ANALISA IMPLEMENTASI VoIP BERBASIS SIP PADA JARINGAN WIRELESS LAN DENGAN KEMAMPUAN AUTO AUTHENTICATION SERVICE

ANALYSIS OF SIP BASED VoIP IMPLEMENTATION ON WIRELESS LAN NETWORK WITH AUTO AUTHENTICATION SERVICE ABILITY

Muhammad Hasan[1], Tody Ariefianto W, ST., MT[2], Istikmal, ST., MT[3]

Prodi S1 Teknik Telekomunikasi, Fakultas Teknik, Universitas Telkom
[1]muhhasan.1311@gmail.com [2]ariefianto@telkomuniversity.ac.id [3]istikmal@ telkomuniversity.ac.id

ABSTRAK

Dalam komunikasi layanan *wireless* LAN, autentikasi merupakan hal biasa yang sering kita temui. Autentikasi digunakan untuk membatasi akses hanya kepada pelanggan yang terdaftar. Begitu pula dengan layanan komunikasi VoIP yang juga membutuhkan autentikasi sebelum kita dapat menggunakan layanan tersebut.

Pada tugas akhir ini dilakukan pengujian proses *auto* autentikasi voip. Proses *auto* autentikasi pada penelitian ini melibatkan server RADIUS sebagai server autentikasi EAP-SIM dan server Asterisk sebagai server VoIP. Agar autentikasi pada RADIUS dapat digunakan secara otomatis sebagai autentikasi pada Asterisk maka baik RADIUS dan Asterisk harus terhubung dengan mysql. Asterisk *realtime* merupakan metode baru dari Asterisk yang dapat digunakan agar semua data autentikasi disimpan ke dalam tabel *database*. Dengan menggunakan *Trigger* SQL pada tabel RADIUS maka setiap perubahan yang terjadi pada tabel RADIUS akan tersalin secara otomatis ke tabel Asterisk.

Hasil dari pengujian ini didapat bahwa rata-rata lama waktu proses autentikasi di sisi server voip adalah 1,614 ms. Dan rata-rata waktu yang dibutuhkan oleh *supplicant* agar terhubung ke jaringan melalui autentikasi EAP-SIM sampai dengan terhubung ke voip server adalah 0.760699 detik.

Kata kunci: *EAP-SIM, Challenge-response, Supplicant, RADIUS, Asterisk*

ABSTRACT

In the wireless LAN communication services, authentication is common that we often encounter. Authentication is being used to restrict access only to registered customers. Similarly, VoIP communications services also require authentication before we can use the service.

In this final project, a test upon voip auto authentication process. Auto authentication process in this study involves the RADIUS server as the authentication server and the EAP-SIM server Asterisk as a VoIP server. In order for the RADIUS authentication can be used automatically as the authentication on Asterisk, both the RADIUS Asterisk and Asterisk must be connected to mysql. Asterisk realtime is a new method of Asterisk that can be used to store all authentication data to a database table. Then by using trigger, we can copy RADIUS data from its table to Asterisk for each changes that occur in it.

The results of the experiments shows that the average time the server-side authentication voip is 1.614 ms. And the average time taken by the supplicant to connect to the network via EAP-SIM authentication and to connect to the VoIP server is 0.760699 seconds.

Keywords*: EAP-SIM, Challenge-response, Supplicant, RADIUS, Asterisk*

1. Pendahuluan

Dalam komunikasi layanan *wireless* LAN, autentikasi merupakan hal biasa yang sering kita temui. Autentikasi digunakan untuk membatasi akses hanya kepada pelanggan yang terdaftar. Pada layanan komunikasi VoIP juga membutuhkan autentikasi sebelum kita dapat menggunakan layanan tersebut. Agar aplikasi VoIP bisa digunakan *administrator* harus mendaftarkan data *user* ke dalam server VoIP yang digunakan dan data *user* tersebut yang akan dipakai oleh pengguna di VoIP *client*.

Untuk memudahkan proses autentikasi pada server VoIP maka autentikasi dilakukan secara otomatis dengan memanfaatkan metode autentikasi EAP-SIM yang digunakan sebagai autentikasi agar klien bisa terhubung ke jaringan. EAP-SIM merupakan protokol autentikasi yang digunakan untuk proses autentikasi pelanggan seluler pada jaringan *wireless*. Metode autentikasi ini menggunakan kunci *triplets* dalam kartu SIM sebagai kunci autentikasi sehingga dapat

menentukan siapa saja yang diperbolehkan mengakses jaringan *wireless* tersebut. Proses *auto* autentikasi pada penelitian ini melibatkan server RADIUS sebagai server untuk autentikasi EAP-SIM dengan server Asterisk sebagai server VoIP.

Agar autentikasi pada RADIUS dapat digunakan secara otomatis sebagai autentikasi pada Asterisk maka baik RADIUS dan Asterisk harus terhubung dengan mysql. Asterisk *realtime* merupakan metode baru dari Asterisk yang dapat digunakan agar semua data autentikasi disimpan ke dalam tabel *database*. Baik tabel RADIUS dan tabel Asterisk dapat dihubungkan dalam satu *database* pada mysql sehingga memungkinkan proses penyalinan data secara otomatis terjadi. Dengan menggunakan *Trigger* SQL pada tabel RADIUS maka setiap perubahan yang terjadi akan tersalin secara otomatis ke tabel Asterisk. Sehingga data *user* yang dimasukkan sebagai autentikasi dari RADIUS akan tersalin otomatis dan juga digunakan sebagai autentikasi dari Asterisk.

2. Dasar Teori

2.1 VoIP *Overview*

Voice over Internet Protocol atau disingkat VoIP, dikenal juga dengan sebutan IP *Telephony*. VoIP didefinisikan sebagai suatu sistem yang menggunakan jaringan *Internet* untuk mengirimkan data paket suara dari suatu tempat ke tempat yang lain menggunakan perantara protokol IP. Sehingga perbedaan VoIP dengan telepon tradisional adalah masalah infrastrukturnya.

2.2 *Session Initiation Protocol* (SIP)

SIP adalah protokol yang dikeluarkan oleh IETF (*International Engineering Task Force*). Di dalam IP dan telepon tradisional, selalu dibedakan dengan jelas dua tahap panggilan *voice*. Tahap pertama adalah *Call Setup* yang mencakup semua detail keperluan agar dua perangkat telepon dapat berkomunikasi. Tahap selanjutnya adalah transfer data dimana *call setup* sudah terbentuk. Di dalam VoIP, SIP adalah *protocol call setup* yang beroperasi pada layer aplikasi. Protokol lain dengan fungsi yang sama adalah H.323 yang dikeluarkan oleh ITU[13].

SIP sangat fleksibel dan didesain secara general untuk *setup real-time multimedia sessions* antara *group participants*. Sebagai contoh, selain untuk *call telephone* yang sederhana, SIP dapat juga digunakan untuk *set-up conference video* dan audio atau *instant messaging*. SIP tidak hanya meng-*handle call setup*, tetapi juga memiliki kemampuan fungsi-fungsi lain untuk mendukung layanan VoIP.

Tabel 2.1 Fungsi SIP [13]

Fungsi	Keterangan
Registrasi dan identifikasi lokasi user	*End points (IP Phones)* melakukan notifikasi lokasi ke *SIP proxies*. SIP juga menentukan *end point* mana yang akan berpartisipasi dalam panggilan.
Ketersediaan User	SIP digunakan oleh *end point* untuk menentukan apakah panggilan yang datang dijawab atau tidak.
Kemampuan User	SIP digunakan *end point* melakukan negosiasi dengan kemampuan network, seperti penggunaan *voice codec*.
Set-up Session	SIP memberitahu ke *end point* bahwa *end point* harus *ringing*, hal ini terkit dengan fitur seperti *conference*.
Management Session	SIP digunakan untuk *transfer calls*, memutuskan *calls*, dan merubah parameter panggilan di tengah *session*.

2.3 *Wireless* LAN

Wireless LAN adalah sebuah standar IEEE 802.11 dalam jaringan komputer yang memanfaatkan media transmisi gelombang radio. WLAN menggunakan frekuensi spectrum tak berlisensi 2,4 GHz dan 5 GHz[5]. Spesifikasi yang termasuk IEEE 802.11 dijelaskan pada Tabel 2.2 berikut.

Tabel 2.2 Spesifikasi IEEE 802.11 [5]

No	Teknologi	Kecepatan	Transmisi	Frekuensi
1	802.11	1 atau 2 Mbps	FHSS atau DSSS	2,4 GHz
2	802.11a	54 Mbps	OFDM	5 GHz
3	802.11b	11 Mbps	DSSS	2,4 GHz
4	802.11g	54 Mbps	OFDM	2,4 GHz
5	802.11n	100 Mbps	OFDM	2,4 GHz

Penggunaan frekuensi pada WLAN berkisar antara 2.412 MHz sampai 2.484 MHz. Kanal yang dapat digunakan dalam satu cakupan WLAN adalah maksimal tiga kanal dengan jarak antar kanal adalah 25 MHz[1].

2.4 Standar Keamanan WiFi

2.4.1 Standar IEEE 802.1X / EAP

IEEE 802.1x atau *port based authentication* merupakan standar yang digunakan mengontrol dua jenis *port logical* yaitu *controlled ports* dan *uncontrolled port*. Sebelum autentikasi berhasil,

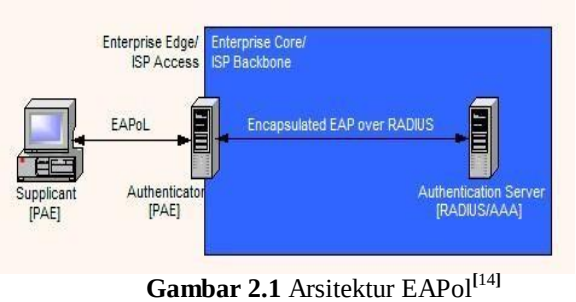
hanya *port* dengan jenis *uncontrolled* yang dibuka. Trafik yang diperbolehkan hanyalah EAPOL sedangkan selain itu akan ditolak oleh *authenticator*. Setelah *supplicant* melakukan auntentikasi dan berhasil, *port* jenis *controlled* dibuka sehingga *supplicant* dapat mengakses LAN secara biasa. [4]

EAP adalah enkapsulasi simpel yang dapat dijalankan di semua link layer. 3 komponen utama untuk proses otentikasi yaitu:

a. *Supplicant* (*Client Software*)
Merupakan perangkat *client* yang akan di autentikasi sebelum diperbolehkan mengakses ke sebuah jaringan. Identitasnya masih tidak diketahui sampai menghasilkan autentikasi yang valid ke *authentication server*.

b. *Authenticator* (*Access Point*)
Merupakan perangkat jaringan layer 2 seperti *ethernet switch* atau *wireless* LAN *access point*. *Authenticator* berperan seperti pintu keamanan antara *supplicant* dan jaringan yang dilindungi. Ketika *supplicant* mengirim *credential* ke *authentication server*, *authenticator* akan membungkus paket *credential* tersebut ke dalam frame EAPoL. Sehingga inisiasi identitas *supplicant* tidak akan diketahui oleh *supplicant* lainnya.

c. *Authentication Server* (RADIUS/AAA Server)
Berperan sebagai server yang akan melakukan validitas dari *credential* sebuah *supplicant*. Setelah semua proses validitas selesai dan *supplicant* dinyatakan valid maka *authenticator* akan memberikan hak akses kepada *supplicant* tersebut menuju sebuah jaringan.

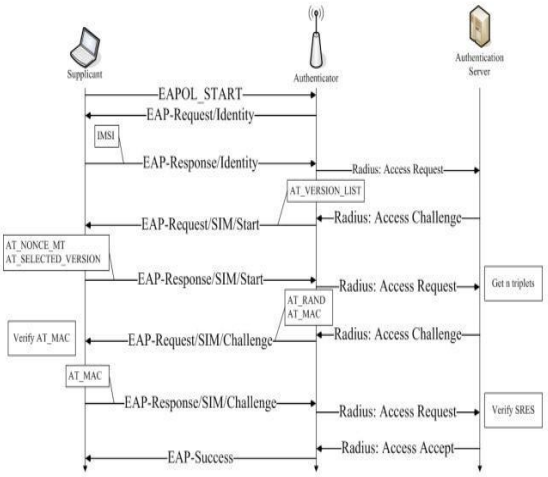


Gambar 2.1 Arsitektur EAPol[14]

2.5 EAP-SIM[3]

EAP-SIM adalah suatu autentikasi EAP yang menggunakan kartu SIM sebagai data identitas untuk melakukan autentikasi ke dalam jaringan WLAN. Kartu SIM merupakan sebuah *token* yang yang biasanya digunakan pada jaringan GSM. Ide dari EAP-SIM adalah melakukan autentikasi jaringan non-GSM seperti WLAN menggunakan identitas yang tersimpan di dalam SIM.

Autentikasi yang terjadi antara *supplicant* dan *authenticator* dimulai dengan pembukaan *port* komunikasi dengan hanya paket EAP saja yang dapat melintas. Untuk itu, paket yang pertama muncul adalah paket EAPOL yang berfungsi untuk membungkus paket EAP. Proses autentikasi yang terjadi ditunjukkan pada Gambar 2.2.



Gambar 2.2 Proses Autentikasi EAP-SIM[2]

2.6 *Remote Authentication Dial-In User Service* (RADIUS)[1]

RADIUS merupakan protokol keamanan komputer yang digunakan untuk melakukan autentikasi, autorisasi, dan pendaftaran akun pengguna secara terpusat untuk mengakses jaringan. RADIUS pada awalnya digunakan untuk koneksi dialup. Saat ini RADIUS telah diimplementasikan untuk melakukan autentikasi terhadap akses jaringan secara jarak jauh dengan menggunakan koneksi *dial up*, seperti halnya VPN, *access point* nirkabel, dan *switch ethernet*.

2.6.1 *Challenge Response*[1]

Dalam autentikasi *Challenge-Response*, pengguna diberikan sebuah nomor acak dan melakukan fungsi *hash* (challenge) untuk mengenkripsi dan mengirimkannya kembali ke server. Paket *Access-Challenge* mengandung pesan balasan termasuk *challenge* untuk ditampilkan ke pengguna seperti nilai numerik yang tidak akan bisa diulang (one way function).

Pengguna memasukkan *challenge* ke dalam perangkatnya dan akan menghitung respon yang merupakan *input* pengguna ke dalam *client* dan meneruskan ke RADIUS server melalui *Access-Request* yang kedua. Jika respon sesuai dengan yang diharapkan, RADIUS server akan membalas dengan paket *Access-Accept* ataupun *Access-Reject* jika tidak sesuai.

2.7 Asterisk[16]

Asterisk merupakan implementasi software dari sentral telepon PBX (*private branch*).

Diciptakan pada tahun 1999 oleh Mark Spencer dari Digium. Seperti PBX, Asterisk memungkinkan telepon dapat melakukan panggilan ke satu dengan yang lainnya, dan terhubung ke layanan telepon lainnya seperti *public switched telephone network* (PSTN) dan *Voice over Internet Protocol layanan* (VoIP).

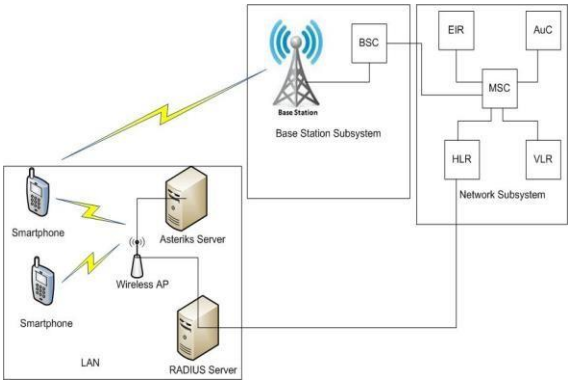
2.7.1 Asterisk *Realtime*

Asterisk Realtime Architecture (ARA) adalah metode menyimpan file-file konfigurasi (yang biasanya akan ditemukan di /etc/asterisk) dan opsi-opsi konfigurasi mereka berada dalam tabel *database*. Asterisk *realtime* dikonfigurasi dalam file *extconfig.conf* yang terletak di direktori /etc/asterisk. *File* ini berfungsi untuk memberitahu Asterisk apa yang harus dimuat dari *database* dan darimana beban itu berasal, *file* ini juga memungkinkan diambil dari database dan dari file lain yang diambil dari konfigurasi file standar.

3. Model Dan Perancangan Sistem

3.1 Model Sistem Dan Cara Kerja

Topologi sistem yang dibuat pada Tugas Akhir ini dimodelkan pada gambar 3.1



Gambar 3.1 Topologi Jaringan Yang Dibangun

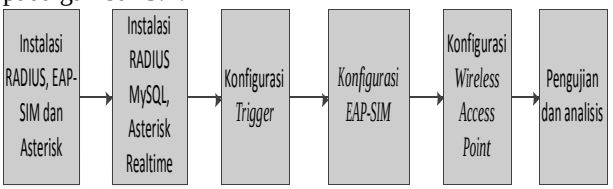
Topologi diatas merupakan gabungan dari model sistem yang dibangun (jaringan LAN) dengan jaringan arsitektur GSM (*Global System For Mobile Communication*) pada umumnya. Proses penyimpanan dan pengambilan kode-kode triplets kartu seluler (IMSI, RAND,SRES dan Kc) pada HLR ataupun VLR dianggap sudah terhubung ke jaringan LAN secara otomatis. Sehingga yang akan dibahas pada implementasi tugas akhir ini hanya berada pada jaringan LAN yang dibangun. Untuk pengujian di jaringan LAN yaitu pengambilan kode triplets dari kartu seluler diperoleh secara manual dengan menggunakan *software* AGSM dan SIM *card reader*.

Keterangan :

a. *Client* berfungsi sebagai pihak yang akan menggunakan layanan dalam jaringan tersebut.
b. *Access Point* sebagai penyedia konektifitas antara *client* yang menggunakan jaringan *wireless* kemudian diteruskan ke server.
c. RADIUS server sebagai server autentikasi yang berguna untuk memeriksa integritas *client* mana yang berhak untuk mengakses ke jaringan.
d. Asterisk server sebagai VoIP server.

3.2 Blok Diagram Pengerjaan

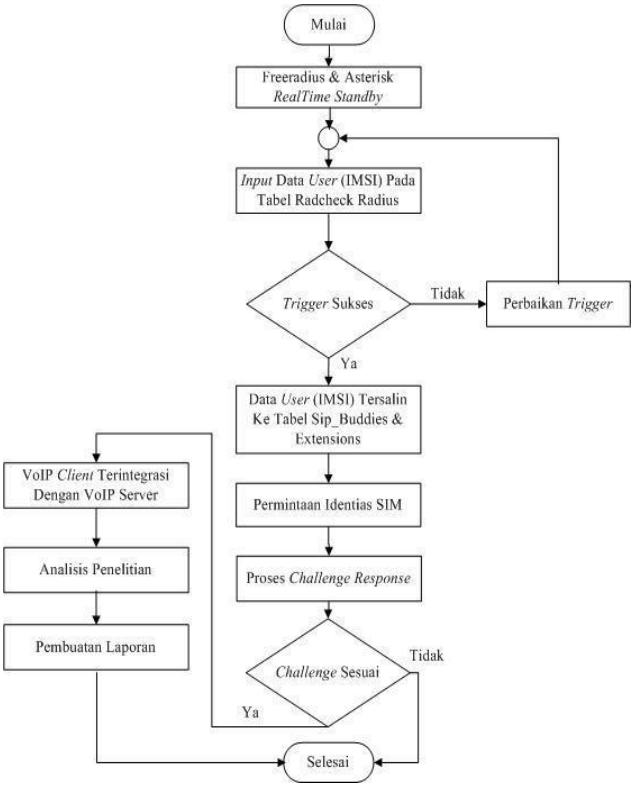
Proses tahapan pengerjaan Tugas Akhir ini melalui beberapa tahapan proses yang dapat dilihat pada gambar 3.2.



Gambar 3.2 Blok Diagram Pengerjaan

3.3 Skenario Pengujian

3.3.1 *Flowchart* Sistem dan Analisis

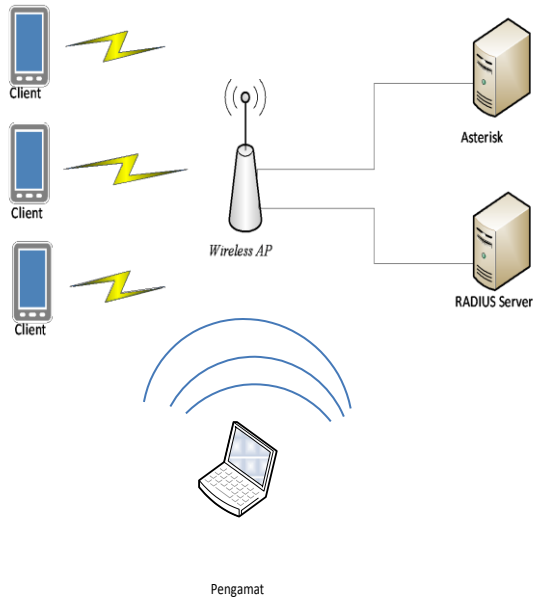


Gambar 3.3 *Flowchart* Sistem

Tahap pengamatan sistem diamati oleh laptop dengan sistem operasi Backtrack 5 untuk melihat proses autentikasi antara *wireless access point* dan supplicant. Pengukuran dilakukan dengan menggunakan software *wireshark* untuk melihat

lalu lintas paket autentikasi yang melintas antara *supplicant* dengan *wireless router*.

Laptop yang dijadikan pengamat lalu lintas trafik antara *wireless access point* dan *supplicant* harus menggunakan *interface monitoring* yang penggunaannya merupakan salah satu fitur yang telah disediakan di dalam sistem operasi Backtrack.



Gambar 3.4 Skenario Pengujian

Pengambilan paket autentikasi antara *supplicant* dengan *authenticator* menggunakan laptop pengamamat dengan sistem operasi Backtrack 5. Tool yang digunakan untuk me-*monitor* trafik data antara *supplicant* dan *authenticator* adalah airmon-ng dan airodump-ng.

3.3.2 Waktu Autentikasi EAP[1]

Sesi autentikasi merupkan waktu yang diperlukan untuk seluruh proses autentikasi dari permintaan autentikasi hingga autentikasi berhasil.

$$A_{total} = A_{End} - A_{Start}$$

Dengan

A_{total} = Total waktu autentikasi

A_{End} = Waktu pesan EAP-Request diterima

A_{Start} = Waktu pesan EAP-Success diterima

3.3.3 Waktu Pemrosesan Autentikasi RADIUS[1]

Waktu Pemrosesan Autentikasi merupakan waktu yang diperlukan server autentikasi untuk melakukan proses autentikasi dari diterimanya permintaan autentikasi dari *authenticator*, proses *challenge* kunci autentikasi, hingga autentikasi berhasil.

$$P_{total} = P_{End} - P_{Start}$$

Dengan

P_{total} = Total waktu pemrosesan autentikasi

P_{End} = Waktu pesan RADIUS-Accept dikirim

P_{Start} = Waktu pesan RADIUS-Request diterima

3.3.4 Waktu Proses *Challenge* Kunci Autentikasi[1]

Waktu proses *challenge* merupakan waktu yang diperlukan untuk melakukan proses *challenge* dan *response* antara *supplicant* dan server autentikasi dimulai dari pengiriman paket kunci autentikasi hingga kunci autentikasi sesuai satu dengan identitas *supplicant*.

$$C_{total} = C_{End} - C_{Start}$$

Dengan

C_{total} = Total waktu proses *challenge*

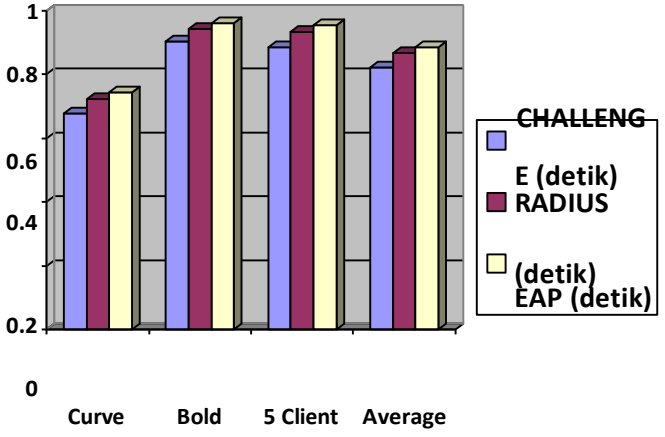
C_{End} = Waktu pesan *Response* Challenge dikirim

C_{Start} = Waktu pesan *Request* EAP-Method diterima

4. Pengujian dan Analisis Hasil Impelementasi

4.1 Analisis Kinerja Protokol Autentikasi

Pengujian parameter untuk menganalisis performansi kualitas kinerja protokol autentikasi EAP-SIM ditunjukan pada Gambar 4.1



Gambar 4.1 Parameter Autentikasi EAP-SIM

Gambar 4.1 menunjukkan rata-rata waktu autentikasi EAP-SIM yang dibutuhkan oleh 5 buah

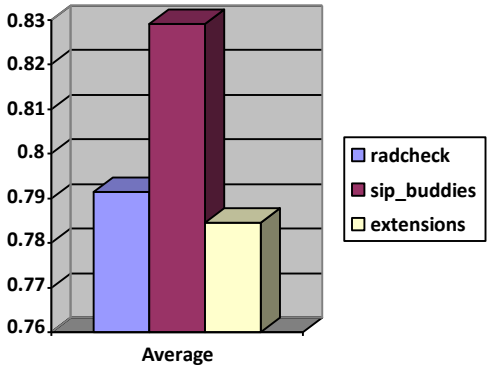
client saat melakukan autentikasi secara bersamaan. Rata-rata waktu yang dibutuhkan oleh 5 buah *client* tersebut untuk autentikasi dengan metode EAP-SIM ini adalah sebesar 0.852098 detik. Sehingga jika dibandingkan ketika sebuah supplicant melakukan autentikasi dengan metode EAP-SIM yang membutuhkan waktu 0.742852 detik maka persentase perbandingannya sebesar 87.18%.

Waktu maksimum yang dibutuhkan kelima *supplicant* adalah 0.9 detik untuk melakukan proses autentikasi.

4.2 Analisis Kinerja Auto Autentikasi VoIP Pada Sisi Server

4.2.1 Analisis Kinerja Trigger SQL

Agar dapat melihat performansi SQL secara keseluruhan pada suatu tabel maka dapat menggunakan *query profiling. Query* ini akan menampilkan semua *query* yang berjalan bersama dengan lama durasinya. Dalam tabel radius ditambahkan sebuah tabel yaitu tabel *users* yang hanya berisikan kolom *user*. Pada tabel ini sudah dibuat *statement/trigger* yaitu *statement after insert* dan *after delete*. Sehingga *username* yang kita butuhkan untuk autentikasi pada VoIP dapat tersalin ke tabel yang kita inginkan.



Gambar 4.2 Waktu Eksekusi Trigger

Dari hasil waktu rata-rata pengujian sebanyak 30 kali dapat disimpulkan bahwa rata-rata waktu eksekusi pada tabel *radchcek* adalah 0.000791467 detik atau 0.791 milidetik. Kemudian rata-rata waktu eksekusi pada tabel *sip_buddies* adalah 0.000829067 atau berkisar 0.829 milidetik. Sedangkan rata-rata waktu eksekusi pada tabel *extensions* adalah 0.0007846 atau sebesar 0.785 milidetik. Sehingga dapat disimpulkan bahwa rata-rata waktu yang dibutukan untuk autentikasi VoIP pada sisi server adalah 1.614 ms.

Sedangkan waktu yang dibutuhkan oleh server voip untuk proses autentikasi secara manual adalah sebesar 2.930 ms.Dengan perbedaan waktu autentikasi di sisi voip server yang lebih dari 1 detik atau lebih tepatnya 1.316 detik maka dengan metode auto autentikasi pada voip server pada implementasi tugas akhir ini lebih bagus dibandingkan jika kita harus *input* data secara manual pada voip server karena waktu yang dibutuhkan lebih cepat.

4.3 Analisis Performansi Registrasi VoIP Client

Berikut adalah hasil pengujian untuk lama waktu ketika voip client melakukan registrasi ke voip server setelah sebelumnya supplicant sudah terhubung ke jaringan melalui metode EAP-SIM.

Tabel 4.1 Lama Waktu Registrasi VoIP Client

Pengujian ke-	Lama Waktu Registrasi VoIP Client
1	0.014934
2	0.027005
3	0.010648
4	0.021291
5	0.013667
6	0.028052
7	0.013902
8	0.034607
9	0.011953
10	0.009356
11	0.011417
12	0.014298
13	0.017731
14	0.010144
15	0.008921
16	0.016699
17	0.015088
18	0.017895
19	0.012290
20	0.017310
21	0.017279
22	0.011135
23	0.016245
24	0.013089
25	0.030917
26	0.033093
27	0.016101
28	0.018583

29	0.031938
30	0.019808
Average	**0.017847**

Tabel diatas menunjukkan lama waktu yang dibutuhkan sebuah voip *client* agar bisa terhubung ke voip server. Rata-rata waktu yang dibutuhkan voip *client* tersebut dapat terhubung ke voip server adalah 0.017847 detik. Apabila dihitung dengan waktu yang dibutuhkan dari supplicant dihubungkan ke jaringan melalui EAP-SIM sampai dengan *supplicant* atau voip *client* terhubung ke voip server maka waktu yang dibutuhkan adalah sebesar 0.760699 detik

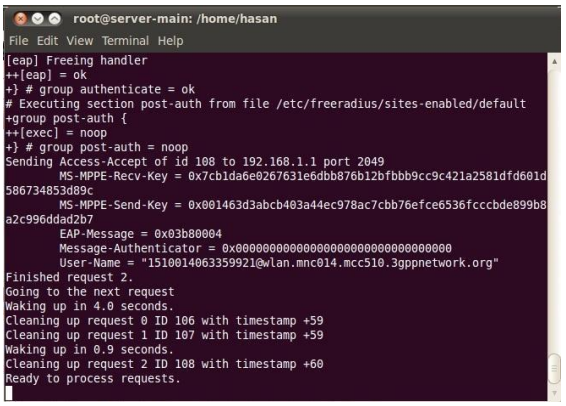
4.4 Analisis Performansi Pada Metode Autentikasi Yang Diimplementasikan

4.4.1 Perbedaan Dari Aspek Keamanan

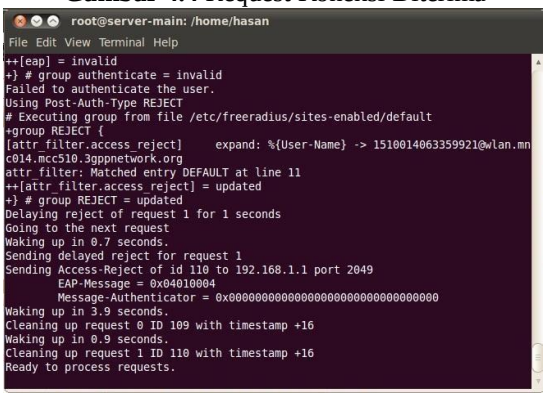
Perbedaan dari aspek keamanan antara metode yang sudah ada dengan metode yang diimplementasikan pada tugas akhir ini adalah metode pada implementasi tugas akhir ini menggunakan metode *wpa2 enterprise*. Sedangkan metode yang digunakan pada umumnya untuk autentikasi voip hanya menggunakan metode biasa seperti wep atau wpa yang masih membutuhkan masukan kata sandi dan masih banyak kelemahan pada sistem keamanannya.

Gambar 4.3 Koneksi Dengan Metode WPA

Dengan memanfaatkan metode EAP dengan data berdasarkan dari kartu seluler atau EAP-SIM maka kita tidak perlu memasukkan kata sandi seperti pada gambar 4.5. Kita bisa langsung melakukan permintaan penghubungan koneksi apabila sebelumnya data dari kode triplets pada kartu seluler sudah didaftarkan terlebih dahulu di server autentikasi. Kelebihan dari sisi keamanan berikutnya dari metode yang diimplementasikan ini adalah tidak semua kartu seluler dapat terkoneksi ke jaringan melainkan kartu seluler yang sudah didaftarkan ke server autentikasi.



Gambar 4.4 Request Koneksi Diterima



Gambar 4.5 Request Koneksi Ditolak

4.4.2 Perbedaan Dari Aspek Waktu Autentikasi

Berdasarkan dari aspek keamanan metode autentikasi yang diimplementasikan pada tugas akhir ini adalah metode autentikasi ini lebih aman dibandingkan dengan metode autentikasi yang biasa digunakan. Namun apabila berdasarkan dari waktu autentikasi yang dibutuhkan dari klien terhubung ke akses poin sampai dengan klien tersebut sudah terhubung ke voip server maka metode yang diimplementasikan pada tugas akhir ini memerlukan lebih banyak waktu dikarenakan pada autentikasi EAP-SIM ada proses pertukaran kunci yang dilakukan antara klien dengan server.

Dari hasil pengujian sebanyak 30 kali didapat bahwa waktu rata-rata yang dibutuhkan oleh sebuah klien agar bisa terhubung ke akses poin adalah sebesar 0.03408 detik. Kemudian waktu yang dibutuhkan oleh klien dari proses autentikasi ke akses poin sampai dengan terhubung ke voip server adalah sebesar 0.052 detik.

Apabila dibandingkan dengan waktu yang dibutuhkan oleh klien sampai dengan terhubung dengan voip server menggunakan metode autentikasi yang diimplementasikan pada tugas akhir ini berdasarkan tabel 4.1 dan tabel 4.6 maka perbedaan waktunya adalah sebesar 0.7087 detik. Sehingga apabila berdasarkan dari segi waktu autentikasi, metode yang biasa digunakan lebih cepat dibandingkan metode yang diimplementasikan.

5 Penutup

5.1 Kesimpulan

Kesimpulan yang dapat diambil dari pembuatan tugas akhir ini adalah :

1. Penambahan jumlah *supplicant* akan mempengaruhi waktu autentikasi EAP-SIM terutama penambahan lima kali lipatnya terhadap lama waktu yang dibutuhkan untuk proses *challenge response* pada pengujian dengan menggunakan 5 buah *supplicant* secara bersamaan.
2. Waktu maksimum yang dibutuhkan lima buah *supplicant* adalah 4 detik untuk melakukan proses autentikasi EAP-SIM secara bersamaan.
3. Dengan Asterisk RealTime asterisk akan selalu terhubung dengan tabel yang telah dibuat pada mysql.
4. SQL Triggers dapat digunakan untuk penyalinan otomatis dari tabel radius ke tabel-tabel asterisk.
5. Metode auto autentikasi pada voip server dengan menggunakan metode EAP-SIM ini akan memberikan waktu yang lebih cepat jika dibandingkan dengan autentikasi pada voip server secara manual dengan selilisih waktu yang dihasilkan sebesar 1.316 ms.
6. Waktu maksimum yang dibutuhkan sebuah supplicant terhubung ke jaringan melalui metode EAP-SIM sampai dengan berhasil registrasi ke voip server adalah 1 detik atau tepatnya 0.760699 detik.
7. Keunggulan metode autentikasi yang diimplementasikan pada tugas akhir ini ada pada sisi keamanan namun membutuhkan waktu yang lebih lama untuk proses autentikasi secara keseluruhan jika dibandingkan dengan metode autentikasi yang biasa digunakan.

5.2 Saran

Saran yang dapat disampaikan untuk pengembangan tugas akhir ini adalah :

1. Percobaan dapat dilakukan menggunakan *wireless access point* yang mengusung teknologi hotspot 2.0 sehingga dapat dilakukan ujicoba *handover* antar *authenticator*.
2. Pengujian keamanan sistem pada protokol autentikasi EAP untuk mengamati kehandalan masing-masing protokol.
3. Implementasi autentikasi voip bisa sampai ke sisi klien dengan membuat aplikasi voip klien yang dapat membaca imsi pada kartu seluler yang digunakan.
4. Pengujian keamanan sistem pada voip agar satu *username* tidak dapat diregistrasi pada server voip dalam waktu yang sama.

Daftar Pustaka

[1] Arzal Fariz, Achmad. 2013. "Analisis Kinerja Protokol EAP-SIM Untuk Mekanisme Autentikasi Jaringan WLAN". Bandung: Universitas Telkom

[2] Cai Siao-Jie, etc , "Design and Implementation of WIRE1x EAP-SIM Module". January 2007. Wireless Internet Research and Engineering Laboratory National Tsing Hua University, Taiwan.

[3] Fuad R,Reza. "Standar IEEE 802.1X Teori dan Implementasi".

[4] Geier, Jim."Implementing 802.1X Security Solution for Wired and Wireless Networks". 2008. Wiley Publishing, Inc.

[5] Gunadi, Hantono Dwi. "WiFi (Wireless LAN) Jaringan Komputer Tanpa Kabel". Bandung : Penerbit Informatika, 2009.

[6] IETF, RFC 2865, C.Rigney, et al, "Remote Authentication Dial In User Service (RADIUS)", 2000.

[7] IETF, RFC 3748, B.Aboba, et al, "Extensible Authentication Protocol (EAP)", 2004.

[8] IETF, RFC 4186, H.Haverinen, et al, "Extensible Authentication Protocol Method for Global System for Mobile Communication (GSM) Subscriber Identity Modules (EAP-SIM)", 2006.

[9] Liang, Wei and Wang,Wenye, "On performance analysis of challenge/response based authentication in wireless networks", 2005.

[10] Sugeng, Winarno. "Membangun Telepon Berbasis VoIP". Bandung : Penerbit Informatika, 2008.

[11] Sunarfrihanto, Bimo. 2003. "PHP dan MySQL Untuk WEB", 2013. Yogyakarta

[12] Tsai, Yuh-Ren. and Chang,Cheng-Ju, "SIM-based subscriber authentication mechanism for wireless local area networks", 2006.

[13] Yoanes (2008). Protokol SIP. Diakses Oktober 27, 2013. Dari http://yoanesbandung.wordpress.com/2008/05/26/protokol-session-initiation-protocol-sip/

[14] http://www.vocal.com/secure-communication/eapol-extensible-authentication-protocol-over-lan/ (diakses tanggal 08 November 2013).

[15] www.aircrack-ng.org (diakses tanggal 05 Oktober 2014).

[16] http://www.asterisk.org (diakses tanggal 08 Oktober 2014).