Keamanan pada Wireless-LAN

Nama: Dannis Muhammad Mangan
NIM: 13507112
Program Studi Teknik Informatika
Jalan Ganeca No.10 Bandung
e-mail: dannis_m@students.itb.ac.id

Abstrak

Wireless LAN merupakan salah satu bentuk LAN (Local Area Network) yang paling populer di dunia. Dengan makin menjamurnya komputer jinjing atau laptop dan kebutuhan akan akses internet nirkabel, wireless LAN (dengan wi-fi merupakan standar yang paling populer) pun semakin banyak dipakai di seluruh dunia , dampaknya kebutuhan akan standar keamanan untuk menjaga aliran data dan informasi pada WLAN pun bersifat mendesak. Makalah ini lebih ditujukan untuk mempelajari standar enkripsi yang sudah ada dan mengetahui kekurangan-kekurangannya melalui serangan sehingga nantinya dapat dievaluasi lebih lanjut

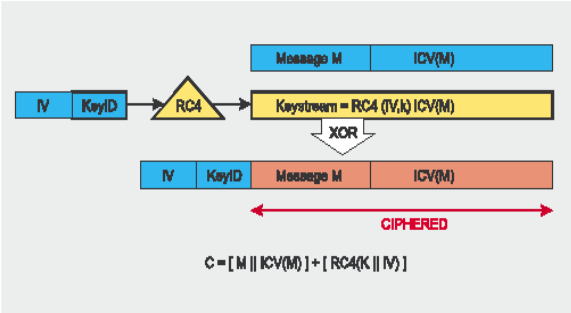
Kata kunci:Wireless, LAN, Keamanan, Serangan, WEP, WPA, WPA2

1. Pendahuluan:

Seiring dengan kemajuan teknologi dan kebutuhan akan akses internet, maka penggunaan jaringan komputer nirkabel juga semakin marak.

Data berdasarkan penelitian diperkirakan jumlah hotspot pada 2009 meningkat sekira 47 persen sehingga total koneksi yang ada mencapai 1,2 miliar. Nantinya, berdasarkan penelitian dari In-Stat perangkat entertainmen yang dilengkapi wifi seperti kamera, ponsel *game*, dan *media player* portabel akan meningkat, dari sebelumnya 108,8 juta pada tahun 2008.

Dengan semakin banyaknya pengguna teknologi nirkabel ini), total persentase trafik penggunaan wifi meningkat dari 20 persen pada tahun 2008 menjadi 35 persen pada tahun 2009. (sumber: *Cellular News*, Sabtu 2/1/2010). Maka ancaman terhadap bahaya keamanan informasi juga semakin meningkat, namun justru algoritma pengamanannya masih rentan dipatahkan, seperti algoritma WEP (Wired Equivalent Privacy) yang memakai algoritma *stream cipher* (algoritma kriptografi modern) yang disebut RC4.



Gambar1. Proses Enkripsi dengan algoritma RC4

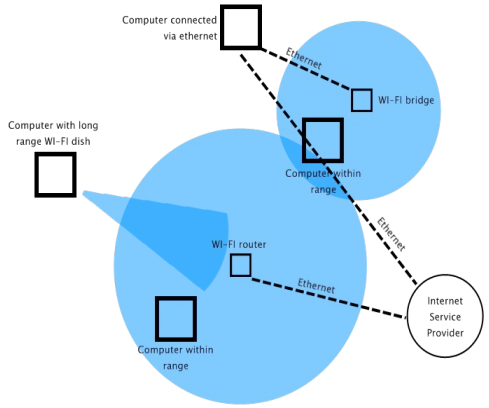
***Data security risks* jika keamanan wireless-LAN dibobol sangatlah besar, sehingga dibutuhkan mekanisme penggunaan standar enkripsi yang baru dari yang sudah ada ataupun dibuat standar enkripsi yang benar-benar baru.**

2. Pengertian LAN dan WLAN:

Local Area Network (LAN) adalah suatu jaringan komputer yang mencakup area yang relatif kecil. Biasanya keuntungan pada LAN adalah kecepatan transfernya tinggi.

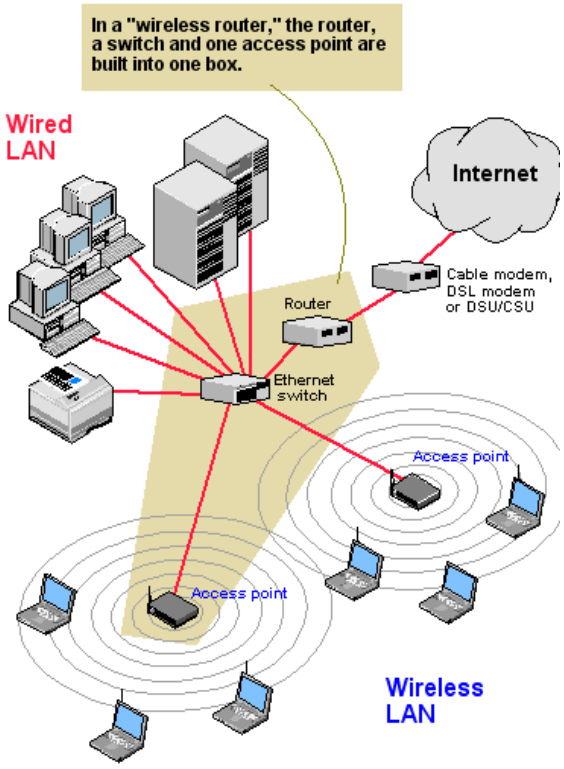
Sedangkan perbedaan dengan Wireless-LAN (WLAN) adalah WLAN menyambungkan *device-device* melalui suatu wireless distribution method, dan biasanya, menyediakan koneksi menuju *acces point* (internet). Keunggulan utama dari sistem ini yaitu memungkinkan para

pengguna untuk tetap dapat bergerak dan tetap terkoneksi pada jaringan selama pengguna tetap berada di dalam cakupan WLAN.



Gambar2. Ilustrasi cakupan area Wireless LAN yang merupakan keunggulan utama

From Computer Desktop Encyclopedia
© 2007 The Computer Language Co. In



Gambar3. Ilustrasi Wireless LAN dengan *access point*.

3. Pengertian WEP

Wireless Equivalent Privacy (WEP) merupakan salah satu algortima pertama yang muncul untuk mengamankan jaringan nirkabel. WEP memakai algoritma stream cipher RC4. Kunci WEP mempunyai 16.7 juta kemungkinan kunci berbeda.

3.1 RC4

RC4 merupakan algoritma stream cipher yang paling banyak digunakan pada software di dunia. Diagram cara kerja enkripsi RC4 seperti pada Gambar1 diatas.
Implementasi program RC4 dalam bahasa C (dengan compiler MinGW pada Windows):

```
unsigned char S[256];
unsigned int i, j;

void swap(unsigned char *s, unsigned int i,
unsigned int j) {
    unsigned char temp = s[i];
    s[i] = s[j];
    s[j] = temp;
}

/* KSA */
void rc4_init(unsigned char *key, unsigned
int key_length) {
    for (i = 0; i < 256; i++)
        S[i] = i;

    for (i = j = 0; i < 256; i++) {
        j = (j + key[i % key_length] + S[i]) &
255;
        swap(S, i, j);
    }

    i = j = 0;
}

/* PRGA */
unsigned char rc4_output() {
    i = (i + 1) & 255;
    j = (j + S[i]) & 255;

    swap(S, i, j);

    return S[(S[i] + S[j]) & 255];
}

#include <stdio.h>
#include <string.h>
#include <stdlib.h>
```

```
#define ARRAY_SIZE(a)
(sizeof(a)/sizeof(a[0]))

int main() {
   unsigned char *test_vectors[][2] =
   {
      {"Key", "Plaintext"},
      {"Kriptografi", "IF"},
      {"contoh", "serang mereka"}
   };

   int x;
   for (x = 0; x <
ARRAY_SIZE(test_vectors); x++) {
      int y;
      rc4_init(test_vectors[x][0],
strlen((char*)test_vectors[x][0]));

      for (y = 0; y <
strlen((char*)test_vectors[x][1]); y++)
         printf("%02X", test_vectors[x][1][y]
^ rc4_output());
      printf("\n");
   }
   return 0;
}
```

4. Pengertian WPA dan WPA2

Wi-Fi Protected Access (WPA) merupakan pengembangan dari WEP dan merupakan jawaban dari Wi-Fi Alliance untuk memperbaiki keamanan pada jaringan nirkabel. Kunci pada WPA mempunyai kemungkinan sebanyak 500 milyar kemungkinan kunci. Selain itu, WPA juga mengimplemetasikan protokol yang mampu mengubah kunci setiap beberapa menit dan dilengkapi dengan algoritma *checksum* CRC yang dikembangkan khusus untuk menghindari berbagai serangan yang mungkin terjadi.

Sedangkan WPA2 adalah perbaikan lanjut dari WPA. Penambahan paling penting pada WPA2 adalah penambahan algoritma kriptografi yang berbasiskan AES yang disebut CCMP dan dianggap *fully secure* / benar-benar aman. Pada saat ini, syarat suatu jaringan untuk dapat memasang logo Wi-Fi adalah pemakaian WPA2 di dalam jaringan tersebut.

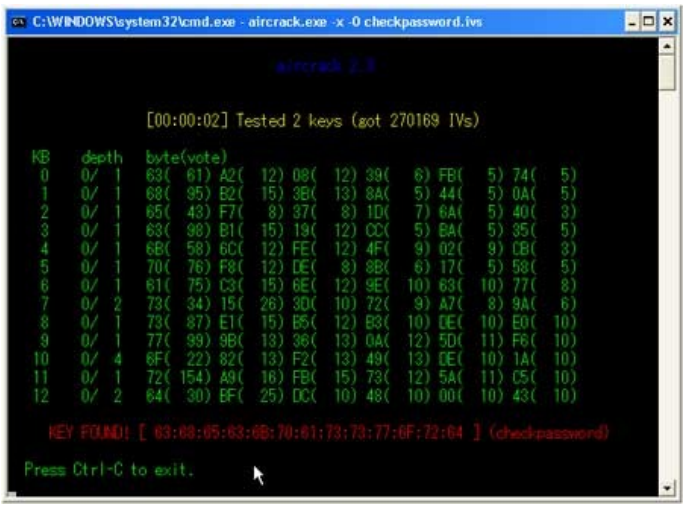
5. Implementasi percobaan penyerangan

5.1 Penyerangan terhadap WEP

. Dengan memanfaatkan ratusan ribu paket digunakan untuk merusak kunci WEP secara statistik. Pada saat paket-paket telah dikumpulkan, dengan teknik kriptoanalisis dapat dengan cepat menemukannya. Lalu dengan bantuan software seperti *Aircrack*, hanya memerlukan beberapa menit saja untuk mencoba 16.7 juta kemungkinan kunci WEP tersebut. Setelah berhasil masuk ke jaringan, pengambilan data dilakukan dengan *'sniffing'* / menyadap jaringan.

.

Jaringan yang diujikan adalah jaringan ad-hoc yang dibuat oleh penulis sendiri.



Gambar4. Demonstrasi Penyerangan WEP melaui AirCrack

Dari hasil uji, dengan menggunakan software *AirCrack* tersebut sandi-lewat pada WEP yang digunakan dapat terlacak. Langkah selanjutnya adalah 'mendengarkan' lalu-lintas data dengan memakai software seperti *WireShark*. Namun bagian ini dilewatkan karena jaringan yang dipakai adalah ad-hoc yang hanya berisi komputer penulis.

5.2 Penyerangan terhadap WPA2

Percobaan penyerangan ini menggunakan software *WireShark* dengan jaringan nirkabel yang digunakan adalah jaringan di dalam tempat kos.

Spesifikasinya sebagai berikut:

Network Name : MundingLaya
Password: mundinglaya
Network Protocol analyzer: **WireShark Version 1.2.6**

Interface: Intel® PRO/Wireless 3945ABGa
Service Set ID: Mundinglaya
Basic SSID : 00:17:3D:A4:8D:A7 (Belkin)
Network type used: 2.4-GHz OFDM
Infrastructure mode: Acces point
Authentication mode: **WPA2-PSK**
Encryption status: WEP&TKIP&AES enabled, transmit key available
TX power: -
RSSI (Received Signal Strengh Indication) : -82 dbM
Supported Rates: -
Desired Rates: -
Channel: 7 (2422 MHz)

Contoh hasil *captured outcoming*:

24 15.261864 192.168.2.2 204.2.171.81 HTTP GET /hprofile-ak-sf2p/hs621.snc3/27352_804224615_9392_q.jpg HTTP/1.1

3952 612.983581 192.168.2.2 68.142.233.119 SIP Unknown request: YAHOOREF sip:**de_em_89**@68.142.233.119:5050; transport=tcp

33 65.998182 192.168.2.3 64.233.181.19 TLSv1 Application Data

115 209.095792 192.168.2.20 192.168.2.255 BROWSER Get Backup List Request

116 209.097152 192.168.2.20 192.168.2.255 NBNS Name query NB MUNDINGLAYA<1b>

43 106.254231 192.168.2.2 192.168.2.1 DNS Standard query A webmail.informatika.org

205 491.916284 192.168.2.3 64.233.181.19 SSL Client Hello

1183 973.416233 192.168.2.20 192.168.2.255 BROWSER Host Announcement DWIKY, Workstation, Server, NT Workstation

1234 1074.324364 192.168.2.20 239.255.255.250 SSDP M-SEARCH * HTTP/1.1

1292 1136.992089 192.168.2.2 64.233.181.19 TCP [TCP segment of a reassembled PDU]

1892 1998.825203 192.168.2.6 192.168.2.255 NBNS Name query NB WORKGROUP<1b>

Contoh hasil *captured incoming*:

79 18.776305 66.220.146.25 192.168.2.2 HTTP HTTP/1.1 200 OK (application/x-javascript)

57 110.220884 167.205.32.3 192.168.2.2 TCP http > xdsxdm [FIN, ACK] Seq=1596 Ack=605 Win=7168 Len=0

44 106.496712 192.168.2.1 192.168.2.2 DNS Standard query response CNAME mail.informatika.org A 167.205.32.3

354 576.378224 192.168.2.1 192.168.2.3 DNS Standard query response CNAME pagead.l.google.com A 216.239.61.164

365 576.557641 216.239.61.104 192.168.2.3 TLSv1 Change Cipher Spec, Encrypted Handshake Message

1411 1363.067869 212.96.161.234 192.168.2.2 HTTP Continuation or non-HTTP traffic

1481 1376.008070 192.168.2.1 192.168.2.2 DNS Standard query response CNAME af.avg.com.edgesuite.net CNAME a702.g.akamai.net A 125.160.18.8 A 125.160.18.33

1577 1379.104179 212.96.161.234 192.168.2.3 TCP http >

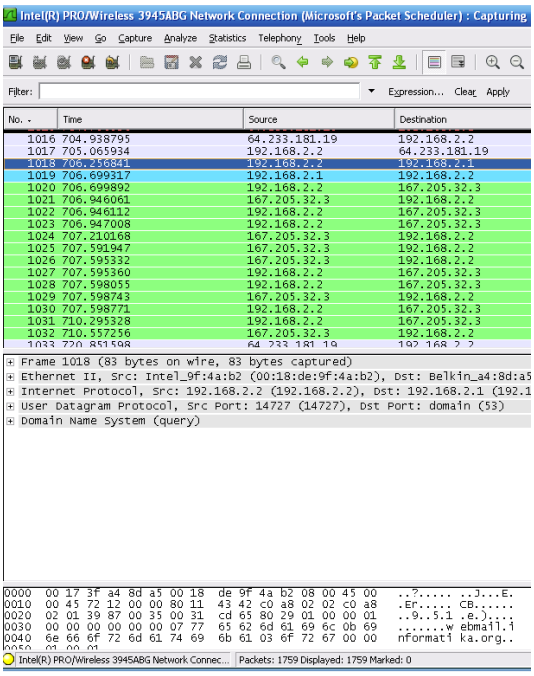
joaJewelSuite [RST, ACK] Seq=153 Ack=387 Win=0 Len=0

Contoh hasil lainnya :

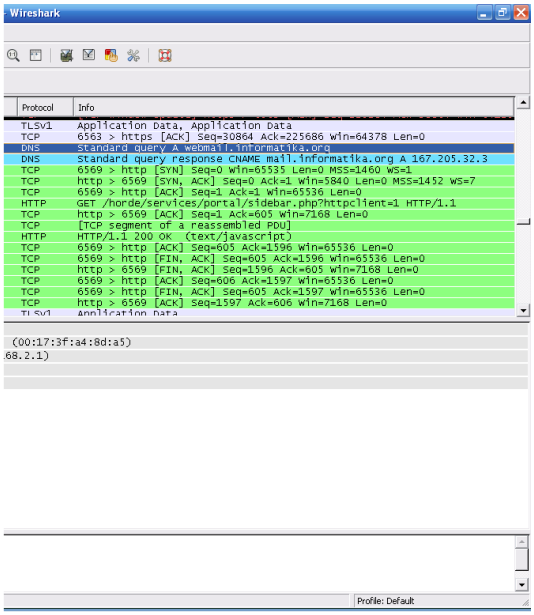
27 26.758010 Belkin_a4:8d:a5 Broadcast ARP Who has 192.168.2.20? Tell 192.168.2.1

150 363.332793 Intel_9f:4a:b2 Belkin_a4:8d:a5ARP 192.168.2.2 is at 00:18:de:9f:4a:b2

Untuk mendapatkan kunci WPA2 jaringan tersebut, dengan menggunakan software waktu yang diperlukan akan sangat lama, dengan asumsi perhitungan yaitu jika kunci WEP dapat dicari dalam 5 menit, maka untuk WPA2 setidaknya membutuhkan waktu 48 hari. Karena itu penulis melakukan penjebolan dengan teknik kriptoanalis heuristik dan password didapat setelah percobaan sekitar 1 jam saja.
Dengan melakukan analisis terhadap data incoming dan outcoming yang didapat, dapat diubah menjadi informasi, seperti misalnya pada contoh captured outcoming diatas, terdapat kode request: YAHOOREF sip:**de_em_89** yang berarti terdapat request data dari salah satu komputer dalam jaringan dengan ID Yahoo! yaitu “de_em_89” .
Kemudian dengan mengecek IP mana yang bertugas sebagai administrator jaringan dapat dilihat seperti pada kode Who has 192.168.2.20? Tell 192.168.2.1 , kemudian kita dapat saja melakukan hak administrator dengan mengakses 192.168.2.1 , biasanya terdapat akses layanan router yang dilindungi oleh sandi-lewat.



Gambar4. Gambar antarmuka *WireShark* yang sedang melakukan penyadapan – bagian 1



Gambar5. Gambar antarmuka *WireShark* yang sedang melakukan penyadapan – bagian 2

Kesimpulan percobaan yaitu data yang masuk maupun keluar dapat dengan mudah di dengarkan/ *'sniff'* atau *traffic* data-nya dapat disimpan. Kemudian hasil dari data tersebut dapat diolah sehingga menjadi informasi bagi si penyadap. Kebocoran informasi ini berbahaya sebab tidak jarang informasi yang lewat tersebut mengandung data-data penting dan rahasia.

6. Kesimpulan

Sebelumnya telah diketahui bahwa enkripsi menggunakan WEP tidak memberikan jaminan keamanan terhadap jaringan mireless secara memadai untuk itu digunakan solusi enkripsi untuk level yang lebih tinggi seperti VPN. WPA dan WPA2 merupakan solusi keamanan sementara untuk memperbaharui peralatan sebelumnya sebagai peralatan keamanan modern, namun keamanannya masih harus ditingkatkan lagi karena bahaya *data security risk* yang ada sangat besar dan terbukti belum *fully secure*.

7. Referensi

Serge Vaudenay and Martin Vuagnoux. Passive-only key recovery attacks on RC4. In Selected Areas in Cryptography 2007, infoscience.epfl.ch/record/115086/files/VV07.pdf

http://en.wikipedia.org/wiki/Wireless_LAN_Security

http://en.wikipedia.org/wiki/RC4

http://en.wikipedia.org/wiki/Stream_cipher

http://www.derrickpark.com/articles/mac/article-7-wep-vs-wpa-wireless-encryption/

http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access