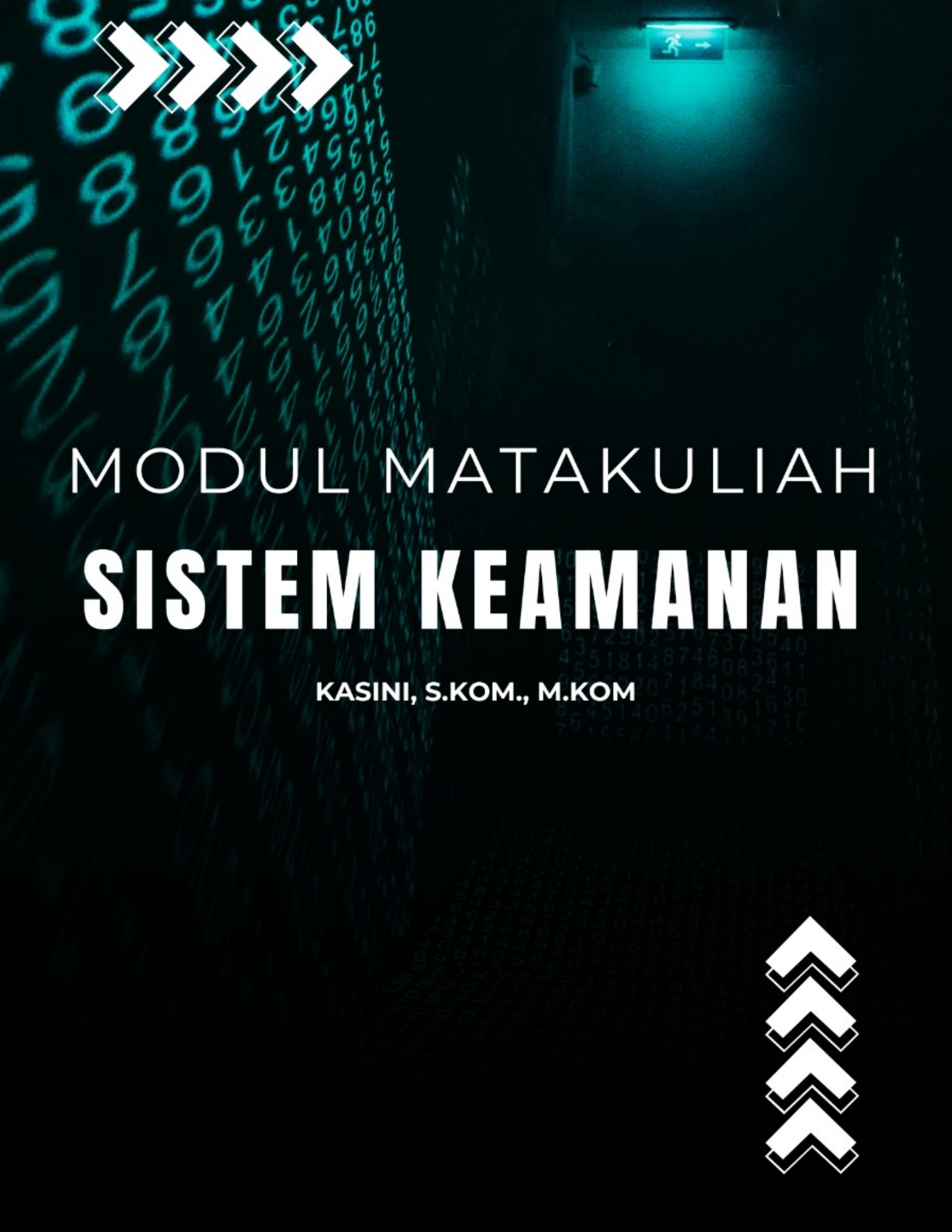


MODUL MATAKULIAH

SISTEM KEAMANAN

KASINI, S.KOM., M.KOM

1. Pendahuluan

The protecetion to an automated information system in order to attain the applicable objectives of preserving the integrity ,availiblity ,and confidentiality ,of information syistem resources (includes hardware ,software,firmware,information/data and telecomunications), (william stalling &lawrie brown, computer securyty principle and practice, 3rd edition,2015)

Keamanan komputer adalah perlindungan yang diberikan pada sistem infomrasi dengan tujuan tertentu untuk menjaga integritas, ketersediaan, dan kerahasiaan sumber daya informasi (perangkat keras, perag kat lunak, firmware, informasi/ data dan informasi.)

Keamannan komputer adalah perlindungan sistem komputer/informasi dari bahaya pencurian atau penggunaan yang tidak sah.

1.1 Sejarah Keamanan Komputer

Arti dari keamanan komputer telah berubah dalam beberapa tahun terakhir. Sebelum masalah keamanan data/informasi menjadi popular, kebanyakan orang berpikir bahwa keamanan computer difokuskan pada alat alat computer secara fisik. Secara tradisional, fasilitas komputer secara fisik dilindungi karena tiga alasan:

1. untuk mencegah pencurian atau kerusakan
2. hardware untuk mencegah pencurian atau kerusakan
3. informasi untuk mencegah gangguan layanan

Prosedur yang sangat ketat untuk akses ke ruang server diaplikasikan oleh sebagian besar organisasi, dan prosedur ini sering digunakan untuk mengukur level keamanan computer. Dengan adanya akses jarak jauh atau remote terminal, jaringan yang sudah banyak serta teknologi internet yang berkembang pesat maka perlindungan secara fisik sudah jarang atau tidak dapat lagi digunakan untuk mengukur level keamanan. Meskipun demikian, masih ada beberapa perusahaan yang masih melindungi fasilitas fisik server mereka dengan peralatan cangih tetapi kurang memperhatikan perlindungan terhadap data atau informasi itu sendiri yang disimpan dalam server. Walupun nilai data atau informasi tersebut beberapa kali lebih besar dari nilai hardware.

Oleh karena itu konsep atau definisi computer security atau keamanan computer saat ini manjadi lebih luas atau bisa juga didefinisikan sebagai berikut: keamanan komputer dirancang untuk melindungi komputer dan segala sesuatu yang berkaitan dengan itu, bangunannya, workstation dan printer, kabel, dan disk dan media penyimpanan lainnya. Yang paling penting, keamanan komputer melindungi informasi yang disimpan dalam sistem anda. Keamanan komputer tidak hanya dirancang untuk melindungi terhadap penyusup dari luar yang masuk ke sistem, tetapi juga bahaya yang timbul dari dalam seperti berbagi password dengan teman, gagal atau tidak dilakukan untuk backup data, menumpahkan kopi pada keyboard dan sebagainya.

Didalam information security sering juga dikenal CIA Triad atau segitiga confidentiality (kerahasiaan), integrity (integritas), dan availability (ketersediaan). Kerahasiaan, integritas dan ketersediaan, yang dikenal sebagai segitiga CIA ini adalah model yang dirancang untuk memandu kebijakan untuk keamanan informasi dalam sebuah organisasi. Model ini juga kadang-kadang disebut sebagai triad AIC (ketersediaan, integritas dan kerahasiaan) untuk menghindari kebingungan dengan Central Intelligence Agency. Unsur-unsur dari tiga serangkai tersebut dianggap tiga komponen yang paling penting dari system keamanan.Bila bicara kerahasiaan

sama dengan bicara privasi. Langkah-langkah yang dilakukan untuk menjamin kerahasiaan dirancang untuk mencegah informasi rahasia dan sensitif di ambil oleh orang yang tidak berhak. Oleh karena itu access harus dibatasi hanya untuk mereka yang berwenang saja yang dapat melihat data yang sensitive atau rahasia tersebut. Sebuah sistem komputer yang aman harus menjaga agar informasi selalu tersedia untuk pengguna. Ketersediaan berarti bahwa perangkat keras dan perangkat lunak sistem komputer terus bekerja secara efisien dan bahwa sistem ini mampu pulih dengan cepat dan benar jika ada bencana.

Integritas melibatkan beberapa unsur yaitu: menjaga konsistensi, akurasi, dan kepercayaan dari data melalui seluruh siklus hidupnya. Data tidak boleh diubah pada saat ditransmisikan. Dalam hal ini harus diambil langkah langkah untuk memastikan bahwa data tidak dapat diubah oleh orang yang tidak berhak dan tidak kurang suatu apapun serta benar adanya. Dalam keamanan komputer ada tiga komponen yang selalu menjadi diskusi:

(a) Kerentanan: adalah kelemahan dari komputer yang memungkinkan penyerang untuk masuk ke sistem jaringann informasi.

(b) Ancaman: adalah kemungkinan bahaya yang mungkin mengeksploitasi kerentanan untuk melakukan gangguan pada system keamanan dan karena itu dapat menyebabkan kemungkinan bahaya bagi organisasi.

(c) Penanggulangan: adalah suatu tindakan, perangkat, prosedur, atau teknik yang mengurangi ancaman, kerentanan, atau serangan dengan menghilangkan atau mencegah, dengan meminimalkan kerugian itu dapat menyebabkan, atau dengan menemukan dan melaporkan masalah system keamanan sehingga tindakan korektif dapat diambil.

ada saat computer diperkenalkan pertama kali, ukuran komputer sangat besar, langka, dan sangat mahal. Oleh karena itu organisasi atau perusahaan yang cukup beruntung memiliki komputer akan mencoba dengan cara terbaik untuk melindungi computer tersebut. Keamanan komputer hanya salah satu aspek dari keamanan secara keseluruhan dari asset organisasi. Keamanan difokuskan pada fisik pembobolan, pencurian peralatan komputer, dan pencurian atau perusakan kemasan disk, gulungan pita, dan media lainnya. Hanya sedikit orang yang tahu bagaimana menggunakan komputer, dan dengan demikian pengguna harus dengan hati-hati dipilih. Pada saat itu computer tidak terhubung dengan jaringan internet sehingga memang masalah keamanan hanya berfokus pada fisik dan lingkungannya saja.

Pada 1970-an, teknologi komunikasi berubah, dan dengan itu cara-cara berkomunikasi juga berubah, pengguna yang berhubungan dengan komputer dan data dapat bertukar informasi dengan menggunakan jaringan telepon. Selain itu multi-programaming, timesharing, dan jaringan mengubah semua aturan dalam berkomunikasi. Dengan terkoneksinya computer pada jaringan telepon maka pengguna berkemampuan untuk mengakses komputer dari lokasi terpencil. Dengan kemampuan itu mengubah penggunaan komputer. Komputer merambah ke bidang bisnis dengan mulai menyimpan informasi secara online dan terkoneksi dengan jaringan secara bersama-sama dan dengan mainframe yang berisi database.

Dengan di mulainya computer dan jaringan untuk keperluan bisnis maka mulai muncul masalah keamanan computer terutama menyangkut pencurian data dan informasi. Sehingga masalah keamanan computer tidak lagi terfokus pada masalah fisik dan lokasi, tetapi di tambah dengan masalah kemanan data dan informasi **(Binus, 2017)**

1.3 Tujuan

Menurut Garfinkel dan Spafford, ahli dalam computer security, komputer dikatakan aman jika bisa diandalkan dan perangkat lunaknya bekerja sesuai dengan yang diharapkan. Keamanan komputer memiliki 5 tujuan, yaitu:

1. Availability
2. Integrity
3. Contro
4. Audit
5. Confdentiality
6.

1.1.1 Mengapa keamanan komputer?

a. Keamanan komputer penting untuk melindungi kerahasiaan integritas ,dan ketersedian sistem komputer dan sumber dayanya .

b. Administrasi dan manajemen komputer menjadi lebih kompleks yang menjadi jalan serangan .

c. Evolusi teknologi berfokus pada kemudahan pengunaan sementara tingkat keahlian yang di butuhkan untuk ekspolitas telah menurun .

d. Lingkungan jaringan dan aplikasi berbasis jaringan menyediakan lebih banyak jalur serangan .

1.1.2 Kenapa kejahatan komputer semakinmeningkat?

a) meningkat nya aplikasi bisnis berbasis teknologi informasi dan internet .

Internet pada awal kemunculan yakni oktober 1960 ,internet disebut sebagai ARPANET (advanced research projec agency network).ARPANET merupakan proyek yang di buat oleh depertemen pertahanan amerika serikat yang di ketuai oleh joseph licklider .

Internet berasal dari istilah interconected network .pada tahun 1990 bernes –lee dan timnya yang berkerja di CERN(organisasi eropa untuk riset nuklir) menciptakan world wide web (www) .public mulai menggunakan ‘ww’.public menggunakan www. yang berfungsi untuk menggunakan dalam menelusuri situs website .pada tahun 1994 mulailah bermunculan situs penyedian email bernama yahoo dan perusahaan berbasis online seperti amozon dan ebay sedangkan kemunculan google terjadi pada tahun 1998. berdasarkan catatan whois arin dan apnic ,protocol ,internet IP pertama dai indonesia ui – netlab di daftarkan oleh universitas indonesia pada tahun pada 24 juni 1988.di sekitar tahun 1994 mulai beroperasi indonet yang di pimpin oleh sanjaya. Indonet merupakan COMERCIAL pertama di indonesia. mulai tahun 1955 dengan memakai remote browser lynk di as, maka pemakai internet di indonesia akses internet (HTTP), tahun 2000 an - sekarang mulai berkembang online banking, e commerce, Ethernet data interchanch (EDI).Desentralisasi server ..

b) Meningkatnya kemampuan pemakai (user) menggunakan teknologi dan kemudahan memperoleh software.
c) Ada kesempatan untuk melakukan uji coba (sekedar ingin tahu) . Dengan mudah mengunduh software yang di inginkan dari internet (script kiddies)
d) Perubahan teknologi yang terlalu cepat

1.1.3 Potensi Kerugian akibat serangan keamanan

Gambar 1.1 Kerugian yang diakibatkan serangan keamanan

1.2 Elemen Keamanan

Didalam keamanan system terdapat elemen elemen yang harus dijaga. Berikut ini adalah elemen elemen nya:

1. Kerahasian adalah " memastikan bahwa informasi hanya dapt di akses oleh mereka yang berwenang untuk memiliki akses"
2. Keaslian adalah "idenfikasi dan jaminan keaslian informasi "
3. integritas adalah "memastikan bahwa informasi informasi tersebut akurat,lengkap,dan dalam bentuk aslinya"
4. ketersedian adalah " memastikan bahwa informasi dapat di akses orang yang berwenang ketika di perlukan tanpa penundaan "
5. non –repudation adalah "memastikan bahwa salah satu pihak dalam kontrak atau komunikasi tidak dapat menyangkal keaslian tanda tangan mereka pada sebuah documen"

1.2.1 Keamanan, fungsi ,dan kemudahan pengunaan

1) keamanan (batasan)
2) Kegunaan(fitur)
3) Kemudahan menggunakan

- ✓ produk aplikasi /perangkat lunak secara default telah di konfigurasi sebelumnya untuk penggunaan ,sehingga membuat pengguna rentan terhadap sebagai kelemahan keamanan

- ✓ Begitu pula dengan peingkatan fungsionalitas (fitur) pada aplikasi terkadang selalu aman.

1.2.2 Konsep Dasar Keamanan

1) Pencegahan : mengikuti tindakan pencegahan saat menggunakan sistem dan aplikasi computer

2) pemeliharaan :mengelolah semua perubahan di aplikasi komputer dan menjaganya tetap mutakhir
3) Reaksi :bertindak tepat waktu saat insiden keamanan terjadi

Berikut ini lapisan keamanan pada system:

LAYER 1	LAYER 2	LAYER 3	LAYER 4	LAYER 5
Keaman fisik (phisical security)	**Keamanan jaringan (network security)**	**Keamanan sistem (sistem security)**	**Keaman aplikasi (aplication security)**	**Keamanan penguna (user security)**
Menjaga personel ,perangkat keras,program,jaringan,dan databdari ancaman fisik.	**Melindungi jaringan dan layan mereka dari modifikasi,perusakan,atau pengungkapan yang tidak sah .**	**Melindungi sistem dan informasinya dan pencurian korupsi ,akses tidak sah ,atau penyalagunaan.**	**Meliputi pengunaan perangkat lunak,perangkat keras, dan metode prosedural untuk melindungi aplikasi dari ancaman eksternal.**	**Memastikan bahwa pengguna yang valid masuk (login)dan bahwa pengguna yang masukitu dari aplikasi sama**

2.1.3 Resiko Keamanann Bagi Pengguna Rumah

a. Komputer rumah rentan terhadap berbagai serangan dunia maya karena menyediakan sasaran empuk bagi penyerang karena tingkat kesadaran yang rendah.
b. Resiko keamanan bagi pengguna rumahan timbul dari berbagai serangan dan kecelakaan komputer yang menyebabakan kerusakan fisik pada sistem komputer

1. Serangan komputer

- serangan malware
- serangan email
- serangan kode seluler (java/ javascipt/active)
- deniel of service dan serangaan scrip lintas situs (cross-site scripsing)
- pencuriaan indentitas dan penipuan komputer
- paket mengendus (packet sniffing)
- menjadi prantara untuk serangan lain

2. kecelakaan komputer

- kegagalan hardisk atau komponen lainya
- kegagalan daya dan lonjakan arus listrik
- pencurian alat komputer

2.1.4 Manfaat Kesadaran Keamanan Komputer

Pengguna atau *user* merupakan salah satu pihak yang dapat melakukan pencegahan dalam keamanan system computer. Ada beberapa manfaat dari pengguna untuk meminimalkan teradinya pencurian data ataupun kerusakan data.

a. Kesadaran keamanan komputer membantu meminimalkan kemungkinan serangan komputer
b. Membantu mencegah hilangnya informasi yang di simpen sistem
c. Membantu pengguna untuk pencegah penjahat dunia maya menggunakan sistem mereka untuk melancarkan serangan ke sistem komputer lain
d. Membantu pengguna meminimalkan kerugian jika terjadi kecelakaan yang menyebabkan kerusakan fisik pada sistem computer
e. Memungkinkan pengguna untuk melindungi informasi sensitif dan sumber dari akses yangtidak sah.

2.1.5 Ancaman Ancaman Terhadap Keamanan Sistem

Ancaman dalam system computer dapat menyerang system komputer sebagai berikut:

a. Virus adalah Program yang mereplikasi dengan menyalin dirinya sendiri ke progam lain,boot sector sistem,atau document,dan mengubah merusak file komputer dan aplikasi
b. Worm merupakan virus yang menggandakan diri yang tidak mengubah file tetapi berada di memori komputer dan bereplikasi diri
c. Backdoor adalah cara tidak sah untuk mengakses sistem dan melewati mekanisme keamanan
d. Rootkit yaitu satu set program atau utlitas yang memungkinkan seseorang untuk mempertahankan akses tingkat root kesistem
e. Trojan adalah program yang tampak nya sah tetapi bertindak jahat,saat di eksekusi
f. Logic bomb adalah program yang melepas atau worm
g. peretasan kata sandi adalah proses mengindenfikasi atau memulihkan data kata sandi yang tidak diketahui atau lupa
h. Guessing/menebak mencoba kata sandi yang berbeda sampai berhasil
i. Brute forcing mencoba kombinasi dan semua karakter sampai ata sandi yang benar di temukan
j. Dictionary attack Menggunakan data yang telah di tentukan sebelumnya
k. Shoulder surfing memperhatikan seseorang mengetik kata sandi
l. Social engineering menipu orang untuk mengungkapkan sandi mereka atau informasi lain yang untuk mengganti sandi

Malware dapat mengancam system computer dengan berbagai cara, berikut penjelasannya:

1. Melalui lampiran email, email yang berisi lamiparan mungkin termasuk malware
2. Mengklik lampiran menginstal program berbahaya di computer
3. Melalui memory stick (USB)
4. Virus membuat file autorun.inf yang merupakan sistem yang tersembunyi dan file hanya-baca, saat pengguna membuka file pen drive,file autorun.inf dijalankan dan menyalin file virus kedalam system
5. Melalaui situs web yang terinfeksi, mengunjungi situs yang disusupin mungkin mengakibatkan penginstalan perangkat lunak berbahaya,dirancang untuk mencuri informasi pribadi,di komputer pengguna.
6. Melalui download, mengunduh perangkat lunak play store,music foto,dan video dari mungkin juga situs web yang tidak terpercaya menyebabakan mengunduh file berbahaya yang terinfeksi virus,worm,trojan,dll.sejumlah besar aplikasi malicius tersedia di internet dengan deskripi yang dapat menipu pengguna agar pengguna mendownlodnya .
7. Melalui fake antivirus, Antivirus 2009 adalah anti virus palsu yang melakukan pemalsuan memindai sistem pengguna dan menunjukan virus yang ada tidak ada system.
8. mengklik tombol register atau scan akan mengunduh malware ke system berbagai file peer-to-peer (p2p) memungkinkan berbagai music,audio,gambar,dokumen,dan program perangkat lunak antara dua komputer melalaui internet.
9. file bersama mungkin mengandung risiko keamanan seperti virus, spyware,dan perangkat lunak lainya.
10. Penyerang dapat membagikan malware yang menyamar sebagi aplikasi yang berguna
11. jaringan P2P dapat di gunakan untuk mendistibusikan secara ilegal materi berhak cipta yang dapat menarik sanksi perdata /dan atau pidana

1.3 Metode Penanganan Keamann Sistem

Berikut ini beberapa strategi dalam meminimalkan terjadinya serangan pada system computer.

1.3.1 kriptografi

Kriptografi adalah praktek melindungi informasi dengan menggunakan algoritma kode, hash, dan tanda tangan. Informasi yang dilindungi bisa berupa data yang diam, seperti file di *hard drive*, atau data yang bergerak, seperti komunikasi elektronik antara dua pihak.

Ilmu ini mempelajari teknik matematika yang berkaitan dengan keamanan informasi, mencakup aspek seperti kerahasiaan, keabsahan, integritas, dan autentikasi data. Istilah *cryptography* sendiri berasal dari bahasa Yunani, yaitu "*crypto*" yang berarti rahasia, dan "*graphia*" yang berarti menulis, sehingga memiliki arti penulisan rahasia.

Dengan menggunakan teknik kriptografi, komunikasi atau informasi dapat dikodekan menjadi bentuk yang aman, di mana hanya pengirim dan penerima yang dapat mengakses isi data tersebut.

Selain itu, kriptografi terkait erat dengan proses enkripsi dan dekripsi. Enkripsi mengubah *plaintext* menjadi *ciphertext*, yang tidak dapat dimengerti, sedangkan dekripsi mengubahnya kembali ke *plaintext*. Proses ini dikendalikan oleh satu atau beberapa kunci, yang dapat berbeda tergantung pada sistem yang digunakan.

Kriptografi adalah ilmu dan seni yang telah ada sejak zaman kuno, mulai dari peradaban Mesir hingga kejayaan Yunani, sekitar 400 tahun sebelum Masehi. Pada masa itu, alat yang digunakan untuk menyembunyikan pesan dinamakan *Scytale*, sebuah batangan silinder yang memiliki kombinasi 18 huruf.

Di masa Romawi, di bawah pimpinan Julius Caesar, teknik kriptografi semakin berkembang, dengan penggunaannya yang lebih intens sebagai langkah menjaga stabilitas negara. Meskipun teknik yang diterapkan tidak serumit di zaman Yunani, memahami pesan kriptografi pada masa Romawi tetap sulit. Sejarah mencatat bahwa kriptografi awalnya digunakan untuk mengirim informasi sensitif antara tokoh militer dan politik, sehingga pesan tersebut tampak acak bagi orang lain namun dapat dipahami oleh penerimanya. Seiring waktu, teknik ini mengalami kemunduran dan hanya muncul dalam bentuk teka-teki di surat kabar.

Namun, dengan perkembangan teknologi, algoritma yang lebih kompleks muncul, menawarkan metode keamanan yang lebih andal. Selama berabad-abad, teknik kriptografi terus berevolusi, seperti penggunaan mesin *Enigma* oleh Nazi Jerman dalam Perang Dunia II yang merupakan contoh kriptografi yang sangat kompleks. Mesin tersebut berhasil dipecahkan oleh Sekutu berkat kemajuan dalam ilmu matematika dan komputer. Kini, ilmu matematika berperan dalam menciptakan algoritma kompleks

yang menyembunyikan pesan, sementara ilmu komputer digunakan untuk menganalisis dan menguji keamanan algoritma kriptografi agar dapat melawan serangan pencurian data.

Secara keseluruhan, baik kriptografi klasik maupun modern memiliki prinsip dasar yang sama dalam menjaga keamanan informasi. Melalui teknik-teknik ini, berbagai teks penting dapat terlindungi kerahasiaannya dan keotentikannya, sehingga membangun kepercayaan antara pihak-pihak yang berkorespondensi.

1.3.2 Tujuan Kriptografi

Kriptografi adalah ilmu yang mempelajari teknik-teknik untuk mengamankan informasi, yang memiliki beberapa tujuan utama dalam meningkatkan keamanan data. Berikut adalah penjelasan mengenai tujuan-tujuan tersebut:

1. Kerahasiaan

Cryptography berfungsi untuk menjaga kerahasiaan informasi, dan memastikan bahwa hanya pihak yang berwenang yang dapat mengaksesnya. Kriptografi adalah teknik yang melindungi isi pesan dengan cara menyandikan informasi sehingga hanya penerima yang memiliki kunci dekripsi yang dapat membukanya. Kerahasiaan dalam kriptografi berlaku untuk siapa saja, tidak hanya untuk Anda yang memiliki kunci rahasia atau kata sandi yang tepat. Misalnya, banyak aplikasi *chatting* saat ini menggunakan teknik kriptografi untuk melindungi isi pesan, sehingga pesan tersebut tidak dapat diakses oleh pihak ketiga yang tidak berwenang.

2. Integritas data

Tujuan lainnya dari Cryptography adalah penting pentingnya dalam menjaga integritas data dengan mencegah perubahan yang tidak sah. Misalnya, sistem kriptografi diperlukan untuk melindungi informasi dari serangan *hacker* yang tidak bertanggung jawab. Untuk mempertahankan integritas data, diperlukan sistem yang mampu mendeteksi *data manipulation* oleh pihak lain. Manipulasi ini dapat mencakup penyisipan, penghapusan, atau pensubstitusian data asli. Kriptografi menjamin bahwa informasi tetap utuh dan tidak dimanipulasi selama proses pengiriman atau penyimpanan hingga mencapai tujuan akhir.

3. Autentikasi

Autentikasi berkaitan erat dengan pengenalan dan identifikasi antara kedua belah pihak yang berkomunikasi. Setiap pihak wajib memperkenalkan diri dan memastikan bahwa informasi yang dibagikan melalui kanal komunikasi telah diautentikasi kebenarannya. Informasi yang diautentikasi ini mencakup isi data, waktu pengiriman, dan detail lainnya. Di sinilah kriptografi berperan, khususnya melalui penggunaan sertifikat digital. Sertifikat digital adalah dokumen elektronik yang mengaitkan identitas pemilik

kunci publik dengan otoritas sertifikasi (*Certification Authority* atau CA) yang terpercaya. CA bertanggung jawab untuk memverifikasi identitas pemilik sebelum menerbitkan sertifikat digital tersebut.Informasi yang terdapat dalam sertifikat digital, seperti nama, alamat email, dan masa berlaku sertifikat, dapat digunakan untuk memverifikasi identitas pengirim pesan atau dokumen elektronik.

Sebagai contoh, saat berbelanja online, sertifikat digital digunakan untuk memverifikasi identitas situs web toko online dan memastikan bahwa informasi pembayaran yang digunakan aman.

4. Non repudiasi

Kriptografi adalah solusi untuk mencegah akses oleh pihak yang tidak berwenang dalam pengiriman atau penandatanganan informasi. Non repudiasi, atau anti penyangkalan, adalah langkah penting dalam kriptografi yang bertujuan mencegah pengirim informasi dari menyangkal pengiriman pesan yang telah dilakukan. Dengan kata lain, non repudiasi memastikan bahwa baik pengirim maupun penerima tidak dapat mengklaim bahwa mereka tidak pernah mengirim atau menerima pesan tersebut. Contoh dalam menggunakan teknik kriptografi adalah tanda tangan digital dapat mengikat kedua belah pihak pada kontrak elektronik.

Tujuannya agar mereka tidak dapat menyangkal telah menandatangani dokumen tersebut di masa depan. Ini memberikan keamanan tambahan dalam transaksi elektronik, memastikan bahwa setiap pihak bertanggung jawab atas tindakan mereka.

1.3.3.Jenis Metode Kriptografi

Metode-metode kriptografi yang biasa digunakan dapat dibagi menjadi tiga jenis: Simetris, Asimetris, dan Hibrid. Berikut adalah deskripsi singkat untuk setiap jenis tersebut:

1. **Simetris**

   Kriptografi adalah suatu algoritma yang menggunakan kunci simetris serta kripto *polyalphabetic*. Jenis *cryptography* ini juga sering dikenal dengan sebutan *hill cipher* atau kode *hill*.

   Teknik kriptografi ini diciptakan oleh Lester S. Hill pada tahun 1929 dengan tujuan menciptakan *cipher* yang sulit dipecahkan, bahkan ketika menggunakan teknik analisis frekuensi.

2. **Asimetris**

Kriptografi asimetris atau *asymmetric cryptography* memanfaatkan dua kunci berbeda, yaitu kunci publik dan kunci privat. Anda dapat membagikan kunci publik secara bebas, sementara kunci privat harus dijaga kerahasiaannya. Pesan yang dienkripsi dengan kunci publik hanya dapat didekripsi menggunakan kunci privat yang sesuai. Sistem ini dikenal sebagai bagian dari teknik kriptografi modern. Selain itu, kriptografi asimetris dianggap lebih aman dibandingkan dengan kriptografi simetris karena tidak memerlukan distribusi kunci rahasia yang aman.

Salah satu contoh algoritma dalam kriptografi asimetris yang terkenal adalah RSA (*Rivest–Shamir–Adleman*). Keunggulan dari *cryptography* ini adalah informasi yang dienkripsi sulit untuk dipecahkan, berkat penggunaan algoritma matematika yang canggih dan teknologi komputer yang modern.

3. Hibrid

Jenis kriptografi yang terakhir adalah kriptografi hibrid. Jenis ini diciptakan untuk mengatasi masalah *trade-off* antara kecepatan dan kenyamanan. Semakin aman sistem kriptografi, semakin kurang nyaman penggunaannya. Sebaliknya, jika sistem dirancang untuk memberikan kenyamanan lebih, maka tingkat keamanannya akan berkurang. Teknik kriptografi ini berusaha menemukan keseimbangan optimal antara kedua faktor tersebut, sehingga pengguna dapat menikmati keamanan tinggi.

1.3.4 Teknik Kriptografi

Teknik kriptografi mencakup berbagai metode untuk mengamankan data. Berikut adalah 5 teknik utama yang sering digunakan:

1. Substitusi

Teknik substitusi merupakan metode enkripsi klasik yang mengganti karakter asli pesan dengan karakter lain berdasarkan aturan tertentu. Contoh sederhana dari teknik ini adalah sandi *Caesar*, yang secara efektif menggantikan huruf dalam pesan dengan huruf lain dalam urutan tertentu.

2. Transposisi

Teknik transposisi merupakan salah satu metode dalam kriptografi yang menggunakan enkripsi klasik. Pesan tersebut akan tampak tidak terbaca bagi siapa pun yang tidak memiliki kunci enkripsi. *Cryptography* ini untuk menjaga kerahasiaan informasi dengan mengacak posisi karakter.

3. Enkripsi Blok

Enkripsi blok merupakan proses di mana pesan dibagi menjadi beberapa blok data, dan setiap blok kemudian dienkripsi menggunakan algoritma tertentu. Teknik kriptografi ini penting dalam menjaga keamanan informasi, di mana setiap blok yang dihasilkan memberikan lapisan perlindungan tambahan.

4. Enkripsi Stream

Salah satu teknik *Cryptography* lainnya untuk mengamankan data adalah Enkripsi *Stream*. Teknik ini merupakan proses yang mengenkripsi pesan dengan cara berurutan, bit demi bit.

5. Hashing

Hashing merupakan metode yang mengonversi data digital, seperti teks, gambar, atau file, menjadi *string* kode unik dengan panjang tetap yang dikenal sebagai *hash value* atau *digest*. Dalam konteks kriptografi, teknik ini sering digunakan untuk memverifikasi integritas data.

1.3.5 Kriptografi Modern

Perkembangan ilmu komputer telah mengubah wajah kriptografi secara drastis. Dengan kemampuan untuk mengembangkan dan menerapkan algoritma kriptografi yang kompleks dengan lebih mudah dan efisien, kriptografi modern kini berakar pada konsep matematika dan komputer yang rumit, didukung oleh algoritma yang canggih.

Saat ini, standar kriptografi yang umum digunakan terus berkembang dan diaudit dengan ketat untuk menjamin keamanannya serta memenuhi standar industri. Beberapa contoh penggunaan kriptografi modern dalam kehidupan sehari-hari meliputi:

1. Belanja online: Informasi kartu kredit Anda dienkripsi menggunakan *Cryptography* untuk mencegah pencurian data.
2. Akses rekening bank online: *Cryptography* memastikan koneksi yang aman, melindungi informasi login, dan menjaga transaksi dengan tanda tangan digital.
3. Pengiriman email: *Cryptography* mengenkripsi isi email untuk menjaga kerahasiaan pesan.
4. Koneksi VPN: *Cryptography* mengenkripsi data yang dikirim dan diterima melalui jaringan internet publik untuk melindungi informasi.

1.3.6 Kriptografi sebagai Cara Meningkatkan Keamanan Data

Tanpa perlindungan yang memadai dan penggunaan *Cryptography*, data pribadi dan transaksi online kita dapat terancam oleh berbagai serangan siber, yang tidak hanya merugikan individu tetapi juga dapat mengganggu kepercayaan dalam transaksi digital.

Oleh karena itu, memahami dan memanfaatkan kriptografi sangat penting untuk menghadapi tantangan keamanan yang terus berkembang. Jangan anggap remeh pentingnya kriptografi! Mengabaikan manfaat dan fungsinya bisa berisiko pada privasi dan keamanan informasi.

1.4 Message Authentication Code

a. Teknik autentikasi (dalam komunikasi data) adalah prosedur yang digunakan untuk membuktikan:
b. Keaslian pesan (message integrity)
c. Keaslian identitas pengirim (userauthentication).
d. Pengirim tidak dapat menyangkal isipesan (non-repudiation
e. Otorisasi berkaitan dengan hak akses untuk masuk ke dalam sistem dan Otorisasi umumnya ditangani dengan penggunaan sandi-lewat (password

Teknik autentikasi: Ada dua cara untuk otentikasi pesan: Menggunakan tanda-tangan digital (digital signature)

a) Tanda-tangan dilekatkan (embed) pada pesan Menggunakan MAC (Message Authentication Code)
b) Kode MAC dilekatkan pada pesan

Perbedaannya:

a) MAC tidak dapat menyediakan mekanisme untuk anti-penyangkalan.
b) MAC: fungsi satu-arah yang menggunakan kunci rahasia (secret key) dalam pembangkitan nilai hash
c) Bandingkan dengan MD5 atau SHA yang tidak memerlukan kunci untuk menghasilkan nilai hash.
d) Nilai hash yang dihasilkan selalu berukuran tetap (fixed) untuk ukuran pesan berapa saja
e) MAC dilekatkan (embed) pada pesan. Selanjutnya, MAC digunakan untuk otentikasi tanpa perlu merahasiakan pesan.
f) MAC bukanlah tanda-tangan digital. MAC hanya menyediakan otentikasi pengirim dan integritas pesan saja.

1.4.1 Tanda tangan digital

Sejak zaman dahulu, tanda-tangan sudah digunakan untuk otentikasi dokumen cetak.Tanda-tangan mempunyai karakteristik sebagai berikut:

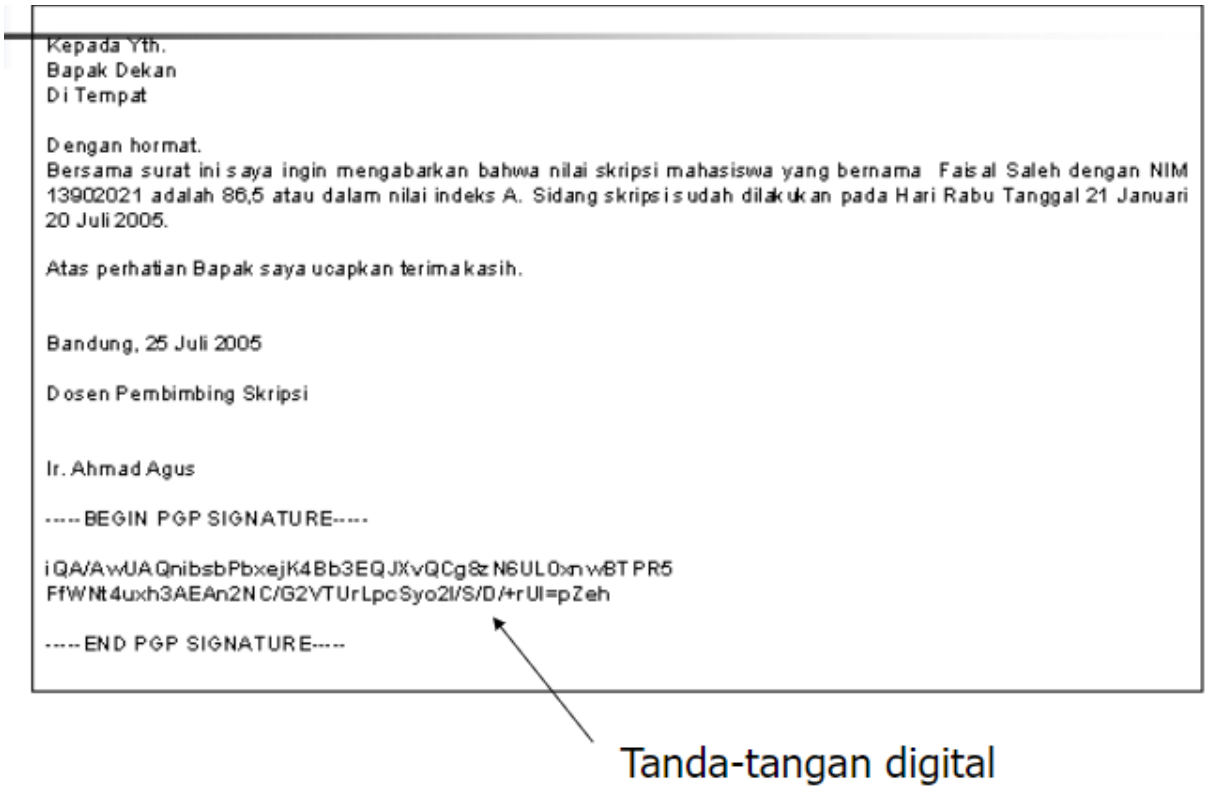
- Tanda-tangan adalah bukti yang otentik.

- Tanda tangan tidak dapat dilupakan.

- Tanda-tangan tidak dapat dipindah untuk digunakan ulang.
- Dokumen yang telah ditandatangani tidak dapat diubah.
- Tanda-tangan tidak dapat disangkal(repudiation).
- fungsi tanda tangan pada dokumen kertas juga diterapkan untuk otentikasi pada data digital (pesan, dokumen elektronik).
- Tanda-tangan untuk data digital dinamakan tanda-tangan digital.Tanda-tangan digital bukanlah tulisan tanda-tangan yang di-digitisasi (di-scan).

Gambar 3.1 Tanda tangan digital

- Tanda-tangan digital adalah nilai kriptografis yang bergantung pada isi pesan dan kunci.
- Tanda-tangan pada dokumen cetak selalu sama, apa pun isi dokumennya.
- Tanda-tangan digital selalu berbeda-beda antara satu isi dokumen dengan dokumen lain.



Gambar 3.2 Tanda tangan digital kriptografi

Ada Dua cara menandatangani pesan:

1. **Menggunakan kriptografi simetri** , Pesan yang dienkripsi dengan algoritma simetri sudah memberikan solusi untuk otentikasi pengirim dan keaslian pesan, karena kunci simetri hanya diketahui oleh pengirim dan penerima. namun cara ini tidak menyediakan mekanisme untuk anti-penyangkalan. Agar dapat mengatasi masalah penyangkalan, maka diperlukan pihak ketiga yang dipercaya oleh pengirim/penerima.Pihak ketiga ini disebut penengah (arbitrase).

   Misalkan BB (Big Brothers) adalah otoritas arbitrase yang dipercaya oleh Alice dan Bob.

   BB memberikan kunci rahasia KA kepada Alice dan kunci rahasia KB kepada Bob.

   Hanya Alice dan BB yang mengetahui KA, begitu juga hanya Bob dan BB yang mengetahui KB.

   Jika Alice menyangkal telah mengirim pesan tersebut, maka pernyataan dari BB pada pesan yang diterima oleh Bob digunakan untuk menolak penyangkalan Alice.

   Bagaimana BB tahu bahwa pesan tersebut dari Alice dan bukan dari Charlie?

   Karena hanya BB dan Alice yang mengetahui kunci rahasia, maka hanya Alice yang dapat mengenkripsi pesan dengan kunci terebut.

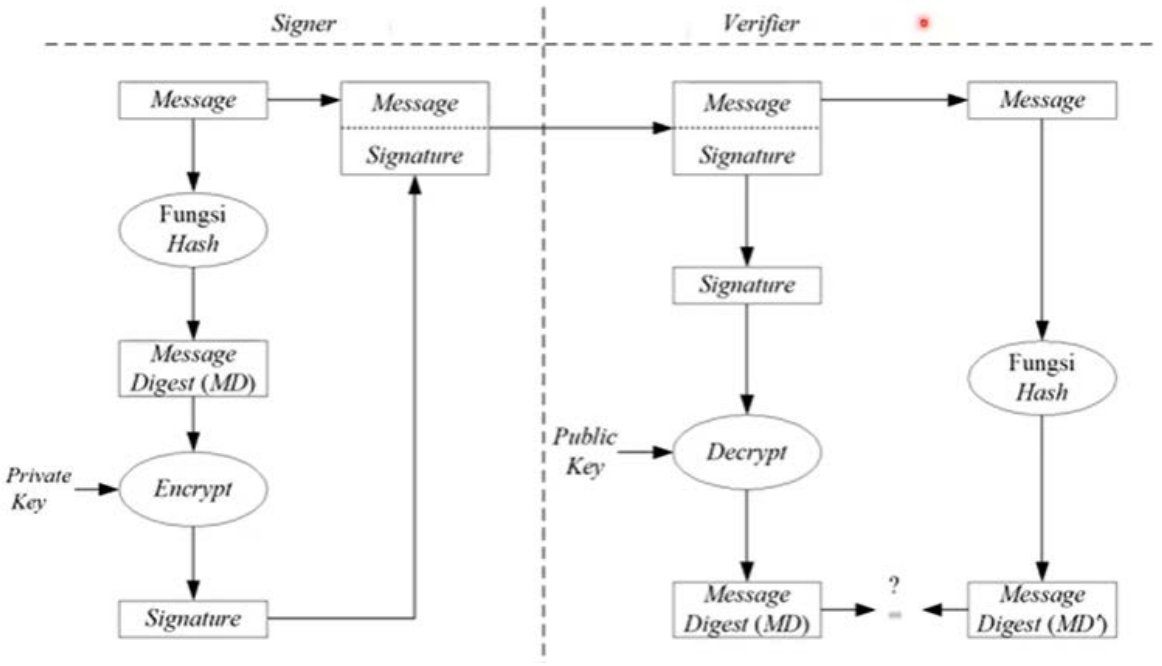
2. **Mengunakan kriptografi kunci-publik**

Gambar 3.3 Kriptografi kunci public

a. Beberapa agoritma kunci-publik dapat digunakan untuk menandatangani pesan dengan cara mengenkripsinya, asalkan algoritma tersebut memenuhi sifat:
   Keterangan:
   PK = kunci public
   SK = kunci privat (secret key).
   E = fungsi enkripsi
   D = fungsi dekripsi
   M = pesanContoh

3. **Menggunakan Krptografi kunci-publik dan Fungsi Hash**

1) Penandanganan pesan dengan cara mengenkripsinya selalu memberikan dua fungsi berbeda: kerahasiaan pesan dan otentikasi pesan.
2) Pada beberapa kasus, seringkali otentikasi yang diperlukan, tetapi kerahasiaan pesan tidak. Maksudnya, pesan tidak perlu dienkripsikan, sebab yang dibutuhkan hanya keotentikan pesan saja.
3) Algoritma kunci-publik dan fungsi hash dapat digunakan untuk kasus seperti ini.



Gambar 1.4 Verifikasi Tanda Tangan

Langkah-langkah verifikasi tanda-tangan

1. Penerima menghitung nilai hash dari pesan M yang akan dikirim, misalkan nilai hash dari M adalah h'.

2. Penerima melakukan dekripsi terhadap tanda-tangan S dengan kunci publik si pengirim menggunakan persamaan dekripsi RSA: h = SPK mod n yang dalam hal ini PK adalah kunci privat pengirim dan n adalah modulus (n = pq, p dan q adalah dua buah bilangan prima).

3. Penerima membandingkan h dengan h'. Jika h = h' maka tanda-tangan digital adalah otentik. Jika tidak sama, maka tanda-tangan tidak otentik sehingga pesan dianggap tidak asli lagi atau pengirimnya

4. Fungsi Hash Disebut juga sidik jari (fingerprint), message integrity check, atau manipulation detection code Untuk integrity-check

5. Dokumen/pesan yang diubah 1 titik saja, sidik jarinya akan sangat berbada

1.5 (SSL atau Secure Sockets Layer)

SSL, atau Secure Sockets Layer) adalah protokol keamanan yang mengenkripsi komunikasi antara pengguna dan website. Hal ini bertujuan untuk melindungi data sensitif, seperti informasi pribadi, informasi login, dan detail transaksi, dari serangan oleh pihak yang tidak berwenang.

Dengan menggunakan SSL, data seperti informasi login, detail kartu kredit, atau data pribadi lainnya akan dienkripsi menjadi format yang tidak dapat dibaca oleh pihak yang tidak berwenang. Hal ini memastikan bahwa informasi sensitif tetap aman dan tidak dapat diakses oleh pihak yang tidak sah saat transit melalui jaringan internet.

Selain enkripsi, SSL juga menyediakan verifikasi identitas. Ketika sebuah situs web menggunakan SSL, server web akan mengirimkan sertifikat digital yang berisi informasi tentang identitasnya kepada browser pengguna. Browser kemudian akan memverifikasi keaslian sertifikat ini dengan otoritas sertifikat yang terpercaya. Jika verifikasi berhasil, browser akan menampilkan indikator keamanan, seperti ikon gembok atau tulisan "https" pada URL, untuk menunjukkan bahwa koneksi aman.

1.5.1 Contoh Aplikasi Dengan SSL

suatu sistem yang memiliki teknologi yang canggih dan keakuratan yang baik, proteksi yang kuat, berbeda untuk tiap ras, stabilitas pola dapat diperoleh dalam jarak jauh (1 meter) dan tidak dipengaruhi oleh kacamata.dikembangkan pada tahun 1994 John Daugman.KeuntunganTeknologi yang canggihPotensi ketelitian yang tinggiProses scanning yang cepatStabilitas jangka panjangKerugianHarga yang mahalJika kesahatan mata terganggu, sistem tidak bisa digunakan.

Eye Biometric sistem retina biometric yang Merupakan sistem biometric yang memiliki teknologi yang canggih, dan keakuratan yang baik, serta proteksi yang kuat karena ada di dalam bola mata.

- Keuntungan Teknologi yang canggih

a. Potensi ketelitian yang tinggi
b. Stabilitas jangka panjang
c. Fitur terlindung
d. perbedaan yang tinggi (ras, suku, dan bangsa)

- Kerugian

a. Susah digunakan
b. Faktor kesehatan
c. Harga yang mahal

Perbedaannya Prinsip teknologi retinal scanning adalah memindai pola pembuluh darah kapiler pada retina dengan sumber cahaya intensitas rendah. Prinsip teknologi iris scanning adalah memindai pola warna dari mata dan pupil.

Pada proses autentikasinya dapat dijabarkan sebagai berikut:

- Membutuhkan dua tahap yaitu tahap identifikasi dan tahap verifikasi. Proses ini dapat dilakukan secara one-to-many (1:m) atau one-to one (1:1).Proses one-to-many akan melibatkan satu database yang berisi user id dan iris template masing-masing id.

- Proses capture akan dilanjutkan dengan searching database untuk mencari iris template yang cocok. Sedangkan prosesone-to-one akan lebih pada membandingkan dua iris, yaitu hasil scan dan iris template yang sudah disimpan. Dari ke dua proses ini sudah tentu proses oneto - one lebih disukai sebab prosesnya lebih cepat karena pembandingan dilakukan dalam skala yang terbatas.

- Iris adalah model scanner biometric yang mempunyai tingkat keakuratan tinggi.Iris mempunyai beberapa metode pendeskripsian yaitu metode dougman, wilde, bole. Yang ketiganya memiliki kelebihan dan kekurangannya masing – masing seperti yang dijelaskan diatas.

1.6 Protocol Security Address

Penggunaan berbagai macam aplikasi internet ataupun transaksi elektronik saat ini sudah menjadi bagian dari masyarakat. Namun, dalam penggunaannya selalu dihadapkan dengan berbagai masalah keamanan, salah satunya adalah masih banyaknya protokol di internet yang belum menjamin autentikasi.Salah satu gambaran dari rawannya autentikasi yaitu banyak tools yang bisa digunakan hacker untuk mencuri password dari client atau server, sehingga hacker tersebut bisa menyamar seolah-olah dialah pemilik password tersebut (seperti halnya man in the middle attack). Dengan demikian password bisa disalahgunakan dengan mengatasnamakan pemilik password.Oleh karena itu, penting adanya jaminan autentikasi karena autentikasi merupakan suatu cara untuk mengetahui keaslian dari informasi, juga mengenai keaslian sumbernya

1.6.1 Protokol Keamanan

- Protokol adalah format message yang dipakai untuk berkomunikasi dalam sistem jaringan. Beberapa protokol-protokol keamanan yaitu:

1. Secure Socket Layer (SSL)SSL biasanya digunakan untuk mengamankan komunikasi antara browser Web dengan server Web. SSL membuat sebuah link terenkripsi antara klien dan server yang memerlukan komunikasi dengan aman. Otentikasi bisa dilakukan baik pada server maupun klien. SSL juga dapat dipakai dengan aplikasi-aplikasi lain, seperti ftp, telnet, dan lainnya.

- Simple Key Management for Internet Protocol (SKIP). SKIP adalah protokol pertukaran secret key yang beroperasi di bawah layer IP dalam protokol komunikasi TCP/IP. Metode ini dapat dipakai untuk menyediakan keamanan yang transparan antar entitas.

- Security Multi-part for MIME (S/MIME)S/MIME adalah protokol keamanan aplikasi. Diimplementasikan pada tetapi dapat lebih luas dipakai dalam pesan-pesan yang bersifat store-and-forward

- Internet Protocol Security Extension (IPSec). IPSec adalah protokol keamanan yang didefinisikan untuk jaringan IP, yang beroperasi pada layer network dalam protokol komunikasi TCP/IP. IPsec menambahkan perpanjangan header pada protokol komunikasi IP dan didesain untuk memberikan keamanan end-to-end bagi paket-paket yang melintasi Internet. Internet protokol adalah jantung dari TCP/IP.

- Internet Key Exchange (IKE)IKE menyediakan manajemen keamanan dan pertukaran kunci kriptografi antar perangkat yang berjauhan. Ini adalah standar mekanisme pertukaran kunci untuk IPsec.

- Protokol AAA (Authentication, Authorization, Accounting) digunakan untuk mengatur mekanisme bagaimana tata cara berkomunikasi, baik antara client ke domain-domain

jaringan maupun antar client dengan domain yang berbeda dengan tetap menjaga keamanan pertukaran data.

Service Yang Digunakan Untuk Protokol Keamanan Berbasis AAA, Terdiri Dari**:**

- Karberos merupakan protokol keamanan yang bekerja menggunakan secret key . Karberos menggunakan algoritma kriptografi Data Encryption Standart (DES) untuk proses enkripsi dan authentikasinya.Dalam implementasinya karberos biasanya menggunakan tiket atau voucher yang mempunyai jangka waktu. Tiket ini digunakan untuk melakukan koneksi terhadap jaringan yang ingin diakses dengan menggunakan service karberos terhadap authentikasinya.

- Kerberos ini merupakan metode pengamanan TCP/IP berbasis server-based password authentication. Pada sistem kerberos server, service yang disediakan oleh server dibatasi oleh suatu daftar host serta daftar user yang boleh dan tidah boleh menggunakan layanan Beberapa contoh implementasi service jaringan yang umumnya memerlukan autentikasi, antara lain penggunaan printer pada sebuah jaringan yang hanya diperbolehkan bagi anggota kelompok saja,remote file access, remote login (rlogin), window system, mail dimana pemilik address saja yang dapat mengambil di POP3, danservice management.

- Tacacs+ merupakan protokol keamanan cukup banyak digunakan saat ini di masyarakat, karena telah melalui beberapa pengembangan dan modifikasi oleh Cisco System, istilah kerennya saat ini Tacacs+ merupakan proprietary milik perangkat jaringan bermerk Cisco dan hanya digunakan di dalam perangkat bermerk tersebut.Service Tacacs ini disimpan dalam database pada program Tacacs Daemon yang berjalan pada sistem operasi windows ataupun Unix. Protokol Tacacs+ bekerja dengan menggunakan protokol komunikasi TCP/IP Port 49 yang terkenal lebih percaya dalam menghantarkan informasi.

- Radius (Remote Authentication Dial-in User Service) merupakan protokol security yang bekerja menggunakan sistem client / server terdistribusi yang banyak digunakan bersama AAA untuk mengamankan jaringan dari orang yang tidak berhak.Dalam topologinya RADIUS klien merupakan perangkat router atau NAS, sedangkan server otentikasinya merupakan RADIUS Server. Dalam server ini semua informasi dan account dari client ditampung.RADIUS menggunakan protokol UDP (User Datagram Protocol) dan menggunakan port 1812 untuk authentication dan 1813 untuk accounting.Saat ini radius banyak digunakan untuk authentikasi hotspot dengan billing system.

- Tacacs+ menggunakan TCP sementara Radius menggunakan UDP. TCP menawarkan transportasi berorientasi koneksi sehingga keamanan data yang dikirim masih sangat terjamin keutuhannya namun memang membutuhkan waktu yang lebih lama pada proses transportasi datanya dibanding UDP, sedangkan UDP menawarkan pengiriman usaha yang terbaik.Tacacs+ server dan Radius server dapat digunakan dalam berbagai macam topologi baik untuk autentikasi antar router yang tehubung dengan PPP, login user pada sebuah website, maupun login user pada sebuah hotspot.Sangat disarankan untuk kepentingan yang mengutamakan keamanan data lebih baik menggunakan Tacacs+, sementara jika digunakan hanya untuk kecepatan akses lebih baik menggunakan Radius.

1.7 Firewall Sistem Keamanan Komputer

- Firewall Berupa seperangkat hardware atau software, bisa juga berupa seperangkat aturan dan prosedur yang ditetapkan oleh organisasi.Sistem Security yang menggunakan device atau sistem yang diletakkan di dua jaringan dengan fungsi utama melakukan filtering terhadap akses yang akan masukBox h/w = PIX Firewall cisco, Pasport Nortel, Checkpoint, Cyberguard,...• H/w atau s/w yang penting "policy“

- Sebagai akses unauthorized yang akan keluar atau masuk ke jaringan LAN dan ke Internet.Seorang satpam yang akan memerikasa semua orang yang akan masuk dan keluar,Kebijakan direktur perusahaan tersebut, satpam hanya menjaga dan menjalankan perintah yang diterimanya

1.7.1 Metode Firewall

- Packet filtering & analysis Protocol (TCP/UDP) Port address Keyword Ip address ApplicationPada umumnya sebuah Internet Firewall diinstall di antara jaringan internal yang terhubung dengan Internet.

1.7.1 Fungsi Firewall

- Firewall sebagai focus keputusan security, Bayangkan firewall sebagai choke point, semua traffic yang masuk dan keluar harus melewati" pos pemeriksaan",

- Firewall Mendukung Security Policy Misalnya Perusahaan menetapkan penggunaan NAT (Network Address Translation),hanya user atau grouphanya protocol tertentu,hanya beberapa aplikasi dan sumber dayaWaktu akses Akses dari tempat tertentu.

- Mencatat Log Aktivitas User, oleh karena trafik melewati firewall, maka disini dapat kita buat suatu system untuk mencatat semua kegiatan system dan user yang menggunakan jaringan. Sebagai dokumentasi yang tepat untuk menentukan policy (AAA)

1.7.3 Metode-Metode Firewall

- Pertimbangan Apa yang akan diproteksi

- Membeli / membangun sendiri

- Box atau by software

- Fasilitas yang disediakan (log, analys,...)Memperhatikan "brand" & standar dipasar

- Anggaran biaya

- User policy

- Upgradeable & standarisasi NCSA (National Computer Security Associates)• Vendor dan dukungan teknis

- Proxy Server merupakan Memenuhi permintaan user untuk layanan Internet (http, FTP,Telnet) dan mengirimkannya sesuai dengan kebijakanBertindak sebagai gateway menuju layananMewakili paket data dari dalam dan dari luarMenangani semua komunikasi internet -ekternal

1.8 Cara Mudah Tingkatkan Keamanan Komputer

Dilansir dari (https://www.liputan6.com/tekno/read/3227324/ini- 7-cara-mudah-tingkatkan-keamanan-komputer), komputer dan laptop merupakan perangkat teknologi yang sering digunakan dalam keseharian. Namun, komputer yang terhubung ke jaringan internet bisa mengancam data dan privasi para penggunanya. Internet memang memudahkan berbagai aktivitas, tapi pengguna tetap harus waspada karena ada berbagai ancaman siber yang mengancam data-data mereka. Oleh karena itu, pengguna komputer atau laptop harus selalu berhati-hati agar data mereka tetap terjaga. Berikut 7 (tujuh) cara untuk meningkatkan keamanan komputer agar terbebas dari berbagai hal yang tidak diinginkan, termasuk malware:

1. **Gunakan selalu Incognito mode saat berada di luar**

   Saat berpergian, kalian terkadang memerlukan komputer atau laptop seperti untuk mengakses email dan media sosial. Untuk melakukan aktivitas tersebut, maka dibutuhkan jaringan internet.

   Fitur Incognito mode sangat berguna ketika mengakses data penting saat berselancar internet, terutama di tempat publik. Saat masuk dalam mode ini, kalian tidak perlu terlalu mengkhawatirkan data yang tersimpan, bahkan saat lupa menekan tombol logout. Incognito mode adalah fitur privasi pada situs web untuk menonaktifkan history dan cache browsing.

2. **Pakai Antivirus**

   Saat membeli komputer baru, banyak orang khawatir mengenai fitur keamanannya. Kekhawatiran tersebut membuat mereka memasang beberapa aplikasi keamanan sekaligus seperti antivirus dan antispyware. Padahal, hal ini akan membebani kinerja komputer yang berimbas pada performa.

   Untuk mengatasi permasalahan semacam itu, saat ini OS seperti Windows 10 sudah menyediakan antivirus bawaan. Namun jika masih terasa kurang, kalian cukup memasang satu antivirus lagi sesuai dengan yang diinginkan.

3. **Selalu update OS dan aplikasi**

   Ada sejumlah orang yang tidak peduli terhadap versi terbaru OS atau aplikasi yang digunakan pada komputer. Berbagai alasan dituturkan seperti proses update lama hingga kinerja komputer akan menurun. Menggunakan versi terbaru OS dan aplikasi merupakan salah satu cara untuk membuat komputer tetap aman. Selain terkait dengan keamanan, proses update terutama OS justru akan meningkatkan performa komputer.

4. **Ganti password secara berkala**

   Mengganti password secara berkala setiap enam bulan hingga satu tahun sekali sangat dianjurkan. Selain itu, sebaiknya gunakan password kuat dengan berbagai kombinasi di dalamnya seperti huruf, angka dan simbol. Kalian bisa menggunakan aplikasi kalender untuk memberikan pemberitahuan jika sudah saatnya mengganti password. Kalian juga bisa menggunakan sejumlah aplikasi password manager untuk mengelola password pada berbagai akun online.

5. **Backup data dan dokumen penting**

   Jika kalian sering bekerja secara offline, pasti akan menyimpan data dan dokumen pada drive penyimpanan yang tersedia. Untuk mencegah kehilangan data yang disebabkan berbagai hal, kalian dapat melakukan proses backup.Saat ini ada banyak layanan cloud seperti OneDrive atau Dropbox untuk menyimpan data dan dokumen secara online. Bagi yang jarang terhubung ke internet, bisa menyimpan data-data tersebut pada flashdisk atau hard disk eksternal.

   Salah satu aktivitas yang sering dilakukan menggunakan komputer adalah belanja online. Selain menghemat waktu dan tenaga, barang yang dijual di situs belanja online juga jauh lebih murah. Namun, kalian harus berhati-hati dan jangan sembarang melakukan pembayaran secara online.Gunakan platform e-Commerce terpercaya dalam melakukan sistem pembayaran. Untuk mencegah penipuan, hindari memberikan data pribadi dan nomor rekening pada saat berbelanja secara pribadi.

6. **Jangan sembarangan melakukan pembayaran online**

   Salah satu aktivitas yang sering dilakukan menggunakan komputer adalah belanja online. Selain menghemat waktu dan tenaga, barang yang dijual di situs belanja online juga jauh lebih murah. Namun, kalian harus berhati-hati dan jangan sembarang melakukan pembayaran secara online.

   Gunakan platform e-Commerce terpercaya dalam melakukan sistem pembayaran. Untuk mencegah penipuan, hindari memberikan data pribadi dan nomor rekening pada saat berbelanja secara pribadi.

7. **Abaikan pesan spam**

   Pengguna komputer sering kali menerina pesan berantai berisi promosi atau iklan menarik di berbagai media sosial. Hal ini sangat berbahaya, terutama jika ternyata itu adalah pesan spam. Oleh karena itu, jangan pernah membuka link di dalam pesan spam tersebut.

   Hal pertama yang perlu dilakukan adalah memastikan link tersebut asli dan bukan jebakan dari penjahat siber. Gunakan Google untuk memeriksa situs web resmi dari pesan yang diterima. Segera hapus jika ternyata pesan tersebut mencurigakan.

DAFTAR PUSTAKA

Anonymous. Sejarah Keamanan Komputer. 2017.https://mti.binus.acnovermber 2018

Anonymous. Pengertian dan Aspek-Aspek Keamanan Komputer. 2018. https://www.ayoksinau.com/pengertian-dan-aspek-aspek-keamanan-komputerlengkap/ diakses novermber 2018

Anwar, N , Modul online, matakuliah system operasi materi system keamanan, 2018.

Stallings, W Cryptography and Network Security , 2016

Kizza, J.MA Guide to Computer Network Security , 2005