Abstrak

IP Multimedia *Subsystem* (IMS) merupakan salah satu *server system* yang dapat menangani sejumlah layanan, salah satunya VoIP (*Voice over Internet Protocol*). Dalam pengimplementasiannya, VoIP ditransmisikan melalui *Real-time Transport Protocol* (RTP) yang notabene tidak memiliki kekuatan dalam hal keamanan. Atas dasar tersebut, maka hadir sejumlah metode yang dapat digunakan untuk mengamankan RTP, terutama dari tindakan *sniffing* (penyadapan), yaitu dengan *Session Description Protocol Security Descriptions* (SDES).

SDES mengamankan RTP dengan cara mempertukarkan kunci simetris, sehingga hanya yang memiliki kunci inilah yang dapat mengenkripsi dan mendekripsi pesan suara yang ditransmisikan dan diterima. Namun, untuk dapat melakukan pertukaran kunci tersebut, harus ada protokol yang menjamin keamanan selama terjadi pertukaran kunci. Oleh akrena itu digunakan protokol TLS.

Laporan tugas akhir ini berisi pembahasan mengenai proses yang terjadi pada SDES ketika *client* dari IMS server melakukan pertukaran kunci dengan *client* dari non-IMS server, dalam hal ini Asterisk server. Kemudian dilakukan pengujian keamanan terhadap tindakan *sniffing*.

Berdasarkan hasil pengujian didapatkan bahwa SDES memberi perlindungan yang optimal atas tindakan *sniffing* terhadap pesan suara yang ditrasmisikan antar-server, serta memiliki *invite time* yang hampir sama dengan jaringan yang tidak mengimplementasikan SDES.

Kata Kunci: a *crypto*, *invite time*, TLS, VoIP