BAB 1
PENDAHULUAN

1.1 Latar Belakang Masalah

VoIP *server* berfungsi sebagai penyedia layanan VoIP. *Initiator* (pemanggil) akan menghubungi VoIP *server* dan memberi informasi bahwa akan menghubungi *responder* (penerima panggilan). VoIP *Server* akan menghubungi responder, dan apabila responder memilih untuk menerima panggilan, maka panggilan akan dihubungkan antara *initiator* dan *responder*. Seluruh proses tersebut berjalan di jaringan internet. Karena itu aspek keamanan merupakan hal yang perlu diperhatikan untuk menjaga keberlangsungan komunikasi VoIP.

Demi menjaga keamanan komunikasi voip maka terdapat tiga metoda yang bisa digunakan, yaitu TLS (*Transport Layer Security*), TLS menyamarkan layer protokol dari VoIP dalam sebuah jaringan, sehingga sulit untuk dideteksi atau diblok. SRTP (*Secure Realtime Transport Protocol*), meng-enkripsi suara dari client ke server, tetapi pengguna yang memiliki akses ke server dapat membaca suara tersebut. *Zimmerman Realtime Transport Protocol* (ZRTP), ZRTP menggunakan public *key cryptography* sehingga enkripsi dapat tersampaikan dari pemanggil dan penerima tanpa diketahui server ataupun pihak ketiga.

ZRTP menghasilkan *shared secret* antara dua *initiator* dan *responder* yang kemudian digunakan untuk menghasilkan kunci Secure RTP (SRTP). ZRTP menggunakan pertukaran kunci *Diffie-Hellman* yang menegosiasikan kunci untuk mengenkripsi suara pada komunikasi VoIP. Pertukaran kunci tersebutlah yang akan menjaga suara atau komunikasi dari serangan pada komunikasi VoIP. Sehingga enkripsi yang dihasilkan adalah end to end antara pemanggil dan penerima. Hal tersebut yang menjadi keunggulan dari ZRTP dibanding metoda pengamanan VoIP yang lainnya.

Dalam tugas akhir ini akan membahas aspek keamanan dalam komunikasi VoIP menggunakan *Zimmerman Realtime Transport Protocol* serta penerapannya

menggunakan metode *Diffie – Hellman* sebagai proses pertukaran kunci antara *initiator* dan *responder*. Lalu melakukan perbandingan keamanan antara sistem voip yang menggunakan zrtp dan tidak menggunakan zrtp.

1.2 Rumusan Masalah

Berdasarkan uraian latar belakang yang dikemukakan diatas, maka didapat permasalahan utama yaitu :

1. Bagaimana meningkatkan keamanan komunikasi voip untuk menghindari penyadapan
2. Bagaimana metode yang digunakan ZRTP untuk mengatasi penyadapan
3. Bagaimana perbandingan sistem komunikasi yang menggunakan ZRTP dan tidak

1.3 Maksud dan Tujuan

1.3.1 Maksud

Berdasarkan Permasalahan yang ada, maka maksud dari penelitian yang dilakukan adalah melakukan analisa dan implementasi terhadap *Zimmerman Real Transport Protocol* (ZRTP) sebagai pengamanan data pada *Voice over Internet Protocol* (VoIP).

1.3.2 Tujuan

Tujuannya melakukan penerapan ini adalah *Zimmerman Real Transport Protocol* (ZRTP) sebagai pengamanan data pada *Voice over Internet Protocol* sebagai berikut :

1. Meningkatkan keamanan untuk menghindari penyadapan pada komunikasi VoIP.
2. Melakukan analisa terhadap cara kerja ZRTP dalam mengenkripsi komunikasi data pada *Voice over Internet Protocol*.
3. Melakukan pengujian perbandingan keamanan terhadap sistem VoIP yang menggunakan ZRTP dan tidak menggunakan ZRTP.

1.4 Batasan Masalah

Agar pembahasan permasalahan tidak menyimpang dari pokok bahasan, maka perlu adanya batasan permasalahan. Dalam penelitian ini, penulis membatasi masalah sebagai berikut :

1. Metode Pertukaran Kunci menggunakan *Diffie – Hellman*
2. VoIP *server* menggunakan GNU Sipwitch 1.5
3. *Operating System* yang digunakan Ubuntu 12.04
4. VoIP server yang tidak menggunakan ZRTP dan menggunakan ZRTP, memiliki versi dan berjalan pada *Operating System* yang sama.

1.5 Metodologi Penelitian

Metodologi penelitian merupakan suatu proses yang digunakan untuk memecahkan suatu masalah yang logis, dimana memerlukan data-data untuk mendukung terlaksananya suatu penelitian. Metode penelitian yang digunakan dalam penulisan tugas akhir ini adalah sebagai berikut :

a. *Observasi* (Pengamatan)

   Teknik Pengumpulan data dengan mengadakan penelitian dan peninjauan langsung terhadap permasalahan yang diambil.

b. Studi Literatur

   Pengumpulan data dengan cara :

   1. Mengumpulkan literatur, jurnal, *paper* dan bacaan yang ada kaitannya dengan judul penelitian
   2. Mempelajari dasar-dasar penerapan *Zimmerman Realtime Transport Protocol* pada voice over internet protocol

c. Perumusan Masalah

   Rumusan masalah yang mempertanyakan suatu fenomena, baik dalam kedudukannya sebagai fenomena mandiri, maupun kedudukannya sebagai fenomena yang saling terkait antara fenomena yang satu dengan yang lainnya, baik sebagai penyebab maupun sebagai akibat.

d. Eksperimen

Eksperimen yang dilakukan penulis adalah mengumpulkan data mengenai kebutuhan sistem, penerapan ZRTP sebagai pengamanan data pada *VoIP*.

e. Pemodelan Simulasi

Pemodelan simulasi merupakan suatu teknik meniru operasi-operasi atau proses- proses yang terjadi dalam suatu sistem dengan bantuan perangkat komputer dan dilandasi oleh beberapa asumsi tertentu sehingga sistem tersebut bisa dipelajari secara ilmiah.

f. Pengujian

Penguujian dilakukan dengan membandingan keamanan dari komunikasi voip yang telah menggunakan ZRTP dan tidak menggunakan. Proses pengujian dilakukan dengan menggunakan metode *Man in The Middle Attack* dengan tujuan untuk melakukan penyadapan terhadap komunikasi VoIP.

1.6 Sistematika Penulisan

Sistematika penulisan proposal penelitian ini disusun untuk memberikan gambaran umum tentang penelitian yang dijalankan. Sistematika penulisan tugas akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Menguraikan tentang latar belakang permasalahan, mencoba merumuskan inti permasalahan yang dihadapi, menentukan tujuan dan kegunaan penelitian, yang kemudian diikuti dengan pembatasan masalah, asumsi, serta sistematika penulisan sebagai ringkasan materi dari masing masing bab.

BAB II. TINJAUAN PUSTAKA

Membahas berbagai konsep dasar dan teori-teori yang berkaitan dengan topik penelitian yang dilakukan dan hal-hal yang berguna dalam proses analisis permasalahan serta tinjauan terhadap penelitian-penelitian serupa yang telah pernah dilakukan sebelumnya termasuk sintesisnya. Teori penunjang yang

berhubungan dengan penerapan *Zimmerman Realtime Transport Protocol* diantaranya teori mengenai sistem keamanan jaringan, VoIP, SIP dan enkripsi data.

BAB III. ANALISIS DAN PERANCANGAN

Menganalisis masalah dari model penelitian untuk memperlihatkan keterkaitan antar variabel yang diteliti serta model matematis untuk analisisnya. Hasil dari analisis tersebut digunakan untuk melakukan perancangan perangkat keras dan lunak

BAB IV. IMPLEMENTASI DAN PENGUJIAN SISTEM

Bab ini menjelaskan implementasi sistem intrusi, dijelaskan mengenai konfigurasi sistem dan instalasi perangkat lunak yang dibutuhkan. Pada bab ini juga dijelaskan pemaparan dari proses translasi dari tahap analisis dan perancangan ke tahap konfigurasi sehingga terbentuk sistem yang sesuai dengan hasil analisis dan perancangan

BAB V. KESIMPULAN DAN SARAN

Berisi kesimpulan dan saran yang sudah diperoleh dari hasil penulisan tugas akhir. Pada bab ini akan dibahas mengenai kesimpulan dari keseluruhan masalah yang telah dibahas pada bab sebelumnya dan dilengkapi dengan saran-saran.