Wireless Access Point: security and attack overview

Oleh: Benfano Soewito

Komunikasi nirkabel adalah pertukaran informasi antara dua atau lebih perangkat yang tidak terhubung oleh konduktor listrik. Sebuah jaringan Wireless Local Area Network (WLAN) menghubungkan dua atau lebih perangkat menggunakan transmisi radio, biasanya koneksi ini melalui access point. Koneksi ini terjadi dengan teknik yangdisebut Spread Spectrum atau lebih spesifuknya adalah dengan menggunakan teknik Orthogonal Frequency Division Multiplexing (OFDM). Disamping mempunyai kelemahan, wireless network atau network nirkabel mempunyai beberapa keuntungan dibanding dengan fixed network atau network dengan menggunakan kabel, kelebihannya adalah:

1. ***Mobility***: pengguna WLAN dapat mengakses internet tidak tergantung dari lokasi, mereka dapat mengakses internet dimana saja sepanjang masih dalam area coverage.

2. ***Scalability***: topology WLAN dapat di konfigure sesuai dengan kebutuhan dan apabila perlu ditambahkan jumlah user, dapat dilakukan dengan mudah, tidak perlu untuk menambah atau mempersiapkan kabel.

3. ***Installation Flexibility***: pengguna WLAN dapat konek ke network tanpa harus menggunakan kabel.

4. ***Simplicity***: untuk membangun wireless network sangat mudah dilakukan baik saat set-up maupun saat mengkonfigurasinya.

Kelemahan utama dari wireless network ini adalah masalah keamanannya. Membangun sistim keamanan pada wireless network lebih sulit dibanding dengan membangun keamanan pada wired network. Hal ini sangat masuk akal, sebab media untuk pertukaran data atau informasi pada WLAN adalah dengan menggunakan transmisi radio. Sehingga sangat mungkin setiap orang dapat mengakses informasi yang transmisikan antara akses point dan pengguna.

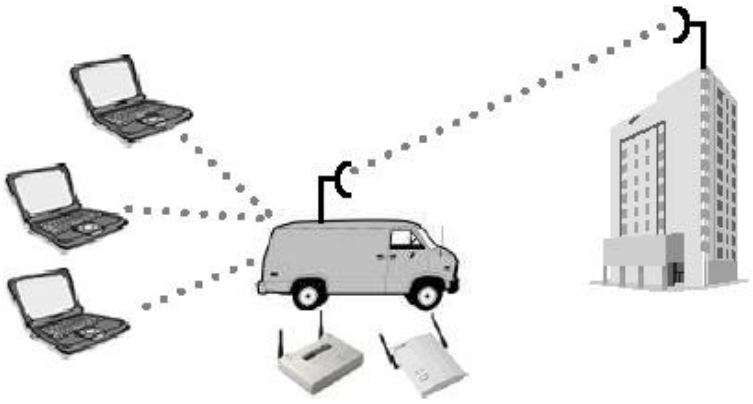
Untuk mengatasi masalah ini banyak teknik keamanan yang digunakan pada wireless network. Selain teknik yang pada dasarnya adalah memperkuat teknik enkripsi atau mengembangkan metodolgi dan rule yang menyangkut teknik enkripsi tersebut, juga ada

beberapa teknik lainnya. Di bawah ini adalah teknik teknik yang sudah dikenal dalam menjaga keamanan WLAN:

1. Encryption
2. Authentication (User name and password)
3. Hidden SSID (Service Set Identifier)
4. MAC address filtering
5. WEP (Wired Equivalent Privacy)
6. WPA / WPA2 (Wi-Fi Protected Access)

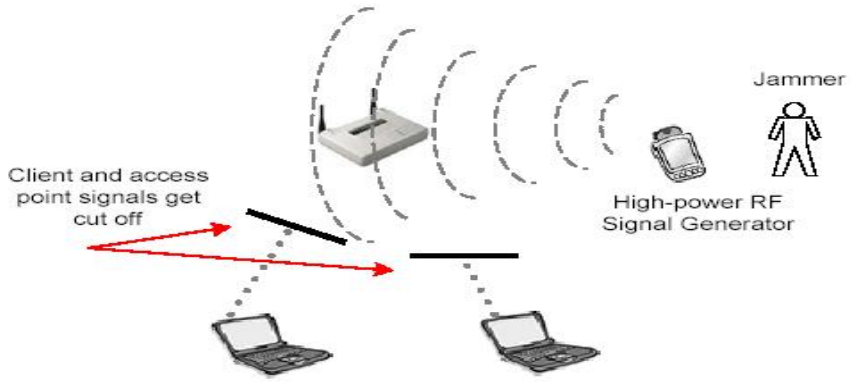
Dengan keterbukaan media transmisi WLAN dan hampir selalu ada orang yang punya waktu untuk mengutak - atik sinyal WLAN, maka akan selalu ada kesempatan untuk menyerang WLAN. Beberapa motif serangan WLAN diantaranya adalah ingin mendapatkan akses internet gratis, mencuri data, memata - matai kegiatan seseorang atau perusahaan, sampai merusak sistem sebuah perusahaan. Beberapa model serangan terhadap WLAN yang berkembang saat ini antara lain:

1. *Wireless Network Sniffing* : Sniffing merupakan kegiatan eavesdropping atau mendengarkan paket data apa saja yang lewat di jaringan. Sebuah sniffer merupakan program yang melakukan intercept (menyadap) dan melakukan decode traffic jaringan yang sedang dipancarkan ke sebuah media. Lebih mudah melakukan *sniffing* pada jaringan wireless. Seperti yang diketahui bahwa WLAN menggunakan medium udara yang berarti sejauh coverage sinyal WLAN, sejauh itu pula dapat dilakukan *sniffing.* Berbeda dengan jaringan wired, jika ingin melakukan *sniffing* si penyerang harus menemukan cara menginstal alat *sniffing*-nya ke dalam jaringan yang hendak diserang. Beberapa kegiatan yang berhubungan dengan *sniffing* adalah *Passive Sniffing, Detection of SSID,* dan *Collecting MAC Address.*
2. *Wireless Man in The Middle Attack* : Serangan Man-in-the-Middle dilakukan dengan mengelabui koneksi antara komputer pengguna resmi dan access point dengan cara memasukkan komputer lain di antara keduanya sebagai pancingan. Jenis serangan ini hampir sama dengan jenis serangan pada jaringan kabel. Program yang digunakan juga sama, kecuali perangkat wirelessnya. Dengan menggunakan sebuah program, penyusup mampu memosisikan diri di antara lalu lintas komunikasi data dalam jaringan nirkabel.



Gambar 1. Wireless Man-in-the-Middle Attack

3. *Denial of Service* : Suatu keadaan di mana sebuah system tidak dapat menyediakan layanan kepada user yang berhak karena sumber daya yang dimiliki tidak bekerja dengan baik yang diakibatkan oleh penyerang. Dalam WLAN serangan DOS sulit untuk dicegah, bahkan si target tidak menyadari adanya serangan. Diantara beberapa serangan DoS antara lain *Signal Jamming, packet flooding.*



Gambar 2. Signal Jamming

4. *Brute Force Attack* : serangan dengan melakukan uji coba terhadap kunci akses dengan mencoba semua kombinasi password yang mungkin, dimana sebagian besar *access point* menggunakan suatu kunci tunggal atau *password* yang dimiliki oleh *wireless user* pada *Wireless LAN*.
5. *Dictionary Attack* : serangan dengan melakukan uji coba terhadap kunci akses dengan mencoba kombinasi password yang ada dalam list password, dimana sebagian besar *access point* menggunakan suatu kunci tunggal atau *password* yang dimiliki oleh *wireless user* pada *Wireless LAN*.

6. *Session Hijacking* : serangan ini dilakukan untuk mencuri *session* dari seorang *wireless user* yang sudah terotentikasi dengan *accces point*. Penyerang akan mengirimkan pesan *disassociate* kepada *wireless user* dengan membuatnya seolah-olah berasal dari *access point*. *Wireless user* akan mengira bahwa koneksi dengan *access point* telah terputus, namun *access point* tetap beranggapan bahwa *wireless user* masih terkoneksi dengannya. Kemudian penyerang akan menggunakan *MAC Address* dan *IP Address* untuk melakukan koneksi dengan *access point* seolah-olah sebagai *wireless user* tersebut

Dalam mengamankan WLAN, selain masalah teknik dan peralatan, perlu diperhatikan juga tentang policy penggunaan WLAN dan pelatihan bagi semua staff dari level terendah sampai tertinggi. Policy untuk penggunaan WLAN pada umumnya adalah sebagai berikut:

1. Jaringan yang akan dipakai oleh user internal terpisah dengan jaringan yang akan disediakan bagi tamu / user external.
2. Perangkat WiFi akan diproteksi dengan password untuk koneksi ke jaringan WiFi serta Login Name dan password untuk akses internet.
3. Password harus diganti tiap 3 (tiga) bulan sekali. User internal tidak diperkenankan untuk memberitahukan username dan password domain kepada tamu / user external / internal lain dengan alasan apapun.
4. Seluruh aktifitas user yang terkoneksi menggunakan jaringan WiFi akan dicatat (logging) secara otomatis, dan dievaluasi, khususnya untuk pemakaian oleh tamu / user external.
5. Filtering terhadap akses ke website yang mengandung pornografi, social networks, dan Trojan Horse. Filtering ini akan diupdate secara rutin setiap sebulan sekali atau tiap kali ada perkembangan atau informasi baru.
6. User tidak diperkenankan untuk melakukan konfigurasi atau usaha pembobolan, pencurian data (sniffing) akses WiFi untuk keperluan apapun.