Implementasi TLS dan SRTP pada VOIP Server

M. Fendi Kurniawan
sipiyuku@gmail.com
http://www.sipiyuku.web.id

❖ LATAR BELAKANG

Kemudahan untuk mengembangkan jaringan yang berbasis Internet Protocol (IP) menyebabkan adanya suatu pergeseran yang menjadikan jaringan IP atau jaringan data sebagai jaringan untuk komunikasi masa depan. Komunikasi suara pada jaringan data (internet) biasa disebut dengan VOIP (Voice Over Internet Protocol). VOIP merupakan suatu alternatif komunikasi masa depan yang akan menggantikan komunikasi via PSTN (Public Switch Telephone Network). Keadaan ini dikarenakan sistem jaringan PSTN yang tertutup dan hanya dapat dikembangkan oleh provider tertentu. Salah satu keunggulan VOIP adalah memiliki sistem komunikasi yang terbuka sehingga dapat dikembangkan oleh banyak kalangan. Selain itu, VOIP menggunakan jaringan IP sebagai media komunikasinya sehingga biaya komunikasi VOIP akan jauh lebih murah bila dibandingkan dengan komunikasi via PSTN. Selain memberikan kemudahan, komunikasi menggunakan VOIP juga akan memberikan beberapa permasalahan. Salah satu dari permasalahan tersebut adalah keamanan jaringan dan privasi pada saat berkomunikasi menggunakan VOIP. Terbukanya sistem komunikasi VOIP dalam jaringan IP menyebabkan semua orang dapat mempelajari dan mengembangkan VOIP, sekaligus merusak dan membajak komunikasi tersebut.

❖ DEFINISI KONSEPTUAL

Voice over Internet Protocol adalah Teknologi yang menjadikan media internet untuk bisa melakukan komunikasi suara jarak jauh secara langsung. Sinyal suara analog, seperti yang biasa didengar ketika berkomunikasi di telepon diubah menjadi data digital dan dikirimkan melalui jaringan berupa paket-paket data secara real time. Dalam komunikasi VoIP, pemakai melakukan hubungan telepon melalui terminal yang berupa PC atau telepon biasa.

TLS (Transport Layer Security) adalah sebuah protokol yang menyediakan komunikasi privasi dan keamanan antara dua aplikasi berkomunikasi melalui jaringan. TLS mengenkripsi komunikasi dan memungkinkan klien untuk mengotentikasi server dan, opsional, server untuk mengotentikasi klien. TLS adalah versi lebih aman dari protokol Secure Sockets Layer (SSL).

Secure Real Time Transport Protocol (SRTP) menyediakan fitur enkripsi pada profil RTP. Enkripsi disini dimaksudkan untuk menyediakan sistem keamanan data dengan otentikasi dan integritas pesan, dan perlindungan terhadap *playback* dengan data RTP dalam aplikasi baik *unicast* maupun *multicast* . SRTP dikembangkan oleh sebuah tim kecil dari Cisco dan Ericsson yang merupakan ahli protokol IP dan kriptografi. SRTP menggunakan algoritma AES (*Advanced Encryption Standart*) sebagai metode enkripsi dalam pengiriman data. Pada aplikasi, SRTP memiliki 2 buah mode, yaitu *Segmented Integer Counter*, dan AES di f8-mode. Selain itu SRTP juga dapat berjalan pada mode *null cipher*, Mode ini adalah mode dimana pengiriman data tidak dilindungi dengan algoritma enkripsi. SRTP pada kenyataannya hanya mengenkripsi *payload* (audio dan video) untuk kerahasiaan.

SIP (Session Initiation Protocol) SIP merupakan protokol yang didesain untuk dapat melakukan pembangunan sesi antar dua titik (user agent) sehingga kedua titik dapat berbagi resource. SIP yang merupakan protokol pada layer aplikasi dapat digunakan bersama dengan proxy server. SIP dapat menangani registrasi user, undangan sesi, dan permintaan lainnya yang bertujuan untuk membangun, memodifikasi, atau menutup sesi. SIP bukanlah media transfer protocol, tapi signaling protocol. Sehingga paket voice dan video tidak dibawa oleh protokol ini, SIP hanya melakukan signaling. **Elemen SIP,** terdiri dari :

a. User Agent (UA), berfungsi untuk menginisiasi atau merespon transaksi SIP. Sebuah UA bisa bertindak sebagai server atau klien.
b. User Agent Client (UAC), berfungsi untuk menginisiasi permintaan SIP dan menerima respon SIP.

c. User Agent Server (UAS), berfungsi menerima permintaan SIP dan mengirimkan kembali respon SIP.
d. SIP Proxy adalah entitas yang berfungsi untuk proses routing dan meneruskan dan meneruskan permintaan SIP kepada UAS atau Proxy lain atas permintaan UAC.
e. Redirect Server adalah sebuah UAS yang membangkitkan respon SIP terhadap permintaan yang diterima, memungkinkan UAC secara langsung menghubungi Uniform Resource Identifiers (URI).
f. Registrar Server adalah sebuah UAS yang menerima permintaan registrasi SIP dan memperbaharui informasi dari pesan tersebut kedalam database lokasi.
g. Back-to-Back User Agent (B2BUA) adalah entitas yang berfungsi untuk memproses permintaan SIP yang diterima dimana B2BUA akan bertindak sebagai UAC, membangkitkan kembali permintaan SIP dan mengirimkannya kedalam jaringan.

❖ PEMBAHASAN

Pada definisi konseptual telah dijelaskan bahwa komunikasi pada VOIP terjadi antara dua titik sesi (user agent). Untuk menangani sesi, registrasi user, dan permintaan lainnya maka kita perlu untuk membuat sebuah **SIP Server**, dan tentunya untuk disisi pengguna menggunakan **SIP Client** yang dalam hal ini bisa menggunakan *Sofphone* maupun *IP Phone*. Penulis menggunakan Sistem Operasi Centos 5.9 sebagai SIP Server dan menggunakan Asterisk 1.8, untuk software SIP Client penulis menggunakan *BLINK*. Dalam tulisan ini tidak membahas bagaimana instalasi sistem operasi Centos 5.9, diasumsikan bahwa sistem operasi Centos 5.9 telah terinstall dan siap untuk dikonfigurasi.

Tahap Instalasi dan Konfigurasi SIP Server

1. Melengkapi *package software* yang dibutuhkan untuk *Asterisk* dan *SRTP* (*dependencyes*), dengan perintah :

```
#yum –y install make wget openssl-devel ncurses-devel newt-devel
libxml2-devel kernel-devel gcc gcc-c++ sqlite-devel
```

Perintah diatas berfungsi untuk menginstall *package dependencyes Asterisk* dan *TLS*.

2. Menginstall *software SRTP Versi 1.4.2* dengan mendownload terlebih dahulu *source code* SRTP dari internet, menggunakan perintah :

```
#wget http://srtp.sourceforge.net/srtp-1.4.2.tgz
```

Unpack source code SRTP yang sudah didownload menggunakan perintah :

```
#tar –zxvf srtp-1.4.2.tgz
```

Install SRTP dari *source code* yang telah di *unpack.*

```
#tar -xvzf srtp-1.4.2.tgz
#cd srtp
#./configure CFLAGS=-fPIC --prefix=/usr
# make && make runtest && make install
```

3. Menginstall *Dahdi 2.7* dan *Libpri 1.4* dengan terlebih dahulu mendownload *source code Dahdi 2.7* dan *Libpri 1.4* dari internet.

```
#wget
http://downloads.asterisk.org/pub/telephony/dahdi-linux-complete/dahdi
-linux-complete-current.tar.gz
#wget
http://downloads.asterisk.org/pub/telephony/libpri/libpri-1.4-current.tar
.gz
```

Setelah *source code* berhasil didownload langkah selanjutnya adalah melakukan *unpack* dan instalasi dari *source code Dahdi 2.7* dan *Libpri 1.4.*

```
# tar zxvf dahdi-linux-complete-current.tar.gz
# cd dahdi-linux-complete-2.7.0.1+2.7.0.1/
# make && make install && make config
# make && make runtest && make install
```

Instalasi *Libpri 1.4* dengan perintah berikut :

```
# tar zxvf libpri-1.4-current.tar.gz
# cd libpri-1.4.14/
# make && make install
```

4. Menginstall *Asterisk 1.8* dengan terlebih dahulu mendownload *source code Asterisk 1.8* dari internet.

```
#wget
http://downloads.asterisk.org/pub/telephony/asterisk/asterisk-1.8.23.1.tar.gz
```

Instalasi *Asterisk 1.8* dengan perintah berikut :

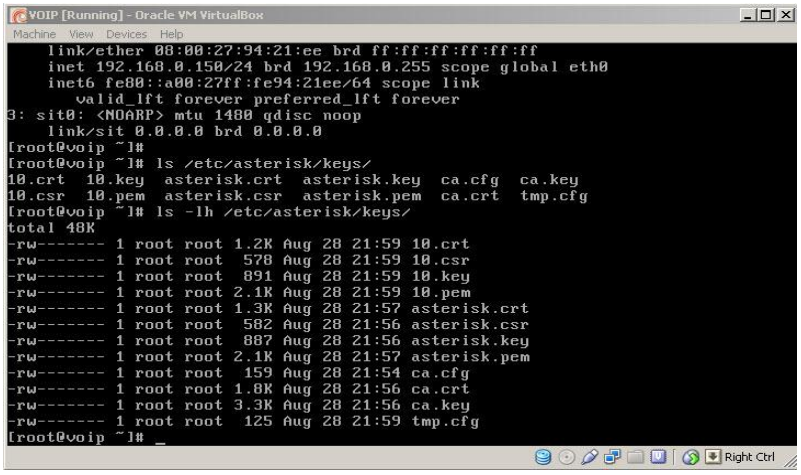
```
# tar zxvf asterisk-1.8.23.1.tar.gz
# cd asterisk-1.8.23.1
# ./configure && make menuselect && make && make install
# make && make install
# make samples && make config
```

5. Membuat *Certificate Authority* (CA) *Transport Layer Security* (TLS) pada server VOIP.

```
# cd /home/master/asterisk-1.8.23.1/contrib/scripts/

# ./ast_tls_cert -C voip.sipiyuku.web.id -O "SRTP Asterisk" -d
/etc/asterisk/keys
```

```
# ./ast_tls_cert -m client -c /etc/asterisk/keys/ca.crt -k
/etc/asterisk/keys/ca.key -C voip.sipiyuku.web.id -O "SRTP Voip" -d
/etc/asterisk/keys -o 10
```

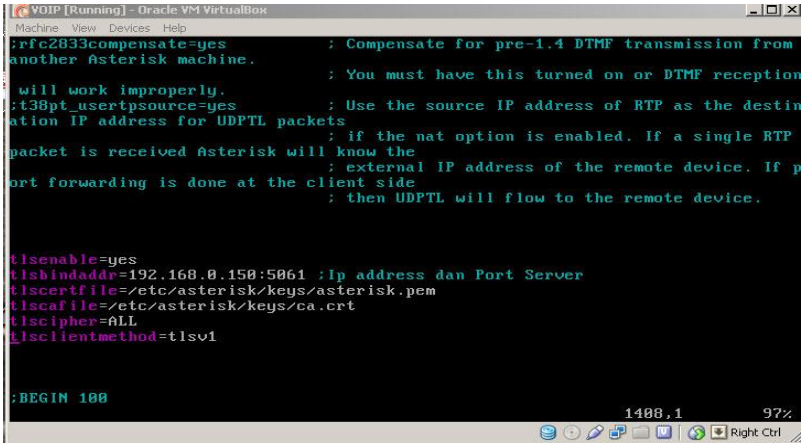


Gambar 1. Daftar file *Certificate Authority* (CA)

Pada gambar 1 nampak hasil pembuatan *Certificate Authority* (CA) *Transport Layer Security* (TLS) pada server VOIP.

6. Konfigurasi TLS pada *Asterisk 1.8*, dengan mengedit file *sip.conf* pada server.

```
# vim /etc/asterisk/sip.conf
```

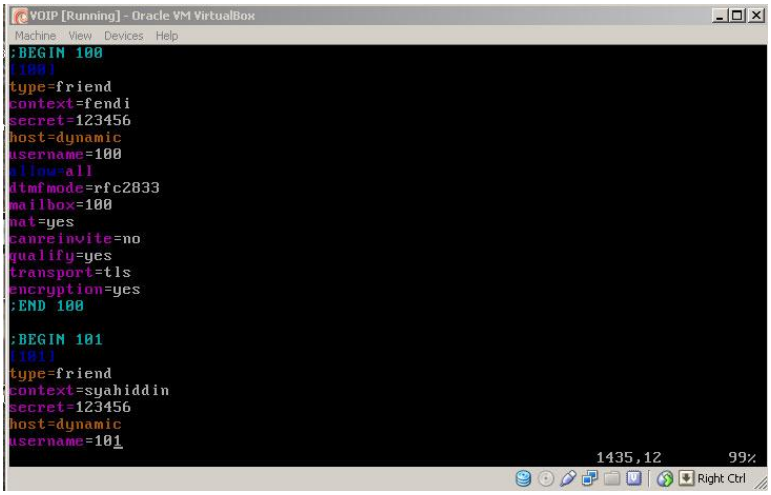


Gambar 2. File konfigurasi TLS pada Server Eksperimen

Pada gambar 2 memperlihatkan bahwa TLS pada server telah diaktifkan, dan menggunakan TLS versi 1. Juga telah ditetapkan file untuk *Certificate Authority* (CA).

7. Membuat ekstensi 100 dan 101 dengan cara menambahkan beberapa konfigurasi pada file *sip.conf*

```
# vim /etc/asterisk/sip.conf
```



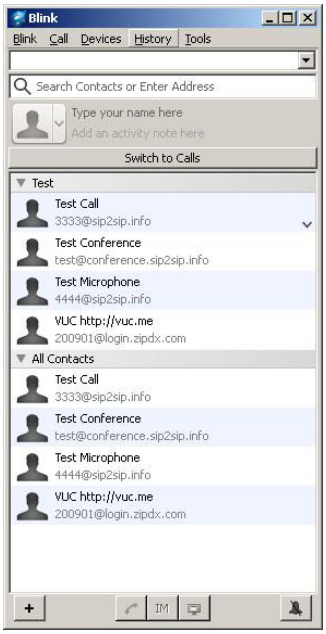
Gambar 3. File konfigurasi SIP Account pada Server

Gambar 3 menunjukkan konfigurasi untuk ekstensi 100 dan 101, dan mendukung TLS dan *enkripsi* SRTP.=

Tahap Konfigurasi SIP Client

Laptop yang digunakan sebagai client, menggunakan *softphone Blink*. Berikut langkah konfigurasinya :

1. Konfigurasi *Softphone Blink* pada pada laptop peneliti ekstensi. 100. Langkah pertama adalah menjalankan *software Blink*. Gambar 4 menunjukkan *software Blink* yang telah berjalan dan sama sekali belum di konfigurasi.



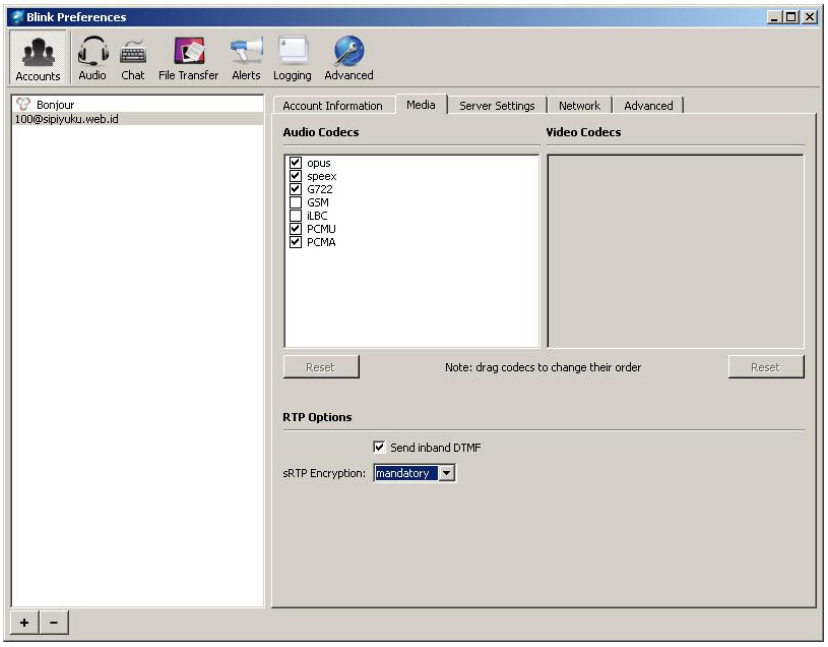
Gambar 4. *Software Blink*

Menambahkan SIP Account dengan menekan tombol ALT+b+a pada keyboard kemudian tekan tombol enter. Selanjutnya muncul kotak dialog seperti pada gambar 5.

Gambar 5. Kotak Dialog Penambahan SIP Account 100

Kemudian pada *software Blink* perlu dikonfigurasi untuk opsi TLS dan SRTP, juga menentukan file *Certificate Authority* (CA) yang digunakan untuk otoritas SIP Account pada server.

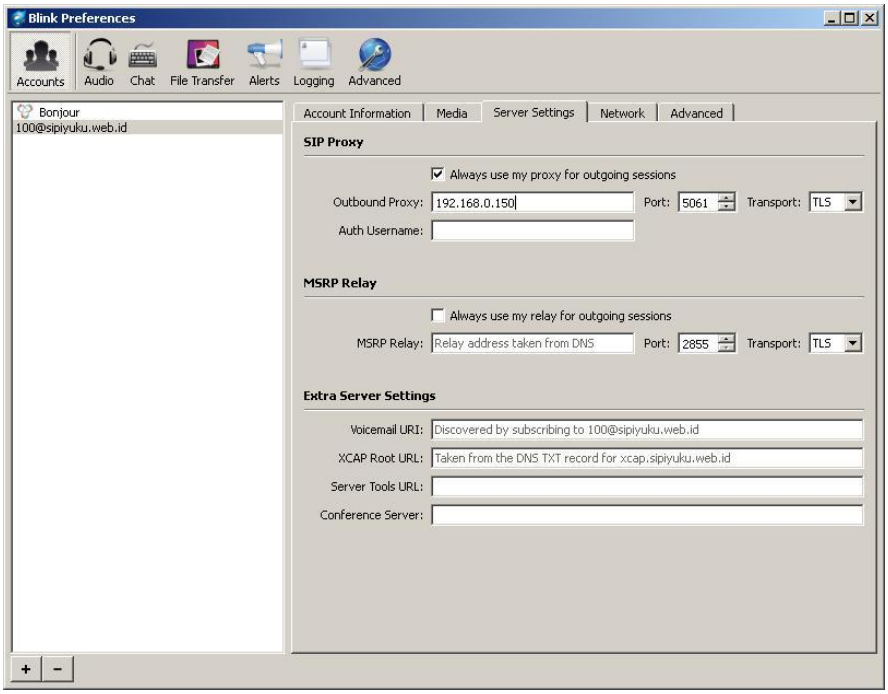
Pada *software Blink* masuk pada menu *Preferences* dengan menekan tombol ctrl+p pada keyboard. Kemudian masuk tab media, dan mengaktifkan *sRTP encryption* pada RTP options. Tampak pada gambar 6, *sRTP encryption* pada RTP options telah diaktifkan.



Gambar 6. Tab media pada *Preferences Blink*

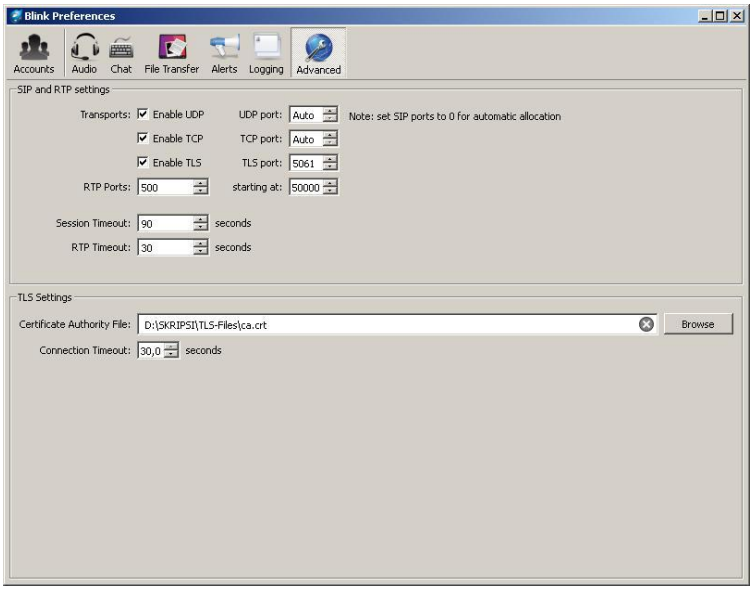
Masuk pada tab Server Setting ip address *outbound proxy* diisi dengan ip address server VOIP yaitu 192.168.0.150, kemudian untuk *port* menggunakan 5061 dan *transport* menggunakan TLS. *Port* 5061 digunakan

oleh TLS. Gambar 7 menunjukkan konfigurasi *outbound proxy*, *port*, dan *transport* pada *software Blink.*



Gambar 7. Tab Server Setting pada *Preferences Blink*

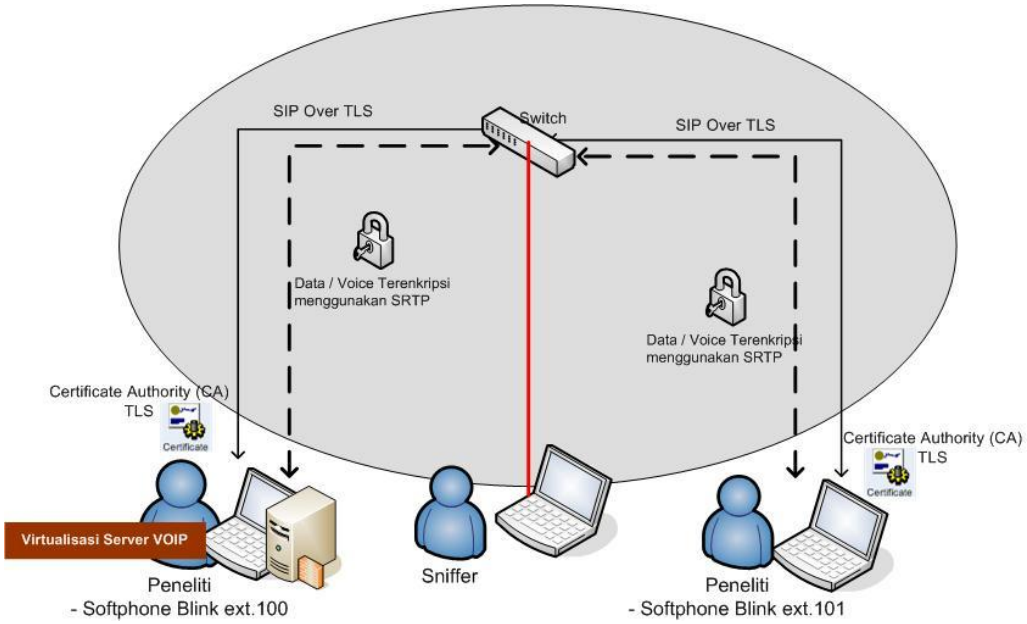
Selanjutnya masuk pada tab Advanced, lalu mengaktifkan TLS menggunakan port 5061. Juga menetapkan lokasi file *Certificate Authority* (CA).



Gambar 8. Tab Advanced pada *Preferences Blink*

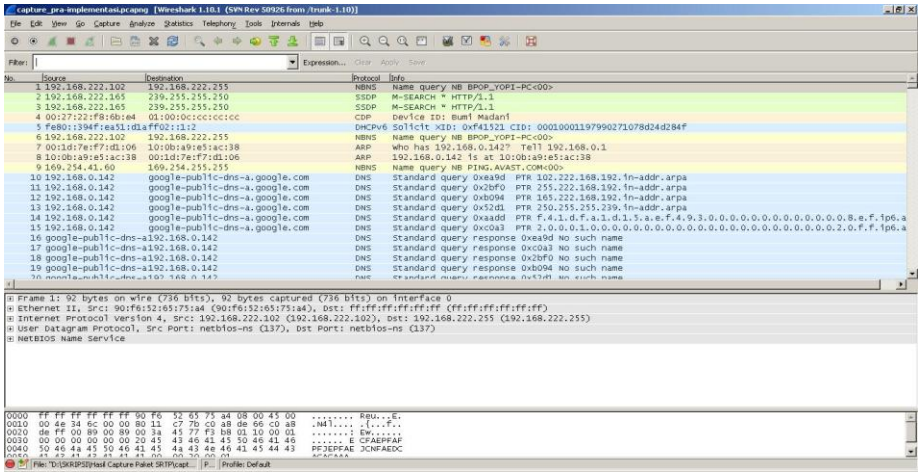
2. Untuk langkah konfigurasi *Softphone Blink* pada laptop peneliti ekstensi 101, dapat merujuk pada langkah-langkah konfigurasi pada *Softphone Blink* ekstensi 100.

Tahap Pengujian Sistem



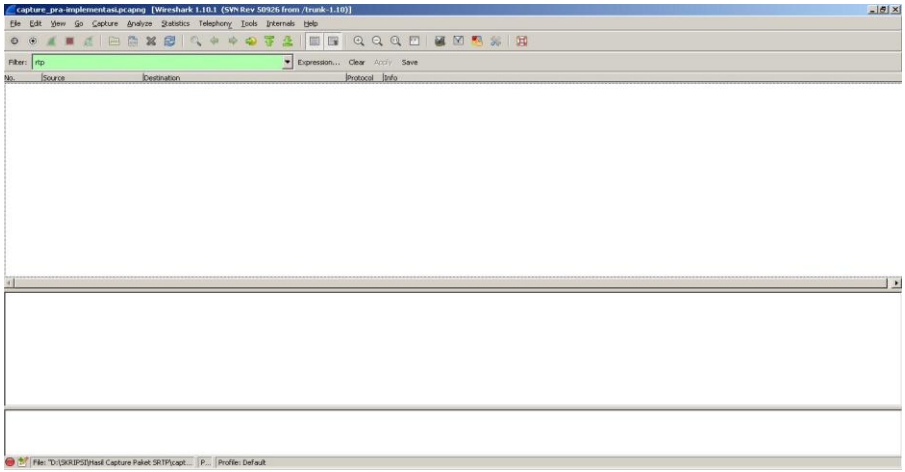
Gambar 9. Topologi saat pengujian

Untuk mengetahui hasil implementasi TLS dan SRTP pada system yang telah dibuat perlu dilakukan pengujian. Gambar 9 menunjukkan topologi pada saat pengujian, penulis menggunakan 3 buah laptop, laptop pertama sebagai SIP Client ekstensi 100, laptop kedua sebagai SIP Client ektensi 101 dan laptop ketiga sebagai Sniffer. Proses pengujian dilakukan dengan melakukan panggilan antara kedua SIP Client yang telah terigester pada SIP server, kemudian laptop sniffer melakukan proses sniffing dengan menggunakan software Wireshark.



Gambar 10. Proses Sniffing pada laptop sniffer menggunakan Wireshark

Pada gambar 10 menunjukkan hasil proses sniffing yang telah dilakukan oleh laptop sniffer, dari gambar tersebut terlihat beberapa protokol IP yang berhasil ditangkap. Untuk mengetahui bahwa software wireshark berhasil atau tidak menangkap paket RTP (Realtime Protocol) perlu dilakukan pencarian paket RTP pada hasil capture. Dengan menggunakan fasilitas filter pada wireshark kita bisa memilih paket-paket apa saja yang akan ditampilkan pada hasil capture, dalam hal ini peneliti menggunkan keyword “rtp” pada kolom filter.



Gambar 11. Hasil filter paket RTP pada Wireshark

Pada gambar 11 menunjukkan bahwa Wireshark tidak menemukan paket RTP. Jika Wireshark dapat menemukan paket RTP maka konfigurasi jaringan VOIP tidak aman dan rentan terhadap upaya pembajakan maupun perusakan system komunikasi.

❖ PENUTUP

Dari hasil pembahasan maka dapat ditarik kesimpun sebagai berikut :

1. Pada hasil pengujian menunjukkan bahwa software sniffer tidak menemukan paket RTP, dengan demikian eksperimen ini berhasil.
2. Implementasi TLS dan SRTP pada VOIP Server terbukti dapat melindungi sistem dari tool penguji dan memperkecil keberhasilan dalam usaha perusakan sistem.

❖ REFERENSI

Asterisk.org. (30 Januari 2014). ***Secure Calling Tutorial,*** diakses 02 Februari 2014 09.24 Wita, dari https://wiki.asterisk.org/wiki/display/AST/

Final, Muhamad Zuhdan, 2009. ***Rancang Bangun dan Analisis VOIP***, Skripsi FTI Universitas Indonesia, Jakarta.

Onno W. Purbo, Anton Raharja. 2011. ***Voip CookBook Building Your Own Telecommunication Infrastructure***, Internet Society Innovation Fund (ISIF).

Raditya, Albert. 2006. ***Studi Algoritma Enkripsi Pada Protokol Secure Real Time Protocol***. Institut Teknologi Bandung, Bandung.

Rizal, Mudrik Alaydrus, Abdi Wahab 2012. ***Jurnal Analisis Kinerja Voip Client Sipdroid Dengan Modul Enkripsi Terintegrasi***. ISSN 1907-5022. Universitas Mercubuana. Jakarta.

Biografi Penulis

M. Fendi Kurniawan

Saat ini penulis aktif sebagai contributor IKC (Ilmu Komputer.com), aktif sebagai Ketua II RelawanTIK Indonesia Wilayah Sulawesi Tenggara, blogger, Internet Sehat Volunteer. Bekerja disalah satu perusahaan TIK di Sulawesi Tenggara sebagai Network Engineer.