Wireless Security

Dalam Era Globalisasi sekarang, penggunaan internet sudah berkembang pesat, dapat kita lihat bahwa hampir di seluruh belahan bumi ini sudah terkoneksi internet. Dahulu untuk melakukan koneksi ke internet kebanyakan orang menggunakan kabel, tetapi sekarang ini untuk koneksi ke internet sudah bisa menggunakan wireless. Wireless memiliki lebih banyak keuntungan , diantaranya user bisa melakukan koneksi internet kapan saja dan dimana saja asal masih berada dalam ruang lingkup hot-spot, selain itu dalam segi biaya pembangunan, wireless jauh lebih murah bila dibandingkan dengan kabel. Walaupun demikian, wireless memiliki lebih banyak kelemahan dibandingkan dengan kabel, khususnya dari segi keamanan.

Wireless tidak cuma bisa diakses melalui komputer saja, wireless juga dapat diakses melalui smart phone ataupun PDA. Alat ini juga dilengkapi dengan sistem metode jaringan nirkabel yang dapat mengakses internet tanpa dibatasi oleh jarak, waktu dan tempat. namun alat ini masih rentan terhadap kode yang mengganggu, karena memang pada dasarnya alat ini dirancang dan di desain tidak dilengkapi dengan adanya perlindungan atau keamanan yang dapat melindungi data/informasi yang disimpannya. Sehingga alat ini masih memerlukan metode system operasi yang dapat melindungi baik data/informasi yang disimpannya maupun jaringan nirkabelnya

Sejak wireless menggunakan komunikasi yang lebih terbuka untuk media komunikasi maka digunakanlah Wired Equivalent Pripacy (WEP), Wi-fi Protected Access (WPA, WPA2) dan Wireless Transpot Layer Security (WTLS) untuk memastikan keamanan jaringan nirkabel computer. Selain memiliki keuntungan, Wireless juga memiliki beberapa kelemahan, Banyak penyedia jasa wireless seperti hotspot komersil, ISP, Warnet, kampus-kampus maupun perkantoran sudah mulai memanfaatkan wireless pada jaringan masing masing, tetapi sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan wireless tersebut. Hal ini membuat para hacker menjadi tertarik untuk mengexplore keamampuannya untuk melakukan berbagai aktifitas yang biasanya ilegal menggunakan wifi.
Banyak hacker wireless ataupun para pemula dalam melakukan wardriving dengan menggunakan berbagai jenis aktivitas dan metode. Wardriving adalah kegiatan atau aktivitas untuk mendapatkan informasi tentang suatu jaringan wifi dan mendapatkan akses terhadap jaringan wireless tersebut. Umumnya bertujuan untuk mendapatkan koneksi internet, tetapi banyak juga yang melakukan untuk maksud-maksud tertentu mulai dari rasa keingintahuan, coba coba, research, tugas praktikum, kejahatan dan lain lain.
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. Penulis sering menemukan wireless yang dipasang pada jaringan masih menggunakan setting default bawaan vendor seperti SSID, IP Address , remote manajemen, DHCP enable, kanal frekuensi, tanpa enkripsi bahkan user/password untuk administrasi wireless tersebut.

Macam-macam usaha dalam pengamanan jaringan wireless:
1. Menyembunyikan SSID
Banyak administrator menyembunyikan Services Set Id (SSID) jaringan wireless mereka dengan maksud agar hanya yang mengetahui SSID yang dapat terhubung ke jaringan mereka. Hal ini tidaklah benar, karena SSID sebenarnya tidak dapat disembuyikan secara sempurna. Pada saat saat tertentu atau khususnya saat client akan terhubung (assosiate) atau ketika akan memutuskan diri (deauthentication) dari sebuah jaringan wireless, maka client akan tetap mengirimkan SSID dalam bentuk plain text (meskipun menggunakan enkripsi), sehingga jika kita bermaksud menyadapnya, dapat dengan mudah menemukan informasi tersebut. Beberapa tools yang dapat digunakan untuk mendapatkan ssid yang dihidden antara lain, kismet (kisMAC), ssid\_jack (airjack), aircrack , void11 dan masih banyak lagi.

2. Keamanan Wireless dengan metode Wired Equivalent Privacy (WEP)
WEP merupakan standart keamanan & enkripsi pertama yang digunakan pada wireless, WEP (Wired Equivalent Privacy) adalah suatu metoda pengamanan jaringan nirkabel, disebut juga dengan Shared Key Authentication. Shared Key Authentication adalah metoda otentikasi yang membutuhkan penggunaan WEP. Enkripsi WEP menggunakan kunci yang dimasukkan (oleh administrator) ke client maupun access point. Kunci ini harus cocok dari yang diberikan akses point ke client, dengan yang dimasukkan client untuk authentikasi menuju access point, dan WEP mempunyai standar 802.11b.

Proses Shared Key Authentication:
1. client meminta asosiasi ke access point, langkah ini sama seperti Open System Authentication.
2. access point mengirimkan text challenge ke client secara transparan.
3. client akan memberikan respon dengan mengenkripsi text challenge dengan menggunakan kunci WEP dan mengirimkan kembali ke access point.
4. access point memberi respon atas tanggapan client, akses point akan melakukan dekripsi terhadap respon enkripsi dari client untuk melakukan verifikasi bahwa text challenge dienkripsi dengan menggunakan WEP key yang sesuai. Pada proses ini, access point akan menentukan apakah client sudah memberikan kunci WEP yang sesuai. Apabila kunci WEP yang diberikan oleh client sudah benar, maka access point akan merespon positif dan langsung meng-authentikasi client. Namun bila kunci WEP yang dimasukkan client adalah salah, maka access point akan merespon negatif dan client tidak akan diberi authentikasi. Dengan demikian, client tidak akan terauthentikasi dan tidak terasosiasi.

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 (CRC-32)
WEP terdiri dari dua tingkatan, yakni kunci 64 bit, dan 128 bit. Sebenarnya kunci rahasia pada kunci WEP 64 bit hanya 40 bit, sedang 24bit merupakan Inisialisasi Vektor (IV). Demikian juga pada kunci WEP 128 bit, kunci rahasia terdiri dari 104bit.

Serangan-serangan pada kelemahan WEP antara lain :
• Serangan terhadap kelemahan inisialisasi vektor (IV), sering disebut FMS attack. FMS singkatan dari nama ketiga penemu kelemahan IV yakni Fluhrer, Mantin, dan Shamir. Serangan ini dilakukan dengan cara mengumpulkan IV yang lemah sebanyak-banyaknya. Semakin banyak IV lemah yang diperoleh, semakin cepat ditemukan kunci yang digunakan
• Mendapatkan IV yang unik melalui packet data yang diperoleh untuk diolah untuk proses cracking kunci WEP dengan lebih cepat. Cara ini disebut chopping attack, pertama kali ditemukan oleh h1kari. Teknik ini hanya membutuhkan IV yang unik sehingga mengurangi kebutuhan IV yang lemah dalam melakukan cracking WEP.
• Kedua serangan diatas membutuhkan waktu dan packet yang cukup, untuk mempersingkat waktu, para hacker biasanya melakukan traffic injection. Traffic Injection yang sering dilakukan adalah dengan cara mengumpulkan packet ARP kemudian mengirimkan kembali ke access point. Hal ini mengakibatkan pengumpulan initial vektor lebih mudah dan cepat. Berbeda dengan serangan pertama dan kedua, untuk serangan traffic injection,diperlukan spesifikasi alat dan aplikasi tertentu yang mulai jarang ditemui di toko-toko, mulai dari chipset, versi firmware, dan versi driver serta tidak jarang harus melakukan patching terhadap driver dan aplikasinya.

3. Keamanan wireless dengan metode WI-FI Protected Accsess (WPA)

 Tidak lama setelah proses pengembangan WEP, kerapuhan dalam aspek kriptografi muncul. Berbagai macam penelitian mengenai WEP telah dilakukan dan diperoleh kesimpulan bahwa walaupun sebuah jaringan wireless terlindungi oleh WEP, pihak ketiga (hackers) masih dapat membobol masuk. Seorang hacker yang memiliki perlengkapan wireless seadanya dan peralatan software yang digunakan untuk mengumpulkan dan menganalisis cukup data, dapat mengetahui kunci enkripsi yang digunakan.
Menyikapi kelemahan yang dimiliki oleh WEP, telah dikembangkan sebuah teknik pengamanan baru yang disebut sebagai WPA (WiFI Protected Access). Teknik WPA adalah model kompatibel dengan spesifikasi standar draf IEEE 802.11i. Teknik ini mempunyai beberapa tujuan dalam desainnya, yaitu kokoh, interoperasi, mampu digunakan untuk menggantikan WEP, dapat diimplementasikan pada pengguna rumahan atau corporate, dan tersedia untuk publik secepat mungkin. Teknik WPA dibentuk untuk menyediakan pengembangan enkripsi data yang menjadi titik lemah WEP, serta menyediakan user authentication yang tampaknya hilang pada pengembangan konsep WEP.
Teknik WPA didesain menggantikan metode keamanan WEP, yang menggunakan kunci keamanan statik, dengan menggunakan TKIP (Temporal Key Integrity Protocol) yang mampu secara dinamis berubah setelah 10.000 paket data ditransmisikan. Protokol TKIP akan mengambil kunci utama sebagai starting point yang kemudian secara reguler berubah sehingga tidak ada kunci enkripsi yang digunakan dua kali. Background process secara otomatis dilakukan tanpa diketahui oleh pengguna. Dengan melakukan regenerasi kunci enkripsi kurang lebih setiap lima menit, jaringan WiFi yang menggunakan WPA telah memperlambat kerja hackers yang mencoba melakukan cracking kunci terdahulu.
Walaupun menggunakan standar enkripsi 64 dan 128 bit, seperti yang dimiliki teknologi WEP, TKIP membuat WPA menjadi lebih efektif sebagai sebuah mekanisme enkripsi. Namun, masalah penurunan throughput seperti yang dikeluhkan oleh para pengguna jaringan wireless seperti tidak menemui jawaban dari dokumen standar yang dicari. Sebab, masalah yang berhubungan dengan throughput sangatlah bergantung pada hardware yang dimiliki, secara lebih spesifik adalah chipset yang digunakan. Anggapan saat ini, jika penurunan throughput terjadi pada implementasi WEP, maka tingkat penurunan tersebut akan jauh lebih besar jika WPA dan TKIP diimplementasikan walaupun beberapa produk mengklaim bahwa penurunan throughput telah diatasi, tentunya dengan penggunaan chipset yang lebih besar kemampuan dan kapasitasnya.

Proses otentifikasi WPA menggunakan 802.1x dan EAP (Extensible Authentication Protocol). Secara bersamaan, implementasi tersebut akan menyediakan kerangka kerja yang kokoh pada proses otentifikasi pengguna. Kerangka-kerja tersebut akan melakukan utilisasi sebuah server otentifikasi terpusat, seperti RADIUS, untuk melakukan otentifikasi pengguna sebelum bergabung ke jaringan wireless. Juga diberlakukan mutual authentification, sehingga pengguna jaringan wireless tidak secara sengaja bergabung ke jaringan lain yang mungkin akan mencuri identitas jaringannya.
Mekanisme enkripsi AES (Advanced Encryption Standard) tampaknya akan diadopsi WPA dengan mekanisme otentifikasi pengguna. Namun, AES sepertinya belum perlu karena TKIP diprediksikan mampu menyediakan sebuah kerangka enkripsi yang sangat tangguh walaupun belum diketahui untuk berapa lama ketangguhannya dapat bertahan.
Untuk dapat menggunakan "kelebihan" yang dimiliki WPA, pengguna harus memiliki hardware dan software yang kompatibel dengan standar tersebut. Dari sisi hardware, hal tersebut berarti wireless access points dan wireless NIC (Network Interface Card) yang digunakan harus mengenali standar WPA. Sayang, sebagian produsen hardware tidak akan mendukung WPA melalui firmware upgrade, sehingga pengguna seperti dipaksa membeli wireless hardware baru untuk menggunakan WPA.
Dari sisi software, belum ada sistem operasi Windows yang mendukung WPA secara default. Komputer yang menggunakan system operasi Windows dengan hardware kompatibel dengan standar WPA dapat mengimplementasikannya setelah menginstal WPA client. WPA client baru dapat bekerja pada sistem operasi Windows Server 2003 dan Windows XP. Bagi para pengguna sistem operasi lainnya belum ditemukan informasi mengenai kemungkinan mengimplementasikan WPA.

4. MAC Filtering
Hampir setiap wireless access point maupun router difasilitasi dengan keamanan MAC Filtering. Hal ini sebenarnya tidak banyak membantu dalam mengamankan komunikasi wireless, karena MAC address sangat mudah dispoofing atau bahkan dirubah. Tools ifconfig pada OS Linux/Unix atau beragam tools spt network utilitis, regedit, smac, machange pada OS windows dengan mudah digunakan untuk spoofing atau mengganti MAC address.

5. Captive Portal
Infrastruktur Captive Portal awalnya didesign untuk keperluan komunitas yang memungkinkan semua orang dapat terhubung (open network). Captive portal sebenarnya merupakan mesin router atau gateway yang memproteksi atau tidak mengizinkan adanya trafik hingga user melakukan registrasi/otentikasi. Berikut cara kerja captive portal :
• user dengan wireless client diizinkan untuk terhubung wireless untuk mendapatkan IP address (DHCP).
• block semua trafik kecuali yang menuju ke captive portal (Registrasi/Otentikasi berbasis web) yang terletak pada jaringan kabel.
• redirect atau belokkan semua trafik web ke captive portal
• setelah user melakukan registrasi atau login, izinkan akses ke jaringan (internet)
Beberapa hal yang perlu diperhatikan, bahwa captive portal hanya melakukan tracking koneksi client berdasarkan IP dan MAC address setelah melakukan otentikasi. Hal ini membuat captive portal masih dimungkinkan digunakan tanpa otentikasi karena IP dan MAC adress dapat dispoofing.. Spoofing MAC adress seperti yang sudah dijelaskan pada bagian 4 diatas. Sedang untuk spoofing IP, diperlukan usaha yang lebih yakni dengan memanfaatkan ARP cache poisoning, kita dapat melakukan redirect trafik dari client yang sudah terhubung sebelumnya. Serangan lain yang cukup mudah dilakukan adalah menggunakan Rogue AP, yaitu mensetup Access Point (biasanya menggunakan HostAP) yang menggunakan komponen informasi yang sama seperti AP target seperti SSID, BSSID hingga kanal frekuensi yang digunakan. Sehingga ketika ada client yang akan terhubung ke AP buatan kita, dapat kita membelokkan trafik ke AP sebenarnya. Tidak jarang captive portal yang dibangun pada suatu hotspot memiliki kelemahan pada konfigurasi atau design jaringannya. Misalnya, otentikasi masih menggunakan plain text (http), managemen jaringan dapat diakses melalui wireless (berada pada satu network), dan masih banyak lagi. Kelemahan lain dari captive portal adalah bahwa komunikasi data atau trafik ketika sudah melakukan otentikasi (terhubung jaringan) akan dikirimkan masih belum terenkripsi, sehingga dengan mudah dapat disadap oleh para hacker.