Arsitektur untuk Mengamankan Jaringan Nirkabel

Eka Santika Misbahudin
Officer Development Program (ODP)
Bank Bukopin - ITB

Urusan Dukungan Sistem dan Komputer (UDSK)
PT. Bank Bukopin
Jalan MT Haryono Kav 50-51 Jakarta 12770

E-mail : eka.santika@bukopin.co.id

Abstrak

Pada jaringan nirkabel, masalah keamanan memerlukan perhatian yang lebih serius, mengingat media transmisi data adalah udara yang bersifat broadcast. Sehingga diperlukan mekanisme keamanan yang tangguh untuk mendapatkan tingkat keamanan setara dengan jaringan yang menggunakan kabel. Masalah keamanan pada jaringan tidak akan bisa lepas dari dua konsep yaitu autentikasi (*access contro*l) dan enkripsi (*data protection*). Standar yang dipakai oleh jaringan nirkabel di seluruh dunia adalah IEEE 802.11, walaupun tidak disiapkan untuk tingkat keamanan yang tinggi dengan hanya mendukung algoritma enkripsi WEP (*Wired Equivalent Privacy*), dan proses otentikasi yang juga memiliki kelemahan. Maka pada journal ini akan dibahas tentang cara menutupi kelemahan-kelemahan yang ada pada standard IEEE 802.11.

***Kata kunci**:wireless, keamanan, jaringan nirkabel, authentication*

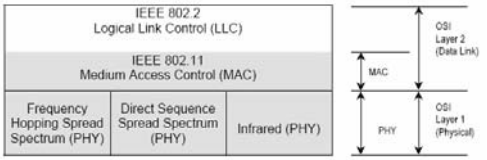
1. Pendahuluan

Sudah bukan rahasia lagi kalau ternyata standar jaringan nirkabel IEEE 802.11 yang menggunakan enkripsi WEP memiliki kelemahan yang memungkinkan seorang hacker mengetahui kode enkripsinya. Akan tetapi bukan sesuatu yg tidak memungkinkan untuk membuat jaringan nirkabel bisa mempunyai tingkat keamanan yang tinggi dengan mengkombinasikan pengukuran keamanan tradisional, keamanan standar terbuka dari jaringan nirkabel dan keamanan yang dimiliki perangkat itu sendiri. Perbaikan untuk menyikapi kelemahan pada WEP telah dikembangkan suatu teknik pengamanan baru yang disebut dengan WPA (*Wi-FI Protected Access*). Teknik WPA ini adalah model pengamanan yang kompartibel dengan draft standar 802.11i yang masih dalam proses pengembangan untuk menggantikan standar 802.11. Pada teknik WPA ini selain pengembangan dari proses enkripsi juga menambahkan proses *user authentication* yang tidak ada pada pada WEP. Proses otentifikasi pada WPA menggunakan 802.1X dan EAP (*Extensible Authentication Protocol*).

2. Standar IEEE 802.11

Standar IEEE 802.11 mendefinisikan *Medium Access Control (MAC)* dan *Physical (PHY)* untuk jaringan nirkabel. Standar tersebut menjelaskan jaringan local dimana peralatan yang terhubung dapat saling berkomunikasi selama berada dalam jarak yang dekat satu sama lain. Standar ini hampir

sama dengan *IEEE 802.3* yang mendefinisikan *Ethernet*, tapi ada beberapa bagian yang khusus untuk transmisi data secara nirkabel.



Gambar 2.1: Layer 802.11

Pada Standar 802.11 mendefinisikan tiga tipe dari *physical layer* seperti pada gambar 1-1, yaitu *Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DHSS) dan* infra merah. Infra merah jarang sekali dipakai karena jangkauannya yang sangat dekat.

Tidak semua dari keluarga 802.11 menggunakan *Physical Layer* yang sama dan mendapatkan kecepatan transmisi data yang sama.

802.11	2.4 GHz FHSS, DHSS, Infrared 1 atau 2 Mbps
802.11a	5 Ghz Orthogonal Frequancy Division Multiplexing (OFDM) 54 Mbps
802.11b	2.4 Ghz DSSS 11 Mbps
802.11g	2.4 Ghz 54 Mbps

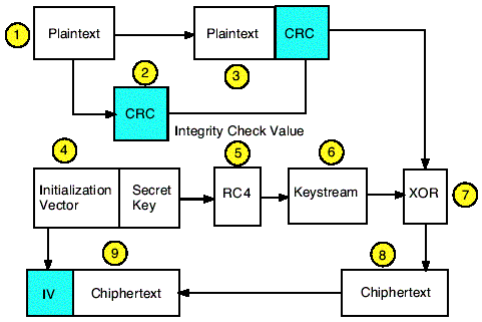
Tabel 2.1. Teknologi 802.11

802.11b paling banyak digunakan saat ini, karena cepat dan mudah diimplemtasikan, dan tersedia banyak sekali produk yang tersedia dipasaran. Mendukung kecepatan transmisi data sampai 11 Mbps, tetapi jika sinyal radio melemah, maka kecepatan akan diturunkan ke 5.5 Mbps, 2 Mbps, dan 1 Mbps untuk menjamin agar komunikasi tidak terputus. 802.11b seringkali disebut juga *Wi-Fi (Wireless Fidelity)* karena *Wi-Fi Alliance* yang bertanggung jawab untuk penngetesan dan sertifikasi untuk dapat bekerja dengan produk jaringan yang berdasarkan 802.11 lainnya

3. WEP *(Wired Equivalent Privacy)*

WEP (*Wired Equivalent Privacy*) adalah standar keamanan pada protokol 802.11, *WEP* mengenkripsi paket pada layer 2 *OSI* yaitu *MAC* (*Media Access Control*). Hanya *Wireless Client* yang mempunyai kunci rahasia yang sama dapat terkoneksi dengan akses poin. Setiap *Wireless Client* yang tidak mempunyai kunci rahasia dapat melihat lalu lintas data dari jaringan, tetapi semua paket data terenkripsi. Karena ekripsi hanya pada layer 2 (data link) maka hanya link nirkabel yang di proteksi.

WEP mengenkripsi traffic data dengan menggunakan stream *cipher* yang disebut dengan *RC4*, metode enkripsinya adalah simetrik, dimana *WEP* menggunakan kunci yang sama baik untuk mengenkripsi data maupun untuk mendekripsi data. RC4 akan dibuat secara otomatis setiap paket data yang baru untuk mencegah masalah sinkronisasi yang disebabkan oleh paket yang hilang.



gambar 2.2 : mekanisme enkripsi *WEP*

4. Standard 802.11 i

Untuk memperbaiki kelemahan pada standard IEEE 802.11 kelompok kerja IEEE 802.11 *Instituted Task Group 'i'* (*TGi*) membuat suatu standar untuk memperbaiki kelemahan security pada 802.11 seperti autentikasi user dan enkripsi.

Komponen ada 802.11i termasuk *IEEE 802.1x* port-based *authentication*, *Temporal Key Integrity Protocol* (*TKIP*), *Advanced Encryption standard (AES)* logaritma enkripsi pengganti enkripsi *WEP*, *RC4*, *key hierarchy* dan kelebihan pada sisi management, *cipher* dan negosisasi autentikasi.

Standar 802.11i diperlukan baik pada mode *infrastructure-based(BSS)* maupun pada *ad-hoc (IBSS)*, dan termasuk dua pengembangan utama yaitu *Wi-Fi Protected Access (WPA)* dan *Robust Security Network (RSN)*.

4.1. *Wi-Fi Protected Access (WPA)*

Meskipun standar 802.1x dapat memperbaiki kelemahan pada static *WEP*, tetapi terbatas pada standar authentikasi bukan pada kelemahan enkripsi dari *WEP*. Konsekwensinya selama 802.11i dikembangkan, dan kebutuhan keamanan pada jaringan nirkabel, bagian dari 802.11i telah dirilis dibawah pengawasan *Wi-Fi alliance* untuk mengganti standar keamanan 802.11. *Wi-Fi Protected Access (WPA)*, yang berbasiskan komponen 802.11i telah stabil dan dapat diimplementasikan pada jaringan 802.11 dan *client* yang telah ada dengan mengupgrade software. *WPA* telah diperkenalkan pada bulan November 2002 dan akan kompatibel dengan standar *802.11i* yang akan datang.

WPA yang ada sekarang hanya mendukung mode *infrastruktur (ad-hoc mode* akan didukung saat standar final dirilis) dan komponen yang terdapat pada 802.11i saat ini adalah:

- Mekanisme autentikasi *based on 802.1x*
- Algoritma *key management*
- Enkripsi data menggunakan *TKIP*
- *Cipher* dan negosisasi autentikasi

4.2. *Temporal Key Integrity Protocol (TKIP)*

WPA menggunakan 802.1x untuk autentikasi dan menambah elemen enkripsi yang lebih kuat dari draft 802.11i, *Temporal Key Integrity Protocol (TKIP)*. *TKIP* menanggulangi kelemahan algoritma *WEP* tetapi tetap dapat dijalankan ada hardware 802.11 biasa.

TKIP bekerja seperti pembungkus *WEP*, menambahkan kelebihan-kelebihan kepada *WEP* cipher engine. *TKIP* menambah IV (*Initialization Vector*) dari 24 bit pada *WEP* menjadi 48 bit, yang merupakan kelemahan dari *WEP*. Penambahan IV menjadi 48 bit menambah jumlah kemungkinan *share*d *keys* untuk pencegahan serangan balik. Beberapa vendor mengimplementasi *WEP* menggunakan IV yang sama untuk semua

paket selamanya atau merotasi *WEP key* selama periode waktu tertentu, lain hanya dengan *TKIP*, menggunakan aturan yang lebih baik untuk meyakinkan bahwa IV tidak bisa digunakan kembali.

TKIP juga menambahkan *Message Integrity Code (MIC)* yang dinamakan *Michael*. *Michael* adalah *cryptographic checksum* yang melindungi dari serangan *forgery*. Pengirim packet menambah 8 bytes (*MIC*) ke packet sebelum enkripsi dan mengirim packet. Penerima mendekript paket dan memeriksa *MIC* sebelum menerima paket, jika *MIC* tidak cocok maka paket akan di drop.

4.3. *Robust Security Network (RSN)*

Seperti telah dijelakan sebelumnya, *WPA* mengkombinasikan beberapa elemen dari standar 802.11i yang telah stabil dan dapat digunakan pada jaringan 802.11 dengan melakukan upgrade software. Oleh sebab itu *WPA* merupakan solusi yang sangat baik sementara 802.11i dikembangkan.

Robust Security Network (RSN) adalah nama yang digunakan untuk mengindentifikasi network pada standar 802.11i dan dipersiapkan untuk solusi keamanan jangka panjang untuk jaringan wireless 802.11.

RSN terdiri dari dua bagian dasar.
Security association management
- prosedur negosiasi *RSN*, membentuk context *security*
- autentikasi *IEEE 802.1x* mengganti autentikasi IEEE 802.11
- *key management IEEE 802.1x* menyediakan cryptographic keys

Mekanisme Data Privacy
- *TKIP* (Protokol perbaikan *WEP*)
- *AES-based protocol* (*long term*)

Menggunakan negosisasi secara dynamic, 802.1x, *EAP* dan AES, *RSN* lebih kuat dibanding dengan *WEP* dan *WPA*.

5. Penerapan Pengamanan

Dari paparan diatas, sebenarnya kita bisa langsung menerapkan standar 802.11i di lingkungan jaringan nirkabel kita, akan tetapi hal ini tidak semudah yang dibayangkan karena terkait dengan perangkat keras dan perangkat lunak yang bisa mendukung standar tersebut, tentunya akan menimbulkan pengeluaran dana untuk bisa upgrade atau mungkin membeli perangkat lunak dan keras.

Untuk menghindari hal tersebut ada beberapa alternatif untuk mengamankan jaringan nirkabel kita.

5.1 Otentifikasi dan Enkripsi

Otentifikasi dapat dipakai pada beberapa tingkatan dengan menggunakan kombinasi dari beberapa metoda. Sebagai contoh dengan menggunakan EAP-TLS yang otentifikasinya berdasarkan pada standar keamanan 802.1x. EAP-TLS adalah IETF standar untuk metode autentikasi (RFC2716) yang didukung oleh semua vendor. Menggunakan protocol TLS (Transort Layer Security) (RFC 2246) dimana standar paling baru dari protocol SSL (secure Socket Layer), digunakan untuk keamanan laulintas data pada web dan dibuat pertama kali oleh netscape. EAP-TLS menggunakan Remote Authenticartion Dial-in User Service (RADIUS) untuk mengontrol user mengakses jaringan nirkabel. Selain itu solusi EAP-TLS ini menggunakan sertifikat digital untuk otentifikasi dari sisi RADIUS server maupun

client. EAP-TLS dibuat berdasarkan pada X.509 certificates untuk menangani autentikasi dan membutuhkan PKI (Public Key Infrastructure). *Supplicant* harus mempunyai sertifikat yang akan divalidasi oleh *authentication server.*

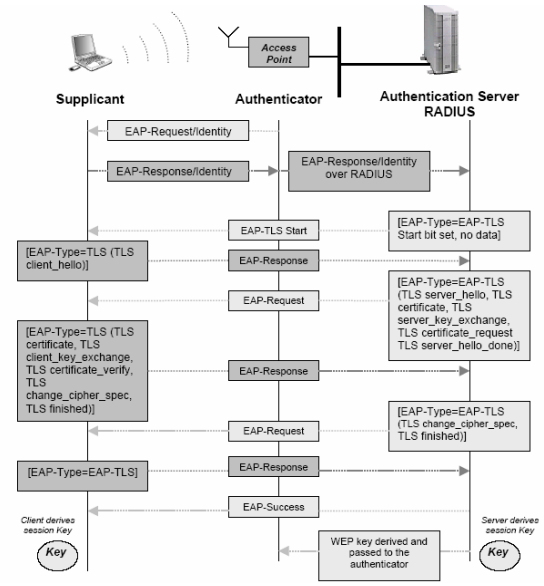
EAP-TLS menyediakan mutual authentication yang kuat antara *supplicant* dan *authentication server* (hal ini hanya benar jika kedua bagian data memvalidasi sertifikat lainnya.

EAP-TLS mengenerate dynamic WEP (*shared secret*) setelah proses pertukaran, sehingga *supplicant* dan *authenticator* dapat melakukan komunikasi yang aman berdasarkan per-packet authenticated.Untuk itu dibutuhan pembuatan PKI (*Public Key Infrastructure*) untuk membuat sertifikat tersebut diatas. Aplikasi untuk membuat sertifikat ini diataranya openssl

Openssl adalah *software open source* untuk mengimplementasikan protokol *Secure Socket Layer* (SSL) dan *Transport Layer Security* (TLS) dan sebagai *Certification Authority* (CA) bagi *server* dan *client.*

Proses authentikasi EAP-TLS berlangsung setelah *supplicant* mengirim pesan EAP-Response *Identity* ke *access poin*t, dengan EAP-request, *authentication server* mengirim sertifikat keada supplicant dan meminta sertifikat dari supplicant. Setelah itu supplicant memvalidasi sertifikat server dan sebagai bagian dari respon EAP, mempersiapkan sertifikat dan juga memulai negosiasi untuk spesifikasi kriptografi.

RADIUS Server memvalidasi sertifikat client dan merespon dengan spesifikasi kriptografi untuk session.



Gambar 5.1 : proses autentikasi EAP-TLS

Proses selanjutnya TLS *handshake* antara authentication server dan client, adalah mengenerate pre-master secret, mengenkripsinya dengan server public key dan mengirim pre-master secret ke server untuk mengenerate master secret yang digunakan untuk membuat secure chanel.

Oleh sebab itu meskipun TLS telah benar-benar mensetup chanel terenkripsi antara authentication server dengan supplicant, chanel ini tidak digunakan (supplicant ingin berkomunikasi dengan authenticator, tidak dengan authentication server). Instead sebuah key dibuat selama proses session TLS untuk chanel tersebut yang dikirim kepada authenticator. Kemudian supplicant yang telah mengetahui TLS secret key) dan authenticator menggunakan key tersebut untuk mengamankan komunikasi dengan enkripsi WEP.

5.2 VPN dan Firewall

Option lain bisa di sediakan untuk mengamankan jaringan nirkabel ini. Desain dengan keamanan yang tinggi didalamnya harus ada minimal *authentication server* seperti radius, algoritma enkripsi seperti IPSec yang berjalan diatas VPN (Virtual Private Network) dan *access point* yang bisa melakukan pembatasan akses. Selain itu dapat juga ditambahan pengontrolan user atau group untuk bisa akses ke jaringan internal yang diatur dalam satu *access policy* pada firewall atau pada VPN. Penggunaan reservasi DHCP (Dynamic Host Configuration Protocol) dan IP addressnya di tunnel ke VPN yang di berikan kepada tiap user bisa membantu memberikan akses hanya kepada klien yang membutuhkan saja

6. Kesimpulan

Jaringan nirkabel yang aman bisa memungkinkan dengan beberapa teknik dan teknologi. Walaupun standar baru (802.11i) sudah ada dan terbukti lebih aman dibanding standar sebelumnya, hal ini tidak mudah apabila merubah jaringan nirkabel yang sudah ada.

Melakukan migrasi hardware dan implementasi WPA dapat dibayangkan sebagai sebuah pekerjaan yang sangat besar. Tetapi hal tersebut bukanlah sesuatu yang harus dilakukan pada saat yang bersamaan. *Wireless Access Points* dapat mendukung WPA dan WEP secara bersamaan. Hal ini memungkinkan migrasi perlahan ke implementasi WPA.

Setelah melakukan pengecekan dan kebutuhan dari keamanan, beberapa kombinasi dari opsi yang ada pada makalah ini ataupun yang tidak ada bisa diimplementasikan untuk mengamankan jaringan nirkabel lama kita. Dan dengan pemilihan yang tepat pada pengukuran keamanan, kerahasian data bisa terjamin ketika jaringan nirkabel ini ada.

[1] N. Borisov, I. Goldberg and D. Wagner, *Security of the WEP Algorithm,*http://www.issac.cs.berkeley.edu/Isaac/wep-faq.html, diakses tgl 17 desember 2005 pukul 20.00

[2] R. Flickenger, *Building Wireless Community Networks*, Second Edition O'Really 2003

[3] A. Mishra, and W. A. Arbaugh. *An Initial Security Analysis of the IEEE 802.1x Standard*, Department of Computing Science, University of Maryland, http://www.cs.umd.edu/. Diakses tgl 17 desember 2005.

[4] R. Munir. *Diktat Bahan Kuliah IF5054 Kriptografi*, 2005.

[5] C. Rigney, S. Willens, A. Rubens and W. Simpson. *Remote Authentication Dial-In User Service.* IETF RFC 2865, Juni 2001.