ANALISA SISTEM KEAMANAN JARINGAN WIRELESS LAN IEEE 802.11

Zulkarnain Sanany
Fasilkom – Universitas INDONUSA Esa Unggul, Jakarta
Jl. Arjuna Utara Tol Tomang Kebun Jeruk, Jakarta 11510
zsanany@yahoo.com

Abstrak

Semenjak diratifikasinya standard Jaringan *Wireless* IEEE 802.11 pada tahun 1999, jaringan *wireless* LAN berkembang sedemikian pesatnya, memenuhi hampir diseluruh pelosok dari pusat perkantoran, daerah industri, hotel, bandara udara, kampus universitas, rumah sakit, bahkan di kafe maupun restoran. Tetapi dibalik semua kesuksesan ini mengganjal sebuah masalah yang krusial, yaitu sistem keamanan jaringan. Jaringan tradisional *Wireless* IEEE 802.11 terfokus pada dua aspek, *access control* dan *data privacy*. *Access control* menjamin hanya klien yang telah dilegitimasi yang dapat mengakses jaringan. *Data privacy* menjamin bahwa informasi yang telah di-enkripsi harus benar sampai pada tangan user yang dituju. Berbeda dengan jaringan IEEE 802.3 LAN Etnernet, informasi tidak ditransmisikam melalui kabel melainkan dipancarkan keudara dari antena dengan gelombang radio RF, siapa saja bisa menerima transmisi ini tanpa pengawasan. Hal inilah yang menyebabkan sistem keamanan jaringan *wireless* 802.11 mendapat kritikan dari para periset, karena mereka telah menemukan beberapa celah kerawanan dan kelemahan, dari sistim autentikasi, keamanan data, dan integritas data yang digunakan. Isi jurnal, menganalisa sistim autentikasi dan enkripsi dari spesifikasi 802.11, membahas titik kelemahan dari sistim keamanan 802.11 dan membahas cara penanggulangannya.

Kata Kunci: *SSID, WEP, Initialization Vector (IV) sequence, MAC authentication, encryption.*

Pendahuluan

SSID *(Service Set Identifiers)* merupakan sistem *password* yang digunakan di dalam sistim jaringan *wireless*, dimana SSID disisipkan pada paket data yang ditransmisikan. SSID dipakai untuk meng-autentikasi klien yang ingin masuk kedalam sebuah jaringan melalui AP *(Access Point).* Semua klien dan AP yang berkomunikasi di dalam jaringan menggunakan SSID yang sama, klien yang menggunakan SSID yang berbeda akan ditolak. Secara default AP mengirim informasi SSID keseluruh klien secara *broadcast* beberapa kali per detik tanpa enksipsi, inilah merupakan salah satu celah kelemahan dari sistim 802.11, *intruder* atau *hacker* dengan menggunakan aplikasi khusus dapat mencegat paket untuk mende teksi informasi yang ada didalamnya. Walaupun sistem keamanan dapat ditingkat kan dengan cara membuat kode SSID maksimum sebanyak 32 karakter, tetap tidak efektif karena klien sulit untuk mengingat kode sepanjang ini. Di dalam standard spesifikasi IEEE 802.11, autentikasi dapat dilakukan dengan dua cara: yaitu *Open Key* dan *Shared Key*. Sistem autentikasi yang dijelaskan diatas adalah *Open Key*, klien hanya cukup mengetahui kode SSID yang diberikan. Di dalam sistem autentikasi *Shared Key*, AP mengirim terlebih dahulu *'challenge text'* yang telah dienkripsi dengan menggunakan WEP *(Wired Equivalent Privacy) key* yang digunakan secara *sharing*, lalu klien mendekripsi *text* dengan menggunakan WEP *key* yang diberikankemudian mengirim responsenya kembali ke AP. Jika klien gagal membuka *'challenge text'* karena menggunakan WEP key yang salah atau ia tidak memiliki WEP keynya, maka klien tidak diizinkan masuk ke sistim jaringan. WEP adalah sistim enkripsi jaringan yang diterapkan pada *standard* IEEE 802.11 yang beroperasi pada *layer-2* MAC *layer*, sesuai dengan fungsi dari *network interface card* (NIC) yang dimiliki oleh setiap klien dan AP, Sistim autentikasi *Shared Key*

ternyata juga tidak aman, karena *intruder* dan *hacker* mampu memecahkan kode *WEP key* yang telah dienkripsi. Sistem enkripsi yang diterapkan pada WEP ternyata memiliki kelemahan pada teknik enkripsinya, dan ini merupakan celah kelemahan yang kedua dari sistem jaringan *wireless* 802.11. Kemudian beberapa vendor menerapkan sistim autentikasi lain yang berdasarkan penyortiran *physical address* atau *MAC address* dari setiap klien pada jaringan, dimana *Access Point* akan memberi izin akses kepada klien dengan membandingkan *MAC address*nya dengan *MAC address* yang ada pada tabel yang dimiliki oleh AP. Sekali lagi, walaupun *MAC address* yang ditransmisikan telah dienkripsi dengan WEP, tetap saja bisa dipecahkan oleh para *hacker* atau *intruder* dengan bantuan program aplikasi *packet analyzer* yang canggih. Penggunaan sistem penyaringan dengan *MAC address* belum bisa menjamin solid-nya sistem keamanan jaringan *wireless* 802.11.

Langkah yang bisa dilakukan oleh *intruder* atau *hacker* di dalam menembus sistim keamanan jaringan 802.11 antara lain:

1. Mendeteksi keberadaan jaringan yang sedang aktif, dengan program aplikasi Kismet, *channel frequency* dan SSID yang digunakan oleh klien atau AP, dapat langsung dideteksi.
2. Melacak *MAC address* dari klien yang sedang aktif, dengan hanya mengetik beberapa command pada program aplikasi Kismet, *list MAC address* dari klien yang aktif di jaringan dapat ditampilkan.
3. Memecahkan *enrypted code WEP key* yang sedang digunakan dengan program aplikasi AirSnort, atau Kismet. AirSnort dapat memecahkan kode WEP *key* setelah memproses 3.4 juta paket, sedang program aplikasi Kismet dapat mendeteksi *WEP key* dalam waktu 27 menit atau setelah 490 Mbyte paket data diproses.

Dengan menggunakan SSID, *MAC address*, dan *WEP key* yang diperoleh secara ilegal, *intruder* atau *hacker* dapat melakukan login ke sistim jaringan, selanjutnya dapat melakukan hal yang tidak diinginkan.

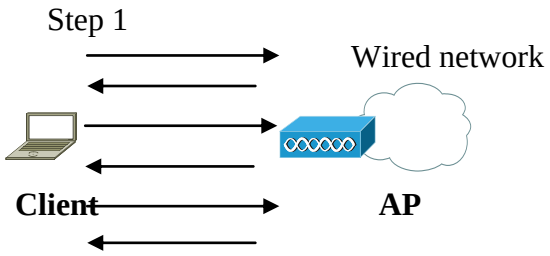
Kelemahan sistim autentikasi 802.11

Seperti yang telah dijelaskan pada paragraf sebelumnya bahwa spesifikasi 802.11 memiliki dua jenis autentikasi yaitu *Open key* dan *Shared key*. Pada umumnya autentikasi menggunakan dua mekanisme yaitu SSID dan *MAC address*. SSID membantu klien untuk membedakan jaringan *wireless* yang sedang diakses secara unik, sehingga dapat dibedakan dengan jaringan *wireless* lainnya. Pada setiap AP dapat dikonfigurasi sebanyak 16 buah SSID yang harus diketik dengan karakter *alpha-numeric, case sensitive* dengan panjang karakter, 2 sampai dengan 32 buah. *MAC address* digunakan sebagai mekanisme autentikasi alternatif, yang berfungsi sebagai filtering, biasanya dikorelasikan dengan *'Client Name'* yang dapat dikonfigurasikan pada setiap klien. Sistim ekripsi yang diadopsi oleh komisi 802.11 adalah WEP, merupakan teknik enkripsi menggunakan WEP *key* dengan panjang kode sebesar 40 bit atau 104 bit.

Autentikasi Radio *Wireless* Klien

Autentikasi yang dimaksudkan didalam sistem jaringan 802.11 adalah autentikasi antara radio *wireless* klien dengan radio *Access Point* (AP), bukan autentikasi usernya. Proses autentikasi ini terdiri dari beberapa *step* seperti yang terlihat pada gambar 1.

1. Klien mengirim *frame probe request* secara *broadcast* ke AP.
2. Jika radio klien berada didalam radius jangkauan transmisi AP, maka AP akan membalas dengan *frame probe response.*
3. Radio klien lalu mengirim *frame authen tication request* ke AP.
4. AP membalas dengan mengirim *authenti cation reply* ke klien.
5. Jika proses autentikasi sukses, klien akan mengirim *frame association request* ke AP untuk bergabung.
6. Kemudian AP membalas dengan *frame association response,* berarti proses auten tikasi berhasil dan klien diizinkan untuk berkomunikasi dengan AP.



Sumber: Hasil Olahan Data

Gambar 1
Proses autentikasi radio klien

Proses pencarian *Access Point* melalui pengiriman *frame probe requests and frame probe responses*

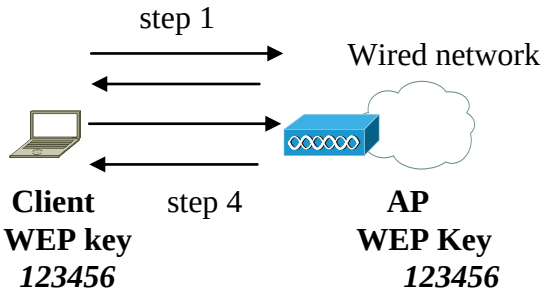
Pada waktu pertama kali radio klien dihidupkan, proses pencarian AP dimulai dengan mengirim *frame probe request* yang berisi SSID klien dan kecepatan pengiriman data *(data rate)* yand diinginkan. Radio klien akan mengirim *frame* dengan memanfaatkan seluruh RF *channel* yang dimiliki sebagai usaha untuk mempercepat proses pencarian AP. *Access Point* yang berada di dalam radius jangkauan klien, akan mengirim *frame* balasan *probe response* yang berisi bit sinkronisasi dan nilai *throughput* yang tersedia pada saat itu. *Data rate* dan *throughput* dijadikan faktor yang digunakan didalam pemilihan AP dan bila AP terpilih klien akan masuk ke fase selanjutnya yaitu fase autentikasi untuk mendapatkan akses ke jaringan.

***Open Authentication* (Proses autentikasi akses jaringan tanpa enkripsi)**

Sistim *Open Authentication* adalah sistim autentikasi pertama yang diterapkan di dalam jaringan 802.11. *Open Authentication* bersifat *connection oriented*, berarti setiap klien bebas melakukan proses autentikasi ke AP tanpa menggunakan kriteria keamanan. AP akan mengizinkan akses kepada klien tanpa menggunakan algoritma pensortiran atau MAC *address filtering.* Sistim autentikasi ini populer karena jenis peralatan *wireless* yang digunakan pada masa itu masih sederhana, seperti *wireless bar code reader* yang tidak menggunakan *micro processor* (CPU), lagipula setiap klien meng inginkan akses ke jaringan dengan cepat, sehingga proses autentikasi yang dilakukan hanya memerlukan pengiriman *frame authentication Request* dan *frame authenti cation Response* saja, Izin akses masuk ke jaringan klien hanya cukup menggunakan SSID tanpa enkripsi. Tetapi jika AP mengaktifkan sistim enkripsi WEP, maka klien tetap harus melakukan proses autentikasi dengan menggunakan kode WEP *key*, jika tidak, izin akses tidak akan diberkan dan klien tidak akan dapat berkomunikasi dengan AP.

***Shared Key Authentication* (Proses autentikasi dengan enkripsi)**

Sistem autentikasi *Shatred Key* adalah opsi yang kedua dari standard 802.11, dimana klien harus meng-konfigurasi radionya dengan enkripsi WEP. AP akan membuat kode WEP *key* dan mengirimkannya ke klien. Proses autentikasi dapat dilihat pada gambar 2.



Sumber: Hasil Olahan Data

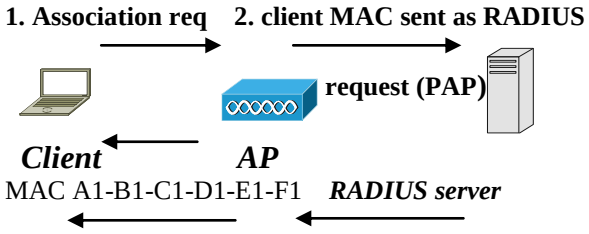
Gambar 2
Proses autentikasi dengan *Shared Key*

1. Klien mengirim *frame probe authentication request* ke AP berupa *challenge text*
2. AP membalas dengan *frame probe authentication response* ke klien berupa *challenge text.*
3. Klien mengirim *frame authentication request* ke AP dengan *response text* yang telah di-enkripsi.
4. AP membalas dengan frame authenti cation response sebagai tanda bahwa izin akses diberikan.

MAC Address Authentication* (Proses autentikasi dengan menggunakan *MAC address).

Sistem autentikasi ini sebenarnya tidak dicantumkan di dalam standard spesifikasi

802.11, tetapi banyak vendor terkemuka menerapkannya sebagai alternatif.dari sistim autentikasi *Open Key* atau *Shared Key*. Akses ke AP dibatasi dengan cara menyeleksi *MAC address* klien kemudian disesuaikan *MAC address* yang tercantum pada list dari sebuah tabel, jika *MAC address* klien ada pada *list*, maka klien akan diberi izin akses, jika tidak, akses klien akan ditolak. *Note:* setiap klien atau AP, memiliki *MAC address* yang disimpan di dalam ROM pada setiap *wireless* NIC. MAC *address* terdiri dari 6 byte atau 48 bit yang ditulis di dalam format *hexadecimal*, contohnya: 00-08-74-97-0B-26. Proses auten tikasi dengan *MAC address* dapat dilihat pada gambar 3.



Sumber: Hasil Olahan Data

Gambar 3

Proses autentikasi dengan *MAC address*

Autentikasi dengan *MAC address* dapat dilakukan secara langsung ke *Access Point* atau melalui sebuah *server* yang dikenal dengan istilah RADIUS. Autentikasi secara dilakukan secara langsung yang melakukan penyortirannya adalah AP. Gambar 3 adalah proses autentikasi dengan menggunakan *server.*

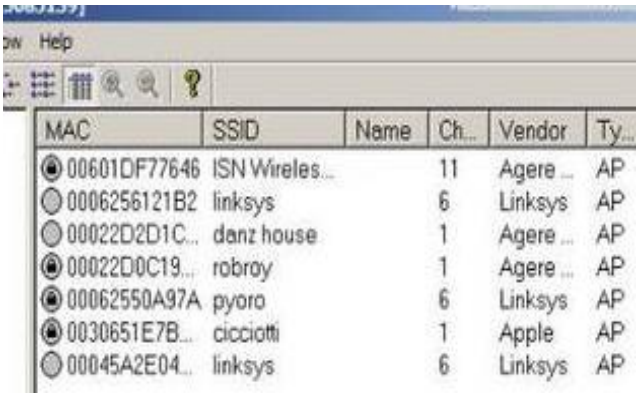
1. Klien mengirim *frame Association request* yang berisi *MAC address* ke AP.
2. AP mengirim *MAC address* klien ke *server* dengan menggunakan *protocol autentikasi* PAP (tanpa enkripsi).
3. Server mengecek *MAC address* klien dengan tabel MAC. Jika *MAC address* klien ada di *list*, *server* akan mengirim *frame RADIUS ACCEPT* ke AP.
4. AP mengirim *frame Association response* ke klien sebagai tanda proses autentikasi melalui *server* telah dilaksanakan dengan sukses.

Klien sekarang dapat mengakses jaringan dan berkomunikasi dengan AP.

Authentication Vulnerabilities (Kerawanan sistem autentikasi 802.11)

Kelemahan penggunaan SSID

Di dalam proses autentikasi, SSID dikirim ke oleh AP seluruh klien di dalam jaringan di dalam bentuk format *plain-text*, proses pengiriman ini yang dikenal dengan istilah *'Beacon Message'*. Meskipun *beacon* ini ditujukan khusus kepada semua klien yang aktif, *intrude*r atau *eavesdropper* dapat melacak dan mendeteksi informasi yang tersimpan di dalamnya dengan mudah, dengan menggunakan program aplikasi seperti packet sniffer. Pada gambar: 4 dapat dilihat kode SSID dan *MAC address* dari sebuah AP yang dilacak dengan program *Network Stumbler*.



Sumber: Hasil Olahan Data

Gambar 4

Contoh SSID dan MAC address yang dilacak dengan program Net work Stumbler

Sebenarnya SSID tidak dapat dipakai sebagai mekanisme *security*, karena sangat rawan dan mudah dideteksi, banyak *vendor* merekomendasikan untuk mendisable pentransmisian *beacon* SSID yang dikirim dari AP, tetapi hal ini akan menimbulkan masa lah pengoperasian sistem jaringan *wireless* yang memiliki multi-vendor.

Open Authentication Vulnerabi lities. (kelemahan sistim *Open Authentication*)

Di dalam sistem *Open Authentication*, *Access Point* sama sekali tidak memiliki kontrol terhadap klien, AP tidak dapat menentukan klien mana yang berhak mengakses j, berarti sistim jaringan sama sekali tidak memiliki fasi-

litas keamanan atau *security*, hal ini merupakan titik kelemahan yang sangat fatal jika opsi enkripsi WEP tidak diaktifkan, sehingga banyak vendor terkemuka menyarankan untuk tidak mengoperasikan sistim jaringann 802.11 tanpa enkripsi WEP, kecuali jaringan tersebut menerapkan opsi sistim autentikasi *Service Selection Gateway* (SSG) yang beroperasi pada *upper layer* dari model OSI.

Kelemahan sistim autentikasi *Shared Key*

Proses autentikasi *Shared Key:*

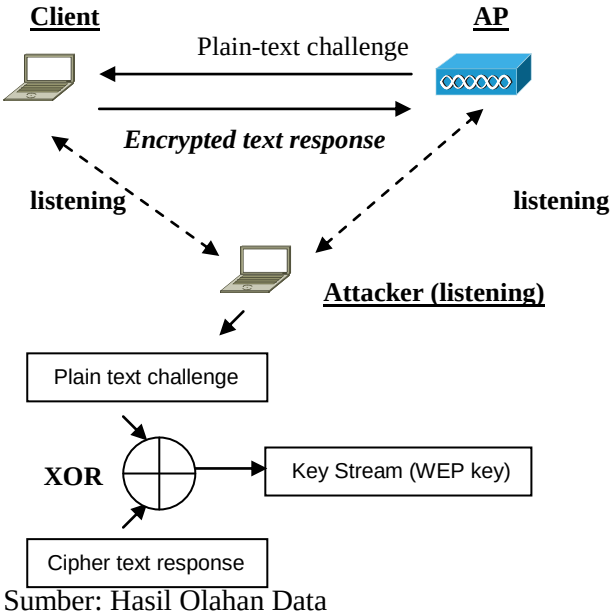
1. Sebelumnya, klien telah menerima WEP *key* yang dibuat AP untuk digunakan secara bersama.
2. Proses autentikasi dimulai, klien mengirim *frame probe request* untuk meminta akses.
3. AP mengirim *challenge-text* ke klien tanpa enkripsi *(plain-text)*
4. Klien kemudian mengenkripsi *challenge-text* dengan WEP *key* yang telah dimiliki nya dan mengirimnya kembali ke AP se bagai *challenge response text.*
5. AP menerima *challenge-response text*, lalu mendekripsinya dengan *WEP key* yang sama, hasilnya dibandingkan dengan *chal lenge text* yang asli.
6. Jika hasil *text*nya sama, maka proses autentikasi berhasil sukses. Klien akan dapat mengakses jaringan dan berkomunikasi dengan AP.

Semua proses autentikasi yang berlangsung dikirim melalui gelombang radio (RF) yang dipancarkan keseluruh penjuru. *Intruder* atau *attacker* dengan mudah bisa memonitor transmisi baik yang dikirim oleh klien maupun AP. Dengan program aplikasi Packet Analyzer yang canggih, plain-text maupun *cipher text* dapat dibaca dan semua kode seperti SSID, MAC address, dan WEP key yang dienkripsi dapat dipecahkan. Proses pemecahan kode WEP *key (Key Stream)* oleh *intruder* dapat dilakukan:

1. Dengan menggunakan program *AirSnort* atau Kismet, *intruder* memonitor *plain text challenge* dan *cipher-text response.*
2. Lalu *intruder* melakukan operasi *Exclusive-OR (XOR)* pada kedua text, untuk memecah kode enkripsi, hasil outputnya adalah berupa WEP *key (Key Stream)* yang diinginkan.

Dapat disimpulkan sistim enkripsi WEP tidak dapat diandalkan sebagai mekanisme sistem keamanan jaringan *wireless* 802.11.

Proses penyadapan pada sistim autentikasi *Shared Key*



Sumber: Hasil Olahan Data

Gambar 5
Kelemahan Autentikasi Shared Key dimana informasi dapat disadap oleh intruder

Kelemahan sistim autentikasi dengan *MAC Address*

Titik kelemahan sistim autentikasi ini sama seperti sistim autentikasi lainnya, intruder dapat menyadap, melacak dan membaca *MAC address* yang ditransmisikan baik oleh klien maupun AP. Teknik penyusupan yang dilakukan oleh *intruder* adalah dengan memanfaatkan atau menggunakan MAC *address* klien lain untuk memperoleh akses ke jaringan, cara ini dikenal dengan istilah *'spoofing'*. MAC *address spoofing* memungkinkan, karena sistem pengalamatan MAC *address* pada *wireless* NIC *card* menggunakan sistem *Universally Administered Address-UAA)* yang dapat dirubah atau diganti menjadi dengan *MAC address* lokal atau *(Locally Administered Address - LAA).* Tidak seperti halnya *MAC address NIC card* pada jaringan LAN ethernet, yang tidak bisa dirubah atau diganti, dimana teknik spoofing bisa

dilakukan dengan cara mengganti IP *address.* Pada gambar: 3 di atas dapat dilihat *MAC address* dari klien atau AP yang disadap dan dilacak dengan program *Network Stumbler*.

Sistim enkripsi WEP dan kelemahannya

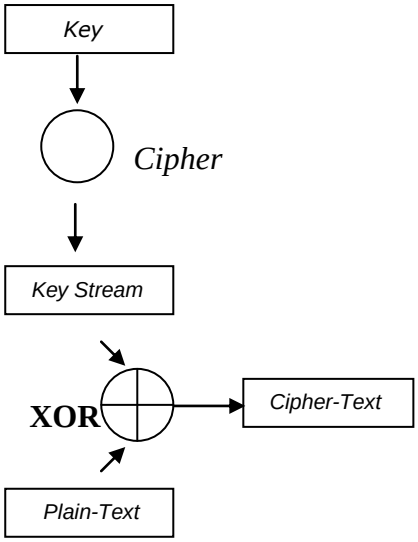
Jika klien atau AP mengaktifkan enkripsi WEP pada radio *wireless*nya, maka setiap frame yang akan ditransmisikan, terlebih dahulu diproses dengan teknik enkripsi *stream cipher* RC4 yang dirancang oleh perusahaan RSA. Proses pembuatan kode cipher ini terjadi di dalam *wireless NIC card*, dengan kata lain WEP hanya mengenkripsi data yang dikirim keluar dari masing radio *wireless* 802.11, begitu *frame*nya masuk ke sistim jaringan LAN, ekripsi WEP tidak digunakan. RC4 menggunakan teknik *stream cipher* simetrik artinya di dalam proses ekripsi dan dekripsi, klien dan AP harus menggunakan *WEP key* yang sama. Teknik enkripsi lain yang digunakan oleh WEP adalah *Block Cipher* yang metodenya hampir sama sperti *Stream Cipher*, kedua teknik enkripsi ini dikenal juga dengan nama *Eletronic Code Book (ECB).*

Teknik enkripsi Stream Cipher

Gambar 6, menjelaskan proses enkripsi *Stream Cipher*. Kode WEP *key* dimasukkan ke alam proses *Cipher,* hasilnya berupa sederetan *encrypted code* yang disebut *Key Stream*. Lalu *Key Stream* diolah dengan *PlainText* melalui operasi XOR, hasilnya adalah *Cipher Text.* Jumlah bit dari *key stream* tidak ditentukan besarnya, tergantung dari kebutuhan proses algoritma yang digunakan, yang penting harus sama dengan jumlah bit dari *Plain Text* yang dibuat.

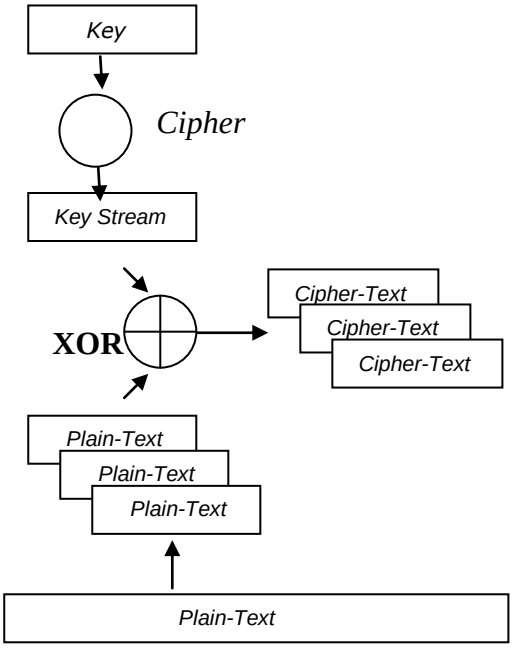
Teknik enkripsi Block Cipher

Jika pada teknik *stream cipher* data yang diproses adalah *frame* per *frame,* maka pada teknik *block cipher* yang diproses adalah sekelompok (satu blok) *frame* yang jumlahnya telah ditentukan sebelumnya (setiap *frame* besarnya 1 *byte*). Misalnya, data yang akan dienkripsi besarnya 38 byte dengan ketentuan satu blok besarnya 16 *byte,* maka jumlah blok yang akan dienkripsi adalah dua blok masing-masing 16 byte, dan satu blok sebesar 6 byte. Kemudian *block* yang 6 *byte* di tambahkan dengan 10 *byte padding*, supaya jumlah *byte* per blok tetap 16. Gambar 7 adalah proses emkripsi *Block Cipher*.



Sumber: Hasil Olahan Data

Gambar 6
proses enkripsi Stream Cipher.

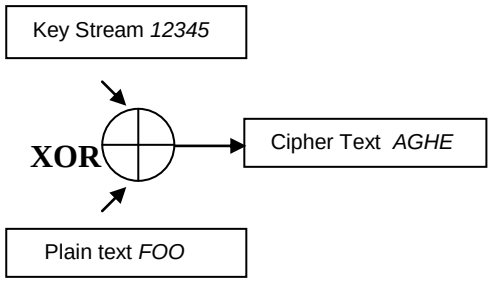


Sumber: Hasil Olahan Data

Gambar 7
Proses enkripsi *Block Cipher*

Salah satu kelemahan dari kedua jenis teknik enkripsi diatas (ECB) adalah terdapat sebuah kondisi dimana jika input *plain text*nya sama akan menghasilkan *cipher text* yang sama, sehingga *intuder* dapat mempelajari dan meng-

analisa *pattern* dari *cipher text* yang mereka sadap, lalu mencoba menebak kode aslinya, apalagi usaha mereka didukung dengan program aplikasi packet sniffer yang canggih yang bebas diperoleh dipasaran, maka sistim enkripsi WEP dengan mudah bisa dipecahkan. Gambar 8, adalah ilustrasi dari teknik enkripsi ECB.



Sumber: Hasil Olahan Data

Gambar 8
teknik enkripsi ECB

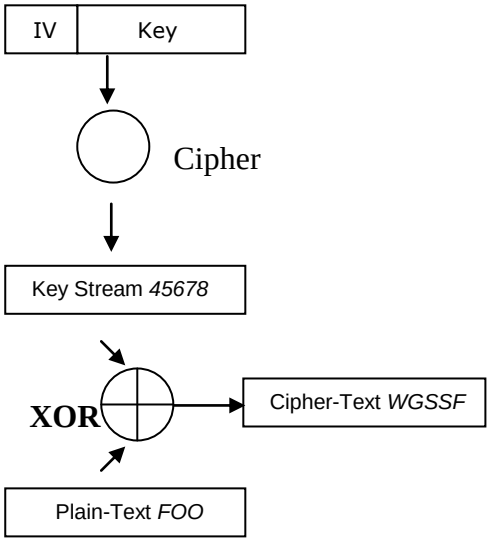
Jika kilen atau AP memasukkan *plain text* yang sama *'FOO',* maka hasil *cipher*nya tetap *AGHE*. Lalu bagaimana cara memecahkan masalah ini ?. Ada dua teknik enkripsi yang dianggap mampu menjadi solusinya:

1. dengan menggunakan *InitializationVector* (IV) sebagai algoritma tambahan
2. dengan menggunakan teknik *feedback* mode (tidak dibahas didalam jurnal)

Penggunaan *Initialization Vectors* pada sistim enkripsi WEP

Initialization Vector disingkat I.V digunakan sebagai kode sisipan untuk menambah tingkat kesulitan pemecahan kode *Key Stream.* I.V. adalah nilai bit yang ditambahkan *kode key* sebelum *key stream* diproses, jadi setiap kali nilai I.V. diganti maka *bit key stream* nya ikut berubah, pada gambar 9 diperlihat kan melalui operasi XOR, bila sebuah *input plain text FOO* diolah dengan *Key* plus I.V. *45678* akan menghasilkan cipher text yang berbeda *WGSSF*. (karena ada tambahan bit I.V)

Komisi 802.11 merekomendasikan, penambahan nilai I.V. sebaiknya dilakukan pada setiap frame, untuk mencegah apabila ada dua frame yang sama ditransmisikan, maka cipher textnya tetap akan berbeda, sehingga menyulitkan *intruder* untuk memecahkan kode cipher yang disadap. Nilai I.V. besarnya 24 bit, jika ditambahkan dengan 40 bit WEP *key, key stream*nya menjadi 64 bit dan. Untuk WEP key 104 bit, panjang *key stream*nya menjadi 128 bit. Sayangnya nilai I.V. yang ditempatkan di dalam *header* dari setiap *frame,* dikirim dalam bentuk *clear text* tanpa enkripsi, sehingga setiap radio wire less yang menerima dapat membacanya.

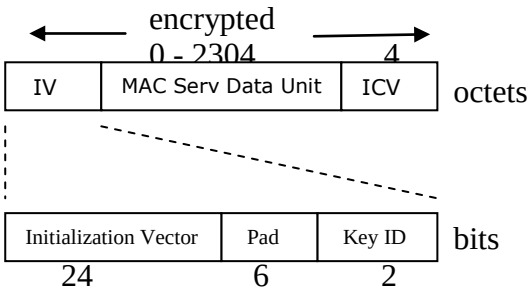


Sumber: Hasil Olahan Data

Gambar 9
Enkripsi dengan Initialization Vector (I.V.)

Jika nilai I.V. tidak sering dirubah atau diganti oleh sipengirim, maka pattern I.V. yang diterima akan selalu sama dan hal ini yang menjadikan salah satu titik rawan dari sistem enkripsi WEP. Jumlah bit (24 bit) yang digunakan I.V terlampau sedikit sehingga kemungkinan terjadinya I.V. *collision* yaitu suatu keadaan dimana diketemukan dua key stream yang sama yang telah dipakai untuk menghasilkan *cipher text*. Dapat dibayang kan bila sebuah AP yang sangat aktif mengirim data sebesar 1500 byte dengan kecepatan 11 Mbps, akan menghabiskan semua kemungkinan permutasi yang bisa dibuat oleh 24 bit I.V. dalam tempo → {(11*10^6)*2^24 = 18000 detik atau 5 jam}, berarti intruder memiliki cukup waktu untuk mencari dan mendeteksi dua *cipher text* yang telah dienkripsi dengan *key stream* yang sama dan melakukan analisa statik untuk memecahkan sebuah kode *WEP key*. Gambar 10 memperlihatkan proses penam bahan I.V. pada *frame* yang telah di-enkripsi dengan WEP. Dan gambar 11, adalah nilai I.V. yang disadap dan dideteksi oleh *intruder*

dengan menggunakan aplikasi program *packet sniffer*.

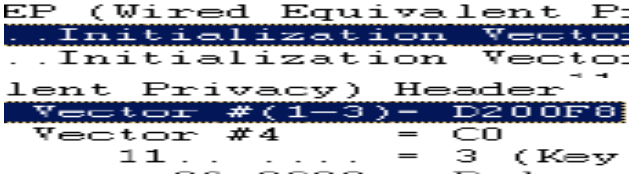


Sumber: Hasil Olahan Data

Gambar 10

Proses penyisipan IV

Dari gambar di atas terlihat I.V dikirim tanpa enkripsi, bahagian yang dienkripsi hanya MAC sevice data unit dan ICV, akibatnya I.V dapat dijadikan *object* untuk dimodifi kasi.



Sumber: Hasil Olahan Data

Gambar 11

Nilai I.V. yang terdeteksi.

Situasinya bertambah parah apabila semua klien dan AP menggunakan WEP *key* yang sama, karena kemungkinan terjadinya I.V. *collision* akan bertambah besar. Contohnya, *wireless* NIC *card* dari sebuah vendor terkenal, secara otomatis akan mereset nilai I.V kembali ke posisi 0, pada setiap kali di pasang atau dikonfigurasi, dan nilai I.V. akan bertambah 1 untuk setiap paket yang dikirim, berarti jika ada dua buah *wireless card* yang dipasang dalam waktu yang sama, maka pada suatu waktu akan terdjadi I.V *collision* yang jumlahnya sangat banyak, sekondisi ini seolah-olah menyediakan kesempatan emas bagi *intruder.*

32 bit ICV *(Integrated Check Value)* adalah mekanisme *error correction* yang digunakan untuk menjaga integritas data yang dikirim melalui media *wireless.* ICV yang dikenal juga dengan istilah CRC *(Cyclical Redundancy Check),* dimana setiap frame yang diterima oleh sebuah radio *wireless,* nilai CRC akan dihitung kembali dan dibandingkan dengan nilai CRC asli, jika nilainya sama maka frame akan diproses, jika tidak, maka telah terjadi kesalahan atau perubahan data selama diperjalanan lalu frame akan di-*reject* dan *wireless* pengirim akan diberitahukan dengan sebuah isyarat agar frame dikirim ulang.

Proses 32 bit CRC adalah proses linier, artinya *intruder* bisa menghitung perbedaan bit dari dua buah CRC berdasar kan perbedaan bit dari dua *cipher text* yang disadap, dengan kata lain *intruder* bisa memodifikasi bit-bit CRC dengan proses *'bit-flipping'* sehingga CRC yang diterima oleh *wireless* penerima seolah-olah valid. Lagi-lagi sistem enkripsi WEP diketemu kan titik rawan yang baru, yang bisa dimanfaatkan oleh *intruder* atau *attacker,* yaitu kelemahan pada *segment* ICV yang dapat dijadikan objek sasaran untuk menyerang sebuah sistim jaringan *wireless.* Bit-bit ICV yang dimodikasi oleh *intruder* dapat mengaki batkan sistem pengiriman menjadi tidak efektif, karena semua *frame* yang telah dimodifikasi oleh *intruder* akan diterima oleh *wireless* sebagai *frame* yang asli dan valid .

Proses pemecahan kode *WEP key*

Pemecahan kode WEP *key* dapat dilakukan *intruder* dengan dua cara penerangan yaitu: *Passive Attack* digunakan untuk *mendecrypt traffic (to decrypt traffic)* dan *Active Attack* digunakan untuk menyisipkan data paslu ke dalam *traffic (to inject traffic).*

Passive Network Attack

Titik kelemahan enkripsi WEP terletak pada metode algoritma *(Key Scheduling Algo rithm-KSA)* dan *initialization Vector* IV yang diterapkan di dalam teknik enkripsi *Stream Cipher. Passive Attacks* terjadi bila *intruder* memonitor atau melakukan *eaves dropping* pada *traffic* data yang sedang aktif di jaringan. *Intruder* menggunakan program aplikasi seperti *AirSnort* yang mudah diperoleh dari Internet, kode WEP key yang panjangnya 128 bit dapat dipecahkan dalam waktu beberapa jam saja karena pattern dari kode enkripsi dapat dianalisa secara statis.

Secara hukum *passive attack* bukanlah merupakan sebuah pelanggaran, karena intruder

secara pasif hanya mengamati lalu lintas traffic data, bukan melakukan kerusakan atau kerugian pada sistim jaringan.

Passive attack sangat sulit dilacak, karena siapa saja boleh menggunakan frekuensi bebas izin yang juga digunakan oleh sistim jaringan *wireless*, lagi pula *passive attack* sekarang sudah menjadi hal yang umum seolah –olah menjadi hobi bagi setiap orang.

Celah kelemahan ini membuat sistim enkripsi WEP menjadi tidak efektif, harus dicari sebuah solusi yang komperehensif untuk memperkuat sistim enkripsi kode WEP *key*.

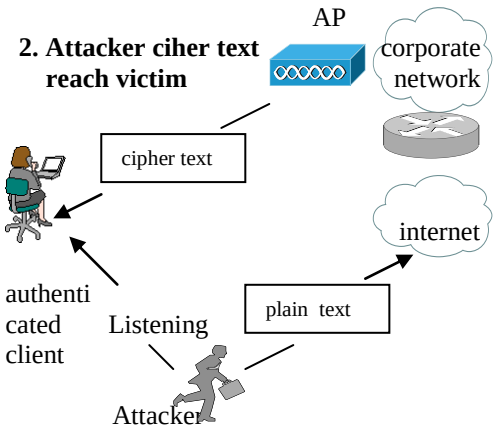
Active Network Attacks

Active attack dimulai jika *intruder* telah berhasil melakukan *passive attack*, dimana informasi-informasi penting yang dibutuhkan semuanya telah diperoleh, kemudian langkah selanjut nya yang harus dilakukankan bagi *intruder-intruder* yang berniat jahat adalah melakukan *active attack.* Pada umumnya kategori *active attack* termasuk: *unauthorized access* (penyusupan ke dalam sistem jaringan secara ilegal), teknik *spoofing, Denial of service (DoS), flooding attack, bit-flipping attack* dan I.V. *replay attack*, atau semua usaha penjegatan, penyadapan dan pemodifikasian *traffic* data diantara dua buah radio *wireles* disebut dengan istilah *Man in The Midlle Attack (MITM).* Dua tipe serangan yang sangat ber bahaya terhadap sistim keamanan jaringan 802.11 adalah I.V *Replay* dan *Bit-Flipping*

Initialization Vector Replay Attacks

I.V. *attack* bersifat induktif yang ancamannya dapat berkembang yang membahayakan sistim jaringan. Gambar 12, mengilustrasikan proses I.V. *attack.*

1. *Attacker* mengirim e-mail dengan alamat pengirimpalsu ke sebuah *wireless* klien yang akan dijadikan korban.
2. *Attacker* memonitor aktifitas korban dengan menggunakan program aplikasi *packet sniffer* yang canggih, dan menunggu jawaban e-mail dari korban, yang diincar adalah *cipher text*nya korban.
3. Begitu *cipher text*nya disadap, *attacker* akan melakukan proses analisis untuk memecahkan kode *key stream* korban.
4. Setelah berhasil, *attacker* akan memodifikasi *key stream* dengan memperbanyak bitnya dan mengirim kembali ke korban dengan menggunakan I.V. dan WEP keynya korban.



Sumber: Hasil Olahan Data

Gambar 12

Kelemahan I.V. *re-use*

I.V. *attack* dapat di-*reuse* atau di-*replay* berulang kali untuk menyerang korban dengan *key stream* yang ber-tubi sehingga melumpuhkan jaringan korban. Biasanya proses I.V. *attack* memanfaatkan *protocol* ICMP salah satu *protocol upper layer* dari model TCP/IP *layer suite* yang digunakan jaringan internet untuk mengontrol proses pengiriman paket data, dimana ICMP akan mengirim *message Echo Reply Message* sebagai laporan kembali ke si pengirim. *Echo Reply Message* inilah yang dijadikan *object* untuk menyerang jaringan korban.

Bit-Flipping Attacks

Bit-flipping attack menyerang kelemahan dari salah satu bagian *frame* yang ditransmisikan yaitu ICV atau 32 bit CRC, yang bertujuan untuk memodifikasi dan merusak data *payload* atau *message* yang dibawa, walaupun ICV itu sendiri berfungsi sebagai mekanisme untuk menjaga integritas *payload* data sewaktu transit. Kelemahan ICV terletak pada algoritma CRC yang linier, dengan perkataan lain jika ada dua message yang dinyatakan dengan X dan Y,

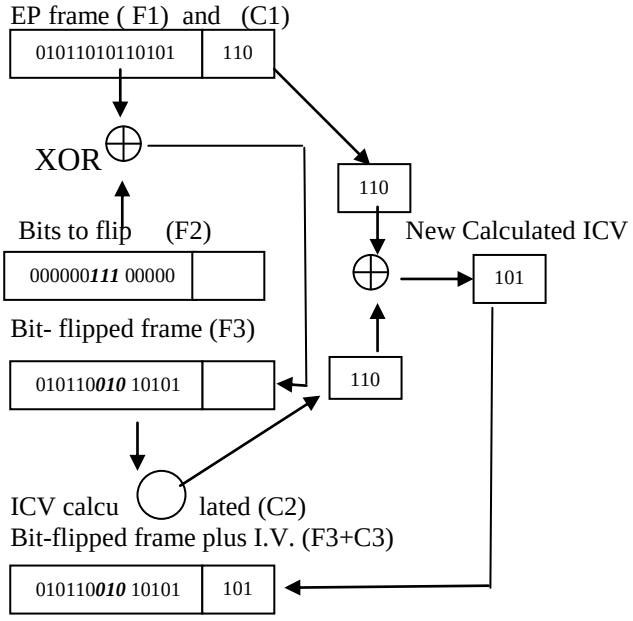
dan tanda adalah exclusive OR atau XOR maka :

$$CRC (X \oplus Y) = CRC (X \oplus CRC (Y)$$

Dapat diartikan, jika seorang *attacker* (MITM) ingin memodifikasi isi data *plain text* yang sedang dikirim dari sebuah radio *wireless* ke radio *wireless* lainnya maka ia cukup merubah salah satu bit yang ada didalam data tersebut, dan *wireless* penerima akan membaca *plain text* yang berbeda, teknik penyerangan ini dikenal dengan istilah *'Bit Flipping Attack'*, Proses detailnya dapat dijelaskan sebagai berikut:

1. *Attacker* melacak *frame* yang sedang dikirim dengan *packet sniffer.*
2. *Attacker* berhasil mendeteksi *frame* dan merubah salah satu bit dari data *payload*.
3. Lalu *attacker* memodifikasi ICVnya supaya CRCnya seolah-olah valid walaupun data nya sudah dimodifikasi.
4. *Attacker* mengirim *frame* yang telah di modifikasi ke korban.
5. Korban menerima frame dan melakukan verifikasi dengan menghitung ICV berda sarkan isi *(content)* frame yang diterima.
6. Korban membandingkan ICV yang telah dihitung dengan field ICV yang ada di frame, ternyata hasilnya cocok.
7. Frame dianggap valid lalu dideencap sulate, dikirim ke layer 3 untuk diproses paket datanya.
8. Data *payload* dari paket diperiksa, dan dihitung *'checksum'* nya ternyata tidak cocok, karena data telah dimodifikasi sewaktu transit. <u>*Note*</u> *: checksum* adalah mekanisme layer 3 untuk mencek integritas data *payload* dan *header* sewaktu transit diantara router, karena paket *layer* 3 tidak menggunakan ICV atau CRC.
9. Sistim TCP/IP *wireless* korban, mendeteksi *error,* lalu mengirim *error message* yang telah dienkripsi ke *wireless* pengirim dengan protocol ICMP. (selama proses ini, attacker tetap mengawasi dan memonitor semua aktifitas *wireless* korban).
10. *Attacker* melacak ICMP *message* yang dikirim, lalu melakukan proses pendeteksian data *key stream*nya untuk melakukan replay attack yang bisa dlaku kan berulang-ulang sampai jaringan *wireless* korban lumpuh total.

Proses pemodifikasian ICV harus dibuat sesuai (match) dengan data yang telah dimodifikasi seperti yang dijelaskan pada step 3, merupakan proses yang kompleks, tetapi dengan bantuan program aplikasi yang cang gih, perhitungan ini dapat dilakukan dengan mudah, secara detail dapat dijelaskan pada gambar: 13.



Sumber: Hasil Olahan Data

Gambar 3
Proses modifikasi IC

I.V. attack dan Bit Flipping attack berakibat sangat fatal terhadap jaringan wireless.

Static WEP Key Management Issues (Masalah pengelolaan *WEP key*)

Di dalam *standard* 802.11 tidak dicantumkan bagaimana cara mengelola mekanisme WEP key, enkripsi WEP menggunakan key secara statis. WEP key dibuat secara sharing, dengan menggunakan kode yang sama, bila *key* dicuri orang atau hilang, akibatnya sangat merepotkan administrator, karena harus mengkonfigurasi kembali setiap peralatan *wireless* yang ada satu per satu demi untuk menjaga keamanan jaringan. Hal ini tidak menjadi masalah untuk jaringan skala kecil, tetapi tidak realistis untuk jaringan skala menengah dan besar, dimana jumlah wireless klien bisa

mencapai ribuan buah. Tanpa menggunakan mekanisme untuk mendistribusi menglelola WEP secara dina mis, administrator harus mengamati dan mengawasi setiap wireless NIC yang ada.

Kesimpulan

Sistem keamanan dari jaringan wireless LAN harus didesign sebaik mungkin, dari isi jurnal dapat dilihat kelemahan-kelemahan dan kerawanan tingkat keamanan jaringan *wireless* 802.11. Berbagai macam serangan dapat menembus sistem keamanan jaringan ini, titik kelemahan dari enkripsi WEP merupakan konsekuensi dari kesalahan pengertian di dalam mendesign *cryptographic protocol*. Produk aplikasi *security* tambahan telah dibuat untuk memperbaiki sistim security jaringan 802.11. Beberapa vendor telah menambah sistim enkripsi dari 40 bit menjadi 152 bit bahkan 256 bit, tetapi sayangnya tidak kompatible dengan puluhan ribu *wireless* telah beroperasi sebelum nya. Vendor-vendor lain juga telah menge-luarkan solusi untuk mangatasi kelemahan WEP, antara lain: IEEE menawarkan 801.X secu rity protocol sebagai solusi, Cisco mena warkan sebuah solusi yang komprehensif yaitu, *Cisco Wireless Security Suite* LEAP, WiFI Alliance memperkenalkan WPA (Wi-Fi *Protec-ted Access*), dengan versi terakhir WPA2 sebagai solusi.

Daftar Pustaka

IEEE Standard 802, *"Standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) spe-cifications",* 1999.

IEEE Standard 802.1x-2001, *"Standard for Port based Network Access Control",* 2001.

Intercepting Mobile Communications: The Insecurity of 802.11 http://www.isaac. cs.berkeley.edu/isaac/mobicom.pdf

Weaknesses in the Key Scheduling Algorithm of RC4 -http://www.eyetap.org/~rguer ra/toronto2001/rc4_ksaproc.pdf

Stubblefield, A., Ioannidis, J., and Rubin, A. "A Key Recovery Attack on the 802.11b

Wired Equivalent Privacy Protocol (WEP)".http://www.cs.jhu.edu/~rubin/c ourses/sp04/wep.pdf