ANALISIS DAN IMPLEMENTASI SECURE REAL-TIME TRANSPORT PROTOCOL TERHADAP LAYANAN IP MULTIMEDIA SUBSYSTEM (IMS)

Adhika Bergi Nugroho[1], Vera Suryani[2], Niken Dwi Wahyu Cahyani[3]

[1]Teknik Informatika, Fakultas Teknik Informatika, Universitas Telkom

Abstrak

Teknologi yang terus berkembang telah menyediakan beragam layanan yang memberikan kemudahan khususnya pada internet. Dengan beragamnya layanan yang tersedia, khalayak ramai menginginkan akan terus ada inovasi teknologi baru yang memberikan kemudahan dengan cara mengintegrasikan beragam teknologi tersebut pada sebuah wadah yang berupa aplikasi. Dengan keinginan tersebut IMS muncul sebagai sebuah arsitektur yang menyediakan tempat untuk menyatukan beragam layanan yang ada.

Kebutuhan keamanan pun muncul ketika ada layanan yang berjalan pada arsitektur IMS yang harus diberikan perlindungan terhadap kerahasiaannya. Pada pengerjaan tugas akhir ini diterapkan salah satu protocol kemanan SRTP pada layanan VoIP di IMS. Kemudian dilihat pengaruhnya terhadap keamanan data dan penambahan waktu akibat penambahan ukuran paket data setelah diterapkan protocol keamanan. Software yang digunakan adalah OpenIMSCore, Asterisk, Boghe IMS client, Blink asterisk client, Wireshark, Cain and Abel.

Dari hasil pengujian yang dilakukan diperoleh hasil SRTP melakukan kemanan berupa rekaman suara hasil VoIP yang tersamarkan saat di sniffing dan data register, invite, pembentukan sesi antar kedua client yang terenkripsi. Waktu yang dibutuhkan pun sedikit lebih lama tetapi tidak mengganggu kenyamanan user.

Kata Kunci : SRTP, IMS, VoIP, Sniffing.

Abstract

The evolving of technology has provided a variety of services that provide convenience especially on the Internet. With a variety of services that have been available, people will continue to want a new technological innovation that provides easy ways to integrate diverse technologies in a container in the form of application. So that IMS became an architecture that provides a place to bring together a variety of existing services.

Security needs also arise when there is a service running on IMS architecture should be given the protection of confidentiality. In this final project implemented a security protocol SRTP to VoIP services in the IMS. Then see its effect on data security and extra time due to the addition of a data packet size after implemented security protocols. Software that used is OpenIMSCore, Asterisk, Boghe IMS client, Blink asterisk client, Wireshark, Cain and Abel.

The test results obtained the results of SRTP doing security in the form of sound recordings that are masked as VoIP results in sniffing and data register, invite, session establishment between the two clients is encrypted. The time required is a bit longer but it did not interfere with the user convenience.

Keywords : SRTP, IMS, VoIP, Sniffing.

1. Pendahuluan

1.1 Latar Belakang

Saat ini layanan multimedia masih merupakan salah satu media utama yang menyajikan informasi dan hiburan. Penggunaan layanan multimedia saat ini sudah mulai berkembang dan telah tersedia berbagai media seperti chating, video streaming, iptv, dan lainnya. Kesemua layanan tersebut memberikan yang lebih interaktif untuk berhubungan dengan dunia luar.

Teknologi IP Multimedia Subsystem(IMS) menyediakan fungsi – fungsi control yang membantu layanan multimedia. Mengapa diperlukan IMS, karena IMS mendefinisakn arsitektur penerapan layanan multimedia berbasis 3G yang memungkinkan tersedia nya akses layanan dimanapun ketika sudah terhubung ke internet. Protocol yang digunakan pada IMS ini adalah *session initiation protocol* dan *real-time transport protocol*. Dengan menggunakan protocol RTP dan SIP karena kebanyakan layanan multimedia berjalan pada *protocol* UDP walaupun ada juga yang berjalan di *protocol* TCP.

Pada layanan multimedia terdapat beberapa jenis layanan yang berbeda yang tentunya dibutuhkan perlindungan keamanan dari attacker seperti *hijacking*, *sniffing* dan bentuk serangan lainnya. Perlindungan terhadap layanan multimedia yang dalam hal ini diterapkan pada server IMS dibutuhkan untuk kelancaran pengiriman paket data kepada tujuan yang tepat tanpa ada hambatan ataupun pencurian. Disamping itu juga pada saat digunakan untuk keperluan komersil akan menghindari gangguan yang mengakibatkan kerugian. Untuk dapat menjamin keamanan tersebut digunakan Secure Real-time Transport Protocol (SRTP).

SRTP merupakan pengembangan dari RTP untuk mengamankan proses Real-Time. Mengapa protocol SRTP, karena saat ini SRTP merupakan satu – satunya protocol yang dapat melindungi payload dari paket RTP. Dengan menggunakan SRTP walaupun terjadi penambahan ukuran , ukuran pada paket tidak terlalu berbeda dengan ukuran paket sebelum di enkripsi, sehingga waktu yang dibutuhkan untuk pengiriman data menjadi hanya sedikit lebih lama.

1.2 Perumusan Masalah

a. Bagaimana Membangun layanan multimedia berbasis IMS menggunakan protocol RTP dan SIP menggunakan media enkripsi *Secure Real-time Transport Protocol* (SRTP)?
b. Bagaimana skenario pengujian untuk mengetahui apa peran protocol SRTP dalam melindungi layanan IMS dengan menggunakan tolak ukur pada parameter *Confidentiality* dan *Integrity* ?
c. Dengan diterapkannya protocol SRTP pada layanan IMS, Apakah protocol tersebut mempengaruhi waktu yang dibutuhkan untuk pengiriman packet data terkait dengan tingkat kenyamanan pengguna ?

1.3 Batasan Masalah

Dalam pengerjaan tugas akhir ini, permasalahan dibatasi dalam beberapa hal yaitu

a. Implementasi dilakukan pada testbed IMS
b. Sistem operasi yang digunakan adalah Ubuntu *desktop* 10.04 dan Windows XP
c. Implementasi IMS menggunakan software OpenIMSCore yang diterapkan pada satu komputer server.
d. Protocol keamanan yang digunakan adalah SRTP private key RSA, dan algoritma enkripsi AES.
e. Tidak membahasa skenario *error request* pada SRTP.
f. Hanya membahas jenis serangan pada SIP.
g. Proses perlindungan diberikan pada aspek *confidentiality* yang bekerja pada layer transport.
h. Menggunakan dua client, dengan layanan VoIP yang melibatkan dua pengguna
i. Layanan IMS yang digunakan terbatas pada layanan VoIP saja.
j. Tidak membahas aspek QoS *Networking*, seperti *troughput, jitter* dan *packet loss*.

1.4 Tujuan

a. Membangun layanan berbasis IMS dengan menggunakan protocol SIP dan RTP dengan media enkripsi SRTP.
b. Menganalisa seberapa baik kinerja protocol SRTP berdasarkan konsep dalam menjaga layanan IMS terhadap aspek *confidentiality* dan *integrity* data.
c. Mengetahui lama waktu yang dibutuhkan dalam pengiriman *packet* data pada layanan multimedia yang sudah menerapkan SRTP berkaitan dengan tingkat kenyamanan pengguna.

1.5 Hipotesis.

Implementasi SRTP sebagai media enkripsi akan menjamin aspek confidentiality dan integrity, tetapi membutuhkan waktu pengiriman *packet* data sedikit lebih lama.

1.6 Metode Penyelesaian Masalah

a. Identifikasi Masalah
   SIP dan RTP merupakan *protocol* yang digunakan untuk mengintegrasikan setiap layanan di layanan IMS baik data ataupun multimedia. Dengan mekanisme control yang diberikan SIP dan RTP, layanan IMS dapat mengendalikan setiap *Channel Change Times, communication* session dan kebijakan pengaturan yang berbeda. Dengan memperhatikan codec video dan bitrate video maka analisis terhadap nilai performansi layanan IMS dapat diketahui. Dari sisi keamanan layanan IMS digunakan SRTP sebagai media enkripsi packet data. SRTP melindungi payload data pada paket RTP yang berjalan pada IMS dengan berbagai metode pertukaran kunci. SRTP merupakan sebuah cara untuk melindungi kerahasiaan dan integritas data pada paket RTP.
b. Studi Literatur.

Mencari sumber dari manapun dan apapun baik berupa data, software, ataupun hardware mengenai konsep layanan IMS,TLS, RTP, SIP, VoIP dan SRTP.

c. Perancangan
   Merancang sistem sesuai kebutuhan spesifikasi sistem.
d. Implementasi protocol SRTP, RTP dan SIP padalayanan IMS sesuai perancangan dan kebutuhan. Penerapan SRTP, pada layanan IMS dilakukan pengukuran keamanan dengan acuan pada konsep CIA.
e. Penyusunan Laporan Tugas Akhir.
   Membuat Laporan berdasarkan proses keamanan SRTP yang diketahui dari hasil penelitian dan pengujian yang dilakukan.

1.7 Sistematika Penulisan

Penulisan tugas akhir ini disusun dengan metode penulisan sebagai berikut :

BAB I Pendahuluan

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

BAB II Dasar Teori

Bab ini membahasa mengenai teori yang berhubungan dengan IMS dan SRTP

BAB III Perancangan dan Implementasi

Bab ini berisi perancangan topologi sistem dan analisis kebutuhan dari sistem serta masalah –masalah yang ada di dalamnya. Dimulai dari tahap analisis kebutuhan kemudian dilanjutkan ke tahap implementasi.

BAB IV Pengujian dan Analisis

Bab ini membahas mengenai pengujian hasil implementasi. Dilakukan beberapa skenario uji untuk memperoleh dan mengetahui pengaruh yang diberikan SRTP terhadap keamanan IMS dan waktu yang dibutuhkan untuk melakukan proses keamanan

BAB V Kesimpulan dan Saran

Bab ini berisi kesimpulan penulisan tugas akhir dan saran –saran yang dibutuhkan untuk pengembangan lebih lanjut.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Berdasarkan analisis hasil pengujian dapat disimpulakan sebagai berikut:
SRTP hanya mengenkripsi payload yaitu berupa audio pada layanan VoIP di IMS untuk aspek confidentiality dan algoritma AES melindungi integritas dari seluruh paket RTP. Setiap SRTP stream membutuhkan metode exchange key. SRTP telah berjalan dengan baik dan mencapai layanan interoperability yang baik, saat dilakukan sniffing VoIP pada Cain&Abel didapatkan suara yang berupa noise. Ini membuktikan bahwa SRTP dapat bekerja dengan baik dalam melindungi layanan VoIP pada IMS. Akan tetapi untuk melakukan penyadapan pada server masih dimungkinkan karena masih ada celah untuk membaca metode yang dilakukan SRTP saat wireshark mengcapture interface jaringan yang sama dengan server, wireshark dapat menemukan paket SDP yang membawa informasi tentang metode atau algoritma yang digunakan untuk mengenkripsi RTP, walaupun dapat diketahui sniffer tetap tidak dapat mndengar hasil percakapan VoIP yang dilakukan. Dipandang dari sisi keamanan, jaringan yang diimplementasikan SRTP lebih aman dibandingkan jaringan non-SRTP, akan tetapi dibutuhkan waktu sedikit lebih lama untuk SRTP dalam melakukan proses keamanan. Namun berdasarkan pengujian waktu tersebut secara nyata dirasakan oleh user tidak menggangu aspek kenyamanan karena hanya membutuhkan waktu kurang dari 1 detik untuk dapat melakukan komunikasi.

5.2 Saran

Untuk dimasa yang akan datang diharapkan dapat diimplementasikan

a. Penerapan SRTP pada layanan IMS lainnya seperti IPTV, Video Confrence, ataupun Chatting.
b. Penerapan SRTP dengan menciptakan source code yang dapat di implementasikan di server IMS tanpa mengalami error di CSCF server. Sehingga SRTP dapat diterapkan langsung pada server IMS tanpa harus terhubung dengan server Asterisk.

6. Daftar Pustaka

[1]. Wikipedia. Openimscore 2013. (online). (http://www.openimscore.org/, diakses Januari 2013)

[2]. Wikipedia. IMS overview 2013. (online) (http://en.wikipedia.org/wiki/File:Ims_overview.png, diakses Juni 2012)

[3]. Wikipedia. SIP 2013. (online) (http://en.wikipedia.org/wiki/Session_Initiation_Protocol, diakses Mei 2012)

[4]. Vocal. TLSv1. 2013 (online) (http://www.vocal.com/networking/sslv3tlsv1/, diakses Januari 2013)

[5]. STUDI ALGORITMA ENKRIPSI PADA PROTOCOL SECURE REAL TIME PROTOCOL Albert Raditya S – NIM : 135060776 Program Studi Teknik Informatika, Institut Teknologi BandungJl. Ganesha 10, Bandung

[6]. Munir, R. 2006. *"Kriptografi"*. Penerbit Informatika

[7]. Wikipedia. VoIP 2013 (online). (http://id.wikipedia.org/wiki/Voice_over_IP, diakses Desember 2012)

[8]. Alexandros, Moraitis. 2010. "*IMS Security*". Brunel Unicersity.

[9]. Lisdyanto. 2012. "*Implementasi TLS pada Gm Interface IMS Menggunakan Open IMS Core*". Institut Teknologi Telkom

[10]. Wikipedia. 2013."*Secure Real-Time Transport Protocol*" (online). (http://en.wikipedia.org/wiki/Session_Description_Protocol, diakses Mei 2012)

[11]. Dierks, T. dan C. Allen. 2008. "*The TLS Protocol Version 1.0*" (online). (http://www.ietf.org/rfc/rfc2246.txt, diakses Januari 2013)

[12]. Shmatikov, Vitaly. "*Security Analysis of Voice-over-IP Protocols*". The University of Texas at Austin

[13]. Wikipedia. 2013."*Session Description Protocol*" (online). (http://en.wikipedia.org/wiki/Session_Description_Protocol, diakses Mei 2012)