Keamanan Jaringan Wireless (Wifi)

Maksudi
Fakultas Teknik, Program Studi Teknik Informatika Universitas Muhammadiyah Cirebon
umaks161203@vahoo.com

Abstrak

Dewasa ini akses wireless data semakin menjadi primadona utama bagi dunia pendidikan, pelaku bisnis dan masyarakat. Teknologi *wireless* sendiri memanfaatkan frekuensi tinggi dalam menghantarkan sebuah komunikasi tanpa kabel, sehingga sangat siginfikan sejalan dengan kebutuhan sistem informasi yang mobil. Banyak penyedia jasa yang memanfaatkan teknologi ini akan tetapi sangat sedikit yang memperhatikan keamanan data yang berpotensi terhadap kerentanan keamanan yang lebih tinggi. Tindakan pencegahan dan keamanan dapat dilakukan melalui perangkat komunikasi yang digunakan oleh *user* maupun penyedia jasa layanan dalam memberikan layanan komunikasi.

Kerentanan pada jaringan *wireless* secara umum dapat terjadi pada 2 jenis, yakni kesalahan pada jenis konfigurasi dan kelemahan pada jenis *enkripsi* yang dipilih. Jaringan *wireless* terbentang di atas empat lapisan *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. Tindakan pengamanan yang dapat dilakukan pada tiap lapis teknologi *wireless* yaitu dengan cara menyembunyikan SSID, memanfaatkan kunci WEP, WPA-PSK atau WPA2-PSK, *filtering* MAC.

Kata kunci: kerentanan, keamanan, *wireless*, enkripsi

A. Pendahuluan

Teknologi wireless (tanpa kabel) dewasa ini menjadi primadona di bandingkan dengan jaringan kabel karena jaringan Wireless lebih praktis dan efisien, apalagi dengan hadirnya perangkat teknologi informasi dan komunikasi. Komputer, laptop, telepon seluler (*handphone*) dan smartphone mendominasi pemakaian teknologi wireless.

Penggunaan teknologi wireless yang diimplementasikan dalam suatu jaringan local sering dinamakan WLAN (Wireless Local Area Network). Sehingga banyak penyedia jasa wireless seperti hotspot komersil, ISP, Warnet, kampus-kampus maupun perkantoran sudah mulai memanfaatkan jaringan wifi .

Dengan adanya teknologi wireless tersebut seseorang dapat bergerak atau beraktifitas kemana dan dimanapun untuk melakukan komunikasi data. Jaringan wireless merupakan teknologi jaringan komputer tanpa kabel, yaitu menggunakan gelombang berfrekuensi tinggi milik umum yang bersifat bebas digunakan oleh semua kalangan dengan batasan-batasan tertentu tergantung area jangkauan dan antenna yang digunakan. Pengguna dapat saling terhubung tanpa menggunakan kabel. Data ditransmisikan di frekuennsi 2.4GHz (802.11b) atau 5GHz (802.11a). Kecepatan maksimumnya 11Mbps (802.11b) and 54Mbps (802.11a).

Secara umum, teknologi wireless dapat digolongkan sebagai berikut:

- Berbasis seluler (*cellular-based*), yaitu solusi yang menggunakan saluran komunikasi *cellular* yang sudah ada dalam mengirimkan data. Jangkauan dari cellullar-based biasanya cukup jauh. Contoh teknologinya GSM, CDMA, TDMA, CDPD, GPRS/EDGE, 2G, 2.5G, 3G, 3.5G, 4G dan UMTS
- 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) dikenal dengan kelompok layer 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) .

Jaringan Wifi memiliki lebih banyak kelemahan dibanding dengan jaringan kabel. Umumnya pengguna sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan wireless tersebut. Hal ini membuat para hacker menjadi tertarik untuk mengexplore kemampuannya untuk melakukan berbagai

aktifitas illegal menggunakan wifi.

Jenis aktivitas dan metode yang dilakukan para hacker wireless ataupun para pemula biasanya dengan melakukan wardriving. Wardriving adalah kegiatan atau aktivitas untuk mendapatkan informasi tentang suatu jaringan wifi dan mendapatkan akses terhadap jaringan wireless tersebut. Tujuan utamanya adalah untuk mendapatkan koneksi internet, tetapi banyak juga yang melakukan hal tertentu mulai dari rasa keingintahuan, coba coba, pengambilan dokumen 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 adalah banyak penyedia jasa menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan wireless yang masih menggunakan konfigurasi wireless settingan default bawaan pabrik.

Wireless yang dipasang pada jaringan masih menggunakan setting default bawaan pabrik seperti SSID, IP Address, DHCP enable, kanal frekuensi, yang tanpa enkripsi pada password maupun user sebagai administrasi wireless akan menimbulkan kerentanan tersendiri terhadap keamanan.

B. Kelemahan Jaringan Wireless

1. Pada laipsan fisik

Pada Lapisan Fisik Wifi menggunakan gelombang radio pada frekwensi milik umum yang bersifat bebas digunakan oleh semua kalangan dengan batasan batasan tertentu. Tidak mudah melakukan pembatasan area yang dijangkau pada wifi.

Hal ini menyebabkan berbagai kemungkinan terjadi pada aktifitas aktifitas, sbb:

- *Interception* atau penyadapan

Hal ini sangat mudah dilakukan, dan sudah tidak asing lagi bagi para hacker. Berbagai tools dengan mudah di peroleh dari internet. Berbagai teknik kriptografi dapat di bongkar oleh tools tools tersebut.

- *Injection*

Pada saat transmisi melalui radio, dimungkinkan dilakukan *injection* karena berbagai kelemahan pada cara kerja wifi dimana tidak ada proses validasi siapa yang sedang terhubung atau siapa yang memutuskan koneksi saat itu.

- *Jamming*

Jamming sangat dimungkinkan terjadi, baik disengaja maupun tidak disengaja karena ketidaktahuan pengguna wireless tersebut. Pengaturan penggunaan kanal frekuensi merupakan keharusan agar jamming dapat dihindari. Jamming terjadi karena frekuensi yang digunakan cukup sempit, penggunaan kembali channel sulit dilakukan pada area yang padat jaringan nirkabelnya.

- *Locating Mobile Nodes*

Dengan berbagai software, setiap orang mampu melakukan *wireless site survey* untuk mendapatkan informasi posisi letak setiap Wifi dengan beragam konfigurasi masing masing. Hal ini dapat dilakukan dengan peralatan sederhana seperti PDA atau laptop dengan yang dukung GPS sebagai penanda posisi.

- *Access Control*

Dalam membangun jaringan wireless perlu di design agar dapat memisahkan node atau host yang dapat dipercaya dan host yang tidak dapat dipercaya. Sehingga adanya *access control* yang baik

- *Hijacking*

Serangan MITM (*Man In The Middle*) dapat terjadi pada wireless, disebabkan berbagai kelemahan protokol yang ada. Memungkinkan terjadinya hijacking atau pengambil alihan komunikasi yang sedang terjadi dan melakukan pencurian atau modifikasi informasi.

2. 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 (Access point) 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. Lapisan data atau MAC juga digunakan dalam otentikasi

dalam implementasi keamanan wifi berbasis WPA Radius (802.1x plus TKIP/AES).

Faktor keamanan teknologi wireless secara umum sudah ada yang menggunakan pengamanan bawaan pabrik (*Share Key /Secure*) juga ada yang belum menggunakan pengamanan (*non secure*). Untuk *share key*, yaitu alternatif pemakaian password/kunci seperti pada jaringan menggunakan WEP, sedangkan *Non Secure*, yaitu tanpa menggunakan keamanan, dimana komputer, laptop, telepon seluler (*handphone)* dan smartphone yang memiliki pacaran gelombang dapat menangkap sinyal transmisi sebuah pancaran gelombang tersebut langsung dapat masuk kedalam jaringan.

C. Keamanan Jaringan Wireless (Wifi)

1. Wired Equivalent Privacy (WEP)

WEP merupakan tipe keamanan jaringan nirkabel di umumkan sebagai standar keamanan Wi-Fi pada bulan September 1999. Sebagai generasi pertama keamanan WEP yang digunakan pada wireless Enkripsi WEP menggunakan kunci 64-bit yang dimasukkan (oleh administrator) ke klien maupun access point. Kondisi ini masih rentan untuk di bobol oleh cracker, hal ini di sebabkan pembatasan Enkripsi yang hanya 64-bit, namun penambahan Enkripsi 128 bit juga tidak membuat tipe keamanan ini menjadi kuat.

Kata sandi pada Enkripsi WEP tersebut harus cocok dengan Access Point yang sudah di setting, sehingga client dapat mengautentikasi kata sandi yang terdapat pada Access Point. Cara kerja WEP adalah Access Point akan menentukan apakah client sudah memasukan kata sandi yang sesuai. Apabila kata sandi tersebut benar, maka Access Point akan merespon positif dan langsung meng-authentikasi client. Namun apabila kata sandi salah, maka Access Point akan merespon negatif dan client tidak akan di beri authentikasi. Dengan demikian, client tidak akan dapat tersambung dengan jaringan.

Alasan Memilih WEP adalah WEP merupakan sistem keamanan yang lemah. Namun WEP dipilih karena telah memenuhi standar dari 802.11 yakni :

- Exportable
- Reasonably strong
- Self-Synchronizing
- Computationally Efficient
- Optional.

Fungsi WEP ini dapat digunakan juga untuk verifikasi identitas pada *authenticating station*.

Kelebihan WEP: - User lebih mudah menggunakan tipe keamanan jaringan ini karena akan secara otomatis masuk ke jaringan dengan hanya memasukan *username* dan *password*.

Kelemahan WEP: - Masalah kata sandi yang lemah, algoritma RC4 yang digunakan dapat di bobol. karena WEP menggunakan kunci yang bersifat statis.

Jenis serangan pada WEP:

- 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 vektor (IV) yang lemah sebanyak-banyaknya. Semakin banyak kelemahan vektor (IV) yang diperoleh, semakin cepat ditemukan kunci yang digunakan.

  (www.drizzle.com/~aboba/IEEE/rc4_ksaproc .pdf)

- Mendapatkan IV yang unik melalui packet data 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 mulai dari chipset, versi

firmware, dan versi driver serta tidak jarang harus melakukan patching terhadap driver dan aplikasinya.

2. Wi-Fi Protected Access (WPA)

WPA merupakan salah satu tipe keamanan jaringan nirkabel yang merupakan pengembangan dari WEP, WPA secara resmi di perkenalkan pada tahun 2003, setahun sebelum WEP resmi tidak di gunakan lagi. konfigurasi WPA yang paling umum adalah WPA-PSK (*Pre-Shared Key*). Enkripsi yang di gunakan oleh WPA adalah 256-bit, WPA mengimplementasikan layer IEEE yaitu Layer 802.11i. WPA di desain untuk menggantikan metode keamanan WEP yang menggunakan kunci keamanan static, WPA menggunakan metode TKIP (*Temporal Key Integrity Protocol*) yang mampu berubah secara dinamis. Protokol TKIP akan mengambil kunci utama sebagai starting point yang kemudian secara reguler berubah sehingga tidak ada kunci enkripsi yang digunakan dua kali. WPA juga menggunakan alat tambahan yaitu PC, Alasannya karena PC berguna sebagai *authentication server* yang akan memberikan kunci berbeda pada masing - masing user.

Kelebihan WPA: - Enkripsi data yang digunakan adalah Temporal Key Integrity Protocol (TKIP). enkripsi yang digunakan masih sama dengan WEP yaitu RC4, karena pada dasarnya WPA ini merupakan perbaikan dari WEP dan bukan suatu level keamanan yang benar – benar baru, walaupun beberapa device ada yang sudah mendukung enkripsi AES yaitu enkripsi dengan keamanan yang paling tinggi.

Kelemahan WPA: - Kelemahan WPA sampai saat ini adalah proses kalkulasi data yang lama. Proses transmisi data akan menjadi lebih lambat di bandingkan jika kita menggunakan protokol WEP tetapi Belum semua wireless mendukung, biasanya butuh upgrade firmware, driver atau bahkan menggunakan software tertentu.

WPAPSK dan LEAP yang dianggap menjadi solusi menggantikan WEP, saat ini juga sudah dapat dipecahkan dengan metode dictionary attack secara offline. dengan menggunakan mencoba-coba banyak kata dari suatu kamus. Serangan ini akan berhasil jika passphrase yang digunakan wireless tersebut memang terdapat pada kamus kata yang digunakan si hacker.

3. Service Set Identifier (SSID)

SSID berfungsi untuk memberikan nama sebuah jaringan wireless yang dipancarkan dari sebuah AP (Access point). Sistem penamaan ini adalah sistem kontrol pertama sebuah jaringan wireless. dengan diberikannya sebuah nama, maka penguna yang bergabung dalam jaringan tersebut harus mengetahui nama SSID nya terlebih dahulu. Jika nama yang dimasukkan oleh klien penguna sama dengan nama yang ada di AP maka jaringan wireless tersebut baru dapat diakses. Jika tidak, maka pengguna tidak akan mendapatkan akses dalam jaringan tersebut meskipun sinyalnya bisa tertangkap. Sistem penamaan SSID dapat diberikan maksimal sebesar 32 karakter. Karakter-karakter tersebut juga dibuat case sensitive sehingga SSID dapat lebih banyak variasinya.

Biasanya SSID untuk tiap wireless access point berbeda-beda. Untuk keamanan jaringan wireless bisa juga SSID nya di hidden sehingga user dengan wireless card tidak bisa mendeteksi keberadaan jaringan wireless kita, ini sebagai antisipasi untuk mengurangi risiko di hack oleh pihak yang tidak bertanggung jawab.

Kelebihan SSID: - Dapat memberikan nama berbeda untuk setiap access poin (AP), Karakter-karakter penamaan dapat dibuat case sensitive sehingga SSID lebih banyak variasinya.

Kelemahan SSID: - Penyembunyikan Services Set Id (SSID) pada jaringan wireless 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 dan masih bisa diteksi oleh penggunaan tools-tools yang ada.

Jenis serangan pada SSID:

- Pada saat-saat tertentu atau saat client akan terhubung (*assosiate*) maupun ketika akan memutuskan diri (*deauthentication*) dari sebuah jaringan wireless, maka client akan tetap mengirimkan SSID dalam bentuk plaintext (walaupun sudah menggunakan enkripsi), sehingga dapat melakukan penyadapan dengan mudah untuk menemukan informasi tersebut. Beberapa tools juga dapat digunakan untuk mendapatkan SSID yang dihidden antara lain, kismet

(kisMAC), SSIDjack (airjack), aircrack, void11 dan masih banyak lagi.

- Pada saat 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 networks yang ada pada wireless client. Jika SSID dimatikan, user harus mengetahui lebih dahulu SSID nya agar dapat terkoneksi dengan network tsb.

Pencegahan: - Ubah setting default SSID. Bawaan pabrik menyediakan default SSID.; Mematikan SSID broadcasting, kegunaannya adalah untuk mencegah orang lain tahu nama dari network, tetapi jika masih memakai default SSID, tidak akan sulit untuk menerka SSID dari network.

D. Penutup

Penggunaan wireless LAN dengan konfigurasi default akan memudahkan para penyusup memanfaatkan jaringan tersebut secara ilegal. Konfigurasi default bawaan pabrik perangkat wireless sebaiknya dirubah sesuai kebutuhan sehingga keamanan akses jaringan wireless (wifi) dapat terjaga dengan baik.

Metode pengamanan jaringan Wireless dapat dilakukan dengan berbagai teknik, uraian diatas sebagai salah satu teknik yang umum dilakukan, untuk lebih menjamin keamanan tidak ada salahnya jika mengkombinasikan beberapa teknik ada dan sudah diuraikan di atas.

E. Daftar Pustaka

[1] Dony A. *Computer Security*. Andi Yogyakarta. November 2005

[2] Gunadi DH, *Wifi (Wireless LAN), Jaringan Komputer Tanpa Kabel*. Informatika Bandung. Oktober 2009

[3] Janner Simarmata, Keamanan Jaringan. Materi kuliah, 2005

[4] William Stalings.*Cryptography and Network Security : Principles and Practice, 2nd Edditio*n. Prentice Hall, Inc..1999.

[5] https://www.delhendro.com/2014/12/jenis-keamanan-pada-jaringan-wireless.html

[6] http://routekno.blogspot.co.id/2016/02/jenis-jenis-keamanan-pada-jaringan.html