Keamanan Wireless LAN

Muhammad Fatkhurrahman
m.fatkhur_rahman@yahoo.co.id
http://sunkrill.blogspot.com

Pendahuluan

Jaringan wireless memiliki nlebih banyak kelemahan dibanding dengan jaringan kabel (wired). Saat ini perkembangan teknologi wireless sangat pesat sejalan dengan kebutuhan sistem informasi yang mobile. Teknologi wireless banyak diaplikasikan untuk hotspot komersil, ISP, warnet, kampus-kampus dan perkantoran, namun hanya sebagian pengelola jaringan yang memperhatikan keamanan komunikasi data pada jaringan wireless tersebut.

Kelemahan jaringan wireless secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Salah satu contoh penyebab kelemahan pada konfigurasi karena saat ini untuk membangun sebuah jaringan wireless cukup mudah. Banyak vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan wireless yang masih menggunakan konfigurasi wireless default bawaan vendor. WEP (Wired Equivalent Privacy) yang menjadi standart keamanan wireless sebelumnya, saat ini dapat dengan mudah dipecahkan dengan berbagai tools yang tersedia gratis di internet. WPA-PSK dan LEAP yang dianggap menjadi solusi menggantikan WEP, saat ini juga sudah dapat dipecahkan dengan metode dictionary attack secara offline.

Kelemahan Wireless pada Lapisan Fisik

Wifi menggunakan gelombang radio pada frekuensi milik umum yang bersifat bebas digunakan oleh semua kalangan dengan batasan batasan tertentu. Setiap wifi memiliki area jangkauan tertentu tergantung power dan antenna yang digunakan. Tidak mudah melakukan pembatasan area yang dijangkau pada wifi.

Hal ini memungkinkan terjadinya tindakan berikut:

1. Interception atau penyadapan
   Hal ini sangat mudah dilakukan oleh para hacker, mengingat berbagai tools dan teknik kriptografi dapat dengan mudah ditemukan di internet.
2. Jamming
   Jamming terjadi karena frekuensi yang digunakan cukup sempit sehingga penggunaan kembali channel sulit dilakukan pada area dengan jaringan nirkabel yang padat.
3. Injection
   Injection dapat dilakukan karena adanya kelemahan pada cara kerja wifi dimana tidak ada proses validasi siapa yang sedang terhubung atau yang sedang memutuskan koneksi saat itu.
4. Hijacking
   Serangan MITM (Man In The Middle) adalah pengambilalihan komunikasi yang sedang terjadi dan melakukan pencurian atau modifikasi data informasi.

Kelemahan pada Lapisan MAC (Data Layer)

Pada lapisan ini terdapat kelemahan yakni jika sudah terlalu banyak node (client) yang menggunakan channel yang sama dan terhubung pada AP yang sama, maka bandwidth yang mampu dilewatkan akan menurun. Selain itu MAC address sangat mudah di spoofing (ditiru atau di duplikasi) membuat banyak permasalahan keamanan.

Teknik Keamanan yang digunakan pada Wireless LAN

Berikut ini adalah beberapa langkah yang dapat dilakukan untuk mengamankan jaringan wireless:

1. Menyembunyikan SSID
   SSID disembunyikan dengan maksud agar hanya yang mengetahui SSID yang dapat terhubung ke jaringan tertentu. Hal ini tidak sepenuhnya benar karena SSID tidak dapat disembunyikan secara sempurna.

2. Menggunakan Kunci WEP
   WEP merupakan standart keamanan & enkripsi pertama yang digunakan pada wireless, WEP memiliki berbagai kelemahan antara lain :
   - Masalah kunci yang lemah, algoritma RC4 yang digunakan dapat dipecahkan.
   - WEP menggunakan kunci yang bersifat statis
   - Masalah initialization vector (IV) WEP
   - Masalah integritas pesan Cyclic Redundancy Check (CRC32)

   WEP merupakan suatu algoritma enkripsi yang digunakan oleh shared key pada proses autentikasi untuk memeriksa user dan untuk meng-enkripsi data yang dilewatkan pada segment jaringan wireless pada LAN. WEP digunakan pada standar IEEE 802.11. WEP juga merupakan algoritma sederhana yang menggunakan pseudo-random number generator (PRNG) dan RC4 stream cipher. RC4 stream cipher digunakan untuk decrypt dan encrypt.

3. MAC Address Filtering
   MAC Address Filtering merupakan metoda filtering untuk membatasi hak akses dari MAC Address yang bersangkutan. MAC filters ini juga merupakan metode sistem keamanan yang baik dalam WLAN, karena peka terhadap jenis gangguan seperti:
   - pencurian pc card dalam MAC filter dari suatu access point
   - sniffing terhadap WLAN

4. Menggunakan kunci WAP-PSK dan WAP2-PSK
   WPA merupakan teknologi keamanan sementara yang diciptakan untuk menggantikan kunci WEP. Ada dua jenis yakni WPA personal (WPA-PSK), dan WPA-RADIUS. Saat ini yang sudah dapat di crack adalah WPA-PSK, yakni dengan metode brute force attack secara offline. Brute force dengan menggunakan mencoba-coba banyak kata dari suatu kamus. Serangan ini akan berhasil jika passphrase yang yang digunakan wireless tersebut memang terapat pada kamus kata yang digunakan si hacker. Untuk mencegah adanya serangan terhadap keamanan wireless menggunakan WPA-PSK, gunakanlah passphrase yang cukup panjang.

Keamanan wireless dapat ditingkatkan dengan menggunakan kombinasi dari beberapa teknik yang disebut di atas. Tata letak wireless dan pengaturan daya transmit sebuah Access Point juga harus diperhatikan untuk mengurangi resiko penyalahgunaan wireless. Konfigurasi default dari tiap vendor perangkat wireless sebaiknya diubah settingannya sehingga keamanan lebih terjaga. Yang paling penting adalah gunakan teknologi wireless dengan bijak.

Referensi

Josua M. Sinambela, http://josh.staff.ugm.ac.id

Biografi Penulis

Muhammad Fatkhurrahman lahir di Sleman, DI Yogyakarta. Telah menyelesaikan pendidikan dasar di SD Muhammadiyah Karanganjir, SMP N 1 Godean, SMK N 2 Yogyakarta. Saat ini penulis sedang menempuh kuliah semester 3 di Politeknik Negeri Semarang Program D3 Teknik Telekomunikasi. Yang bersangkutan adalah pengelola blog *http://sunkrill.blogspot.com*.