MODUL BAHAN AJAR SISTEM KEAMANAN KOMPUTER

Modul ini menjadi bahan referensi mahasiswa untuk memperlajari model sistem keamanan computer dan segala asfek Teknik dan resiko model pengamanan komputer

SECURITY SYSTEM

Dosen Pengampu :
Agus Suryana

Kata pengantar

Puji syukur kehadirat Tuhan Yang Maha Kuasa atas segala limpahan rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan Modul Bahan Ajar yang berjudul tentang Sistem Keamanan; Sebuah pegangan untuk mahasiswa Prodi Sistem Informasi STMIK Pringsewu. Modul Bahan Ajar ini digunakan bagi dosen untuk mengajar mata kuliah Sistem Keamanan di Prodi Sistem Informasi

Modul Bahan Ajar Sistem Keamanan ini disusun secara sistematis dalam menjelaskan konsep dasar sistem pengamanan data agar pembacanya dapat dengan mudah memahami materi perkuliahan. Pada Modul Bahan Ajar ini, menyajikan berbagai materi dasar terkait sistem keamanan pada sistem operasi, database maupun jaringan. Mata kuliah ini juga memberikan pemahaman tentang kriptografi klasik dan modern sehingga peserta akan dapat memahami konsep dari Sistem Keamanan. Selain itu juga dibahas studi kasus pada sistem keamanan dan tren terkini dalam sistem keamanan. Pada setiap bab pembahasannya, mengarahkan pembacanya agar dapat mencapai kompentensi dasar dan tujuan pembelajaran.

Akhirnya, harapan penulis adalah dengan adanya Modul Bahan Ajar ini dapat membantu mahasiswa dalam belajar mengenai Sistem Keamanan sehingga dapat bermanfaat dalam pengembangan ilmu dan pengetahuan.

Pringsewu, 6 Januari 2018

Agus Suryana

Daftar Isi

Daftar Gambar

Daftar Tabel

BAB I Pendahuluan

A. Informasi Mata Kuliah

1) Nama Mata Kuliah : Sistem Keamanan
2) Bobot Kredit : 4 SKS
3) Program Studi : Sistem Informasi
4) Kode Mata Kuliah : INF 11013
5) Status Mata Kuliah : Wajib
6) Semester : Genap
7) Prasyarat : -
8) Bentuk Pengajaran :*Ceramah,Project Based Learning*
9) Jumlah pertemuan : 16 kali pertemuan
10) Masa perkuliahan : 150 menit pertemuan
11) Dosen Pengampu : Agus Suryana., M.T.I
12) Tujuan Mata Kuliah :Mahasiswa dapat memahami bagaimana keamanan pada sebuah sistem komputer, memahami kriptografi klasik dan kriptografi modern, memahami ancaman keamanan pada OS, basis data dan jaringan, dapat menganalisa dan membuat sebuah kebijakan yang baik dalam sebuah organisasi yang mengedepankan masalah keamanan.

B. Deskripsi Mata Kuliah

Mata kuliah ini memberikan pemahaman terhadap bagaimana sistem keamanan pada sistem operasi, basis data maupun jaringan. Mata kuliah ini juga memberikan pemahaman tentang kriptografi klasik dan modern sehingga peserta akan dapat memahami konsep dari sistem keamanan. Selain itu juga dibahas studi kasus pada sistem keamanan dan tren terkini dalam sistem keamanan.

C. Sub Capaian Pembelajaran Mata Kuliah dan Bahan Kajian

Sub Capaian Pembelajaran Mata Kuliah (CPMK) dan bahan kajian yang digunakan pada mata kuliah ini dapat dilihat pada Tabel 1.

Tabel 1. Sub-CPMK dan Bahan Kajian Mata Kuliah

Pert.	Sub-CPMK	Bahan Kajian
1	Mahasiswa mampu : 1) Memahami konsep dasar keamanan sistem komputer 2) Memahami etika penggunakaan komputer 3) Memahami dasar-dasar gangguan keamanan komputer beserta akibatnya	Pendahuluan 1. Kontrak perkuliahan 2. Masalah keamanan sistem komputer secara umum. 3. Masalah etika. 4. Dasar-dasar gangguan keamanan komputer.

	4) Memahami prinsip dasar perancangan sistem komputer yang aman	
2	Mahasiswa mampu : 1. Memahami konsep dasar jaringan komputer 2. Mengenali bentuk-bentuk ancaman terhadap jaringan komputer 3. Memahami pengendalian terhadap keamanan jaringan komputer	Keamanan Jaringan Komputer 1. Konsep dasar jaringan komputer 2. Bentuk-bentuk ancaman terhadap jaringan komputer 3. Bentuk pengendalian terhadap keamanan jaringan komputer
3	Mahasiswa mampu : *1.* Memahami konsep *trusted guards*, *gateways* dan *firewall* *2.* Memahami konsep keamanan dalam LAN *(Local Area Network)* *3.* Memahami konsep kemanan dalam WAN *(Wide Area Networ)*	Keamanan Jaringan Komputer 1. Konsep trusted guards, gateways dan firewall 2. Keamanan dalam LAN(Local Area Network) 3. Kemanan dalam WAN (Wide Area Networ)
4	Mahasiswa mampu : 1. Memahami cara kerja web browser. 2. Memahami komponen dan kelemahan pada Web Browser. 3. Mengetahui titik-titik kelemahan dari Web	*Internet Security* 1. Pendahuluan 2. Bentuk ancaman keamanan internet. 3. Cara mengatasi ancaman kemanan pada internet.

	Browser. 4. Memahami teknik penerepan keamanan untuk meminimalkan kelemahan dari Web Browser.	
5	Mahasiswa mampu : 1. Memahami cara kerja Web System 2. Memahami komponen dan kelemahan pada Web System. 3. Mengetahui titik-titik kelemahan dari Web System. 4. Memahami teknik penerepan keamanan untuk meminimalkan kelemahan dari Web System.	*Internet Security* Keamanan pada : *1. Web Service* *2. Software as service* *3. Cloud Computing*
6	Mahasiswa mampu : 1) Memahami model-model keamanan dalam sistem operasi 2) Memahami perancangan sistem operasi yang aman 3) Mengenali bentuk serangan terhadap sistem operasi Windows 4) Melakukan evaluasi terhadap sistem operasi Windows	Keamanan Sistem Operasi (Windows) 1. Model-model keamanan dalam sistem operasi 2. Perancangan sistem operasi yang aman 3. Bentuk serangan terhadap sistem operasi 4. Tinjauan terhadap sistem operasi yang aman

		5. Contoh sistem operasi yang aman
7	Mahasiswa mampu : 1. Mengenali bentuk serangan terhadap sistem operasi Linux 2. Melakukan evaluasi terhadap sistem operasi Linux	Keamanan Sistem Operasi (Linux) 1. Model-model keamanan dalam sistem operasi 2. Perancangan sistem operasi yang aman 3. Bentuk serangan terhadap sistem operasi 4. Tinjauan terhadap sistem operasi yang aman 5. Contoh sistem operasi yang aman
8	**Ujian Tengah Semester**	
9	Mahasiswa mampu : 1. Memahami teknik-teknik pengamanan database yang handal 2. Mengenali perlindungan terhadap data yang sensitif 3. Merangkuman masalah-masalah keamanan dalam penggunaan database 4. Memahami konsep database multilevel 5. Memahami konsep keamanan bertingkat dalam database	Keamanan Database 1. Teknik-teknik pengamanan database yang handal dan memiliki integritas 2. Perlindungan terhadap data yang sensitif 3. Rangkuman permasalahan keamanan database 4. Konsep database multilevel 5. Konsep keamanan bertingkat dalam

		database
10	Mahasiswa mampu : 1. Memahami teknik-teknik perlindungan program terhadap virus. 2. Mengendalikan program terhadap bentuk ancaman dari luar	*Malicious software* 1. Perlindungan terhadap virus komputer. 2. Pengendalian program terhadap ancaman lainnya.
11	Mahasiswa mampu : 1. Memahami pengembangan SOP dan Audit pada keamanan sistem komputer. 2. Memahami penerapan SOP dan Audit pada keamanan sistem komputer.	Pengaturan Keamanan 1. Pengaturan keamanan dalam Sistem. 2. Analisa resiko. 3. Perencanaan SOP keamanan dalam sistem komputer. 4. Pengembangan Audit keamanan dalam sistem komputer
12	Memahami permasalahan keamanan komputer secara umum	Studi Kasus 1. Autentikasi dengan menggunakan password 2. Enkripsi data dalam proses kompresi dokumen 3. Transaksi pembayaran melalui ATM secara aman

13	Mahasiswa mampu memahami teknik-teknik: 1. Penyandi monoalfabetik 2. Penyandi polialfabetik 3. Penggunaan publickey	Kriptografi Klasik 1. Pengertian Kriptografi 2. Penynadi monoalfabetik 3. Penyandi polialfabetik 4. Penggunaan public key
14	Mahasiswa mampu memahami teknik-teknik: 1. Metode enkripsi DES 2. Metode enkripsi RSA	Kriptografi Modern 1. Metode enkripsi DES (*Data Encryption Standar*) 2. Metode enkripsi RSA (Rivest, Shamir, Adleman)
15	Mahasiswa mampu : 1. Melakukan analisa terhadap proses autentikasi sistem dengan menggunakan password 2. Melakukan analisa terhadap proses enkripsi data dalam proses kompresi dokumen 3. Melakukan analisa dalam proses transaksi pembayaran melalui ATM secara aman	Trend Kedepan *1) Trusted Computing Group* *2) Digital Right Management* *3)* Kasus-kasus terkini *4)* Trend kasus dan masalah keamanan ke depan.
16	**Ujian Akhir Semester**	

D. Referensi

1) Alexander, M. The Underground Guide to Computer Security, Addison-Wesley Publishing, I1994
2) Denning, Peter J., Computer Under Attack : Intruders, Worms, and Viruses, Addison-Wesley Publishing, 1991
3) Ford, Warwick, Computer Communications Security, Prentice-Hall, 1994
4) Pfleeger, C.P. Security in computing, Prentice-Hall, 1997
5) Rhee, Man Young, Cryptography and Secure Communications, McGraw Hill, 1994
6) Morrie Grasser, Building A Secure Computer System, Edisi 4, Nelson Canada, 1988

Bab II Konsep Dasar Keamanan

A. TIU

Setelah membaca materi ini diharapkan mahasiswa mampu :

1) Memahami konsep dasar keamanan sistem komputer
2) Memahami etika penggunaan komputer
3) Memahami dasar-dasar gangguan keamanan komputer beserta akibatnya
4) Memahami prinsip dasar perancangan sistem komputer yang aman

B. Segitiga CIA (CIA Triad)

Mendengar kata CIA mungkin sebagian orang akan merujuk pada sebuah badan intelijen milik Amerika Serikat. Namun, nyatanya ada perujukan lain untuk kata CIA pada sistem keamanan secara umum. CIA merupakan singkatan dari *Confidentiality, Integrity*, dan *Availability*. CIA atau sering juga disebut CIA Triad merupakan salah satu aturan dasar dalam menentukan keamanan jaringan atau informasi. Aturan lainnya dikenal dengan Perkerian Hexad (*Confidentiality*, *Posession or Control*, *Integrity*, *Authenticity*, *Availability*, dan *Utility*).

Gambar 1. Segitiga CIA
(sumber: https://www.readynez.com/)

Confidentiality (rahasia) berarti menjaga kerahasiaan informasi dengan melakukan pembatasan hak akses seseorang, yang paling umum dengan menggunakan enkripsi. Contoh data-data yang harus dijaga kerahasiaannya seperti data-data yang sifatnya pribadi (nama, tanggal lahir, penyakit yang pernah diderita, nomor kartu kredit, nama ibu kandung, dan sebagainya), data-data milik organisasi atau perusahaan. Ada kalanya *confidentiality* sejalan dengan *privacy*. Aspek ini bertujuan untuk:

a. Membatasi pengaksesan terhadap informasi sesuai tingkat kerahasiaannya

b. Melindungi data / informasi agar tidak diketahui oleh pihak yang tidak berwenangan

Integrity (keaslian) berarti menjamin bahwa data/informasi yang dimiliki terjaga keasliannya, tidak berubah tanpa pemilik informasi. *Integrity* merujuk pada tingkat kepercayaan terhadap suatu informasi. Di dalam *integrity* terdapat 2 mekanisme pengamanan yaitu mekanisme priventif dan mekanisme detektif. Mekanisme **priventif** merupakan kontrol akses untuk menghalangi terjadinya modifikasi data. Sedangkan mekanisme **detektif** adalah untuk melakukan deteksi terhadap modifikasi yang telah dilakukan oleh orang lain. Aspek ini bertujuan untuk:

a. Melindungi data dan atau program agar tidak dimodifikasi tanpa izin oleh pihak yang tidak berwenang.
b. Memberikan jaminan bahwa data / informasi yang ada pada *resource* dapat dipercaya.

Availability (ketersediaan) berhubungan dengan ketersediaan informasi ketika dibutuhkan. Artinya, informasi harus selalu tersedia saat dibutuhkan oleh user, dan dapat dengan cepat diakses. Serangan yang paling lazim untuk jenis keamanan ini adalah *Distributed Denial of Service* (DDoS). Serangan ini memenuhi *resource* atau sumber informasi (server) dengan permintaan yang banyak atau permintaan

diluar perkiraan sehingga server tidak dapat melayani permintaan lain atau bahkan *down*.

"On the Internet, nobody knows you're a dog." by Peter Steiner, 1993

C. Ancaman Keamanan

Ancaman-ancaman yang sering dihadapi oleh masalah keamanan dapat dikategorikan sebagai berikut:

1) Manusia, ancaman dari manusia dapat berupa:
   a. *Hacking*, *cracking* atau sesiapa saja yang berusaha atau telah mengakses sistem tanpa izin dari pihak yang berwenang. Tujuannya bisa untuk melakukan pencurian data/informasi atau perusakan.
   b. Memasukkan program illegal seperti virus, worm (*malicious software*)

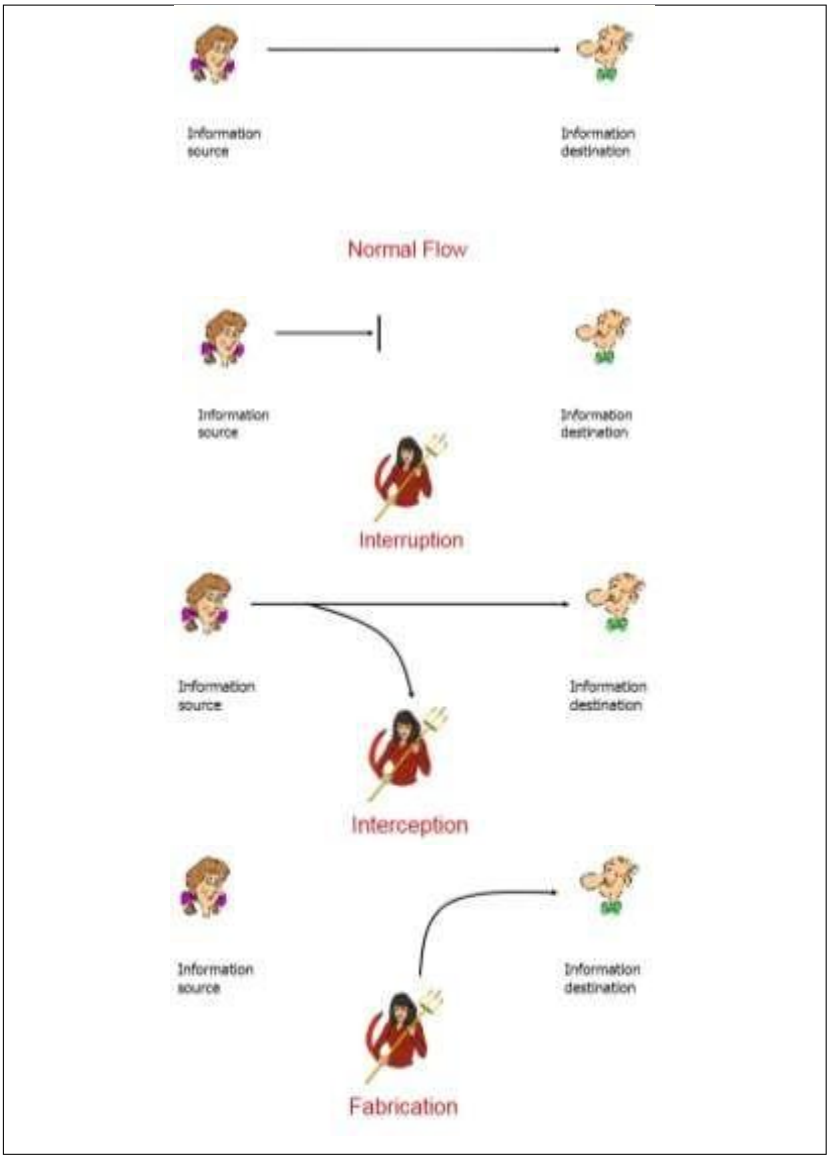
c. Kemampuan user yang terbatas dalam menggunakan dan memelihara sistem serta rendahnya kesadaran akan keamanan sistem.

2) Kesalahan perangkat keras, ancaman ini dapat berupa:
   a. Tidak stabilnya suplai listrik dalam jangka waktu panjang sehingga mengakibatkan kerusakan pada perangkat.
   b. Terjadinya korsleting listrik yang dapat mengakibatkan terhentinya proses sistem atau bahkan kerusakan sistem.
   c. Segala macam bentuk gangguan fisik yang berdampak langsung maupun tak langsung terhadap perangkat.
3) Kegagalan perangkat lunak, ancaman ini dapat berupa:
   a. Adanya kesalahan pada sistem operasi
   b. Adanya kesalahan saat meng-*update* program
   c. Uji coba program yang tidak memadai sehingga menyisakan *error* pada perangkat lunak.
4) Alam, merupakan ancaman yang tidak bisa dicegah seperti banjir, gempa bumi, kebakaran, dan sebagainya.

D. Model Serangan Keamanan

Beberapa model serangan terhadap keamanan (Stalling, 1995):

1) *Interruption*. Serangan ini ditujukan untuk aspek ketersediaan (*availability*), yang menjadikan sistem tidak tersedia atau rusak. Contoh serangan *denial of service attack*.
2) *Interception*. Serangan ini berupa pihak yang tidak memiliki wewenang berhasil mengakses data / informasi. Misalnya dengan melakukan penyadapan (*wiretapping*).
3) *Modification*. Serangan ini berupa pihak yang tidak memiliki wewenang berhasil memodifikasi aset atau data/informasi yang dimiliki organisasi/perusahaan.
4) *Fabrication*. Serangan ini berupa pihak yang tidak berwenang menjadi seolah-olah pengguna sah dan mengirimkan pesan palsu kedalam sistem. Menyerang aspek autentikasi. Contoh dengan memasukkan pesan-pesan palsu seperti e-mail palsu ke jaringan komputer.



Gambar 2. Security Attack
(sumber: https://slideplayer.com/slide/7649243/)

E. Mengenal Rekayasa Sosial

Menurut salah satu perusahaan antivirus terbesar, Norton social engineering atau rekayasa sosial adalah tindakan menipu seseorang untuk mengungkapkan informasi atau mengambil tindakan yang dilakukan melalui teknologi. Gagasan utamanya adalah untuk mengambil keuntungan dari kecenderungan alami dan reaksi emosional korban. Berikut 6 tipe dari serangan rakayasa sosial:

1. *Baiting*. Jenis rekayasa sosial ini bergantung pada korban untuk mengambil "umpan" atau tidak sehingga melakukan tindakan tertentu. Conoth: seorang *cybercriminal* mungkin meninggalkan stik USB yang penuh dengan malware ditempat dimana target akan melihatnya yang sudah di labeli dengan kata-kata menarik seperti "rahasia" atau "bonus". Target yang mengambil umpan akan mengambil USB tersebut dan menghubungkannya ke komputer untuk melihat apa yang ada didalamnya. Malware akan kemudian secara otomatis menginjeksi dirinya ke komputer.
2. *Phising*. *Phising* adalah cara terkenal untuk mengambil informasi dari korban. Pelaku biasanya mengirim email atau teks ke target, mencari informasi

yang dapat membantu kejahatan yang lebih signifikan.

3. *Email hacking & contact spamming*. Beberapa pelaku mengambil keuntungan dengan mencoba memerintahkan akun email dan daftar kontak akun spam. Contoh. Jika seorang teman mengitim email dengan subjek "Lihatlah situs ini", mungkin kita tidak akan berfikir dua kali untuk membukanya. Dengan mengambil alih akun email seseorang, pelaku dapat membuat mereka yang ada di daftar kontak percaya bahwa mereka menerima email dari seseorang yang mereka kenal. Tujuannya adalah menyebarkan malware dan menipu orang-orang dari data mereka.
4. *Pretexting*. Pelaku menggunakan dalih yang menarik untuk menipu korban. Katakanlah Anda menerima email, menyebut Anda sebagai penerima wasiat. Email meminta informasi pribadi Anda untuk membuktikan bahwa Anda adalah penerima sebenarnya dan untuk mempercepat transfer warisan Anda. Sebaliknya, Anda berisiko memberi penipu kemampuan untuk tidak menambahkan ke rekening bank Anda, tetapi untuk mengakses dan menarik dana Anda.
5. *Quid pro quo*. Penipuan jenis ini melibatkan pertukaran tertentu. Pelaku mencoba membuat korban

percaya bahwa pertukaran itu adil. Contoh Scammer dapat memanggil target, berpura-pura menjadi teknisi dukungan TI. Korban mungkin menyerahkan kredensial masuk ke komputer mereka, mengira mereka menerima dukungan teknis sebagai imbalan. Sebagai gantinya, scammer sekarang dapat mengendalikan komputer korban, memuatnya dengan malware atau, mungkin, mencuri informasi pribadi dari komputer untuk melakukan pencurian identitas.

6. *Vishing*. *Vishing* adalah versi suara phishing. "V" adalah singkatan dari *voice*, tetapi sebaliknya, upaya penipuannya sama. Penjahat menggunakan telepon untuk menipu korban agar menyerahkan informasi yang berharga. Contoh Seorang penjahat mungkin memanggil seorang karyawan, menyamar sebagai rekan kerja. Penjahat mungkin menang atas korban untuk memberikan kredensial masuk atau informasi lain yang dapat digunakan untuk menargetkan perusahaan atau karyawannya.

F. Prinsip-prinsip Keamanan

7 prinsip dasar pada keamanan sistem (Stoneburner, dkk., 2004) adalah sebagai berikut:

Prinsip 1. Menetapkan kebijakan (*policy*) keamanan yang baik sebagai dasar untuk desain sistem.

Kebijakan keamanan merupakan dokumen penting untuk dikembangkan saat mencang sebuah sistem informasi. Dimulai dengan komitmen dasar organisasi untuk keamanan informasi dirumuskan sebagai pernyataan kebijakan umum. Kebijakan tersebut kemudian diterapkan untuk semua aspek desain sistem atau solusi keamanan saat terjadi insiden. Dokumen ini harus mengindentifikasi sasaran keamanan, berisi prosedur, standar, serta protokol yang digunakan sebagai arsitektur keamanan.

Prinsip 2. Perlakukan keamanan sebagai bagian integral dari keseluruhan sistem.

Keamanan haruslah dipertimbangkan saat merancang sebuah sistem informasi. Keamanan akan sulit dan mahal untuk diimplementasikan ketika sistem telah selesai dikembangkan, sehingga harus diintegrasikan sepenuhnya kedalam proses siklus sistem.

Prinsip 3. Perjelas batas keamanan fisik dan logic yang diatur oleh dokumen kebijakan keamanan.

Teknologi informasi berada di 2 area yaitu area fisik dan area logic. Kedua area ini memiliki batasan yang jelas. Mengetahui tentang apa yang harus dilindungi dari factor eksternal dapat memastikan langkah-langkah perlindungan yang dibutuhkan. Oleh karena itu, batasan keamanan harus

dipertimbangkan dan dimasukkan dalam dokumentasi sistem dan dokumen kebijakan keamanan.

Prinsip 4. Pastikan pengembang dilatih tentang cara mengembangkan keamanan perangkat lunak.

Perlu dipastikan bahwa pengembang cukup terlatih dalam pengembangan perangkat lunak yang aman. Hal ini termasuk dalam perancangan, pengembangan, kontrol konfigurasi, integrasi dan pengujian.

Prinsip 5. Kurangi resiko ke tingkat yang dapat diterima.

Resiko didefinisikan sebagai kombinasi dari kemungkinan ancaman tertentu (secara sengaja mengekpoitasi atau tidak sengaja memicu kerentanan sistem) dan dampak buruk yang dihasilkan pada operasi organisasi, asset organisasi, atau individu jika hal ini terjadi. Harus diakui bahwa analisis resiko efektif dari segi biaya. Analisis terhadap biaya dari kemungkinan-kemungikinan insiden keamanan harus dilakukan untuk setiap kontrol yang diusulkan. Tujuannya adalah untuk meningkatkan kemampuan bisnis dengan mengurangi resiko bisnis ke tingkat yang dapat diterima.

Prinsip 6. Asumsikan bahwa sistem eksternal tidak aman.

Secara umum, sistem eksternal seharusnya dianggap tidak aman. Oleh karena itu pengembang harus merancang fitur

keamanan sesdemikian rupa untuk mengatasi permasalahan ini.

Prinsip 7. Identifikasi potensi pertukaran antara pengurakan resiko dengan peningkatan/penurunan biaya dalam aspek lain efektivitas operasional.

Prinsip ini berhubungan dengan prinsip nomor 4. Untuk memenuhi persyaratan keamanan maka perancang sistem perlu mengidentifikasi dan menangani semua kebutuhan operasional. Dalam memodifikasi tujuan keamanan, resiko biaya yang lebih besar mungkin tidak bisa dihindari. Dengan mengidentifikasi dan mengatasi maslaah keamanan sedini mungkin, maka akan tercapai sistem yang lebih efektif.

Diskusi

Di antara tantangan mendasar dalam keamanan informasi adalah *confidentiality* (kerahasiaan), *integrity* (integritas), dan *availability* (ketersediaan), atau CIA. Berikan contoh di mana kerahasiaan diperlukan, tapi tidak integritas. Berikan contoh di mana integritas diperlukan, tetapi bukan kerahasiaan. Berikan contoh di mana ketersediaan adalah perhatian utama.

Bab III Keamanan Jaringan

A. TIU

Setelah membaca materi ini diharapkan mahasiswa mampu:

1) Memahami konsep dasar jaringan komputer
2) Memahami konsep *trusted guards*, *gateways* dan *firewall*
3) Memahami konsep keamanan dalam LAN (*Local Area Network*)
4) Memahami konsep kemanan dalam WAN (*Wide Area Network*)

B. Konsep Dasar Jaringan Komputer

Keamanan jaringan komputer sebagai bagian dari sebuah sistem sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunaannya. Sistem keamanan jaringan komputer harus dilindungi dari segala macam serangan dan usaha-usaha penyusupan atau pemindaian oleh pihak yang tidak berhak.

Sistem deteksi penyusup jaringan yang ada saat ini umumnya mampu mendeteksi berbagai jenis serangan tetapi tidak mampu mengambil tindakan lebih lanjut. Selain itu sistem juga tidak memiliki interaktivitas dengan administrator pada saat administrator tidak sedang

mengadministrasi sistemnya. Hal ini merupakan suatu hal yang tidak efektif terutama pada saat sistem berada dalam kondisi kritis.

Selain itu sistem pertahanan terhadap aktivitas gangguan saat ini umumnya dilakukan secara manual oleh administrator. Hal ini mengakibatkan integritas sistem bergantung pada ketersediaan dan kecepatan administrator dalam merespons gangguan. Apabila terjadi malfungsi, administrator tidak dapat lagi mengakses sistem secara *remote* sehingga tidak akan dapat melakukan pemulihan sistem dengan cepat.

Oleh karena itu dibutuhkan suatu sistem yang dapat menanggulangi ancaman yang mungkin terjadi secara optimal dalam waktu yang cepat dan secara otomatis sehingga memungkinkan administrator mengakses sistem walaupun terjadi malfungsi jaringan. Hal ini akan mempercepat proses penanggulangan gangguan serta pemulihan sistem atau layanan.

Jaringan komputer adalah sistem yang terdiri atas dua atau lebih komputer serta perangkat-perangkat lainnya yang saling terhubung. Media penghubung tersebut dapat berupa kabel atau nirkabel sehingga memungkinkan para pengguna jaringan.

Komputer melakukan pertukaran informasi seperti berbagai file, dokumen, data serta menggunakan perangkat keras atau perangkat lunak yang terhubung ke jaringan.

C. Jenis-jenis Jaringan Komputer

Berdasarkan jangkauan area atau lokasi, jaringan dibedakan menjadi beberapa jenis yaitu:

1) *Personal Area Network* (PAN)

Gambar 3. Personal Area Network)
(sumber: educba.com)

Personal Area Network (PAN) yaitu saat anda menghubungkan komputer atau perangkat lain seperti handphone, *personal digital assistant*, keyboard, mouse, headset wireless, kamera dan peralatan lain yang jaraknya cukup dekat sekitar 4-6 meter, maka anda telah membentuk suatu sistem jaringan pribadi atau PAN. Dalam hal ini yang paling penting adalah anda sendiri yang mengendalikan (*authority*) pada semua peralatan

tersebut. Selain dihubungkan langsung ke port USB atau FireWire, Personal Area Network (PAN) juga sering dibentuk dengan teknologi *wireless* atau nirkabel seperti bluetooth, infrared atau WIFI.

2) *Local Area Network* (LAN)

Gambar 4. Local Area Network (LAN)
(sumber: qtera.co.id)

Local Area Network (LAN) adalah jaringan yang dibatasi oleh area yang relatif kecil. Jaringan jenis ini biasanya menghubungkan antara komputer satu dengan komputer lainnya atau bisa juga node satu dengan node lainnya. Daerah jangkauan *Local Area Network* (LAN) tidaklah terlalu jauh, misal dalam suatu ruangan atau satu area dengan radius antara 100 meter sampai 2.000 meter, tergantung dari jenis kabel yang digunakan. Penerapan jaringan jenis ini biasanya dibangun untuk perkantoran skala kecil atau Usaha Kecil Menengah (UKM). Jika diterapkan pada perusahaan besar maka penggunaanya

hanya akan diletakkan dalam ruang lingkup kecil, seperti per-ruangan atau per-kantor.

a. VLAN (Virtual Local Area Network)

Suatu model jaringan yang tidak terbatas pada lokasi fisik seperti LAN, hal ini mengakibatkan suatu network dapat dikonfigurasi secara virtual tanpa harus menuruti lokasi fisik peralatan. Penggunaan VLAN akan membuat pengaturan jaringan menjadi sangat fleksibel dimana dapat dibuat segmen yang bergantung pada organisasi atau departemen,tanpa bergantung pada lokasi workstation.

b. Firewall

Suatu cara/sistem/mekanisme yang diterapkan baik terhadap *hardware*, *software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah workstation, server, router, atau local area network (LAN) anda.

c. Port Security

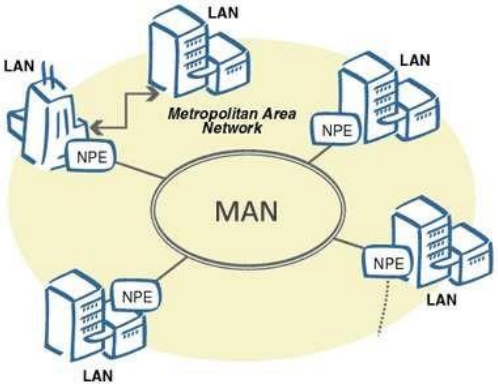
Port security adalah sebuah trafik kontrol yang bekerja di layer 2 data link. berfungsi untuk mendaftarkan dan membatasi perangkat end devices

mana saja yang dapat terkoneksi pada suatu port di switch tersebut.

d. RADIUS/TACACS Server TACACS (Terminal Access Controller Access-Control SystemServer)

Merupakan protokol yang menyediakan layanan akses kontrol pada router, switch, dan peralatan jaringan lainnya digunakan untuk mempermudah dalam pengelolaan authentikasi, *authorization* dan accounting menjadi terpusat. Bayangkan jika kita mempunyai banyak router atau switch, jika kita ingin mengganti *password* maka akan memerlukan waktu yang banyak jika mengganti satu persatu maka disinilah Server TACACS berperan.

3) *Metropolitan Area Network* (MAN)

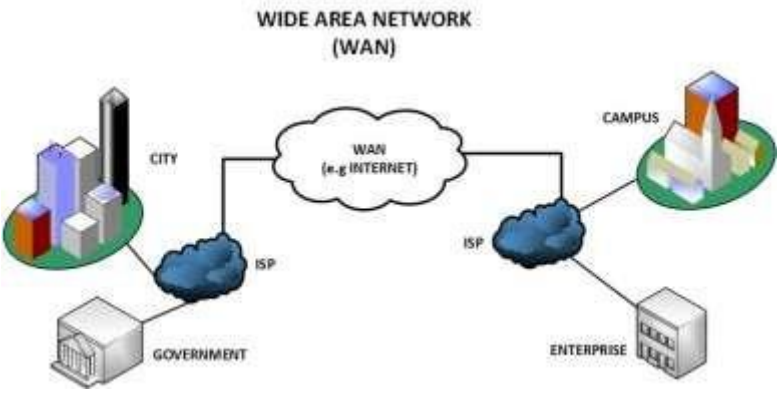


Gambar 5. Metropolitan Area Network (MAN)
(sumber: presburner.com)

Metropolitan Area Network (MAN) adalah jaringan komputer yang memiliki area yang lebih besar dari *Local Area Network* (LAN), biasanya antar wilayah dalam stu provinsi. Jaringan *Metropolitan Area Network* (MAN) menghubungkan beberapa buah jaringan kecil ke dalam lingkungan area yang lebih besar. Jika suatu instansi atau perusahaan memiliki cabang dalam kota atau provinsi dengan jarak antara 10-50 km, dan setiap cabang saling berhubungan untuk bertukar data dan informasi, maka jaringan ini disebut *Metropolitan Area Network* (MAN).

4) *Wide Area Network* (WAN)

Wide Area Network (WAN) merupakan gabungan dari *Local Area Network* (LAN) dan *Metropolitan Area Network* (MAN), yang telah mengalami perkembangan infastruktur jaringan sehingga jarak cakupannya semakin jauh yaitu dunia. Sebuah WAN memiliki ruang lingkup yang sangat besar dan sudah menggunakan sarana satelit, wireless, ataupun kabel fiber optik. Jika anda ingin menggunakan jaringan WAN, anda membutuhkan jaringan lain yang dimiliki perusahaan yang bergerak pada bidang komunikasi, misalnya Telkom. Infastruktur yang digunakan oleh jaringan ini bisa lebih murah bila dibandingkan dengan jaringan MAN. Namun, ada biaya tambahan yang harus anda bayar untuk setiap bulan atau tahunnya.



Gambar 6. Wide Area Network (WAN)
(sumber: snabaynetworking.com)

Langkah instalasi sistem keamanan jaringan dapat membantu menghentikan pengguna tidak sah atau penyusup untuk mengakses bagian jaringan komputer. Keamanan jaringan berfungsi untuk mengantisipasi risiko berupa ancaman fisik maupun logic baik secara langsung maupun tidak langsung.

a. Memasang filter di router dengan memanfaatkan infress serta angress filtering. Cara ini merupakan langkah awal dalam mempertahankan diri serta mengantisipasi serangan spoofing.
b. Melakukan enkripsi dan autentifikasi, dengan melakukan hal ini juga dapat mengatasi dan mengantisipasi serangan spoofing dengan mengimplemantasi autentifikasi dan enkripsi data.
c. Memasang firewall

d. Memasang IDS atau intrusion Detection System
e. Memasang jaringan secara regular
f. Melakukan autentifikasi host yang akan dihubungi. Model ini banyak dipakai dengan mempergunakan sertifikat digital. Dengan ini, seseorang dapat meyakinkan bahwa *host* yang diakses merupakan *host* yang sebenarnya.
g. Tidak melakukan aktivitas yang bersifat rahsaia pada jaringan yang belum dikenal.

5) Jaringan nirkabel (*Wireless*)

Jaringan tanpa kabel (*wireless*) atau jaringan nirkabel merupakan suatu jalan keluar terhadap komunikasi yang tidak bisa dilakukan dengan jaringan yang menggunakan kabel. Pada saat ini jaringan nirkabel atau *wireless* sudah banyak digunakan dengan memanfaatkan jasa satelit dan bahkan mampu memberi kecepatan akses yang lebih cepat bila dibandingkan dengan jaringan yang menggunakan kabel.

Gambar 7. Jaringan Nirkabel (*wireless*)
(sumber: networkencylopedia.com)

D. Keamanan Jaringan Komputer

Di lansir dari Securelist Bulletin milik Kaspersky Lab, menyatakan bahawa Indonesia termasuk kedalam 10 peringkat Negara yang paling banyak mendapat serangan pada jaringan per-bulan Mei 2020.

Gambar 8. Peta Sebaran Serangan Jaringan (sumber: Kaspersky Security Bulletin)

Top Countries

1	Cayman Islands	50.31%
2	Federal Democratic Republic of Ethiopia	18.23%
3	People's Republic of China	16.95%
4	Islamic Republic of Iran	16.67%
5	Republic of Suriname	16.37%
6	Republic of the Sudan	14.57%
7	Republic of Seychelles	13.97%
8	Islamic Republic of Pakistan	13.73%
9	Republic of Indonesia	12.47%
10	Socialist Republic of Vietnam	12.43%

Top Infections

1	Bruteforce.Generic.Rdp.d	16,96%
2	Intrusion.Win.MS17-010.o	9,74%
3	Bruteforce.Generic.Rdp.a	5,31%
4	Intrusion.Win.MS17-010.p	2,83%
5	Scan.Generic.PortScan.TCP	2,44%
6	Scan.Generic.PortScan.UDP	1,98%
7	DoS.Generic.Flood.TCPSYN	0,86%
8	Bruteforce.Generic.RDP	0,27%
9	Bruteforce.Generic.Rdp.c	0,19%
10	Intrusion.Win.NETAPI.buffer-overflow.exploit	0,11%

Data diatas menunjukkan bahawa Indonesia masih lemah dalam hal keamanan jaringan dan kerap kali dijadikan target dari intruder. Keamanan jaringan komputer sebagai bagian dari sebuah sistem informasi adalah sangat penting untuk menjaga validitas dan integritas data serta menjamin ketersediaan layanan bagi penggunanya. Sistem harus dilindungi dari segala macam serangan dan usaha penyusupan atau pemindaian pihak yang tidak berhak.

Komputer yang terhubung ke jaringan mengalami ancaman keamanan yang lebih besar daripada *host* yang tidak terhubung keamanan. Dengan mengendalikan keamanan jaringan, resiko tersebut dapat dikurangi. Namun keamanan jaringan biasanya bertentangan dengan akses jaaringan, karena bila akses jaringan semakin mudah, keamanan jaringan akan semakin rawan. Bila keamanan jaringan main baik, *network access* semakin terbatas. Suatu jaringan didesain sebagai komunikasi data *highway* dengan tujuan meningkatkan akses ke sistem komputer, sementara keamanan dirancang untuk mengontrol akses. Penyediaan keamanan jaringan adalah sebagai penyeimbang antara *open access* dengan keamanan.

E. Konsep Trusted Guards, Gateways dan Firewall

1) Trusted Guards

Trusted guards adalah tipe khusus firewall yang dibangun pada trusted sistem. Bahkan setiap elemen itu harus memenuhi persyaratan, *trusted guard* juga berbeda dari firewall normal bahwa mereka dirancang untuk memenuhi Mandatory Access Control (MAC) pada lalu lintas jaringan, data, file dan objek lain. Hal ini dicapai melalui proxy pada layer aplikasi dan pelabelan data, dimana semua data bergerak dari satu domain ke domain lain melalui firewall diberi label dengan klasifikasi tertentu, dan tidak diizinkan untuk pindah ke tingkat yang lebih rendah dari klasifikasi tanpa otoritas sebelumnya. Hal ini juga disebut sebagai perpindahan dari sisi tinggi ke sisi rendah penjaga yang akan mencoba untuk memindahkan data rahasia ke suatu daerah yang tidak diizinkan untuk data rahasia. *Trusted guards* utamanya digunakan dalam lingkungan yang memerlukan klasifikasi, tetapi juga dapat digunakan dalam lingkungan non pemerintah di mana persyaratan keamanan data mungkin lebih ketat.

2) Gateways

Gateway adalah sebuah perangkat yang digunakan untuk menghubungkan satu jaringan komputer dengan satu atau lebih jaringan komputer yang menggunakan

protokol komunikasi yang berbeda sehingga informasi dari satu jaringan komputer dapat diberikan kepada jaringan komputer lain yang protokolnya berbeda

3) Firewall

Firewall merupakan suatu cara/sistem/mekanisme yang diterapkan baik terhadap *hardware*, *software* ataupun sistem itu sendiri dengan tujuan untuk melindungi, baik dengan menyaring, membatasi atau bahkan menolak suatu atau semua hubungan/kegiatan suatu segmen pada jaringan pribadi dengan jaringan luar yang bukan merupakan ruang lingkupnya. Segmen tersebut dapat merupakan sebuah *workstation, server*, router, atau *local area network* (LAN).

Firewall secara umum di peruntukkan untuk melayani:

a. Mesin/komputer: setiap individu yang terhubung langsung ke jaringan luar atau internet dan menginginkan semua yang terdapat pada komputernya terlindungi.
b. Jaringan: jaringan komputer yang terdiri lebih dari satu buah komputer dan berbagai jenis topologi jaringan yang digunakan, baik yang dimiliki oleh perusahaan, organisasi dsb.

Karakteristik Firewall:

a. Seluruh hubungan/kegiatan dari dalam ke luar harus melewati firewall. Hal ini dapat dilakukan dengan cara memblok/membatasi baik secara fisik semua akses terhadap jaringan lokal, kecuali melewati firewall. Banyak sekali bentuk jaringan yang memungkinkan.
b. Hanya kegiatan yang terdaftar/ dikenal yang dapat melewati atau melakukan hubungan, hal ini dapat dilakukan dengan mengatur *policy* pada konfigurasi keamanan lokal. Banyak sekali jenis firewall yang dapat dipilih sekaligus berbagai jenis policy yang ditawarkan.
c. Firewall itu sendiri haruslah kebal atau relatif kuat terhadap serangan/kelemahan. Hal ini berarti penggunaan sistem yang dapat dipercaya dan dengan sistem operasi yang relatif aman.

Diskusi

RFID adalah perangkat yang sangat kecil yang mampu memancarkan nomor melalui internet yang dapat dibaca oleh sensor terdekat. Diperkirakan bahawa RFID akan digunakan disemua jenis barang, seperti uang, pakaian, dan sebagainya. Misalkan, seseorang dikelilingi oleh "*cloud*" dari nomor RFID yang akan memberikan banyak informasi tentang orang tersebut.

Diskusikan beberapa masalah *privacy* dan keamanan yang mungkin timbul.

Bab IV Keamanan Sistem Operasi (Windows & Linux)

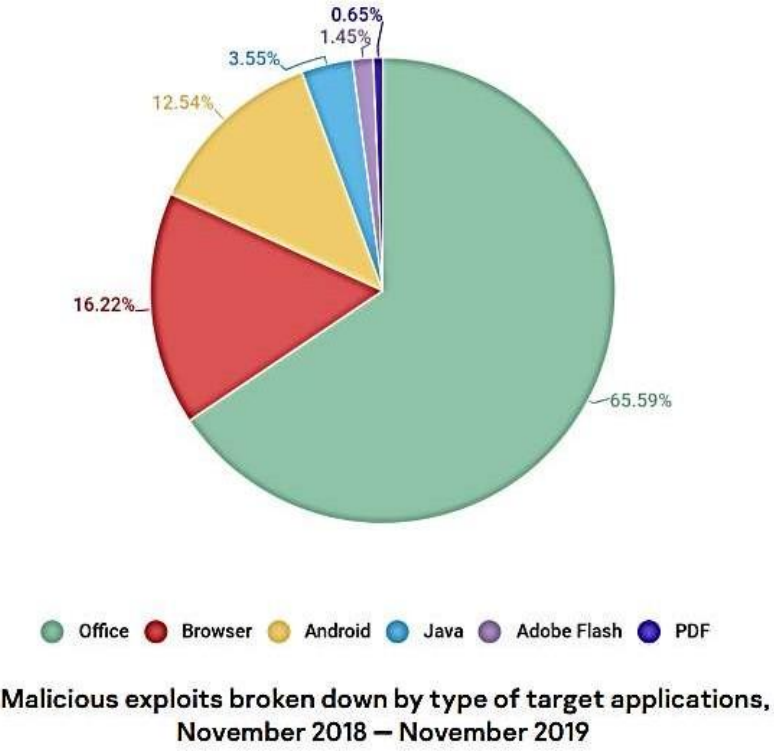
A. TIU

Setelah membaca materi ini mahasiswa diharapkan mampu:

1) Memahami model-model keamanan dalam sistem operasi
2) Memahami perancangan sistem operasi yang aman
3) Mengenali bentuk serangan terhadap sistem operasi Windows dan Linux
4) Melakukan evaluasi terhadap sistem operasi Windows dan Linux

B. Keamanan pada Sistem Operasi

Sebuah bulletin yang dilaporkan oleh Kaspersky Lab menyatakan bahwa sepanjang tahun 2019 merupakan tahun yang banyak mendapatkan serangan di subsistem desktop jarak jauh di versi sistem operasi windows. Statistik aplikasi yang paling rentan adalah Microsoft Office dengan persentase 65,59%.



Gambar 9. Serangan Malware Terhadap Aplikasi Komputer (sumber: Kaspersky Security Bulletin, 2019)

Keamanan pada sistem operasi merupakan kebutuhan yang sangat utama dan penting, bayangkan jika sebuah sistem operasi tidak dilengkapi dengan keamanan yang mumpuni, maka sistem operasi yang ada pada komputer tersebut akan selalu mendapat serangan dari virus, spam, worm, dan lain-lain.

Sistem operasi hanya satu porsi kecil dari seluruh perangkat lunak di suatu sistem. Tetapi karena peran sistem operasi mengendalikan pengaksesan ke sumber daya, dimana perangkat lunak lain meminta pengaksesan, maka sistem operasi menempati posisi yang penting dalam pengamanan sistem.

Dengan mempelajari cara penanganan virus dengan memahami kinerja sistem keamanan pada sistem operasi yang digunakan, setidaknya kita dapat menyelamatkan data- data penting sebelum hilang atau rusak karena adanya virus worm tersebut.

C. Perancangan Sistem Operasi yang Aman

Mencegah hilangnya data dan mencegah masuknya penyusup merupakan aspek dasar yang harus dipertimbangkan saat merancang sistem. Ada beberapa lapisan keamanan pada sistem operasi, yaitu:

a. Lapisan fisik.

   Pada lapisan ini keamanan yang dilakukan merupakan pengamanan secara langsung terhadap perangkat. Beberapa diantaranya seperti membatasi akses fisik ke mesin dengan menyediakan akses masuk khusus ke ruangan komputer, penguncian komputer secara hardware, keamanan BIOS, keamanan Bootloader. Untuk mengatasi terjadinya insiden pada lapisan ini dapat

dilakukan dengan *back-up* data: pemilihan piranti *back- up* (missal: hardisk external) dan melakukan penjadwalan *back-up* data. Sedangkan untuk mendeteksi gangguan fisik dapat dilakukan menggunakan log file. Seperti log yang pendek atau tidak lengkap, log yang berisikan wkatu yang aneh, log dengan kepemilikan yang tidak tepat, catatan *reboot* atau *restart*, log yang hilang, dan sebagainya. Dapat diminimalisir dengan mengontrol akses ke sumber daya (*resource*).

b. Keamanan lokal

Pada lapisan ini berkaitan dengan user dan hak- haknya seperti memberi user fasilitas minimal yang diperlukan, hati-hati terhadap saat/dari mana user login, atau tempat seharusnya user login, pastikan dan hapus rekening mereka ketika mereka tidak lagi membutuhkan akses.

c. Keamanan root

Ketika melakukan perintah yang kompleks, cobalah dalam cara yang tidak merusak dulu, terutama perintah yang menggunakan globbing: contoh, saat ingin melakukan "rm foo*.bak", pertama coba dulu: "ls foo*.bak".

Beberapa orang merasa terbantu ketika melakukan "touch /-i" pada sistem mereka. Hal ini akan membuat perintah-perintah seperti : "rm -fr *" menanyakan apakah

benar-benar ingin menghapus seluruh file. Selanjutnya yaitu hanya mengggunakan root ketika melakukan tugas tunggal tertentu. Untuk mengetahui bagaimana melakukan sesuatu, kembali ke shell user normal hingga yakin apa yang perlu dilakukan oleh root.

Jalur perintah untuk pemakai root sangat penting. Jalur perintah, atau variabel lingkungan PATH mendefinisikan lokal 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. Sebagai tambahan, jangan pernah menaruh direktori yang dapat ditulis pada jalur pencarian, karena hal ini memungkinkan penyerang memodifikasi atau menaruh file biner dalam jalur pencarian, yang memungkinkan penyerang tersebut menjadi root ketika perintah tersebut dijalankan.

Selain itu jangan pernah menggunakan seperangkat utilitas rlogin/rsh/rexec (disebut utilitas r) sebagai root. Karena utilitas tersebut menjadi sasaran banyak serangan, dan sangat berbahaya bila dijalankan sebagai root. Jangan membuat file .rhosts untuk root. Dan juga selalu perlahan dan berhati-hati ketika berlaku menjadi root

d. Keamanan file dan sistem file

Beberapa cara yang dapat dilakukan untuk melakukan pengamanan pada lapisan ini seperti *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, writa, execute bagi user maupun group, selalu cek program-program yang tidak dikenal.

e. Keamanan *password* dan enkripsi

Pada keamanan *password* dan kernel merupakan keamanan mendasar yang sebaiknya diimplementasikan oleh semua pengguna. Hal-hal yang harus diperhatikan yaitu berhati-hati terhadap *bruto force attack* dengan membuat *password* yang baik, selalu mengenkripsi file yang dipertukarkan, lakukan pengamanan pada level tampilan, seperti *screen saver.*

f. Keamanan kernel

Kernel harus selalu *update* dan mengikuti *review* terhadap *bugs* atau kekurangan-kekurangan pada sistem operasi.

g. Keamanan jaringan

Keamanan ini secara umum dapat dilakukan dengan mewaspadai paket sniffer yang sering menyadap port Ethernet, melakukan prosedur untuk mengecek integritas data, memverifikasi informasi DNS, melindungi *network*

file system, gunakan firewall untuk barrier antara jaringan privat dengan jaringan eksternal.

D. Tinjauan Sistem Operasi yang Aman (Windows)

a. Windows Firewall

Pada tahun 2001 Windows firewall pertama kali diperkenalkan ke OS WindowsXP, dan sejak saat itu Windows Firewall terus mengalami peningkatan baik dari segi fitur maupun keamanan. Windows Firewall merupakan salah satu elemen terpenting dari OS Windows. Sebelumnya nama Windows Firewall adalah Internet Connection Firewall, namun sudah dirubah sejak Microsoft mengeluarkan Service Pack 2 untukWindows XP.

Pada versi pertama Windows Firewall, Windows Firewall hanya mampu untuk memfilter & memblok koneksi yang masuk. Kemudian Fitur Windows Firewall terus ditingkatkan seperti mengontrol koneksi keluar dari suatu aplikasi serta user juga mampu mengatur Windows Firewall dengan cukup mudah. Program-program pada Windows ini akan secara otomatis membuat sebuah Rules/Aturan di dalam Windows Firewall sehingga program tersebut bisa melakukan Update. Namun apabila ada kejadian mencurigakan, Windows Firewall akan memberitahu pengguna dengan sebuah Window / Jendela

apakah aplikasi tersebut layak untuk terkoneksi kejaringan atau tidak.

b. Windows Update

Windows update memeriksa update yang diberikan oleh Microsoft untuk memberi patch atau menambal celah pada Windows 7. Update Windows biasanya dilakukan secara bertahap. Setelah update yang pertama, akan ada lagi update selanjutnya dan begitu seterusnya sampai keberadaan celah menjadi seminimal mungkin di Windows 7. Untuk melihat update apa saja yang sudah di tambahkan, kamu bisa klik View Update History pada Windows Update

c. Windows Defender

Windows Defender adalah *software* antivirus internal yang sudah disediakan Windows secara gratis. Antivirus ini juga tidak kalah dengan antivirus hebat lainnya seperti Avast, Avira, AVG. atau apapun antivirus yang terkenal dan biasanya berbayar. Windows Defender pada windows 8, akan selalu melakukan pengecekan *update software* ketika sedang online.

d. Windows Hello

Windows Hello adalah fitur yang memungkinkan penggunanya untuk login ke dalam windows dengan menggunakan deteksi wajah, iris dan sidik jari untuk membuka *device*.

e. Bitlocker

BitLocker Drive Encryption adalah sebuah fitur enkripsi satu cakram penuh yang terdapat di dalam sistem operasi Microsoft Windows Vista, Windows 7 dan Windows Server 2008 yang di desain untuk melindungi data dengan melakukan enkripsi terhadap keseluruhan partisi. Secara default, BitLocker Drive Encryption menggunakan algoritma AES dalam mode CodeBlock Chaining (CBC) dengan panjang kunci 128-bit, yang di gabungkan dengan Elephant Diffuser untuk meningkatkan keamanannya. Pada Windows Vista dan Windows 7, perangkat lunak ini hanya tersedia di edisi Ultimate dan Enterprise, dan tidak ada pada edisi-edisi lainnya. Pada saat WinHEC 2006, Microsoft mendemonstrasikan versi pra-rilis dari Windows Server 2008 yang mengandung dukungan terhadap partisi berisi data yang diamankan oleh BitLocker selain tentunya partisi berisi sistem operasi.

E. Tinjauan Terhadap Sistem Operasi yang Aman (Linux)

Mengevaluasi keamanan sistem informasi linux yang anda miliki. Meski sebuah system informasi sudah dirancang memiliki perangkat pengamanan, dalam operasi masalah

keamanan harus selalu dimonitor. Hal ini disebabkan oleh beberapa hal, antara lain:

a. Ditemukannya lubang keamanan (security hole) yang baru. 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.
b. Kesalahan konfigurasi. 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 tidaksengaja diubah sehingga dapat diubah atau ditulis oleh orang-orang yang tidak berhak
c. Penambahan perangkat baru (*hardware* dan/atau *software*) yang menyebabkan menurunnya tingkat keamanan atau berubahnya metode untuk mengoperasikan sistem linux anda. 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).

Dari sekian banyak jenis sistem operasi, Linux merupakan OS yang aman terhadap virus, karena selain

jumlah virus pada OS ini sangatlah minim sekali, OS linux melakukan pengelolaan keamanan yang sangat ketat sehingga biasanya akan membuat virus tidak mampu beroperasi/berjalan pada OS Linux ini, dengan begitu user bisa langsung menghapus virus dengan mudah melalui tombol delete.

Linux juga memiliki kemampuan melakukan Perbaikan bug atau yang cacat dengan sangat cepat. Hal ini dikarenakan Linux dikembangkan oleh sebuah komunitas linux, dimana pada komunitas linux dapat memberikan saran dan melakukan perbaikan *bug* atau cacat dengan melalui dokumentasi.

Diskusi

Apa maksud dari suatu sistem dapat "dipercaya (*trusted*)"? apakah Anda setuju bahwa hanya sistem yang dipercaya yang dapat "merusak" keamanan? Mengapa?

Bab IV Keamanan Database

A. TIU

1) Memahami teknik-teknik pengamanan database yang handal
2) Mengenali perlindungan terhadap data yang sensitif
3) Merangkum masalah-masalah keamanan dalam penggunaan database
4) Memahami konsep database multilevel
5) Memahami konsep keamanan bertingkat dalam database

B. Konsep Dasar Keamanan Database

Database atau basis data merupakan salah satu perangkat yang sangat vital bagi sebuah organisasi. Karena database mengandung informasi yang sangat sensitif yang harus dilindungi dari kerentanan dan eksploitasi keamanan. Seluruh perangkat organisasi harus bekerja terus menerus untuk mengidentifikasi dan memulihkan kerentanan tersebut dengan menggunakan berbagai alat yang tersedia. Selain itu, penting untuk melakukan analisis dan audit untuk memastikan bahwa postur keamanan basis data tetap baik, dan juga menunjukkan kepatuan terhadap dokumen kebijakan yang menuntuk tingkat keamanan tinggi.

Keamanan database merupkan suatu cara untuk melindungi database dari ancaman, baik dalam bentuk yang disengaja maupun bukan. Artian ancaman disini berarti segala situasi yang sifatnya mempengaruhi sistem atau bahkan merugikan. Pada sebuah sistem database dikenal istilah administrator database. Administrator database memegang peranan penting karena mempunyai hak untuk mengontrol dan mengatur database.

Hampir semua organisasi menggunakan database dalam beberapa bentuk untuk melacak informasi seperti catatan pelanggan dan transaksi, informasi keuangan, dan catatan lainnya (Howard, 2013). Database yang mengandung banyak data sensitive ini dapat dijual atau dicuri yang menyebabkan organisasi tersebut kehilangan bisnis atau reputasi. Terutama jika organisasi tersebut ditemukan melanggar peraturan atau standar industry yang menuntuk tingkat keamanan data yang tinggi, contoh bank.

10 ancaman teratas terkait database menurut Aplication Security, Inc., adalah sebagai berikut:

1. Password yang lemah
2. SQL *injection*
3. Hak user dan grup yang berlebihan
4. Fitur-fitur DBMS yang tidak perlu diaktifkan
5. Manajemen konfigurasi yang rusak

6. *Buffer overflow*
7. Hak istimewa untuk beberapa user
8. Keagalan layanan
9. *Un-patched* RDBMS
10. Data tidak terenkripsi

D. Kategori Keamanan Database

Diambil dari Panduan Penangan Insiden Keamanan Database oleh Badan Pengkajian dan Penerapan Teknologi Kementerian Komunikasi dan Informatika Republik Indonesia Tahun 2014, berikut garis besar kategori keamanan database:

a. Keamanan Server

Perlindungan Server adalah suatu proses pembatasan akses yang sebenarnya pada database dalam server itu sendiri. Menurut Blake Wiedman ini adalah suatu sisi keamanan yang sangat penting dan harus direncanakan secara hati-hati. Ide dasarnya adalah kita tidak dapat mengakses apa yang kita tidak dapat lihat, atau apakah kita ingin database server kita dapat dilihat oleh orang lain. Database bukanlah suatu web server, dimana koneksi yang tidak dikenali tidak diijinkan.

b. Trusted Ip Access

Setiap server harus dapat mengkonfigurasikan alamat ip yang diperbolehkan mengakses dirinya. Sebagaimana tidak

mengijinkan orang lain memasuki rumah seseorang tanpa ijin maka tidak dapat pula mengijinkan semua orang dapat mengakses server dari sebuah organisasi. Jika server melayani suatu web server maka hanya alamat web server itu saja yang dapat mengakses server database tersebut. Jika server database melayani jaringan internal maka hanya alamat jaringanlah yang boleh menghubungi server. Sangat perlu diperhatikan bahwa jangan pernah menggabungkan server database web dengan server database informasi internal perusahaan anda, ini adalah suatu mental yang buruk untuk seorang admin. Trusted Ip Access merupakan server database terbatas yang hanya akan memberi respon pada Ip yang dikenali saja

c. Database Connection

Saat ini semakin banyaknya aplikasi dinamis menjadi sangat menggoda untuk melakukan akses yang cepat bahkan update yang langsung tanpa authentifikasi. Jika kita ingin mengijinkan pemakai dapat mengubah database melalui web page, pastikan memvalidasi semua masukan untuk memastikan bahwa inputan benar, terjamin dan aman.Sebagai contoh, pastikan menghilangkan semua code SQL agar tidak dapat dimasukan oleh user. Jika seorang admin yang membutuhkan koneksi ODBC, pastikan koneksi yang digunakan unik

d. Table Access Control

Kontrol akses table ini adalah salah satu bentuk keamanan database yang sering diabaikan,karena cukup sulit penerapannya. Penggunaan control akses table yang benar dibutuhkan kolaborasi antara system administrator dengan pengembang database. Hal inilah yang sulit dilakukan. Pemberian ijin user untuk mengakses informasi dapat membuat informasi terbuka kepada public. Jika seorang user mengakses informasi apakah akan dilihat menggunakan session yang samaa tau jika tabel digunakan sebagai referensi sistem mengapa ia diberikan ijin selain hak membaca saja.

E. 5 Tahap Keamanan pada Database

Terdapat 5 langkah utama untuk memastikan keamanan database menurut Application Security, Inc.:

1) Pisahkan database sensitif. Pertahankan inventaris yang akurat dari semua database yang digunakan di seluruh organisasi/perusahaan dan identifikasi semua data sensitif yang berada di database tersebut.
2) Eliminasi kerentanan. Terus menerus melakukan identifikasi dan memulihkan kerentanan yang mengekspos database.
3) *Enforce least privileges*. Identifikasi hak pengguna dan menegakkan kontrol akses dan hak istimewa pengguna

untuk membatasi akses hanya pada data minimum yang diperlukan bagi karyawan untuk melakukan pekerjaan.

4) Pantau penyimpangan/anomali. Terapkan kebijakan yang sesuai dan pantau kerentanan yang tidak dapat diperbaiki untuk setiap dan semua kegiatan yang menyimpang dari kegiatan yang diperbolehkan.
5) Tanggapi perilaku yang mencurigakan. Waspada dan tanggapi perilaku abnormal atau mencurigarakan secara *real time* untuk meminimalkan resiko serangan.

E. Best Practice pada Keamanan Database

Langkah pertama untuk memastikan keamanan database adalah dengan mengembangkan rencana keamanan database yang mempertimbangakn penggunaan standar keamanan yang harus dipatuhi oleh organisasi. Sebagai bagian dari pengembangan rencana ini, organisasi harus melakukan inventarisasi semua database dalam lingkungan jaringan organisasi. Hal ini dapat dilakukan secara lebih efisien melalui penggunaan teknologi manajemen kerentanan yang dapat secara otomatis menemukan semua database dan menjalankan pemindaian untuk mengidentifikasi yang mengandung data sensitif, seperti data keuangan dan data pelanggan.

Penilaian yang dilakukan oleh teknologi tersebut akan dapat menilai kerentanan database dan kesalah konfigurasi,

mengidentifikasi masalah sepertifi password yang lemah, kontrol akses yang buruk, dan mencari tahu kerentanan mana yang dapat dieksploitasi sehingga dapat memprioritaskan perbaikan terhadap kesalahan/kerentanan tersebut.

Teknologi seperti Database Activity Monitoring (DAM) akan membantu dalam proses mengurangi kerentanan dengan memberikan visibilitas secara *real time* ke semua aktivitas database. Data akan dikumpulkan dan dianalisis untuk mencari kegiatan yang melanggar kebijakan keamanan atau yang mengindikasikan anomali terjadi.

Langkah penting lain yaitu memastikan penggunaan *password* yang baik (*strong password*) yang digunakan untuk mengenkripsi data. Sering kali password bawaan (*default password*) tidak diubah oleh pengguna sehingga bisa menjadi salah satu penyebab anomali terjadi. Untuk tahapan lebih lanjut dalam melindungi data/informasi, maka semua data harus disimpan dalam database dalam keadaan yang sudah terenkripsi, dengan catatan akses ke kunci enkripsi terkontrol dan dipantau dengan ketat.

Salah satu aspek lain yang perlu dipertimbangkan dalam menjaga keamanan database adalah dengan pelatihan keamanan dan kesadaran karyawan. Hal ini dilakukan untuk memastikan bahwa semua karyawan mengetahui kebijakan keamanan organisasi dan praktik terbaik yang disyaratkan.

Pelatihan yang berkelanjutan dianggap sebagai praktik terbaik dalam mencegah data sensitif terekspos keluar.

Diskusi

Diskusikan dengan rekan Anda seberapa pentingnya *melakukan back-up* database dan berapa jangka waktu untuk menjadwalkan *back-up* data yang paling baik.

Bab V Malicious Software

A. TIU

Setelah mempelajari materi mahasiswa diharapkan mampu:

1) Memahami teknik-teknik perlindungan program terhadap virus.
2) Mengendalikan program terhadap bentuk ancaman dari luar

B. Malware

Secara umum, kita lebih sering menggunakan istilah virus untuk segala hal yang menunjukkan kesalahan pada sistem operasi atau aplikasi. Malicious software atau disingkat malware merupakan perangkat lunak berbahaya yang dapat menggangu atau bahkan merusak komputer, data, dan jaringan kita. Malware bisa dibagi menjadi dua kategori yaitu yang membutuhkan program host (program induk) dan yang independen.

Kategori pertama disebut sebagai parasit yang pada dasarnya adalah potongan program yang tidak dapat “hidup” secara mandiri tanpa aplikasi, utilitas, atau program sistem lain. Virus dan bom logika dijadwalkan dan dijalankan oleh sistem operasi. Contoh dari kategori ini adalah logic bomb dan program bot. Kategori kedua terdiri dari potongan program atau program yang dapat berdiri sendiri /

independen yang ketika dieksekusi dapat menghasilkan satu atau lebih salinan dirinya.

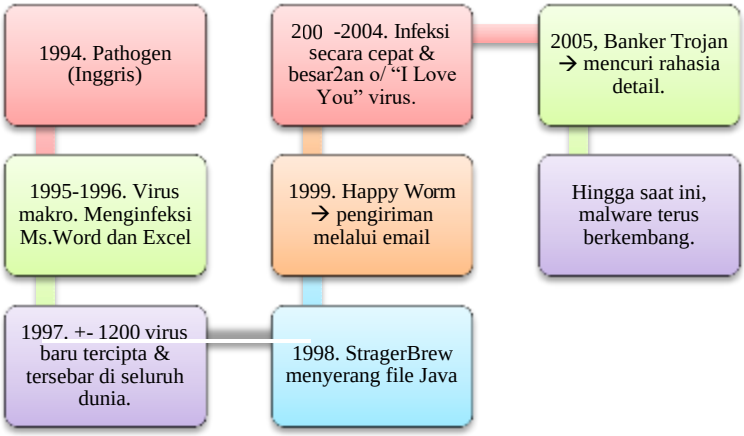
C. Sejarah Malware

Pertama kali digagas oleh Von Neuman pada tahun 1949 dengan mencoba mempraktekkan teori *Self Replication* Automata. Yakni mempresentasikan untuk pertama kalinya kemungkinan untuk mengembangkan program pengganda kecil yang mampu mengendalikan program lain.

Lalu pada tahun 1959 di laboratorium komputer Bell, Morris, McIlroy, dan Vysottsky membuat sebuah permainan yang bernama CoreWare game berdasarkan teori Neuman. Program ini harus saling bersaing untuk menguasai sebanyak-banyaknya memori di komputer lawan. Inilah yang menjadi cikal bakal dari virus.

Pada tahun 1972 Morris menciptakan virus pertama yang dikenal dengan Creeper. Virus ini menginfeksi komputer IBM 360 di jaringan ARPANET (cikal bakal internet). Apabila sebuah komputer terinfeksi maka layar hanya akan menampilkan pesan “Im the creeper, catch me if you can!”. Pada tahun yang sama diciptakanlah sebuah program yang disebut Reaper untuk mengani Creeper. Reaper inilah yang menjadi cikal bakal program antivirus.

Sepanjang tahun 1980, PC semakin popular dan banyak digunakan. Maka semakin banyak pula orang yang mulai bereksperimen dengan program buatan mereka sendiri. Malware-malware ini terus berkembang dan masih menjadi salah satu hal yang sangat mengganggu.



Gambar 10. Perkembangan Malware dari 1994

Sistem operasi yang paling sering menjadi sasaran para pencipta malware adalah sistem operasi Windows 32- bit. Sebuah survey dari Stack Overflow pada tahun 2018 menunjukkan bahwa serangan malware pada Windows mencapai 49.4%, menyusul MacOs 27,4%, Linux 23%, dan BSD/Linux 0,2%.

D. Ragam Malware

1) **Virus**. Merupakan program replikasi diri yang menempel pada perangkat lunak yang sah dan membutuhkan

interaksi pengguna untuk berhasil menginfeksi sistem. Virus dapat menyebar & berkembang didalam sistem komputer serta dapat memperbanyak diri sehingga berkurangnya ruang di memori / hard disk. Pencegahan terhadap virus bisa dilakukan dengan Menghindari membuka lampiran e-mail dari sumber yang tidak diketahui.

2) **Trojan**. jenis malware yang memiliki sifat seperti kuda Trojan. Trojan horse terkenal dalam mitologi Yunani. Dapat berupa program apapun yang menyerupai program yang sah, namun didalamnya memiliki beberapa kode berbahaya. Sifatnya non-replikasi & umumnya parasit artinya membutuhkan program lain untuk menyembunyikan diri. Sebuah Trojan Backdoor, setelah diinstal dapat memungkinkan hacker untuk mengakses secara remote terhadap komputer yang terkena. Mulai dengan mencuri informasi sampai menggunakan komputer untuk mengirimkan spam. Pencegahan Trojan dapat dilakukan dengan menghindari membuka lampiran e-mail dari sumber yang tidak diketahui, menghindari mengunduh software/file secara illegal, memastikan browser selalu dalam kondisi up to date.
3) **Spyware**. Malware ini adalah jenis kode berbahaya yang digunakan utnuk memata-matai kegiatan korban & juga mencuri informasi sensitif. Alat yang paling populer yang

digunakan untuk melakukan pencurian identitas, yang merupakan resiko utama bagi pengguna sistem publik online tanpa adanya jaminan keamanan. Mengumpulkan informasi tanpa persetujuan pengguna & melaporkannya ke penciptanya (username, password, dll)

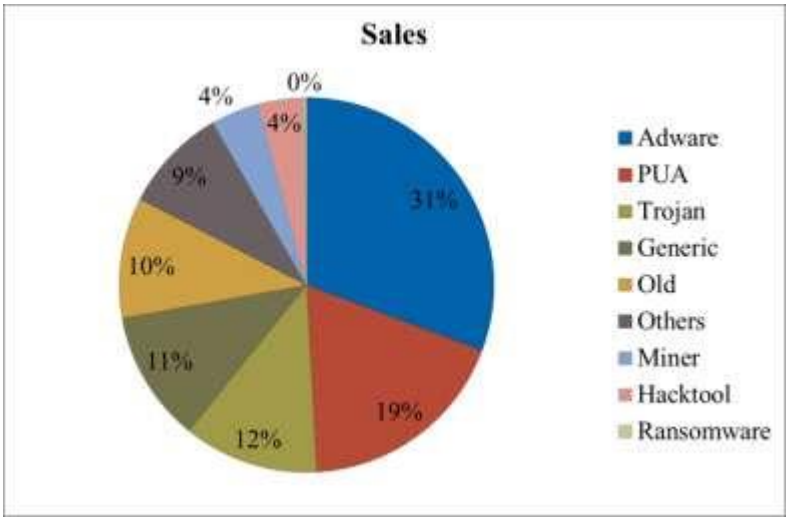
4) **Worm**. Sebuah program replikasi diri yang menggunakan kerentanan dalam jaringan untuk menyebarkan diri. Berbeda dengan virus, worm tidak perlu melampirkan diri ke program lain & tidak memerlukan interaksi pengguna untuk menjalankannya. Pencegahan dapat dilakukan dengan menghindari membuka lampiran e-mail dari sumber yangg tidak diketahui, menghindari unduh software secara illegal, memastikan browser selalu up-to-date, tidak membuka link di email. Sedangkan bila ingin dilakukan penghapusan: karena merambat melalui jaringan, penghapusan bisa menjadi rumit. Setiap mesin yang terinfeksi harus diambil dari jaringan & dibersihkan. Setelah terhubung kembali, harus selalu dipantau agar tidak terinfeksi kembali.
5) **Trapdoor**. Istilah trapdoor dapat berarti pintu masuk alternatif ke dalam sistem. Jenis malware yang digunakan untuk memotong mekanisme keamanan yang ada dibangun ke dalam sistem. Umumnya dibuat oleh programmer untu menguji fungsi kode tertentu dalam waktu yang singkat, sehingga dalam banyak kasus tidak

sengaja tertinggal. Namun, malware ini juga mungkin ditanam oleh penyerang untuk menikmati akses istimewa. Umumnya bersifat non-replikasi malware.

6) **Logic Bomb**. Jenis malware yang mengeksekusi beberapa set instruksi untuk menyerang sistem informasi berdasarkan logika yang didefinisikan oleh penciptanya. Biasanya berupa program yang menggunakan waktu / peristiwa yang baik sebagai pemicu. Ketika kondisi yang ditetapkan dalam set instruksi terpenuhi, kode yang berada di *payload* dijalankan.
7) **Rootkit**. Kumpulan program yang digunakan untuk mengubah fungsi sistem operasi standar. Bertujuan menyembunyikan kegiatan berbahaya yang dilakukan olehnya. Umumnya mengganti utilitas umum seperti kernel, netstat, ls, ps dengan set dari program mereka sendiri, sehingga satu aktivitas yang berbahaya dapat disaring sbelum menampilkan hasilnya pada layar. Dapat dihapus dengan tool anti-rootkit dan juga anti-virus
8) **Bot dan Botnet**. Bot adalah program yang melakukan tidakan berdasarkan instruksi yang diterima dari *controller*nya (tuannya). Jaringan yang digunakan disebut **botnet**. Sering digunakan dalam lingkungan komunitas tertutup untuk menyelesaikan banyak tugas berbahaya dengan teknik remote kontroler.

9) Adware. Program yang berisi promosi dari suatu produk / iklan. Seringkali berisi iklan yang tidak layak dan sangat menganggu.

Kategori malware yang paling banyak terdeteksi di Indonesia (Q1) Tahun 2018 terlihat pada gambar berikut:



Gambar 11. Kategori Malware di Indonesia Q1 2018 (sumber: https://kumparan.com/alfons-tanujaya/statistik-malware-indonesia-q1-2018)

E. Siklus Hidup Malware

Siklus hidup malware berupa 4 tahapan, yaitu:

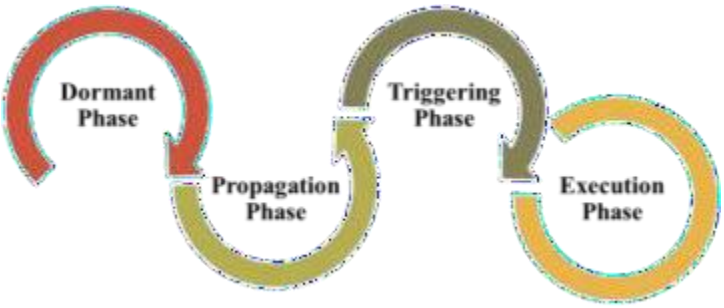
a. **Dormant phase** (fase istirahat/tidur). Pada fase ini, malware tidak aktif. Malware akan diaktifkan oleh kondisi tertentu, misal Tanggal tertentu, kehadiran

program lain / dieksekusinya program lain, dsb. Tidak semua malware malalui fase ini.

b. **Propagation phase** (fase penyebaran). Malware akan mengkopi dirinya ke suatu program / tempat (hardisk, ram, dsb). Setiap program yang terinfeksi akan menjadi hasil "kloningan" dari malware terebut (tergantung cara malware tersebut menginfeksinya).

c. **Trigerring phase** (fase aktif). Pada fase ini malware tersebut akan aktif dan hal ini juga dipicu oleh beberapa kondisi seperti pada Dormant phase.

d. **Execution phase** (fase eksekusi). Pada fase inilah malware yang telah aktif tadi akan melakukan fungsinya. Seperti menghapus file, menampilkan pesan-pesan, dsb.



Gambar 12. Cara Kerja Malware

F. Pencegahan Terhadap malware

Ada hal-hal yang harus diperhatikan bila kita ingin mencegah komputer kita terinfeksi malware. Berikut beberapa diantaranya.

a. Email. Merupakan perantara yang banyak digunakan.

- Berikan perhatian lebih pada SPAM email.
- Jangan membuka spam email dari sumber yang tak jelas. Itulah alasan kenapa Gmail, Ymail, Hotmail menyediakan foleder SPAM.
- Email yang dicurigai dapat merusak komputer karena mengandung virus, malware / sejenisnya.
- Lakukan scan sebelum membuka *attachment*.

b. Internet menjadi media besar dalam penyebarluasan malware.
    - Jangan tergiur dengan pop-up iklan yang muncul tiba-tiba dan menyebutkan Anda memenangkan hadiah/undian
    - Tutup pop-up / sekalian tinggalkan situs tersebut
    - Beberapa program antivirus menyediakan toolbar pencarian khusus seperti AVG Link Scanner.

c. Melakukan scan terlebih dahulu sebelum menyalin (copy) file dari USB . Memory card.
    - Menghindari membuka file yang mencurigakan dalam flashdisk misal file / folder dalam bentuk *shortcut*.

d. Menginstall anti-virus dan melakukan update secara berkala.
    - Bertujuan agar anti-virus dapat mengenali varian virus terbaru.
    - Memasang juga antivirus lokal, karena lebih mengenali varian virus buatan lokal
e. Berhati-hati bila mengunduh file dari situs yang menyediakan file ilegal seperti *cracks, serials, warez*. Situs web ini umumnya dijadikan tempat penyebaran virus, worm dan trojan.
f. Membuat jadwal untuk update dan *scan* hal ini diharapkan dapat meminimalkan kerusakan.
g. Memeriksa *removable media* yang dihubungkan ke komputer (USB, Eksternal untuk transkasi penting seperti oerbankan / jual beli → **HTTPS/SSL**.
h. Tidak mematikan firewall dalam keadaan komputer aktif online terhubung ke internet.
i. Tidak cepat percaya dengan mail yang diterima, memeriksa dengan baik sebelum membuka lampiran dan tidak sembarangan HDD, dll). Karena terdapat aktifasi otomatis begitu *removable media* dihubungkan ke komputer.
j. Mencari situs yang memiliki akses online terenkripsi.
k. Memberikan alamat email ke sembarang website.

Diskusi

Diskusikan kenapa banyak sekali malware yang mengancam keamanan baik data, komputer maupun jaringan dan bagaimana tren malware kedepannya.

Bab VI Kriptografi

A. TIU

Setelah mempelajari materi ini mahasiswa diharapkan mampu:

1) Memahami konsep kriptografi
2) Memahami kriptografi klasik dan modern
3) Memahami kriptografi kunci simetri
4) Memahami kriptografi kunci asimetri

B. Pengertian Kriptografi

Salah satu metode pengamanan yang dapat dilakukan untuk pengamanan pesan adalah dengan menggunakan kriptografi. Kriptografi telah digunakan selama berabad-abad oleh raja dan ratu di Eropa untuk memberi perintah terhadap pasukan perang mereka. Hal ini dilakukan untuk menghindari informasi penting tersebut jatuh ke tangan orang yang salah sehingga dapat membongkar rahasia kerajaan. Ancaman dari para musuh tersebut yang memotivasi untuk melakukan pengkodean dan enkripsi terhadap pesan sehingga dengan kunci yang tepat hanya orang tertentu saja yang dapat membaca pesan tersebut (Singh, 2001).

Kriptografi adalah ilmu yang menggunakan teknik matematika yang berhubungan dengan aspek keamanan informasi (Menezes dkk., 1996). Kriptografi adalah ilmu

yang mempelajari bagaimana membuat pesan yang dikirim dapat sampai kepada penerima dengan aman. Pesan asli yang dimengerti isinya/maknanya dinamakan plainteks. Pesan yang tidak dimengerti, yang merupakan hasil transformasi dari plainteks disebut cipherteks (Schneier, 1996). Sementara itu menurut Arvandi (2005), kriptografi memiliki tiga karakteristik utama yaitu operasi yang digunakan untuk mengubah plainteks ke cipherteks, kunci yang digunakan, dan bagaimana plainteks tersebut di proses.

Kriptografi (*Chryptography*) berasal dari bahasa Yunani yaitu *Kryptos* yang artinya tersembunyi dan *graphien* yang artinya tulisan. Secara harfiah, kriptografi dapat diartikan sebagai tulisan yang tersembunyi atau tulisan yang dirahasiakan. Kriptografi merupakan suatu cara menjaga agar pesan tetap aman dari pihak ketiga (Murtiyasa, 2005). Kriptografi adalah ilmu yang mempelajari dalam merahasiakan pesan. Pesan asli disebut dengan plainteks sedangkan pesan yang telah di sandikan disebut dengan cipherteks. Proses dalam merubah plainteks ke cipherteks disebut dengan enkripsi. Proses merubah cipherteks ke plainteks disebut dengan dekripsi (Arvandi, 2003).

Beberapa istilah yang berhubungan dengan transformasi dari plainteks ke cipherteks diantaranya adalah cipher, kunci, encipher, decipher, kriptanalisis, dan kriptologi. Cipher

adalah algoritma yang digunakan untuk melakukan transformasi plainteks ke cipherteks. Kunci adalah beberapa infomasi kritis yang diperlukan cipher, dimana kunci ini hanya diketahui oleh pengirim dan penerima pesan. Encipher adalah proses mentransformasi plainteks ke cipherteks dengan menggunakan cipher dan kunci. Decipher adalah proses transformasi cipherteks kembali ke plainteks dengan menggunakan cipher dan kunci. Kriptanalisis (*cyptanalysis*) adalah ilmu yang mempelajari prinsip-prinsip atau metode-metode mentransformasikan cipherteks kembali ke plainteks tanpa mengetahui kunci untuk decipher. Sedangkan kriptologi (*cryptology*) adalah ilmu yang berhubungan dengan kriptografi dan kriptanalisis.

Teknik yang digunakan untuk mendekripsi pesan tanpa mengetahui pengetahuan mengenai detail pengenkripsian disebut dengan kriptanalisis (*Cryptanalysis*). Kriptografi dan kriptanalisis selanjutnya disebut dengan kriptologi. Sistem kriptografi terdiri dari 5 bagian (Sadikin, 2012), yakni :

1) Plainteks (M)

Plainteks adalah pesan atau data masukan yang bentuk aslinya dapat dimengerti maknanya. Plainteks merupakan masukan untuk enkripsi.

2) Kunci rahasia (K)

Kunci rahasia juga merupakan masukan untuk enkripsi. Kunci rahasia adalah nilai bebas yang nantinya akan dikenakan terhadap teks asli dan mempengaruhi keluaran.

3) Cipherteks (C)

Cipherteks adalah hasil dari algoritma enkripsi yang tidak dapat diketahui lagi makna sebenarnya.

4) Algoritma enkripsi (Ek)

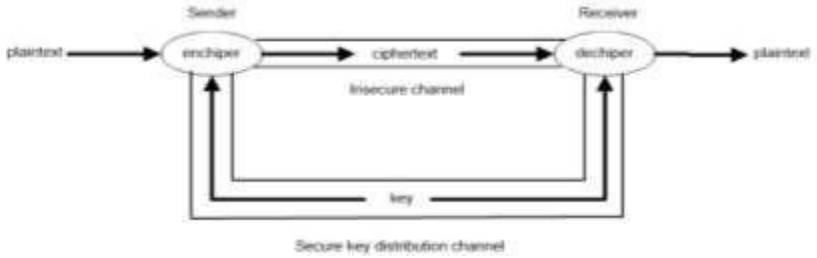
Memiliki dua data masukan yakni plainteks dan kunci rahasia. Algoritma enkripsi melakukan transformasi dari plainteks sehingga menghasilkan pesan yang telah disandikan. $Ek{:}M \rightarrow C, dimana\ k \in K$

5) Algoritma dekripsi (Dk)

Memiliki dua data masukan yakni pesan yang sudah disandikan (cipherteks) dan kunci rahasia. Merupakan algoritma mengembalikan cipherteks menjadi plainteks.

$Dk{:}C \rightarrow M, dimana\ k \in K$

Skema kriptografi dapat dilihat pada Gambar 3.1 (Denning, 1982):



Gambar 13. Channel Informasi Klasik (Denning, 1982)

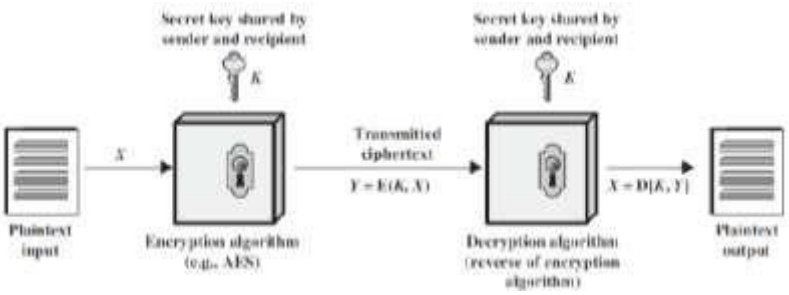
Menurut Denning (1982), pada umumnya kriptografi sistem harus memenuhi tiga syarat. Syarat tersebut adalah bahwa transformasi enkripsi dan dekripsi harus efisien untuk semua kunci, kunci haruslah mudah untuk digunakan, dan keamanan sistem harus bergantung pada kerahasiaan kunci dan tidak pada kerahasiaan algoritma enkripsi atau dekripsi.

Dalam perkembangannya, kriptografi memiliki dua jenis algoritma, yaitu algoritma enkripsi kunci simetri (symmetric-key encryption algorithm) dan algoritma enkripsi kunci publik/asimetri (public-key encryption algorithm). Algoritma enkripsi kunci simetri menggunakan kunci yang sama atau disebut juga kunci rahasia, baik untuk enkripsi maupun dekripsi. Oleh karena itu kunci ini harus dirahasiakan oleh pengirim dan penerima pesan agar cipherteks tetap aman dari gangguan serangan. Algoritma enkripsi kunci publik menggunakan dua kunci pasangan namun berbeda. Satu kunci dipakai untuk enkripsi, yaitu kunci publik, pasangan kuncinya digunakan untuk dekripsi, yaitu kunci privat.

C. Kriptografi Kunci Simetri

Dalam kriptografi klasik atau juga disebut kriptografi simetri adalah kriptografi yang menggunakan kunci yang sama untuk melakukan enkripsi dan dekripsi pesan. Algoritma kriptografi simetri dibagi menjadi 2 kategori yaitu Stream Cipher dan Block Cipher. Stream Cipher melakukan

penyandian pesan pada satu bit atau satu byte data, sedangkan Block Cipher melakukan proses penyandian pada sekumpulan bit (per blok).



Gambar 14. Skema Enkripsi Kunci Simetri (Stalling, 2011)

Menurut Stalling (2011), terdapat dua syarat yang harus dipenuhi oleh enkripsi konvensional agar dapat digunakan, yaitu:

1) Dibutuhkan suatu algoritma enkripsi yang kuat. Walaupun pihak lawan mengetahui algoritma yang digunakan dan memiliki cipherteks, haruslah sulit untuk pihak lawan melakukan dekripsi atau mendapatkan kunci rahasia.
2) Pengirim dan penerima pesan harus memiliki salinan kunci rahasia pada suatu "ruang" rahasia dan menjaganya tetap aman. Bila pihak lawan mengetahui kunci dan algoritma enkripsi, maka keseluruhan komunikasi yang menggunakan kunci tersebut akan dapat diketahui/dibaca.

Algoritma kunci simetri pada umumnya membutuhkan waktu yang singkat dalam melakukan proses enkripsi dan dekripsi serta memiliki ukuran kunci yang relatif pendek. Otentikasi pengirim pesan dapat langsung diketahui dari cipherteks yang dikirimkan, karena hanya pengirim dan penerima saja yang mengetahui kunci rahasia. Namun, kunci simetri memiliki kelemahan seperti membutuhkan saluran yang aman untuk mengirimkan kunci ke pihak kawan komunikasi. Kunci harus sering diubah, bahkan mungkin pada setiap akan melakukan komunikasi.

D. Kriptografi Kunci Asimetri (Publik)

Konsep kriptografi kunci publik pertama kali diperkenalkan oleh Diffie Hellman pada tahun 1976. Kriptografi kunci publik menjawab permasalahan yang ada pada kriptografi kunci simetri yaitu pertama, bila dua orang yang akan berkomunikasi sama-sama memiliki kunci, maka yang manakah dari dua orang tersebut yang harus mendistribusikan kunci. Kedua, permasalahan pada pendistribusian kunci yang menggunakan *Key Ditribution Center* (KDC).

Kunci publik/asimetri adalah dua kunci yang saling berhubungan, yaitu kunci publik dan kunci privat. Kunci ini digunakan untuk operasi enkripsi dan dekripsi atau verifikasi tanda tangan (tanda tangan digital). Keduanya memiliki sifat

turunan dimana antara kunci privat dan kunci publik dapat di komputasikan. (Stalling, 2011).

Skema enkripsi kunci publik memiliki enam elemen (Arvandi, 2003):

a. Plainteks, yang merupakan data atau pesan asli. Plainteks adalah masukan untuk algorima.
b. Algoritma enkripsi, menghasilkan transformasi dari plainteks.
c. Kunci publik dan kunci privat, pasangan kunci yang dipilih dimana satu kunci untuk enkripsi, satu kunci lainnya untuk dekripsi.
d. Cipherteks, pesan yang telah disandikan, merupakan keluaran dari algoritma enkripsi. Cipherteks bergantung kepada plainteks dan kunci rahasia.
e. Algoritma dekripsi, merubah cipherteks dengan memprosesnya dengan kunci yang cocok yang selanjutnya akan menghasilkan plainteks.

Algoritma kunci publik bertumpu pada satu kunci untuk enkripsi dan satu kunci yang berbeda namun memiliki keterhubungan untuk melakukan dekripsi. Algoritma kunci publik memiliki ketentuan sebagai berikut (Stalling, 2011):

1) Secara komputasi mudah bagi pihak B untuk membangkitkan sepasang kunci, kunci publik (Kpub) dan kunci privat (Kpv).

2) Secara komputasi mudah bagi pengirim A dengan mengetahui kunci publik B untuk melakukan enkripsi (E) pesan (M), untuk menghasilkan cipherteks (C).

$$C=E(Kpub,M)$$

3) Secara komputasi mudah bagi penerima B untuk melakukan dekripsi (D) terhadap cipherteks menggunakan kunci privat sehingga akan menghasilkan pesan asli.

$$M=D(Kpv,C)=D[Priv,E(Kpub,M)]$$

4) Secara komputasional adalah hampir tidak mungkin atau sulit bila diketahui kunci publik, untuk mendapatkan kunci privat.
5) Secara komputasional adalah hampir tidak mungkin atau sulit bila diketahui kunci publik dan cipherteks untuk mengahasilkan pesan asli.

Dapat ditambahkan syarat ke-6, meskipun sangat berguna namun tidak menjadi suatu keharusan bagi semua kriptografi kunci publik untuk mengaplikasikannya, yaitu:

6) Kedua kunci dapat diaplikasikan untuk enkripsi maupun dekripsi.

$$M=D[Kpub,E(Kpv,M)]=D[Kpub,M)]$$

Langkah-langkah pada kriptografi kunci publik dapat dilihat sebagai berikut (diasumsikan Alice dan Bob adalah dua orang yang akan melakukan komunikasi) (Stalling, 2011)
:

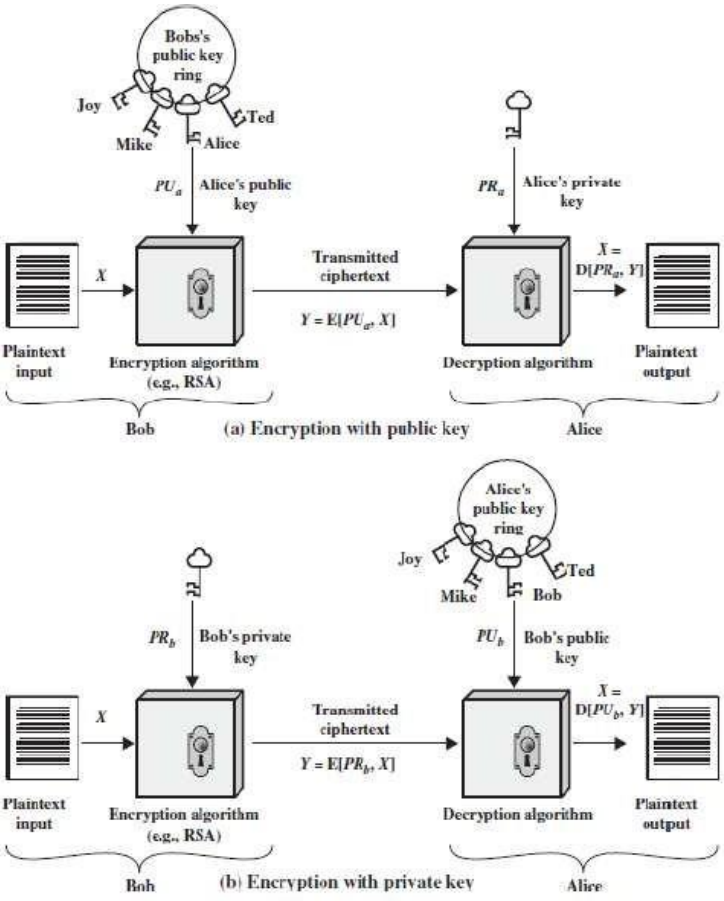
a. Setiap pengguna membangun sepasang kunci yang akan digunakan untuk enkripsi dan dekripsi pesan.
b. Setiap user meletakkan satu buah kunci pada domain publik atau file lain yang dapat diakses, dalam hal ini adalah kunci publik. Pasangan kunci yang satunya harus dijaga kerahaisaannya (kunci privat).
c. Jika Bob ingin mengirimkan pesan rahasia ke Alice, maka Bob harus mengenkripsi pesan menggunakan kunci publik Alice.

Ketika Alice menerima pesan tersebut, Alice akan mendekripsi pesan menggunakan kunci privat miliknya. Tidak ada penerima pesan lainnya yang dapat mendekripsi pesan karena kunci untuk membuka pesan tersebut hanya diketahui oleh Alice. Skema kriptografi kunci publik dapat dilihat pada Gambar 15. Berikut penjelasannya (Sadikin, 2012):

1) Sebelum Alice melakukan enkripsi, Bob membangkitkan sepasang kunci yaitu kunci privat dan kunci publik miliknya dengan memanggil fungsi **PembangkitKunci** dengan persamaan 1:

$$(Kpub, Kpv) \leftarrow \textbf{PembangkitKunci} \quad (1)$$

Bob mempublikasikan kunci publik *Kpub*, namun tetap menjaga kerahasiaan kunci privat Kpv



Gambar 15. Skema Kriptografi Kunci Publik (Stalling, 2011)

2) Alice mengenkripsi sebuah teks asli (*M*) dengan kunci publik Bob (*Kpub*) menghasilkan sebuah teks sandi (*C*) dengan memanggil fungsi **Enkripsi** dengan persamaan 2:

$$C \leftarrow \text{Enkrips}(Kpub, M) \qquad (2)$$

Alice mengirim teks sandi *C* ke Bob melalui saluran tidak aman.

3) Bob mendekripsi teks sandi (*C*) dengan kunci privat Bob (*Kpv*) untuk mendapatkan teks asli *M* dengan fungsi **Dekripsi** dengan persamaan 3:

$$M \leftarrow \text{Dekrips}(Kpv, C) \quad (3)$$

Bob mendapatkan M jika teks sandi C dienkripsi dengan kunci publik Bob.

E. Kriptografi Klasik

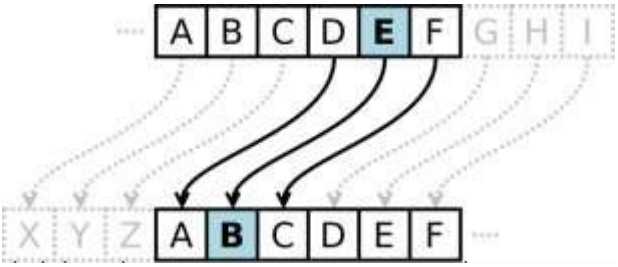
a. Scytale

Metode scytale digunakan oleh bangsa Sparta sekitar tahun 475 S.M pada jaman Yunani kuno untuk memperkuat kekuatan militer mereka. Scytale terbuat dari tongkat dengan lembaran papyrus yang mengelilingi secara spiral dimana diameter tongkatlah yang menjadi kunci rahasia. Jadi walaupun pihak lawan memiliki pesan yang ada di lembaran papyrus tersebut, hanya orang yang memiliki diameter tongkat yang benarlah yang bisa membaca isi pesan.

Gambar 16. Scytale dengan Gulungan Papyrus (sumber: en.wikipedia.org/wiki)

b. Caesar Cipher

Caesar ciper pertama kali digunakan oleh Julius Caesar untuk menaklukkan banyak bangsa-bangsa di eropa. Teknik yang digunakan adalah mensubstitusikan alphabet secara berurutan dengan kunci berupa alphabet yang digeser sejumlah bilangan tertentu ke kanan.



Gambar 17. Ilustrasi Caesar Cipher
(sumber: en.wikipedia.org/wiki)

Misalkan A = 0, B = 1, …, Z = 25, maka secara matematis caesar cipher dirumuskan sebagai berikut:

Enkripsi: ci = E(pi) = (pi + 3) mod 26

Dekripsi: pi = D(ci) = (ci – 3) mod 26

Jika pergeseran huruf sejauh k, maka:

Enkripsi: ci = E(pi) = (pi + k) mod 26

Dekripsi: pi = D(ci) = (ci – k) mod 26

k = kunci rahasia

Untuk 256 karakter ASCII, maka:

Enkripsi: $c_i = E(p_i) = (p_i + k) \bmod 256$

Dekripsi: $p_i = D(c_i) = (c_i - k) \bmod 256$

k = kunci rahasia

Kelemahan *Caesar cipher* adalah mudah dipecahkan dengan *exhaustive key search* karena jumlah kuncinya sangat sedikit (hanya ada 26 kunci).

Kriptografi dapat di karakteristikkan kedalam tiga area (Arvandi, 2003):

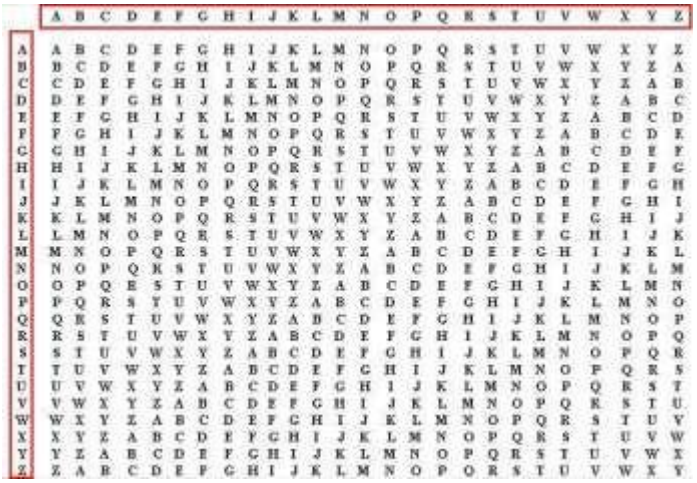
a. Tipe operasi yang digunakan untuk merubah plainteks ke ciperteks. Terdapat dua prinsip umum untuk algoritma pengenkripsian yaitu substitusi (menukar bit, karakter, atau blok karakter dari plainteks dengan substitusi) dan transposisi (menyusun elemen-elemen plainteks). Pada area ini, seluruh operasi harus dapat dibalik dan tidak ada informasi yang hilang.
   i. Cipher Substitusi
      - Cipher abjad tunggal atau *monoalphabetic cipher*. Satu karakter di plainteks diganti dengan satu karakter yang bersesuaian. Jumlah kemungkinan susunan huruf-huruf cipherteks yang dapat dibuat adalah sebanyak :

        26! = 403.291.461.126.605.635.584.000.000

        Contoh: *Caesar Cipher*

        Polyalphabetic substitution cipher. Panjang kunci sepanjang plainteks. Jika kunci kurang

dari plainteks, maka kunci di ulang sepanjang plainteks. Contoh Vigenere Cipher:



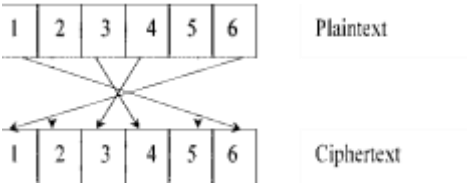
Plainteks: SHE SELLS SEA SHELLS

+ Kunci : KEY KEYKE YKE YKEYKE

Cipherteks: CLC CIJVW QOE QRIJVW

ii. Cipher Transposisi / Permutasi.

Cipherteks diperoleh dengan mengubah posisinya. Dengan kata lain, algoritma ini melakukan *transpose* terhadap rangkaian karakter di dalam teks. Nama lain untuk metode ini adalah **permutasi**, karena *transpose* setiap karakter di dalam teks sama dengan mempermutasikan karakter-karakter tersebut.



b. Jumlah kunci yang digunakan. Terdapat dua sistem yaitu simetri atau enkripsi kunci rahasia (pengirim dan penerima menggunakan kunci yang sama) dan asimetri atau enkripsi kunci publik (pengirim dan penerima menggunakan kunci yang berbeda). Telah dijelaskan pada sub-bab sebelumnya.

c. Cara plainteks tersebut diproses. Terdapat dua proses, cipher blok (adalah suatu fungsi pemetaan *n*-bit blok plainteks ke *n*-bit blok cipherteks) dan cipher stream (string plainteks dan menghasilkan string cipherteks, dimana pada suatu blok tertentu saling berhubungan dengan blok tertentu lainnya).

   i. Cipher Blocking.

      Sistem enkripsi terkadang membagi plainteks menjadi blok-blok yang terdiri dari beberapa karakter yang kemudian dienkripsikan 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.

      Contoh Reverse Cipher:

      Misalkan plainteks adalah

      FAKULTAS TEKNIK INFORMATIKA UMRAH

Kunci baris 5, kolom 6; maka untuk melakukan enkripsi:

Enkripsi:

F	A	K	U	L	T
A	S	T	E	K	N
I	K	I	N	F	O
R	M	A	T	I	K
A	U	M	R	A	H

Cipherteks: (baca secara vertikal)

FAIRAASKMUKTIAMUENTRLKFIATNOKH

Untuk melakukan dekripsi bagi panjang cipherteks dengan kunci kolom: 30/6 = 5, maka

F	A	I	R	A
A	S	K	M	U
K	T	I	A	M
U	E	N	T	R
L	K	F	I	A
T	N	O	K	H

Plainteks: (dibaca secara vertikal)

FAKULTAS TEKNIK INFORMATIKA UMRAH

ii. 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 plainteks terjadi sebagai berikut :

Plainteks: `5 TEKNIK DASAR KRIPTOGRAFI`

Cipher: `5AN EKNIKTAN ASARDAN RIPTOGRAFIKAN`

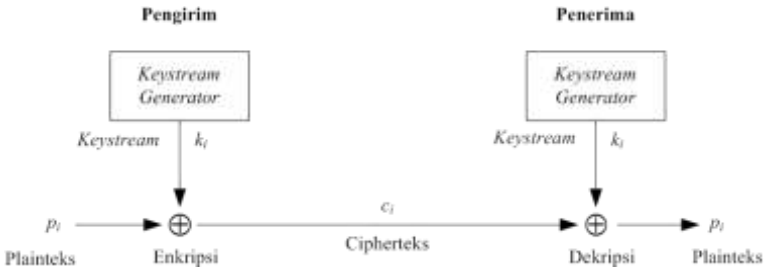
G. Kriptografi Modern

Kriptografi modern menggunakan gagasan dasar yg sama seperti kriptografi klasik (permutasi & transposisi) tetapi penekanannya berbeda. Bila kriptografi klasik berorientasi pada karakter, kriptografi modern berorientasi pada bit, sehingga penyandiannya dengan menggunakan media komputer. Kriptografi modern tidak selalu berupa karakter, tetapi bisa berupa gambar atau video.

Kategori algoritma (cipher) berbasis bit adalah sebagai berikut:

1) Stream Cipher (cipher aliran).

Tipe ini beroperasi pada bit tunggal. Mengenkripsi plainteks menjadi chiperteks bit per bit (1 bit setiap kali transformasi) atau ***byte*** per *byte* (1 *byte* setiap kali transformasi) dengan kunci *keystream*. Diperkenalkan oleh Vernam melalui algoritmanya, **Vernam *Cipher***. Vernam *cipher* diadopsi dari *one-time pad cipher*, yang dalam hal ini karakter diganti dengan bit (0 atau 1).



Gambar 18. Konsep Stream Cipher
(sumber: dinus.ac.id)

Bit-bit kunci untuk enkripsi/dekripsi disebut *keystream*. Keystream dibangkitkan oleh *keystream generator. Keystream* di-XOR-kan dengan bit-bit plainteks, p_1, p_2, …, p_n menghasilkan aliran bit-bit cipherteks:

$$c_i = p_i \oplus k_i$$

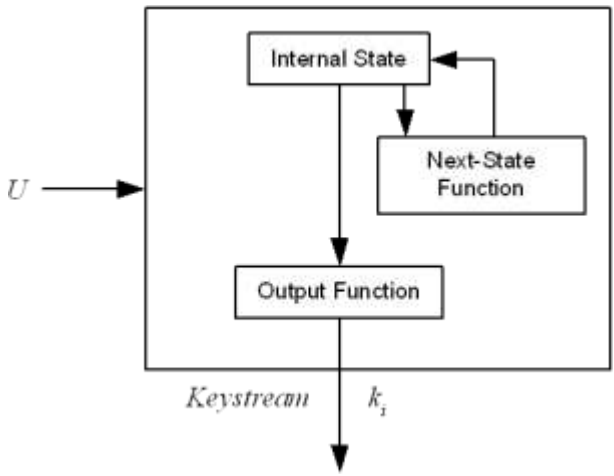
Di sisi penerima dibangkitkan *keystream* yang sama untuk mendekripsi aliran bit-bit cipherteks:

$$p_i = c_i \oplus k_i$$

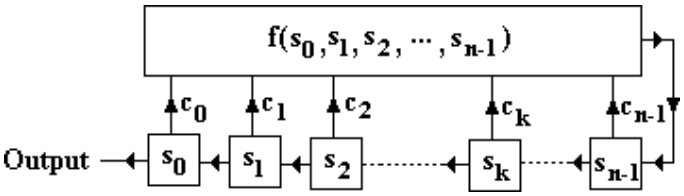
keamanan sistem ini bergantung pada keystream generator.

Keystream Generator

Keystream generator diimplementasikan sebagai prosedur yang sama di sisi pengirim dan penerima pesan. *Keystream generator* dapat membangkitkan *keystream* berbasis bit per bit atau dalam bentuk blok-blok bit. Jika *keystream* berbentuk blok-blok bit, *cipher* blok dapat digunakan untuk untuk memperoleh *cipher* aliran.



Gambar 19. Proses di dalam Keystream Generator (sumber: semanticscholar.org)



Gambar 20. Linear Feedback Shift Register (sumber: math.ucdenver.edu)

Contoh *keysteam generator* ada yang dikenal dengan *Linear Feefback Shift Register* (LFSR). LFSR terdiri dari dua bagian: register geser (*n* bit) dan fungsi umpan balik. Dapat dilihat pada Gambar 20.

2) Block Cipher

Bit-bit plainteks dibagi menjadi blok-blok bit dengan panjang sama, misalnya 64 bit. Panjang kunci enkripsi = panjang blok. Enkripsi dilakukan terhadap blok bit plainteks menggunakan bit-bit kunci. Algoritma enkripsi menghasilkan blok cipherteks yang panjangnya = blok plainteks.

Blok plainteks berukuran *m* bit:

$$P = (p_1, p_2, \ldots, p_m), \qquad p_i \in \{0, 1\}$$

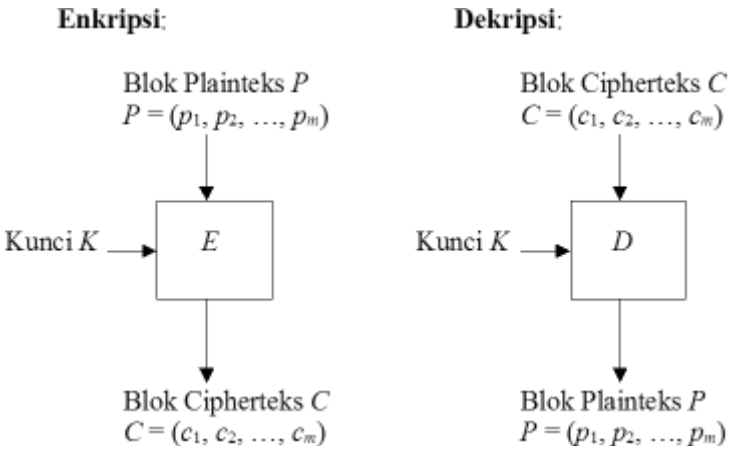
Blok cipherteks (C) berukuran *m* bit:

$$C = (c_1, c_2, \ldots, c_m), \qquad c_i \in \{0, 1\}$$

Skema enkripsi dan dekripsi blok cipher dapat dilihat pada gambar 21.

Block cipher memiliki 4 mode operasi. Mode operasi merupakan model yang berkaitan dengan cara blok dioperasikan.

a. *Electronic Code Block* (ECB)
b. *Cipher Block Chaining* (CBC)
c. *Cipher Feedback* (CFB)
d. *Output Feedback* (OFB)



Gambar 21. Skema enkripsi dan dekripsi pada block cipher

Diskusi

Diskusikan yang manakah dari dua kriptografi (klasik dan modern) yang telah dijelaskan diatas kriptografi yang paling baik? Lalu rancanglah metode pengamanan pesan dengan kriptografi.

Daftar pustaka

Arvandi, M., 2005, Analysis of Neural Network Based Ciphers, Thesis, Computer Science, Ryerson University, Toronto.

Denning, D.E., 1982, Cryptography and Data Security, Addison-Wesley Publishing, Canada.

Howarth, F., 2013, 5 Key Steps to Ensuring Database Security, Faulkner Information Services.

Kementerian Komunikasi dan Informatika Republik Indonesia, 2014, Panduan Penangan Insiden Keamanan Database, BPPT CSIRT.

Menezes, A. J., Orschot, P.C. dan Vanstone, S.A., 1996, Handbook of Applied Cryptography, Electrical Engineering and Computer Science, Massachusetts Institute of Technology.

Sadikin, R., 2012, Kriptografi untuk Keamanan Jaringan, Penerbit ANDI, Yogyakarta.

Singh, S., 2001, The Code Book: How to Make it, Break it, Hack it, Crack it, Delacorte Press, New York.

Stalling, W., 2011, Cryptography and Network Security Principles and Practice, Fifth Edition, Prentice Hall, New York.