**JURUSAN TEKNIK INFORMATIKA**

**FAKULTAS TEKNOLOGI INFORMASI**

**INSTITUT TEKNOLOGI SEPULUH NOPEMBER**

**USULAN TUGAS AKHIR**

1. **IDENTITAS PENGUSUL**

**NAMA : Kadek Dwijaya Suryawan**

**NRP : 5108 100 093**

**DOSEN WALI : Umi Laili Yuhana, S.Kom.,M.Sc.**

1. **JUDUL TUGAS AKHIR**

***“Analisis Layanan Kinerja Jaringan VoIP Pada Protokol SRTP dan VPN”***

1. **LATAR BELAKANG**

Pada masa kini, teknologi jaringan komputer mengalami perkembangan yang sangat cepat, dimana teknologi tersebut memungkinkan untuk saling bertukar informasi dan data, bahkan dapat saling berkomunikasi dan bertukar informasi berupa suara atau video secara langsung. Dengan perkembangan teknologi jaringan komputer, memungkinkan kita untuk bertukar informasi melalui media suara yang dikenal dengan *VoIP (Voice Over Internet Protocol)*.

VoIP adalah teknologi yang menawarkan layanan transmisi suara secara langsung melalui internet dengan menggunakan protokol TCP/IP. Dengan teknologi ini mengubah suara menjadi kode digital melalui jaringan paket-paket data, bukan melalui sirkuit analog telepon biasa atau yang biasanya disebut dengan *PSTN (Public Switching Telephone Network)*. Teknologi ini dapat menghemat biaya komunikasi, karena teknologi ini bersifat gratis.

Namun, komunikasi menggunakan VoIP tidak memiliki jaminan keamanan terhadap data paket pada setiap komunikasi suara yang dilakukan. Hal tersebut disebabkan oleh media transmisi paket data yang melalui *unprotected network* pada jaringan *public* internet, sehingga memungkinkan untuk pihak yang tidak berwenang untuk melakukan penyadapan komunikasi. Macam-macam gangguan yang terjadi pada data yang melewati suatu jaringan antara lain: data disalah gunakan *(abuse)*, pembajakan dari isi data *(sniffing)*, dan tidak dapat mengakses server dikarenakan server kelebihan muatan *(denial of service)*. Salah satu upaya penanggulangan terhadap usaha penyadapan yang dilakukan oleh pihak yang tidak berwenang adalah menambah keamanan pada arsitektur VoIP. Beberapa metode pengamanan pada VoIP seperti menggunakan SRTP *(Secure Real Time Protocol)*, atau dapat juga dengan menggunakan VPN *(Virtual Private Network)*. Sebaliknya, dengan menggunakan beberapa metode keamanan dalam jaringan VoIP, maka semakin berat juga hambatan yang dilalui oleh data tersebut karena data akan melewati beberapa tahap keamanan sebelum pada akhirnya terkirim pada tujuannya yang menyebabkan *Delay*.

Teknologi VoIP mungkin sangat menguntungkan bagi para penggunanya, karena menyediakan media komunikasi yang murah, namun sedikit yang sadar dengan sisi keamanan pada VoIP itu sendiri. Sehingga perlu ditambahkan proteksi pada arsitektur VoIP demi terjaganya privasi dari komunikasi, selain itu juga perlu sedikit dipertimbangkan terkirimnya data secara *real-time* agar tercapainya *Quality Of Service* (QoS) pada jaringan VoIP.

QoS adalah isu utama dalam implementasi sebuah jaringan VoIP. Tujuan dari QoS dalam sebuah jaringan VoIP adalah menjamin lalu lintas paket suara atau media koneksi tidak akan ditunda, atau terjadi gangguan akibat lalu lintas lain yang memiliki prioritas lebih rendah.

1. **TUJUAN**

Tujuan pembuatan tugas akhir ini adalah untuk mengetahui kinerja dan keamanan jaringan VoIP yang menerapkan penggunaan protokol SRTP dan VPN.

1. **PERMASALAHAN**

Adapun yang menjadi permasalahan utama dalam tugas akhir ini :

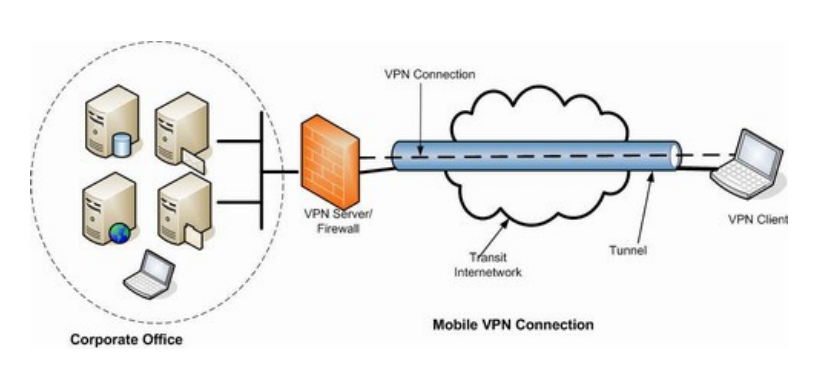
1. Bagaimana cara mengimplementasikan protokol SRTP dan VPN dalam jaringan VoIP?
2. Metode apakah yang baik untuk digunakan dalam tujuan mencapai keamanan dalam jaringan VoIP demi tercapainya QoS?
3. **BATASAN MASALAH**

Dari permasalahan yang telah diuraikan di atas, terdapat beberapa batasan masalah terhadap tugas akhir ini, yaitu :

1. Implementasi dilakukan pada jaringan VoIP dengan menggunakan protokol SRTP dan protokol VPN.
2. Pengujian dilakukan pada jaringan VoIP yang menggunakan sistem keamanan dan tanpa sistem keamanan.
3. Server yang digunakan adalah asterisk dan VoIP menggunakan protokol SIP dan menggunakan aplikasi *softphone* untuk melakukan pengujian panggilan.
4. Pengukuran menggunakan *software network protocol analyzer* seperti: Aethereal, sebagai pengukur kualitas VoIP dan pengujian keamanan menggunakan *software network traffic analyzer* seperti: Wireshark.
5. Parameter yang digunakan untuk pengukuran QoS adalah *delay*, *jitter*, dan *packet loss*.
6. Sebagai bahan pengukuran kualitas VoIP secara subjektif, dilakukan analisis MOS *(Mean Opinion Score)* terhadap 20 responden.
7. **RINGKASAN ISI TUGAS AKHIR**

Tugas akhir ini akan membangun dan menganalisis 2 buah arsitektur keamanan yang berbeda pada jaringan VoIP. Arsitektur yang pertama adalah *Secure Real Time Protocol (SRTP)*, SRTP merupakan protokol *Real Time Protocol (RTP)* yang menyediakan layanan enkripsi, otentifikasi, dan integritas pesan. SRTP sangat ideal untuk melindungi VoIP, karena dapat digunakan bersama dengan kompresi *header*, sehingga data yang melewati protokol ini menjadi lebih aman. Protokol ini terdapat pada *Layer Transport*. SRTP sangat menguntungkan untuk VoIP yang menggunakan *codec* suara dengan *bitrate* rendah seperti G.729 dan iLBC. SRTP akan dibangun pada sebuah server VoIP yang berbasis Asterisk.

Arsitektur keamanan VoIP yang kedua adalah menggunakan IPsec dalam sebuah VPN. VPN adalah teknik pengamanan jaringan dengan cara membuat suatu *Tunnel* pada jaringan public atau internet, sehingga jaringan bersifat *private* dan aman. VPN bersifat *private* karena terbentuknya sebuah koneksi VPN dibutuhkan otentifikasi untuk memastikan bahwa kedua ujung dalam koneksi adalah pengguna yang sesuai yang diberi kewenangan untuk mengakses suatu *server*. Pada VPN, *Tunnel* bertugas untuk menangani dan menyediakan koneksi *point-to-point* dari sumber ke tujuannya, *Tunnel* tersebut dilengkapi dengan teknologi enkripsi untuk melindungi data-data yang melewati *Tunnel* tersebut. Berikut penjelasan tentang VPN terdapat pada Gambar 1.



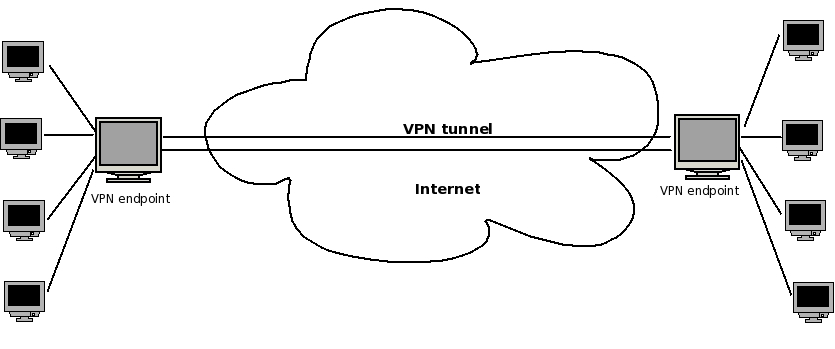
Gambar 1. Virtual Private Network

[http://nirlog.com/2006/01/23/secure-remote-access-ssl-vpn/]

IPsec adalah sebuah framework  standar terbuka yang dikembangkan oleh Internet Engineering Task Force (IETF). IPSec ini juga menyediakan keamanan untuk transmisi informasi yang bersifat sensitif melalui jaringan yang tanpa proteksi dan bebas seperti internet. IPsec yang dijalankan pada layer ke 3 yaitu network pada jaringan, yang berfungsi untuk melindungi dan melakukan otentifikasi paket IP antara device IPsec (*peer*). Pengertian IPSec ini juga adalah sebuah standar protokol yang menyediakan fasilitas layanan keamanan pada komunikasi internet. IPSec ini pada keamanan juga melindungi keseluruhan datagram dalam mode *end-to end* di mana tidak ada node jaringan *intermediate* pada internet publik yang dapat mengakses atau memodifikasi informasi pada layer IP dalam sebuah paket yang dilindungi oeh IPsec.

IPsec dapat bekerja pada 2 mode yaitu mode *Transport* dan mode *Tunnel*. Pada mode transport IPsec melakukan pengamanan terhadap yang dikirimkan pada layer *transport* ke layer *network*. Pada mode ini IPsec juga tidak melakukan proteksi terhadap IP *header*. IPsec pada mode ini normalnya digunakan saat pengamanan data secara *host-to-host*. Pada mode tunnel IPsec melakukan proteksi terhadap seluruh paket IP termasuk headernya. IP *header* yang dihasilkan akan memiliki informasi yang berbeda dari pada IP *header* asli.

Pada Gambar 2, terdapat gambar arsitektur IPsec yang menempatkan *security gateway* (G1 dan G2) pada masing masing batasan jaringan lokal yang aman dan jaringan publik yang tidak aman yaitu internet. Pada awalnya, G1 sebagai sumber, membangun sebuah hubungan yang aman dengan G2 (tujuan), dimana hubungan tersebut akan melibatkan kerja sama tentang servis keamanan dan rahasia yang akan di bagi melalui sebuah *tunnel* IPsec.



**G2**

**G1**

Gambar 2. IPsec

[http://www.linuxjournal.com/article/9916]

Setelah kedua arsitektur keamanan yang berbeda ini dibangun, dilakukan sebuah pengujian keamanan pada jaringan VoIP. Untuk model serangan yang bisa terjadi pada VoIP terdapat pada Tabel 1 berikut.

|  |  |
| --- | --- |
| **Jenis Serangan** | **Keterangan** |
| *Interception of Calls* | Gangguan yang terjadi apabila *hacker* memiliki akses fisik terhadap jaringan LAN yang digunakan oleh paket VoIP. |
| *Denial of Service Attacks* | Jenis serangan ini bertujuan menghabiskan *resource* dari suatu elemen dalam jaringan, biasanya dengan mengirimkan paket dalam jumlah besar ke suatu target (*network flooding*). |
| *Theft of Service* | Serangan jenis ini melakukan pencurian informasi pada VoIP, biasanya dilakukan dengan cara penyadapan (*sniffing*). |
| *Exfiltration of data via Media Session* | Mengirimkan data keluar dari *media session.* Menggunakan RTP sebagai saluran komunikasi rahasia. |
| *Malware embedded in signaling and media session* | Menyisipkan muatan berbahaya (*malware*) pada SIP, RTP, atau *media stream* lainnya. |

Tabel 1. Jenis Serangan pada VoIP.

Keamanan dalam jaringan VoIP merupakan aspek yang penting untuk mewujudkan komunikasi yang aman dan lancar. Keamanan yang akan di uji coba adalah aspek *privacy* yaitu untuk menjaga informasi dari pihak yang tidak berhak untuk mengakses atau melakukan pencurian informasi dalam komunikasi VoIP. Pengujian keamanan VoIP nanti akan menggunakan *software network traffic analyzer* seperti: Wireshark. untuk melakukan uji coba *sniffing* VoIP.

Setelah hasil pengujian, dilakukan analisis berikutnya untuk mencapai nilai QoS dalan jaringan VoIP. QoS mengacu ke tingkat kecepatan dan keandalan penyampaian berbagai jenis beban data di dalam suatu komunikasi, baik data suara atau berupa video. QoS merupakan kumpulan dari beberapa parameter, antara lain:

1. *Availability*, adalah persentase hidupnya sistem atau subsistem telekomunikasi. Idealnya, *availability* harus mencapi nilai 100%. Nilai *availability* yang diakui cukup baik adalah 99,9999% *(six nines)* yang menunjukkan tingkat kerusakan sebesar 2,6 detik per bulan.
2. *Throughput*, adalah kecepatan transfer data efektif, yang diukur dalam satuan bps *(bit-per-second)*.
3. *Delay*, adalah waktu tunda yang disebabkan oleh proses transmisi dari satu titik ke titik lain yang menjadi tujuannya. Jenis-jenis dari *Delay* akan dijelaskan pada Tabel 1.

|  |  |
| --- | --- |
| **Jenis Delay** | **Keterangan** |
| *Algorithmic Delay* | *Delay* ini disebabkan oleh standar codec yang digunakan.Contohnya, *Algorithmic delay* untuk G.723.1 adalah 7.5 ms |
| *Packetization Delay* | *Delay* yang disebabkan oleh peng-akumulasian bit voice sample ke *frame*. Seperti contohnya, standar G.711 untuk payload 160 bytes memakan waktu 20 ms |
| *Serialization Delay* | *Delay* ini terjadi karena adanya waktu yang dibutuhkan untuk pentransmisian paket IP dari sisi *originating* (pengirim). |
| *Propagation Delay* | *Delay* ini terjadi karena perambatan atau perjalanan. Paket IP di media transmisi ke alamat tujuan. Seperti contohnya delay propagasi di dalam kabel akan memakan waktu 4sampai 6 µs per kilometernya. |
| *Component Delay* | *Delay* ini disebabkan oleh banyaknya komponen yang digunakan di dalam sistem transmisi. |

Tabel 2. Jenis-jenis *Delay*.

Rekomendasi ITU-T [5] G.114 merekomendasikan standar *delay*. Terdapat 3 kualifikasi yang ditunjukkan ITU-T untuk *delay* seperti pada Tabel 2.

|  |  |
| --- | --- |
| **Jarak Dalam Milisecon** | **Keterangan** |
| 0 – 150 msec | Dapat diterima oleh banyak pengguna aplikasi. |
| 150 – 400 msec | Diterima asalkan administrator menyadari waktu transmisi dan hal tersebut berdampak pada kualitas transmisi dari aplikasi pengguna. |
| >400 msec | Tidak dapat diterima untuk tujuan perencanaan jaringan umum. |

Tabel 3. Rekomendasi ITU-T G.114 untuk *Delay*.

1. *Jitter*, adalah perbedaan selang waktu kedatangan antar paket di terminal tujuan. Jitterdapat disebabkan oleh terjadinya kongesti, kurangnya kapsitas jaringan, variasi ukuran paket, serta ketidakurutan paket.
2. *Packet Loss*, adalah dari data (packet packet) yang dikirim ke server yang tidak pernah sampai. apapun nilainya jika diatas 0% harusnya menjadi perhatian karena akan menghasilkan kualitas yang buruk pada VoiP.

Di dalam analisis yang akan dilakukan, tingkat penurunan kualitas yang disebabkan oleh transmisi data memegang peranan penting terhadap kualitas suara yang dihasilkan. Hal yang menjadi penyebab penurunan QoS yang akan di analisis secara objektif adalah *Delay*, *Packet Loss*, dan *Jitter.*

Untuk menentukan kualitas layanan VoIP dapat digunakan beberapa parameter yang subjektif dengan menggunakan metode MOS *(Mean Opinion Score)*. Metode ini merupakan metode yang digunakan untuk menentukan kualitas suara dalam jaringan IP yang berdasarkan kepada standar ITU-T P.800. Metode ini bersifat subjektif, karena berdasarkan pendapat perorangan. Untuk mendapatkan nilai MOS, terdapat 2 macam cara pengujian, yaitu *conversation opinion test* dan *listening test*. Rekomendasi nilai dari ITU-T P.800 adalah sebagai yang ditunjukkan pada Tabel 3 berikut.

|  |  |
| --- | --- |
| **Nilai MOS** | **Opini** |
| 5 | Sangat Baik |
| 4 | Baik |
| 3 | Cukup Baik |
| 2 | Tidak Baik |
| 1 | Buruk |

Tabel 4. Rekomendasi ITU-T P.800 untuk nilai kualitas berdasarkan MOS.

Secara garis besar penjelasan tentang pembuatan tugas akhir ini adalah :

1. Implementasi VoIP dengan SRTP dalam upaya pengamanan jaringan VoIP menggunakan protokol SIP.
2. Implementasi VoIP pada VPN IPsec untuk membangun sebuah jaringan VoIP yang terenkripsi.
3. Melakukan pengujian keamanan pada jaringan kedua jaringan VoIP yang berbeda yang telah dibangun tersebut dengan menggunakan *software network traffic analyzer*.
4. Melakukan analisa menggunakan *software network protocol analyzer* sebagai pengukur QoS pada 2 jaringan VoIP yang telah dibangun dengan arsitektur keamanan yang berbeda.
5. Melakukan analisis terhadap 20 responden untuk mendapatkan nilai subjektif MOS, dalam upaya pengukuran kualitas VoIP.
6. **METODOLOGI**

Beberapa tahapan metodologi yang akan dilakukan dalam Tugas Akhir ini, di antaranya sebagai berikut:

1. **Studi Literatur**

Tahap ini merupakan tahap pengumpulan informasi yang diperlukan untuk pengerjaan tugas akhir sekaligus mempelajarinya. Mulai dari pengumpulan literatur, diskusi, serta pemahaman topik tugas akhir.

1. **Perancangan Sistem**

Pada tahap ini dilakukan analisis awal dan pendefinisian kebutuhan sistem untuk mengetahui masalah yang sedang dihadapi. Dari proses tersebut selanjutnya dirumuskan rancangan sistem yang dapat memberi permecahan masalah tersebut.

1. **Konfigurasi dan Implementasi Sistem**

Pada tahap ini dilakukan konfigurasi dan implementasi rancangan sistem yang telah dibuat. Tahapan ini merealisasikan apa yang terdapat pada tahapan sebelumnya sehingga menjadi sebuah jaringan keamanan dsesuai dengan apa yang telah direncanakan.

1. **Pengujian dan Analisis Hasil Implementasi**

Pada tahap ini, kedua protokol keamanan pada jaringan VoIP yang telah selesai dibuat akan diuji. Analisis akan dilakukan dengan menggunakan aplikasi untuk menguji sistem keamanan yang telah diterapkan. Hasil analisa tersebut diharapkan dihasilkan suatu kesimpulan, rekomendasi teknis, dan penelitian selanjutnya.

1. **Penyusunan Buku Tugas Akhir**

Tahap terakhir merupakan penyusunan laporan yang memuat dokumentasi mengenai pembuatan serta hasil dari ujicoba dari implementasi jaringan keamanan yang telah dibuat. Secara garis besar, Buku Tugas Akhir yang nantinya akan dibuat terdiri dari beberapa bagian antara lain

1. Pendahuluan

Menjelaskan mengenai latar belakang, permasalahan, tujuan, batasan permasalahan, metodologi, dan sistematika penulisan. Pendahuluan terdiri dari:

* 1. Latar Belakang
  2. Permasalahan
  3. Batasan Tugas Akhir
  4. Tujuan
  5. Metodologi

1. Landasan Teori

Bab ini membahas beberapa teori penunjang yang berhubungan dengan pokok pembahasan dan mencakupi dasar ilmu yang mendukung pembahasan tugas akhir ini.

1. Implementasi

Berisi tentang konfigurasi dan implementasi dari arsitektur jaringan yang akan dibangun dengan komponen-komponen yang telah ada yang sesuai dengan permasalahan dan batasannya yang telah dijabarkan pada bab pertama.

1. Uji Coba dan Analisis Hasil Implementasi

Jaringan keamanan yang telah selesai ini nantinya juga akan diuji coba berdasarkan parameter-parameter yang ditetapkan dan dievaluasi untuk diperbaiki demi kelayakan sistem dan keberhasilan dari sistem ini sesuai dengan tujuannya dibangun.

1. Kesimpulan dan Saran

Pada bab ini, kesimpulan yang diperoleh dari serangkaian kegiatan terutama pada bagian analisis pengujiannya diungkapkan. Selain itu saran-saran pengembanganlebih lanjut dari tugas akhir yang telah dibuat dituliskan pada bab ini.

1. Daftar Pustaka
2. **JADWAL KEGIATAN**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Kegiatan** | **Bulan** | | | | | | | | | | | | | | | | | |
| **Maret** | | | | **April** | | | | **Mei** | | | | | **Juni** | | | | |
| 1. | Studi Literatur |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
| 2. | Perancangan Sistem |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
| 3. | Implementasi & Pembuatan Jaringan |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
| 4. | Uji Coba dan Evaluasi |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |
| 5. | Penyusunan Buku Tugas Akhir |  |  |  |  |  |  |  |  |  |  |  |  |  | |  |  |  |

1. **DAFTAR PUSTAKA**

[1] Ahman Ghafarian, Randolph Draughorne, Steven Grainger, Shelly Hargraves, Stacy High, Crystal Jackson. Securing Voice Over Internet Protocol. North Georgia College & State University. United States of America.

[2] Thomas, Tom. Computer Networking First Step. Penerbit Andi, Yogjakarta.

[3] Thomas, Tom. Network Security First Step. Penerbit Andi, Yogjakarta.

[4] VoIP Security [Internet]. 2011 [Diambil 29 Maret 2012]. Tersedia di: http://www.voip-info.org/wiki/view/VOIP+Security

[4] QOS (Quality Of Service) [Internet]. 2011 [Diambil 28 Februari 2012]. Tersedia di: http://www.voip-info.org/wiki/view/QoS

[6] MOS (Mean Opinion Score) [Internet]. 2012 [Diambil 29 Februari 2012]. Tersedia di: http://voip.about.com/od/voipbasics/a/MOS.htm

[7] ITU-T Recommendation (International Communication Union) [Internet]. 2009 [Diambil 29 Februari 2012]. Tersedia di: http://www.itu.int/itu-t/recommendations/index.aspx?ser=P

**LEMBAR PENGESAHAN**

Surabaya, 2 April 2012

Mengetahui/Menyetujui,

|  |
| --- |
| Dosen Pembimbing I |
| **Ir. Muchammad Husni, M.Kom.**  **NIP. 196002211984031001** |

|  |
| --- |
| Dosen Pembimbing II |
| **Erina Letivina Anggraini, S.Kom.** |