BAB VIII
Keamanan Wireless

Pengertian Wi-FI

- Wi-Fi merupakan kependekan dari Wireless Fidelity, yang memiliki pengertian yaitu kelompok standar yang digunakan untuk Jaringan Lokal Nirkabel (Wireless Local Area Networks - WLAN) yang didasari pada spesifikasi IEEE 802.11. Standar terbaru dari spesifikasi 802.11a atau b, seperti 802.11 g, saat ini sedang dalam penyusunan, spesifikasi terbaru tersebut menawarkan banyak peningkatan mulai dari luas cakupan yang lebih jauh hingga kecepatan transfernya

- Awalnya Wi-Fi ditujukan untuk penggunaan perangkat nirkabel dan Jaringan Area Lokal (LAN), namun saat ini lebih banyak digunakan untuk mengakses internet. Hal ini memungkinan seseorang dengan komputer dengan kartu nirkabel (wireless card) atau personal digital assistant (PDA) untuk terhubung dengan internet dengan menggunakan titik akses (atau dikenal dengan hotspot) terdekat.

Standar Perangkat Wi-Fi

- Dalam teknologi Wireless ada dua standar yang digunakan yakni :

1. 802.11 standar indoor yang terdiri dari :

- 802.11 - 2,4 GHz 2 Mbps
- 802.11a - 5 GHz 54 Mbps
- 802.11a - 2X 5 GHz 108 Mbps
- 802.11b - 2,4 GHz 11 Mbps
- 802.11g - 2.4 GHz 54 Mbps
- 802.11n - 2,4 GHz 120 Mbps

2. 802.16 standar outdoor salah satunya adalah WiMAX (World Interoperability for Microwave Access) yang sedang marak penggunaannya di Indonesia.

Kelebihan Wi-Fi

- Kemudahan akses
- Tanpa kabel, praktis dan effisien.
- Dapat digunakan selama 24 jam sehari, 7 hari seminggu tanpa pulsa telpon.
- Koneksi Internet ke Backbone International dan koneksi ke Indonesia Internet Exchange (IIX)

Kekurangan Wi-Fi

- Biaya peralatan mahal
- Delay yang sangat besar
- Kesulitan karena masalah propagasi radio
- Mudah untuk terinterferensi
- Kapasitas jaringan kecil karena keterbatasan spektrum (pita frekuensi yang tidak dapat diperlebar)
- Keamanan/kerahasiaan data kurang terjamin

Macam Perangkat Wi-Fi

- Access Point

Merupakan pusat dari client atau node yang terhubung ke jaringan dengan menggunakan gelombang radio atau wireles. Untuk memiliki jaringan Wi-Fi, terlebih dahulu harus terpasang Access Point sebagai pusat akses jaringan tersebut.

- Wireless Adapter untuk Desktop

Perangkat ini yang digunakan untuk 'berkomunikasi' secara wireless, dengan Access Point menggunakan desktop.

- Wi-Fi PCI Adapter

Dipasangkan pada Slot PCI pada motherboard, di dalam CPU. Perangkat ini adalah wi-fi internal adapter.

- Wi-fi USB Adapter

Merupakan External Adapter yang dihubungkan langsung melalui port USB.

Linksys WiFi USB Adapter

- PCMCIA dan ISA Card

Jika kita sudah memiliki wi-fi PCMCIA dan tidak ingin membeli perangkat baru untuk Wi-Fi, dapat menggunakan ISA / PCI PCMCIA Converter.

PCI PCMCIA Coverter

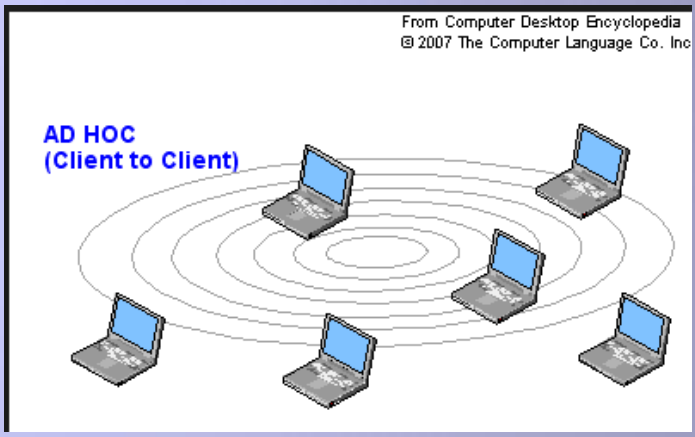
- **Wireless Router**

Wireless router adalah perangkat yang melakukan fungsi sebuah router , tetapi juga mencakup fungsi sebuah titik akses nirkabel dan switch jaringan . Mereka umumnya digunakan untuk memungkinkan akses ke internet atau jaringan komputer tanpa memerlukan koneksi kabel. Hal ini dapat berfungsi dalam kabel LAN , WLAN , atau Wireless.

Mode Jaringan Wi-Fi

- **Adhoc**
- Sistem Adhoc bisa disebut sistem peer to peer, dalam arti satu computer dihubungkan ke 1 computer dengan saling mengenal SSID. Bila digambarkan mungkin lebih mudah membayangkan sistem direct connection dari 1 computer ke 1 computer lainnya dengan mengunakan Twist pair cable tanpa perangkat HUB. Jadi terdapat 2 computer dengan perangkat WIFI dapat langsung berhubungan tanpa alat yang disebut access point mode. Pada sistem Adhoc tidak lagi mengenal sistem central (yang biasanya difungsikan pada Access Point). Sistem Adhoc hanya memerlukan 1 buah computer yang memiliki nama SSID atau sederhananya nama sebuah network pada sebuah card/computer.

Mobile PCs can use Ad-Hoc WiFi to create their own peer-to-peer network (without an Internet connection).



- **Infrasructure**
- Sistem Infra Structure membutuhkan sebuah perangkat yaitu Access point bila mengunakan jenis Wireless Network dengan perangkat PCI card. Access Point berfungsi sebagai pengatur lalu lintas data, sehingga memungkinkan banyak Client dapat saling terhubung melalui jaringan (Network).

Keamanan Jaringan Wireless

- Saat ini perkembangan teknologi wireless sangat signifikan sejalan dengan kebutuhan sistem informasi yang mobile. Banyak penyedia jasa wireless seperti hotspot komersil, ISP, Warnet, kampus-kampus maupun perkantoran sudah mulai memanfaatkan wireless pada jaringan masing masing, tetapi sangat sedikit yang memperhatikan keamanan komunikasi data pada jaringan wireless tersebut.

- Jaringan Wireless memiliki lebih banyak kelemahan dibandingkan dengan jaringan kabel.

Kelemahan Jaringan Wireless

1. Kelemahan Wireless Pada Lapisan Fisik

Wifi menggunakan gelombang radio pada frekwensi milik umum yang bersifat bebas digunakan oleh semua kalangan dengan batasan batasan tertentu. Setiap wifi memiliki area jangkauan tertentu tergantung power dan antenna yang digunakan. Tidak mudah melakukan pembatasan area yang aktifitas aktifitas antara lain:

a.Interception atau penyadapan

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

b.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 yangmemutuskan koneksi saat itu.

Kelemahan Jaringan Wireless

c.Jamming

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

d.Locating Mobile Nodes

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

e.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 diperlukan access control yang baik.

f. Hijacking

Serangan MITM (Man In The Middle) yang dapat terjadi pada wireless karena berbagai kelemahan protokol tersebut sehingga memungkinkan terjadinya hijacking atau pengambillalihan komunikasi yang sedang terjadi dan melakukan pencurian atau modifikasi informasi.

Kelemahan Jaringan Wireless

2. Kelemahan 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 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).

Solusi Jaringan Wireless

Kelemahan jaringan wireless secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan.

Berikut adalah kegiatan atau aktifitas yang dilakukan untuk pengamanan jaringan wireless

- Menyembunyikan SSID
- VPN dan Firewall
- Menggunakan Enkripsi
- Ganti Password Administrator standar
- Matikan AP Saat Tidak Dipakai
- Ubah default SSID
- Memakai MAC Filtering
- Mengisolasi Wireless Network dari LAN
- Mengontrol Signal Wireless
- Memancarkan Gelombang pada Frekuensi yang Berbeda
- WEP (Wired Equivalent Privacy)
- WPA(WI-FI Protected Access)
- MAC Filtering

Solusi Jaringan Wireless

Kelemahan jaringan wireless secara umum dapat dibagi menjadi 2 jenis, yakni kelemahan pada konfigurasi dan kelemahan pada jenis enkripsi yang digunakan.

Berikut adalah kegiatan atau aktifitas yang dilakukan untuk pengamanan jaringan wireless

- WEP (Wired Equivalent Privacy)
- WPA(WI-FI Protected Access)
- MAC Filtering

WEP (Wired Equivalent Privacy)

WEP adalah suatu metode pengamanan jaringan nirkabel, merupakan standar keamanan & enkripsi pertama yang digunakan pada wireless

Enkripsi WEP menggunakan kunci yang dimasukkan (oleh administrator) ke klien maupun access point. Kunci ini harus cocok dari yang diberikan akses point ke client, dengan yang dimasukkan client untuk authentikasi menuju access point, dan WEP mempunyai standar 802.11b.

Alasan Memilih WEP dan Fungsi WEP

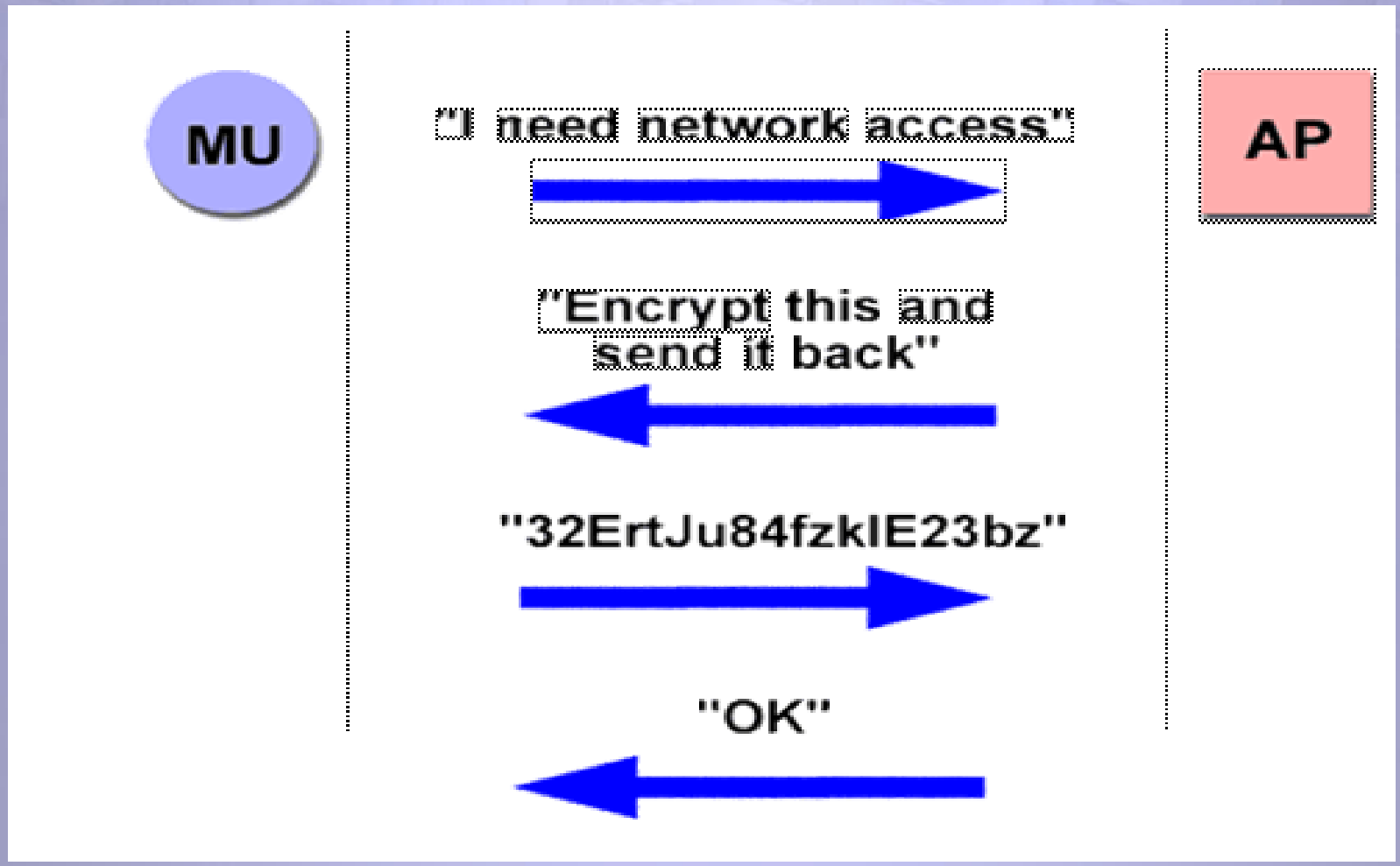
WEP merupakan sistem keamanan yang lemah. Namun WEP dipilih karena telah memenuhi standar dari 802.11 yakni

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

- WEP ini dapat digunakan untuk verifikasi identitas pada authenticating station.

- WEP dapat digunakan untuk data encryption.

Proses WEP


MU
"I need network access"
AP
"Encrypt this and send it back"
"32ErtJu84fzklE23bz"
"OK"

Kelebihan WEP

Saat user hendak mengkoneksikan laptopnya, user tidak melakukan perubahan setting apapun, semua serba otomatis, dan saat pertama kali hendak browsing, user akan diminta untuk memasukkan Username dan password

Hampir semua komponen wireless sudah mendukung protokol ini.

Kelemahan WEP

- 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)

WPA(WI-FI Protected Access)

Suatu sistem yang juga dapat diterapkan untuk mengamankan jaringan nirkabel.

Metoda pengamanan dengan WPA ini diciptakan untuk melengkapi dari sistem yang sebelumnya, yaitu WEP.

WPA mengimplementasikan layer dari IEEE, yaitu layer 802.11i. Nantinya WPA akan lebih banyak digunakan pada implementasi keamanan jaringan nirkabel.

WPA(WI-FI Protected Access)

Teknik WPA didesain menggantikan metode keamanan WEP, yang menggunakan kunci keamanan statik, dengan menggunakan TKIP (Temporal Key Integrity Protocol) yang mampu berubah secara dinamis.

Protokol TKIP akan mengambil kunci utama sebagaistarting point yang kemudian secara reguler berubah sehingga tidak ada kunci enkripsi yang digunakan dua kali.

Kelebihan WPA

Meningkatkan enkripsi data dengan teknik 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 enkripsi/dekripsi yang lebih lama dan data overhead yang lebih besar.

Dengan kata lain, proses transmisi data akan menjadi lebih lambat dibandingkan bila Anda menggunakan protokol WEP

Belum semua wireless mendukung, biasanya butuh upgrade firmware, driver atau bahkan menggunakan software tertentu

MAC Filter

MAC Address Filtering merupakan metoda filtering untuk membatasi hak akses dari MAC Address yang bersangkutan

Hampir setiap wireless access point maupun router difasilitasi dengan keamanan MAC Filtering.

MAC filters ini juga merupakan metode sistem keamanan yang baik dalam WLAN, karena peka terhadap jenis gangguan seperti:

- pencurian pc card dalam MAC filter dari suatu access point
- sniffing terhadap WLAN

Fungsi MAC Filter

MAC filter fungsinya untuk menseleksi komputer mana yang boleh masuk kedalam jaringan berdasarkan MAC Address. Bila tidak terdaftar, tidak akan bisa masuk ke jaringan

MAC filter Address akan membatasi user dalam mengakses jaringan wireless. Alamat MAC dari perangkat komputer user akan didaftarkan terlebih dahulu agar bisa terkoneksi dengan jaringan wireless,

Kelemahan MAC Filter

MAC Address bisa di ketahui dengan software kisMAC. Setelah diketahui MAC Address bisa ditiru dan tidak konflik walau ada banyak MAC Address sama terkoneksi dalam satu AP

Kesimpulan

Banyaknya wireless LAN yang aktif dengan konfigurasi default akan memudahkan para hacker dapat memanfaatkan jaringan tersebut secara ilegal. Konfigurasi default dari tiap vendor perangkat wireless sebaiknya dirubah settingnya sehingga keamanan akses terhadap wifi tersebut lebih baik. Keamanan jaringan Wireless dapat ditingkatkan dengan cara tidak hanya menggunakan salah satu cara mensetting yang sudah dibahas diatas, tetapi dapat menggunakan kombinasi beberapa teknik sehingga keamanan lebih terjamin.

Merci bien
ありがとう
Matur Nuwun
Hatur Nuhun
Obrigado
Dank
Thanks
Matur se Kelangkong
Syukron
Kheili Mamnun
ευχαριστιες
Danke
Grazias
谢谢
Terima Kasih


Irawan_afrianto@yahoo.com

Irawan.afrianto

@Irawan_afrianto

+628170223513