BERBAGAI JENIS ENKRIPSI KEAMANAN JARINGAN NIRKABEL

Darwin (13508102)

Jurusan Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : dawn0689@aol.com

Abstrak

Pada masa sekarang ini keamanan jaringan nirkabel merupakan salah satu bagian yang paling berkembang dalam penggunaan jaringan. Sering kali kita dapat menemukan berbagai sinyal nirkabel yang dapat kita akses. Pengembangan jaringan menggunakan nirkabel ini berbeda dengan jaringan yang menggunakan kabel karena pada jaringan nirkabel ini tidak ada restriksi banyaknya pengguna yang dapat terhubung sehingga lebih fleksibel. Tetapi kekurangan yang sangat besar ialah tidak adanya keamanan yang memadai karena terlalu fleksibel. Siapa saja yang menemukan sinyal nirkabel ini dapat melakukan koneksi hubungan sehingga dapat menerima juga data-data yang penting yang terjadi pada koneksi tersebut. Pada jaringan dengan menggunakan kabel dapat dicegah dengan membatasi kabel-kabel yang dapat dipasang ke jaringan tersebut. Tetapi pada jaringan nirkabel hal itu sangatlah tidak mungkin karena sistem nirkabel menggunakan gelombang dan gelombang tidak dapat dibatasi.

Untuk mencegah hal itu terjadi, kita dapat melakukannya dengan melakukan enkripsi terhadap jaringan kita sehingga penyadapan terhadap jaringan kita tidak dapat dilakukan.

Dalam melakukan pengenkripsian jaringan ini terdapat berbaga jenis. Dalam makalah ini akan dibahas mengenai WEP (Wired Equivalent Privacy), WPAv1, EAP, WPAv2, token encryption, RF shielding dan juga WAPI.

Seluruh jenis enkripsi di atas memilki ada yang memilki kelemahan tersendiri. Berbagai penyempurnaan dilakukan sehingga lahirnya jenis-jenis enkripsi seperti di atas.

Kata kunci: keamanan, jaringan nirkabel, enkripsi.

1. Pendahuluan

Pada dewasa ini, jarigan (network) merupakan salah satu bagian yang paling penting. Dengan penggunaan jaringan ini kita dapat menyambungkan data dari berbagai lokasi secara menyeluruh sehingga dapat dibuka di mana saja. Sebagai contoh sekarang telah ada *Local Area Network* (LAN) yang menggunakan kabel LAN dan juga jaringan LAN yang bersifat nirkabel.

Jaringan tersebut dapat dibentuk dalam skala kecil maupun skala yang sangat besar. Bila dalam skala kecil, kita dalam melakukan pengawasan apakah jaringan kita disadap oleh orang lain yang dapat mengambil data kita atau tidak. Meskipun hal tersebut sangatlah tidak fleksibel tetapi masih dapat dimungkinkan. Tetapi bila jaringan tersebut sudah bergerak dalam skala besar maka pengawasan terhadap segala jalur yang terjadi adalah suatu hal yang mustahil.

Bila terjadi adanya kebocoran jaringan dari jaringan yang sangat besar tersebut, maka hal tersebut akan dapat berakibat sangat fatal karena segala informasi yang ada dapat disadap oleh penyadap tersebut. Karena itu, untuk mencegah hal tersebut terjadi maka dikembangkan sebuah teknik kriptografi yang digunakan di bidang jaringan. Terutama pada jaringan nirkabel karena pada nirkabel tidak dapat dilakukan pembatasan koneksi seperti pada jaringan kabel yang dapat dibatasi dengan membatasi banyaknya kabel jaringan yang dapat terhubung.

Pengembangan enkripsi jaringan melahirkan banyak jenis enkripsi dengan menggunakan berbagai jenis informasi. Jenis-jenis enkripsi tersebut memiliki kelemahan tersendiri sehingga kemudian dikembangkan lagi untuk menutupi kelemahan sebelumnya.

Sebagai contoh bila dalam suatu perusahaan atau organisasi jaringan nirkabel mereka tidak dilakukan suatu enkripsi maka bisa saja ada seseorang yang menggunakan jaringan tersebut untuk mengambil informasi-informasi penting dari tempat tersebut. Karena jaringan ini bersifat nirkabel maka tidak dapat diketahui siapa yang

mengambil dan dari lokasi mereka masuk ke jaringan tersebut. Bisa saja mereka masuk ke jaringan tersebut dari tempat parkir ataupun dari kamar kecil. Bisa juga diluar gedung tersebut apabila besarnya sinyal jaringan yang digunakan tidak dikendalikan dengan benar.

1.1 Pengertian dari kriptografi

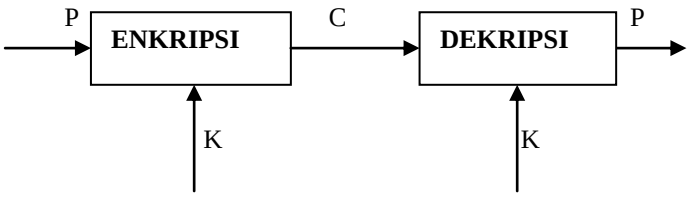
Kriptografi adalah suatu ilmu dan seni dalam menyembunyikan suatu informasi agar tidak dapat dibaca dan diperoleh pihak yang tidak bersangkutan. Kriptografi berasal dari bahasa yunani yang terdiri dari krypto yang artinya rahasia dan grafi yang artinya tulisan. Kriptografi merupakan suatu tulisan rahasia.

Seni kriptografi adalah suatu seni yang sangat tua. Penggunaan dari kriptografi sudah sangat lama. Penggunaan yang pertama kali digunakan adalah kriptografi transposisi yaitu menukar posisi dari huruf tersebut dengan sebelahnya contoh kalimat “saya tidur” dengan kriptografi tersebut maka berubah menjadi “asay itdru”. Jenis kriptografi yang lain adalah kriptografi substitusi yaitu dengan menambahkan posisi dari kalimat tersebut maju ke depan selangkah. Contoh pada kalimat “makalah ini” maka akan berubah menjadi “nblbmbi joj”.

Teknik dari kriptografi tersebut semuanya menggunakan sistem enkripsi dan dekripsi. Dimana enkripsi digunakan untuk membuat pesan tersebut tidak terbaca atau dapat berubah menjadi sebuah sandi dan dekripsi membuat hasil dari sandi tersebut dapat dibaca kembali.

Pada umunya kriptografi mempunyai beberapa komponen utama yang dibutuhkan yaitu :

1. Plaintext : pesan asli yang ingin disampaikan
2. Chipertext : pesan tersandi, pesan yang sudah mengalami pemrosesan
3. Cipher dan kunci, cipher adalah suatu algoritma yang digunakan untuk membentuk pesan tersebut menjadi sebuah chipertext, sedangkan kunci adalah sekumpulan bit yang diperlukan untuk mengenkripsi dan mendekripsi data.



Gambar 1 : Proses enkripsi / dekripsi sederhana
P : Plaintext
C : Ciphertext
K : Kunci

Pada proses enkripsi sebuah pesan dibutuhkan sebuah kunci yang berfungsi sebagai acuan dari enkripsi tersebut. Pada enkrispi transposisi digunakan kunci pemindahan posisi sehingga pada saat dekripsi sandi tersebut maka hasilnya akan berubah menjadi pesan awal. Pada enkripsi substitusional digunakan pemindahan setiap huruf maju satu abjad ke depan. Sehingga dapat kita lihat bahwa pada proses enkripsi yang paling penting adalah kunci yang digunakan untuk enkripsi pesan tersebut. Semakin panjang proses kunci yang digunakan maka semakin susah pula kunci tersebut dapat diterka. Cipher tersebut terletak pada saat enkripsi dan dekripsi. Input dari kunci tersebut kemudian akan dimasukkan ke algoritma tersebut yang akan mengubah bentuk dari pesan tersebut. Bila pesan yang sudah tersandi tersebut dimasukkan kembali ke dekripsi dengan kunci yang berbeda maka hasil keluaran tersebut akan tetap ada tetapi berbeda dengan yang pesan awal yang sudah ditulis.

1.2 Fungsi dari kriptografi

Kriptografi mempunyai fungsi yang sangat penting yaitu sebagai media untuk menyimpan pesan yang tidak dapat dibaca oleh orang kecuali yang bersangkutan.Tetapi dengan semakin berkembangnya zaman dan juga semakin berkembangnya ilmu kriptografi, fungsi-fungsi dari kriptografi tidak hanya terbatas untuk menyimpan sebuah pesan.

Adapun fungsi-fungsi dari kriptografi ialah :

1. Kerahasiaan (*confidentiality*), dengan enkripsi maka kerahasiaan dapat terjaga.
2. Privasi (*privacy*), dengan adanya enkripsi maka hal-hal yang bersifat pribadi tidak dapat diketahui oleh orang lain maupun dipergunakan oleh orang lain.
3. Autentikasi (a*uthenticity*), dengan adanya enkripsi sandi maka yang dapat menerima pesan tersebut adalah yang sudah terauntentikasi sehingga orang yang tidak diinginkan tidak dapat menerimanya atau menggunakannya.

4. Tanda tangan (*signature*), penerima dapat menerima pesan atau menggunakan hasil yang diterima dari orang yang yang diinginkan.

5. Koordinasi (*coordinate*), pada saat komunikasi dengan banyak pihak, setiap pihak dapat berkoordinasi tanpa diketahui oleh pihak yang lain.

6. Minimal (*minimalism*), tidak ada yang dapat berkomunikasi dengan pihak selain yang diinginkan.

2. Prinsip dasar enkripsi terhadap jaringan nirkabel

Pengenkripsian terhadap jaringan nirkabel menggunakan berbagai jenis informasi dari yang terdapat dari server nirkabel tersebut sampai dengan input yang diinginkan untuk membuat enkripsi tersebut.

Dari berbagai jenis informasi yang digunakan untuk enkripsi tesebut maka terbentuklah berbagai jenis enkripsi yang dapat digunakan.

2.1 Jenis-jenis enkripsi untuk jaringan nirkabel

Di bawah ini akan dijelaskan bebagai jenis enkripsi yang dilakukan berdasarkan jenis informasi yang digunakan.

2.1.1. WEP (*Wired Equivalent Privacy*)

WEP (*Wired Equivalent Privacy*) pertama kali diperkenalkan pada tahun 1997 sebagai suatu jaringan enkripsi. WEP merupakan standar yang digunakan untuk pengenkripsian jaringan yang dilakukan. WEP ini menggunakanm algoritma RC4 untuk melakukan enkripsi dan CRC-32 untuk mengecek integritas dari pengenkripsian ini. WEP merupakan salah satu sistem pengenkripsian jaringan yang paling lemah.

Beberapa tahun setelah diresmikannya WEP mulai ditemukan banyak kelemahan dari sistem enkripsi ini. Hal ini dapat terjadi karena penyadap hanya perlu menyadap proses yang terjadi di jaringan tersebut selama beberapa saat dan kemudian langsung dapat menembus sandi lewat yang dibentuk oleh pengguna tersebut. Jika digunakan sebuah sandi lewat yang lebih panjang untuk keamanan lebih, hal itu tidak akan berpengaruh. Karena pada sandi yang lebih panjang penyadap hanya perlu menyadap lebih proses yang terjadi pada jaringan tersebut dan kemudian dapat menembus enkripsi pertahanan yang terjadi. Penggunaan enkripsi WEP ini juga digunakan pada penyambungan jaringan ad-hoc sesama komputer.

2.1.2. WPAv1 (*Wi-Fi Protected Access 1*)

WPA1 adalah suatu sistem yang dikembangkan dari WEP. Di sini seluruh kelemahan dari WEP telah dihilangkan dalam WPA1. Dalam WPA1 ini penggunaan enkripsi yang digunakan adalah dari 8 sampai 63 karakter. Pada WPA1 ini dikembangkan enkripsi dengan menggunakan TKIP (*Temporal Key Integrity Protocol*) Bila sandi lewat yang digunakan semakin pendek, maka akan semakin mudah dijebol. Pada saat pemasukan salah, penyadap dapat menerkan sandi kita pada saat autentikasi kita salah. Bila kunci yang kita gunakan semakin panjang maka penyadap akan mengalami kesusahan dalam menerka kunci tersebut. Pada sistem VPN juga dapat digunakan fungsi ini.

2.1.3. EAP (*Extensible Authentication Protocol*)

EAP adalah suatu jenis autentikasi yang bersifat universal yang pada umunya digunakan pada jaringan nirkabel. Pada EAP ini dapat juga digunakan pada jaringan kabel, tetapi lebih sering digunakan pada jaringan nirkabel. EAP ini berfungsi kerangka yang berfungsi utnuk melakukan autentikasi bukan sebagai mekanisme autentikasi. EAP menyediakan beberapa fungsi umum dan pilihan dari mekanisme autentikasi yang diinginkan. Terdapat beberapa metoda autentikasi yang bisa digunakan. EAP dapat menggunakan NAS (*Network Access Server*) yang dapat memberikan mekanisme autentikasi yang lebih aman dengan menggunakan PMK (*Pair-wise Master Key*) antara klien dengan NAS. PMK ini kemudian dapat digunakan sebagai kunci untuk melakukan enkripsi berdasarkan enkripsi TKIP (*Temporal Key Integrity Protocol*) ataupun CCMP (*Counter Mode with Cipher Block Chaining Message Authentication Code Protocol*).

EAP mengandung banyak jenis mekanisme autentikasi. Pada bagian ini akan dijelaskan mengenai 2 bagian dari EAP yaitu LEAP dan PEAP.

2.1.3.1. LEAP (*Lightweight Extensible Authentication Protocol*)

Pada LEAP ini digunakan WEP dan dilakukan minimisasi terhadap WEP orisinil sehingga kelemahan-kelemahan ini dapat tertutupi dan juga digunakan suatu sistem pengaturan kunci yang lebih terstruktur. Pada mekanisme autentikasi ini juga digunkan MAC *address* sebagai bagian dari autentikator. MAC *address* adalah suatu *Media Access Control address* yang mempunyai suatu identifikator yang unik. Identifikator ini terpasang pada perangkat keras ethernet yang kita miliki.

LEAP bukanlah suatu mekanisme autentikasi yang kuat. Pada LEAP mekanisme autentikasi relatif lemah. Karena pada MAC *address* yang kita gunakan untuk autentikasi dapat digunakan suatu software open source untuk memanipulasi MAC *address* yang kita miliki untuk melewati autentikasi tersebut.

2.1.3.2. PEAP (*Protected Extensible Authentication Protocol*)

Pada PEAP ini digunakan suatu metoda untuk dapat mengirimkan informasi autentikasi secara aman, termasuk sandi lewat, pada jaringan lain maupun pada jaringan nirkabel. Sistem ini dikembangkan oleh Cisco Systems, Microsoft, dan RSA Security. Perlu diingat juga bahwa PEAP ini bukanlah suatu sistem enkripsi melainkan hanyalah suatu sistem autentikasi dari suatu klien ke sebuah jaringan.

PEAP menggunakan kunci publik server untuk mengauntentikasi. Kemudian membuat sebuah jalur SSL (*Secure Socket Layer*) /TLS (*Transport Layer Security*) antara klien dengan server untuk diauntentikasi. Pembuatan jalur ini menggunakan kunci publik dari server sehingga pergantian informasi tidak dapat disadap.

2.1.4. WPAv2 (*Wi-fi Protected Access 2*)

Pada WPA2 dilakukan perbaikan terhadap kelemahan yang terdapat pada WPA1. Dari perubahan maka WPA semakin kuat dalam menjaga keamanan dan tidak mudah untuk disadap.

2.1.5. Token encryption

Token encryption adalah salah satu jenis enkripsi yang sangat kuat keamanannya. Ketika digabungkan dengan beberapa perangkat lunak server, perangkat keras server atau kartu perangkat lunak, token ini akan mengambil nomor identitas dari perangkat-perangkat ini digabung dengan masukan dari pengguna untuk menghasilkan suatu algoritma yang akan menghasilkan suatu kunci enkripsi yang baru. Server tersebut akan menggunakan sinkronisasi waktu dengan kartu tersebut. Ini merupakan salah satu cara yang paling aman untuk membentuk suatu jaringan nirkabel yang kita inginkan.

Pada *enkripsi token* ini, kunci enkripsi akan selalu berubah berdasarkan komputer server tersebut. Bila komputer server menambahkan suatu perangkat keras yang baru maka perangkat keras tersebut akan mempengaruhi algoritma tersebut yang akan mengakibatkan berubahnya kunci enkripsi. Kestabilitas dari server tersebut adalah hal yang sangat penting.

2.1.6. RF shielding

Penggunaan perisai untuk menahan suatu sinyal tersebut tidak keluar dari jalur yang seharusnya juga merupakan suatu bagian yang sangat penting. Dengan dibuatnya erisai ini maka keamanan dari jaringan nirkabel tersebut semakin kuat dan semakin aman. Hal ini dapat terjadi karena dengan adanya perisai yang menutupi sinyal tersbut maka akan lebih sulit bagi penyadap untuk mengambil sinyal jaringan di luar dari yang kita kendalikan.

2.1.7. WAPI (WLAN Authentication and Privacy Infrastructure)

WAPI adalah sistem standar yang digunakan oleh pemerintahan Cina untuk jaringan LAN (*Local Area Network*). Meskipun ini dikembangkan untuk digunakan di atas WiFi tetapi masih mengalami masalah yang amat besar karena hanya 11 dari perusahaan Cina yang mempunyai akses untuk penggunaan ini.

WAPI ini dikembangkan agar dapat menyelesaikan masalah kelemahan keamanan yang terjadi WEP. WAPI ini diisukan oleh pemerintahan Cina pada tahun 2003. WAPI bekerja dengan menggunakan ASU (*Authentication Service Unit*). Standar WAPI menggunakan algoritma enkripsi simetrik.

IV. KESIMPULAN

Pada masa sekarang ini dibutuhkan adanya fleksibilitas sehingga dikembangkan berbagai jenis teknologi yang mendukung agar hal tersebut dapat terjadi. Salah satunya adalah dengan dibuatnya sistem jaringan nirkabel. Sistem jaringan nirkabel ini diprediksi akan mengganti sistem jaringan kabel.

Pada sistem jaringan nirkabel banyaknya pengguna yang masuk ke jaringan berbeda dengan sistem jaringan yang menggunakan kabel. Pada sistem jaringan dengan menggunakan kabel, banyaknya pengguna yang dapat masuk ke jaringan terbatas pada banyaknya kabel yang dapat dipasang pada komputer pengguna.

Pada sistem jaringan nirkabel menggunakan gelombang sinyal yang beredar dalam suatu lingkup daerah tertentu. Siapa saja yang berada dalam daerah tersebut yang mendapatkan sinyal gelombang tersebut dapat melakukan koneksi ke jaringan tersebut. Masalah yang terjadi ialah bagaimana merestriksi terhadap siapa saja jaringan ini boleh terhubung dan terhadap siapa saja jaringan ini tidak boleh terhubung.

Karena adanya permasalahan seperti itu maka dikembangkanlah suatu jaringan yang bersifat dienkripsi. Jaringan yang dienkripsi tersebut dapat berupa

menggunakan sandi lewat ataupun hal-hal lainnya seperti MAC *address*. Karena dimungkinkan melakukan sebuah enkripsi dengan berbagai teknik dan algoritma yang berbeda maka terbentuklah berbagai jenis enkripsi jaringan.

Ditelusuri dari perkembangannya masih ditemukannya banyak kelemahan dalam pengembangan enkripsi jaringan sehingga penyadapan masih dapat dimungkinkan. Sampai dengan sekarang pengenkripsian jaringan nirkabel yang dilakukan sudah sangat kuat keamanannya. Meskipun begitu pengembangan masih terus dilakukan agar keamanan tersebut dapat terjaga dan terus dicari sebuah solusi yang dapat memungkinkan.

REFERENSI

[1] Wireless Security.
http://en.wikipedia.org/wiki/Network_encryption#802.11_security
Tanggal akses 13 December 2009, pukul 14.00

[2] Wired Equivalent Privacy.
http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy
Tanggal akses 13 December 2009, pukul 16.00

[3] Wired Equivalent Privacy.
http://kb.netgear.com/app/answers/detail/a_id/1141
Tanggal akses 13 December 2009, pukul 16.00

[4] Wireless Protected Access.
http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access
Tanggal akses 13 December 2009, pukul 16.30

[5] Munir, Rinaldi. 2008. Diktat Kuliah IF2091 Struktur Diskrit. Departemen Teknik Informatika, Institut Teknologi Bandung.
Tanggal Akses 13 Desember 2009
Pukul 17.00

[6] Extensible Authentication Protocol.
http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
Tanggal akses 13 December 2009, pukul 17.00

[7] Protected Extensible Authentication Protocol.
http://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol
Tanggal akses 13 December 2009, pukul 18.00

[8] Protected Extensible Authentication Protocol.
http://en.wikipedia.org/wiki/WLAN_Authentication_and_Privacy_Infrastructure
Tanggal akses 13 December 2009, pukul 18.30