IMPLEMENTASI VOIP MENGGUNAKAN ZRTP, G.729A, DAN FREESWITCH

Eko Budianto[1], Rr Yuliana Rachmawati K[2], Uning Lestari[3]

[1,2,3] Teknik Informatika, Institut Sains & Teknologi AKPRIND Yogyakarta
[1]admin@kenari22.net, [2]yuli_rachma@yahoo.com, [3]uning@yahoo.com

ABSTRACT

Nowadays, the existence of VoIP communication is growing fast. However, communication that is common at this time has not fulfilled the needs of specific users. For particular users, the safety and fluency of the communication is the fundamental needs. This is about VoIP communication that combined between FreeSWITCH as SIP Server, ZRTP as an encryption method to securing communication, and the use of G.729A as an audio codec. To collect the data, it will use the wireshark application for observing Quality of Service during the communication such as delay, jitter, and packet loss. While cain& able application is used for sniffing the process of communication on the network. Using a process of testing using sniffing method, communication on the network which is not using encryption can be caught and read by both wireshark and cain& able application, while communication on the network which is using encryption can not be read by both application. The result of VoIP communication using ZRTP protocol as an encryption method is can not be read and decoded by wireshark and cain& able and the use of codec G.729A is more suiteable for VoIP communication.

Keywords*: VoIP, FreeSWITCH, G.729A, ZRTP, Encryption*

PENDAHULUAN

Perkembangan komunikasi saat ini sangat pesat, trend penggunaan trafik telpon dan sms semakin berkurang, justru yang semakin meningkat adalah penggunaan trafik data. Pertumbuhan teknologi yang semakin pesat dan murah juga membuat tingkat adopsi *smartphone* menjadi tinggi. Sehingga layanan berbasis internet seperti *XMPP* dan *SIP* menjamur dimana mana, seperti *whatsapp*, *line*, *bbm*, dan sebaginya. Layanan yang disebutkan juga memberikan fitur *voice call* maupun *video call*. Hal ini memicu semakin tingginya penggunaan trafik data dibandingkan dengan trafik sms dan telepon.

Belum lagi layanan *voice* dan *video call* yang ekslusif seperti *facetime* dan *iMessage* milik *Apple* yang sama berbasis *XMPP* dan *SIP* semakin mempermudah dan mempermurah pelanggan dalam melakukan komunikasi seperti misalnya yang semula telepon antar negara membutuhkan internasional roaming, sekarang bisa dilakukan secara gratis. Akan tetapi tidak semua komunikasi yang disediakan memiliki tingkat keamanan yang baik.

Keamanan dan privasi menjadi hal yang penting dewasa ini. Tingkat kemanan suatu jalur komunikasi sangat diperlukan agar komunikasi yang dilakukan sulit disadap oleh orang lain. Tidak semua aplikasi *voice call* dan *video call* menyediakan fitur enkripsi, sehingga komunikasi antar sesama pengguna kemungkinan dapat disadap oleh orang lain. Oleh karena itu, diperlukan suatu aplikasi yang menjamin keamanan komunikasi yang terjadi antara pengguna yang satu dan yang lainnya agar tidak mudah untuk disadap oleh pihak yang tidak bertanggung jawab.

Berdasarkan latar belakang masalah di atas, dapat dirumuskan beberapa masalah di antaranya bagaimana mengkonfigurasi *SIP Server* menggunakan *FreeSWITCH* menggunakan metode enkripsi *ZRTP* dan G.729A sebagai *codec audio* dan melihat kinerja dari sistem komunikasi menggunakan *VoIP* yang telah dikonfigurasi dengan menganalis *delay, jitter,* dan *packet loss* pada jaringan seluler.

Dalam penelitian ini diambil referensi dari beberapa penelitan dan jurnal yang berhubungan dengan perencanaan pengembangan *VoIP* diantaranya adalah (Maknum, 2014) dengan judul "*Implementasi Voice Over Internet Protocol (VoIP) IP Phone Sebagai Media KomunikasiPengganti Private Automatic Branch Exchange (PABX) (StudiKasusInstitutTeknologi Padang)*". Dalam jurnal penelitian ini dibahas mengenai implementasi *VoIP* secara umum pada jaringan LAN menggantikan fungsi *PABX* yang digunakan.

Referensi selanjutnya (Rekyanata, 2010) dengan judul *"Analisis Implementasi VoIP-SIP Menggunakan Zimmerman Real-Time Transport Protocol (ZRTP) Pada Server Asterisk".*Dalam penelitian tersebut dijelaskan mengenai implementasi protocol keamanan *VoIP* menggunakan *ZRTP* pada jaringan LAN beserta analisanya baik dari segi analisa *delay, packet loss, jitter,*dan *throughput* menggunakan perhitungan *Mean Opinion Score (MOS)* dan*R-Factor* seperti pada tabel 1, beserta uji keamanannya.

Tabel 1 Tabel*MOS*dan*R-Factor*

User Satisfaction Level	MOS	R-Factor
Maximum using G.711	4.4	93
Very satisfied	4.3-5.0	90-100
Satisfied	4.0-4.3	80-90
Some users satisfied	3.6-4.0	70-80
Many users dissatisfied	3.1-3.6	60-70
Nearly all users dissatisfied	2.6-3.1	50-60
Not recommended	1.0-2.6	Less than 50

Referensi selanjutnya (Saputra, 2010) dengan judul*"Implementasi dan Analisa Unjuk Kerja Secure VoIP pada Jaringan VPN Berbasis MPLS dengan Menggunakan Tunneling IPSEC".*Dalam penelitian tersebut dijelaskan mengenai komunikasi *VoIP* yang menggunakan jaringan *VPN* yang berbasis *IPSEC*.

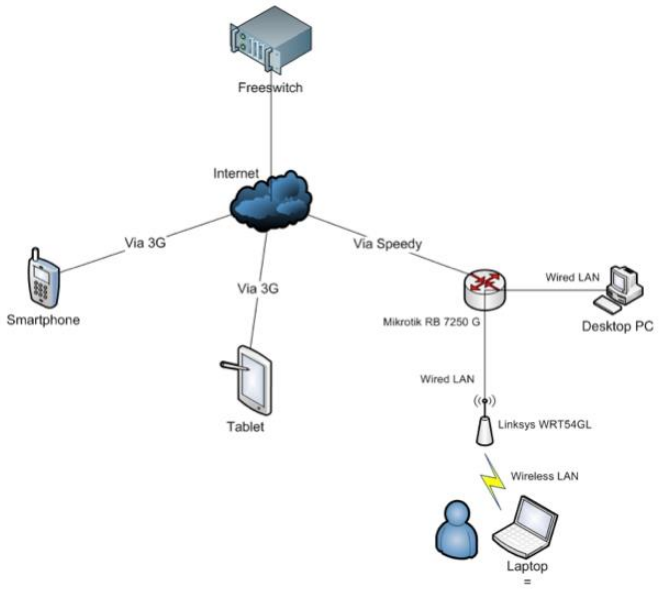
METODOLOGI PENELITIAN

Penelitian dilakukan dengan melakukan studi pustaka, untuk mengetahui beberapa penelitian yang pernah dilakukan sebelumny

a. Dalam tahap perancangan jaringan, penempatan *VoIP Server* akan diletakkan di sebuah data center yang terhubung ke jaringan internet, sehingga da lam tahap uji fungsi dapat dilakukan dari mana saja dan dari jaringan yang heterogen dan kompleks seperti jaringan yang menggunakan teknologi *ADSL* dan jaringan seluler. Setelah itu akan dilakukan dokumentasi terhadap hasil yang diperoleh dari uji fungsi tersebut. Hasil pengujian *Mean Opinion Score (MOS)* dan *R-Factor* mengacu pada tabel 1.

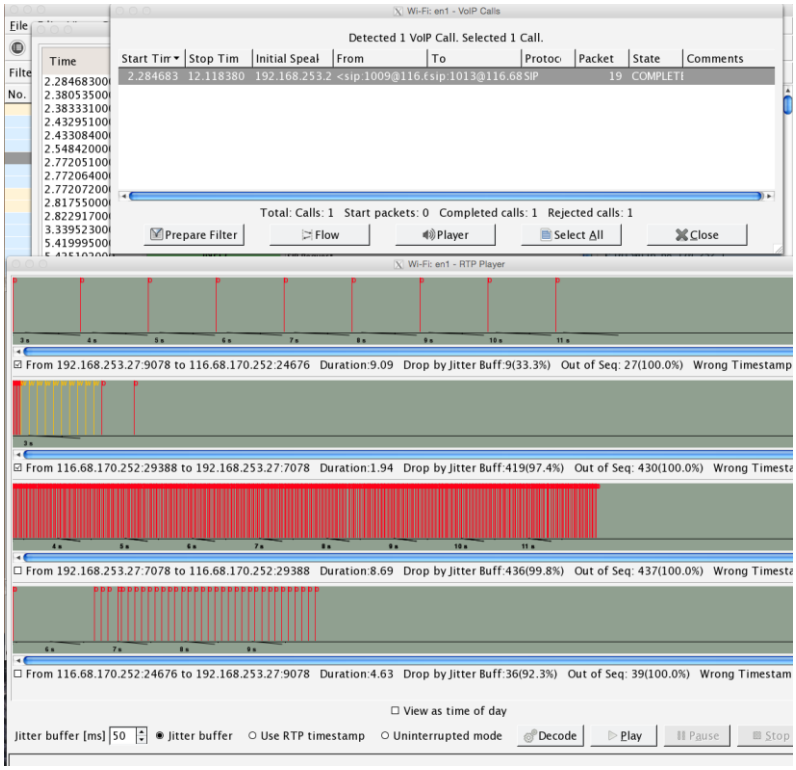
HASIL DAN PEMBAHASAN

Pada topologi yang ditunjukan pada gambar 1 menunjukkan bahwa terdapat sebuah *SIP Server Free SWITCH* yang terkoneksi melalui internet yang nantinya akan melayani komunikasi dari beberapa peralatan seperti smartphone dan tablet yang terkoneksi melalui jaringan seluler, dan beberapa peralatan lain seperti desktop PC dan notebook yang terkoneksi ke internet melalui jaringan ADSL.

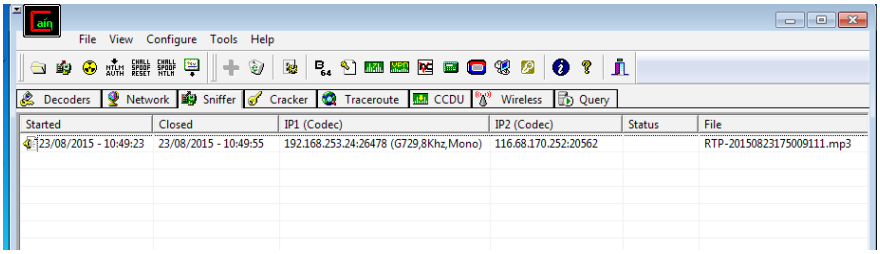


Gambar1 TopologiJaringan

Pada saat dilakukan pengujian komunikasi antar 2 *end* point tanpa menggunakan protocol enkripsi, didapatkan bahwa komunikasi *VoIP* yang terjadi dapat ditangkap dan dilakukan *decoding* bahkan dapat dilakukan play back menggunakan aplikasi *wires hark* seperti pada gambar 2. Hasil pengujian di konfirmasi menggunakan aplikasi *cain & able* juga dapat ditangkan dan dilakukan *recording* yang selanjutnya dari hasi recording tersebut dapat dilakukan *playback* seperti pada gambar 3.

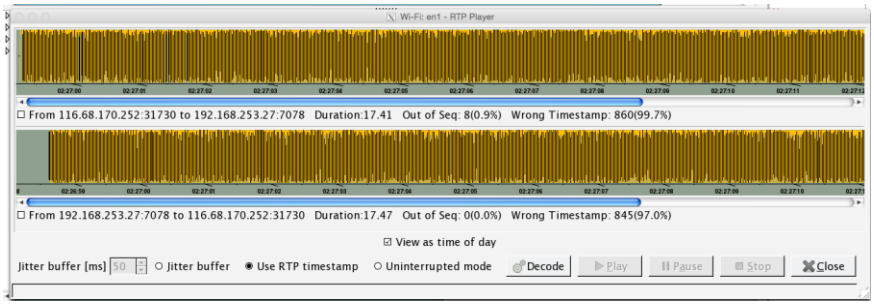


Gambar 2 hasil*sniffing* komunikasi*VoIP*menggunakanaplikasi*wireshark*



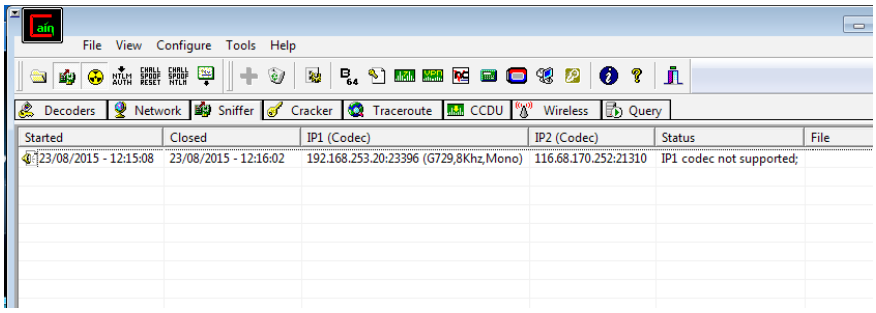
Gambar 3hasil*sniffing* komunikasi*VoIP*menggunakanaplikasi*cain& able*

Pada saat dilakukan pengujian menggunakan protocol enkripsi, didapatkan hasil yang berbeda pada saat dilakukan pengujian tanpa menggunakan protocol enkripsi. Dari hasil pengujian didapatkan bahwa komunikasi *VoIP* yang terjadi dapat di baca akan tetapi tidak dapat dilakukan *decoding* oleh aplikasi *wireshark* seperti pada gambar 4.



Gambar 4. Hasil*sniffing*protokolenkripsimenggunakanaplikasi*wireshark*

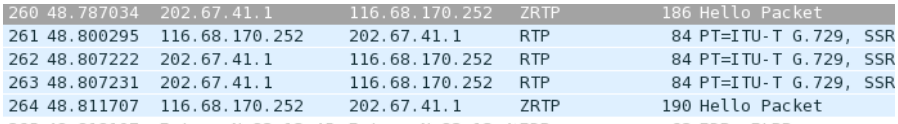
Hal ini juga dikonfirmasi pada saat dilakukan pengujian menggunakan aplikasi *cain & able*, pada saat melakukan komunikasi menggunakan protocol enkripsi tidak dapat dibaca oleh aplikasi *cain & able*, bahkan tidak dapat dikenali dan tidak dapat dilakukan *recording* pada saat komunikasi antar *end point* terjadi seperti pada gambar 5.



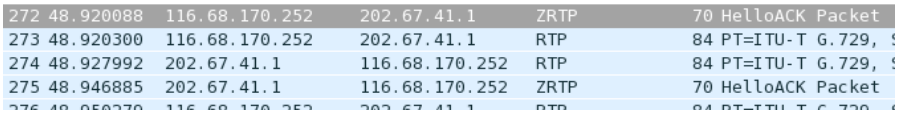
Gambar 5. Hasil *sniffing* protocol enkripsi menggunakan aplikasi *cain & able*

ZRTP bukan merupakan penggantian dari protocol enkripsi *VoIP* sebelumnya yaitu *SRTP*, akan tetapi *ZRTP* merupakan sebuah mekanisme negosiasi *session key* yang tidak diimiliki oleh *SRTP* menggunakan *Short Authentication String (SAS)*. *ZRTP* memungkinkan komunikasi yang lebih aman dikarenakan setiap terjadinya komunikasi, *key* tersebut akan selalu berubah.

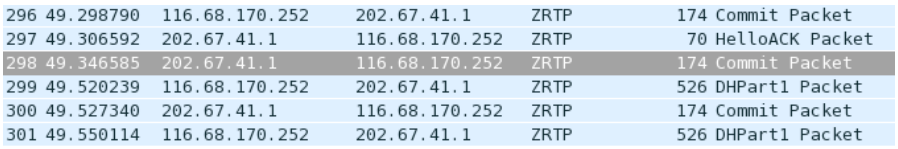
Hal ini memberikan keamanan dari *end user* satu ke *end user* lainnya, dimana pada saat terjadinya komunikasi kedua user tersebut harus menerima terlebih dahulu pada saat terjadinya proses pertukaran *key* antar *end user* seperti pada gambar 6-9 merupakan hasil yang di dapat dari *capture packet* menggunakan aplikasi wires hark pada saat dilakukan komunikasi antar 2 *end point* menggunakan protocol enkripsi *ZRTP* dimana sebelum terjadinya komunikasi, terlebih dahulu ada proses pertukaran kunci antar kedua *end point* yang akan melakukan komunikasi.



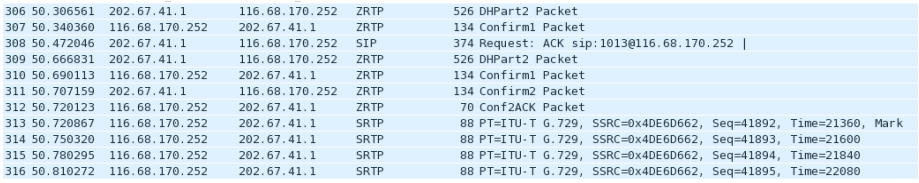
Gambar 6 Inisialisasiawal*Hello Packet ZRTP*



Gambar 7 Proses *Acknowledge Hello Packet*



Gambar 8 Proses pertukaran*key* 1



Gambar 9 Proses pertukaran*key* 2

Dari hasil pengujian codec dengan dan tanpa menggunakan protokol enkripsi didapatkan nhasil seperti dalam tabel 1 dan tabel2 :

Tabel 1 HasilUji CodectanpamenggunakanProtokolenkripsi

Codec	Bandwidth	Delay	Jitter	Packet Loss	MOS	R-Factor
G729A	22.20kbps	25.5ms	9.5ms	3.33%	3.92	77.68
G711	74.90kbps	15.6ms	10.21ms	2.79%	4.4	91.94
Opus	77.60kbps	17.6ms	12.05ms	5.77%	4	80.52

Tabel 2 HasilUji CodecMenggunakanProtokolEnkripsi

Codec	Bandwidth	Delay	Jitter	Packet Loss	MOS	R-Factor
G.729A	22.70kbps	21.5ms	7.52ms	0.70%	4	79.92
G.711	74.90kbps	18.9ms	8.38ms	0.16%	4.38	89.94
Opus	76.53kbps	19.9ms	11.56ms	1.71%	4.38	91.86

Dari table 1 dan tabel 2 dapat dilihat bahwa penggunaan *bandwidth* pada saat komunikasi menggunakan protokol enkripsi atau puntanpa menggunakan protocol enkripsi tidak berpengaruh banyak perbedaannya hal ini menunjukkan bahwa penggunaan protocol enkripsi atau pun tidak, tidak terlalu berpengaruh banyak pada kebutuhan minimum *bandwidth* yang dibutuhkan oleh *VoIP*.

Terlihat juga pada tabel1 2 code c G.729 lebih baik dalam hal jitter (waktu kedatangan paket) yaitu sebesar 9.5ms pada saat tanpa menggunakan enkripsi, dan 7.52 ms pada saat menggunakan enkripsi. Ketiga codec dari hasil pengujian memiliki nilai rata rata 4, dalam *Mean Opinion Score* yang artinya memiliki *User Satisfaction Level* dalam kategori *satisfied.*

KESIMPULAN

Berdasarkan dari hasil pengujian, dapat ditarik beberapa kesimpulan antara lain:

1. *ZRTP* memberikan solusi keamanan lebih baik yaitu dengan menggunakan *session management key* yang memberikan keamanan *end to end user* pada saat digunakan di jaringan public hal ini memberikan proteksi minimum yang lebih baik tanpa menambahkan secondary layer seperti *VPN* dan *MPLS*.
2. Penggunaan *codec G.729A* sangat baik dalam menunjang kelancaran komunikasi tanpa mengurangi tingkat keamanan dalam komunikasi *VoIP*.
3. Tidak ditemukan permasalahan interoperabilitys antar plat form dalam melakukan komunikasi *VoIP* baik menggunakan protokol enkripsi ataupun tidak.
4. Pada jaringan publik, penerapan enkripsi pada komunikasi *VoIP* dapat menghindari kemungkinan penyadapan.

DAFTAR PUSTAKA

Maknum, J. (2014) *Implementasi Voice Over Internet Protocol (VoIP) IP Phone Sebagai Media KomunikasiPengganti Private Automatic Branch Exchange (PABX) (StudiKasusInstitutTeknologi Padang)*. *Jurnal.* JurusanTeknikInformatika, FTI, InstitutTeknologi Padang, Padang.

Rekyanata, I. (2010).*AnalisisImplementasi VoIP-SIP Menggunakan Zimmermann Real-Time Transport Protocol (ZRTP) Pada Server Asterisk*. Teknik Telekomunikasi, Universitas Telkom, Bandung.

Saputra, A.T. (2010). *Implementasi dan Analisa Unjuk Kerja Secure VoIP pada Jaringan VPN Berbasis MPLS dengan Menggunakan Tunneling IPSEC*. Skripsi. Jurusan Teknik Elektro, FT, Universitas Indonesia.