Analisis Kelemahan Keamanan pada Jaringan Wireless

Aji Supriyanto
Fakultas Teknologi Informasi, Universitas Stikubank Semarang
e-mail : ajisup@gmail.com

ABSRAK : Pemakaian perangkat teknologi berbasis wireless pada saat ini sudah begitu banyak, baik digunakan untuk komunikasi suara maupun data. Karena teknologi wireless memanfaatkan frekwensi tinggi untuk menghantarkan sebuah komunikasi, maka kerentanan terhadap keamanan juga lebih tinggi dibanding dengan teknologi komunikasi yang lainnya. Berbagai tindakan pengamanan dapat dilakukan melalui perangkat komunikasi yang digunakan oleh user maupun oleh operator yang memberikan layanan komunikasi. Kelemahan jaringan wireless secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan. Secara garis besar, celah pada jaringan wireless terbentang di atas empat layer di mana keempat lapis (*layer*) tersebut sebenarnya merupakan proses dari terjadinya komunikasi data pada media wireless. Keempat lapis tersebut adalah lapis fisik, lapis jaringan, lapis user, dan lapis aplikasi. Model-model penanganan keamanan yang terjadi pada masing-masing lapis pada teknologi wireless tersebut dapat dilakukan antara lain yaitu dengan cara menyembunyikan SSID, memanfaatkan kunci WEP, WPA-PSK atau WPA2-PSK, implementasi fasilitas MAC *filtering*, pemasangan infrastruktur *captive portal*.

Kata kunci : wireless,kelemahan, keamanan, WEP, dan enkripsi.

PENDAHULUAN

Teknologi wireless (tanpa kabel / nirkabel) saat ini berkembang sangat pesat terutama dengan hadirnya perangkat teknologi informasi dan komunikasi. Computer, notebook, PDA, telepon seluler (*handphone*) dan pheripheralnya mendominasi pemakaian teknologi wireless. Penggunaan teknologi wireless yang diimplementasikan dalam suatu jaringan local sering dinamakan WLAN (*wireless Local Area Network*). Namun perkembangan teknologi wireless yang terus berkembang sehingga terdapat istilah yang mendampingi WLAN seperti WMAN (*Metropolitan*), WWAN (*Wide*), dan WPAN (*Personal/Private*).

Dengan adanya teknologi wireless seseorang dapat bergerak atau beraktifitas kemana dan dimanapun untuk melakukan komunikasi data maupun suara. Jaringan wireless merupakan teknologi jaringan komputer tanpa kabel, yaitu menggunakan gelombang berfrekuensi tinggi. Sehingga komputer-komputer itu bisa saling terhubung tanpa menggunakan kabel. Data ditransmisikan di frekuennsi 2.4Ghz (for 802.11b) atau 5Ghz (for 802.11a). Kecepatan maksimumnya 11Mbps (untuk 802.11b) and 54Mbps (untuk 802.11a).

Secara umum, tekonologi wireless dapat dibagi menjadi dua:

a. Berbasis seluler (*cellular-based*), yaitu solusi yang menggunakan saluran komunikasi cellular atau pager yang sudah ada untuk mengirimkan data. Jangkauan dari cellullar-based biasanya cukup jauh. Contoh teknologinya GSM, CDMA, TDMA, CDPD, GPRS/EDGE, 2G, 2.5G, 3G, UMTS
b. Wireless LAN (WLAN): yaitu komunikasi wireless dalam lingkup area yang terbatas, biasanya antara 10 sampai dengan 100 meter dari base station ke Access Point (AP). keluarga IEEE 802.11 (seperti 802.11b, 802.11a, 802.11g), HomeRF, 802.15 (Personal Area Network) yang berbasis Bluetooth, 802.16 (Wireless Metropolitan Area Network)

Pemakaian teknologi wireless secara umum dibagi atas tanpa pengamanan (*nonsecure*) dan dengan pengamanan (*Share Key /secure*). Non Secure (open), yaitu tanpa

menggunakan pengaman, dimana computer yang memiliki pancaran gelombang dapat mendengar transmisi sebuah pancaran gelombang dan langsung masuk kedalam network. Sedangkan *share key*, yaitu alternatif untuk pemakaian kunci atau password. Sebagai contoh, sebuah network yang mengunakan WEP.

MASALAH KEAMANAN WIRELESS

Sistem wireless memiliki permasalahan keamanan secara khusus yang berhubungan dengan wireless. Beberapa hal yang mempengaruhi aspek keamanan dari sistem wireless antara lain:

- Perangkat pengakses informasi yang menggunakan sistem wireless biasanya berukuran kecil sehingga mudah dicuri. Seperti notebook, PDA, handphone, palm, dan sejenisnya sangat mudah dicuri. Jika tercuri maka informasi yang ada di dalamnya (atau kunci pengakses informasi) bisa jatuh ke tangan orang yang tidak berhak.
- Penyadapan pada jalur komunikasi (*man-in-the-middle attack*) dapat dilakukan lebih mudah karena tidak perlu mencari jalur kabel untuk melakukan hubungan. Sistem yang tidak menggunakan pengamanan enkripsi dan otentikasi, atau menggunakan enkripsi yang mudah dipecahkan (kriptanalisis), akan mudah ditangkap.
- Perangkat wireless yang kecil membatasi kemampuan perangkat dari sisi CPU, RAM, kecepatan komunikasi, catu daya. Akibatnya sistem pengamanan (misalnya enkripsi) yang digunakan harus memperhatikan batasan ini. Saat ini tidak memungkinkan untuk menggunakan sistem enkripsi yang canggih yang membutuhkan *CPU cycle* yang cukup tinggi sehingga memperlambat transfer data.
- Pengguna tidak dapat membuat sistem pengaman sendiri (membuat enkripsi sendiri) dan hanya bergantung kepada vendor (pembuat perangkat) tersebut. Namun mulai muncul perangkat handphone yang dapat diprogram oleh pengguna. Begitu juga saat ini notebook sudah menggunakan pengaman otentikasi akses dengan sistem biometric.
- Adanya batasan jangkauan radio dan interferensi menyebabkan ketersediaan servis menjadi terbatas. DoS attack dapat dilakukan dengan menginjeksikan *traffic* palsu.
- Saat ini fokus dari sistem wireless adalah untuk mengirimkan data secepat mungkin. Adanya enkripsi akan memperlambat proses pengiriman data sehingga penggunaan enkripsi masih belum mendapat prioritas. Setelah kecepatan pengiriman data sudah memadai dan harganya menjadi murah, barulah akan melihat perkembangan di sisi pengamanan dengan menggunakan enkripsi.

KELEMAHAN DAN CELAH KEAMANAN WIRELESS

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. Sering ditemukan wireless yang dipasang pada jaringan masih menggunakan setting default bawaan vendor seperti SSID, IPAddress , remote manajemen, DHCP enable, kanal frekuensi, tanpa enkripsi bahkan user (password) untuk administrasi wireless tersebut.

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.

Secara garis besar, celah pada jaringan wireless terbentang di atas empat layer di mana keempat layer tersebut sebenarnya merupakan proses dari terjadinya komunikasi data pada

media wireless. Jadi sebenarnya, pada setiap layer proses komunikasi melalui media wireless terdapat celah-celah yang menunggu untuk dimasuki. Maka itu, keamanan jaringan wireless menjadi begitu lemah dan perlu dicermati dengan ekstra teliti. Layer-layer beserta kelemahannya tersebut adalah sebagai berikut:

a. **Physical Layer.** Seperti diketahui, Physical layer (layer fisik) dari komunikasi data akan banyak berbicara seputar media pembawa data itu sendiri. Di dalam sistem komunikasi data wireless, yang menjadi media perantaranya tidak lain adalah udara bebas. Di dalam udara bebas tersebut, data yang berwujud sinyal-sinyal radio dalam frekuensi tertentu lalu-lalang dengan bebasnya. tentu sudah bisa dibayangkan bagaimana rentannya keamanan data tersebut karena lalu-lalang di alam bebas. Siapa saja mungkin bisa menangkapnya, menyadapnya, bahkan langsung membacanya tanpa sepengetahuan. Jika hanya untuk penggunaan pribadi yang sekadar iseng-iseng saja, disadap atau dibaca oleh orang lain tentu tidak akan terlalu berbahaya meskipun agak menjengkelkan juga. Namun, bagaimana jika kelemahan-kelemahan ini terdapat pada jaringan wireless perusahaan yang didalamnya terdapat berbagai transaksi bisnis, proyek-proyek perusahaan, info-info rahasia, rahasia keuangan, dan banyak lagi informasi sensitif di dalamnya. Tentu penyadapan tidak dapat ditoleransi lagi kalau tidak mau perusahaan menjadi bulan-bulanan orang.

b. **Network Layer.** Network layer (layer jaringan) biasanya akan banyak berbicara seputar perangkat-perangkat yang memiliki kemampuan untuk menciptakan sebuah jaringan komunikasi yang disertai juga dengan sistem pengalamatannya. Pada jaringan komunikasi wireless, perangkat yang biasa digunakan sering disebut dengan istilah Access Point atau disingkat AP. Sistem pengalamatan IP tentu akan banyak ditemukan pada perangkat ini. Karena melayani komunikasi menggunakan media bebas yang terbuka, maka AP-AP tersebut juga dapat dikatakan sebagai perangkat yang terbuka bebas.Perangkat jaringan yang tidak diverifikasi dan dikontrol dengan baik akan dapat menjadi sebuah pintu masuk bagi para pengacau. Mulai dari hanya sekadar dilihat-lihat isinya, diubah sedikit-sedikit, sampai dibajak penuh pun sangat mungkin dialami oleh sebuah AP. Untuk itu, perlu diperhatikan juga keamanan AP-AP pada jaringan wireless yang ada. Selain itu, komunikasi antar-AP juga harus dicermati dan perhatikan keamanannya.

c. **User Layer.** Selain keamanan perangkat jaringan yang perlu diperhatikan, juga perlu diperhatikan dan dicermati siapa-siapa saja yang mengakses jaringan wireless yang ada. Jaringan wireless memang menggunakan media publik untuk lalu-lintas datanya, namun jika jaringan yang ada bukan merupakan jaringan publik yang dapat diakses oleh siapa saja, tentu harus ada batasan-batasan pengaksesnya. Tidak sulit bagi para pengguna yang tidak berhak untuk dapat mengakses sebuah jaringan wireless. Jika sembarangan pengguna dapat menggunakan jaringan yang ada, tentu hal ini akan sangat merugikan para pengguna lain yang memang berhak. Sebuah jaringan wireless yang baik harus memiliki kepastian bahwa hanya para pengguna yang dikenal, yang dipercaya, dan yang memang berhak yang dapat mengakses jaringan tersebut. Perangkat-perangkat jaringan yang biasa bergabung dalam jaringan wireless tersebut juga harus dapat di-track dan dimonitor dengan benar, karena hal ini akan sangat berguna untuk kepentingan monitoring, accounting, untuk mengetahui tren-tren yang terjadi dalam jaringan yang ada, dan banyak lagi.

d. **Application Layer.** Jaringan yang menggunakan media kabel saja dapat membuka celah-celah yang ada pada aplikasi dengan cukup lebar, apalagi jaringan wireless yang memang rentan di seluruh layer-nya. Aplikasi-aplikasi bisnis yang penggunaannya lalu-lalang melalui media wireless tentu sangat rentan keamanannya, baik sekadar disusupi maupun di DoS (Denial of Service). Untuk itu, jaringan wireless yang baik harus juga dapat melindungi aplikasi-aplikasi yang

berjalan di dalamnya agar tidak dengan mudah dikacaukan.

Melihat kelemahan-kelemahan dan celah seperti pada penjelasan di atas, tentu dapat digambarkan begitu banyaknya jalan untuk dapat menyusup ke dalam jaringan wireless. Tidak hanya dari satu layer saja, melainkan keempat layer tersebut di atas dapat menjadi sebuah jalan untuk mengacaukan jaringan yang ada. Mengatur, memantau, dan mengamankan jaringan wireless menjadi berlipat-lipat kesulitannya dibandingkan dengan media wire. Untuk itu, seharusnya perlu dikenali celah-celah apa saja yang ada pada jaringan wireless pada umumnya. Lebih baik lagi jika mengenali kelemahannya mulai dari layer yang paling bawah sampai dengan layer aplikasinya.

Berikut ini adalah beberapa celah yang sangat umum terdapat di dalam sebuah jaringan wireless mulai dari layer yang paling bawah:

a. **Physical Layer**

- **Bleeding Coverage Area**. Seperti diketahui, sinyal radio yang dipancarkan oleh *Access Point* (AP) berpropagasi dalam berbentuk tiga dimensi, memiliki panjang jangkauan, lebar jangkauan, dan tinggi jangkauan. Sinyal radio cukup sulit untuk diketahui dan diprediksi area-area mana saja yang dapat dijangkaunya. Melihat hal ini, sangatlah mungkin bagi sebuah jaringan wireless untuk dapat melebarkan jangkauannya di luar dari batasan-batasan fisik yang dibutuhkan. Misalnya, memasang sebuah AP di ruangan kantor untuk meng-cover seluruh ruangan kantor, namun kenyataannya kantor tetangga yang berada tepat di sebelah, juga masih dapat menggunakan jaringan wireless ini. Inilah yang disebut dengan bleeding coverage area. Dengan adanya coverage area yang tidak diinginkan ini, resource-resource sensitif perusahaan akan sangat berpotensial untuk dieksploitasi oleh orang-orang luar dengan perangkat wireless-nya. Bahkan ada juga beberapa orang yang dengan sengaja mencari-cari bleeding coverage area ini untuk digunakan dan dieksploitasi. Apa yang dilakukan oleh orang-orang ini sering disebut dengan istilah war driving.
- **AP External Pengacau** . Para pengguna yang memiliki perangkat wireless di PC, notebook, PDA, ponsel, dan banyak lagi, memiliki kemungkinan untuk berasosiasi dengan AP manapun selama AP tersebut memang meng-cover lokasi di mana perangkat tersebut berada dan juga memberikan izin. Jika berada di kantor, tentunya harus terkoneksi ke dalam jaringan wireless yang dipancarkan oleh AP yang telah ditentukan oleh kantor tersebut. Namun, apa jadinya jika ada sebuah AP milik orang lain yang area coverage-nya juga menjangkau perangkat yang ada. Kemudian perangkat yang ada tersebut tanpa atau dengan disadari berasosiasi dengan external AP tersebut. Apa yang akan terjadi? Tentunya akan terkoneksi ke dalam jaringan external tersebut yang tidak ketahui ada apa di balik jaringan tersebut. Dari segi keamanan, hal ini sangat berbahaya karena mungkin tanpa disadari memberikan data sensitif, misalnya password-password otentikasi yang sebenarnya harus diketikkan di dalam jaringan wireless yang sesungguhnya. Atau mungkin saja ketika sudah terkoneksi ke dalam jaringan wireless external tersebut, perangkat yang ada akan segera dieksploitasi dan data dicuri. Atau mungkin juga jaringan tersebut memberikan koneksi Internet untuk digunakan, namun dengan dilengkapi packet sniffer dan penyadap-penyadap canggih lainnya sehingga semua transaksi Internet dapat diketahui oleh orang lain. Jika sudah berada dalam kondisi ini, sudah dapat dikatakan sebagai korban pencurian yang tanpa disadari masuk sendiri ke dalam sarang pencuri. Atau mungkin juga jaringan tersebut memberikan koneksi Internet untuk digunakan, namun dengan dilengkapi packet sniffer dan penyadap-penyadap canggih lainnya sehingga semua transaksi internet dapat diketahui oleh orang lain. Selain itu, adanya AP

external yang area coverage-nya masuk ke dalam area tentu juga dapat menyebabkan interferensi terhadap sinyal-sinyal komunikasi jaringan yang ada. Interferensi ini tentu akan sangat mempengaruhi performa dan kelangsungan jaringan wirelss ini.

b. **Network Layer**

- **Rogue AP**. "Rogue AP", maksud dari kata ini adalah ditujukan untuk AP-AP yang tidak diketahui atau tidak terdaftar keberadaannya oleh para administrator sebuah jaringan wireless. Atau mungkin bisa juga disebut dengan istilah AP liar. AP-AP liar ini sangat berbahaya sekali bagi keamanan jaringan wireless karena AP-AP ini memang tidak pernah diinginkan keberadaannya. Selain mengganggu keamanan, tentu juga bisa mengganggu sinyal-sinyal pembawa data pada frekuensi tertentu. Biasanya keberadaan AP liar cukup sulit untuk dicegah karena ketidakpastian area yang dijangkau oleh sebuah jaringan wireless, apalagi untuk yang berskala besar. Secara umum, ada dua sumber yang dapat membuat rogue AP muncul di dalam jaringan wireless yang ada:

  1. Operator atau karyawan yang tidak melakukan operasi secara prosedural. Untuk alasan memudahkan pekerjaannya atau untuk penggunaan pribadi, seringkali terjadi di mana seorang karyawan diam-diam memasang sebuah AP untuk dapat terkoneksi ke dalam jaringan internal. Sehingga ia bisa mendapatkan koneksi ke dalam jaringan dari mana saja di sekitarnya. Kebanyakan AP yang digunakan oleh perorangan ini merupakan AP kelas konsumer di mana fitur-fitur sekuritinya tidak lengkap atau bahkan tidak ada. Bisa juga jika memang ada, tidak di-setting dengan benar atau tidak sesuai dengan standar karena ketidaktahuannya. Padahal seluruh AP sudah diamankan oleh para administrator dengan standar-standar yang berlaku di perusahaan tersebut. Dengan adanya AP "bandel" ini, maka terbukalah sebuah gerbang di mana orang-orang dari luar dapat masuk ke dalam jaringan dengan begitu mudahnya. Mereka memiliki hak akses dan kemampuan yang sama dalam memanfaatkan sumber-sumber di dalam jaringan.
  2. Hacker. Selain karyawan, para hacker yang dengan sengaja meninggalkan perangkat AP nya di dalam jaringan kantor juga bisa terjadi. Jika di kantor memang disediakan port-port ethernet yang dapat digunakan untuk umum, maka ini juga perlu diwaspadai karena mungkin saja para hacker diam-diam menancapkan AP-nya dan kemudian menyembunyikannya, sehingga ia masih dapat mengakses jaringan wireless meskipun secara fisik ia sudah meninggalkan ruangan.

- **Fake AP** . Fake AP atau arti secara harafiahnya AP palsu, merupakan sebuah teknik pencurian hak akses oleh sebuah AP untuk dapat tergabung ke dalam sebuah jaringan wireless dan ikut melayani para penggunanya. Tidak hanya melayani penggunanya, AP-AP lain juga mungkin akan berasosiasi dengan AP ini. Hal ini disebabkan karena mungkin pemilik AP palsu tersebut berhasil mendapatkan SSID dari jaringan wireless tersebut dan menggunakan AP-nya untuk mem-broadcast SSID itu. Sehingga pengguna akan melihat SSID yang sama baik dari AP yang sebenarnya maupun dari AP yang palsu. Jika pengguna tersebut tergabung dalam jaringan AP yang palsu, maka datanya akan dengan mudah dapat dicuri. Lebih parahnya lagi, jika AP ini juga memiliki kemampuan memalsukan alamat MAC dari sebuah AP sebenarnya yang ada di dalam jaringan tersebut. Dengan MAC yang disamakan dengan MAC dari AP

sebenarnya, AP palsu akan dikenal sebagai AP yang memang telah diotorisasi di dalam jaringan tersebut. Akibatnya AP palsu tersebut dapat juga berasosiasi dengan AP-AP lain dan diperlakukan seperti halnya AP yang sebenarnya. Ini akan sangat berbahaya karena informasi login, otentikasi, dan banyak lagi dapat diambil oleh pengguna AP palsu ini. Bahkan jika bisa berasosiasi dengan AP lainnya, lebih banyak lagi yang dapat dilakukan.

MODEL PENANGANAN

Dengan adanya kelemahan dan celah keamanan seperti diatas, beberapa kegiatan dan aktifitas yang dapat dilakukan untuk mengamankan jaringan wireless antara lain:

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 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. **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* (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. **Menggunakan kunci WPA-PSK atau WPA2-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 serangan wireless menggunakan WPA-PSK, gunakanlah *passphrase* yang cukup panjang (satu kalimat). Tools yang sangat terkenal digunakan melakukan serangan ini adalah CoWPAtty dan aircrack. Tools ini memerlukan daftar kata atau *wordlist*, dapat di ambil dari http://wordlist.sourceforge.net/.
4. **Memanfaatkan Fasilitas 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. Masih sering ditemukan wifi di perkantoran dan bahkan ISP (yang biasanya digunakan oleh warnet-warnet) yang hanya menggunakan proteksi MAC Filtering. Dengan menggunakan aplikasi wardriving seperti kismet/kisMAC atau aircrack tools, dapat diperoleh informasi MAC address tiap client yang sedang terhubung ke sebuah Access Point. Setelah mendapatkan informasi tersebut, dapat terhubung ke Access point dengan mengubah MAC sesuai dengan client tadi. Pada jaringan wireless, duplikasi MAC address tidak mengakibatkan konflik. Hanya membutuhkan IP yang berbeda dengan client yang tadi.
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)

Cara-cara diatas lebih lengkapnya dapat dijelaskan sebagai berikut :

1. **Memakai Enkripsi**. Enkripsi adalah ukuran security yang pertama, tetapi banyak wireless access points (WAPs) tidak menggunakan enkripsi sebagai defaultnya. Meskipun banyak WAP telah memiliki Wired Equivalent Privacy (WEP) protocol, tetapi secara default tidak diaktifkan. WEP memang mempunyai beberapa lubang di securitynya, dan seorang hacker yang berpengalaman pasti dapat membukanya, tetapi itu masih tetap lebih baik daripada tidak ada enkripsi sama sekali. Pastikan untuk men-set metode WEP authentication dengan "shared key" daripada "open system". Untuk "open system", dia tidak meng-encrypt data, tetapi hanya melakukan otentifikasi client. Ubah WEP key sesering mungkin, dan pakai 128-bit WEP dibandingkan dengan yang 40-bit.
2. **Gunakan Enkripsi yang Kuat**. Karena kelemahan kelemahan yang ada di WEP, maka dianjurkan untuk menggunakan Wi-Fi Protected Access (WPA) juga. Untuk memakai WPA, WAP harus men-

supportnya. Sisi client juga harus dapat men-support WPA tsb.

3. **Ganti Default Password Administrator**. Kebanyakan pabrik menggunakan password administrasi yang sama untuk semua WAP produk mereka. Default password tersebut umumnya sudah diketahui oleh para hacker, yang nantinya dapat menggunakannya untuk merubah setting di WAP. Hal pertama yang harus dilakukan dalam konfigurasi WAP adalah mengganti password default tsb. Gunakan paling tidak 8 karakter, kombinasi antara huruf dan angka, dan tidak menggunakan kata kata yang ada dalam kamus.
4. **Matikan SSID Broadcasting**. Service Set Identifier (SSID) adalah nama dari wireless network. Secara default, SSID dari WAP akan di broadcast. Hal ini akan membuat user mudah untuk menemukan network tsb, karena SSID akan muncul dalam daftar available networks yang ada pada wireless client. Jika SSID dimatikan, user harus mengetahui lebih dahulu SSID-nya agak dapat terkoneksi dengan network tsb.
5. **Matikan WAP Saat Tidak Dipakai**. Cara yang satu ini kelihatannya sangat simpel, tetapi beberapa perusahaan atau individual melakukannya. Jika mempunyai user yang hanya terkoneksi pada saat saat tertentu saja, tidak ada alasan untuk menjalankan wireless network setiap saat dan menyediakan kesempatan bagi intruder untuk melaksanakan niat jahatnya. Access point dapat dimatikan pada saat tidak dipakai.
6. **Ubah default SSID**. Pabrik menyediakan default SSID. Kegunaan dari mematikan broadcast SSID adalah untuk mencegah orang lain tahu nama dari network, tetapi jika masih memakai default SSID, tidak akan sulit untuk menerka SSID dari network.
7. **Memakai MAC Filtering**. Kebanyakan WAP (bukan yang murah murah tentunya) akan memperbolehkan memakai filter media access control (MAC). Ini artinya dapat membuat "white list" dari computer computer yang boleh mengakses wireless network, berdasarkan dari MAC atau alamat fisik yang ada di network card masing masing pc. Koneksi dari MAC yang tidak ada dalam list akan ditolak. Metode ini tidak selamanya aman, karena masih mungkin bagi seorang hacker melakukan sniffing paket yang transmit via wireless network dan mendapatkan MAC address yang valid dari salah satu user, dan kemudian menggunakannya untuk melakukan spoof. Tetapi MAC filtering akan membuat kesulitan seorang intruder yang masih belum jago jago banget.
8. **Mengisolasi Wireless Network dari LAN**. Untuk memproteksi internal network kabel dari ancaman yang datang dari wireless network, perlu kiranya dibuat wireless DMZ atau perimeter network yang mengisolasi dari LAN. Artinya adalah memasang firewall antara wireless network dan LAN. Dan untuk wireless client yang membutuhkan akses ke internal network, dia haruslah melakukan otentifikasi dahulu dengan RAS server atau menggunakan VPN. Hal ini menyediakan extra layer untuk proteksi.
9. **Mengontrol Signal Wireless**. 802.11b WAP memancarkan gelombang sampai dengan kira kira 300 feet. Tetapi jarak ini dapat ditambahkan dengan cara mengganti antenna dengan yang lebih bagus. Dengan memakai high gain antena, bisa mendapatkan jarak yang lebih jauh. Directional antenna akan memancarkan sinyal ke arah tertentu, dan pancarannya tidak melingkar seperti yang terjadi di antenna omnidirectional yang biasanya terdapat pada paket WAP setandard. Selain itu, dengan memilih antena yang sesuai, dapat mengontrol jarak sinyal dan arahnya untuk melindungi diri dari intruder. Sebagai tambahan, ada beberapa WAP yang bisa di setting kekuatan sinyal dan arahnya melalui config WAP tersebut.
10. **Memancarkan Gelombang pada Frequensi yang Berbeda**. Salah satu cara untuk bersembunyi dari hacker yang biasanya memakai teknologi 802.11b/g yang lebih populer adalah dengan memakai 802.11a. Karena 802.11a bekerja pada frekwensi yang berbeda (yaitu di frekwensi

5 GHz), NIC yang di desain untuk bekerja pada teknologi yang populer tidak akan dapat menangkap sinyal tersebut.

KESIMPULAN

Teknologi wireless adalah teknologi yang dapat dimanfaatkan untuk aplikasi teknologi informasi yang berbasis jaringan yang memiliki sifat *mobile*. Oleh karena itu portabilitas dan fleksibilitas adalah kunggulan utama dalam pemakaian teknologi wireless. Pemakaian jalur komunikasi wireless menggunakan teknologi frekwensi tinggi dengan spesifikasi frekwensi tergantung peralatan dan operator yang menyediakannya.

Karena pemakaian frekwensi yang sifatnya lebih terbuka dibanding dengan menggunakan kabel, maka kerentanan keamanan jalur komunikasi akan lebih berbahaya dibanding menggunakan kabel. Kerentanan terjadi hampir pada semua lapis protocol yang dimiliki pada jaringan komunikasi wireless. Untuk itu perlu dilakukan penanganan keamanan yang lebih ekstra pada peralatan komunikasi yang digunakan.

Model-model penanganan keamanan pada pemakaian jalur komunikasi yang menggunakan teknologi wireless antara lain yaitu dengan cara menyembunyikan SSID, memanfaatkan kunci WEP, WPA-PSK atau WPA2-PSK, implementasi fasilitas MAC *filtering*, pemasangan infrastruktur *captive portal*. Model penanganan keamanan tersebut sampai saat ini adalah yang paling umum dan tersedia untuk dapat diimplementasikan guna mengatasi masalah-masalah yang terjadi terhadap ancaman keamanan penggunaan teknologi wireless.

DAFTAR PUSTAKA

1. http://id.wikipedia.net
2. http://www.drizzle.com/aboba/IEEE/rc4_ksaproc.pdf , diakses januari 2006
3. http://www.wikipedia.org
4. Jusua M.S., 2007, http://www.te.ugm.ac.id/~josh/seminar/hacking-wifi-josh.pdf.
5. Network and Security Services, Generate Revenue Growth in 2002, Market Trends, ©2003 Gartner, Inc. and/or its Affiliates. All Rights Reserved.
6. Philipus Bayu MP, 2004, "Sistem Keamanan Bluetooth" ITB Bandung.
7. William Stalings, 1999, "Cryptography and Network Security :Principles and Practice", 2nd Eddition, Prentice Hall, Inc.