IMPLEMENTASI VOIP SIP MENGGUNAKAN DATAGRAM TRANSPORT LAYER SECURITY (DTLS) PADA ASTERISK SERVER

IMPLEMENTATION OF VOIP SIP USING DATAGRAM TRANSPORT LAYER SECURITY (DTLS) ON ASTERISK SERVER

[1] Emeraldo Faris Aufar[2] Dr. Ir. Rendy Munadi, M.T.[3] Leanna Vidya Yovita, S.T., M.T.
[1,2,3]Prodi S1 Teknik Telekomunikasi,Fakultas Teknik Elektro,Universitas Telkom
[1]emeraldofaris@gmail.com, [2]rendy_munadi@yahoo.co.id, [3]leanna.vidya@gmail.com

Abstrak

***Internet protocol* (IP) yang sangat mudah untuk dikembangkan menyebabkan peningkatan yang signifikan pada penggunanya. Sehingga tren perkembangan komunikasi masa depan akan mengarah kepada komunikasi melalui jaringan IP. Komunikasi suara pada jaringan data (internet) biasa disebut dengan istilah VoIP (*Voice over* IP).**

VoIP merupakan salah satu bentuk komunikasi pada jaringan IP yang mulai banyak digemari. Selain karena pertumbuhan pengguna jaringan IP yang masif, VoIP juga mudah dari segi penggunaan, dan lebih murah dari segi biaya dibandingkan dengan komunikasi pada jaringan legacy seperti PSTN. Namun dari segala kelebihannya, komunikasi VoIP juga memiliki kekurangan-kekurangan, salah satunya adalah masalah keamanan jaringan dan privasi pada saat berkomunikasi.

Dalam tugas akhir yang berjudul "Implementasi VoIP SIP menggunakan *Datagram Transport Layer Security* (DTLS) pada Asterisk Server" telah diimplementasikan suatu pembangunan jaringan sistem komunikasi VoIP yang terproteksi dari usaha-usaha mengganggu atau perusakan komunikasi VoIP pada saat pengiriman data yang berupa suara. Penggunaan VoIP yang berbasis datagram ini membuatnya membutuhkan proteksi yang tepat dan memang dirancang untuk memproteksi aplikasi berbasis datagram. Dan dengan proteksi DTLS terbukti dapat melindungi sistem dari *tool* penguji *(penetration tester)* dan mempersempit peluang keberhasilan dalam usaha perusakan sistem ini. Dari hasil pengujian yang dilakukan dapat disimpulkan bahwa penambahan protokol keamanan DTLS-SRTP pada server Asterisk akan menambahkan aspek privacy, confidentiality dan integrity pada server dan kanal medianya, sedangkan dari hasil pengukuran kualitas komunikasi VoIP didapatkan delay sebesar 14 ms, jitter 0,2 ms, packet loss 0% dan throughput 0,094 MBps dengan menggunakan codec PCMU G.711 dan protokol keamanan tambahan DTLS-SRTP.

Kata kunci : VoIP, SIP, DTLS, DTLS-SRTP, Asterisk

Abstract

Internet Protocol (IP) which is very easy to develop makes it way to popularity. So it makes the development trend of next generation communication heads to IP-based communication. Voice communication over IP usually called VoIP (Voice over IP).

VoIP is a form of IP-based communication which starts to get very popular. Beside the massive growth of Internet users, VoIP is easy to use, and much cheaper than the older system such as PSTN. But from all those advantages, VoIP communication also has its weaknesses, security and *privacy* aspect is one of them.

In this final project entitled "Implementation of VoIP SIPI Using Datagram Transport Layer Security (DTLS) on Asterisk Server" has been implemented a VoIP communication network that is secured from common attacks and disturbance on a VoIP call service. The usage of VoIP is based on datagram, so it needs the right form of protection that secure datagram-based services. With the DTLS being implemented, the goal is to secure the system from penetration tester tools and narrow down the attack possibilities from being successful. From the test results, it can be concluded that the addition of DTLS-SRTP will add privacy, confidentiality, and integrity aspects to the server and the media channel, while the quality of the measurement results obtained VoIP communication average delay of 14 ms, average jitter of 0,2 ms, packet loss at 0% and througput of 0,094 MBps by using PCMU G.711 audio codec and with the additional security protocol, DTLS-SRTP.

Keywords: VoIP, SIP, DTLS, DTLS-SRTP, Asterisk

1. Pendahuluan

Teknologi VoIP (*Voice over Internet Protocol*) saat ini tengah gencar digunakan dan dikembangkan oleh konsumen, perusahaan, pemerintaham maupun pihak militer. Teknologi ini menawarkan fleksibilitas yang tinggi dan lebih banyak fitur dibandingkan dengan infrasturktur telefon tradisional seperti PSTN[2]. Dengan segala

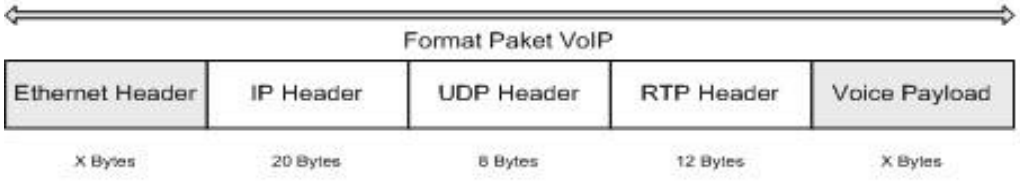
keunggulan ini, haruslah diimbangi dengan fitur keamanan yang baik untuk menghindari terjadinya kebocoran pada saat komunikasi. Salah satu cara untuk mengamankan VoIP SIP adalah dengan menggunakan DTLS (*Datagram Transport Layer Security*). Pada penelitian [5] dibuktikan bahwa penggunakan TLS (*Transport Layer Security*) pada SIP server kurang tepat, terbukti pada penurunan performa yang cukup signifikan.

Pada tulisan ini, penulis akan mencoba mengimplementasikan DTLS sebagai tambahan keamanan bagi server Asterisk dengan layanan voice call. DTLS sendiri merupakan sebuah protokol keamanan yang serupa dengan TLS, yang diperuntukkan bagi *datagram-based applications* [4]. DTLS mengamankan jalur komunikasi sehingga dapat memperkecil kemungkinan dicurinya informasi pada saat komunikasi berlangsung pada layanan VoIP. Setelah mengimplementasikan DTLS pada Asterisk server, orang ketiga tidak dapat melakukan mencuri dengar percakapan yang berlangsung dan kerahasiaan pembicaraan terjamin meski berjalan di jaringan publik. Parameter keberhasilan pada tulisan ini yaitu dengan berjalannya komunikasi dengan aman tanpa menurunkan kualitas suara sampai dibawah standar. Kualitas layanan VoIP diuji dengan parameter QoS (*Quality of Service*), MOS (*Mean Opinion Score*), serta diuji dengan teknik serangan sniffing.

2. Landasan Teori

2.1 *Voice over* IP (VoIP)

Voice over Internet Protocol adalah teknologi yang mampu melewatkan sinyal suara (analog) menjadi bit digital dalam paket-paket data yang dikirim melalui jaringan IP yang bersifat real-time[8]. Tiap paket *VoIP* terdiri atas dua bagian, yakni *header* dan *payload* (beban). Header terdiri atas IP header, RTP *(Real-time Transport Protokol) header*, UDP *(User Datagram Protocol) header*, dan *Ethernet header*[8].



Gambar 1 Format Paket VoIP [8]

IP header bertugas menyimpan informasi routing untuk mengirimkan paket-paket ke tujuan. Pada setiap IP header disediakan tipe layanan atau TOS (Type of Service) yang memungkinkan paket tertentu seperti suara diperlakukan berbeda dengan paket yang non real time[8].

UDP header memiliki ciri tertentu, yaitu tidak menjamin paket akan mencapai tujuan sehingga UDP cocok untuk digunakan pada aplikasi *voice real time* yang sangat peka terhadap *delay* dan *latency*[1].

RTP *header* adalah header yang digunakan untuk melakukan fragmen, segmentasi data real time dan sebagai sebuah protokol multicast[9]. Seperti UDP, RTP juga tidak mendukung reliabilitas paket untuk sampai tujuan. RTP menggunakan protokol kendali yang disebut RTCP (Real Time Control Protocol) yang mengendalikan QoS dan sinkronisasi media stream yang berbeda[9].

2.2 DTLS

DTLS menggunakan hampir semua elemen protokol TLS dengan perubahan *minor* tapi penting, agar dapat bekerja secara tepat pada datagram trasnport. TLS bergantung pada fitur reliable pada TCP untuk deteksi replay dan deteksi urutan paket. Sayangnya fitur-fitur ini tidak ada pada datagram transport. Perubahan-perubahan pada DTLS ada pada *Sequence Number*nya[3].

TLS menggunakan RSN (*Record Sequence Numbers*) secara implisit untuk *replay protection*. RSN memainkan peran yang sama pada DTLS, namun harus ditentukan secara explisit dikarenakan *records* dapat hilang atau sampai tidak berurutan akibat sifat dari *datagram transport*. Sequence number DTLS adalah 48 bits (TLS 64 bits). RSN yang terlalu tua akan dibuang[3].

Perbedaannya dengan TLS adalah *"ClientHello"* pada DTLS mengandung *cookie* yang memungkinkan datagram melakukan *handshake* dengan tepat. Karena pada dasarnya DTLS mengadopsi TLS, tidak banyak perbedaan prinsip kerja antara TLS dan DTLS[3].

2.3 Quality of Service

QoS adalah hasil kolektif dari berbagai kriteria performansi (parameter) yang menentukan tingkat kepuasan penggunaan suatu layanan. Umumnya QoS dikaji dalam kerangka pengoptimalan kapasitas network untuk berbagai jenis layanan, tanpa terus menerus menambah dimensi network [4].

2.3.1 Packet Loss

Packet loss didefinisikan sebagai kegagalan transmisi paket IP mencapai tujuannya. Paket loss dapat terjadi ketika sebuah paket dibuang oleh jaringan karena tidak dapat diteruskan pada output interface. Ada beberapa alasan kenapa terajadi paket loss antara lain :

a. Congestion yang disebabkan terjadinya antrian yang berlebihan dalam jaringan
b. Node yang bekerja melebihi kapasitas buffer
c. Memory yang terbatas pada node

d. Policing, atau control terhadap jaringan untuk memastikan bahwa jumlah trafik yang mengalir sesuai dengan besarnya bandwidth. Jika besarnya trafik yang mengalir di dalam jaringan melebihi dari kapasitas bandwidth yang ada maka policiing control akan membuang kelebihan trafik yang ada.

Di dalam implementasi jaringan IP, nilai packetloss ini diharapkan mempunyai nilai yang minimum. Secara matematis diekspresikan dengan persamaan sebagai berikut :

$$\text{Packet loss} = \frac{\text{Jumlah paket yang hilang}}{\text{Jumlah Paket yang Dikirim}} \times 100\% \quad \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (1)$$

2.3.2 Delay

Delay adalah waktu rata-rata yang dibutuhkan suatu paket untuk menempuh route dari asal ke tujuan. Dalam penelitian tugas akhir ini delay yang dimaksudkan adalah delay rata- rata yang merupakan one way delay, yaitu jumlah total waktu pengiriman paket dalam satu kali pengalamatan dalam hal ini satu kali simulasi dibagi dengan jumlah usaha pengiriman yang berhasil dalam satu kali pengamatan tersebut.

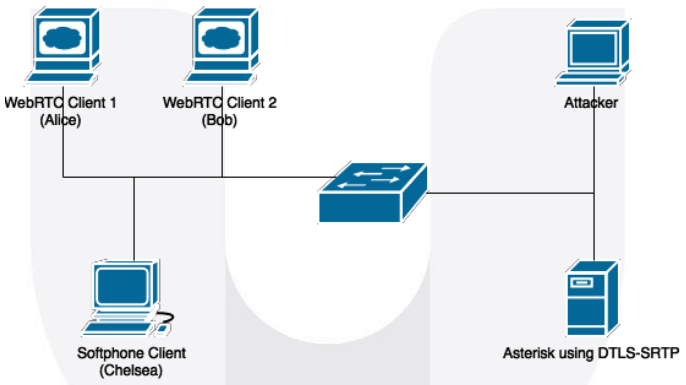
2.3.3 Throughput

Throughput dapat diartikan sebagai jumlah data per satuan waktu yang dikirim di dalam sebuah jaringan, dari suatu titik jaringan ke titik jaringan yang lain.

2.3.4 Jitter

Jitter merupakan merupakan variasi dari delay atau selisih antara delay pertama dengan delay selanjutnya. Jitter merupakan masalah khas dari connectionless network atau packet switched network serta slow speed links. Besarnya nilai jitter akan sangat dipengaruhi oleh variasi beban trafik dan besarnya tumbukan antar paket (congestion) yang ada dalam jaringan IP. Semakin besar beban trafik di dalam jaringan akan menyebabkan semakin besar pula peluang terjadinya congestion dengan demikian nilai jitter-nya akan semakin besar. Semakin besar nilai jitter akan mengakibatkan nilai QoS akan semakin turun. Untuk mendapatkan nilai QoS jaringan yang baik, nilai jitter harus dijaga seminimum mungkin

3. Perancangan dan Implementasi



Gambar 3.2 Topologi Jaringan

Gambar 3.2 merupakan topologi jaringan yang akan dibangun untuk menguji aspek keamanan yang dilindungi DTLS-SRTP pada Asterisk server dan menganalisis pula kualitas layanan dengan tambahan protokol keamanan. Gambar di atas terdiri dari dua jenis perangkat, yaitu :

Perangkat Lunak

a) Asterisk 11.18.0 sebagai server VoIP pada OS Ubuntu 12.04.
b) Sipml5 sebagai webphone WebRTC pada web browser Google Chrome 43 yang digunakan client "Alice" dan "Bob" pada 2 PC yang berbeda pada OS Windows 8.
c) Jitsi sebagai softphone yang digunakan client "Chelsea" pada OS Windows 8.
d) Wireshark, Cain & Abel sebagai tools penguji Asterisk server pada Windows 7.

Perangkat Keras

a) Satu unit PC *server* dengan spesifikasi : Intel® *Core*™ i5 processor, 4 GB RAM Harddisk 640 GB, 1 slot 100Mbps / Fast ethernet.
b) Tiga unit *client* dengan menggunakan PC dengan spesifikasi : Intel® *Core*™ i3 processor, 2 GB RAM Harddisk 200 GB, 2 slot 100Mbps / Fast ethernet.
c) Satu unit attacker dengan menggunakan Notebook dengan spesifikasi : Intel® *Core*™ i5 processor, 4 GB RAM Harddisk 640 GB, 1 slot 100Mbps / Fast ethernet.
d) Kabel UTP dan konektor RJ45.
e) Satu buah switch.

4. Pengujian dan Analisis Implementasi Sistem

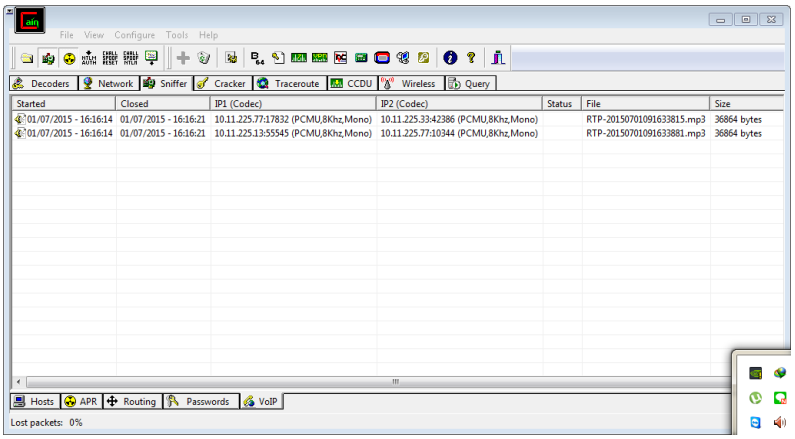
Sesuai dengan [16], DTLS-SRTP dibuat untuk *point-to-point media sessions*, yakni terdiri dari tepat dua pengguna, maka skenario pengujian penelitian kali ini hanya melibatkan dua pengguna pada tiap sesinya.

4.1. Skenario Pertama

Skenario pertama yaitu Pengujian sniffing paket RTP yang terproteksi DTLS-SRTP pada saat terjadinya sesi komunikasi antara client WebRTC (Alice) dengan client WebRTC (Bob) dan pengujian antara client WebRTC (Alice) dengan client softphone (Chelsea)

1. Hasil Pengujian dan Analisis

Untuk menggunakan Cain& Abel sebagai tool penguji, PC Attacker sebelumnya melaukan sniffing kemudian melakukan APR poisoning kepada client Alice (10.11.225.33) dan server Asterisk (10.11.225.77). Cain& Abel memiliki program untuk otomatis merekam dan menyimpan VoIP call yang berlangsung, kemudia menyimpannya dalam format ".mp3".



Gambar 4.1 Sesi komunikasi dapat direkam oleh Cain& Abel

Adanya sesi yang terekam oleh Cain& Abel menunjukkan bahwa percakapan masih dapat terlacak oleh Attacker/ orang ketiga. Cain& Abel terbukti berfungsi dengan baik dalam mendeteksi adanya paket VoIP yang sedang atau sudah berlangsung. Kendati demikian, ketika file yang sudah disimpan Cain& Abel ini diputar ulang, suara yang dapat kita dengar adalah suara yang *noisy* atau berisik tanpa kita dapat mengetahui apa pesan yang sebenarnya terdapat pada percakapan tersebut.

Pengujian juga dilakukan pada skenario komunikasi client WebRTC (Alice) dan client softphone (Chelsea). Kali ini dilakukan analisis terhadap paket yang di-*capture* oleh wireshark network protocol analyzer pada sisi penerima (Chelsea). Paket yang tertangkap berupa paket-paket UDP, namun setelah di-*decode* menjadi RTP, VoIP call terdeteksi dan dapat di playback.

Terbukti wireshark juga dapat menangkap dan mengubah paket RTP menjadi suara. Namun sama halnya dengan Cain& Abel, wireshark tidak menangkap adanya informasi berupa percakapan normal selain suara yang *noisy* dan tidak mengandung informasi apa-apa yang dapat dimengerti hanya dari suara yang terekam.

Bila dianalisis dari kedua kasus tersebut, protokol DTLS-SRTP ini memberikan tambahan aspek keamanan bagi server asterisk, yaitu *confidentiality*. Setelah hubungan terbangun, protokol DTLS-SRTP menjaga kanal media sehingga data yang dikirim-diterima menjadi aman. DTLS-SRTP membuat data menjadi samar dengan menjadikan paket RTP yang tertangkap *attacker* atau orang ketiga penuh dengan noise sehingga menyembunyikan percakapan yang asli. Selain aspek confidentiality, aspek keamanan yang diperkaya dengan tambahan DTLS-SRTP pada Asterisk server adalah aspek integrity, protokol DTLS-SRTP mengenkrpisi percakapan yang sedang berlangsung, sehingga jika data tersebut disadap oleh pihak ketiga yang tidak berwenang, pihak ketiga tersebut tidak akan bisa mengubah isi percakapan yang dikirimkan oleh kedua end point.

4.2 Skenario Kedua

Skenario kedua membahas tentang kualitas layanan VoIP yang menggunakan protokol keamanan tambahan DTLS-SRTP menurut parameter QoS (*Quality of Service*) dan kuisioner MOS (*Mean Opinion Score*).

4.2.1 Analisis Performansi QoS

Pada sub bab ini ditunjukkan hasil pengukuran dan analisis sistem yang telah dilakukan. Adapun parameter yang dianalisis adalah delay, jitter, throughput, dan packet-loss dari layanan VoIP yang diperkaya dengan protokol keamanan tambahan DTLS-SRTP. Menurut standarisasi ITU-T G.1010 dan Cisco, ada beberapa parameter performansi beserta kategori baik/ tidaknya parameter tersebut dengan detail sebagai berikut :

Parameter Performansi		VoIP / RTC
One Way *Delay*	ITU.T G. 1010	preffered < 150 ms ;

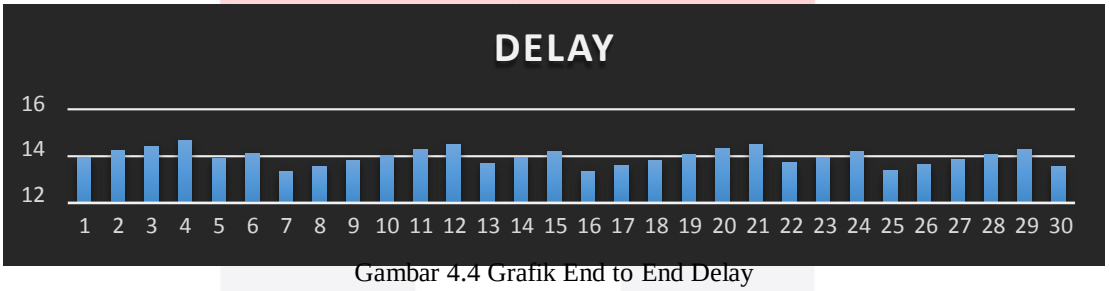
		Acceptable < 400 ms
	Cisco	< 150 ms
Jitter	ITU.T G.1010	< 1 ms
	Cisco	< 30 ms
Packet loss	ITU.T G. 1010	< 3 %
	Cisco	< 5%
Bitrate	ITU.T G. 1010	4 - 64 kbps
	Cisco	

Tabel 4.3 Referensi Standarisasi

1. Delay

Delay merupakan waktu yang diperlukan sebuah paket untuk melakukan perjalanan dari sisi pengirim ke penerima. Pengukuran delay digunakan untuk mengevaluasi performansi dari layanan yang dilewatkan pada jaringan. Dengan melakukan pengukuran kemudian hasilnya dibandingkan dengan nilai yang ditetapkan oleh badan standarisasi tertentu, maka dapat disimpulkan layanan tersebut sudah atau belum memenuhi standar. Delay yang diukur merupakan end-to-end delay.

Pengukuran dilaksanakan dengan melakukan komunikasi VoIP dengan dua skenario berbeda, yaitu client WebRTC ke client WebRTC dan client WebRTC ke client softphone. Setiap panggilan berdurasi 1 menit dan data diambil sebanyak 30 kali. End to end delay diperoleh dari selisih waktu paket dikirim dan waktu paket sampai. Setelah dilakukan pengukuran, hasil delay yang diperoleh diperlihatkan pada grafik dibawah :



Gambar 4.4 Grafik End to End Delay

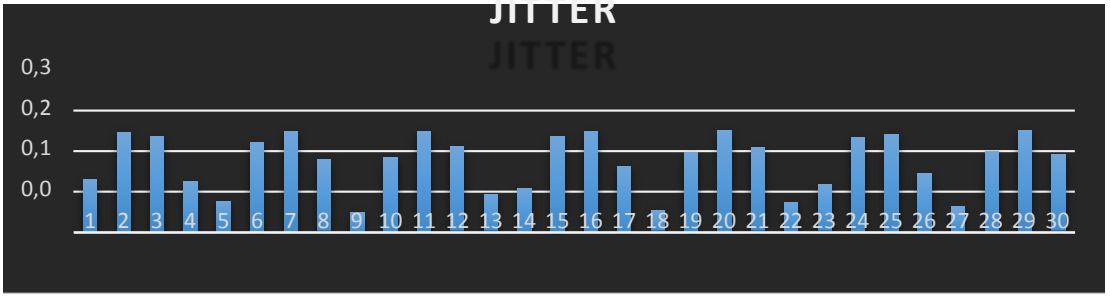
Pada gambar 4.3, terlihat bahwa hasil pengukuran delay pada saat komunikasi WebRTC berlangsung menunjukkan nilai yang tidak beraturan namun menunjukkan tren perubahan yang tidak signifikan. Setelah dilakukan percobaan 30 kali panggilan, di dapat lah nilai rata-rata *end-to-end delay* sebesar 14 ms. Pada aplikasi WebRTC, *end-to-end delay* paling dipengaruhi oleh processing delay. Hal ini dikarenakan WebRTC biasanya berjalan diatas beberapa struktur lapisan. Berjalan di atas browser akan mempengaruhi performansi jika dibandingkan dengan teknologi lainnya yang berdiri langsung diatas *Operating System*.

Dengan melihat hasil nilai end-to-end delay pada pengukuran dan mengacu pada standarisasi yang ditetapkan ITU-T dan Cisco, maka layanan VoIP dengan menggunakan DTLS-SRTP dapat dikategorikan *preferred* atau disarankan.

2. Jitter

Jitter didefinisikan sebagai variasi delay yang diakibatkan oleh panjang antrian dalam suatu pengolahan data dan reassemble paket-paket data di akhir pengiriman akibat kegagalan sebelumnya. Jitter merupakan masalah yang khas pada connectionless atau packet switched network. Cisco menetapkan bahwa jitter untuk komunikasi realtime seperti WebRTC tidak boleh melebihi 30 ms, sedangkan berdasarkan standar ITU-T G.1010 nilai jitter < 1 ms.

Pengukuran dilaksanakan dengan melakukan komunikasi VoIP dengan dua skenario berbeda, yaitu client WebRTC ke client WebRTC dan client WebRTC ke client softphone. Setiap panggilan berdurasi 1 menit dan data diambil sebanyak 30 kali. Jitter dapat diukur berdasarkan nilai delay yang sebelumnya telah diketahui. Nilai jitter didapat dengan menghitung varian delay, nilai akhir jitter didapat dari rata-rata jitter pada setiap sesi panggilan. Data diambil sebanyak 30 kali. Setelah dilakukan pengukuran, hasil jitter yang diperoleh diperlihatkan pada grafik dibawah:



Bagan 4.5 Hasil Pengukuran Jitter

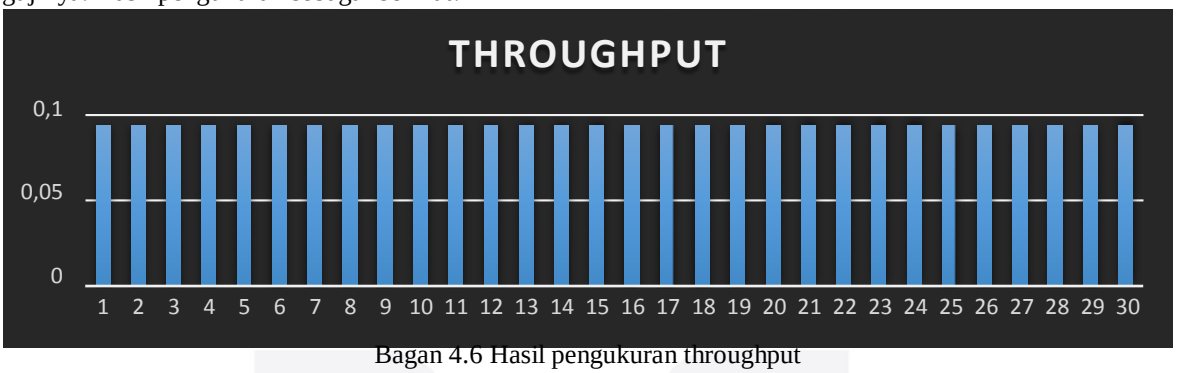
Bagan 4.5 merupakan hasil pengukuran jitter untuk layanan VoIP menggunakan protokol keamanan tambahan DTLS-SRTP. Terlihat bahwa pada 30 kali pengujian, bahwa nilai jitter tidak memiliki nilai yang konstan melainkan unik setiap percobaannya. Jitter rata-ratanya bernilai 0,2 ms.

Variasi delay terjadi karena pengaruh beban trafik dan besarnya congestion (tumbukan) yang ada di dalam jaringan. Saat beban trafik dalam jaringan besar, maka congestion juga banyak terjadi sehinga delay akan lebih bervariasi.

Berdasarkan hasil pengukuran, jitter layanan VoIP pada tiap skenario masih memnuhi standar jitter yang dibuat Cisco yaitu dibawah 30 ms namun tidak dinyatakan lolos standar ITU-T yaitu dibawah 1 ms sementara nilai variasi delay yang didapat adalah 1,22 ms.

3. Throughput (Mbps)

Throughput adalah perbandingan antara paket yang diterima dengan waktu pengamatan. Pengukuran dilaksanakan dengan menggunakan komunikasi VoIP dengan DTLS-SRTP menggunakan wireshark sebagai alat pengujinya. Hasil pengukuran sebagai berikut:



Bagan 4.6 Hasil pengukuran throughput

Secara perhitungan, nilai *bandwidth* yang dibutuhkan layananVoIP berdasarkan codec yang dipakai yaitu G.711 dengan payload 160 bytes dan bitrate 50 kbps dapat dilakukan perhitungan sebagai berikut [5].

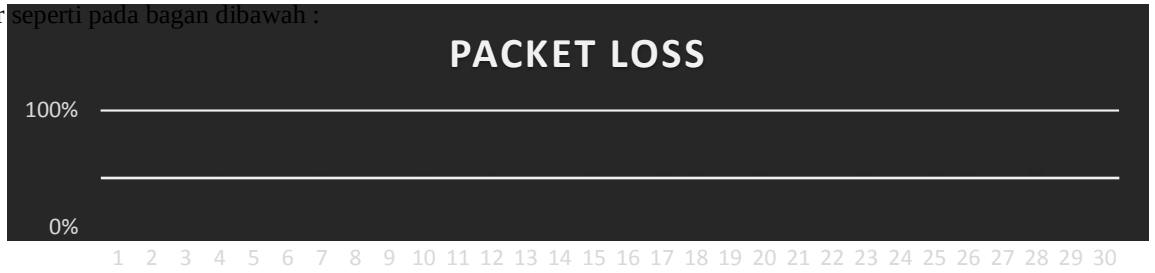
- Bitrate = 50 kbps
- bitrate = payload x 8 x pps (dimana payload G.711 160 bytes)
- pps = 50k / (160 x 8) x pps = (64000 / 1280) x 50
- IP Layer *packet* size = payload codec + RTP header + UDP header + IP header (IPv4)
- Penambahan enkripsi pada paket = 200 + 10 = 210
- Frame Size (on Ethernet links) = 210 + 14 = 224 bytes (disebut juga total *packet* size)
- *Bandwith* = 224 bytes x 50 = 11200 bytes/sec = 0,089 Mbytes/sec (*bandwidth* minimal yang harus tersedia atau minimal yang terbaca di wireshark)

Berdasarkan hasil pengukuran, dapat dilihat bahwa throughput yang terukur pada wireshark menunjukkan nilai yang sesuai dengan perhitungan bandwidth minimal untuk tiap layanan. Dari hasil pengukuran, di dapat nilai rata-rata sebesar 0,094 Mbitps. Adanya variasi nilai throughput dikarenakan throughput merupakan jumlah paket yang sukses diterima dalam satuan detik, maka ketika jaringan dilewatkan paket yang semakin banyak maka jumlah paket yang sampai dalam satuan waktu juga akan berkurang, itulah yang menyebabkan penurunan nilai throughput. Nilai throughput juga berbanding terbalik dengan delay; semakin besar delay maka nilai throughput akan semakin kecil karena throughput dinilai per satuan waktu (dalam sekon).

4. Packet Loss

Packet loss adalah banyaknya paket yang terbuang pada saat proses pengiriman berlangsung dibandingkan dengan banyaknya paket yang selamat. Satuan yang dipakai adalah persen.

Pengukuran packet loss dilakukan dengan melakukan pengukuran pada end user dan tiap pengujian menggunakan wireshark network protocol analyzer. Setelah dilakukan pengukuran, maka diperoleh hasil nilai jitter seperti pada bagan dibawah :



Bagan 4.7 Packet Loss

Melihat hasil pengukuran packet loss yang digunakan pada layanan VoIP menggunakan DTLS-SRTP sebagai protokol keamanan DTLS-SRTP selama 30 kali pengambilan data pengujian, ditunjukkan pada bagan dengan total 0% pada setiap panggilan/ uji coba. Nilai packet loss yang ditunjukkan dengan nilai 0% menunjukkan keandalan jaringan yang baik.

Packet loss sangat dipengaruhi oleh keadaan link serta banyaknya paket yang harus dilewatkan pada jaringan yang menyebabkan kongesti pada jaringan. Karena jaringan yang diimplementasikan pada penelitian ini tidak terhubung secara langsung ke internet, maka ketika muncul angka 0% pada semua percobaan adalah sangat logis.

4 KESIMPULAN

Dari hasil perancangan dan implementasi yang telah dilakukan pada Tugas Akhir ini, maka dapat ditarik kesimpulan sebagai berikut :

Keamanan komunikasi suara pada jaringan IP cukup penting untuk menghindari berbagai bentuk serangan yang dapat menghilangkan aspek privacy/confidentiality, integrity, authentication, availability, access control, dan non-repudation.

Proses komunikasi VoIP SIP yang menggunakan DTLS-SRTP melalui WebRTC masih dalam kualitas yang baik menurut ITU-T dengan rata-rata delay 14 ms.

Komunikasi VoIP SIP sangat rentan terhadap adanya suatu penyerangan/pengujian maupun manipulasi data. Pada proses komunikasi setelah terjadinya pembentukan hubungan atau *signaling*, terdapat *tool-tool* penguji VoIP yang mampu mendeteksi suara sehingga dapat mencuri informasi yang rahasia dan lebih lanjut dapat merugikan pengguna layanan VoIP. Serangan di tingkat lebih tinggi bahkan dapat mengubah isi pesan ketika sedang berlangsungnya sesi komunikasi.

DTLS-SRTP pada komunikasi VoIP berfungsi sebagai media enkripsi untuk komunikasi data VoIP sehingga jaminan pada aspek *privacy* dan *integrity* dapat diusahakan. Hal ini terbukti dapat mencegah adanya suatu pencurian data maupun pengubahan isi informasi pada komunikasi VoIP.

Komunikasi VoIP SIP dengan DTLS/SRTP memberikan perlindungan yang tidak menyeluruh, hanya pada saat sudah terjadi komunikasi di kanal media saja. Komunikasi dengan DTLS-SRTP berlangsung pada keadaan data yang terenkripsi. Penggunaan protokol keamanan tambahan pada Asterisk Server sangat perlu dilakukan untuk mencegah kerusakan-kerusakan yang belum terjadi.

DAFTAR PUSTAKA

[1] J. Postel. User Datagram Protocol. RFC 768, August 1980.

[2] Angelos D. Keromytis, Symantec Research Labs Eurpe, and Sophia-Antipolis, France. Voice over IP: Risks, Threats and Vulnerabilities, 2008.

[3] Nagendra Modadugu and Eric Rescorla. The Design and Implementation of Datagram TLS.

[4] E. Rescorla and N. Modadugu. Datagram Transport Layer Security Version 1.2. RFC 6347, January 2012.

[5] Charles Shen, Erich Nahum, Henning Schulzrinne, Fellow, IEEE, and Charles P. Wright. The Impact of TLS on SIP Server Performance: Measurement and Modeling, August 2012.

[6] Milda M. N. Gamha. Implementasi VoIP SIP Menggunakan Secure Real-Time Transfer Protocol, 2009.

[7] J. Rosenberg, H. Schulzrinee, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler. SIP: Session Initiation Protocol. RFC 3261, June 2002.

[8] ITU-T. P.832 TELECOMMUNICATION STANDARDIZATION SECTOR OF ITU SERIES P: TELEPHONE TRANSMISSION QUALITY, TELEPHONE INSTALLATIONS, LOCAL LINE NETWORKS Methods for objective and subjective assessment of quality Subjective performance evaluation of hands-free terminals. May 2000

[9] H. Schulzrinne, S. Casner, R. Frederick, V. Jacobson. RTP: A Transport Protocol for Real-Time Application. July 2003.

[10] https://wiki.asterisk.org/wiki/display/AST/Home

[11] ITU-T. E.800 SERIES E: OVERALL NETWORK OPERATION, TELEPHONE SERVICE, SERVICE OPERATION AND HUMAN FACTORS Quality of telecommunication services: concepts, models, objectives and dependability planning – Terms and definitions related to the quality of telecommunication services Definitions of terms related to quality of service. September 2008.

[12] ITU-T. SERIES G: TRANSMISSION SYSTEMS AND MEDIA,DIGITAL SYSTEMS AND NETWORKS Quality of service and performance. November 2001.

[13] ITU-T. P.800.1 SERIES P: TELEPHONE TRANSMISSION QUALITY, TELEPHONE INSTALLATIONS, LOCAL LINE NETWORKS Methods for objective and subjective assessment of Quality Mean Opinion Score (MOS) terminology. July 2006.

[14] Zeltsan, Zachary. ITU-T Recommendation X.805 and its application to NGN. April 2005.

[15] R. Munadi, Teknik Switching, Bandung: Informatika, 2011.

[16] D. McGrew, E.Rescorla. Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP). RFC5764. May 2010.