/nt/ecommerce/security/mail.html www.mastercard.com

Important “Security” Webs (3/3)

Subject	Web
MS Authenticode	<ul style="list-style-type: none"> ■ msdn.microsoft.com/workshop/security/authcode/signfaq.asp ■ msdn.microsoft.com/workshop/security/authcode/authwp.asp
Firewalls	<ul style="list-style-type: none"> ■ www.interhack.net/pubs/fwfaq
Kerberos	<ul style="list-style-type: none"> ■ www.pdc.kth.se/kth-krb
Magazines	<ul style="list-style-type: none"> ■ www.networkcomputing.com/consensus ■ www.scmagazine.com ■ www.insightview.com

Kesimpulan:

- Security Profile:

- **Basic Factors:** *Technology / Organization / People / Environment*
 - **Levels:** *User / Intranet / Extranet / Internet*
 - **Sublevels:** *Application / Service / System*
 - **Challenges / Protection / Security Measures**
- **Development Framework / Process:**
 - **Base:** *Organization / Network / Security Profile*
 - **Case:** *Requirements / Tools / Current State*
 - **Development:** *Risk / Cost / Priorities / Cost*
 - **Target / Implementation / Testing / Cooperative Development**

Daftar Pustaka

1. **Saad Haj Bakry, PhD, CEng, FIIE**, PRESENTATIONS IN NETWORK SECURITY
2. <https://ruswendar.wordpress.com/computer/keamanan-jaringan/>



MODUL PERKULIAHAN

Keamanan Jaringan

Kriptografi, Cryptography Attack

Fakultas
Fasilkom

Program Studi
Teknik Informatika

TatapMuka

11

Kode MK
MK:15020

Di susun Oleh
Tim Dosen

Abstract

Keamanan jaringan ([Bahasa Inggris: Network Security](#)) dalam [jaringan komputer](#) sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah.

Kompetensi

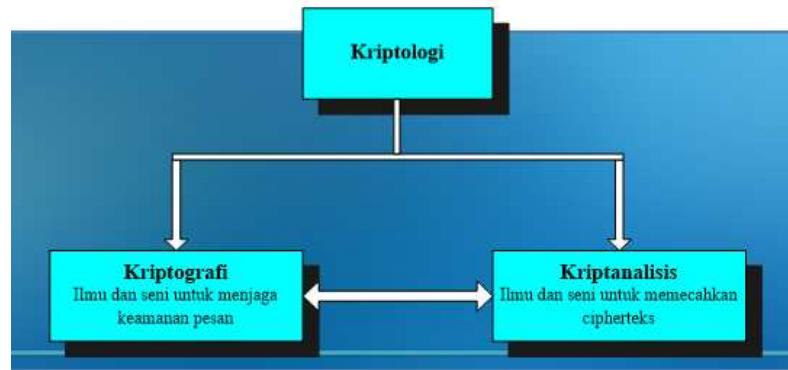
Setelah membaca modul ini diharapkan mahasiswa :

- Memahami konsep dasar peningkatan keamanan jaringan
- Mampu menjelaskan teknik keamanan jaringan secara umum, Kriptografi Attack

Terminologi

- **Kriptografi** (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. “*Crypto*” berarti “*secret*” (rahasia) dan “*graphy*” berarti “*writing*” (tulisan).
- Para pelaku atau praktisi kriptografi disebut **cryptographers**.
- Sebuah algoritma kriptografik (*cryptographic algorithm*), disebut **cipher**, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi.
- **Enkripsi** merupakan proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*)
- **Ciphertext** adalah pesan yang sudah tidak dapat dibaca dengan mudah.
- **Dekripsi** merupakan proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*.
- **Cryptanalysis** adalah seni dan ilmu untuk memecahkan *ciphertext* tanpa bantuan kunci.
- *Cryptanalyst* adalah pelaku atau praktisi yang menjalankan *cryptanalysis*.
- **Penyadap** (*eavesdropper*): orang yang mencoba menangkap pesan selama ditransmisikan.
Nama lain: *enemy, adversary, intruder, interceptor, bad guy*
- **Attack/serangan** adalah upaya sengaja untuk mengganggu sebuah sistem; biasanya mengeksplorasi kelemahan dalam sistem desain, implementasi, operasi, atau manajemen
attacks can be
 - ❖ **passive**
 - ❑ attempts to learn or make use of information from the system but does not affect system resources
 - ❑ examples: eavesdropping message contents, traffic analysis
 - ❑ difficult to detect, should be prevented
 - ❖ **active**
 - ❑ attempts to alter system resources or affect their operation
 - ❑ examples: masquerade (spoofing), replay, modification (substitution, insertion, destruction), denial of service
 - ❑ difficult to prevent, should be detected

Kriptologi (*cryptology*): studi mengenai kriptografi dan kriptanalisis.



- Persamaan kriptografer dan kriptanalisis:
 → Keduanya sama-sama menerjemahkan ciphertext menjadi plainteks
- Perbedaan kriptografer dan kriptanalisis:
 → Kriptografer bekerja atas legitimasi pengirim atau penerima pesan
 → Kriptanalisis bekerja tanpa legitimasi pengirim atau penerima pesan.

Sejarah

- Kriptografi mempunyai sejarah yang panjang.
- Tercatat Bangsa Mesir 4000 tahun yang lalu menggunakan *hieroglyph* yang tidak standard untuk menulis pesan
- Jaman dahulu orang Yunani menggunakan tool yang disebut *Scytale* untuk membantu mengenkripsi pesan yang akan mereka kirimkan. Mereka akan membungkus silinder dengan kertas, menulis pesan dan mengirimkannya.
- Metode enkripsi ini sangat mudah dipecahkan, tidak mengherankan karena ini adalah enkripsi pertama di dunia yang digunakan di dunia nyata.

Teknik Dasar Kriptografi

- **Substitusi**
- **Blocking**
- **Permutasi**
- **Ekspansi**
- **Pemampatan**
- **Substitusi**
 - Langkah pertama adalah membuat suatu tabel substitusi. Tabel substitusi dapat dibuat sesuka hati, dengan catatan bahwa penerima pesan memiliki tabel yang sama untuk keperluan dekripsi.
 - Bila tabel substitusi dibuat secara acak, akan semakin sulit pemecahan ciphertext oleh orang yang tidak berhak.

Contoh :

- Tabel subsitusi
- Caesar Chipher
- ROT 13

Tabel Subtitusi

A-B-C-D-E-F-G-H-I-J-K-L-M-N-O-P-Q-R-S-T-U-V-W-X-Y-Z-1-2-3-4-5-6-7-8-9-0-.,

B-F-1-K-Q-G-A-T-P-J-6-H-Y-D-2-X-5-M-V-7-C-8-4-I-9-N-R-E-U-3-L-S-W-,-.-O-Z-0

Contoh :

SISTEM

7P7CQY (TABEL SUBSITUSI)

VLVWHP (CAESAR CHIPHER)

FVFGRZ (ROT13)

- **Caesar Cipher**

Metode Caesar Cipher yang digunakan oleh Julius Caesar. Pada prinsipnya, setiap huruf digantikan dengan huruf yang berada tiga (3) posisi dalam urutan alfabet.

Sebagai contoh huruf “a” digantikan dengan huruf “D” dan seterusnya.

Transformasi yang digunakan adalah:

plain : a b c d e f g h i j k l m n o p q r s t u v w x y z

cipher: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Contoh:

WINPOIN maka dituliskan ZLQSRLQ.

- **ROT13**

Pada sistem ini sebuah huruf digantikan dengan huruf yang letaknya 13 posisi darinya.

Sebagai contoh, huruf “A” digantikan dengan huruf “N”, huruf “B” digantikan dengan huruf “O”, dan seterusnya.

Secara matematis, hal ini dapat dituliskan sebagai:

$$C \text{ ROT13} = (M)$$

Untuk mengembalikan kembali ke bentuk semulanya dilakukan proses enkripsi ROT13 dua kali.

$$M = \text{ROT13}(\text{ROT13}(M))$$

- **Blocking**

- Sistem enkripsi terkadang membagi plaintext menjadi blok-blok yang terdiri dari beberapa karakter yang kemudian dienkripsi secara independen.
- Dengan menggunakan enkripsi blocking dipilih jumlah lajur dan kolom untuk penulisan

pesan. Jumlah lajur atau kolom menjadi kunci bagi kriptografi dengan teknik ini.

- Plaintext dituliskan secara vertikal ke bawah berurutan pada lajur, dan dilanjutkan pada kolom berikutnya sampai seluruhnya tertulis. Ciphertext-nya adalah hasil pembacaan plaintext secara horizontal berurutan sesuai dengan blok-nya.

Jika plaintext adalah 5 TEKNIK DASAR KRIPTOGRAFI maka hasil ciphertext) .

Jika menggunakan teknik blocking dengan 1blok berisi 4 karakter.

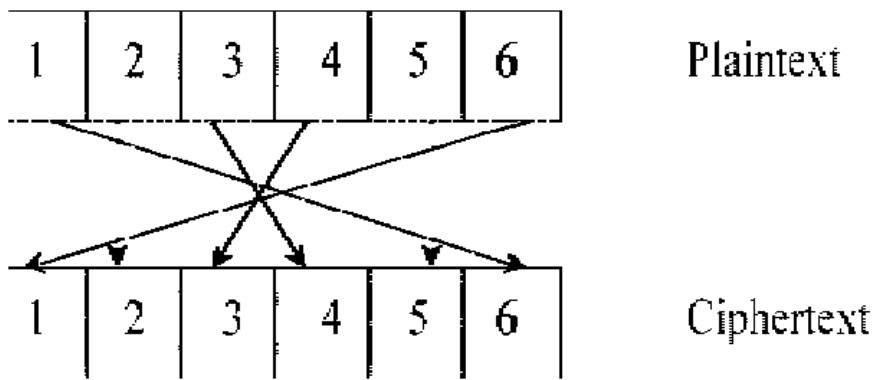
5	K		G		BLOK 1
		K	R		BLOK 2
T	D	R	A		BLOK 3
E	A	I	F		BLOK 4
K	S	P	I		BLOK 5
N	A	T			BLOK 6
I	R	O			BLOK 7

Jadi ciphertext yang dihasilkan dengan teknik ini adalah

"5K G KRTDRAEAIFKSPINAT IRO".

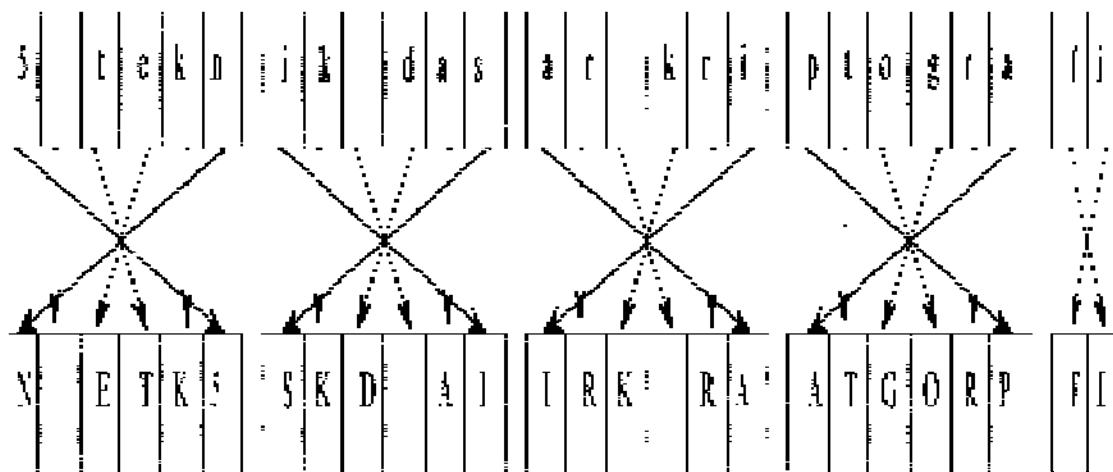
Plaintext dapat pula ditulis secara horizontal dan ciphertextnya adalah hasil pembacaan secara vertikal.

- **Permutasi**
- Salah satu teknik enkripsi yang terpenting adalah permutasi atau sering juga disebut transposisi. Teknik ini memindahkan atau merotasikan karakter dengan aturan tertentu. Prinsipnya adalah berlawanan dengan teknik substitusi.
- Dalam teknik substitusi, karakter berada pada posisi yang tetap tapi identitasnya yang diacak. Pada teknik permutasi, identitas karakternya tetap, namun posisinya yang diacak.
- Sebelum dilakukan permutasi, umumnya plaintext terlebih dahulu dibagi menjadi blok-blok dengan panjang yang sama.
- Untuk contoh diatas, plaintext akan dibagi menjadi blok-blok yang terdiri dari 6 karakter, dengan aturan permutasi sebagai berikut :



- **Permutasi**

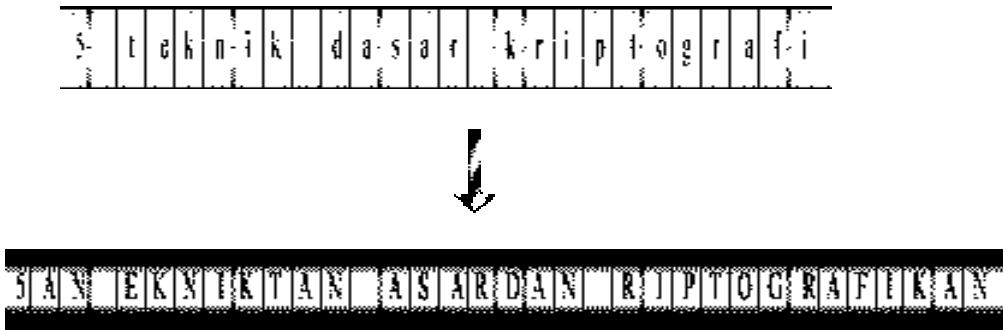
Dengan menggunakan aturan diatas, maka proses enkripsi dengan permutasi dari plaintext adalah sebagai berikut :



Ciphertext yang dihasilkan dengan teknik permutasi ini adalah "N ETK5 SKD AIIRK RAATGORP FI".

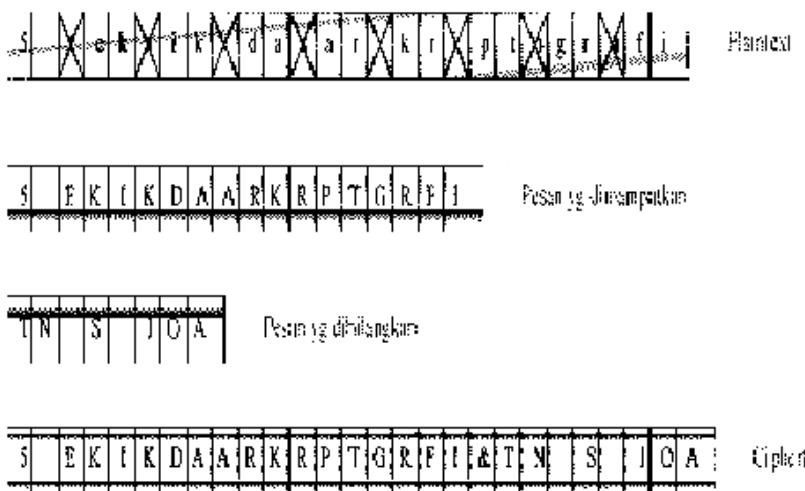
- **Ekspansi**

- Suatu metode sederhana untuk mengacak pesan adalah dengan memelarkan pesan itu dengan aturan tertentu.
- Salah satu contoh penggunaan teknik ini adalah dengan meletakkan huruf konsonan atau bilangan ganjil yang menjadi awal dari suatu kata di akhir kata itu dan menambahkan akhiran "an".
- Bila suatu kata dimulai dengan huruf vokal atau bilangan genap, ditambahkan akhiran "i".
- Proses enkripsi dengan cara ekspansi terhadap plaintext terjadi sebagai berikut :



Ciphertextnya adalah
"5AN EKNIKTAN ASARDAN RIPTOGRAFIKAN".

- Pemampatan
- Mengurangi panjang pesan atau jumlah bloknya adalah cara lain untuk menyembunyikan isi pesan. Contoh sederhana ini menggunakan cara menghilangkan setiap karakter ke-tiga secara berurutan.
- Karakter-karakter yang dihilangkan disatukan kembali dan disusulkan sebagai "lampiran" dari pesan utama, dengan diawali oleh suatu karakter khusus, dalam contoh ini digunakan "&".
- Proses yang terjadi untuk plaintext kita adalah :



Teknik Dasar Kriptografi

• Penggunaan Kunci

- Salah satu cara untuk menambah tingkat keamanan sebuah algoritma enkripsi dan dekripsi adalah dengan menggunakan sebuah kunci (*key*) yang biasanya disebut *K*.
- Sehingga persamaan matematisnya menjadi:

$$EK(M) = C$$

$$DK(C) = M$$

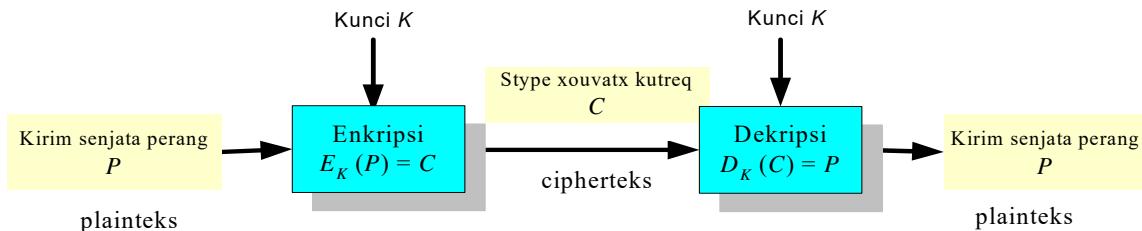
- Atau:

Enkripsi: $E_K(P) = C$

Dekripsi: $D_K(C) = P$

Harus dipenuhi: $D_K(E_K(P)) = P$

- Terdapat 2 macam kunci :
- 1. Algoritma Simetris
- 2. Algoritma Asimetris



Algoritma kriptografi berdasarkan jenis kunci yang digunakan:

- Algoritma *simetris*

Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi adalah kunci yang sama

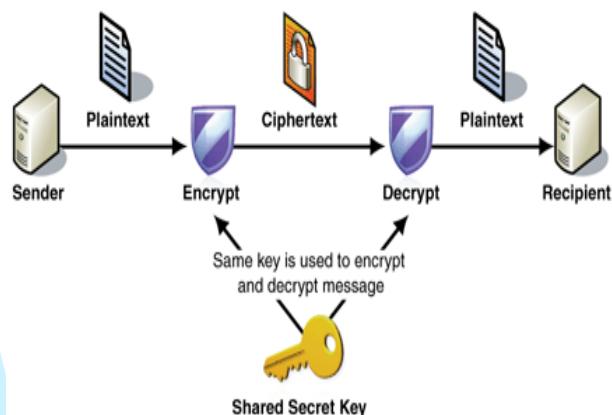
- Algoritma *asimetris*

Dimana kunci yang digunakan untuk proses enkripsi dan dekripsi menggunakan kunci yang berbeda.

- Algoritma simetris (*symmetric algorithm*)** adalah suatu algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm*.

Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu suatu kunci tertentu yang sama untuk dipakai bersama, dan kunci ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini disebut juga algoritma kunci rahasia (*secret-key algorithm*).

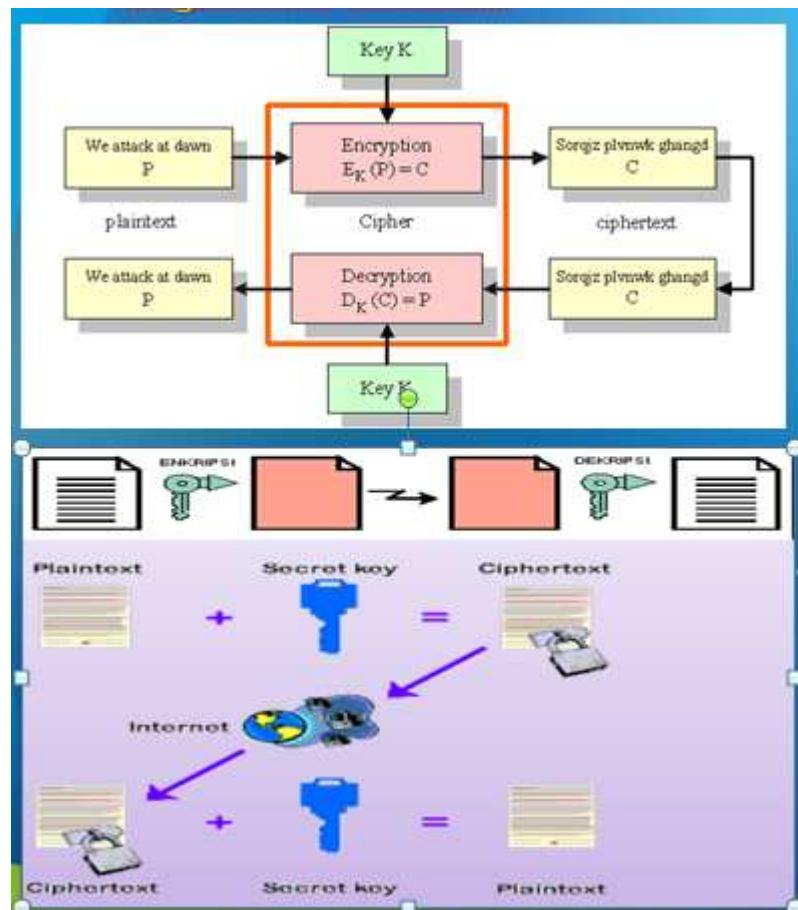
Metode : DES (*Data Encryption Standard*)



Alice menaruh sebuah pesan rahasia di dalam kotak dan mengunci kotak menggunakan

gembok dan ia memiliki kuncinya. Kemudian dia mengirimkan kotak ke Bob melalui surat biasa. Ketika Bob menerima kotak, ia menggunakan kunci salinan sama persis yang dimiliki Alice untuk membuka kotak dan membaca pesan. Bob kemudian dapat menggunakan gembok yang sama untuk membalas pesan rahasia.

Algoritma Simetris



Contoh algoritma simetri:

- **DES (Data Encryption Standard)**
- **Rijndael**
 - **Blowfish**
 - **IDEA**
 - **GOST**
 - **Serpent**
 - **RC2, RC4, Rc5, dll**

- **Algoritma ASimetris**

Algoritma asimetris (*asymmetric algorithm*) adalah suatu algoritma dimana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi.

Pada algoritma ini menggunakan dua kunci yakni kunci publik (*public key*) dan kunci privat (*private key*).

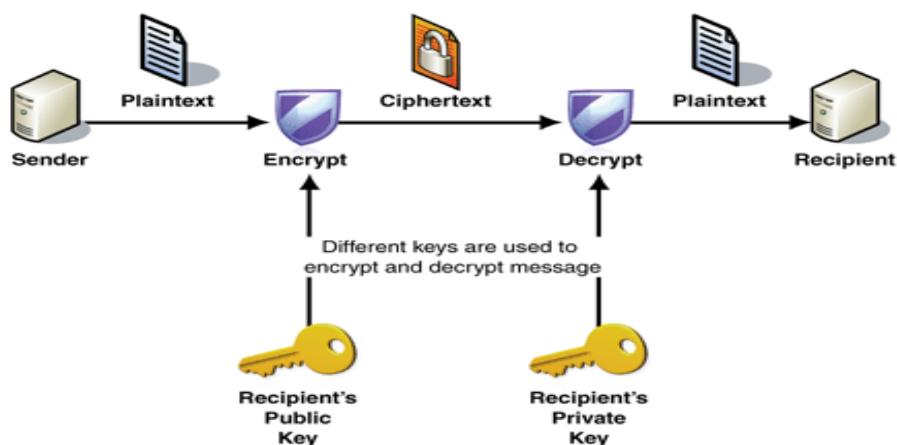
Kunci publik disebarluaskan secara umum sedangkan kunci privat disimpan secara rahasia

oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci privat yang digunakan.

Metode : RSA (Rivest, Shamir, Adleman)

Contoh algoritma nirsimetri/Asimetris:

- RSA
- ElGamal
- Rabin
- Diffie-Hellman Key Exchange
- DSA
- dll



- Pertama Alice meminta Bob untuk mengirim gembok yang terbuka melalui surat biasa, sehingga ia tidak membagikan kuncinya. Ketika Alice menerimanya, ia menggunakannya untuk mengunci sebuah kotak yang berisi pesan dan mengirimkan kotak dengan gembok terkunci tadi ke Bob. Bob kemudian membuka kotak dengan kunci yang ia pegang karena itu gembok miliknya untuk membaca pesan Alice. Untuk membalasnya, Bob harus meminta Alice untuk melakukan hal yang sama.
- Keuntungan dari metode asymmetric key adalah Bob dan Alice tidak pernah berbagi kunci mereka. Hal ini untuk mencegah pihak ketiga agar tidak menyalin kunci atau memata-matai pesan Alice dan Bob. Selain itu, jika Bob ceroboh dan membiarkan orang lain untuk menyalin kuncinya, pesan Alice ke Bob akan terganggu, namun pesan Alice kepada orang lain akan tetap menjadi rahasia, karena orang lain akan memberikan gembok milik mereka ke Alice untuk digunakan.

Berdasarkan besar data yang diolah dalam satu kali proses

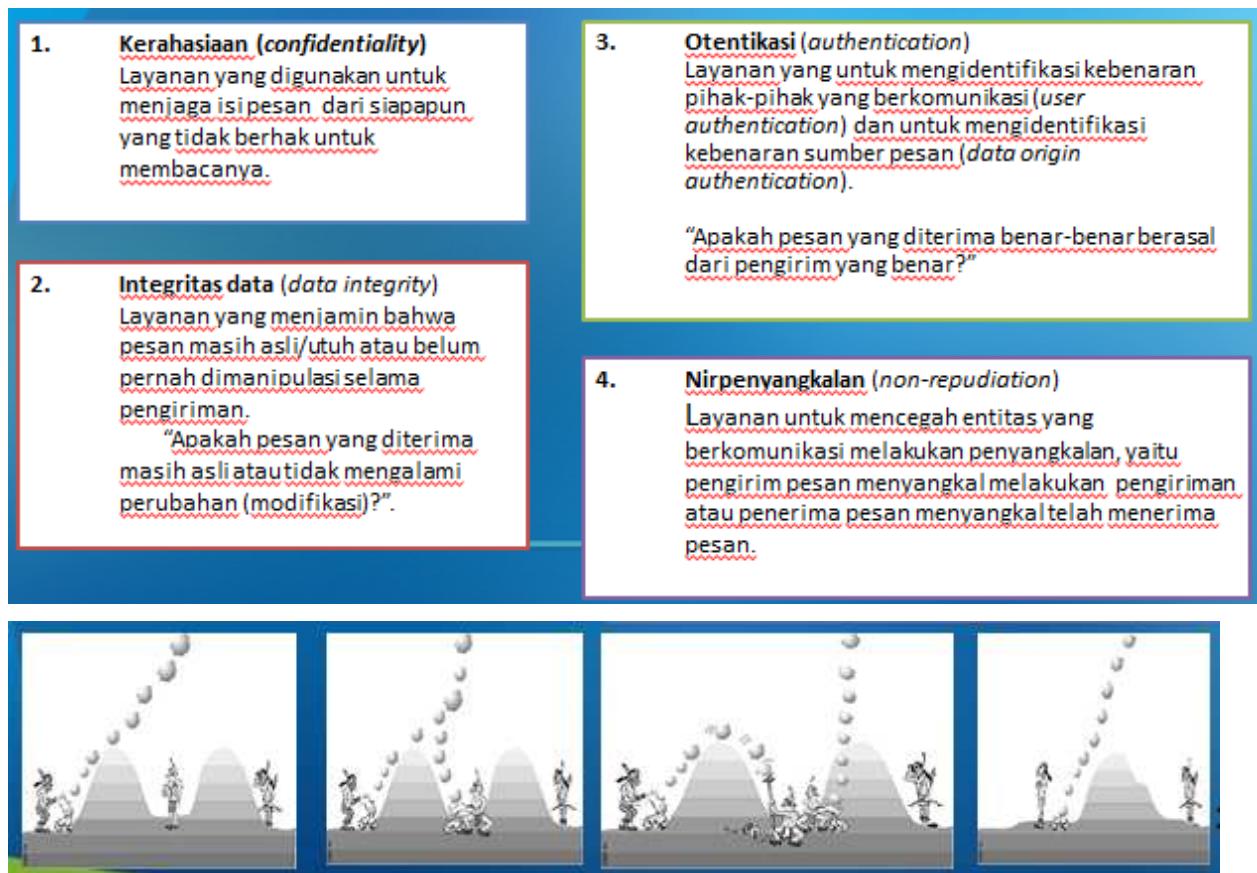
- **Algoritma *block cipher***

Informasi/data yang hendak dikirim dalam bentuk blok-blok besar (misal 64-bit) dimana blok-blok ini dioperasikan dengan fungsi enkripsi yang sama dan akan menghasilkan informasi rahasia dalam blok-blok yang berukuran sama.

- **Algoritma *stream cipher***

Informasi/data yang hendak dikirim dioperasikan dalam bentuk blok-blok yang lebih kecil (byte atau bit), biasanya satu karakter persatuan persatuan waktu proses, Penggunaan transformasi enkripsi yang berubah setiap waktu.

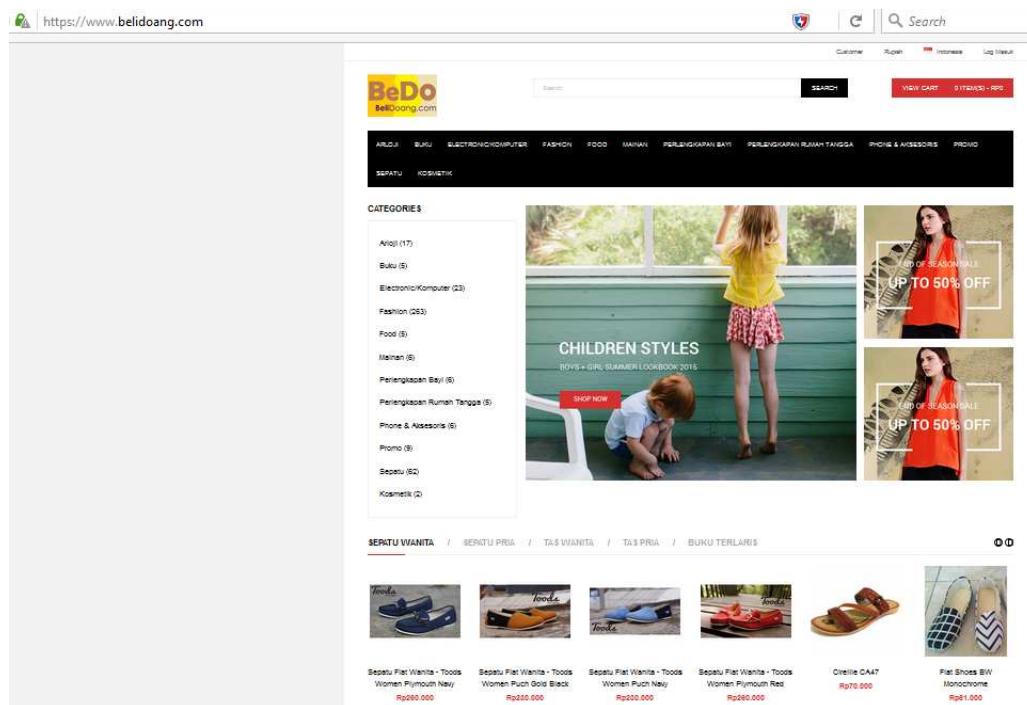
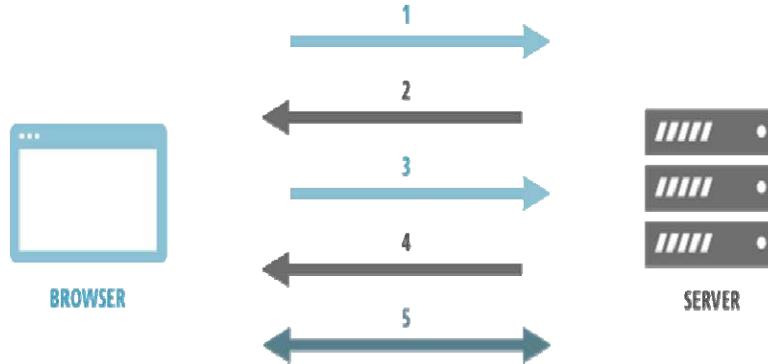
Layanan Kriptografi



Keamanan Enkripsi di Bidang Web

- Selama bertahun-tahun, protokol SSL (Secure Sockets Layer) telah mengamankan transaksi web menggunakan enkripsi antara web browser dan web server, melindungi kamu dari siapa pun yang mengintai kamu.
- SSL sendiri memiliki konsep yang sederhana. Dimulai ketika browser meminta halaman yang aman (biasanya https://).
- Web server mengirimkan kunci publik dengan sertifikat.
- Browser memeriksa sertifikat yang dikeluarkan oleh pihak terpercaya (biasanya CA), bahwa sertifikat tersebut masih berlaku dan sertifikat masih berkaitan dengan web tersebut.
- Browser kemudian menggunakan kunci publik untuk mengenkripsi kunci symmetric secara acak dan mengirimkannya ke server dengan URL terkenkripsi, membutuhkan juga enkripsi http data.
- Web server mendekripsi enkripsi symmetric key menggunakan kunci pribadi dan menggunakan kunci sysmmetric untuk mendekripsi URL dan http data.
- Web server mengirimkan kembali permintaan dokumen html dan enkripsi http data

dengan browser symmetric key. Browser mendekripsi http data dan dokumen html menggunakan symmetric key dan menampilkan informasi.



Cryptography Attack

1. Attack on Caesar Cipher.

Although historically Julius Caesar used a shift of 3 for his cipher, any ciphering based on alphabet shifting of the plaintext is called Caesar cipher. This is a very simple method of ciphering, and provides very little security. However it is still applied mostly in forum or bulletin board to post possibly offensive materials, or to provide answers to riddles where there would be no accident of unintended glimpse. For shift value 3, we have "A" encrypted to "D", "B" encrypted to "E", "C" encrypted to "F" and so on. "X", "Y" and "Z" will be encrypted to "A", "B" and "C" respectively.

Caesar cipher only has 25 possibilities of a key. A direct brute-force attack testing each key is simplest and fastest for attacking the ciphertext.

For example, suppose we intercepted a ciphertext below and we suspected it had been

encrypted with Caesar Cipher.

KIMAIZKQXPMZQA MIAG

We could then start our brute-force attack. For shift of 1, we have obtain,

CIPHER	K	I	M	A	I	Z	K	Q	X	P	M	Z	Q	A	M	I	A	G
PLAIN	J	H	L	Z	H	Y

It is already apparent that 1 is not the key and we may continue with 2 and so on. With key = 8, we finally get intelligible result.

CAESARCIPHERISEASY

Attack was successful.

Types of Attack

- 1) Ciphertext-only
 - 2) Known Plaintext
 - 3) Chosen Plaintext
 - 4) Chosen Ciphertext
 - 5) Side Channel Attack
- 2) 1. Ciphertext-Only

All attacks described so far are examples of ciphertext-only attack where the attacker only has ciphertext. This type of attack is most common, but also most difficult because of lack of information.

2. Known Plaintext

Information can never make things harder. With this type of attack, the attacker possesses a string of plaintext, x and the corresponding ciphertext, y.

Consider this example of known plaintext attack with monoalphabetic substitution cipher. The following ciphertext is intercepted and is known to contain information about a person called "ANDERSON" and a place called "MISSISSIPPI".

JZKGXAHZDAVGZGBWGJKHUAIDGADZEDAADAADIID

Here, rather than applying frequency analysis which might not be helpful particularly on short ciphertext, we could use our information of the plaintext to devise stronger attack. Since we know the message contains the word MISSISSIPPI, we look for a sequence of 11 letters where the 3rd, 4th, 6th and 7th letters are the same and so are the 2nd, 5th, 8th and 11th. It would not take long to notice that the sequence 'EDAADAADIID' is the ciphertext for 'MISSISSIPPI'.

2. Known Plaintext

Information can never make things harder. With this type of attack, the attacker possesses a string of plaintext, x and the corresponding ciphertext, y.

Consider this example of known plaintext attack with monoalphabetic substitution cipher.

The following ciphertext is intercepted and is known to contain information about a

person called “ANDERSON” and a place called “MISSISSIPPI”.

JZKGXAHZDAVGZGBWGJKHUAIDGADZEDAADAADIID

Here, rather than applying frequency analysis which might not be helpful particularly on short ciphertext, we could use our information of the plaintext to devise stronger attack. Since we know the message contains the word MISSISSIPPI, we look for a sequence of 11 letters where the 3rd, 4th, 6th and 7th letters are the same and so are the 2nd, 5th, 8th and 11th. It would not take long to notice that the sequence ‘EDAADAADIID’ is the ciphertext for ‘MISSISSIPPI’.

Similarly for ANDERSON, we look for a sequence of 8 letters where all characters are different except for the 2nd and the 8th. A small branch of computing studies called regular expression along with appropriate software will be helpful to speed up the search, but eventually the attacker will find that ‘JZKGXAHZ’ represents ‘ANDERSON’

With the newly gained information so far, the ciphertext has been decrypted to

ANDERSONISVWENEBWEADOUSPIESINMISSISSIPPI

Subsequent effort of cryptanalysis may eventually reveal the secret,

ANDERSON IS THE NEW HEAD OF SPIES IN MISSISSIPPI

Here, it can be seen that information of plaintext opens up new possibilities of attacking methods. This type of attack is possible with encryption of documents which are known to follow certain templates. For example, an email usually starts with ‘Dear Sir’ or ‘Dear Madam’ and ends with ‘Yours Sincerely’ or ‘Regards’.

3. Chosen Plaintext Attack

This attack is different from Known Plaintext Attack in such way that the attacker can choose which plaintext is to be encrypted, and later analyse the relationship of the output ciphertext to get the key used for encryption.

For example, suppose we want to attack communication from Alice to Bob which is encrypted by monoalphabetic substitution cipher. The intercepted messages so far could not be solved using frequency analysis. And we know how helpful it is if we can get Alice to send an encrypted message to Bob which contains the word ‘MISSISSIPPI’.

Here, we can send an email to Alice, “Please tell Bob that saying Mississippi will take exactly one second”. Then, whether Alice sends a fresh email to Bob or simply forward our written email, we can intercept the message and obtain some information about the mapping of plaintext to ciphertext used in encryption of communication from Alice to Bob.

This type of attack is even stronger as the attacker has more control of the operation.

4. Chosen Ciphertext Attack

This type of attack is normally associated with the decryption process where the opponent has obtained temporary access to the decryption machinery.² He may then select a ciphertext string to construct the corresponding plaintext string.

5. Attack on Polyalphabetic Substitution Cipher

It was evident that monoalphabetic substitution ciphers had a lot of weaknesses, so cryptographers came up with a stronger solution, polyalphabetic cipher. Whereas monoalphabetic substitution cipher has one-to-one relationship between plaintext and ciphertext, polyalphabetic substitution cipher has one-to-many relationship. This means the letter 'E' in plaintext may be encrypted to 'J' or 'X'. This is a useful encryption technique against frequency analysis as the letters frequencies are more obscured.

Viginere Cipher

This is a type of polyalphabetic substitution cipher. With this cipher, if the encryption key is "SECRETKEY", the first letter of the message will be encrypted with 'S' , second letter of the message with 'E' and so on, following the order of the key's character order. If the encryption reaches the last character of the key, the next message's letter will be encrypted with the first character of the key again and the cycle continues.

Attacking Viginere Cipher

This ciphertext is from Cryptology Theory and Practice.

CHREEVOAHMAERATBIAXXWTNXBEEOPHBSQMQUEQERBWVXUOAKX
AOSXXWEAHBWGJMMQMNMGRFGXWTRZXWIAKLXFPSKAUTEMND
MGTSXMXBTUIADNGMGPSRELXNJELXVRVPRTULHDNQWTWDTYGBPH
XTFALJHASVBFXNGLLCHRZBWELEKMSJIKNBHWRJGNMGJSGLXFEYP
HAGNRBIEQJTAMRVLCRREMNDGLXRRIMGNSNRWCHRQHAEYEVTAQE
BBIPEEWEVKAKOEWADREMXTBHHCHRTKDNRZCHRCLOHPWQAI
IWXRNRMGWOIIFKEE

The first operation is to guess the length of the key used to encrypt. This can be done by performing Kasiski test, performed with the following steps.

- 1) Record where similar sequences of letters occur in many places.

Here we notice the sequence CHR occurs in five places beginning at position 1, 166, 236, 276, and 286.

- 2) Calculate the distance between occurrences and the first occurrence. a) $166 - 1 = 165$
b) $236 - 1 = 235$
c) $276 - 1 = 275$
d) $286 - 1 = 285$
- 3) Calculate the greatest common divisor of the calculated values. gcd (165, 235, 275, 285)
- 4) The result is the likely length of the key used.

If we had guessed the key length correctly, the complexity of polyalphabetic substitution cipher is reduced to that of monoalphabetic substitution cipher. Suppose the guessed key length is 5, we may then proceed by dividing the ciphertext into a group of 5. Group 1 formed by 1st, 6th, 11th ... letters, Group 2 by 2nd, 7th, 12th ... letters. Frequency analysis can then be formed on these individual groups.

Kesimpulan:

- Cryptography is the heart of security. While strong cryptography does not guarantee strong security, weak cryptography certainly guarantees weak security. Equally important is the protocol and management involved in implementing the cryptography.
- However, the impracticality of perfect security is often not a problem, as the main concern is to make the attack to imperfect security instead to be impractical.

DaftarPustaka

- <https://idazuwaika.files.wordpress.com/2008/06/attack-on-cryptography.pdf>
- https://id.wikipedia.org/wiki/Serangan_DoS
- <http://www.braingle.com/brainteasers/codes/caesar.php>



MODUL PERKULIAHAN

Keamanan Jaringan

Algoritma Kriptografi,
Cryptography One way Hash

Fakultas
Fasilkom

Program Studi
Teknik Informatika

TatapMuka

Kode MK
MK:15020

Di susun Oleh
Tim Dosen

12

Abstract

Keamanan jaringan ([Bahasa Inggris: Network Security](#)) dalam [jaringan komputer](#) sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah.

Kompetensi

Setelah membaca modul ini diharapkan mahasiswa :

- Memahami konsep dasar peningkatan keamanan jaringan
- Mampu menjelaskan teknik keamanan jaringan secara umum, One wa hash

Pendahuluan

- Kerahasiaan dan keamanan saat melakukan pertukaran data adalah hal yang sangat penting dalam komunikasi data, baik untuk tujuan keamanan bersama, maupun untuk privasi individu.
- Mereka yang menginginkan agar datanya tidak diketahui oleh pihak-pihak yang tidak berkepentingan selalu berusaha melakukan upaya-upaya pengamanan informasi terhadap informasi yang akan dikomunikasikan.
- Untuk menjamin keaslian dari suatu data yang dikirim perlu adanya suatu tindakan yang mengarah pada konsep otentikasi agar integritas data tetap terjaga.
- Konsep Otentikasi tersebut meliputi Fungsi hash, identifikasi, Otentikasi entitas, dan tanda tangan digital.

Jenis Algoritma Kriptografi

Algoritma Simetri

- a. Blok Chiper : DES, IDEA, AES
- b. Stream Chiper : OTP, A5 dan RC4

Algoritma Asimetri : RSA, DH, ECC, DSA

Fungsi Hash : MD5, SHA1

Dalam presentasi ini , dipelajari Algoritma AES, RSA dan MD5

ALGORITMA SIMETRI : BLOK CHIPER

AES (Advanced Encryption Standard)

- DES dianggap sudah tidak aman.
- Perlu diusulkan standard algoritma baru sebagai pengganti DES.
- National Institute of Standards and Technology (NIST) mengusulkan kepada Pemerintah Federal AS untuk sebuah standard kriptografi kriptografi yang baru.
- NIST mengadakan lomba membuat standard algoritma kriptografi yang baru. Standard tersebut kelak diberi nama Advanced Encryption Standard (AES).
- Pada bulan Oktober 2000, NIST mengumumkan untuk memilih Rijndael (dibaca: Rhine-doll)
- Pada bulan November 2001, Rijndael ditetapkan sebagai AES
- Diharapkan Rijndael menjadi standard kriptografi yang dominan paling sedikit selama 10 tahun.
- Tidak seperti DES yang berorientasi bit, *Rijndael* beroperasi dalam orientasi byte.
- Setiap putaran menggunakan kunci internal yang berbeda (disebut *round key*).
- *Enciphering* melibatkan operasi substitusi dan permutasi.
- Karena AES menetapkan panjang kunci adalah 128, 192, dan 256, maka dikenal AES-128, AES-192, dan AES-256

	Panjang Kunci (Nk words)	Ukuran Blok (Nb words)	Jumlah Putaran (Nr)
AES-128	4	4	10
AES-192	6	4	12
AES-256	8	4	14

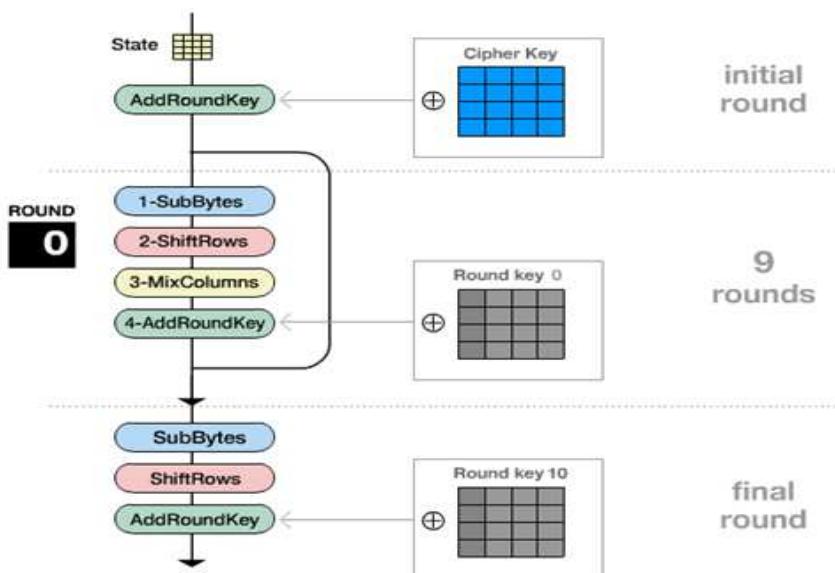
Catatan: 1 word = 32 bit

Garis besar Algoritma *Rijndael* yang beroperasi pada blok 128-bit dengan kunci 128-bit adalah sebagai berikut (di luar proses pembangkitan *round key*):

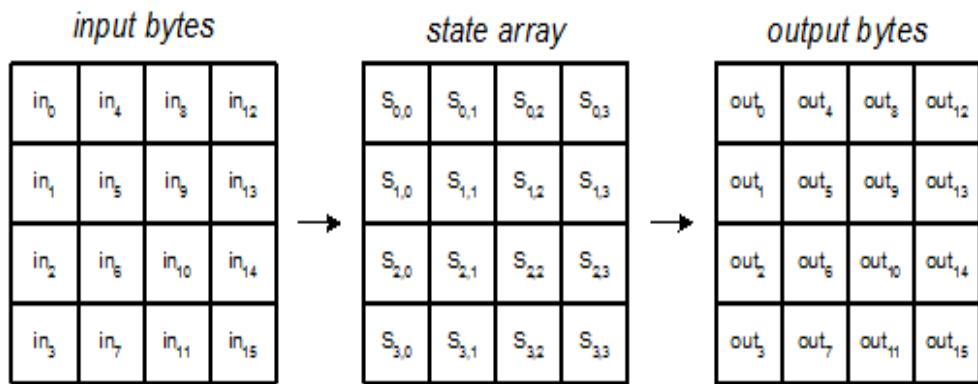
- *AddRoundKey*: melakukan XOR antara *state* awal (plainteks) dengan *cipher key*. Tahap ini disebut juga *initial round*.
- Putaran sebanyak $Nr - 1$ kali. Proses yang dilakukan pada setiap putaran adalah:
 - *SubBytes*: substitusi *byte* dengan menggunakan tabel substitusi (*S-box*).
 - *ShiftRows*: pergeseran baris-baris *array state* secara *wrapping*.
 - *MixColumns*: mengacak data di masing-masing kolom *array state*.
 - *AddRoundKey*: melakukan XOR antara *state* sekarang *round key*.

Final round: proses untuk putaran terakhir:

- *SubBytes*
- *ShiftRows*
- *AddRoundKey*



- Selama kalkulasi plainteks menjadi cipherteks, status sekarang dari data disimpan di dalam *array of bytes* dua dimensi, *state*, yang berukuran $\text{NROWS} \times \text{NCOLS}$.
- Untuk blok data 128-bit, ukuran *state* adalah 4×4 .
- Elemen *array state* diacu sebagai $S[r,c]$, $0 \leq r < 4$ dan $0 \leq c < Nb$ (Nb adalah panjang blok dibagi 32).
- Pada AES-128, $Nb = 128/32 = 4$



Contoh: (elemen state dan kunci dalam notasi HEX)

Input							
State				Cipher Key			
32 88 31 e0				2b 28 ab 09			
43	5a	31	37	7e	ae	f7	cf
f6	30	98	07	15	d2	15	4f
a8	8d	a2	34	16	a6	88	3c

hexadecimal notation:

Ex: 32 = $\underbrace{0011}_{3\text{hex}} \underbrace{0010}_{2\text{hex}}$ (1 byte)

ALGORITMA ASIMETRI

RSA

- ❖ Ditemukan oleh tiga orang yaitu Ron Rivest, Adi Shamir, dan Leonard Adleman yang kemudian disingkat menjadi RSA.
- ❖ Termasuk algoritma asimetri karena mempunyai dua kunci, yaitu kunci publik dan kunci privat.
- ❖ Algoritma kunci-publik yang paling terkenal dan paling banyak aplikasinya.
- ❖ Ditemukan oleh tiga peneliti dari MIT (Massachusetts Institute of Technology), yaitu Ron Rivest, Adi Shamir, dan Len Adleman, pada tahun 1976.
- ❖ Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima.

Pembangkitan pasangan kunci

1. Pilih dua bilangan prima, a dan b (rahasia)
2. Hitung $n = a \cdot b$. Besaran n tidak perlu dirahasiakan.

3. Hitung $\phi(n) = (a - 1)(b - 1)$.
4. Pilih sebuah bilangan bulat untuk kunci publik, sebut namanya e , yang relatif prima terhadap $\phi(n)$.
5. Hitung kunci dekripsi, d , melalui $ed \equiv 1 \pmod{m}$ atau $d \equiv e^{-1} \pmod{\phi(n)}$

Hasil dari algoritma di atas:

- Kunci publik adalah pasangan (e, n)
- Kunci privat adalah pasangan (d, n)

Catatan: n tidak bersifat rahasia, namun ia diperlukan pada perhitungan enkripsi/dekripsi

Kunci Publik

Misalkan $a = 47$ dan $b = 71$ (keduanya prima), maka dapat dihitung:

$$n = a \times b = 3337$$

$$\phi(n) = (a - 1) \times (b - 1) = 46 \times 70 = 3220.$$

Pilih kunci publik $e = 79$ (yang relatif prima dengan 3220 karena pembagi bersama terbesarnya adalah 1).

Hapus a dan b dan kunci publiknya adalah $n=3337$ dan $e=79$

Kunci Privat

Selanjutnya akan dihitung kunci privat d dengan kekongruenan:

$$e \times d \equiv 1 \pmod{m} \Rightarrow d = \frac{1 + (k \times 3220)}{79}$$

Dengan mencoba nilai-nilai $k = 1, 2, 3, \dots$, diperoleh nilai d yang bulat adalah 1019. Ini adalah kunci privat (untuk dekripsi).

Misalkan plainteks $M = \text{HARIINI}$

atau dalam ASCII: 7265827332737873

Pecah M menjadi blok yang lebih kecil (misal 3 digit):

$m_1 = 726$	$m_4 = 273$
$m_2 = 582$	$m_5 = 787$
$m_3 = 733$	$m_6 = 003$

(Perhatikan, m_i masih terletak di dalam antara 0 sampai $n - 1$)

Enkripsi setiap blok:

$$c_1 = 726^{79} \pmod{3337} = 215$$

$$c_2 = 582^{79} \pmod{3337} = 776, \text{ dst}$$

Chiperteks $C = 215\ 776\ 1743\ 933\ 1731\ 158$.

Dekripsi (menggunakan kunci privat $d = 1019$)

$$m_1 = 215^{1019} \bmod 3337 = 726$$

$$m_2 = 776^{1019} \bmod 3337 = 582 \text{ dst untuk sisi blok lainnya}$$

Plainteks $M = 7265827332737873$ yang dalam ASCII karakternya adalah HARI INI.

Kekuatan dan Keamanan RSA

- ✓ Kekuatan algoritma RSA terletak pada tingkat kesulitan dalam memfaktorkan bilangan non prima menjadi faktor primanya, yang dalam hal ini $n = a \times b$.
- ✓ Sekali n berhasil difaktorkan menjadi a dan b , maka $\phi(n) = (a - 1) \times (b - 1)$ dapat dihitung. Selanjutnya, karena kunci enkripsi e diumumkan (tidak rahasia), maka kunci dekripsi d dapat dihitung dari persamaan $ed \equiv 1 \pmod{n}$.
- ✓ Penemu algoritma RSA menyarankan nilai a dan b panjangnya lebih dari 100 digit. Dengan demikian hasil kali $n = a \times b$ akan berukuran lebih dari 200 digit.
- ✓ Menurut Rivest dan kawan-kawan, usaha untuk mencari faktor bilangan 200 digit membutuhkan waktu komputasi selama 4 miliar tahun! (dengan asumsi bahwa algoritma pemfaktoran yang digunakan adalah algoritma yang tercepat saat ini dan komputer yang dipakai mempunyai kecepatan 1 milidetik).

Algoritma MD5

Hash

- **Hash function atau fungsi hash** adalah suatu cara menciptakan “fingerprint” dari berbagai data masukan. Hash function akan mengganti atau mentranspose-kan data tersebut untuk menciptakan fingerprint, yang biasa disebut hash value.
- *Hash function adalah suatu fungsi yang berguna untuk mengkompresi/memperkecil sebuah string yang panjang menjadi sebuah string yang lebih pendek.*
- fungsi yang menerima masukan string yang panjangnya sembarang kemudian mentransformasikannya menjadi string keluaran yang panjangnya tetap (fixed) dan umumnya berukuran jauh lebih kecil daripada ukuran string semula. Di samping ini merupakan skema fungsi hash di mana ukuran dari masukan sembarang, namun menghasilkan output yang ukurannya tetap.
- Hash value biasanya digambarkan sebagai suatu string pendek yang terdiri atas huruf dan angka yang terlihat random (data biner yang ditulis dalam notasi heksadesimal). Suatu hash function adalah sebuah fungsi matematika, yang mengambil sebuah panjang variabel string input, yang disebut pre-image dan mengkonversikannya ke sebuah string output dengan panjang yang tetap dan biasanya lebih kecil, yang disebut message digest 5.
- Hash function digunakan untuk melakukan fingerprint pada pre-image, yaitu menghasilkan sebuah nilai yang dapat menandai (mewakili) pre-image sesungguhnya.
- Fungsi hash satu arah (one-way hash function) adalah hash function yang bekerja satu arah, yaitu suatu hash function yang dengan mudah dapat menghitung hash value dari

pre-image, tetapi sangat sukar untuk menghitung pre-image dari hash value. Sebuah fungsi hash satu arah, $H(M)$, beroperasi pada suatu pre-image pesan M dengan panjang sembarang, dan mengembalikan nilai hash h yang memiliki panjang tetap.

Persamaan fungsi hash :

$$h = H(M)$$

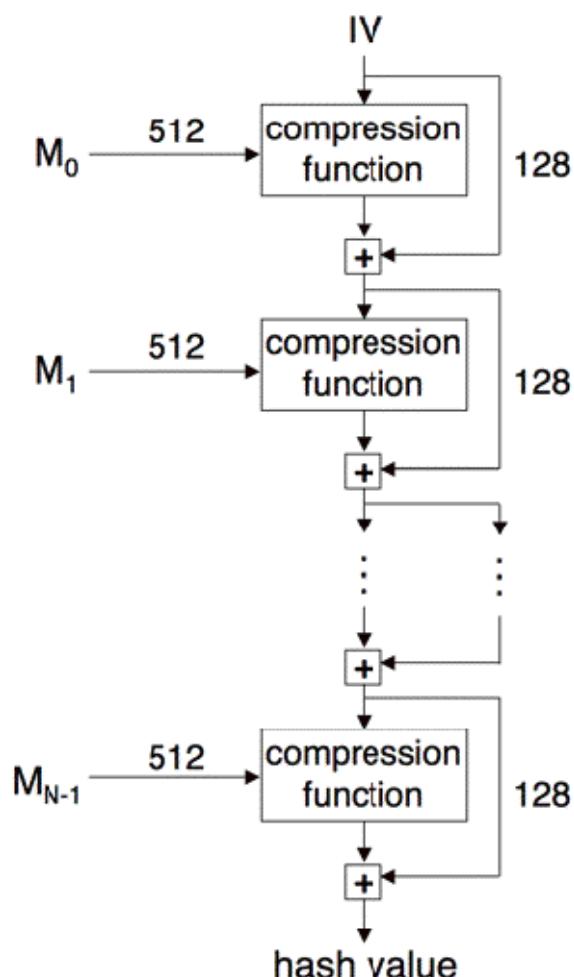
M = pesan ukuran sembarang

h = nilai hash atau pesan singkat (message digest)

$h \ll\ll M$

Fungsi Hash juga memiliki nama-nama lain seperti :

- Fungsi kompresi (compression function);
- Cetak-jari (fingerprint);
- Cryptographic checksum;
- Message Integrity Check (MIC);
- Manipulation Detection Code (MDC).
- Input or “message” blocks M_0, M_1, \dots, M_{N-1}
- Addition is mod 2^{32} per 32-bit word
- This is known as **Merkle-Damgard construction**



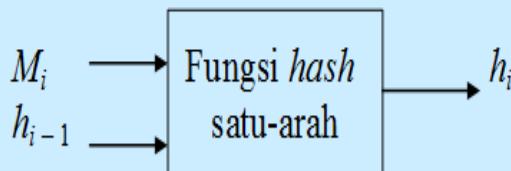
Pada fungsi hash terdapat istilah fungsi hash satu arah (one way function) yang merupakan fungsi hash yang bekerja dalam satu arah. Artinya pesan yang sudah diubah menjadi message digest tidak dapat dikembalikan lagi menjadi pesan semula (irreversible). Ada pun sifat-sifat dari fungsi hash satu arah, yaitu :

1. Fungsi H dapat diterapkan pada blok data berukuran berapa saja.
2. H menghasilkan nilai (h) dengan panjang tetap (fixed length output).
3. $H(x)$ mudah dihitung untuk setiap nilai x yang diberikan.
4. Untuk setiap h yang dihasilkan, tidak mungkin dikembalikan nilai x sedemikian sehingga $H(x)=h$. Itulah sebabnya fungsi H dikatakan fungsi hash satu arah(one way hash function).
5. Untuk setiap x yang diberikan, tidak mungkin mencari y tidak sama dengan x sedemikian sehingga $H(y)=H(x)$.
6. Tidak mungkin mencari pasangan x dan y sedemikian sehingga $H(x)=H(y)$.

Masukan fungsi *hash* adalah blok pesan (M) dan keluaran dari *hashing* blok pesan sebelumnya,

$$h_i = H(M_i, h_{i-1})$$

Skema fungsi *hash* ditunjukkan pada Gambar di bawah:



Gambar Fungsi *hash* satu-arah

Ada banyak fungsi yang mampu menerima input dengan panjang sembarang dan menghasilkan output dengan panjang tetap, tetapi fungsi hash satu arah memiliki karakteristik tambahan yang membuatnya satu arah :

Diberikan M , mudah menghitung h .

Diberikan h , sulit menghitung M agar $H(M) = h$.

Diberikan M , sulit menemukan pesan lain, M' , agar $H(M) = H(M')$.

Dalam dunia nyata, fungsi hash satu arah dikembangkan berdasarkan ide sebuah fungsi kompresi. Fungsi satu arah ini menghasilkan nilai hash berukuran n bila diberikan input berukuran b . Input untuk fungsi kompresi adalah suatu blok pesan dan hasil blok teks sebelumnya.

Sehingga hash suatu blok M , adalah

$h_i = f(M_i, h_{i-1})$ dengan

hi = hash value saat ini.

M_i = blok pesan saat ini.

hi-1 = hash value blok teks sebelumnya.

Fungsi hash sangat berguna untuk menjaga integritas sebuah data. Sudah banyak algoritma hash function yang diciptakan, namun hash function yang umum digunakan saat ini adalah MD5 dan SHA (Secure Hash Algorithm). Algoritma hash function yang baik adalah yang menghasilkan sedikit hash collision.

Hash

Ada pun beberapa fungsi hash satu arah yang pernah dibuat, antara lain :

- MD2(Message Digest2), MD4(Message Digest4), MD5(Message Digest5);
- Secure Hash Function (SHA);
- Snefru;
- N-has;
- RIPE-MD, dan lain sebagainya.

- MD4 (128-bit), sudah tidak dipakai

- **MD5 (128-bit)**

- RIPEMD-160 (160-bit)

- SHA-1 (160-bit)

Algoritma	Ukuran <i>message digest</i> (bit)	Ukuran blok pesan	Kolisi
MD2	128	128	Ya
MD4	128	512	Hampir
MD5	128	512	Ya
RIPEMD	128	512	Ya
RIPEMD-128/256	128/256	512	Tidak
RIPEMD-160/320	160/320	512	Tidak
SHA-0	160	512	Ya
SHA-1	160	512	Ada cacat
SHA-256/224	256/224	512	Tidak
SHA-512/384	512/384	1024	Tidak
WHIRLPOOL	512	512	Tidak

MD5

- MD5 adalah fungsi hash satu-arah yang dibuat oleh Ron Rivest.
- MD5 merupakan perbaikan dari MD4 setelah MD4 berhasil diserang oleh kriptanalisis.
- Algoritma MD5 menerima masukan berupa pesan dengan ukuran sembarang dan menghasilkan message digest yang panjangnya 128 bit.
- Dengan panjang message digest 128 bit, maka secara brute force dibutuhkan percobaan sebanyak 2¹²⁸ kali untuk menemukan dua buah pesan atau lebih yang mempunyai message digest yang sama.

Ada pun manfaat dari fungsi hash satu arah, antara lain :

1. Menjaga integritas data

Fungsi hash sangat peka terhadap perubahan 1 bit pada pesan. Pesan berubah 1 bit maka nilai hash berubah sangat signifikan.

2. Menghemat waktu pengiriman

Misalnya untuk memverifikasi sebuah salinan arsip dengan arsip asli. Di sini salinan dokumen berada di tempat yang jauh dari basis data arsip asli. Daripada mengirim salinan arsip tersebut secara keseluruhan ke komputer pusat (yang membutuhkan waktu transmisi lama), lebih baik mengirimkan message digestnya. Jika message digest salinan arsip sama dengan message digest arsip asli, berarti salinan arsip tersebut sama dengan arsip master.

3. Menormalkan panjang data yang beraneka ragam

Misalnya password yang panjangnya bebas (minimal 8 karakter). kemudian password disimpan di komputer host (server) untuk keperluan otentikasi pemakai komputer. Untuk menyeragamkan panjang field password di dalam basis data, password disimpan dalam bentuk nilai hash (panjang nilai hash tetap).

Kekurangan:

1. Memiliki kemungkinan untuk terjadi bantuan. Hal ini tidak dapat dihindari untuk semua fungsi hash, namun ada beberapa fungsi hash dibuat khusus untuk menghindari terjadinya bantuan.
2. Fungsi hash adalah fungsi satu arah, jadi jika kita hanya mendapat sebuah nilai hash, kita tidak bisa mengembalikannya menjadi data yang asli. Hal ini dipersulit dengan kemungkinan terjadinya bantuan.
3. Tingkat keamanan suatu fungsi hash dinilai berdasarkan jumlah kemungkinan nilai hash, yaitu 2^n , dengan n adalah panjang nilai hash dalam bit. Jadi semakin panjang nilai hash semakin aman.

MD5 (Algoritma)

- Penambahan Bit-bit Pengganjal
 - Pesan ditambah dengan sejumlah bit pengganjal sedemikian sehingga panjang pesan (dalam satuan bit) kongruen dengan 448 modulo 512.
 - Jika panjang pesan 448 bit, maka pesan tersebut ditambah dengan 512 bit menjadi 960 bit. Jadi, panjang bit-bit pengganjal adalah antara 1 sampai 512.
 - Bit-bit pengganjal terdiri dari sebuah bit 1 diikuti dengan sisanya bit 0

Penambahan Nilai Panjang Pesan

Pesan yang telah diberi bit-bit pengganjal selanjutnya ditambah lagi dengan 64 bit yang menyatakan panjang pesan semula.

Jika panjang pesan $> 2^{64}$ maka yang diambil adalah panjangnya dalam modulo 2^{64} . Dengan kata lain, jika panjang pesan semula adalah K bit, maka 64 bit yang ditambahkan menyatakan K modulo 2^{64} .

Setelah ditambah dengan 64 bit, panjang pesan sekarang menjadi kelipatan 512 bit

- Inisialisasi Penyangga MD
 - *MD5* membutuhkan 4 buah penyangga (*buffer*) yang masing-masing panjangnya 32 bit. Total panjang penyangga adalah $4 \times 32 = 128$ bit. Keempat penyangga ini menampung hasil antara dan hasil akhir.
 - Keempat penyangga ini diberi nama A, B, C, dan D. Setiap penyangga diinisialisasi dengan nilai-nilai (dalam notasi HEX) sebagai berikut:

$$A = 01234567$$

$$B = 89ABCDEF$$

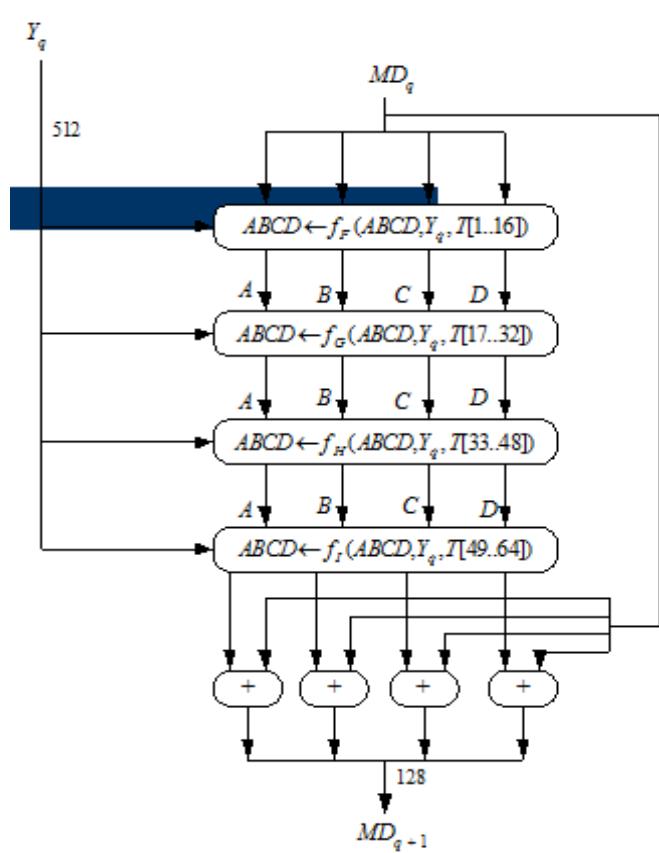
$$C = FEDCBA98$$

$$D = 76543210$$

Pengolahan Pesan dalam Blok Berukuran 512 bit

Pesan dibagi menjadi L buah blok yang masing-masing panjangnya 512 bit (Y_0 sampai Y_{L-1}).

Setiap blok 512-bit diproses bersama dengan penyangga *MD* menjadi keluaran 128-bit, dan ini disebut proses H_{MD5}



- Y_q : blok 512-bit ke-q dari pesan + bit-bit pengganjal + 64 bit nilai panjang pesan semula
- Fungsi-fungsi f_F , f_G , f_H , dan f_I masing-masing berisi 16 kali operasi dasar terhadap masukan, setiap operasi dasar menggunakan elemen Tabel T

Tabel 1. Fungsi-fungsi dasar MD5

Nama	Notasi	$g(b, c, d)$
f_F	$F(b, c, d)$	$(b \wedge c) \vee (\neg b \wedge d)$
f_G	$G(b, c, d)$	$(b \wedge d) \vee (c \wedge \neg d)$
f_H	$H(b, c, d)$	$b \oplus c \oplus d$
f_I	$I(b, c, d)$	$c \oplus (b \wedge \neg d)$

Catatan: operator logika AND, OR, NOT, XOR masing-masing dilambangkan dengan \wedge , \vee , \sim , \oplus

Tabel 2. Nilai $T[i]$

$T[1] = D76AA478$	$T[17] = F61E2562$	$T[33] = FFFA3942$	$T[49] = F4292244$
$T[2] = E8C7B756$	$T[18] = C040B340$	$T[34] = 8771F681$	$T[50] = 432AFF97$
$T[3] = 242070DB$	$T[19] = 265E5A51$	$T[35] = 69D96122$	$T[51] = AB9423A7$
$T[4] = C1BDCEEE$	$T[20] = E9B6C7AA$	$T[36] = FDE5380C$	$T[52] = FC93A039$
$T[5] = F57C0FAF$	$T[21] = D62F105D$	$T[37] = A4BEEA44$	$T[53] = 655B59C3$
$T[6] = 4787C62A$	$T[22] = 02441453$	$T[38] = 4BDECFA9$	$T[54] = 8F0CC92$
$T[7] = A8304613$	$T[23] = D8A1E681$	$T[39] = F6BB4B60$	$T[55] = FFEFF47D$
$T[8] = FD469501$	$T[24] = E7D3FBBC$	$T[40] = BEBFBC70$	$T[56] = 85845DD1$
$T[9] = 698098D8$	$T[25] = 21E1CDE6$	$T[41] = 289B7EC6$	$T[57] = 6FA87E4F$
$T[10] = 8B44F7AF$	$T[26] = C33707D6$	$T[42] = EAA127FA$	$T[58] = FE2CE6E0$
$T[11] = FFFF5BB1$	$T[27] = F4D50D87$	$T[43] = D4EF3085$	$T[59] = A3014314$
$T[12] = 895CD7BE$	$T[28] = 455A14ED$	$T[44] = 04881D05$	$T[60] = 4E0811A1$
$T[13] = 6B901122$	$T[29] = A9E3E905$	$T[45] = D9D4D039$	$T[61] = F7537E82$
$T[14] = FD987193$	$T[30] = FCEFA3F8$	$T[46] = E6DB99E5$	$T[62] = BD3AF235$
$T[15] = A679438E$	$T[31] = 676F02D9$	$T[47] = 1FA27CF8$	$T[63] = 2AD7D2BB$
$T[16] = 49B40821$	$T[32] = 8D2A4C8A$	$T[48] = C4AC5665$	$T[64] = EB86D391$

Putaran 2 : 16 kali operasi dasar dengan $g(b,c,d) = G(b,c,d)$

Tabel 4. Rincian operasi pada fungsi $G(b, c, d)$

No .	[abcd k s i]
1	[ABCD 1 5 17]
2	[DABC 6 9 18]
3	[CDAB 11 14 19]
4	[BCDA 0 20 20]
5	[ABCD 5 5 21]
6	[DABC 10 9 22]
7	[CDAB 15 14 23]
8	[BCDA 4 20 24]
9	[ABCD 9 5 25]
10	[DABC 14 9 26]
11	[CDAB 3 14 27]
12	[BCDA 8 20 28]
13	[ABCD 13 5 29]
14	[DABC 2 9 30]
15	[CDAB 7 14 31]
16	[BCDA 12 20 32]

Putaran 3 : 16 kali operasi dasar dengan $g(b,c,d) = H(b,c,d)$

Tabel 5. Rincian operasi pada fungsi $H(b, c, d)$

No .	[abcd k s i]
1	[ABCD 5 4 33]
2	[DABC 8 11 34]
3	[CDAB 11 16 35]
4	[BCDA 14 23 36]
5	[ABCD 1 4 37]
6	[DABC 4 11 38]
7	[CDAB 7 16 39]
8	[BCDA 10 23 40]
9	[ABCD 13 4 41]
10	[DABC 0 11 42]
11	[CDAB 3 16 43]
12	[BCDA 6 23 44]
13	[ABCD 9 4 45]
14	[DABC 12 11 46]
15	[CDAB 15 16 47]
16	[BCDA 2 23 48]

Putaran 4 : 16 kali operasi dasar dengan $g(b,c,d) = I(b,c,d)$

Tabel 6. Rincian operasi pada fungsi $I(b, c, d)$

No .	[abcd k s i]
1	[ABCD 0 6 49]
2	[DABC 7 10 50]
3	[CDAB 14 15 51]
4	[BCDA 5 21 52]
5	[ABCD 12 6 53]
6	[DABC 3 10 54]
7	[CDAB 10 15 55]
8	[BCDA 1 21 56]
9	[ABCD 8 6 57]
10	[DABC 15 10 58]
11	[CDAB 6 15 59]
12	[BCDA 13 21 60]
13	[ABCD 4 6 61]
14	[DABC 11 10 62]
15	[CDAB 2 15 63]
16	[BCDA 9 21 64]

- Setelah putaran keempat, a , b , c , dan d ditambahkan ke A , B , C , dan D , dan selanjutnya algoritma memproses untuk blok data berikutnya (Y_{q+1}).
- Keluaran akhir dari algoritma $MD5$ adalah hasil penyambungan bit-bit di A , B , C , dan D .

- <http://jo-ardianto.blogspot.co.id/2012/05/pengertian-kriptografi.html>
- <https://stsn6.wordpress.com/2009/10/15/konsep-fungsi-hash-function-pada-aplikasi-kriptografi/>
- <http://sharingilmu.web.id/317/>
- <http://informatika.stei.itb.ac.id/~rinaldi.munir/Matdis/2006-2007/Makalah/Makalah0607-42.pdf>
- web2.utc.edu/~Li-Yang/cpsc4600/06-UTC-authentication.ppt
- http://www.academia.edu/1528069/Keamanan_Komputer
- docplayer.info/97100-Fungsi-hash-bahan-kuliah-if3058-criptografi..
- armastuti.staff.gunadarma.ac.id/Downloads/files/25754/Algoritma+Kriptografi.ppt
- [https://yenikustiyahningsih.files.wordpress.com/.../4algoritma-criptografi-modern.ppt](http://yenikustiyahningsih.files.wordpress.com/.../4algoritma-criptografi-modern.ppt)
- elearning.upnjatim.ac.id/courses/ISI3118/work/53a3ada7c0208slide_14.ppt



MODUL PERKULIAHAN

Keamanan Jaringan

Steganografi LSB, Watermarking
Audio, Watermark

Fakultas Fasilkom	Program Studi Teknik Informatika	TatapMuka 13	Kode MK MK:15020	Di susun Oleh Tim Dosen
----------------------	-------------------------------------	------------------------	---------------------	----------------------------

Abstract

Keamanan jaringan ([Bahasa Inggris: Network Security](#)) dalam [jaringan komputer](#) sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah.

Kompetensi

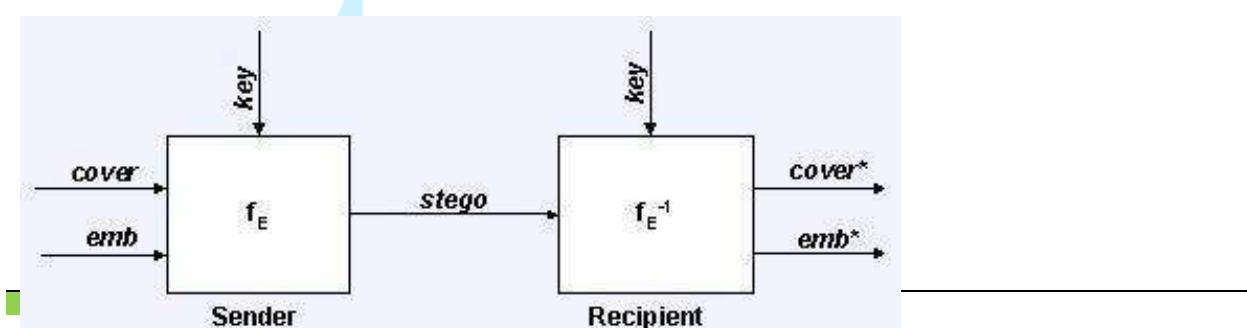
Setelah membaca modul ini diharapkan mahasiswa :

- Memahami konsep dasar peningkatan keamanan jaringan
- Mampu menjelaskan teknik keamanan jaringan secara umum, Steganografi.

Steganography

- **Steganography** adalah seni dan ilmu untuk menyembunyikan pesan didalam pesan lainnya dengan sedemikian rupa sehingga orang lain yang melihatnya tidak menyadari bahwa ada suatu pesan rahasia didalam teks tersebut.
- kata steganography itu sendiri berasal dari bahasa yunani *steganos* yang artinya "tersembunyi/terselubung" sedangkan *graphien* artinya " menulis " sehingga dapat disimpulkan bahwa *steganography* artinya tulisan yang tersembunyi.
 - Tujuan dari steganography adalah merahasiakan atau menyembunyikan keberadaan dari sebuah pesan tersembunyi atau sebuah informasi.
 - Kelebihan steganography jika dibandingkan dengan cryptography adalah pesan-pesannya tidak menarik perhatian orang lain. Pesan-pesan berkode dalam crytography yang tidak disembunyikan, walaupun tidak dapat dipecahkan, akan menimbulkan kecurigaan. Seringkali, steganography dan crptography digunakan secara bersamaan untuk menjamin keamanan pesan rahasianya.
- Dalam praktiknya, kebanyakan pesan disembunyikan dengan membuat perubahan tipis terhadap data digital lain yang isinya tidak akan menarik perhatian dari penyerang potensial, sebagai contoh sebuah gambar yang terlihat tidak berbahaya. Perubahan ini bergantung pada kunci (sama pada kriptografi) dan pesan untuk disembunyikan. Orang yang menerima gambar kemudian dapat menyimpulkan informasi terselubung dengan cara mengganti kunci yang benar ke dalam algoritma yang digunakan.
- Pada metode steganografi cara ini sangat berguna jika digunakan pada cara steganografi komputer karena banyak format berkas digital yang dapat dijadikan media untuk menyembunyikan pesan. Format yang biasa digunakan di antaranya:
 - Format *image* : bitmap (bmp), gif, pcx, jpeg, dll.
 - Format *audio* : wav, voc, mp3, dll.
 - Format lain : teks file, html, pdf, dll.

Gambaran Sistem



Gambar. menunjukkan sebuah sistem steganography umum dimana di bagian pengirim pesan (**sender**), dilakukan proses embedding (**fe**) pesan yang hendak dikirim secara rahasia (**emb**) ke dalam data cover sebagai tempat meyimpannya (**cover**), dengan menggunakan kunci tertentu (**key**), sehingga dihasilkan data dengan pesan tersembunyi di dalamnya (**stego**). Di bagian penerima pesan (**recipient**), dilakukan proses extracting (**fe-1**) pada stego untuk memisahkan pesan rahasia (**emb**) dan data penyimpan (**cover**) tadi dengan menggunakan kunci yang sama seperti pada proses embedding tadi. Jadi hanya orang yang tahu kunci ini saja yang dapat mengekstrak pesan rahasia tadi.

Ada 4 metode dalam steganography diantaranya :

1. Least Significant Bit Insertion (LSBI)
2. Algorithms and Transformation
3. Redundant Pattern Encoding
4. Spread Spectrum Method

Least Significant Bit Insertion (LSBI)

- Dengan cara memanipulasi LSB dari suatu image.
- Untuk image dengan 24 bit color dapat digunakan 3 bit per pixel untuk dimanipulasi, untuk 8 bit color hanya 1 bit per pixel saja yang dapat dimanipulasi.
- Jika Stego dilakukan kompresi, maka harus menggunakan Lossless Compression supaya data tidak hilang.
- Berfungsi sangat baik ketika image yang digunakan dalam format grayscale karena perubahannya akan sulit dideteksi oleh mata.
- Contohnya, pada berkas image pesan dapat disembunyikan dengan menggunakan cara menyisipkannya pada bit rendah atau bit yang paling kanan (LSB) pada data pixel yang menyusun file tersebut. Pada berkas bitmap 24 bit, setiap pixel (titik) pada gambar tersebut terdiri dari susunan tiga warna merah, hijau dan biru (RGB) yang masing-masing disusun oleh bilangan 8 bit (byte) dari 0 sampai 255 atau dengan format biner 00000000 sampai 11111111. Dengan demikian, pada setiap pixel berkas bitmap 24 bit kita dapat menyisipkan 3 bit data

Least Significant Bit Insertion (LSBI)

- Kekurangan dari LSB Insertion: Dapat diambil kesimpulan dari contoh 8 bit pixel, menggunakan LSB Insertion dapat secara drastis mengubah unsur pokok warna dari pixel. Ini dapat menunjukkan perbedaan yang nyata dari *cover image* menjadi *stego image*, sehingga tanda tersebut menunjukkan keadaan dari steganografi. Variasi warna kurang jelas dengan 24 bit image, bagaimanapun file tersebut sangatlah besar. Antara 8 bit dan 24 bit *image* mudah diserang dalam pemrosesan *image*, seperti *cropping*

(kegagalan) dan *compression* (pemampatan).

- Keuntungan dari LSB Insertion : Keuntungan yang paling besar dari algoritma LSB ini adalah cepat dan mudah. Dan juga algoritma tersebut memiliki *software* steganografi yang mendukung dengan bekerja di antara unsur pokok warna LSB melalui manipulasi *palette* (lukisan).

Algorithms and Transformation

Algoritma *compression* adalah metode steganografi dengan menyembunyikan data dalam fungsi matematika.

Dua fungsi tersebut adalah *Discrete Cosine Transformation* (DCT) dan *Wavelet Transformation*.

Fungsi DCT dan Wavelet yaitu mentransformasi data dari satu tempat (domain) ke tempat (domain) yang lain.

Fungsi DCT yaitu mentransformasi data dari tempat spatial (*spatial domain*) ke tempat frekuensi (*frequency domain*).

Redundant Pattern Encoding

Redundant Pattern Encoding adalah menggambar pesan kecil pada kebanyakan gambar.

Keuntungan dari metode ini adalah dapat bertahan dari *cropping* (kegagalan). Kerugiannya yaitu tidak dapat menggambar pesan yang lebih besar.

Spread Spectrum method

Spread Spectrum steganografi terpencar-pencar sebagai pesan yang diacak (*encrypted*) melalui gambar (tidak seperti dalam LSB).

Untuk membaca suatu pesan, penerima memerlukan algoritma yaitu *crypto-key* dan *stego-key*.

Metode ini juga masih mudah diserang yaitu penghancuran atau pengrusakan dari kompresi dan proses *image*.

Steganalisis dan Stegosystem

- Seperti Kriptografi dan Kriptanalisis, Steganalisis didefinisikan sebagai suatu seni dan ilmu dalam mendeteksi informasi tersembunyi. Sebagai tujuan dari steganografi adalah untuk merahasiakan keberadaan dari sebuah pesan rahasia, satu keberhasilan penyerangan pada sebuah sistem steganografi terdiri dari pendekripsi bahwa sebuah berkas yang diyakini berisikan data terselubung. Seperti dalam Kriptanalisis, diasumsikan bahwa sistem steganografi telah diketahui oleh si penyerang. Maka dari itu, keamanan dari sistem steganografi bergantung hanya pada fakta bahwa kunci rahasia tidak diketahui oleh si penyerang.
- *Stegosystem* di sini berisi tentang penyerangan-penyerangan yang dilakukan terhadap suatu sistem steganografi, sebuah perbedaan penting harus dibuat di antara penyerangan-penyerangan pasif di mana penyerang hanya dapat memotong data, dan penyerangan-penyerangan aktif di mana penyerang juga dapat memanipulasi data.

Penyerangan-penyerangan berikut memungkinkan dalam model dari stegosistem ini:

- *Stego-Only-Attack* (Penyerangan hanya Stego). Penyerang telah menghalangi stego data dan dapat menganalisisnya.
- *Stego-Attack* (Penyerangan Stego). Pengirim telah menggunakan *cover* yang sama berulangkali untuk data terselubung. Penyerang memiliki berkas stego yang berasal dari *cover file* yang sama. Dalam setiap berkas stego tersebut, sebuah pesan berbeda disembunyikan.
- *Cover-Stego-Attack* (Penyerangan selubung Stego). Penyerang telah menghalangi berkas stego dan mengetahui *cover file* mana yang digunakan untuk menghasilkan berkas stego ini. Ini menyediakan sebuah keuntungan melalui penyerangan *stego-only* untuk si penyerang.
- *Manipulating the stego data* (Memanipulasi data stego). Penyerang memiliki kemampuan untuk memanipulasi data stego. Jika penyerang hanya ingin menentukan sebuah pesan disembunyikan dalam berkas stego ini, biasanya ini tidak memberikan sebuah keuntungan, tapi memiliki kemampuan dalam memanipulasi data stego yang berarti bahwa si penyerang mampu memindahkan pesan rahasia dalam data stego (jika ada).
- *Manipulating the cover data* (Memanipulasi data terselubung). Penyerang dapat memanipulasi data terselubung dan menghalangi hasil data stego. Ini dapat membuat tugas dalam menentukan apakah data stego berisikan sebuah pesan rahasia lebih mudah bagi si penyerang.

Penggunaan:

- Digunakan untuk informasi penjelasan yang menyertai sebuah gambar (seperti catatan dokter yang menyertai sebuah X-ray)
- Menanamkan data yang dapat memperbaiki audio atau image pada kerusakan yang terjadi dari koneksi atau transmisi yang jelek.
- Komunikasi private peer-to-peer
- Mengirimkan komunikasi rahasia pada web untuk menghindari penyebaran
- Perlindungan hak cipta
- Menyembunyikan data pada jaringan untuk menghindari pelanggaran.

Contoh:

- **Dari Iringan Air Mata**
- **Jiwa Nona Gadis Anak Nirwana**
- **Bicara Ingin Cinta Andai Rasanya Ada**
 - Mudah sekali kan menebak pesan tersembunyi diatas, caranya adalah dengan mengambil huruf pertama pada teks diatas. Dan pesan tersembunyi tersebut adalah “ **DIAM JANGAN BICARA**

Watermarking

Salah satu karya intelektual yang dilindungi adalah barang dalam bentuk digital, seperti

software dan produk multimedia seperti teks, musik (dalam format MP3 atau WAV), gambar/citra (*image*), dan video digital (VCD). Selama ini penggandaan atas produk digital tersebut dilakukan secara bebas dan leluasa. Pemegang hak cipta atas produk digital tersebut tentu dirugikan karena ia tidak mendapat royalti dari usaha penggandaan tersebut.

Salah satu cara untuk melindungi hak cipta multimedia (gambar/foto, suara, teks, video) adalah dengan menyisipkan informasi ke dalam data multimedia tersebut dengan teknik *watermarking*. Informasi yang disisipkan ke dalam data multimedia disebut *watermark*, dan *watermark* dapat dianggap sebagai **sidik digital** (*digital signature*) atau stempel digital dari pemilik yang sah atas produk multimedia tersebut.

Pada dasarnya, teknik *watermarking* adalah proses menambahkan kode identifikasi secara permanen ke dalam data digital.

Kode identifikasi tersebut dapat berupa teks, gambar, suara, atau video. Selain tidak merusak data digital produk yang akan dilindungi, kode yang disisipkan seharusnya memiliki ketahanan (*robustness*) dari berbagai pemrosesan lanjutan seperti pengubahan, transformasi geometri, kompresi, enkripsi, dan sebagainya.

Sifat *robustness* berarti data *watermark* tidak terhapus akibat pemrosesan lanjutan tersebut



<http://www.mediafire.com/download/lqjyxokkm2d/Steganografi+dan+Watermarking.doc>

Gambar memperlihatkan sebuah gambar (*image*) paprika yang disisipi dengan *watermark* berupa gambar hitam putih yang menyatakan identifikasi pemiliknya (Shanty). Perhatikanlah bahwa setelah disisipi *watermark*, gambar paprika tetap kelihatan mulus, seolah-olah tidak pernah disisipi *watermark* sebelumnya. Sebenarnya tidaklah demikian, gambar paprika tersebut mengalami *sedikit* perubahan akibat *watermarking*, namun mata manusia mempunyai sifat kurang peka terhadap perubahan kecil ini, sehingga manusia sukar membedakan mana gambar yang asli dan mana gambar yang sudah disisipi *watermark*.

Sejarah

Watermarking sudah ada sejak 700 tahun yang lalu. Pada akhir abad 13, pabrik kertas di Fabriano, Italia, membuat kertas yang diberi *watermark* atau tanda-air dengan cara menekan

bentuk cetakan gambar atau tulisan pada kertas yang baru setengah jadi. Ketika kertas dikeringkan terbentuklah suatu kertas yang ber-watermark. Kertas ini biasanya digunakan oleh seniman atau sastrawan untuk menulis karya mereka. Kertas yang sudah dibubuh tanda-air tersebut sekalius dijadikan identifikasi bahwa karya seni di atasnya adalah milik mereka.

Ide *watermarking* pada data digital (sehingga disebut *digital watermarking*) dikembangkan di Jepang tahun 1990 dan di Swiss tahun 1993. *Digital watermarking* semakin berkembang seiring dengan semakin meluasnya penggunaan internet, objek digital seperti video, citra, dan suara yang dapat dengan mudah digandakan dan disebarluaskan.

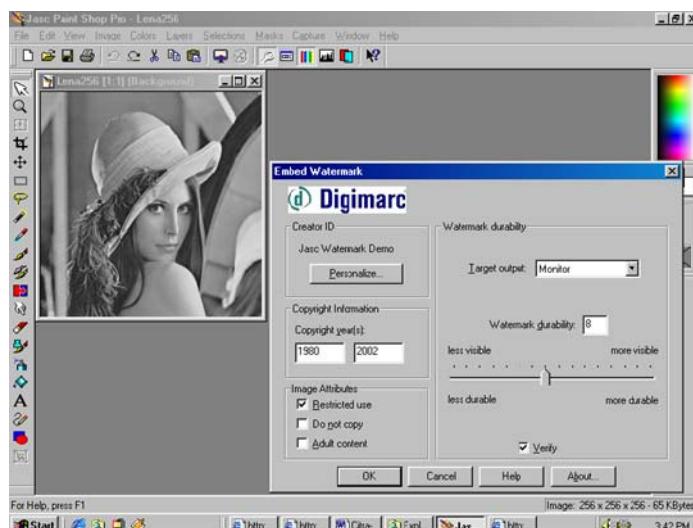
Perbedaan Steganografi dengan *Watermarking*

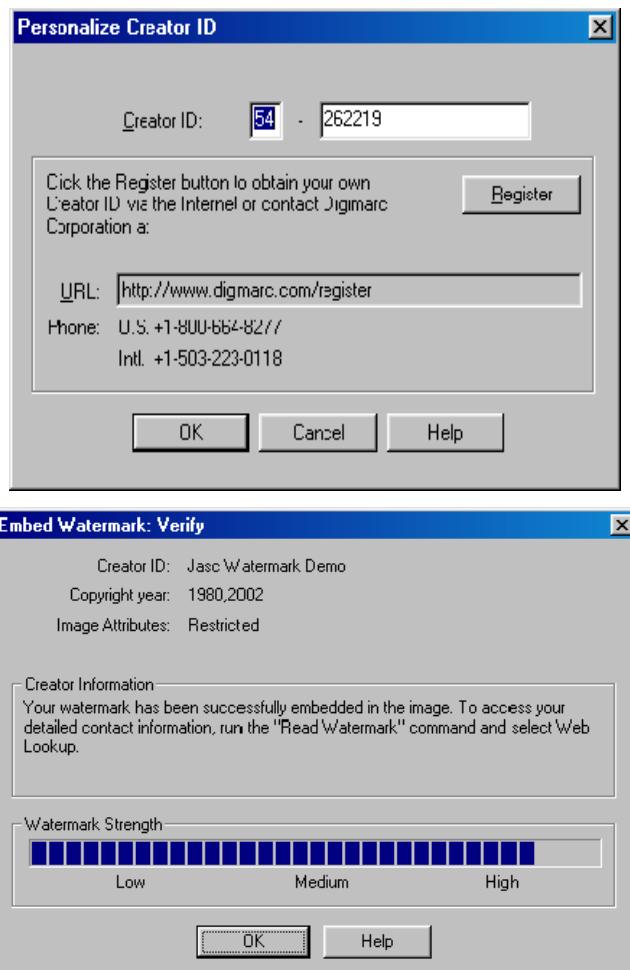
- *Watermarking* merupakan aplikasi dari steganografi, namun ada perbedaan antara keduanya. Jika pada steganografi informasi rahasia disembunyikan di dalam media digital dimana media penampung tidak berarti apa-apanya, maka pada *watermarking* justru media digital tersebut yang akan dilindungi kepemilikannya dengan pemberian label hak cipta (*watermark*).

Meskipun steganografi dan *watermarking* tidak sama, namun secara prinsip proses penyisipan informasi ke dalam data digital tidak jauh berbeda.

Implementasi

Menu *watermark* pada program **Paintshop Pro. 6**:





Audio Watermark

Terdapat beberapa metode watermarking untuk file audio (atau metode steganografi audio). Masing-masing memiliki kelebihan dan kekurangannya sendiri, terutama dalam segi pengaruh kualitas audio, robustness , dan kapasitas payload dalam penyisipan.

Metode:

A. Metode Modifikasi LSB

Algoritma watermarking ini menyisipkan watermark

dalam data sample audio dengan cara mengganti nilai bit terakhirnya (least significant bits, LSB). Algoritma ini bekerja dalam domain spasial (atau waktu dalam audio).

Algoritma ini memiliki tiga parameter, yaitu:

1. Kunci rahasia

k, sebagai umpan untuk pembangkit bilangan acak semu (PRNG) dalam urutan pemilihan sample.

2.Kode koreksi galat (ECC) c, jika digunakan panjang pesan yang disisipkan dilipatgandakan dan galat selama pemrosesan dapat dideteksi dan dikoreksi pada ambang tertentu.

3.Parameter m

untuk menentukan pesan rahasia dan menyisipkannya dalam sinyal audio.

B. Metode Spread Spectrum

Algoritma watermarking ini mentransformasikan sinyal audio terlebih dahulu ke dalam domain frekuensi menggunakan transformasi Fourier. Watermark disisipkan ke dalam koefisien-koefisien frekuensi.

Algoritma ini memiliki tiga parameter, yaitu:

1. Parameter m

untuk menyisipkan pesan rahasia dalam sinyal audio.

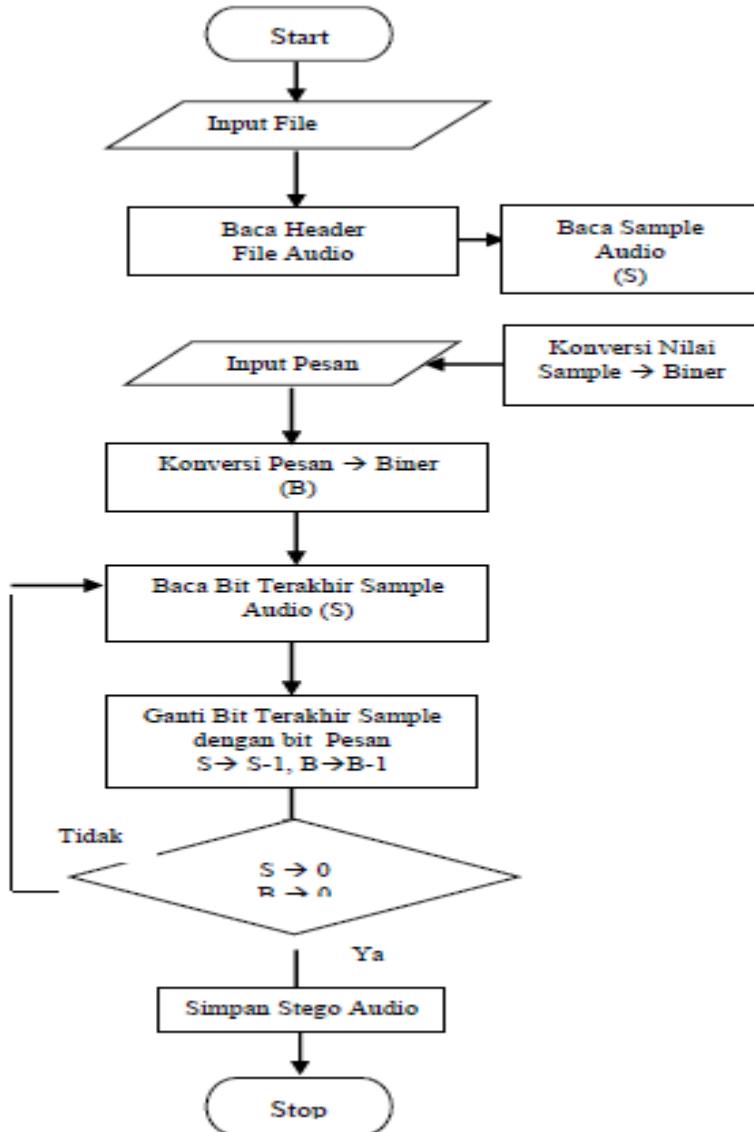
2. Kunci rahasia k

, sebagai umpan untuk pembangkit bilangan acak semu (PRNG) dalam urutan pemilihan sample.

3. Parameter l dan h

menentukan bandwidth dengan memilih batas frekuensi bawah (l) dan atas (h) untuk penyisipan. Kedua parameter tersebut menunjukkan rentang frekuensi.

Flowchart Sistem:



Percobaan & Hasil:

Pada percobaan ini digunakan sebuah file audio dengan ukuran 568272 bytes dan sebuah pesan watermark dengan ukuran 156 bytes yang disisipkan.

A. Metode Modifikasi LSB

Pada file audio tersebut, ukuran tiap sample adalah 4 bytes sehingga ukuran maksimum watermark yang dapat disisipkan untuk domain spasial adalah 35513 bytes.

```
Embed message to (1) / extract from audio file? 1
Method: LSH modification (1) / Spread Spectrum (2)? 1
Input file: DooBeDoo.wav
Output file: sda.wav
Message file: prepatch.log

ChunkSize = 568272
Subchunk1Size = 18
AudioFormat = 1
NumChannels = 1
SampleRate = 16000
ByteRate = 32000
BlockAlign = 2
BitsPerSample = 16
FactChunkSize = 4
dwSampleLength = 284111

Subchunk2Size = 568222
Duration = 17.756937 s
Embedding payload size = 35513 bytes
Message file size: 156 bytes
Data embedded.
```

```
Embed message to (1) / extract from audio file? 1
Method: LSH modification (1) / Spread Spectrum (2)? 1
Input file: DooBeDoo.wav
Output file: sda.wav
Message file: prepatch.log

ChunkSize = 568272
Subchunk1Size = 18
AudioFormat = 1
NumChannels = 1
SampleRate = 16000
ByteRate = 32000
BlockAlign = 2
BitsPerSample = 16
FactChunkSize = 4
dwSampleLength = 284111

Subchunk2Size = 568222
Duration = 17.756937 s
Embedding payload size = 35513 bytes
Message file size: 156 bytes
Data embedded.
```

<http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2011-2012/Makalah-2012/Makalah-Kripto-2012-033.pdf>

Kesimpulan:

Penyisipan watermark dengan modifikasi LSB sangat rapuh (fragile) terhadap modifikasi sedikit apapun, sedangkan metode spread spectrum lebih “tahan banting” (robust) terhadap berbagai bentuk modifikasi.

DaftarPustaka

- http://www.academia.edu/6124616/Rinaldi_Munir_IF5054_Kriptografi_1_Bahan_Kuliah_ke-10_IF5054_Kriptografi
- <https://shineofscience.wordpress.com/2013/09/30/kiptografi-sistem-keamanan-komputer/>
- <http://ditonugroh08.blogspot.co.id/2012/09/keamanan-jaringan-komputer-menggunakan.html>
- <https://segi3hijau.wordpress.com/2012/11/01/teknik-steganografi-dengan-metode-lsb/>
- <https://id.wikipedia.org/wiki/Steganografi>
- http://www.academia.edu/5306496/Pengamanan_Pesan_Steganografi_dengan_Metode LSB_Berlapis_Enkripsi_dalam_PHP
- http://www.academia.edu/5306496/Pengamanan_Pesan_Steganografi_dengan_Metode LSB_Berlapis_Enkripsi_dalam_PHP
- <http://apasihbursasahamitu.blogspot.co.id/2010/10/steganografi-dan-contohnya.html>
- <http://www.mediafire.com/download/lqjyxokkm2d/Steganografi+dan+Watermarking.doc>
- <http://guritac-tecnologi4.blogspot.co.id/2010/04/steganografi-dan-watermarking.html>



MODUL PERKULIAHAN

Keamanan

Jaringan

Security management.

Abstract

Keamanan jaringan terutama security management dapat dipelajari sebagai proses pengumpulan dan penilaian bukti – bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien

Kompetensi

Setelah membaca modul ini diharapkan mahasiswa :

- Mengetahui Kontrak Perkuliahuan
- Setelah mengikuti mata kuliah ini diharapkan mahasiswa memiliki kemampuan untuk:
 - Mempelajari security Management utk bisnis besar & menengah.

Pentingnya Manajemen Kontrol Keamanan pada Sistem

- **Tujuan manajemen informasi** adalah untuk melindungi kerahasiaan, integritas dan ketersediaan informasi.
 - Dengan tumbuhnya berbagai penipuan, spionase, virus, dan hackers sudah mengancam informasi bisnis manajemen oleh karena meningkatnya keterbukaan informasi dan lebih sedikit kendali/control yang dilakukan melalui teknologi informasi modern.
 - Sebagai konsekuensinya , meningkatkan harapan dari para manajer bisnis, mitra usaha, auditor, dan stakeholders lainnya menuntut adanya manajemen informasi yang efektif untuk memastikan informasi yang menjamin kesinambungan bisnis dan meminimalkan kerusakan bisnis dengan pencegahan dan meminimalisasi dampak peristiwa keamanan.

Mengapa harus mengamankan informasi?

- Keamanan Informasi adalah suatu upaya untuk mengamankan aset informasi yang dimiliki. Kebanyakan orang mungkin akan bertanya, mengapa “**keamanan informasi**” dan **bukan** “keamanan teknologi informasi” atau IT Security.
- Kedua istilah ini sebenarnya sangat terkait, namun mengacu pada dua hal yang sama sekali berbeda. “Keamanan Teknologi Informasi” atau IT Security mengacu pada usaha-usaha mengamankan infrastruktur teknologi informasi dari gangguan-gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan
- Berbeda dengan “keamanan informasi” yang fokusnya justru pada data dan informasi milik perusahaan.

Pada konsep ini, usaha-usaha yang dilakukan adalah merencanakan, mengembangkan serta mengawasi semua kegiatan yang terkait dengan bagaimana data dan informasi bisnis dapat digunakan serta diutilisasi sesuai dengan fungsinya serta tidak disalahgunakan atau bahkan dibocorkan ke pihak-pihak yang tidak berkepentingan.

Definisi

Etika:

- Ilmu yang membahas perbuatan baik dan perbuatan buruk manusia sejauh yang dapat dipahami oleh pikiran manusia
- Etika adalah studi ttg kehendak manusia, yaitu kehendak yg berhubungan dg keputusan yg benar dan yg salah dalam tindak perbuatannya. *Fagothey (1953)*

Menurut Kamus Besar Bahasa Indonesia, ada 3 pengertian tentang etika, yaitu:

- ❖ Ilmu tentang apa yg baik dan yg buruk, ttg hak dan kewajiban sosial.
- ❖ Kumpulan azas atau nilai yg berkenaan dg akhlak.

- ❖ Nilai mengenai benar dan salah yg dianut masyarakat

Pengertian lain dari Etika dirumuskan oleh Sumaryono (1995), yakni:

Etika adalah studi ttg kebenaran dan ketidak benaran berdasarkan kodrat manusia yg diwujudkan melalui kehendak manusia dlm perbuatannya.

- **Etika komputer** merupakan analisis mengenai sifat dan dampak sosial teknologi komputer, serta formulasi dan justifikasi kebijakan untuk menggunakan teknologi tsb secara etis.
- **Etika komputer** juga bisa di definisikan sebuah frase yang sering digunakan namun sulit untuk didefinisikan.

Untuk menanamkan kebiasaan komputer yang sesuai, etika harus dijadikan kebijakan organisasi etis.

Sejumlah organisasi mengalamatkan isu mengenai etika komputer dan telah menghasilkan guideline etika komputer, kode etik.

Tujuan mempelajari Etika

- Untuk menyamakan persepsi tentang penilaian perbuatan baik dan perbuatan buruk bagi setiap manusia dalam ruang dan waktu tertentu.

Sejarah Etika Komputer

- **Era 1940 – 1950-an**

Diawali dengan penelitian Norbert Wiener (Prof. dari MIT) tentang komputasi pada meriam yang mampu menembak jatuh pesawat yang melintas di atasnya (PD II).

Ramalannya tentang komputasi modern yang pada dasarnya sama dengan system jaringan syaraf yang bisa melahirkan kebaikan sekaligus malapetaka

- **Era 1960-an**

Ungkapan Donn Parker : “*that when people entered the computer center, they left their ethics at the door*”.

Dalam contoh kasus pemrosesan data, spesialis computer bisa mengetahui data apa saja secara cepat.

Pada tahun 1968 memimpin pengembangan kode etik profesional untuk ACM (Association Computing Machinery)

- **Era 1970-an**

Joseph Weizenbaum ilmuan komputer MIT di Boston menciptakan program yang disebut ELIZA dalam eksperimennya melakukan wawancara dengan pasien yang akan diobatinya (otomatisasi psikoterapi)

- **Era 1980-an**

Kemunculan kejahatan computer (virus, unauthorized login, etc).

Pertengahan 80-an James Moor dari Dartmouth college membuat artikel menarik yang berjudul *What is Computer Ethics ?*

Studi berkembang menjadi suatu diskusi serius tentang masalah etika computer. Lahirlah buku "Computer Ethics" (Johnson, 1985).

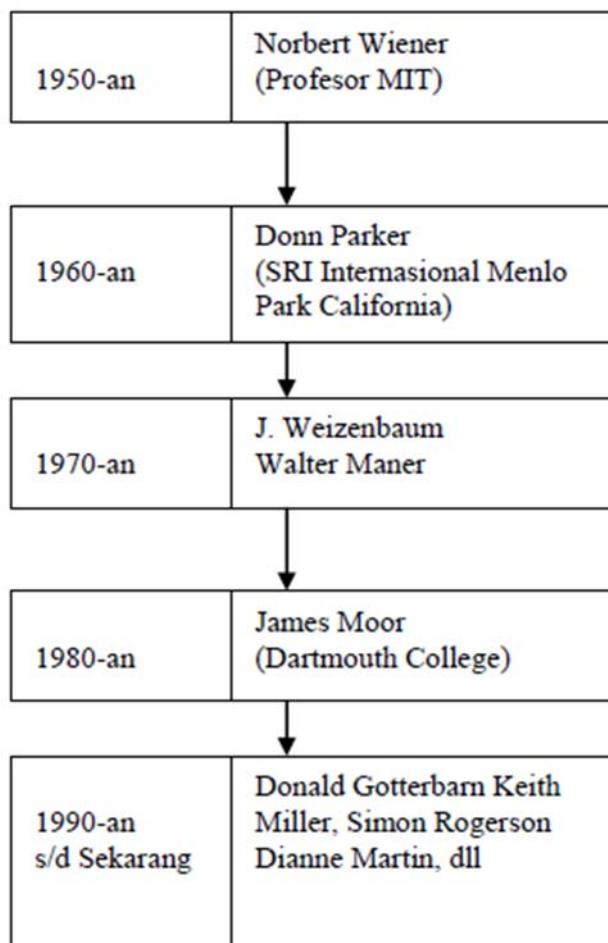
- **Era 1990-an sampai sekarang**

Donald Gotterbarn, Keith Miller, Simon Rogers, Dianne Martin melakukan riset mengenai tanggung jawab profesional di bidang komputer

Di Australia terjadi riset terbesar Etika Komputer yang dipimpin oleh Chris Simpson dan Yohanes Wecker.

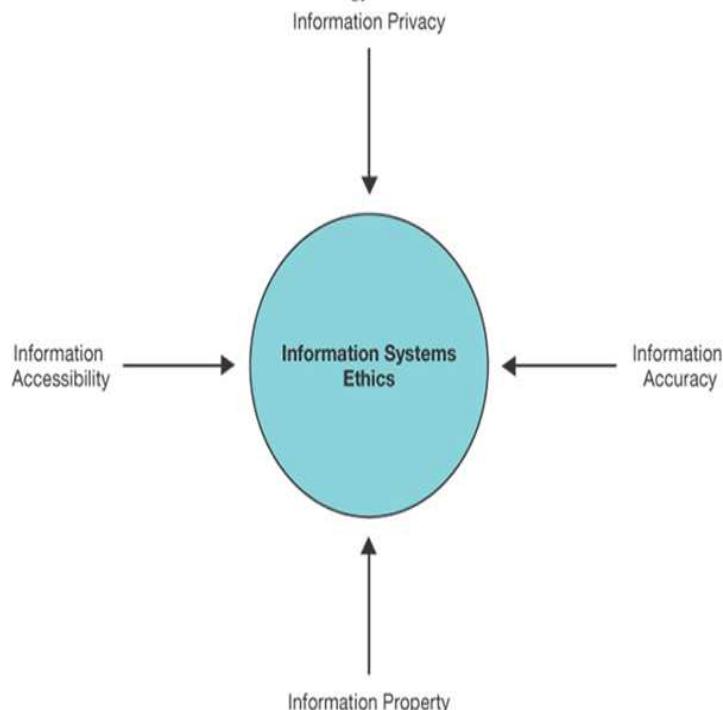
Implikasi pada bisnis yang semakin meluas akibat dari kejadian computer, membuat lahirnya forum-forum yang peduli pada masalah tersebut. (*ETHICOMP by Simon Rogerson, CEPE by Jeroe van Hoven etc*).

Tokoh-Tokoh Pelopor Etika Komputer



- Di Indonesia Etika komputer tidak berdiri sebagai bidang studi tersendiri, namun dimasukkan dalam bidang studi yang relevan.
- Misalnya memasukkan etika komputer dalam mata kuliah etika profesi bidang Teknologi Informasi.

Figure 9.5 Information privacy, accuracy, property, and accessibility are central to most ethical concerns about information technology.



© 2003 Prentice Hall, Inc.

Isu-Isu Pokok Etika Komputer

- **Kejahatan Komputer**

Definisi: kegiatan penggunaan komputer untuk melakukan tindakan ilegal

Hak pengaksesan komputer

Contoh:

- Mencuri waktu pada komputer perusahaan
- Membobol situs web pemerintah
- Pencurian informasi kartu kredit

Jenis-jenis kejahatan komputer

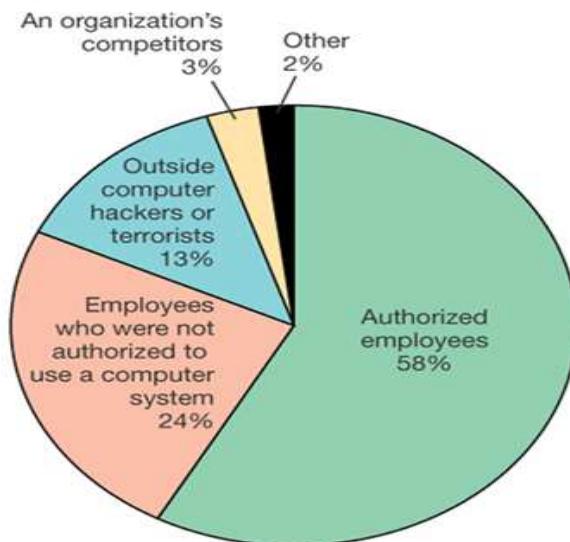
- **Data diddling:** manipulasi atau pemalsuan data
- **Salami slicing:** bagian program yang memotong sebagian kecil dari nilai transaksi yang besar dan mengumpulkan-nya dalam suatu periode tertentu
- **Phreaking:** making free long distance calls
- **Cloning:** penyalahgunaan telpon selular menggunakan scanner
- **Carding:** pencurian nomor kartu kredit secara online
- **Piggybacking:** pencurian nomor kartu kredit dengan memata-matai

- **Social engineering**: menipu pegawai untuk mendapatkan akses
- **Dumpster diving**: pencarian informasi pribadi di bak sampah
- **Spoofing**: pencuri

Isu-Isu Pokok Etika Komputer

Siapa yang berkomitmen melakukan kejadian komputer?

Figure 9.10 Who makes unlawful intrusions into computer systems.



© 2003 Prentice Hall, Inc.

• **Cyber ethics**

Implikasi dari INTERNET (Interconnection Networking), memungkinkan pengguna IT semakin meluas, tak terpetakan, tak teridentifikasi dalam dunia *anonymous*.

Social engineering adalah manipulasi psikologis dari seseorang dalam melakukan aksi atau menguak suatu informasi rahasia. **Social engineering** umumnya dilakukan melalui telepon atau Internet.

Social engineering merupakan salah satu metode yang digunakan oleh hacker untuk memperoleh informasi tentang targetnya, dengan cara meminta informasi itu langsung kepada korban atau pihak lain yang mempunyai informasi itu.

Social engineering mengkonsentrasi diri pada rantai terlemah sistem jaringan komputer, yaitu manusia. Tidak ada sistem komputer yang tidak melibatkan interaksi manusia. Dan parahnya lagi, celah keamanan ini bersifat universal, tidak tergantung platform, sistem operasi, protokol, software ataupun hardware. Artinya, setiap sistem mempunyai kelemahan yang sama pada faktor manusia. Setiap orang yang

mempunyai akses kedalam sistem secara fisik adalah ancaman, bahkan jika orang tersebut tidak termasuk dalam kebijakan kemanan yang telah disusun. Seperti metoda hacking yang lain, social engineering juga memerlukan persiapan, bahkan sebagian besar pekerjaan meliputi persiapan itu sendiri.

- Di balik semua sistem keamanan dan prosedur-prosedur pengamanan yang ada, masih terdapat faktor lain yang sangat penting, yaitu manusia.
- Pada banyak referensi, faktor manusia dinilai sebagai rantai paling lemah dalam sebuah sistem keamanan.
- Sebuah sistem keamanan yang baik, akan menjadi tidak berguna jika ditangani oleh administrator yang kurang kompeten. Selain itu, biasanya pada sebuah jaungan yang cukup kompleks terdapat banyak user yang kurang mengerti masalah keamanan atau tidak cukup peduli tentang hal itu. Ambil contoh di sebuah perusahaan, seorang network admin sudah menerapkan kebijakan keamanan dengan baik, namun ada user yang mengabaikan masalah kemanan itu. Misalnya user tersebut menggunakan password yang mudah ditebak, lupa logout ketika pulang kerja, atau dengan mudahnya memberikan akses kepada rekan kerjanya yang lain atau bahkan kepada kliennya. Hal ini dapat menyebabkan seorang penyerang memanfaatkan celah tersebut dan mencuri atau merusak datadata penting perusahaan. Membuang sampah yang bagi kita tidak berguna, dapat dijadikan orang yang berkepentingan lain. Misal: slip gaji, slip atm. Barang tersebut kita buang karena tidak kita perlukan, namun ada informasi didalamnya yang bisa dimanfaatkan orang lain.

Atau pada kasus di atas, seorang penyerang bisa berpura-pura sebagai pihak yang berkepentingan dan meminta akses kepada salah satu user yang ceroboh tersebut. Tindakan ini digolongkan dalam Social Engineering.

- Diperlukan adanya aturan tak tertulis (Netiket, Emoticon).
- **E-commerce**

Otomatisasi bisnis dengan internet dan layanannya, mengubah bisnis proses yang telah ada dari transaksi konvensional kepada yang berbasis teknologi, melahirkan implikasi negative; bermacam kejahatan, penipuan, kerugian karena ke-anonymous-an tadi.

- **Pelanggaran HAKI**

Masalah pengakuan hak atas kekayaan intelektual. Pembajakan, cracking, illegal software dst.

Pembajakan software

- Amerika Utara – 25%
- Eropa barat – 34%
- Asia / Pasifik – 51%
- Timur tengah / Afrika – 55%

- Amerika Latin – 58%
- Eropa Timur – 63%

- **Tanggung jawab profesi**

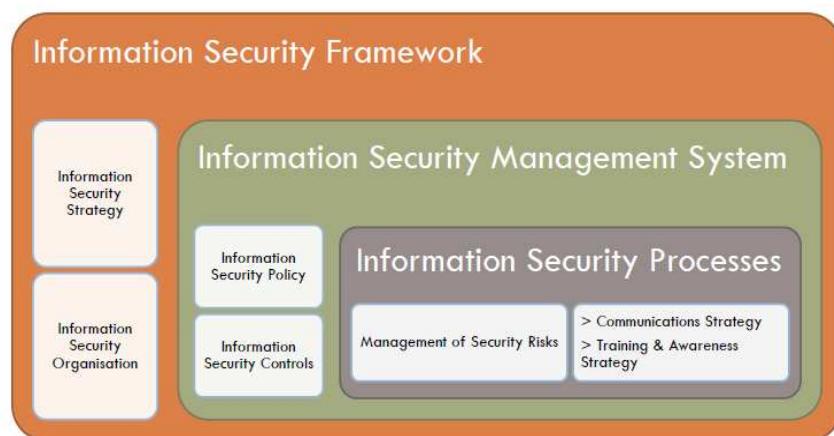
Sebagai bentuk tanggung jawab moral, perlu diciptakan ruang bagi komunitas yang akan saling menghormati. Misalnya IPKIN (Ikatan Profesi Komputer & Informatika-1974)

- ACM
“Code of Ethics and Professional Conduct”
- Computer Ethics Institute
“The Ten Commandments of Ethic's”
- Data Processing Management Association
“Code of Ethics and Standards of Conduct”

Sepuluh Perintah untuk Etika Komputer Dari Institut Etika Komputer

1. Jangan menggunakan komputer untuk membahayakan orang lain.
2. Jangan mencampuri pekerjaan komputer orang lain.
3. Jangan mengintip file orang lain.
4. Jangan menggunakan komputer untuk mencuri.
5. Jangan menggunakan komputer untuk bersaksi dusta.
6. Jangan menggunakan atau menyalin perangkat lunak yang belum kamu bayar.
7. Jangan menggunakan sumber daya komputer orang lain tanpa otorisasi.
8. Jangan mengambil hasil intelektual orang lain untuk diri kamu sendiri.
9. Pikirkanlah mengenai akibat sosial dari program yang kamu tulis.
10. Gunakanlah komputer dengan cara yang menunjukkan tenggang rasa dan rasa penghargaan.

Information Security Framework



© Crown Copyright 2011. Reproduced under licence from the Cabinet Office.

© Simplilearn Solutions Pvt. Ltd. 2012

ITIL® is a Registered Trade Mark of The Cabinet Office .

Terdiri dari:

- ✓ An overall information security policy
- ✓ Use and misuse of IT assets policy
- ✓ Access control policy
- ✓ Password control policy
- ✓ E-mail policy
- ✓ Internet policy
- ✓ Anti-virus policy
- ✓ Information classification policy
- ✓ Document classification policy
- ✓ Remote access policy
- ✓ Policy for supplier access of IT service, information and components
- ✓ Asset disposal policy

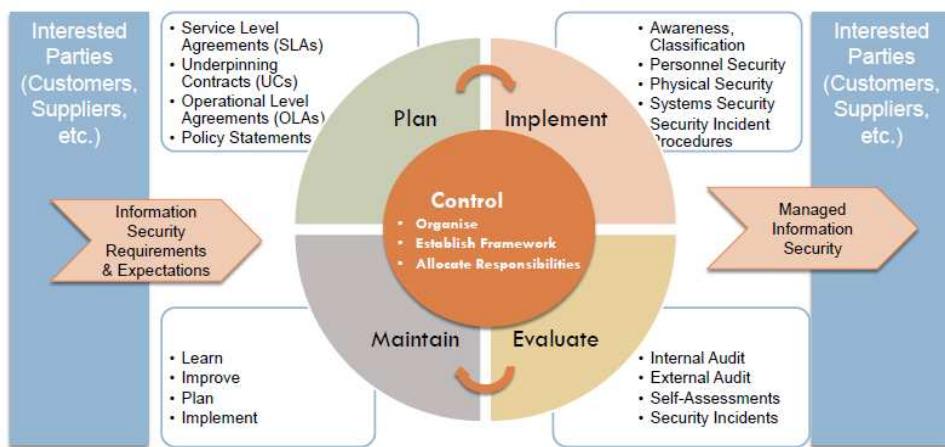
Keamanan Komputer / Jaringan

Tindakan pencegahan yang diambil untuk menjaga komputer/Jaringan dan informasi yang ada di dalamnya tetap aman dari pengaksesan yang tidak berhak.

Pengamanan yang disarankan

- Terapkan rencana pengamanan untuk mencegah pembobolan
- Miliki rencana jika pembobolan terjadi
- Buatlah backup!
- Hanya ijinkan akses untuk pegawai tertentu
- Ubah password secara teratur
- Jagalah informasi yang tersimpan dengan aman
- Gunakan software antivirus
- Gunakan biometrik untuk mengakses sumberdaya komputasi
- Rekrut tenaga kerja / pegawai yang bisa dipercaya

Information Security Management System(ISMS)



Implementasi:

- **Enkripsi** digunakan untuk menyandikan data-data atau informasi sehingga tidak dapat dibaca oleh orang yang tidak berhak.

Pendekatan enkripsi yang lain

- Pretty good privacy (PGP)

Phil Zimmerman

- Clipper Chip

- **Keamanan Internet**

Firewall – hardware dan software yang dirancang untuk menjaga agar user yang tidak berhak tidak dapat masuk ke sistem jaringan

Pencegahan Virus

- Install software antivirus
- Buat data cadangan
- Hindari pemakaian program bebas yang tidak dikenal
- Hapus email dari sumber yang tidak dikenal
- Jika komputer kena virus ...

Bagaimana menjaga privasi saat online

- Pilih situs web yang dimonitor oleh pengacara privasi
- Hindari "cookies"
- Kunjungi situs secara anonim

- Gunakan peringatan saat meminta konfirmasi email

Hindari penipuan di dunia cyber

- Pelelangan Internet
- Akses Internet
- Men-dial modem internasional
- *Web cramming*
- Multilevel marketing (skema piramida)
- Bepergian / liburan
- Kesempatan bisnis
- Penanaman modal
- Produk-produk perawatan kesehatan

DaftarPustaka

- *Etika komputer dan tanggung jawab Profesional di Bidang Teknologi Informasi, Tegus Wahyono,S.Kom.*
- [https://id.wikipedia.org/wiki/Social_engineering_\(keamanan\)](https://id.wikipedia.org/wiki/Social_engineering_(keamanan))
- didiktristianto.dosen.narotama.ac.id/.../Materi-ke-9-Etika-profesi-T...
- amutiara.staff.gunadarma.ac.id/.../1_Tinjauan+Umum+Etika+Kom...
- https://wahyumi.files.wordpress.com/.../bab-2_etika-komputer-sejar..
- Simplilearn.com



MODUL PERKULIAHAN

Keamanan

Jaringan

Security management.

Abstract

Keamanan jaringan terutama security management dapat dipelajari sebagai proses pengumpulan dan penilaian bukti – bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien

Kompetensi

Setelah membaca modul ini diharapkan mahasiswa :

- Mengetahui Kontrak Perkuliahuan
- Setelah mengikuti mata kuliah ini diharapkan mahasiswa memiliki kemampuan untuk:
 - Mempelajari security Management utk bisnis besar & menengah.

Pentingnya Manajemen Kontrol Keamanan pada Sistem

- **Tujuan manajemen informasi** adalah untuk melindungi kerahasiaan, integritas dan ketersediaan informasi.
- Dengan tumbuhnya berbagai penipuan, spionase, virus, dan hackers sudah mengancam informasi bisnis manajemen oleh karena meningkatnya keterbukaan informasi dan lebih sedikit kendali/control yang dilakukan melalui teknologi informasi modern.
- Sebagai konsekuensinya , meningkatkan harapan dari para manajer bisnis, mitra usaha, auditor, dan stakeholders lainnya menuntut adanya manajemen informasi yang efektif untuk memastikan informasi yang menjamin kesinambungan bisnis dan meminimise kerusakan bisnis dengan pencegahan dan meminimalisasi dampak peristiwa keamanan.

Mengapa harus mengamankan informasi?

- Keamanan Informasi adalah suatu upaya untuk mengamankan aset informasi yang dimiliki. Kebanyakan orang mungkin akan bertanya, mengapa “**keamanan informasi**” dan **bukan** “keamanan teknologi informasi” atau IT Security.
- Kedua istilah ini sebenarnya sangat terkait, namun mengacu pada dua hal yang sama sekali berbeda. “Keamanan Teknologi Informasi” atau IT Security mengacu pada usaha-usaha mengamankan infrastruktur teknologi informasi dari gangguan-gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan
- Berbeda dengan “keamanan informasi” yang fokusnya justru pada data dan informasi milik perusahaan.

Pada konsep ini, usaha-usaha yang dilakukan adalah merencanakan, mengembangkan serta mengawasi semua kegiatan yang terkait dengan bagaimana data dan informasi bisnis dapat digunakan serta diutilisasi sesuai dengan fungsinya serta tidak disalahgunakan atau bahkan dibocorkan ke pihak-pihak yang tidak berkepentingan.

CIA

Keamanan informasi terdiri dari perlindungan terhadap aspek-aspek berikut:

- **Confidentiality (kerahasiaan)** aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.
- **Integrity (integritas)** aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin sihak yang berwenang (authorized), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek integrity ini.
- **Availability (ketersediaan)** aspek yang menjamin bahwa data akan tersedia saat

dibutuhkan, memastikan user yang berhak dapat menggunakan informasi dan perangkat terkait (aset yang berhubungan bilamana diperlukan).

Mengapa harus mengamankan informasi?

Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktek-praktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak.

Informasi yang merupakan aset harus dilindungi keamanannya. Keamanan, secara umum diartikan sebagai “*quality or state of being secure-to be free from danger*”[1]. Untuk menjadi aman adalah dengan cara dilindungi dari musuh dan bahaya. Keamanan bisa dicapai dengan beberapa strategi yang biasa dilakukan secara simultan atau digunakan dalam kombinasi satu dengan yang lainnya. Strategi keamanan informasi memiliki fokus dan dibangun pada masing-masing ke-khusus-annya.

Contoh dari tinjauan keamanan informasi adalah:

- **Physical Security** yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
- **Personal Security** yang overlap dengan ‘*physical security*’ dalam melindungi orang-orang dalam organisasi.
- **Operation Security** yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.
- **Communications Security** yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.
- **Network Security** yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Bagaimana mengamankannya?

Manajemen keamanan informasi memiliki tanggung jawab untuk program khusus, maka ada karakteristik khusus yang harus dimilikinya, yang dalam manajemen keamanan informasi dikenal sebagai **5P** yaitu:

1. Planning

Planning dalam manajemen keamanan informasi meliputi proses perancangan, pembuatan, dan implementasi strategi untuk mencapai tujuan. Ada tiga tahapannya yaitu:

- 1) ***strategic planning*** yang dilakukan oleh tingkatan tertinggi dalam organisasi untuk periode yang lama, biasanya lima tahunan atau lebih,

2) **tactical planning** memfokuskan diri pada pembuatan perencanaan dan mengintegrasikan sumberdaya organisasi pada tingkat yang lebih rendah dalam periode yang lebih singkat, misalnya satu atau dua tahunan,

3) **operational planning** memfokuskan diri pada kinerja harian organisasi. Sebagaimana tambahannya, planning dalam manajemen keamanan informasi adalah aktivitas yang dibutuhkan untuk mendukung perancangan, pembuatan, dan implementasi strategi keamanan informasi supaya diterapkan dalam lingkungan teknologi informasi.

Ada beberapa tipe planning dalam manajemen keamanan informasi, meliputi :

1) *Incident Response Planning (IRP)*

IRP terdiri dari satu set proses dan prosedur detil yang mengantisipasi, mendeteksi, dan mengurangi akibat dari insiden yang tidak diinginkan yang membahayakan sumberdaya informasi dan aset organisasi, ketika insiden ini terdeteksi benar-benar terjadi dan mempengaruhi atau merusak aset informasi. Insiden merupakan ancaman yang telah terjadi dan menyerang aset informasi, dan mengancam *confidentiality*, *integrity* atau *availability* sumber daya informasi. *Incident Response Planning* meliputi *incident detection*, *incident response*, dan *incident recovery*.

2) *Disaster Recovery Planning (DRP)*

Disaster Recovery Planning merupakan persiapan jika terjadi bencana, dan melakukan pemulihan dari bencana. Pada beberapa kasus, insiden yang dideteksi dalam IRP dapat dikategorikan sebagai bencana jika skalanya sangat besar dan IRP tidak dapat lagi menangani secara efektif dan efisien untuk melakukan pemulihan dari insiden itu. Insiden dapat kemudian dikategorikan sebagai bencana jika organisasi tidak mampu mengendalikan akibat dari insiden yang terjadi, dan tingkat kerusakan yang ditimbulkan sangat besar sehingga memerlukan waktu yang lama untuk melakukan pemulihan.

3) *Business Continuity Planning (BCP)*

Business Continuity Planning menjamin bahwa fungsi kritis organisasi tetap bisa berjalan jika terjadi bencana. Identifikasi fungsi kritis organisasi dan sumberdaya pendukungnya merupakan tugas utama business continuity planning. Jika terjadi bencana, BCP bertugas menjamin kelangsungan fungsi kritis di tempat alternatif. Faktor penting yang diperhitungkan dalam BCP adalah biaya.

2. Policy

Dalam keamanan informasi, ada tiga kategori umum dari kebijakan yaitu:

1. ***Enterprise Information Security Policy (EISP)*** menentukan kebijakan departemen keamanan informasi dan menciptakan kondisi keamanan informasi di setiap bagian organisasi.
2. ***Issue Specific Security Policy (ISSP)*** adalah sebuah peraturan yang menjelaskan perilaku yang dapat diterima dan tidak dapat diterima dari segi keamanan informasi

pada setiap teknologi yang digunakan, misalnya e-mail atau penggunaan internet.

3. **System Spesific Policy (SSP)** pengendali konfigurasi penggunaan perangkat atau teknologi secara teknis atau manajerial.

3. Programs

Programs

Adalah operasi-operasi dalam keamanan informasi yang secara khusus diatur dalam beberapa bagian. Salah satu contohnya adalah program security education training and awareness. Program ini bertujuan untuk memberikan pengetahuan kepada pekerja mengenai keamanan informasi dan meningkatkan pemahaman keamanan informasi pekerja sehingga dicapai peningkatan keamanan informasi organisasi.

4. Protection

Protection

Fungsi proteksi dilaksanakan melalui serangkaian aktifitas manajemen resiko, meliputi perkiraan resiko (*risk assessment*) dan pengendali, termasuk mekanisme proteksi, teknologi proteksi dan perangkat proteksi baik perangkat keras maupun perangkat keras. Setiap mekanisme merupakan aplikasi dari aspek-aspek dalam rencana keamanan informasi.

5. People

People

Manusia adalah penghubung utama dalam program keamanan informasi. Penting sekali mengenali aturan krusial yang dilakukan oleh pekerja dalam program keamanan informasi. Aspek ini meliputi personil keamanan dan keamanan personil dalam organisasi.

Standard

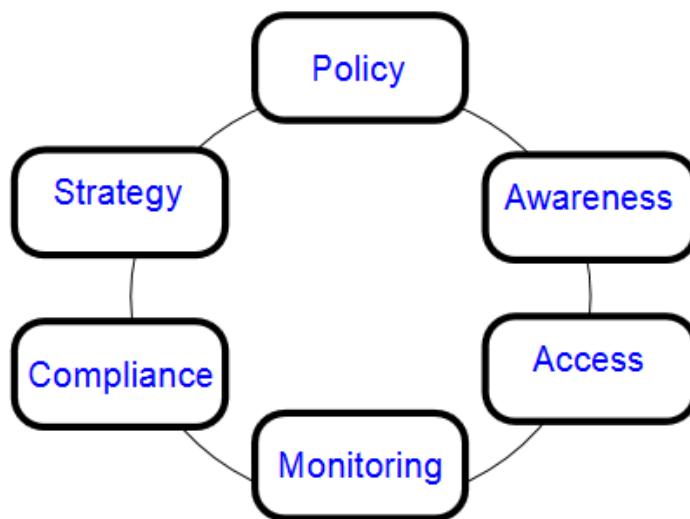
- ISO/IEC 27001 adalah standar information security yang diterbitkan pada October 2005 oleh International Organization for Standardization dan International Electrotechnical Commission. Standar ini menggantikan BS-77992:2002.
- ISO/IEC 27001: 2005 mencakup semua jenis organisasi (seperti perusahaan swasta, lembaga pemerintahan, dan lembaga nirlaba). ISO/IEC 27001: 2005 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa dan memelihara seta mendokumentasikan Information Security Management System dalam konteks resiko bisnis organisasi keseluruhan
- ISO/IEC 27001 mendefenisikan keperluan-keperluan untuk sistem manajemen keamanan informasi (ISMS). ISMS yang baik akan membantu memberikan perlindungan terhadap gangguan pada aktivitas-aktivitas bisnis dan melindungi proses

bisnis yang penting agar terhindar dari resiko kerugian/bencana dan kegagalan serius pada pengamanan sistem informasi, implementasi ISMS ini akan memberikan jaminan pemulihan operasi bisnis akibat kerugian yang ditimbulkan dalam masa waktu yang tidak lama.

Security management process

effective security management process comprises six sub processes:

- Policy
- Awareness
- Access
- Monitoring
- Compliance
- Strategy



<http://csrc.nist.gov/nissc/1996/papers/NISSC96/paper015/bayuk.pdf>

Policy:

to establish a framework for the development of organizational standards with respect to security.

Awareness:

to educate those affected by security policy on their roles and responsibilities.

Access:

to limit dissemination and modification of customer data and other sensitive information

Monitoring:

to detect policy violations and other security vulnerabilities

Compliance:

to educate those affected by security policy on their roles and responsibilities.

to track security issues and help ensure that resources facilitate the resolution of security issues

Strategy:

to meet the security challenges presented by new information technologies

Taken together, these six processes form one high-level security management process.

Security management process

Example:

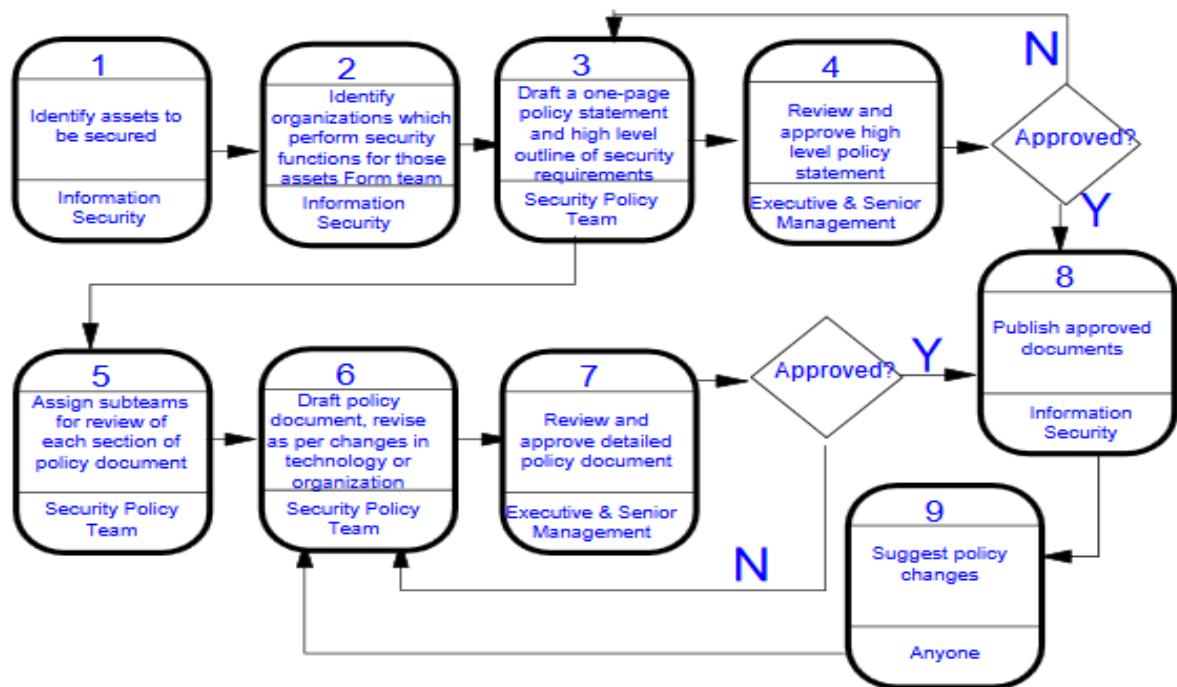


Figure 1: Example Policy Process

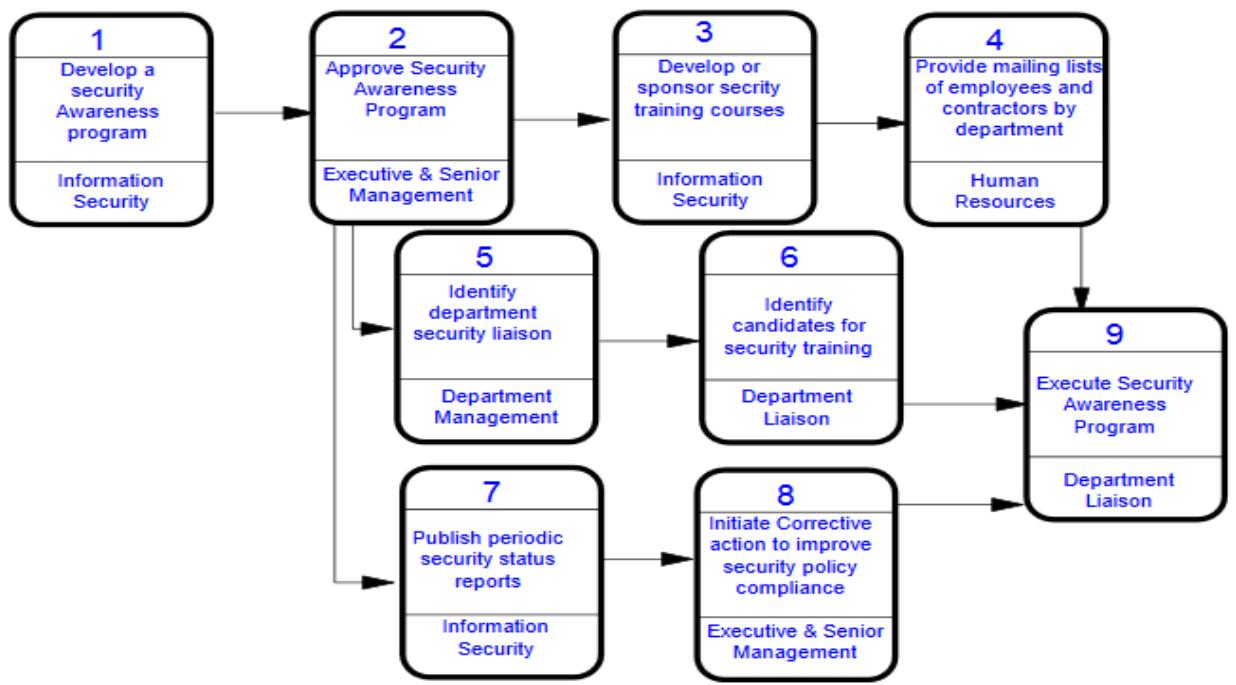


Figure 2: Example Awareness Process

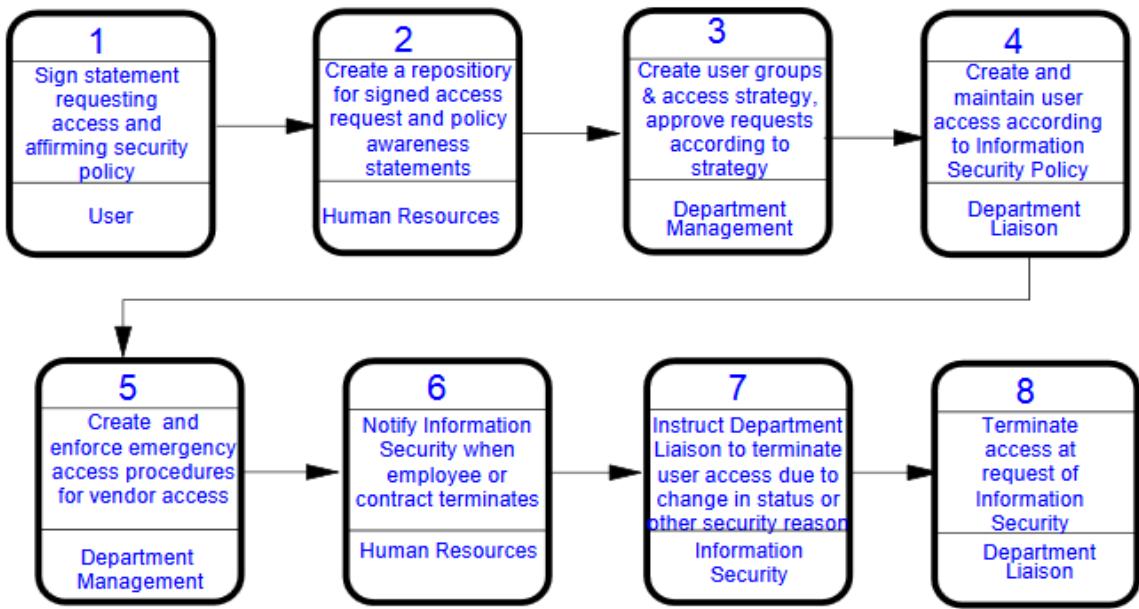


Figure 3: Example Access Process

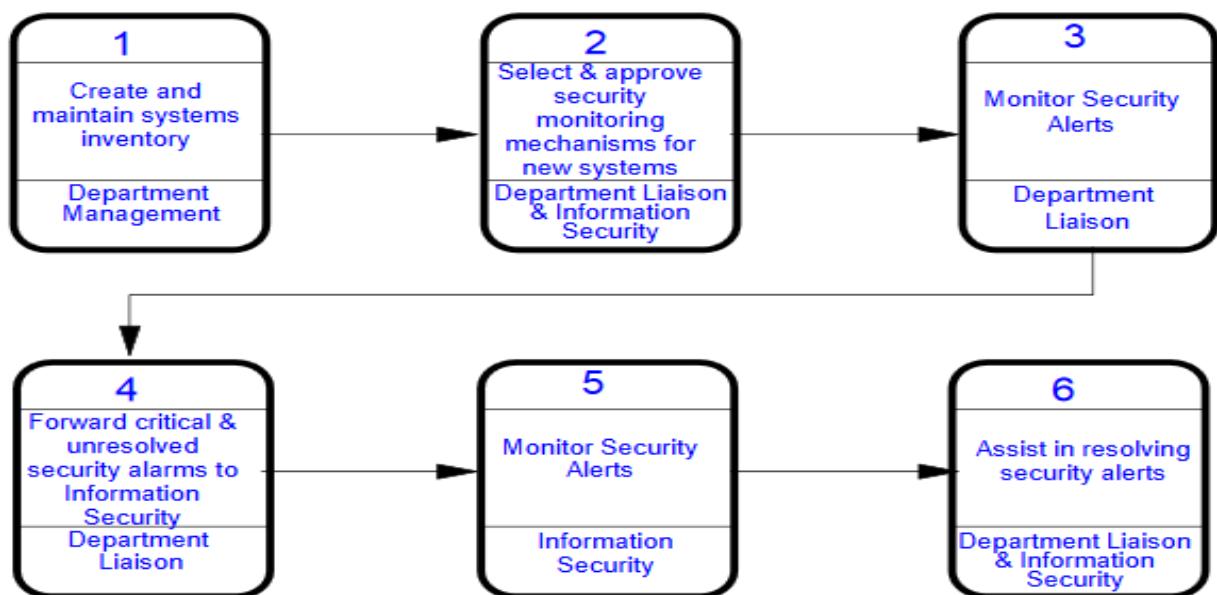


Figure 4: Example Monitoring Process

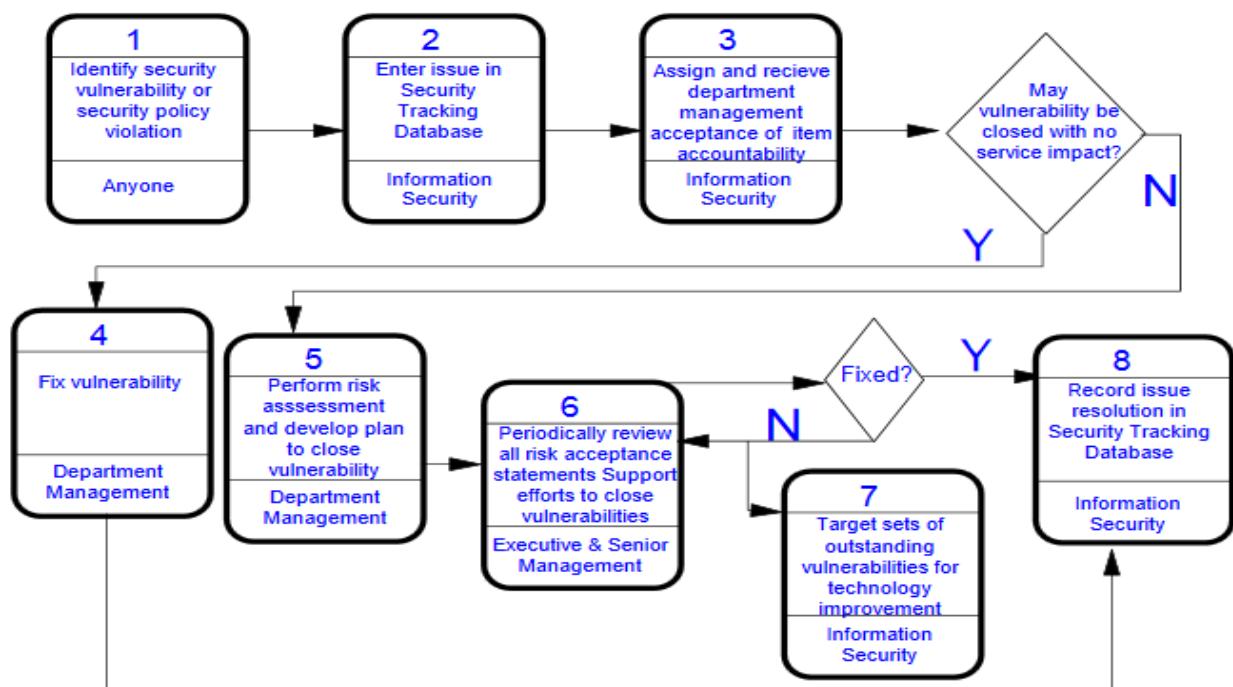


Figure 5: Example Compliance Process

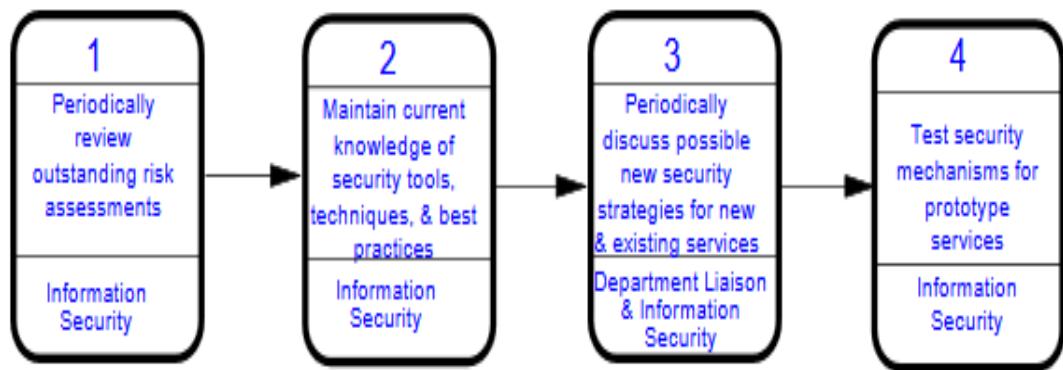


Figure 6: Example Strategy Process

Daftar Pustaka

- Information System Audit and Control Association (ISACA) (2003), IS Standards, Guidelines and Procedures for Auditing and Control Professionals, <http://www.isaca.org>.
- <https://idadwiw.wordpress.com/2013/12/26/pentingnya-manajemen-kontrol-keamanan-pada-sistem/>
- https://en.wikipedia.org/wiki/ITIL_security_management
- <http://csrc.nist.gov/nissc/1996/papers/NISSL96/paper015/bayuk.pdf>