SISTEM PEGAMANAN KOMPUTER

1. Aspek aspek keamanan komputer
2. Security Methodology
3. kriptografi

Disampaikan oleh: WANHENDRA. M.SI

Aspek aspek keamanan komputer

Authentication:

Agar penerima informasi dapat memastikan keaslian pesan tersebut datang dari yang dimintai informasi. (asli dari org yang dikehendai)

Integrity:

Keaslian pesan yang dikirim melalui sebuah jaringan dan dapat dipastikan Bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak dalam perjalanan informasi tersebut

Nonrepudiation:

Merupakan hal yang bersangkutan dengan sipengirim. Sipengirim tidak dapat mengelak bahwa dialah yang mengirim informasi tersebbut.

Authority:

Informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak atas akses tersebut.

Confidentiality:
Merupakan usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Confidentiality merupakan berhubungan dengan informasi yang diberikan kepada pihak lain.

Privacy:
Merupakan lebih kearah data-data yang sifatnya privat(pribadi)

Availability:
Aspek availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan

Access control:
Aspek ini berhubungan dengan cara pengaturan akses kepada informasi. Hal itu biasanya berhubungan dangan masalah authentication dan juga privacy.

Aspek-Aspek ancaman keamanan

Interruption

Merupakan suatu ancaman terhadap availability.informasi dan data yang ada dalam sistem komputer dirusak dan dihapus sehingga jika dibutuhkan, data atau informasi tersebut tidak ada lagi.

Interception

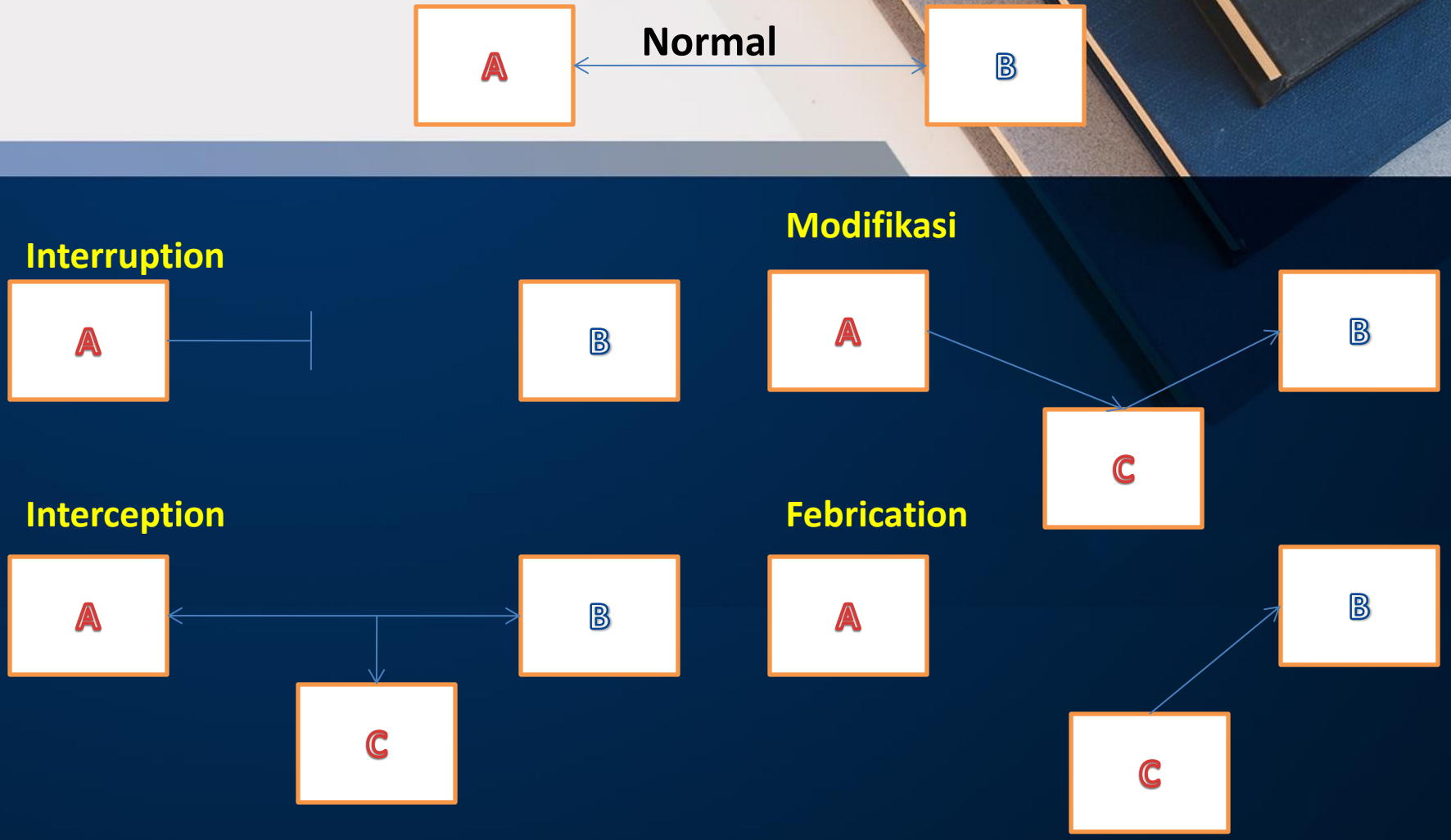
Merupakan ancaman terhadap kerahasiaan (secrecy). Informasi yang ada disadap atau orang yang tidak berhak mendapatkan akses kekomputer dimana informasi tersebut disimpan.

Modifikasi

Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalulintas informasi yang sedang dikirim dan diubah sesuai keinginan tersebut.

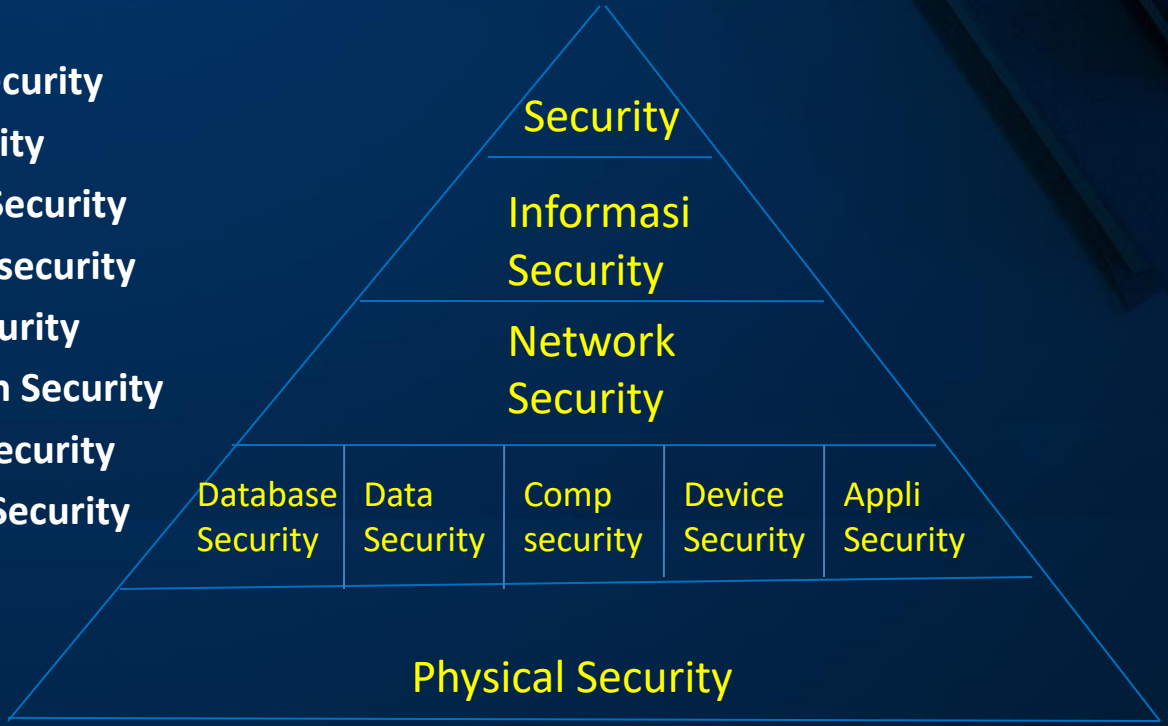
Febrication

Merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru (memalsukan) suatu informasi yang ada sehingga orang yang menerima informasi tersebut menyangka informasi tersebut berasal dari orang yang dikehendaki oleh sipenerima informasi tersebut.


A
Normal
B
Interruption
A
B
Modifikasi
A
B
C
Interception
A
B
C
Febrication
A
B
C

Security Methodology

- Physical Security
- Data Security
- Database Security
- Computer security
- Device Security
- Application Security
- Network Security
- Informasi Security
- Security



Kriptografi

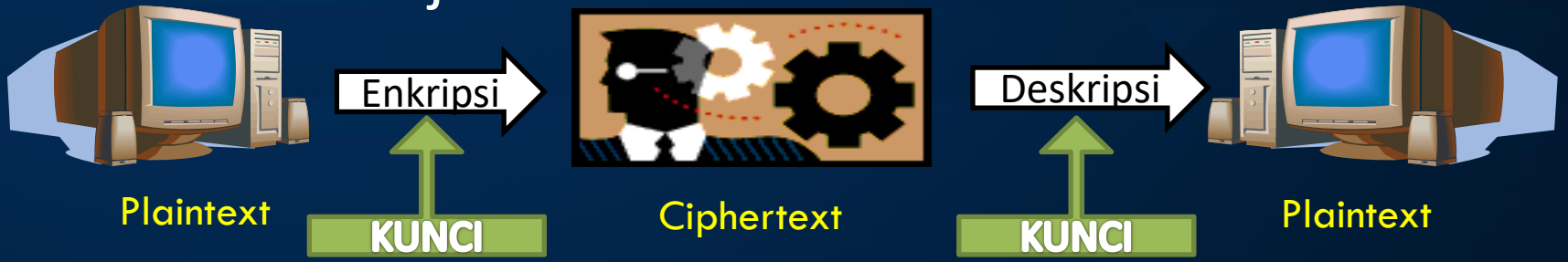
Dari bahasa Yunani

- Kripto = rahasia
- Graphia = tulisan

Menurut terminologinya kriptografi adalah ilmu seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain.

Konsep Kriptografi

- Enkripsi = merubah pesan atau data menjadi bentuk yang sulit diartikan
- Deskripsi = merubah pesan atau data yang sulit diartikan menjadi mudah untuk diartikan atau dibaca



Kriptografi klasik

Kriptografi merupakan suatu strategi supaya data atau dokumen kita aman dari orang yang tidak berhak.

-Teknik Substitusi Cipher merupakan penggantian setiap karakter dari plaintext dengan karakter lainnya.

-Teknik Shift Cipher Teknik dari Shift Cipher dengan modulus 26 memberikan angka ke setiap alphabet seperti a<--->0,.....z <---->25 (Jika lebih dari 26 setelah ditambah kunci, maka dikurangi dengan 26 seperti 22+11=33-26=7 setelah di-convert menjadi huruf kita akan mandapatkan ciphertext.

Ex :Teknik Substitusi Cipher

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

Plain text = Keamanan

Chipher text =

Key : roberto =

Ex :Teknik Substitusi Cipher

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

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

Plain text = Keamanan jiwa bulan puasa ramadhan
Chipher text =

Key 1: roberto =
Key 2: margaret =

Ex :Teknik Substitusi Cipher

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

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

Plain text = Keamanan jiwa bulan puasa ramadhan
Chipher text =

Key 1: roberto =
Key 2: margaret =

Teknik Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plain text = Keamanan

Chipher text = 21,15,11,23,11,24,11,24

V P L X L Y L Y D F C L E

Key : 11 = 11

Chipher text (C) =2+26=28-11=17 (R)

Teknik Shift Cipher

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Plain text = Keamanan S UR A T

Chipher text = 21,15,11,23,11,24,11,24 3,5,2 11 4

V P L X L Y L Y D F C L E

Key : 11 = 11

(C)=2+26=28-11=17 (R)

Tugas

Kriptographia

Tugas kriptographia

1. Teknik Substitusi Cipher
2. Teknik Shift Cipher

Ketentuan: Kerjakan dengan tulis tangan, hasil pekerjaan di scan kumpulkan di ketua kelas dan ketua kelas send ke email: wan.stti@gmail.com

Tugas

1. Teknik Substitusi Cipher

- Plain text = SECURITY WEB
- Chipher text =
- Key 1: Nama depan anda sendiri =
- Key 2: nama dosen matkul SPK = Wanhendra

2. Teknik Shift Cipher

- Plain text = SECURITY WEB
- Chipher text =
- Key : 11 = 11

LATIHAN :
Mendeskrisikan Chipertext

1. Teknik Substitusi Cipher
- Plain text =
- Chipher text =
- Key 1: =
- Key 2: =
2. Teknik Shift Cipher
- Plain text =
- Chipher text =
- Key : =

- Silahkan anda buat proses kedua teknik diatas dengan key sesuai dengan kemauan anda, jika hasilnya sudah dapat anda cukup mengisi chipertexnya saja dan kata kuncinya.
- Untuk plaintext nya maksimal 3 kata kunci EX: (dbms security web)
- Diprint dan dibawa minggu depan.

Format yang dikumpulkan

Nama : Kelas A/B Kode:

Nim :

1. Deskripsikan Chipher text ini : .....

Dengan Teknik Substitusi Cipher

key 1:

Key 2:

Hasil/ plain text:

2. Deskripsikan Chipher text ini : .....

Dengan Teknik Shift Cipher

key 1:

Hasil/ plain text:

Note: Kelas lingkari, kode isi bebas tp samakan kode dengan jawaban Anda (misalnya kode soal 909 maka kode yang dikumpulkan sama 909.

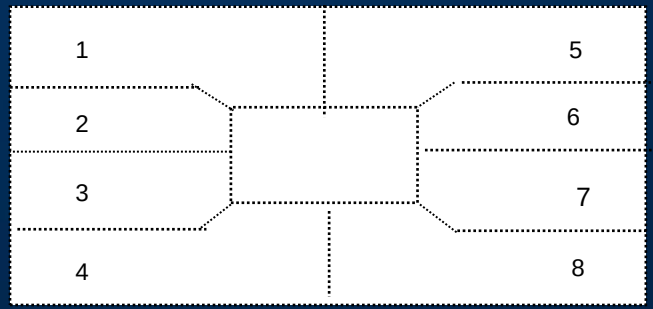
- Kartu Pintar (*Smart Card*)
  - Jenis Memori Pada Kartu Pintar
  - Komunikasi *Kartu Pintar* dengan Aplikasi
- Kriptografi
  - Kunci Simetris
  - Kunci Asimetris
  - Fungsi *Hash* Satu Arah (*one-way hash function*)
  - SECURE SOCKET LAYER (SSL)
  - Tanda Tangan Digital
  - Sertifikasi
  - Masalah Pertukaran Kunci Publik
- Serangan Pada Kartu Pintar (Smart Card)
  - Serangan Secara Logika
  - Serangan Secara Fisik
  - Dumb Mouse
  - Serangan Pertukaran Pesan Melalui Jaringan Komputer

Kartu Pintar (*Smart Card*)

Kartu Pintar *(Smart Card)* merupakan kartu plastik yang memiliki ukuran sama dengan kartu kredit yang berisi *chip* silikon yang disebut *microcontroller*. *Chip* merupakan *integrated circuit (IC)* yang terdiri dari memori dan prosesor. *Chip*, mirip halnya CPU (*Central Processing Unit*) di komputer, yang bertugas melaksanakan perintah dan menyediakan *power* bagi kartu pintar. kartu pintar mempunyai kemampuan untuk memproses dan menginter-pretasikan data, juga dapat menyimpan data tersebut secara aman. Dalam rangka penyesuaian pasar yaitu, untuk mengurangi the *time-to-markets* dan untuk meningkatkan exibilitas aplikasi kartu, di keluarkan generasi baru kartu pintar yang disebut juga Kartu Pintar Terbuka (*Open Smart Card* yang popular dengan sebutan *Open Card*).

Skema Kartu Pintar

Ukuran dan dimensi kartu pintar berdasarkan ISO 7816-95, yaitu panjang 87,6 mm, lebar 53,98 mm dan tebal 0,76 mm, pembagian model fisiknya seperti gambar berikut ini.



Keterangan :

1 = Vcc (5V)	5 = Gnd
2 = R/W	6 = Vpp (12V)
3 = Clock	7 = I/O
4 = Reset	8 = Fuse

Sekarang ini dengan pesatnya perkembangan algoritma kriptografi, data yang disimpan sebelumnya dienkripsi dahulu, sehingga sulit dibaca oleh orang/pihak yang tidak memiliki wewenang/hak akses. Hal ini yang membuat pemalsuan kartu pintar *susah*.

Jenis Memori Pada Kartu Pintar

- *Random Access Memory* (RAM), yang berfungsi untuk menyimpan data sementara ketika proses sedang berjalan.
- *Read Only Memory* (ROM), yang berfungsi untuk menyimpan program utama dan sifatnya permanen.
- *Electrically Erasable Programmable Read Only Memory* (EEPROM), yang berfungsi untuk menyimpan program dan data yang sewaktu-waktu bisa diubah.

Lima Langkah keamanan komputer

Aset Apa yang akan diamankan.

Contoh: ketika mendesain sebuah website

E-commerce, yang perlu dipikirkan adalah?...

Analisis Resiko adalah tentang identifikasi akan resiko yang mungkin akan terjadi, sebuah even yang potensial yang bisa mengakibatkan suatu sistem dirugikan.

Perlindungan pada era jaringan, perlu dikhawatirkan tentang keamanan dari sistem komputer, baik kom puter PC atau pun yang terkoneksi dgn jarigan, seperti LAN yang perlu dilindungi antara user yg terkoneksi dgn LAN.

Alat alat atau tool yang digunakan pada suatu komputer merupakan peran penting dalam hal keamanan karena tool yang digunakan benar-benar aman, (SO open source yg memiliki backdoor ditanamkan oleh pembuatnya u/ keperluan tertentu, maka akan sangat merugikan sistem komputer itu sendiri).

Prioritas Perlindungan komputer secara menyeluruh, hal-hal apa yang memiliki prioritas paling tinggi dari policy (kebijakan) jika keamanan jaringan maka suatu organisari harus membayar harga baik material atau nonmaterial

Strategi dan teknik keamanan komp

Keamanan fisik
Kunci komputer
Keamanan Bios
Keamanan boot loader
Xlock dan vlock

xlock=sebuah pengunci tampilan X
vlock=program kecil sederhana yang memungkinkan mengunci beberapa atau seluruh console pada mesin komputer.

Tugas

Hacker

Kracker

Carding

Pasal-pasal KUHP tentang tindak kejahatan Carding

Thank you ☺

wan.stti@gmail.com