SinkrOn
JURNAL & PENELITIAN TEKNIK INFORMATIKA
Jurnal & Penelitian Teknik Informatika
Volume 1 Nomor 1, Oktober 2016
e-ISSN : 2541-2019
p-ISSN : 2541-044X

Teknik Keamanan Jaringan Wireless LAN Pada Warnet Salsabila Computer Net

Jamaludin
Politeknik Ganesha Medan
Jl. Veteran No. 190 Pasar VI Manunggal
74342.kampus@gmail.com

Abstrak — Perangkat teknologi berbasis wireless pada saat ini sudah banyak digunakan terutama pada jasa warnet. Semakin bertambahnya populasi warnet yang berbasis wireless tersebut akan mempengaruhi minat para pengunjung, sehingga apabila tidak diperhatikan dari segi kecepatan atau kinerja dari warnet tersebut maka para pengunjung akan meninggalkan warnet yang lambat dan memilih warnet yang memiliki access kecepatan yang lebih baik. Salah satu kecepatan jaringan wireless LAN sangat ditentukan oleh rasio ketersediaan dari *bandwitdth* dengan banyaknya jumlah pengunjung yang mengakses jaringan tersebut. Disamping kecepatan, pengamanan data juga menjadi hal yang penting. Oleh karena itu memberikan system keamanan yang baik akan sebanding dengan tingkat kecepatan dan sensitifitas data yang harus dilindungi. Tingkat keamanan pada wireless LAN tidaklah sama dengan jaringan kabel LAN, di mana secara fisik adalah aman sementara jaringan wireless LAN tidak hanya bisa dibatasi oleh dinding di dalam gedung namun jaringan wireless bisa menembus dinding pembatas gedung. Hal ini menjadikan jaringan wireless sangat rentan dan lemah terhadap segala macam ancaman dan gangguan jaringan. Teknik 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, dan implementasi fasilitas MAC Address. Untuk penanganan keamanan jaringan wireless di Salsabila Net dengan cara menyembunyikan SSID, memanfaatkan kunci WEP, WPA-PSK dan mengimplementasikan fasilitas MAC Address

Kata Kunci —**Wireless LAN, SSID, WEP, WPA-PSK**

I. PENDAHULUAN

Secara teknis operasional, Wi-Fi merupakan salah satu varian teknologi komunikasi dan informasi yang bekerja pada jaringan dan perangkat WLANs (*wireless local area network*). Dengan kata lain, Wi-Fi adalah sertifikasi merek dagang yang diberikan pabrikan kepada perangkat telekomunikasi (internet) yang bekerja di jaringan WLANs dan sudah memenuhi kualitas kapasitas interoperasi yang dipersyaratkan.

Tingginya minat masyarakat khususnya di kalangan komunitas internet menggunakan teknologi Wi-Fi dikarenakan para pengguna internet dalam satu area dapat mengakses internet secara bersamaan tanpa perlu direpotkan dengan kabel. Konsekuensinya, pengguna yang ingin melakukan *surfing* atau *browsing* berita dan informasi di internet, cukup membawa laptop atau PDA (*pocket digital assistance*) yang sudah mendukung Wi-Fi ke tempat dimana terdapat *access point* atau *hotspot*. Saat ini perkembangan teknologi wifi sangat signifikan sejalan dengan kebutuhan system informasi, Warnet, kampus-kampus maupun perkantoran sudah mulai memanfaatkan wifi pada jaringan masing masing,

Meskipun terdapat kemudahan dari teknologi Wi-Fi ternyata jaringan WiFi memiliki kelemahan dibanding dengan jaringan kabel diantaranya menyangkut keamanan. Penanganan pada jaringan kabel hanya mencakup pada computer yang terhubung dengan jaringan tersebut, beda dengan jaringan yang menggunakan teknologi Wi-Fi yang jangkauannya lebih luas dan bisa diaccess di mana saja yang memungkinkan orang untuk masuk atau memanfaatkan fasilitas Wi-Fi atau bahkan mengambil data-data kita untuk kepentingan tertentu. Oleh karena itu pengamanan pada jaringan yang menggunakan teknologi Wi-Fi harus lebih maksimal.

Untuk mendapatkan jaringan *wireless* dengan keamanan sempurna merupakan pekerjaan yang hampir tidak mungkin. Akan tetapi pencegahan tetap harus dilakukan ketika kita merancang jaringan *wireless*. Hal ini berarti kita harus benar-benar memperhatikan *access point*. *Access point* harus yang pertama kali kita perhatikan untuk mengkonfigurasi jaringan *wireless* dengan keamanan yang baik

e-ISSN : 2541-2019
p-ISSN : 2541-044X

II. TINJAUAN PUSTAKA

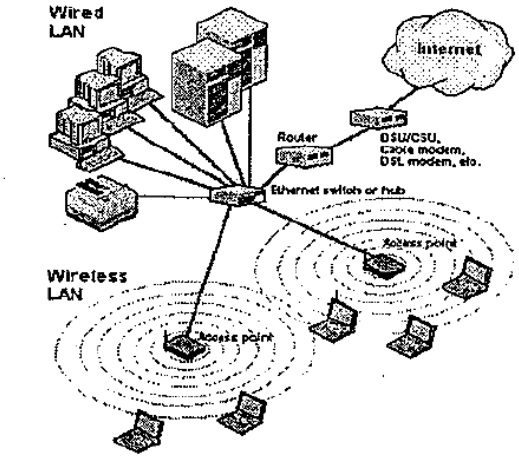
A. *Jaringan Wireless, Wi-Fi, dan Hot Spot*

Jaringan *wireless* atau yang dikenal dengan jaringan *nirkabel Wireless* atau *wireless network* merupakan sekumpulan komputer yang saling terhubung antara satu dengan lainnya sehingga terbentuk sebuah jaringan komputer dengan menggunakan media udara/gelombang sebagai jalur lintas datanya. Teknologi *wireless* adalah salah satu pilihan yang tepat untuk menggantikan teknologi jaringan yang terdiri dari banyak kabel dan merupakan sebuah solusi akibat jarak antar jaringan yang tidak mungkin dihubungkan melalui kabel. Keuntungan terbesar dari wireless yaitu sangat praktis, dimana komputer dapat terhubung ke jaringan tanpa membutuhkan kabel.

Wi-Fi (Wireless Fidelity) adalah standar yang dibuat oleh konsorsium perusahaan produsen peranti W-LAN yaitu *Wireless Ethernet Communications Alliance* untuk mempromosikan kompatibilitas perangkat 802.11.

Hot Spot adalah definisi untuk daerah yang dilayani oleh satu Access Point Wireless LAN standar 802.11a/b/g, dimana pengguna (user) dapat masuk ke dalam Access Point secara bebas dan *mobile* menggunakan perangkat sejenis notebook, PDA atau lainnya (Deris Stiawan, *Wireless Fundamental, Instalation & Implemetations*, 2008).

Ada dua cara untuk menghubungkan antar PC dengan system *wireless*, yaitu sistem ***adhoc*** dan ***Access point.*** Sistem *adhoc* merupakan hubungan antar PC berdasarkan nama SSID (*Service Set Identifier*) hampir sama dengan jaringan *peer to peer*. SSID adalah nama komputer yang memiliki *card*, USB dan perangkat *wireless*. Setiap perangkat harus diberi nama tersendiri sebagai identitas. Saat ini system *Access point* paling umum dipakai dalam teknologi *wireless*. Koneksi infra strukturnya menggunakan *Access point* membutuhkan paling tidak sebuah jaringan *wireless* yang memiliki satu titik di satu tempat, sehingga komputer lain dapat mencari dan menerima sinyal agar bisa masuk ke jaringan tersebut.



Gambar 1. Sistem *Access Point*

WLAN menggunakan *access point* untuk mengirim dan mentransmisikan sinyal radio dari komputer pengguna ataupun dari peralatan lain. Perangkat pengguna harus memiliki *card* khusus yang berisikan radio *transmitter* dan *receiver* kecil. *Access point* terkoneksi ke *local area network*
(LAN) sehingga bisa terkoneksi ke internet. WLAN memungkinkan pengguna berpindah (dari satu titik ke titik lain) tanpa harus melepas kabel jaringan dari satu *jack* dan memasangnya di tempat lain.

B. *Standarisasi Jaringan Wireless*

Standarisasi 802.11 *wireless* pertama kali dikeluarkan oleh IEEE di tahun 1997. *Institute of Electrical and Electronics Engineers* (IEEE) merupakan organisasi professional bagi *engineer*, ilmuwan dan pelajar. IEEE mengembangkan banyak standarisasi termasuk jaringan dan komputasi. Standar 802.11 merupakan protocol yang digunakan *wireless client (*perangkat pengguna*)* dan *base station (access point)* atau antara dua *wireless clients.* Versi IEEE sebelumnya hanya untuk jaringan dengan range 2 Mbps (megabits per second), tapi dengan IEEE 802.11 telah direvisi sejak 1997. Standar 802.11b, juga dikenal dengan Wi-Fi (*Wireless Fidelity), bandwidth*nymeningkat menjadi 11 Mbps. 802.11b menjadi standar yang paling banyak digunakan dengan frekuensi 2.4 GHz sama dengan frekuensi yang digunakan *cordless phone*..

Untuk Standard 802.11a, potensial untuk *bandwidth* hingga 54 Mbps. 802.11a beroperasi di frekuensi 5 GHz, frekuensi yang banyak digunakan di kalangan militer dan tidak tersedia di setiap negara. Tetapi saat ini sudah mulai banyak yang menggunakan frekuensi 802.11a. Karena jaringan "a" dan "b" beroperasi di frekuensi yang berbeda maka keduanya tidak kompatibel. 802.11a lebih bebas ganguan sinyal *oven microwave* dan *cordless phone* dibandingkan “b”, tetapi harga perangkatnya

e-ISSN : 2541-2019
p-ISSN : 2541-044X

lebih mahal dan daya jangkau relatif lebih pendek. 802.11a kompatibel dengan standar internasional lain seperti Hiperlan/1dan /2. Yang merupakan standar Eropa yang dikeluarkan oleh *European Telecommunications Standards Institute* (ETSI) untuk *wireless* LAN standard di negara-negara Eropa.

Standar *wireless networking* yang lain adalah standar 802.11 g yang cukup kompatibel dengan tipe 802.11 b dan memiliki kombinasi kemampuan tipe a dan b. Standar 802.11g menggunakan frekuensi 2,4Gz yang memiliki kecepatan transmisi sebesar 54 Mbps bahkan dapat mencapai 108 Mbps (apabila terdapat inisial G atau turbo). *Hardware* pendukung 802.11g paling banyak diproduksi oleh vendor. Secara teoritis, tipe ini mampu mentransfer data kurang lebih 20 Mbps atau 4 kali lebih cepat dari tipe b dan sedikit lebih lambat dari tipe a.Tipe ini menempatkan sistem OFDM yang berfungsi untuk menghadapi gangguan frekuensi.

C. Perbandingan Jaringan Kabel dan Jaringan Wireless

Local area network (jaringan komputer lokal) memungkinkan terjadinya pertukaran data dan informasi melalui komputer, dengan menyediakan koneksi yang cepat dan andal. Jaringan komputer konvesional menggunakan media transmisi kabel, *coaxial*, *twisted pair* ataupun *fiber optic* untuk memenuhi kebutuhan tersebut. Pengkabelan ini selain *hardware* dan *software*, juga merupakan bagian yang besar dari biaya investasi instalasi sebuah jaringan komputer. Untuk jaringan yang ada pada kantor kantor besar, biaya pengkabelan ini dapat mencapai lebih dari 40% dari biaya total yang dibutuhkan. Untuk kasus pengkonfigurasian ulang jaringan, akan dibutuhkan biaya yang hampir sama dengan biaya instalasi LAN baru.

Masalah ini ikut memacu dikembangkannya *wireless* LAN, mengingat karakteristik sistem *wireless* yang fleksibel untuk diimplementasikan dimana saja seperti perkantoran, industri, rumah sakit maupun perguruan tinggi. Disamping itu sistem *wireless* juga menawarkan berbagai aplikasi diantaranya aplikasi komunikasi antar terminal PC dan koneksi ke jaringan telepon misalnya *wireless* PABX. Dengan pertimbangan tersebut, *wireless* LAN dapat memberikan biaya instalasi yang lebih ekonomis, disamping sifatnya yang portabel. Jaringan *wireless* tetap saja tidak bisa menggantikan jaringan kabel sepenuhnya. WLAN bisaanya terhubung dengan jaringan utama yang menggunakan kabel, sehingga bisa dikatakan *wireless network* sebagai tambahan. Kenyataannya tiap teknologi jaringan memiliki kelebihan dan kekurangan. Yang paling membedakan antara jaringan kabel dengan *wireless* adalah : jaringan kabel lebih cepat dibandingkan *wireless*. Sebagian besar jaringan kabel beroperasi pada kecepatan 100 Mbps, dengan menggunakanteknologi *switching*. Sehingga seorang pengguna bisa mendapatkan data dengan kecepatan *bandwidth* penuh 100 Mbps dengan teknologi *switching*, meskipun terdapat 20 orang pengguna lain di *switch* yang sama. Sedangkan *Wireless networks*, menggunakan teknologi sharing. Dengan kata lain 11 Mbps yang tersedia mesti dibagi dengan semua pengguna yang berkomunikasi dengan*access point* yang sama. Di sisi lain banyak aplikasi yang membutuhkan *bandwidth* yang lebih tinggi dibandingkan *bandwidth* yang bisa disediakan WLAN. Misalnya aplikasi *Computer Aided Design (CAD)* yang ukurannya relatif besar jika diakses menggunakan WLAN akan menghasilkan respon yang sangat lambat. File stream MPEG yang diakses menggunakan koneksi 11 Mbps, akan mengambil sebagian besar *bandwidth* yang ada untuk seluruh user yang menggunakan *access point*. Hal yang bisa dilakukan *wireless* sedangkan kabel tidak adalah: mobilitas. Mobilitas dan fleksibilitas memungkinkan komputer pengguna yang ada di lingkungan komputer *wireless* menjadi lebih atraktif. Untuk jaringan WLAN sendiri ada empat jenis:

1. *LAN extensions:* yang memungkinkan koneksi antara *mobile wireless device* dan jaringan kabel. Contohnya aplikasi-aplikasi manufacturing pertukaran stock, dan warehouses
2. *Cross-building interconnects:* koneksi *wireless* yang cepat antar gedung. Digunakan komunikasi *microwave* dengan menggunakan antenna.
3. *Nomadic access:* memungkinkan komunikasi antar perangkat mobile seperti laptops, dan PDA dengan jaringan kabel yang sudah ada. Sebagai contoh aplikasi-aplikasi bisa menggunakan system ini untukmentransfer data dari perangkat *wireless* ke rumah, kantor atau kampus.
4. *Mobile ad hoc networks (MANET):* mobile *wireless* computer dan perangkatnya menjadi lebih cerdas, kecil, portable, dan powerful seiring dengan meningkatnya kebutuhan. MANET memungkinkan perangkattadi bisa digunakan digunakan di jaringan tanpa mengubah infrastruktur yang ada. Aplikasi-aplikasi yang menggunakan MANET misalnya pemulihan bencana, misi-misi militer, ruang kelas dan konferensi. *Routing multi-hop* digunakan untuk komunikasi antar *node* (laptop ataukomputer di dalam kendaraan) yang berjauhan satu sama lain. Tiap *host*memiliki kemampuan routing ke *mobile network*. MANET memiliki Stopologi dinamis

e-ISSN : 2541-2019
p-ISSN : 2541-044X

D. Keamanan Wireless

Keamanan system *wireless* bisa dibagi menjadi empat bagian yaitu · Keamanan aplikasi. Yang berarti keamanan aplikasi user dan aplikasi
standar seperti email. · Keamanan perangkat. Bagaimana memmproteksi perangkat fisik darikasus kerusakan, hilang ataupun dicuri. · Keamanan dari komunikasi *wireless*. Bagaimana memproteksi pesan saat dikirimkan.· Keamanan server yang terkoneksi menggunakan internet atau jaringan kabel.Resiko serangan yang mungkin akan terjadi pada standard 802.11b dapat dikatagorikan kedalam tujuh jenis serangan : 1) *Insertion Attack;* 2) *Interception* dan *Monitoring Traffic Wireless;* 3) *Jamming*(dikenal dengan *denial of service*); 4) *Client-to-Client Attack*; 5) *Brute Force Attack Againts Access point Password;* 6) *Attack againts encription,*dan 7) *Misconfiguration*

E. Wireless Access point

Wireless Access Point merupakan *hardware* atau *software* komputer yang berfungsi sebagai hub untuk pengguna ataupun perangkat *wireless* agar dapat terkoneksi ke jaringan kabel. AP adalah sistem yang penting untukmeningkatkan keamanan *wireless* dan memperluas layanan kepada pengguna. *Access point* inilah yang memberikan tanda apakah disuatu tempat memiliki jaringan WIFI dan secara terus menerus mentransmisikan namanya – *Service Set Identifier* (SSID) dan dapat diterima oleh komputer lain untuk dikenal. Bedanya dengan HUB, HUB menggunakan kabel tetapi tidak memiliki nama (SSID). Sedangkan *Access point* tidak mengunakan *cable network* tetapi harus memiliki sebuah nama yaitu nama SSID.
Keuntungan pada sistem *access point* (AP mode):

1. Untuk sistem AP dengan melayani banyak PC tentu lebih mudah pengaturan dan komputer *client* dapat mengetahui bahwa di suatu ruang ada sebuah *hardware* atau komputer yang memancarkan *signal Access point* untuk masuk kedalam sebuah *network* .
2. Keuntungan kedua bila mengunakan *hardware* khusus, maka tidak diperlukan sebuah PC berjalan 24 jam untuk melayani *network*. Banyak *hardware Access point* yang yang dihubungkan ke sebuah hub atau sebuah jaringan LAN. Dan komputer pemakai Wifi dapat masuk kedalam sebuah jaringan *network*.· Dan sistem *security* pada model AP lebih terjamin. Untuk fitur pengamansebuah *Hardware Access point* memiliki beberapa fitur seperti melakukan *block IP*, membatasi pemakai pada *port* dan lainnya.
   Sebuah *Access point* baik berupa sebuah card WIFI yang ditancapkan pada slot komputer atau jenis USB *card* dan lainnya dengan mengaktifkan fungsi *Access point* ataupun sebuah alat khusus *Access point* yang berdiri sendiri dengan antena dan *adaptor power* bisa difungsikan sebagai *Bridge network, router (gateway).* Sistem *Access point* juga diterapkan pada sebuah layanan. Misalnya layanan *network* disebuah terminal airport atau layanan khusus yang dibuat sebuah *service provider* untuk internet umumnya mengunakan sistem *Adhoc*. Pada sistem layanan tersebut bisaanya pemakai Wifi harus login sesuai ketentuan yang diperlukan.

III. PEMBAHASAN

A. Pengamanan Wireless Access Point

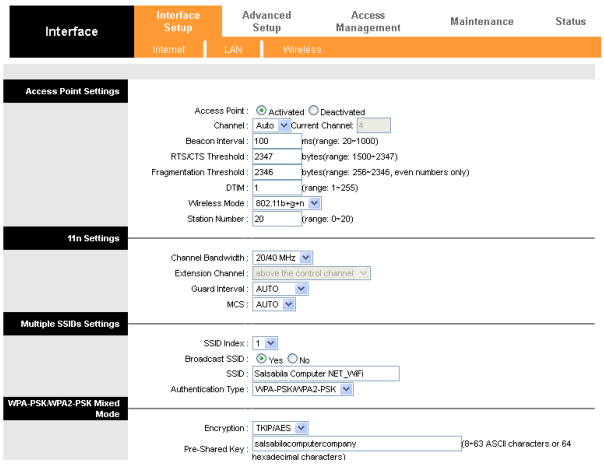
Daerah diantara *Access point* dengan pengguna merupakan daerah dengan kemungkinan gangguan keamanan paling tinggi dari jaringan *nirkabel*. Daerah ini merupakan daerah bebas, dimana komunikasi data dilakukan melalui frekuensi radio sehingga berbagai gangguan keamanan dapat terjadi di sini. Secara umum gangguan keamanan yang ada di daerah antara *Access point* dengan pengguna adalah: otentikasi dan *eavesdroping* (penyadapan). *Access point* harus bisa menentukan apakah seorang pengguna yang berusaha membangun koneksi ke jaringan tersebut memiliki hak akses atau tidak dan juga berusaha agar komunikasi dengan pengguna dilakukan secara aman. Selama ini ada beberapa teknik yang digunakan untuk mendukung keamanan *Access point*, antar lain: *Service Set ID (SSID), Wired Equivalent privacy (WEP), WiFi Proteced Access (WPA), dan Media Access Control (MAC) address.*. Pada umumnya teknik-teknik tersebut tidak berdiri sendiri, melainkan dikombinasikan dengan teknik-teknik lainnya.

Untuk pengamanan jaringan, faktor yang sangat penting adalah pemilihan *Access point* yang baik. AP merupakan hal pertama yang perlu kita perhatikan dalam mengkonfigurasi keamanan jaringan *wireless*. Hal pertama yang perlu kita pertimbangkan adalah kelancaran dan kekuatan sinyal serta penempatan *access point*. Untuk kelancaran sinyal, hal yang perlu diperhatikan adalah objek logam, rentang jarak, konstruksi gedung, jendela kaca dan material lain yang mempengaruhi kekuatan sinyal. Komponen kedua adalah *access point* itu sendiri; lebih baik menamakan *access point* dengan tepat sehingga bisa ditelusuri dengan mudah jika terjadi *troubleshooting. Access point* harus dipasang di lokasi yang potensial untuk layanan yaitu tempat yang biasanya mudah dijangkau oleh user. Jika *access point* diletakkan di luar, maka peralatan tersebut harus diletakkan di tempat yang aman, dengan resiko kerusakan yang kecil.

Untuk memasuki interface access point, maka pada URL ketik http://192.168.1.100/ dan isikan user dan

e-ISSN : 2541-2019
p-ISSN : 2541-044X

passwordnya. Maka akan muncul interface access point seperti gambar 2 berikut :



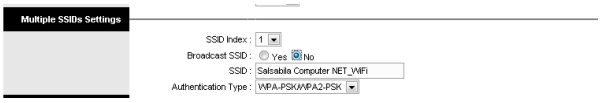
Gambar 2. Tampilan pengamanan computer keseluruhan pada interface access point

B. *Service Set Identifier (SSID)*

Service Set Identifier (SSID) merupakan parameter pertama yang bisa digunakan untuk mengamankan *wireless* LAN. SSID merupakan 1 sampai 32 karakter alphanumeric yang digunakan untuk mengindentifikasi keanggotaan di sebuah *access point* di *wireless* local area *network* (WLAN). Fungsi SSID ini sangat mirip seperti nama *network* pada jaringan kabel. SSID inilah yang merupakan garda terdepan untuk sistem keamanan jaringan *wireless*. Untuk dapat mengakses *access point* yang menjadi pusat dari system jaringan *wireless*, *client* harus mengetahui SSID yang digunakan oleh *access point* yang terdekat. Namun demikian, SSID dapat dengan mudah diketahui oleh pengguna lain selama SSID diatur pada *setting* "*broadcast*". Dengan *setting* semacam ini, siapa pun yang memiliki perangkat WLAN yang cocok dapat masuk dengan cara melakukan pencarian *access point* terdekat dengan metode pencarian sederhana yang dimiliki *software utility* yang diinstal terpisah maupun pada sistem operasi.

Pada perangkat modern, metode pencarian *access point* dapat dengan mudah menangkap *access point* terdekat, lengkap dengan nama SSID yang digunakan sehingga pengguna yang tak terotorisasi pun dapat dengan mudah terkoneksi ke dalam jaringan dengan mengatur alamat IP pada *setting* DHCP (*Dynamic Host Configuration protocol*).Sehingga sebaiknya SSID yang baik tidak diberikan nama yang berhubungan dengan nama organisasi sehingga tidakmenarik perhatian penyusup. Selain itu juga status SSID dari *access point* tidak di *broadcast*, dengan cara membuat status SSID *broadcast* menjadi *no* (non aktif) lihat gambar 2. Sehingga pengguna yang ingin terkoneksi ke *wireless* harus mengetahui SSID *access point*.

Adapun nama SSID pada gambar 3 adalah Salsabila Computer Net.Wifi



Gambar 3. Tampilan *interface SSID Acess Point*

Gambar 4. Tampilan *interface SSID Acess Point pada pemilihan wifi yang terpancar*

C. *Wired Equivalent Privacy (WEP)*

Wired Equivalent *Privacy (WEP)* merupakan protokol khusus yang ditetapkan oleh IEEE 802.11 untuk melindungi user *wireless* LAN terhadap penyadapan.Untuk menyerang WEP, *autentifikasi key* bisa di *sniff* olehpenyerang, dan *replay attack* akan dilakukan untuk mengetahui *initialization vectors (IV)* yang bisa digunakan untuk mengetahui WEP. Standar *Wired Equivalent Privacy (WEP)* dibuat untuk memberikan pengamanan jaringan dengan bentuk keamanan yang sama dengan jaringan kabel. WEP diberikan sebagai alternatif mekanisme kriptographi rahasia yang digunakan untuk pengiriman data penting yang secara subjektif hampir sama dengan kerahasiaan media kabel *local area network* (LAN) yang tidak memberlakukan teknik kriptografi untuk menjaga privasi. Hal inilah yang menjadi alasan dibuatnya WEP. Untuk memenuhi tujuannya, *wireless* harus memenuhi tiga prinsip keamanan informasi, yaitu: (1) *confidentiality*, (2)*availability*, and (3) *integrity*.

1. Tujuan utama WEP adalah untuk mencegah *eavesdropping* (penyadapan), disebut *confidentiality*.
2. Tujuan kedua adalah untuk memberikan otoritas akses ke jaringan *wireless*, disebut *availability*.
3. Tujuan ke tiga adalah untuk mencegah kebocoran komunikasi *wireless*, disebut *integrity*. Protokol WEP digunakan untuk mengenkrip data dari suatu client *wireless* ke *access point*. Hal ini berarti data dikrim tanpa enkripsi di jaringan kabel. Protokol WEP bekerja berdasarkan *RSA Securities RC4*

e-ISSN : 2541-2019
p-ISSN : 2541-044X

stream cipher. *Cipher* ini digunakan pada *body* masing-masing *frame* dan CRC. Ada dua level WEP yang secara umum ada: (1) yang satu berdasarkan enkripsi kunci 40 bit dan 24 bit vektor awal, yang berarti sama dengan 64 bit; dan (2) yang lainnya, berdasarkan 104 bit kunci enkripsi dan 24 bit vektor awal, yang berarti sama dengan 24 bit Protokol ini marak digunakan sejak mulai ditemukan. Besarnya eksploitasi, elemen desain yang buruk, dan masalah manajemen kunci yang umum membuat WEP menjadi mekanisme yang sangat kurang memadai dalam pengamanan. WEP digunakan untuk keamanan transfer data melalui metode enkripsi dan dekrsipsi, selain itu WEP dapat juga digunakan untuk otentikasi pengguna melalui protokol WEP. WEP menggunakan algoritma RC4 yang merupakan algoritma kriptografi *stream chiper*. Pesan dienkripsi terlebih dahulu sebelum dikirimkan dan sebuah *Integrity check* akan memeriksa apakah terjadi perubahan pada pesan yang dikirimkan.

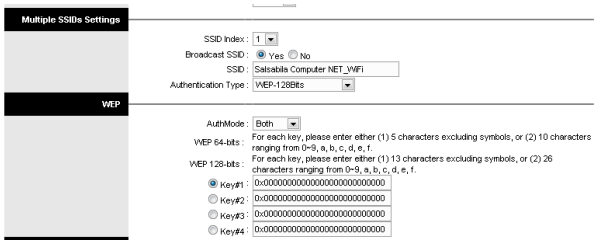
Dalam metoda WEP, kunci rahasia dibagikan ke semua pengguna yang memiliki hak akses (*shared key*) . Bisaanya kunci ini sama untuk semua pengguna dan berlaku untuk selamanya atau dalam waktu yang lama. Metode demikian sering disebut dengan metode *static shared key*. Seperti yang sudah disebutkan di atas, WEP juga bisa digunakan untuk otentikasi pengguna melalui protokol WEP. Mekanismenya sebagai berikut: *Access point* membangkitkan nilai random yang disebut dengan "*challenge*". *Challenge* ini disebarkan (*broadcast*) ke pengguna. Pengguna yang berada dalam jangkauan *access point* yang sedang membangun koneksi dengan jaringan akan menerima *challenge* tersebut. Di sisi pengguna, *challenge* tersebut akan dienkripsi dengan kunci (*shared key*) yang ia miliki.

Proses ini tentunya tanpa sepengetahuan penggunanya dan dijalankan secara otomatis oleh sistem yang ada di komputernya. Setelah dienkripsi, *challenge* tersebut kemudian dikirimkan kembali ke *access point*. Kemudian *access point* akan meng-otentikasi *challenge* yang telah dienkripsi tersebut untuk menentukan apakah pengguna yang mengirimkan *chllenge* tersebut boleh melakukan koneksi dengan jaringan atau tidak.

Metode WEP ini setidaknya memiliki dua kelemahan, yaitu dalam hal manajemen kunci dan *chipertext atatck*. Seperti yang sudah dijelaskan di atas, pada umumnya, WEP menerapkan manajemen kunci yang statis. Satu kunci untuk semua pengguna dan berlaku selamanya. Hal ini menyebabkan jika ada pengguna yang sebenarnya tidak memiliki hak akses dapat mengetahui kunci (*shared key*) , maka ia dapat melakukan koneksi ke jaringan dengan bebas dan gratis selama kunci tersebut berlaku. Kelemahan ini dapat diatasi dengan menerapkan manajemen kunci secara dinamis. Secara dinamis dalam selang waktu tertentu, *access point* membangkitkan kunci kemudian dikirimkan ke pengguna yang memiliki otentikasi ke jaringan tersebut.

WEP juga rentan dengan serangan *chipertext attack*. Jika seorang penyadap dapat memperoleh dua *chipertext* yang dikirimkan menggunakan algoritma RC4, misalnya c1 dan c2, maka ia bisa memperoleh kunci (*shared key*) yang digunakan untuk mendeskripsikan *chipertext* tersebut. Kelemahan ini dapat diatasi dengan menggunakan *initial vector* (IV) yang berubah-ubah setiap kali pengiriman data walaupun kunci yang digunakannya sama. Jadi, walaupun seorang penyadap dapat memperoleh dua *chipertext*, namun jika IV yang digunakan untuk mengenkripsi pesan tersebut tidak sama, penyadap tersebut tidak akan mendapatkan kunci.

Tampilan pada WEP bisa dilihat pada interface setup wireless seperti pada gambar 5



Gambar 5. Tampilan pada WEP pada interface setup wireless

D. Wi-Fi Protected Access (WPA)

Teknik WPA (Wi-Fi Protected Access) merupakan salah satu pengamanan pada jaringan yang menggunakan teknologi Wi-Fi, memiliki model kompatibel dengan spesifikasi standar draft IEEE 802.11i dan mempunyai beberapa tujuan dalam desainnya, yaitu kokoh, interoperasi, mampu digunakan untuk menggantikan WEP, dapat diimplementasikan pada pengguna rumahan atau corporate dan tersedia untuk public secepat mungkin. Teknik WPA dibentuk untuk menyediakan pengembangan enkripsi data yang 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 static dengan menggunakan TKIP (*Temporal Key Integrity Protocol)* yang mampu secara dinamis berubah setelah 10.000 paket data ditransmisikan. Protokol TKIP akan mengambil kuni utama sebagai starting point yang kemudian secara regular berubah sehingga tidak ada kunci enkripsi yang digunakan dua kali. Background

e-ISSN : 2541-2019
p-ISSN : 2541-044X

process secara otomatis dilakukan tanpa diketahui oleh pengguna. Dengan melakukan regenerasi kunci enkripsi kurang lebih setiap lima menit, 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 yang berhubungan dengan *throughput* seperti yang dikeluhkan oleh para pengguna jaringan wireless seperti tidak menemui jawaban dari dokumen standar yang dicari. Sebab, masalah yang berhubungan dengan thoroughput sangatlah bergantung pada hardware yang dimiliki, secara lebih spesifik adalah chipset yang digunakan.

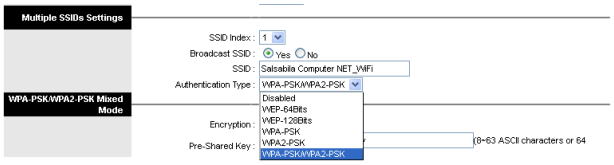
Proses otentifikasi WPA menggunakan 802.1x dan EAP (Extensible Authentication Protocol). Secara bersamaan, implementasi tersebut akan menyediakan kerangka kerja yang kokoh pada proses otentifikasi pengguna. Kerangka-kerangka tersebut akan melakukan utilisasi sebuah server otentifikas terpusat seperti RADIUS untuk melakukan otentifikasi pengguna sebelum bergabung ke jaringan wireless.

Mekanisme enkripsi AES *(Advanced Encryption Standard)* tampaknay akan diterapkan 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 ketangguhan itu dapat bertahan.

Untuk dapat menggunakan kelebihan yang dimiliki WPA, pengguna harus memiliki hardware dan software yang compatible dengan standar tersebut. Dari sisi hardware, hal tersebut berarti wireless access point dan wireless NIC (Network Interface Card) yang digunakan harus mengenali standar WPA. Sayang, sebagai 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 system operasi yang mendukung WPA secara default. WPA client baru dapat bekerja pada system operasi Windows Server 2003 dan Windows XP. Bagi para pengguna system operasi lainnya belum ditemukan informasi mengenai kemungkinan menginplementasikan WPA.

Tampilan pada WPA bisa dilihat pada interface setup wireless seperti pada gambar 6.



Gambar 6. WPA-PSK/WPA2 =PSK Mixed Mode

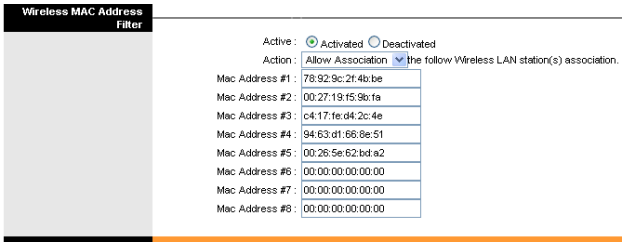
E. Media Access Control (MAC) Address

Setiap peralatan yang terkoneksi ke jaringan memiliki *hardware* addresss yang unik yang disebut *MAC addresss (Media Access Control)*. Alamat ini merupakan 48-bit addresss yang diekspresikan sebagai 12 digit bilangan heksadesimal. 12 digit *hexa number* bisa dipecah menjadi 2 *field*. Bagian MAC yang pertama adalah 24 bit *vendor code*. Bit ini mengindentifikasikan apa yang dibuat vendor untuk peralatan jaringan tertentu. 24 bit terakhir pada *MAC addresss* merupakan serangkaian nomor dari kartu *interface* jaringan. Kita bisa saja mengindentifikasikan *Access point* dengan menggunakanSSID, tapi bagaimana cara mengidentifikasikan *client wireless* secara unik. Kita bisa mengindentifikasikannya dengan *MAC addresss* yang unik. Jadi, denganmembuat daftar *MAC addresss*es yang unik kita bisa membatasi PC yang bisa tersambung ke AP. Ini dikenal dengan istilah *filter MAC addresss*. Jika suatu PC dengan *MAC addresss* yang tak dikenal mencoba konek, maka pc tersebut tidak akan diizinkan untuk tersambung ke AP. Dengan adanya otorisasi menggunakan *MAC addresss* ini, *access point* dapat mengenali masing-masing client yang terkoneksi berdasarkan *MAC addresss* yang dimiliki untuk melakukan otorisasi. *MAC addresss* yang sebelumnya sudah dimasukkan akan memeriksa siapa pengguna yang boleh terkoneksi ke dalam jaringan dan siapa yang tidak.

Tampilan *interface tools Acess Point* pada gambar 4, memperlihatkan daftar *wireless* yang terdeteksi pada target laptop. SSID bertindak sebagai password sederhana dan *MAC addresss* bertindak sebagai nomor personal identifikasi yang sering digunakan untuk memverifikasi client yang berhak untuk koneksi ke *access point*. Dikarenakan standar enkripsi yang ada tidaklah gampang, penyusuf yang pintar bisa mencuri SSID dan *MAC addresss*es untuk tersambung ke LAN sebagai user resmi dengan maksud mencuri *bandwidth*, mengambil atau mendownload file, dan menimbulkan malapetaka di seluruh jaringan.

Pada gambar 4. Tampilan *interface tools Acess Point* yang memfilter *MAC Address* Namun demikian, nyatanya otorisasi dengan *MAC addresss* ini tidak seratus persen menjamin sistem jaringan *wireless* aman. Jaringan masih juga dapat ditembus dengan metode

yang disebut *sniffing*, dimana pengguna yang tidak terotorisasi masih dapat masuk dengan beragam cara. Dengan menggunakan *software sniffing* sederhana yang dapat diperoleh dengan mudah via Internet, pengguna yang tak terotorisasi pun dapat dengan mudah melihat *MAC addresss* yang digunakan masing-masing *client* yang sudah terotorisasi untuk selanjutnya menggunakannya untuk masuk secara ilegal ke dalam jaringan *wireless*. Bisaanya seorang penyusup mengetahui *MAC addresss* yang bisa terkoneksi ke *access point* dari data yang tersimpan di *ACL (Access Control List)* dari *access point*. Sehingga jika ada orang yang dapat mencuri data-data *MAC addresss* yang ada di dalam ACL, ia dapat mengkonfigurasikan *MAC addresss*-nya sesuai dengan *MAC addresss* yang ada di dalam ACL sehingga ia mendapatkan hak akses secara gratis. Tetapi salah satu cara untuk mengurangiresiko ini adalah dengan menyimpan nilai *hash* dari *MAC addresss* di ACL, sehingga walaupun ada orang yang dapat mencuri data-data di ACL, ia tidak dapat mengkonfigurasikan *MAC addrerss*-nya sesuai dengan *MAC addresss* yang ada di ACL tersebut.



Gambar 7. Tampilan *interface tools Acess Point* yang memfilter *MAC Address*

IV. PENUTUP

A. Kesimpulan

Berdasarkan pembahasan dari bab-bab terdahulu, maka dapat ditarik kesimpulan sebagai berikut :

1. Tingkat keamanan pada wireless LAN lebih tinggi dibanding dengan jaringan kabel LAN biasa di mana secara fisik adalah aman sementara jaringan wireless LAN tidak hanya bisa dibatasi oleh dinding di dalam gedung namun jaringan wireless bisa menembus dinding pembatas gedung
2. Untuk penanganan keamanan jaringan wireless di Salsabila Net menggunakan cara menyembunyikan SSID, memanfaatkan kunci WEP, WPA-PSK dan mengimplementasikan fasilitas MAC Address

B. Saran

Berikut adalah saran-saran untuk pengamanan lebih baik :

1. Gunakan password yang kuat dengan mengkombinasikan huruf, angka kemudian secara berkala diganti
2. Mewaspadai pelanggan yang ingin mengetahui atau mencuri data pada system komunikasi sehingga bisa masuk bahkan mengambil data di Salsabila Net
3. Gunakan keamanan Fire Wall, untuk mencegah para hacker atau cracker yang ingin mencoba masuk ke dalam system jaringan

REFERENSI

[1] Ariyus, D, 2006, *Komputer Security*, CV Andi Perbuanan, Yogyakarta
[2] Budi Rahardjo, 2005, *Keamanan Sistem Informasi Berbasis Internet*, http://budi.insan.co.id
[3] Joseph Migga Rizza, 2005, Computer Network Security, Springer,
[4] Munir, R, 2006, *Kriptografi*. Penerbit Informatika, Bandung