1. Pendahuluan

1.1 Latar Belakang

Voice Over Internet Protocol (VOIP) merupakan teknologi yang dapat melewatkan data berupa suara melalui jaringan IP, sedangkan *Voice and Video Over Internet Protocol* (VVOIP) merupakan teknologi yang dapat melewatkan data berupa suara dan video melalui jaringan IP [14]. Sebagai contoh layanan VOIP yaitu panggilan suara, sedangkan layanan VVOIP yaitu layanan panggilan video dan *video conference* [6]. Layanan VOIP atau VVOIP rentan dengan masalah keamanan seperti beberapa kasus yang pernah terjadi yaitu perusahaan di Perth, Australia yang mengalami kerugian sebesar $70.000 diakibatkan adanya panggilan internasional yang dilakukan oleh *hacker* [10]. Selain itu juga pernah terjadi di rumah sakit San Diego, dimana *hacker* mengakibatkan layanan telepon yang ada di rumah sakit tersebut menjadi tidak tersedia selama selama 2 hari [19]. Selain itu juga ada seorang *hacker* bernama HD Moore dimana dia dapat menguping dan mengakses layanan *video conference* seperti pada ruang pertemuan antara pengacara narapidana di penjara, ruang operasi di pusat medis universitas dan ruang pertemuan sebuah perusahaan keuangan [17]. Melihat beberapa kasus yang pernah terjadi membuktikan bahwa saat membangun suatu layanan VOIP dan VVOIP aspek keamanannya merupakan aspek yang penting untuk diperhatikan.

Protokol SIP merupakan salah satu protokol yang dapat digunakan untuk membangun layanan VOIP dan VVOIP. Di dalam protokol SIP memiliki 2 komponen utama yaitu s*ignaling* dan *media stream. Signaling* mengirimkan pesan (memiliki peran seperti *phone registration, ringing, busy signal,* dan *terminate of call)* antara server dengan user. Sedangkan *media stream* yang didalamnya terdapat data berupa suara atau video yang di transportasikan dengan menggunakan RTP (*Real-time Transport Protocol)* [4]. Pada umumnya SIP hanya menyediakan fasilitas keamanan yang terbatas hanya dalam autentifikasi dengan user berdasarkan password. Apabila menggunakan protokol SIP yang masih standar tanpa adanya penambahan sistem keamanan masih dapat terkena beberapa serangan seperti *information gathering* [18], *attacking authentication* [18], *eavesdropping* [16], *denial of service* [16], *media alteration* [16] dan *false caller-ID* oleh *attacker* [16]. Salah satu solusi untuk mengamankan data yang mengalir pada layanan VOIP dan VVOIP yaitu dengan dilakukannya proses enkripsi dan deskripsi, seperti dengan menggunakan TLS (*Transport Layer Security*) untuk komponen *signaling* dan ZRTP (*Zimmermann Real-Time Protocol*) untuk komponen *media stream* [4]. Dengan adanya pengamanan yang berikan maka perlu perhatikan beberapa aspek dalam dimensi keamanan berdasarkan ITU-T (*International Telecommunication Union Telecommunication Standardization Sector)* X.805 seperti *authentication, data confidentiality, data integrity* dan *availability* [11].

Dalam TLS semua data *signaling* di kirimkan dalam bentuk data yang terenkripsi. Dalam menggunakan protokol TLS pada sesi *signaling,* dilakukan pertukaran kunci yang biasa disebut TLS *handshake.* Pada saat melakukan TLS *handshake*, dimana *client* memvalidasi sertifikat yang dikirimkan *server* lalu melanjutkan proses untuk mendapatkan kunci dari enkripsi [21]. ZRTP

menggunakan Diffie-Hellman (DH) *key exchange* pada saat proses *key agreement*, setelah *key agreement* berhasil dan mendapatkan kunci untuk enkripsi RTP, maka data suara maupun video pada RTP akan dienkripsi seperti pada SRTP (*Secure RTP)*[20].

Oleh karena itu tugas akhir ini akan menganalisis keamanan pada layanan VOIP dan VVOIP untuk panggilan suara dan video yang menggunakan sistem keamanan TLS dan ZRTP terhadap serangan-serangan yang disebutkan sebelumnya.

1.2 Perumusan Masalah

Berdasarkan latar belakang yang dipaparkan, berikut adalah rumusan masalah yang dapat dirumuskan:

a. Bagaimana pengaruh sebelum dan sesudah penerapan TLS dan ZRTP pada dimensi keamanan *authentication*, *data confidentiality*, *data integrity*, dan *availability* terhadap serangan yang dilakukan?
b. Bagaimana mengukur performansi terhadap parameter waktu proses register yang dibutuhkan pada TLS, waktu proses enkripsi pada ZRTP dan pengaruh sebelum dan sesudah penerapan ZRTP terhadap parameter *end-to-end delay, jitter,* dan *throughput*?

1.3 Batasan Masalah

Dalam penelitian ini adapun batasan-batasan yang digunakan sebagai berikut:

a. Server VOIP dan VVOIP yang digunakan menggunakan SIP dengan menggunakan *freeswitch*.
b. Jaringan yang dibangun hanya untuk jaringan lokal dan merupakan jaringan kabel.
c. Menggunakan IPv4 kelas C.
d. Hanya untuk layanan panggilan suara dan panggilan video.
e. Implementasi dilakukan pada sebuah *testbed* atau *prototype* layanan VOIP dan VVOIP.
f. Metode penyerangan hanya dengan *information gathering, attacking authentication, eavesdropping, denial of service*, *media alteration* dan *false caller-ID.*
g. Dimensi keamanan yang digunakan adalah *authentication*, *data confidentiality*, *data integrity*, dan *availability.*

1.4 Tujuan

Tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut:

a. Menganalisis pengaruh sebelum dan sesudah penerapan TLS dan ZRTP pada dimensi keamanan *authentication, data confidentiality, data integrity*, dan *availability* berdasarkan serangan-serangan yang dilakukan.
b. Menganalisis hasil waktu proses *register* pada TLS, waktu proses enkripsi paket RTP pada ZRTP dan pengaruh sebelum dan sesudah penerapan ZRTP terhadap parameter *end-to-end delay, jitter,* dan *throughput*.

1.5 Hipotesa

Dari penelitian ini dapat diambil hipotesa bahwa dengan adanya penambahan keamanan dengan TLS dan ZRTP dalam layanan VOIP dan VVOIP tersebut maka akan dapat lebih menjamin dalam dimensi keamanan *authentication, data confidentiality, data integrity* dan *availability* dibandingkan tanpa penerapan sistem keamanan. Dengan adanya penambahan keamanan maka hasil performansinya akan menjadi lebih buruk dengan adanya penambahan nilai pada *end-to-end delay, jitter, throughput* dan waktu proses register. Pada penggunaan ZRTP karena menggunakan media RTP untuk proses pembentukan kunci maka paket RTP yang dikirimkan tidak dapat langsung dienkripsi dan membutuhkan waktu hingga paket RTP tersebut terenkripsi.

1.6 Metodologi Penyelesaian Masalah

Tahapan-tahapan yang dilakukan dalam penyelesaian tugas akhir ini adalah sebagai berikut:

a. Studi literatur
   Studi literatur dilakukan dengan membaca materi yang terkait seperti VOIP, VVOIP, *freeswitch,* TLS, ZRTP yang diperoleh melalui media *internet,* buku, artikel, *paper, publication(magazine),* dll.
b. Perencanaan
   Perancanaan yang dilakukan dalam pengerjaan penelitian ini dilakukan dengan menyiapkan segala sesuatu yang dibutuhkan untuk menyelesaikan tugas akhir ini dan mempersiapkan *software* seperti *softphone, freeswitch, operating system,* mikrotik, dll dan *hardware* seperti komputer, *switch,* kabel UTP, dll.
c. Perancangan
   Melakukan perancangan arsitektur jaringan dan skenario uji yang akan dibuat berdasarkan materi dan konsep-konsep VOIP, VVOIP, *freeswitch,* TLS, ZRTP yang sudah dipelajari pada saat studi literatur.
d. Implementasi
   Melakukan implementasi layanan VOIP dan VVOIP dari tahapan-tahapan yang sudah dirancang pada tahapan perancangan.
e. Pengujian
   Melakukan pengujian terhadap topologi yang sudah dibuat untuk membangun layanan VOIP dan VVOIP apakah semuanya berfungsi dengan baik dan juga melakukan pengambilan data dengan menerapkan scenario-skenario pengujian yang sudah dirancang.
f. Analisis
   Melakukan analisis terhadap dimensi keamanan dan performansi dari data yang sudah didapatkan pada saat pengujian berdasarkan skenario-skenario yang sudah dirancang.
g. Pembuatan Laporan
   Tahap akhir dari tugas akhir ini yaitu dengan membuat laporan dari hasil penelitian yang telah dilakukan sebagai bukti dan dokumentasi terhadap pengerjaan selama melakukan penelitian ini.