Daftar Tabel

1. Pendahuluan

1.1 Latar Belakang

Sebagai salah satu media komunikasi yang sering digunakan banyak orang, terutama masyarakat Indonesia, telepon atau *handphone* terus dikembangkan dalam hal teknologi. Dewasa ini, untuk dapat melakukan komunikasi melalui media telepon tidak hanya melalui jaringan PSTN, melainkan juga bisa melalui jaringan Internet, yaitu VoIP (*Voice over Internet Protocol*).

IP *Multimedia Subsystem* (IMS) merupakan sebuah teknologi jaringan yang mendukung sejumlah media komunikasi, salah satunya VoIP. IMS hadir atas alasan ketidakstabilan kualitas layanan yang berbasiskan IP. IMS diciptakan untuk mengatasi masalah tersebut, yaitu dengan memberikan penjaminan atas kualitas data yang ditransmisikan pada suatu layanan, salah satunya dalam hal keamanan. Dalam penjaminan data, protokol keamanan tentu sangat dibutuhkan, agar data yang ditransmisikan berjalan dengan aman dari asal sampai tujuannya tanpa perlu khawatir terjadi pencurian di tengah perjalanannya.

Session Description Protocol Security Descriptions (SDES) merupakan salah satu cara yang dapat diimplementasikan untuk menegosiasikan *Real-time Transport Protocol* (RTP) agar melakukan pengamanan data. SDES digunakan dalam pertukaran *encryption mutual key* pada pengirim dan penerima data, sehingga *payload* tidak dapat diterjemahkan oleh *end-user* yang tidak memiliki kunci pertukaran tersebut.

Penambahan fitur (keamanan) tentu memengaruhi waktu sistem dalam memproses data, oleh karena itu perlu dilakukan juga analisis terhadap waktu pada jaringan yang mengimplementasikan dan tidak mengimplementasikan jenis pengamanan ini.

1.2 Perumusan Masalah

Berdasarkan latar belakang tersebut, maka dapat dirumuskan permasalahannya sebagai berikut.

a. Apakah proses pertukaran kunci menggunakan SDES dapat melindungi *client* dari tindakan penyadapan (*sniffing*) VoIP?
b. Bagaimana pengaruh implementasi SDES terhadap *invite time*?

1.3 Tujuan

Tugas akhir ini memiliki tujuan untuk mendapatkan analisis kapabilitas SDES dalam mengamankan data VoIP antara dua *client* yang saling berkomunikasi berdasarkan parameter *confidentiallity*, serta diketahui presentase penambahan waktu yang dibutuhkan jaringan SDES dalam melakukan *invite*.

1.4 Batasan Masalah

Pembatasan masalah dalam pengerjaan tugas akhir ini adalah sebagai berikut.

a. Server IMS diimplementasikan di sebuah komputer menggunakan *software* OpenIMSCore.
b. Layanan IMS yang digunakan hanya VoIP.
c. Server dijalankan di atas sistem operasi Ubuntu 10.04.
d. Server mengimplementasikan *Transport Layer Secure* (TLS) terhadap *client*-nya.
e. Tidak membahas mengenai QoS.
f. IMS *client* yang melakukan *Invite* dan *sniffer* berada dalam satu jaringan yang sama.
g. Tidak membahas mengenai proses pembuatan atau pendefinisian kunci, serta cara melakukan enkripsi dan dekripsi payload.

1.5 Hipotesis

SDES memberi pengamanan data yang lebih baik dibanding tanpa menggunakannya, sebab *payload* hanya dapat diterjemahkan jika memiliki kunci pertukaran SDES.

1.6 Metodologi Penyelesaian masalah

Untuk menyelesaikan permasalahan, dibuatlah susunan kegiatan yang harus dilakukan, yaitu sebagai berikut.

a. Identifikasi Masalah
   IMS merupakan sebuah *framework* yang dapat menjembatani berbagai teknologi jaringan. Implementasi IMS pada jaringan diharapkan dapat menjamin kualitas data yang ditransmisikan. Untuk dapat menjamin kualitas data, diperlukan pengamanan pada setiap *layer* punyusunnya, salah satunya pada *transport layer*. VoIP merupakan layanan yang paling sering diterapkan di IMS dewasa ini, oleh karena itu pengamanan perlu diterapkan pada layanan ini. Pengamanan itu salah satunya bisa diterapkan menggunakan SDES pada *transport layer*. SDES mempertukarkan kunci untuk mengamankan *Real-time Transport Protocol* (RTP).
b. Studi Literatur
   Pada tahap ini, dilakukan pengumpulan literatur terkait dengan IMS, SIP, SDES, VoIP, TLS, dan SRTP dari berbagai sumber, seperti Internet dan buku. Selain itu, dilakukan diskusi bersama pembimbing tugas akhir, teman, dan anggota laboratorium yang terkait.
c. Melakukan Perancangan
   Sebelum SDES diterapkan, perlu diidentifikasi arsitektur, topologi, dan perangkat yang dibutuhkan terkait dengan penelitian ini.
d. Implementasi Sesuai Perancangan
   Setelah dilakukan perancangan, penelitian dimulai dari pengidentifikasian aliran SDES dalam mempertukarkan kunci hingga pengujian keamanan terhadap tindakan *sniffing* (penyadapan)

e. Penyusunan Laporan
   Setelah *traffic* SDES dapat diidentifikasi dan diuji terhadap tindakan *sniffing*, maka dapat ditarik kesimpulan untuk kemudian dijadikan laporan karya ilmiah.

1.7 Sistematika Penulisan

BAB I Pendahuluan

Bab ini menguraikan tugas akhir ini secara umum, meliputi latar belakang masalah, perumusan masalah, tujuan, batasan masalah, dan metode yang digunakan

BAB II Landasan Teori

Bab ini membahas mengenai teori-teori atau pustaka yang berhubungan dengan IMS, SDES, VoIP, dan SRTP.

BAB III Perancangan dan Implementasi Sistem

Pada bagian ini diuraikan langkah-langkah yang harus dipersiapkan sebelum dilakukan penelitian. Persiapan itu meliputi penyediaan perangkat keras serta instalasi dan konfigurasi perangkat lunak, kemudian pengimplementasian masalah sesuai skenario.

BAB IV Pengujian dan Analisis

Setelah skenario berhasil diimplementasikan, pada bab ini diuraikan hasil analisis terhadap skenario tersebut.

BAB V Kesimpulan dan Saran

Bab ini berisi kesimpulan dari pengerjaan Tugas Akhir ini serta saran-saran yang diperlukan untuk pengembangan lebih lanjut.