Serangan Terhadap Kriptografi

Bahan kuliah

IF4020 Kriptografi

Pendahuluan

- Keseluruhan *point* dari kriptografi adalah menjaga kerahasiaan plainteks atau kunci dari penyadap (*eavesdropper*) atau kriptanalis (*cryptanalyst*).

- Kriptanalis berusaha memecahkan cipherteks dengan suatu serangan terhadap sistem kriptografi.

Serangan (*attack*)

- **Serangan**: setiap usaha (*attempt*) atau percobaan yang dilakukan oleh kriptanalis untuk menemukan kunci atau menemukan plainteks dari cipherteksnya.
- Asumsi: kriptanalis mengetahui algoritma kriptografi yang digunakan

Prinsip Kerckhoff: Semua algoritma kriptografi harus publik; hanya kunci yang rahasia.

Satu-satunya keamanan terletak pada kunci!

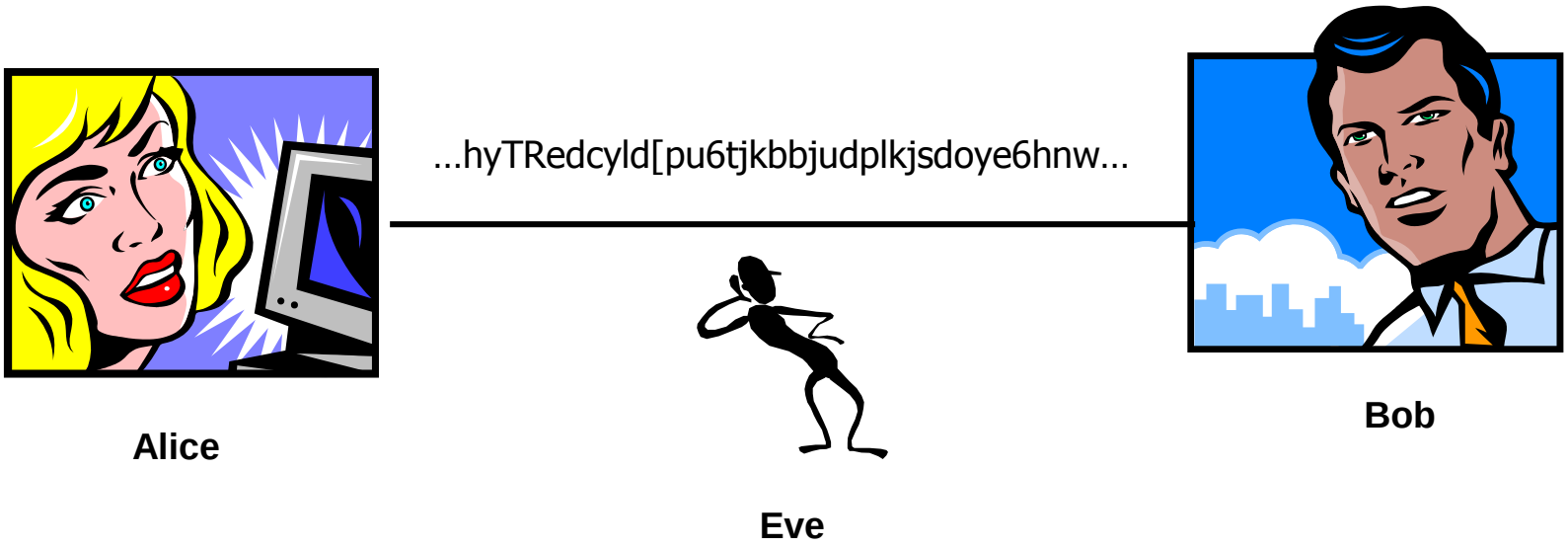
Jenis-jenis Serangan

- Berdasarkan keterlibatan penyerang dalam komunikasi

  1. Serangan pasif (*passive attack*)

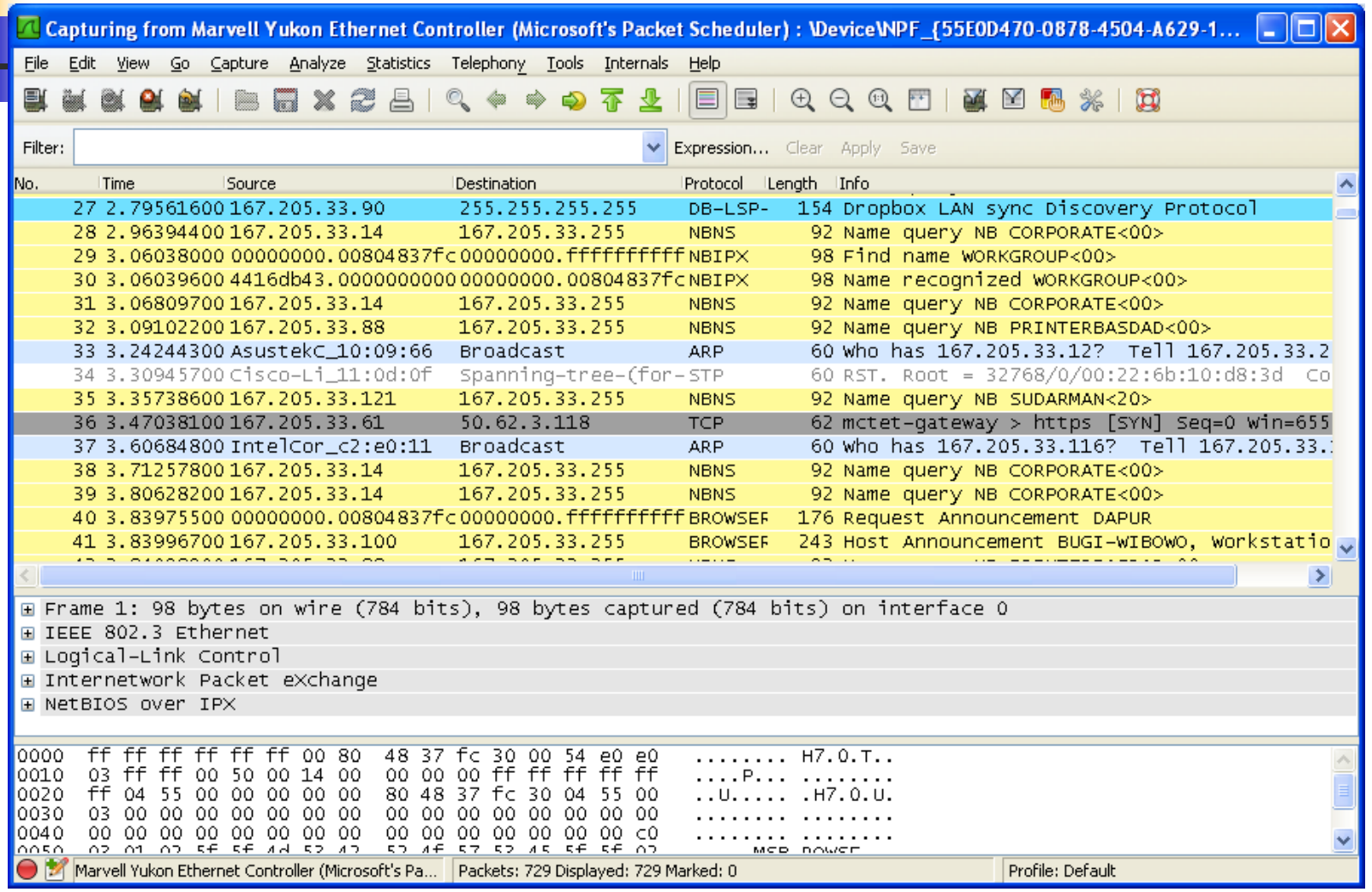
  - penyerang tidak terlibat dalam komunikasi antara pengirim dan penerima
  - penyerang hanya melakukan penyadapan untuk memperoleh data atau informasi sebanyak-banyaknya

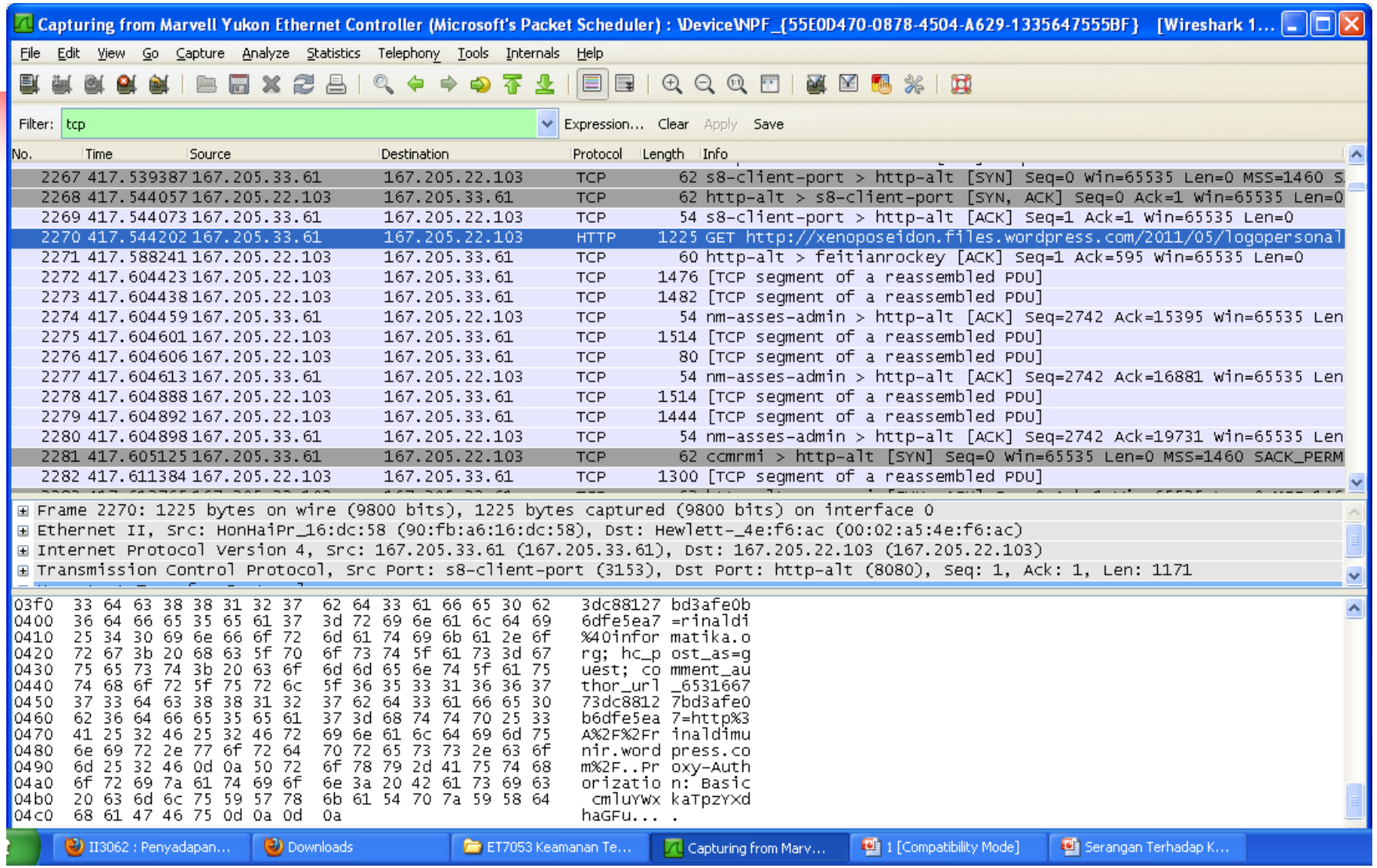
Jenis-jenis Serangan

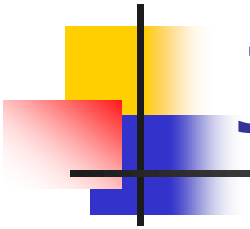


Serangan Pasif

Screenshot Wireshark (memantau *network traffic*)




Capturing from Marvell Yukon Ethernet Controller (Microsoft's Packet Scheduler) : \Device\NPF_{55E0D470-0878-4504-A629-1335647555BF} [Wireshark 1...
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: tcp
Expression... Clear Apply Save
No. Time Source Destination Protocol Length Info
2267 417.539387 167.205.33.61 167.205.22.103 TCP 62 s8-client-port > http-alt [SYN] Seq=0 Win=65535 Len=0 MSS=1460 S
2268 417.544057 167.205.22.103 167.205.33.61 TCP 62 http-alt > s8-client-port [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0
2269 417.544073 167.205.33.61 167.205.22.103 TCP 54 s8-client-port > http-alt [ACK] Seq=1 Ack=1 Win=65535 Len=0
2270 417.544202 167.205.33.61 167.205.22.103 HTTP 1225 GET http://xenoposeidon.files.wordpress.com/2011/05/logopersonal
2271 417.588241 167.205.22.103 167.205.33.61 TCP 60 http-alt > feitianrockey [ACK] Seq=1 Ack=595 Win=65535 Len=0
2272 417.604423 167.205.22.103 167.205.33.61 TCP 1476 [TCP segment of a reassembled PDU]
2273 417.604438 167.205.22.103 167.205.33.61 TCP 1482 [TCP segment of a reassembled PDU]
2274 417.604459 167.205.33.61 167.205.22.103 TCP 54 nm-asses-admin > http-alt [ACK] Seq=2742 Ack=15395 Win=65535 Len
2275 417.604601 167.205.22.103 167.205.33.61 TCP 1514 [TCP segment of a reassembled PDU]
2276 417.604606 167.205.22.103 167.205.33.61 TCP 80 [TCP segment of a reassembled PDU]
2277 417.604613 167.205.33.61 167.205.22.103 TCP 54 nm-asses-admin > http-alt [ACK] Seq=2742 Ack=16881 Win=65535 Len
2278 417.604888 167.205.22.103 167.205.33.61 TCP 1514 [TCP segment of a reassembled PDU]
2279 417.604892 167.205.22.103 167.205.33.61 TCP 1444 [TCP segment of a reassembled PDU]
2280 417.604898 167.205.33.61 167.205.22.103 TCP 54 nm-asses-admin > http-alt [ACK] Seq=2742 Ack=19731 Win=65535 Len
2281 417.605125 167.205.33.61 167.205.22.103 TCP 62 ccmrmi > http-alt [SYN] Seq=0 Win=65535 Len=0 MSS=1460 SACK_PERM
2282 417.611384 167.205.22.103 167.205.33.61 TCP 1300 [TCP segment of a reassembled PDU]
Frame 2270: 1225 bytes on wire (9800 bits), 1225 bytes captured (9800 bits) on interface 0
Ethernet II, Src: HonHaiPr_16:dc:58 (90:fb:a6:16:dc:58), Dst: Hewlett-_4e:f6:ac (00:02:a5:4e:f6:ac)
Internet Protocol Version 4, Src: 167.205.33.61 (167.205.33.61), Dst: 167.205.22.103 (167.205.22.103)
Transmission Control Protocol, Src Port: s8-client-port (3153), Dst Port: http-alt (8080), Seq: 1, Ack: 1, Len: 1171
03f0 33 64 63 38 38 31 32 37 62 64 33 61 66 65 30 62 3dc88127 bd3afe0b
0400 36 64 66 65 35 65 61 37 3d 72 69 6e 61 6c 64 69 6dfe5ea7 =rinaldi
0410 25 34 30 69 6e 66 6f 72 6d 61 74 69 6b 61 2e 6f %40infor matika.o
0420 72 67 3b 20 68 63 5f 70 6f 73 74 5f 61 73 3d 67 rg; hc_p ost_as=g
0430 75 65 73 74 3b 20 63 6f 6d 6d 65 6e 74 5f 61 75 uest; co mment_au
0440 74 68 6f 72 5f 75 72 6c 5f 36 35 33 31 36 36 37 thor_url _6531667
0450 37 33 64 63 38 38 31 32 37 62 64 33 61 66 65 30 73dc8812 7bd3afe0
0460 62 36 64 66 65 35 65 61 37 3d 68 74 74 70 25 33 b6dfe5ea 7=http%3
0470 41 25 32 46 25 32 46 72 69 6e 61 6c 64 69 6d 75 A%2F%2Fr inaldimu
0480 6e 69 72 2e 77 6f 72 64 70 72 65 73 73 2e 63 6f nir.word press.co
0490 6d 25 32 46 0d 0a 50 72 6f 78 79 2d 41 75 74 68 m%2F..Pr oxy-Auth
04a0 6f 72 69 7a 61 74 69 6f 6e 3a 20 42 61 73 69 63 orizatio n: Basic
04b0 20 63 6d 6c 75 59 57 78 6b 61 54 70 7a 59 58 64 cmluYWx kaTpzYXd
04c0 68 61 47 46 75 0d 0a 0d 0a haGFu... .
II3062 : Penyadapan...
Downloads
ET7053 Keamanan Te...
Capturing from Marv...
1 [Compatibility Mode]
Serangan Terhadap K...



Jenis-jenis Serangan

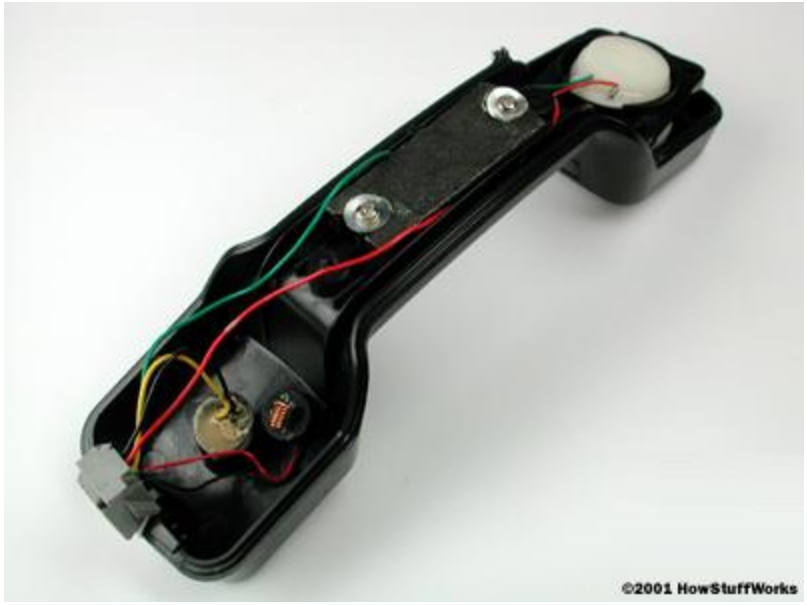
Metode penyadapan:

1. *Wiretapping*
2. *Electromagnetic eavesdropping*
3. *Acoustic Eavesdropping*

- *Wiretapping*

How Wiretapping Works

(sumber: http://www.howstuffworks.com/wiretapping.htm)



When you open up a phone, you can see that the technology inside is very simple. The simplicity of design makes the phone system vulnerable to surreptitious eavesdropping.

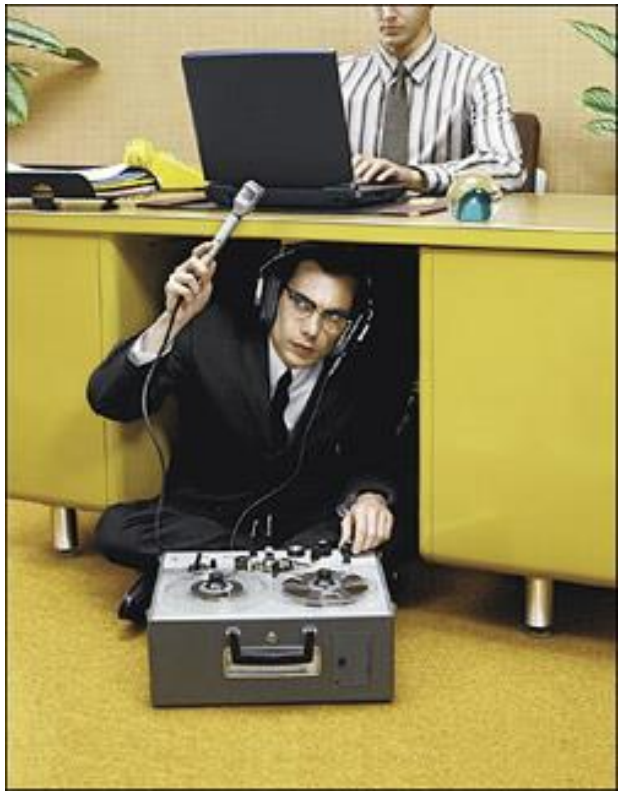
Inside a standard phone cord, you'll find a red wire and a green wire. These wires form a circuit like the one you might find in a flashlight. Just as in a flashlight, there is a negatively-charged end and a positively-charged end to the circuit. In a telephone cord, the green wire connects to the positive end and the red cord connects to the negative end.

Electromagnetic eavesdropping

Lihat info alat penyadap suara GSM:

http://indonetwork.web.id/Matama_Security/1168831/spy-ear-gsm-penyadap-suara-dengan-kartu-gsm.htm

Acoustic Eavesdropping



15506-41DG
'Office: 9am' Disc
© JupiterImages

Creatas
www.comstock.com

Jenis-jenis Serangan

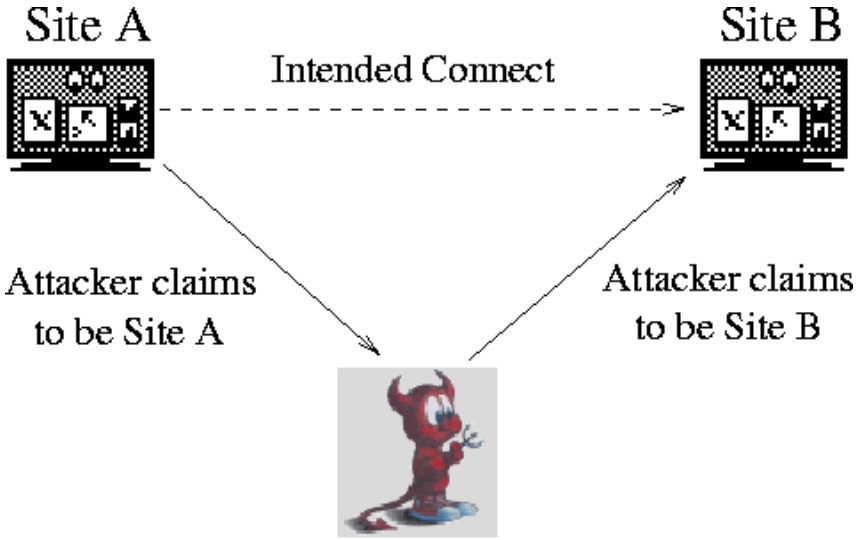
2. Serangan aktif (*active attack*)

- penyerang mengintervensi komunikasi dan ikut mempengaruhi sistem untuk keuntungan dirinya
- penyerang mengubah aliran pesan seperti:
  menghapus sebagian cipherteks,
  mengubah cipherteks,
  menyisipkan potongan cipherteks palsu,
  me-*replay* pesan lama,
  mengubah informasi yang tersimpan, dsb

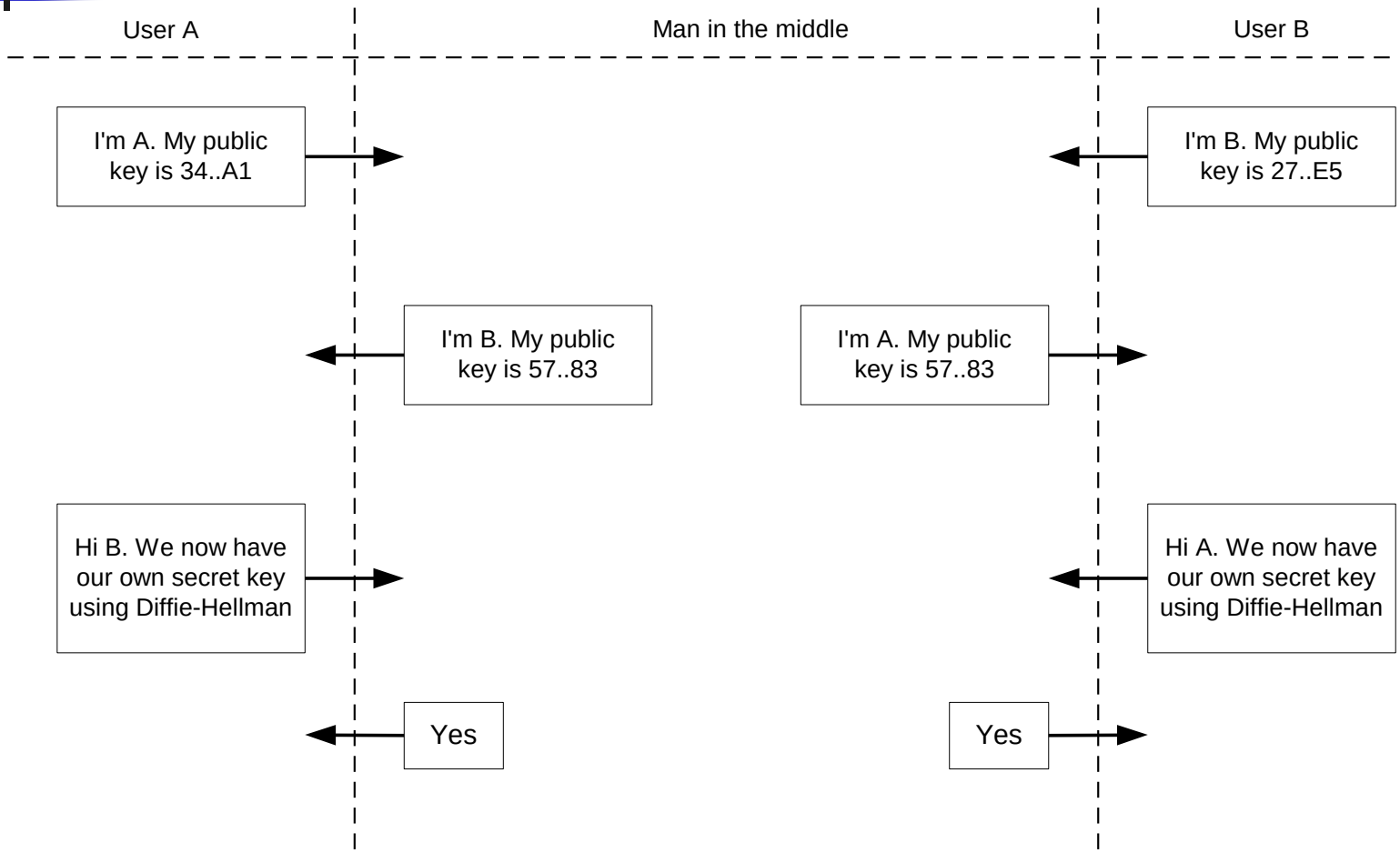
Jenis-jenis Serangan

- *Man-in-the-middle-attack*

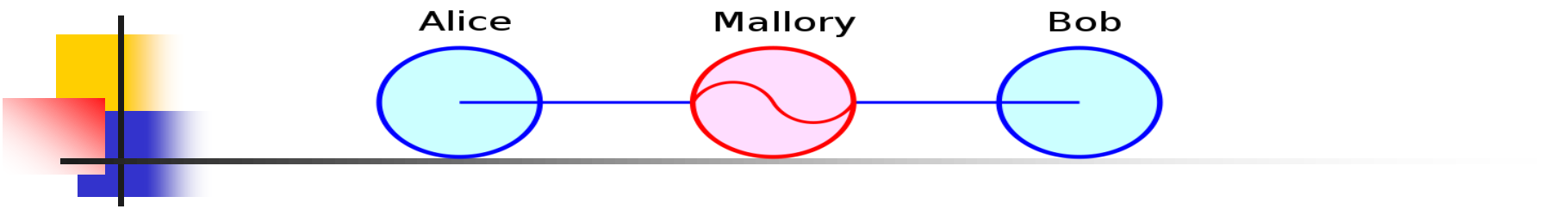
  - Serangan aktif yang berbahaya



Man-in-the-middle-attack



Man in the Middle Attack



1. Alice sends a message to Bob, which is intercepted by Mallory:

Alice *"Hi Bob, it's Alice. Give me your key"*--> **Mallory Bob**

2. Mallory relays this message to Bob; Bob cannot tell it is not really from Alice:

Alice Mallory *"Hi Bob, it's Alice. Give me your key"*--> **Bob**

3. Bob responds with his encryption key (Public Key's Bob):

Alice Mallory <--*[Bob's_key]* **Bob**

4. Mallory replaces Bob's key with her own, and relays this to Alice, claiming that it is Bob's key:

Alice *<--[Mallory's_key]* **Mallory Bob**

5. Alice encrypts a message with what she believes to be Bob's key, thinking that only Bob can read it:

Alice *"Meet me at the bus stop!"[encrypted with Mallory's key]-->* **Mallory Bob**

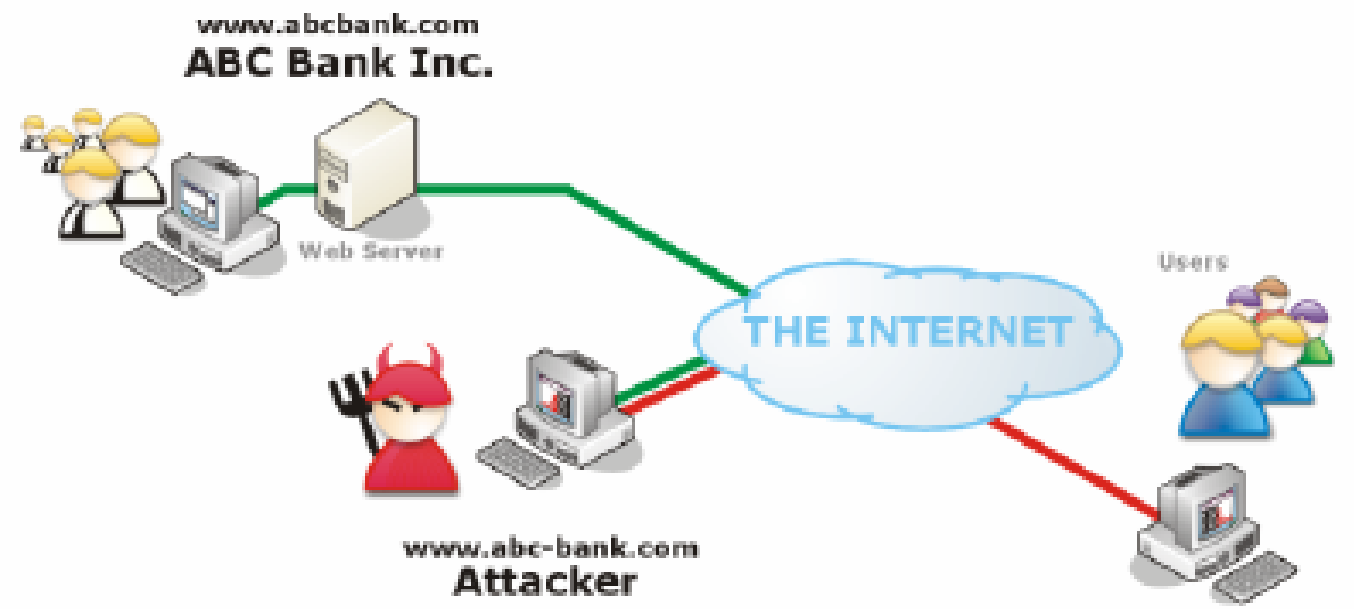
6. However, because it was actually encrypted with Mallory's key, Mallory can decrypt it (with his private key), read it, modify it (if desired), re-encrypt with Bob's key, and forward it to Bob:

Alice Mallory *"Meet me at 22nd Ave!"[encrypted with Bob's key]-->* **Bob**

7. Bob thinks that this message is a secure communication from Alice.

Dikutip dari Wikipedia

Man-in-the-middle-attack



With no entity authentication consumers have no ability to know if they are subject to a man-in-the-middle attack.

Man-in-the-middle attack di bidang *e-commerce*

Jenis-jenis Serangan

Berdasarkan teknik yang digunakan untuk menemukan kunci:

1. Exhaustive attack | brute force attack

- Mengungkap plainteks/kunci dengan mencoba semua kemungkinan kunci.
- Pasti berhasil menemukan kunci jika tersedia waktu yang cukup

Jenis-jenis Serangan

Tabel 1 Waktu yang diperlukan untuk *exhaustive key search*
(Sumber: William Stallings, *Data and Computer Communication Fourth Edition*)

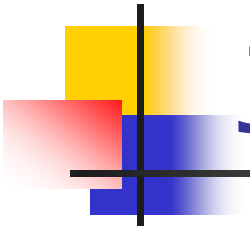
Ukuran kunci	Jumlah kemungkinan kunci	Lama waktu untuk 10^6 percobaan per detik	Lama waktu untuk 10^{12} percobaan per detik
16 bit	$2^{16} = 65536$	32.7 milidetik	0.0327 mikrodetik
32 bit	$2^{32} = 4.3 \times 10^9$	35.8 menit	2.15 milidetik
56 bit	$2^{56} = 7.2 \times 10^{16}$	1142 tahun	10.01 jam
128 bit	$2^{128} = 4.3 \times 10^{38}$	5.4×10^{24} tahun	5.4×10^{18} tahun

Solusi: Kriptografer harus membuat kunci yang panjang dan tidak mudah ditebak.

Jenis-jenis Serangan

2. *Analytical attack*

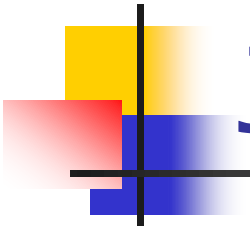
- Menganalisis kelemahan algoritma kriptografi untuk mengurangi kemungkinan kunci yang tidak mungkin ada.
- Caranya: memecahkan persamaan-persamaan matematika (yang diperoleh dari definisi suatu algoritma kriptografi) yang mengandung peubah-peubah yang merepresentasikan plainteks atau kunci.



Jenis-jenis Serangan

- Metode *analytical attack* biasanya lebih cepat menemukan kunci dibandingkan dengan *exhaustive attack*.

- Solusi: kriptografer harus membuat algoritma kriptografi yang kompleks



Jenis-jenis Serangan

- Data yang digunakan untuk menyerang sistem kriptografi:

1. *Chipertext only*.
2. *Known plaintext* dan *corresponding chipertext*.
3. *Chosen plaintext* dan *corresponding chipertext*.
4. *Chosen chipertext* dan *corresponding plaintext*.

Jenis-jenis Serangan

Berdasarkan ketersediaan data:

1. Chipertext-only attack

Kriptanalis hanya memiliki cipherteks

Teknik yang digunakan: *exhaustive key search* dan teknik analisis frekuensi (akan dijelaskan kemudian)

Diberikan: $C_1 = E_k(P_1), C_2 = E_k(P_2), \ldots, C_i = E_k(P_i)$

Deduksi: $P_1, P_2, \ldots, P_i$ atau k untuk mendapatkan P_{i+1} dari $C_{i+1} = E_k(P_{i+1})$.

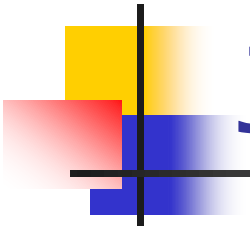
Jenis-jenis Serangan

2. ***Known-plaintext attack***

Diberikan:

P_1, $C_1 = E_k(P_1)$,
P_2, $C_2 = E_k(P_2)$,
... ,
P_i, $C_i = E_k(P_i)$

Deduksi: k untuk mendapatkan P_{i+1} dari $C_{i+1} = E_k(P_{i+1})$.



Jenis-jenis Serangan

Beberapa pesan yang formatnya terstruktur membuka peluang untuk menerka plainteks dari cipherteks yang bersesuaian.

Contoh:

From dan *To* di dalam *e-mail*,

"Dengan hormat", *wassalam*, pada surat resmi.

#include, *program*, di dalam *source code*

Jenis-jenis Serangan

3. ***Chosen-plaintext attack***

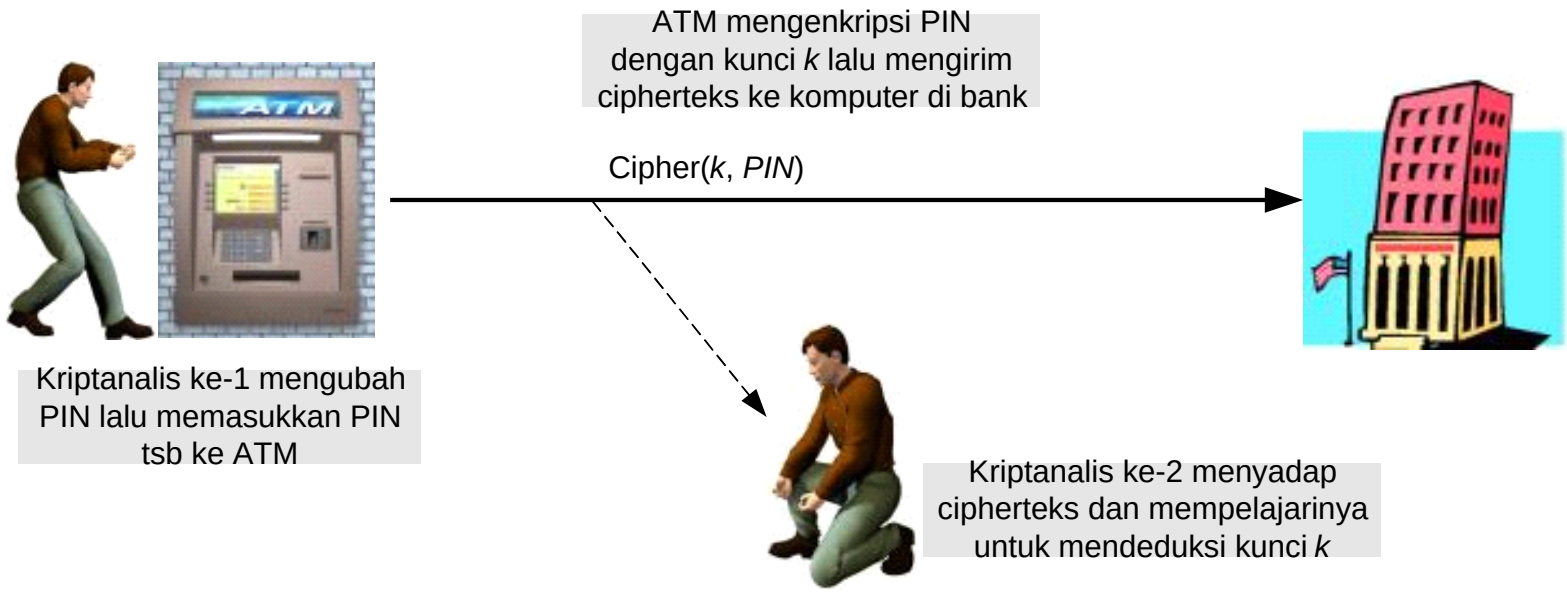
   Kriptanalis dapat memilih plainteks tertentu untuk dienkripsikan, yaitu plainteks-plainteks yang lebih mengarahkan penemuan kunci.

Jenis-jenis Serangan

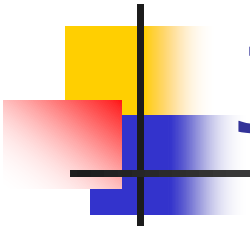
Diberikan: $P_1, C_1 = E_k(P_1), P_2, C_2 = E_k(P_2), \ldots, P_i, C_i = E_k(P_i)$
di mana kriptanalis dapat memilih diantara $P_1, P_2, \ldots, P_i$

Deduksi: k untuk mendapatkan P_{i+1} dari $C_{i+1} = E_k(P_{i+1})$.

Jenis-jenis Serangan



Chosen-plaintext attack



Jenis-jenis Serangan

4. Adaptive-chosen-plaintext attack

Kriptanalis memilih blok plainteks yang besar, lalu dienkripsi, kemudian memilih blok lainnya yang lebih kecil berdasarkan hasil serangan sebelumnya, begitu seterusnya.

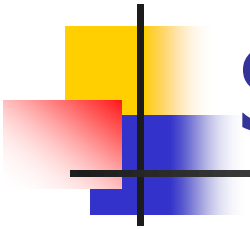
Jenis-jenis Serangan

5. Chosen-ciphertext attack

Diberikan:

C_1, $P_1 = D_k(C_1)$, C_2, $P_2 = D_k(P_2)$, ..., C_i, $P_i = D_k(C_i)$

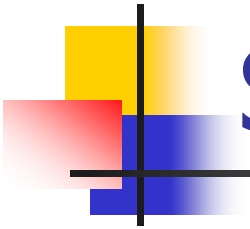
Deduksi: *k* (yang mungkin diperlukan untuk mendekripsi pesan pada waktu yang akan datang).



Serangan jenis lainnya:

6. Chosen-key attack

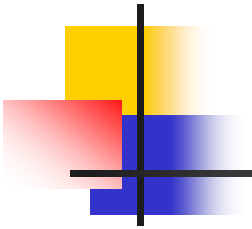
Kriptanalis memiliki pengetahuan mengenai hubungan antara kunci-kunci yang berbeda, dan memilih kunci yang tepat untuk mendekripsi pesan



Serangan jenis lainnya:

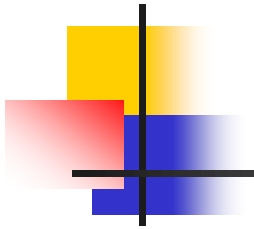
7. ***Rubber-hose cryptanalysis***

Mengancam, mengirim surat gelap, atau melakukan penyiksaan sampai orang yang memegang kunci memberinya kunci untuk mendekripsi pesan



- Sebuah algoritma kriptografi dikatakan aman (*computationally secure*) bila ia memenuhi tiga kriteria berikut:

1. Persamaan matematis yang menggambarkan operasi algoritma kriptografi sangat kompleks sehingga algoritma tidak mungkin dipecahkan secara analitik.



2. Biaya untuk memecahkan cipherteks melampaui nilai informasi yang terkandung di dalam cipherteks tersebut.

3. Waktu yang diperlukan untuk memecahkan cipherteks melampaui lamanya waktu informasi tersebut harus dijaga kerahasiaannya.