Sistem Keamanan Jaringan NIRKABEL

Jutono Gondohanindijo
Fakultas Ilmu Komputer Universitas AKI

Abstract

The development of IT wireless network helps computer users much in connecting to the Internet by using a wave medium.

The security of the Wi-Fi network has many weaknesses. Many wireless service providers such as commercial hotspots, ISP, internet cafes, colleges, and offices use the wireless network, but they have very little attention to the security of data communication in the wireless network.

The modus that the wireless hackers do in breaking into the security system is wardriving. Wardriving is an activity to get information about a wireless network and get access to the wireless network that aim to get an internet connection. But on the contrary wardriving is also done for certain purposes, such as curiosity, trial and error, research, practical tasks, crime and others.

***Keywords** : Wireless, Network, Security, Crime, Hacker*

1. Pendahuluan

Perkembangan internet sangat cepat sekali dan penggunaannya sudah menyebar di berbagai pelosok belahan bumi baik yang menggunakan jaringan kabel maupun yang jaringan nirkabel (Jaringan Wifi). Namun Jaringan Wifi memiliki lebih banyak kelemahan dibanding dengan jaringan kabel, namun saat ini perkembangan teknologi wifi sangat signifikan sejalan dengan kebutuhan sistem informasi yang mobile.

Teknologi wireless menggunakan transmisi frekwensi radio sebagai alat untuk mengirimkan data, sedangkan teknologi kabel menggunakan kabel. Teknologi wireless berkisar dari sistem komplek seperti Wireless Local Area Network (WLAN) dan telepon selular hingga peralatan sederhana seperti headphone wireless, microphone wireless dan peralatan lain yang tidak memproses atau menyimpan informasi. Penggunaan penyedia jasa wireless antara lain ISP, Warnet, hotspot komersil,

kampus-kampus maupun perkantoran sudah banyak yang memanfaatkan wifi pada jaringan masing masing, tetapi sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan wireless tersebut. Oleh karena itu banyak hacker yang tertarik untuk mengexplore keamampuannya dalam melakukan berbagai aktifitas yang biasanya ilegal menggunakan wifi.

Kelemahan jaringan wireless terletak pada kelemahan pada konfigurasi dan jenis enkripsi yang digunakan. Dengan kemudahan dalam mengkonfigurasi sebuah jaringan wireless, tambah dengan banyaknya vendor yang menyediakan fasilitas yang memudahkan pengguna atau admin jaringan sehingga sering ditemukan wireless yang masih menggunakan konfigurasi wireless default bawaan vendor seperti SSID, IP Address , remote manajemen, DHCP enable, kanal frekuensi, tanpa enkripsi bahkan user/password untuk administrasi wireless tersebut.

1.1 Jaringan Komputer

Dahulu komputer lebih dianggap sebagai sebuah kemewahan daripada sebuah kebutuhan. Hanya orang-orang kaya dan beruntung saja yang dapat mempunyai sebuah komputer, sedangkan jaringan merupakan hal yang hanya dapat disediakan untuk perusahaan besar.

Jaringan komputer adalah sebuah kumpulan komputer, printer, dan peralatan lainnya yang terhubung dalam satu-kesatuan. Informasi dan data bergerak melalui kabel-kabel, atau tanpa kabel, sehingga memungkinkn pengguna jaringan komputer dapat saling bertukar dokumen dan data, mencetak pada printer yang sama, dan bersama-sama menggunakan hardware/software yang terhubung dengan jaringan (Herwindo, 2005:100).

LAN merupakan jaringan pribadi di dalam sebuah gedung atau kampus berukuran sampai 10 Km. LAN sering digunakan untuk menghubungkan komputer-komputer pribadi dan workstation dalam kantor perusahaan atau pabrik-pabrik untuk pemakaian resource bersama misalnya printer (Tanenbaum, 2008).

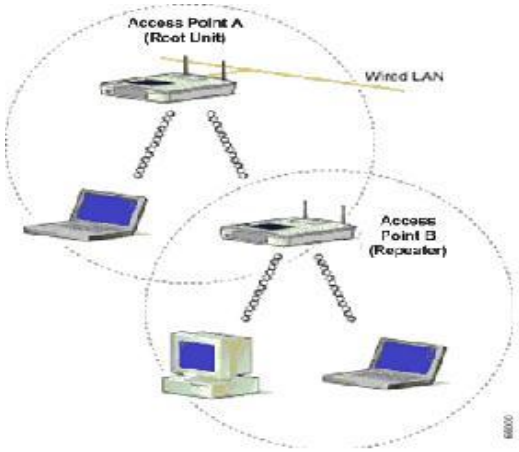
LAN mempunyai ukuran yang terbatas, yang berarti bahwa suatu transmisi pada keadaan terburuknya terbatas dan dapat diketahui sebelumnya. Dengan mengetahui keterbatasannya menyebabkan adanya kemungkinan untuk menggunakan jenis desain tertentu. Hal ini juga memudahkan manajemen jaringan. Terdapat beberapa

topologi yang dapat digunakan pada LAN, pada LAN konvensional topologi yang digunakan yaitu topologi Bintang, Cincin, Pohon, Lengkap, Cincin berinteraksi.

Sejalan dengan kemajuan yang pesat pada dekade ini, maka sekarang setiap orang masing-masing dapat mempunyai komputernya sendiri. Seperti yang banyak kita temui, biasanya setiap orang tua mempunyai komputernya sendiri, begitu pula dengan si anak dapat mempunyai komputernya sendiri walaupun mungkin hanya digunakan untuk bermain dan mengerjakan tugas-tugas sekolah. Para pengguna rumahan juga telah berkembang dari yang semula tidak mempunyai akses Internet, kemudian mulai memakai koneksi dial-up Internet dengan kecepatan 9600 kbps melebihi 56 kbps dial up akses, dan kini berkembang menjadi koneksi broadband menyaingi koneksi T1 yang sering dinikmati orang saat bekerja.

Sebagaimana Internet dan World Wide Web telah menjadi trend dalam kebudayaan kita dan menggantikan format media massa lainnya dalam menyampaikan informasi yang dicari, mulai dari informasi pemberitaan, olahraga, cuaca, resep, yellow pages (buku telepon), dan masih banyak hal lainnya yang kesemuanya itu merupakan sebuah cara baru, bukan hanya dalam pemakaian komputer di dalam rumah, tapi juga dalam hal pemakaian koneksi Internet.

Sementara itu perusahaan perangkat keras maupun perangkat lunak kini telah menawarkan berbagai solusi yang memungkinkan para pemakai Internet di rumah saling berbagi koneksi antara lebih dari dua komputer. Meskipun semua komputer tersebut harus terhubung jaringan.



Gambar 1. Wireless LAN

Untuk menghubungkan satu komputer dengan komputer yang lainnya biasanya membutuhkan berbagai macam media fisik, seperti kabel telepon, kabel coaxial, ataupun kabel CAT5 kabel telegram yang ada di mana-mana. Namun baru-baru ini telah ditemukan cara baru pemakaian Internet tanpa menggunakan berbagai macam

media penghubung tersebut, teknologi ini kini lazim disebut koneksi jaringan Nirkabel (tanpa kabel). Pemakaian Internet dengan menggunakan koneksi jaringan nirkabel ini tentu saja sangat memudahkan pemakainya dalam mengakses Internet, tanpa melalui proses instalasi dan pemasangan kabel yang memusingkan.

Adapun susunan koneksi jaringan nirkabel ini sangat sederhana. Koneksi Internet masuk dari Internet Provider kemudian dihubungkan dengan suatu titik penerus akses nirkabel atau router yang memancarkan sinyal. Ketika Anda terhubung dengan memakai kartu atau antena jaringan nirkabel untuk menerima sinyal, begitu pula sebaliknya, maka koneksi Anda telah berhasil.

Jaringan tanpa kabel sebenarnya tidak sesulit sistem cable network bahkan lebih mudah. Sistem jaringan WIFI atau Wireless tidak memerlukan penghubung cable network antar komputer . Bila jenis coax atau UTP cable memerlukan kabel sebagai media tranfer, dengan Wireless network hanya dibutuhkan ruang atau space dimana jarak jangkau network dibatasi kekuatan pancaran signal radio dari masing masing komputer .

Keuntungan dari sistem WIFI , pemakai tidak dibatasi ruang gerak dan hanya dibatasi pada jarak jangkauan dari satu titik pemancar WIFI. Untuk jarak pada sistem WIFI mampu menjangkau area 100 feet atau 30M radius. Selain itu dapat diperkuat dengan perangkat khusus seperti booster yang berfungsi sebagai relay yang mampu menjangkau ratusan bahkan beberapa kilometer ke satu arah (directional). Bahkan hardware terbaru, terdapat perangkat dimana satu perangkat Access Point dapat saling merelay (disebut bridge) kembali ke beberapa bagian atau titik sehingga memperjauh jarak jangkauan dan dapat disebar dibeberapa titik dalam suatu ruangan untuk menyatukan sebuah network LAN.

Sebelumnya, perlu diketahui bahwa ada 2 cara menghubungkan antar PC dengan sistem Wireless yaitu Adhoc dimana 1 PC terhubung dengan 1 PC dengan saling terhubung berdasarkan nama SSID (Service Set IDentifier). SSID sendiri tidak lain nama sebuah komputer yang memiliki card USB atau perangkat wireless dan masing masing perangkat harus diberikan sebuah nama tersendiri sebagai identitas.

Kedua jaringan paling umum dan lebih mudah saat ini dengan sistem Access point dengan bentuk PCI card atau sebuah unit hardware yang memiliki fungsi Access point untuk melakukan broadcast ke beberapa komputer client pada jarak radius tertentu.

1.2. Teknologi Keamanan Jaringan

1. 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 seperti 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, kita 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 setiap clientnya.

Pemfilteran MAC address merupakan pemfilteran di atas standar 802.11b untuk mengamankan jaringan. Dalam hal ini setiap MAC address client memiliki alamat fisik yang pasti berbeda untuk setiap cardnya. Cara kerja sistem ini yaitu mendaftarkan alamat MAC addressnya agar mendapat otorisasi dari Access Point saat akan berasosiasi.

2. WEP (Wired Equivalent Privacy)

WEP merupakan standar keamanan dan 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 Access 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, Access Point akan melakukan decrypt terhadap respon enkripsi dari client untuk melakukan verifikasi bahwa text challenge dienkripsi dengan menggunakan WEP key 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.

Komunikasi Data via IEEE 802.11 (Gunawan, Arief Hamdani dan Andi Putra, 2003) dengan Shared Key Authentication kelihatannya lebih aman dari dari pada Open System Authentication, namun pada kenyataannya tidak. Shared Key malah membuka pintu bagi penyusup atau cracker. Penting untuk dimengerti dua jalan yang digunakan oleh WEP. WEP bisa digunakan untuk memverifikasi identitas client selama proses shared key dari authentikasi, tapi juga bisa digunakan untuk men-dekripsi data yang dikirimkan oleh client melalui Access Point.

WEP memiliki berbagai kelemahan antara lain :

a. Masalah kunci yang lemah, algoritma RC4 yang digunakan dapat dipecahkan.
b. WEP menggunakan kunci yang bersifat statis
c. Masalah *initialization vector* (IV) WEP
d. 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 24 bit merupakan Inisialisasi Vektor (IV). Demikian juga pada kunci WEP 128

bit, kunci rahasia terdiri dari 104 bit. Serangan-serangan pada kelemahan WEP antara lain :

1. 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.
2. Mendapatkan IV yang unik melalui paket data yang diperoleh untuk diolah untuk proses cracking kunci WEP dengan lebih cepat. Cara ini disebut chopping attack, pertama kali ditemukan oleh Hikari. Teknik ini hanya membutuhkan IV yang unik sehingga mengurangi kebutuhan IV yang lemah dalam melakukan cracking WEP.
3. Kedua serangan diatas membutuhkan waktu dan paket 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. 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 digunakan wireless tersebut memang terdapat pada kamus kata yang digunakan si hacker. Untuk mencegah adanya serangan terhadap keamanan wireless menggunakan WPA-PSK, gunakanlah passphrase yang cukup panjang (satu kalimat).

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 user 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 proses secara otomatis dilakukan tanpa diketahui oleh user. 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 user jaringan wireless seperti tidak menemui jawaban dari dokumen standar yang dicari. Masalah yang berhubungan dengan throughput sangatlah bergantung pada hardware yang dimiliki, secara lebih spesifik adalah chipset yang digunakan.

Proses otentifikasi WPA menggunakan 802.1x dan EAP (Extensible Authentication Protocol). Secara bersamaan, implementasi tersebut akan menyediakan kerangka kerja yang kokoh pada proses otentifikasi user. Kerangka-kerja tersebut akan melakukan utilisasi sebuah server otentifikasi terpusat, seperti RADIUS, untuk melakukan otentifikasi user 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) akan diadopsi WPA dengan mekanisme otentifikasi user. 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, user 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. Pada jaringan wireless yang membutuhkan tingkat sekuriti tingkat tinggi, variasi sistem tambahan proprietari dibuat untuk menjadi standar transmisi WiFi. Pada perkembangannya, beberapa produsen WiFi telah mengembangkan teknologi enkripsi untuk mengakomodasi kebutuhan pengamanan jaringan wireless (Edi S. Mulyanta, 2009).

1.3. Jaringan Wireless

Jaringan Wireless berfungsi sebagai mekanisme pembawa antara peralatan atau antar peralatan dan jaringan kabel tradisional (jaringan perusahaan dan internet). Jaringan wireless banyak jenisnya tapi biasanya digolongkan ke dalam tiga kelompok berdasarkan jangkauannya: Wireless Wide Area Network (WWAN), WLAN, dan Wireless Personal Area Network (WPAN). WWAN meliputi teknologi dengan daerah jangkauan luas seperti selular 2G, Cellular Digital Packet Data (CDPD), Global System for Mobile Communications (GSM), dan Mobitex. WLAN, mewakili local area network wireless, termasuk diantaranya adalah 802.11, HiperLAN, dan beberapa lainnya. WPAN, mewakili teknologi personal area network wireless seperti Bluetooth dan infra merah. Semua teknologi ini disebut "tetherless" dimana mereka menerima dan mengirim informasi menggunakan gelombang electromagnet (EM). Teknologi wireless menggunakan panjang gelombang berkisar dari frekwensi radio (RF) hingga inframerah. Frekwensi pada RF mencakup bagian penting dari spectrum radiasi EM, yang berkisar dari 9 kilohertz (kHz), frekwensi terendah yang dialokasikan untuk komunikasi wireless,

hingga ribuan gigahertz (GHz). Karena frekwensi bertambah diluar spectrum RF, energi EM bergerak ke IR dan kemudian ke spectrum yang tampak.

1.4. Teknologi Wireless

Mulanya, peralatan handheld mempunyai kegunaan yang terbatas karena ukurannya dan kebutuhan daya. Tapi, teknologi berkembang, dan peralatan handheld menjadi lebih kaya akan fitur dan mudah dibawa. Yang lebih penting, berbagai peralatan wireless dan teknologi yang mengikutinya sudah muncul. Telepon mobil, sebagai contoh, telah meningkat kegunaannya yang sekarang memungkinkannya berfungsi sebagai PDA selain telepon. Smart phone adalah gabungan teknologi telepon mobil dan PDA yang menyediakan layanan suara normal dan email, penulisan pesan teks, paging, akses web dan pengenalan suara. Generasi berikutnya dari telepon mobil, menggabungkan kemampuan PDA, IR, Internet wireless, email dan global positioning system (GPS). Pembuat juga menggabungkan standar, dengan tujuan untuk menyediakan peralatan yang mampu mengirimkan banyak layanan. Perkembangan lain yang akan segera tersedia adalahl sistem global untuk teknologi yang berdasar komunikasi bergerak (berdasar GSM) seperti General Packet Radio Service (GPRS), Local Multipoint Distribution Service (LMDS), Enhanced Data GSM Environment (EDGE), dan Universal Mobile Telecommunications Service (UMTS). Teknologi-teknologi ini akan menyediakan laju transmisi data yang tinggi dan kemampuan jaringan yang lebih besar. Tapi, masing- masing perkembangan baru akan menghadirkan resiko keamanannya sendiri,dan badan pemerintah harus memikirkan resiko ini untuk memastikan bahwa asset yang penting tetap terjaga.

1.3. Tujuan dan Manfaat Penelitian

Tujuan umum penelitian ini adalah untuk menganalisa sistem keamanan yang ada dalam jaringan nirkabel (wireless), sedangkan manfaatnya adalah memahami konsep keamanan yang diberikan oleh layanan jaringan nirkabel.

2. Metodologi

Dalam penulisan penelitian ini penulis mendapatkan data dari berbagai sumber yang relevan sebagai bahan untuk penyusunan penelitian ini dengan jenis data:

a. Data Primer

Data Primer diperoleh langsung melalui proses pengamatan dan wawancara secara langsung dengan sumber atau pihak yang bersangkutan (responden) yang siap untuk diolah (Wirartha, 2006, Hal.35). Dalam penelitian ini data primer diperoleh melalui wawancara dan observasi pada Instansi Pemerintah maupun Swasta yang bergerak dibidang bisnis maupun non bisnis pada bagian pengolahan datanya, data berupa dokumen informasi serta wawancara praktisi / pakar teknologi dibidang informasi yang berhubungan dengan aplikasi jaringan nirkabel.

b. Data Sekunder

Data sekunder adalah data yang diperoleh dan dikumpulkan secara tidak langsung yaitu melalui buku-buku, majalah – majalah, dan semua media yang berkaitan dengan permasalahan pada objek penelitian (Wirartha, 2006, Hal.35).

2.1. Metode Pengumpulan Data :

Sesuai dengan jenis data dan maksud serta tujuan penyusunan penulisan ini maka dalam menyusun penelitian, penulis menggunakan metode sebagai berikut:

a. Metode Wawancara / *Interview*

Merupakan salah satu metode pengumpulan data dengan jalan komunikasi yaitu dengan kontak dan hubungan pribadi antara pengumpul data dengan sumber data (Wirartha, 2006, Hal.37). Penulis melakukan wawancara pada personal yang ada di bagian Pengolahan Data serta pakar teknologi informasi yang ada di instansi / lembaga terkait.

b. Metode Pengamatan

Data dapat diperoleh melalui pengamatan terhadap gejala yang diteliti. Dalam hal ini, panca indra manusia (penglihatan dan pendengaran). hasil pengamatan tersebut ditangkap kemudian di analisis untuk menjawab masalah penelitian (Wirartha, 2006, Hal.37). Dari pengamatan ini, penulis mendapatkan data dari dokumen-dokumen informasi yang ada, tampilan media elektronik (komputer) serta dari tanya jawab langsung dengan nara sumber.

c. Studi Pustaka

Metode ini dilakukan dengan cara mempelajari literatur – literatur yang ada hubungannya dengan objek penelitian (Wirartha, 2006, Hal.36). Dalam hal ini referensi yang digunakan adalah buku –

buku dan e-book berkaitan dengan tema penelitian.

3. Pembahasan

3.1. Standarisasi *Wireless*

Beberapa standar yang dikenal dan diterapkan pada produk-produk *wireless LAN* saat ini 802.11a, 802.11b dan 802.11g (Gunawan, Arief Hamdani dan Andi Putra, 2003) Dalam sejarah dan perkembangannya, standarisasi *wireless LAN* dimulai dengan standar 802.11. standar ini dicetuskan pada tahun 1997 oleh *IEEE (institute of Electrical and Electronics Engineers).* Kecepatan transfer data pada standar 802.11 adalah sekitar 2 Mbps.

Perbedaan antara standar 802.11a dan 802.11b terletak pada frekuensi radio tempat standar ini bekerja dan pada kecepatan transfer datanya. 802.11a bekerja pada frekuensi radio 5.15 dan 5.875 Ghz. Kecepatan transfer data pada 802.11a mencapai 54 Mbps. Namun pemanfaatan standar ini tidak terlalu menggembirakan, karena sedikitnya produk yang mengadopsi teknologi dengan standar ini, berbeda dengan standar 802.11b, justru lebih banyak dipakai. 802.11b bekerja pada frekuensi radio 2.4 Ghz, namun sayangnya kecepatan transfer data pada 802.11b hanya 11 Mbps. Jauh dibawah standar 802.11a.

Tabel 1. Standarisasi *Wireless*

Standar	**802.11a**	**802.11b**	**802.11g**
Kompatibilitas	*IEEE* 802.11a	*IEEE* 802.11b	*IEEE* 802.11b dan 802.11g
Jumlah *channel*	8 *Non overlapping*	3 *Non Overlapping*	3 *Non overlapping*
Jangkauan dalam ruang	12 m@54 Mbps; 91 m @ 6Mbps	30 m@11Mbps; 91 m@1 Mbps	30 m @ 54 Mbps; 91 m @ 1 Mbps
Jangkauan di luar ruang	30 m@54 Mbps; 305 m @ 6Mbps	120 m@11Mbps; 460 m@ 1Mbps	120 m@54 Mbps; 460 m@1Mbps
Data *rates*	54, 48, 36, 24, 18, 12, 8, dan 6 Mbps	11, 5.5, 2, dan 1 Mbps	54, 48, 36, 24, 18, 12, 9, dan 6 Mbps

Modulasi dan frekuensi	*Orthogonal freqeunce division multiflexing*, 5 Ghz	*Direct Sequerence Spread*, 2.4 Ghz	Orthogonal *freqeunce division multiflexing*, 2.4 Ghz

(Sumber : Membangun *Wireless LAN*; Jhonsen, 2005)

Kemanan Jaringan Wireless

Keamanan bisa jadi merupakan hal terakhir yang anda pikirkan dalam usaha anda membangun jaringan wireless baik dirumah maupun dikantor. Anda tidak sadar bahwa banyak sekali orang disekitar anda menghabiskan waktu berusaha untuk mencuri file pribadi orang, mencuri data credit card di Internet, bahkan kalau di kantor banyak juga karyawan berusaha iseng menghabiskan waktu untuk melihat-lihat data pribadi orang lain baik berupa file, photo, atau bahkan email jika mereka dapat kesempatan untuk itu. Tentunya anda tidak ingin membiarkan komputer atau laptop anda tanpa suatu proteksi dan keamanan tertentu bukan?

Sebagai rumusan umum, anda harus memberikan suatu system tingkat keamanan yang memadai dan sebanding dengan tingkat sensitifitas data yang harus anda lindungi. Tidak seperti system jaringan LAN kabel, dimana secara fisik adalah aman, jaringan wireless tidaklah bisa hanya dibatasi oleh dinding didalam gedung. Jaringan wireless bisa menembus dinding pembatas gedung anda, dan tergantung seberapa bagus kualitas jangkauan jaringan wireless anda, jangkauan wireless bisa sejauh sekitar 300 an meter diluar gedung hanya dengan menggunakan labtop dan antenna penguat. Hal ini menjadikan jaringan wireless sangat rentan dan lemah terhadap segala macam usaha pencegatan dan perampokan data anda. Seperti halnya pada jaringan LAN kabel, jaringan wireless juga rentan terhadap segala macam ancaman dan gangguan jaringan seperti DoS, Spamming, Sniffers dan lain-lain.

Ada beberapa alasan dimana anda mengharuskan untuk melindungi komputer anda dari segala bentuk ancaman jaringan yaitu:

a. Data personal dan financial anda ataupun data sejarah medical anda ada di hard-disk komputer atau laptop anda
b. Koneksi Internet anda bukanlah murah, tentunya anda tidak mau membagi

dengan semua orang yang tidak berhak, bukannya pelit sebenarnya, akan tetapi efek dari system yang rentan yang bisa menyebabkan kerugian kita.

c. Anda tidak ingin ada orang yang menggunakan komputer anda untuk dipakai menyebarkan spam dari komputer anda atau dari email address anda.

Keamanan jaringan wireless pada dasarnya lebih mudah di crack daripada jaringan LAN kabel, karena sebenarnya anda tidak memerlukan koneksi secara fisik terhadap jaringan wireless. Transfer data terjadi lewat gelombang udara, yang oleh karenanya pengaksesannya jadi lebih gampang. Maka dari itu, suatu pendekatan yang systematic dalam keamanan jaringan wireless termasuk perlindungan terhadap serangan virus menjadi suatu keharusan.

Service set ID (SSID) adalah suatu string atau nama yang digunakan untuk mendefinisikan suatu domain roaming dalam suatu access point (AP) didalam suatu jaringan wireless yang terdiri dari banyak Access Point (AP). SSID yang berbeda pada beberapa access point bisa memungkinkan suatu jaringan wireless network yang saling tumpang tindih. Pada awalnya SSID ini dianggap sebagai suatu password untuk masuk ke suatu jaringan wireless, tanpa SSID client tidak akan bisa konek ke jaringan. Akan tetapi SSID client ini ditolak karena Access Point melakukan broadcast SSID beberapa kali per detik dan segala macam alat analisa standard 802.11 seperti Airmagnet, NetStumbler, atau Wildpacket Airopeek bisa digunakan untuk membacanya. Karena user sering melakukan konfigurasi clients, apa yang disebut password ini menjadi sering diketahui secara luas. Jadi kalau kita menggunakan SSID ini sebagai password jadi tidak berguna.

Apakah seharusnya kita mengubah SSID ini? Jelas sekali harus. Walaupun SSID ini tidak merupakan salah satu layer dari system keamanan, nama SSID haruslah diubah dari nama bawaan default dari pabrik sehingga orang tidak menduga-duga jaringan wireless anda dengan mudah.

Hampir semua wireless router dan adapter wireless sekarang ini mendukung standard keamanan jaringan wireless seperti WEP dan WPA enkripsi 64-bit/128-bit. Apa artinya WEP atau WPA ini?

Dalam keamanan jaringan wireless, WAP kepanjangan dari Wi-Fi Protected Access (WPA atau versi terbarunya WPA2)

yang merupakan program sertifikasi yang dibuat oleh Wi-Fi Alliance yang menunjukkan adanya suatu compliant (tunduk terhadap suatu aturan atau standard yang digariskan) dengan protocol keamanan yang diciptakan oleh Wi-Fi Alliance untuk keamanan jaringan wireless komputer. Protocol ini diciptakan menjawab adanya banyak diketemukannya (oleh para peneliti) kelemahan system standard keamanan wireless pendahulunya yaitu WEP (Wired Equivalent Privacy).

Wired Equivalent Privacy (WEP) dalam keamanan jaringan wireless adalah suatu algoritme tertentu yang diciptakan untuk keamanan jaringan wireless IEEE 802.11. jaringan wireless melakukan broadcast messages menggunakan sinyal radio, makanya sangat rentan terhadap segala usaha "pengupingan" dibanding jaringan LAN kabel. Ketika diperkenalkan di tahun 1977, WEP dimaksudkan untuk memberikan kerahasiaan yang setara dengan jaringan kabel tradisional.

Tanda Certifikasi WPA2 pada keamanan jaringan wireless kemudian menunjukkan suatu compliant dengan suatu protocol advance yang meng-implementasikan standard penuh. Protocol tingkat advance ini tidak akan berjalan atau tidak mendukung pada piranti adapter wireless versi sebelumnya (kuno). Produk yang lulus uji testing oleh Wi-Fi Alliance untuk suatu compliant dengan protocol ini berhak memberikan label WPA pada produknya.

WPA2 menggantikan WPA, seperti WPA, WPA2 memerlukan testing dan certifikasi oleh Wi-Fi Alliance. WPA2 meng-implementasikan elemen-2 mandatory dari 802.11i. Khususnya ia memperkenalkan suatu algoritma baru berdasarkan AES, CCMP, yang dianggap sangat aman. Certifikasi dimulai sejak tahun 2004 September dan sejak tanggal 13 Maret 2006, certifikasi WPA2 adalah suatu keharusan untuk semua piranti wireless yang baru jika ingin mendapatkan label Wi-Fi.

IEEE 802.11i-2004 atau 802.11i dalam keamanan jaringan wireless adalah suatu amandemen pada standard IEEE 802.11 yang men-spesifikasikan mekanisme keamanan jaringan wireless.

Ia menggantikan klausa pendek "Authentication and privacy"dari standard asli dari klausa rinci "security", dalam proses depresiasi kebocoran WEP. Amandemen ini kemudian dilegalkan

kedalam standard yang dipublikasikan yaitu standard IEEE 802.11-2007.

Sekarang kita sudah mempunyai sedikit pegetahuan mengenai standard keamanan jaringan wireless, dimana hampir semua producen wireless memberikan label compliant WPA/WPA2 pada produk piranti wireless mereka.

Hampir semua piranti wireless router dari pabriknya di set defaultnya untuk tidak memberikan keamanan (disable security), jadi anda harus mensettingnya untuk enable security standard. Jika anda tidak mau menggunakan keamanan wireless, maka anda biarkan saja setting default pabriknya. Sungguh sangat mengejutkan bahwa hampir kebanyakan orang tidak menggunakan fasilitas keamanan jaringan wireless ini dan membiarkan setting default aslinya, entah alasan tidak praktis sampai alasan tidak tahu cara melakukan settingan keamanannya. Kebiasaan ini menimbulkan suatu hobby dari sebagian orang berkeliling mencari sinyal wireless dengan laptop mereka atau dengan PDA atau Blackberry yang dilengkapi dengan piranti Wi-Fi. Akan tetapi yang lebih bahaya adalah sebagian orang yang memang berusaha mencari celah untuk bisa masuk ke jaringan wireless untuk mencuri data atau usaha hacking yang merugikan perusahaan anda.

Perlu diingat, jika anda menggunakan jaringan wireless WPA, bahwa anda harus mensetting metoda WPA dan shared key yang sama dalam usaha koneksi ke jaringan wireless, kalau tidak maka akan tidak bisa jalan jaringan anda.

Selain WEP dan WPA, anda juga bisa melakukan filter terhadap computers atau adapter yang boleh masuk atau akses terhadap jaringan wireless. MAC address adalah address fisik yang unik didalam suatu jaringan termasuk adapter wireless. MAC address ditanam secara permanen kedalam piranti jaringan. Bagaimana cara mengetahui address fisik dari piranti jaringan?

Address MAC biasanya ditulis dibagian adapter itu sendiri seperti pada contoh gambar diatas ini yang menunjukkan “hardware address” atau address fisik piranti. Akan tetapi jika adapter tersebut sudah terinstall didalam salah satu slot komputer anda bagaimana cara mengetahuinya? Tentunya anda tidak bisa melihatnya secara visual. Pada command prompt (tekan tombol Windows dan tombol R secara bersamaan dan kemudian ketik “cmd” terus tekan Enter untuk masuk ke

command prompt, kemudian ketik command "ipconfig /all" maka akan muncul dilayar dan anda bisa mengetahui address fisik seperti pada contoh diatas adalah 00-1C-F0-B9-F3-24.

Didalam wireless router, kebanyakan filter wireless MAC ini secara default di "disabled". Jika anda ingin mem-filter users berdasarkan MAC address, baik dilarang atau diberi ijin akses, pilih "enable". Ilustrasi berikut ini, wireless router hanya mengijinkan komputer dengan address fisik 00-1C-F0-D9-F3-24. Karenanya untuk laptop yang ada dalam radius ini dimana address fisiknya 00-1C-F0-D9-F3-11 tidak bisa mengakses jaringan wireless.

3.3. Langkah Pengamanan Jaringan

Berikut ini adalah beberapa langkah dalam mengamankan jaringan nirkabel:

1. Ubahlah Sistem ID (Identitas)

Biasanya suatu layanan nirkabel dilengkapi dengan suatu standart pengamanan identitas atau yang sering disebut SSID (Service Set Identifier) or ESSID (Extended Service Set Identifier). Sangat mudah bagi seorang hacker untuk mencari tahu identitas default dari suatu layanan atau jaringan, jadi sebaiknya Anda segera mengubahnya menjadi suatu identitas yang unik, yang tidak mudah ditebak orang lain.

2. Mematikan identitas pemancar

Dengan mengumumkan kepada umum bahwa Anda memiliki suatu jaringan nirkabel akan membuat para hacker penasaran untuk membobol jaringan nirkabel Anda. Mempunyai suatu jaringan nirkabel bukan berarti harus memberitahukannya kepada semua orang. Periksalah secara manual perangkat keras yang Anda pakai untuk jaringan nirkabel tersebut, dan pelajarilah bagaimana cara mematikannya.

3. Sediakanlah enkripsi

WEP (Wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) dapat meng-enkripsi data Anda sehingga hanya penerima saja yang diharapkan dapat membaca data tersebut. WEP (Wired Equivalent Privacy) mempunyai banyak kelemahan yang membuatnya mudah disusupi. Kunci 128-bit hanya mempunyai tingkat pencapaian yang relatif rendah tanpa peningkatan keamanan yang signifikan, sedangkan untuk 40-bit atau 64-bit pada beberapa perlengkapan lainnya, mempunyai enkripsi yang sama baiknya. Dengan cara pengamanan yang standart saja

pastilah tetap akan mudah bagi hacker untuk menyusup, namun dengan cara enkripsi ini pastilah akan membuat jaringan Anda lebih aman dari hacker. Jika memungkinkan, ada baiknya untuk menggunakan enkripsi WPA (peralatan yang lebih tua dapat diupgrade terlebih dahulu agar compatible dengan WPA). WPA dapat sangat menjanjikan dalam menjamin keamanan jaringan nirkabel Anda, namun masih tetap dapat dikalahkan oleh serangan DOS (denial of services).

4. Membatasi dari penggunaan traffic yang tidak perlu

Banyak router jaringan kabel maupun nirkabel yang dilengkapi firewalls. Bukan bermaksud mengedepankan firewalls, namun firewalls telah membantu dalam pertahanan keamanan jaringan. Bacalah petunjuk manual dari perangkat keras Anda dan pelajarilah cara pengaturan konfigurasi router Anda, sehingga hanya traffic yang sudah seijin Anda saja yang dapat dijalankan.

5. Ubahlah 'kata sandi' default Administrator milik Anda

Hal ini baik untuk semua penggunaan perangkat keras maupun perangkat lunak. Kata sandi default sangat mudah disalahgunakan, terutama oleh para hacker. Oleh karena itu sebaiknya ubahlah kata sandi Anda, hindari penggunaan kata dari hal-hal pribadi Anda yang mudah diketahui orang, seperti nama belakang, tanggal lahir, dan sebagainya.

6. Kunci dan lindungilah komputer Anda

Hal ini merupakan cara pengamanan terakhir untuk komputer Anda. Gunakanlah firewall, perangkat lunak Anti Virus, Zone Alarm, dan lain sebagainya. Setidaknya setiap satu minggu perbaharuilah Anti Virus yang Anda pakai.

3.4. Prinsip Keamanan Jaringan

Untuk merancang mekanisme keamanan yang efektif, terdapat beberapa prinsip keamanan, contohnya :

a) Principle of least privilege : memberi hak kepada user atau proses untuk melakukan pekerjaan yang sesuai dengan haknya
b) Meminimalkan trusted components: mengidentifikasi komponen-komponen sistem yang dapat dipercaya dan menjaga agar jumlahnya sesedikit mungkin

c) Jangan ingin sempurna : sempurna tidak mungkin diwujudkan, sehingga kita harus siap untuk mendeteksi masalah, merancang penanggulangannya dan memulihkan diri dari serangan.

4. Kesimpulan

Berikut ini adalah kesimpulan setelah melakukan penelitian : jaringan nirkabel harus memenuhi prinsip-prinsip keamanan yang dijelaskan diatas dalam penerapannya karena implementasi jaringan nirkabel dalam kenyataannya masih ditemukan celah bagi penyusup untuk menyusup kedalam komputer.

4.1. Saran

Dalam menggunakan jaringan nirkabel maka sebaiknya menggunakan pengaman untuk melindungi komputer kita dari penyusup, misalnya dengan menggunakan program untuk mendeteksi adanya penyusup karena sinyal WiFi dapat ditangkap oleh penyusup.

Daftar Pustaka

Edi S. Mulyanta, 2005, "Jaringan Wireless Komputer", Yogyakarta.

Gunawan, Arief Hamdani dan Andi Putra, 2003, "Komunikasi Data Via IEEE 802.11", Jakarta: Dinastindo.

Herwindo dan Ali Akbar, 2005, "Mengenal Sistem Komputer Masa Kini", Bandung : Yrama Widya

Jhonsen dan Jhon Edison, CCNA, 2005. "Membangun Wireless LAN", Jakarta: PT Elex Media Komputindo.

Kamei, S, et al, 2003, " Practicable network design for handling growth in the volume of peer-to-peer traffic", Communications, Computers and signal Processing.

Kjetil Haslum, et al, 2009, " Real-time Intrusion Prevention and Security of

Network using HMMs", Local Computer Networks.

Robert Richardson, 2009, "CSI Computer Crime & Security Survey 2009".

Simarmata, Hamer. (2005). Sistem Jaringan Wireless. Ilmu Komputer

Tanenbaum, S. Andrew, 1996, "Komputer Networks", Terjemahan Gurnita Priatna, 2000, Jakarta: Prenhallindo.

Wirartha, I.M., 2006, "Metodologi Penelitian Sosial Ekonomi", Yogyakarta, Penerbit Andi.