ANALISIS ASPEK KEAMANAN VOIP PADA NEXT GENERATION NETWORK (ANALYSIS OF VOIP SECURITY ASPECT IN NEXT GENERATION NETWORK)

Ruslan Haris[1]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Kata Kunci :

Abstract

Keywords :

BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Jaringan Telco (PSTN/ISDN dan PLMN) yang berbasis *circuit switched* dengan elemen utamanya sentral telepon, memiliki banyak keterbatasan baik dari segi arsitektur maupun efisiensi pemakaian *resources* (bandwidth). Dari segi arsitekturnya elemen kontrol, elemen media dan aplikasinya bersifat *propietary* (vendor dependent) sehingga disamping relatif mahal, juga sulit dikembangkan. Dari segi pemakaian kanal bandwidth, karena koneksinya bersifat dedicated yang bersifat TDM (Time Division Multiplexing), utilitas kanal rendah yang berarti kurang efisien. Di sisi lain jaringan IP, protokolnya yang bersifat open system dan mode paket switch yang lebih efisien, membuatnya jaringan IP mampu berkembang lebih pesat, semakin mendominasi, bahkan mulai mengambil alih peran PSTN/ISDN bahkan PLMN atau selular

Sekarang ini komunikasi multimedia sudah menjadi hal yang tidak dapat dipisahkan lagi dalam aplikasi internet. Aplikasi ini meliputi Voice over Internet Protocol (VoIP), konferensi multimedia, Instant Messaging, dan sebagainya. Oleh karena itu sangat dibutuhkan adanya suatu manajemen dalam pertukaran data yang melibatkan sekumpulan pengguna ini. Fungsi manajemen ini dapat dilakukan oleh Session Initiation Protocol (SIP). Masalah keamanan merupakan salah satu aspek yang sangat penting pada sebuah sistem informasi. Demikian juga dengan masalah keamanan pada SIP. Meskipun demikian SIP bukanlah protokol yang mudah dijamin keamanannya. Operasinya yang melibatkan banyak pengguna, elemen intermediate, dan protokol lainnya menyebabkan faktor keamanan jauh dari sederhana

Perkembangan teknologi komputer seperti konvergensi antara data analog menjadi digital dan teknologi telekomunikasi yang cepat membawa dampak pada tumbuhnya aplikasi baru khususnya pada aplikasi yang berbasis IP dan berhubungan dengan

komunikasi dan efek dari kemajuan internet yang semakin pesat juga ikut mendorong kemajuan di berbagai bidang, beberapa faktor mengapa teknologi *IP telepony* ini sangat perlu dikembangkan

- Biaya perawatan yang dapat ditekan karena menggunakan jaringan *public* (internet).
- Biaya instalasi mudah baik di tingkat end user maupun di server.
- Variasi fitur yang beragam dan mengikuti perkembangan.
- Bisa bersifat mobility dan fixed karena bisa *loggin* dimana pun dan di perangkat apapun.
- Mudah dikembangkan ataupun di *upgrade* karena berbasis open source.
- Mudah di interkoneksi pada aplikasi yang lain seperti email, fax,IP PBX. dll

1.2 MAKSUD DAN TUJUAN

Untuk mengetahui bagian-bagian yang berpotensi atau rentan terhadap gangguan dan ancaman keamanan (signaling, audio payload, dll) pada layanan VoIP, dan mengetahui jenis-jenis gangguan keamanaan yang dapat mengganggu layanan ini pada protokol yang akan diujikan yaitu SIP, sampai sejauh mana tingkat ketahanan gangguan keamanan pada VoIP untuk berbagai jenis gangguan, baik dari segi infrastruktur operator maupun privasi pengguna

1.3 PERUMUSAN MASALAH

VoIP sering dikatakan sebagai sebuah aplikasi yang akan menggantikan aplikasi *telepony* saat ini kedepannya, mengingat komunikasi adalah suatu faktor penting, apakah kita sudah cukup yakin untuk menggunkan aplikasi ini, mengingat medium yang digunakan adalah internet dan tidak ada penjaminan keamanan dan bagaimana cara kita untuk mengurangi *vulnarbility* pada aplikasi tersebut.

1.4 BATASAN MASALAH

Pembahasan sistem pengamanan pada NGN ini berdasarkan studi aspek-aspek pengamanan dan **emulasi** yang dilakukan akan membahas hal-hal sebagai berikut :

1. Sifat mudah terhadap serangan (***Vulnerability***):
2. Jenis ancaman **(*Threat*)**
3. Resiko **(*Risk*)**

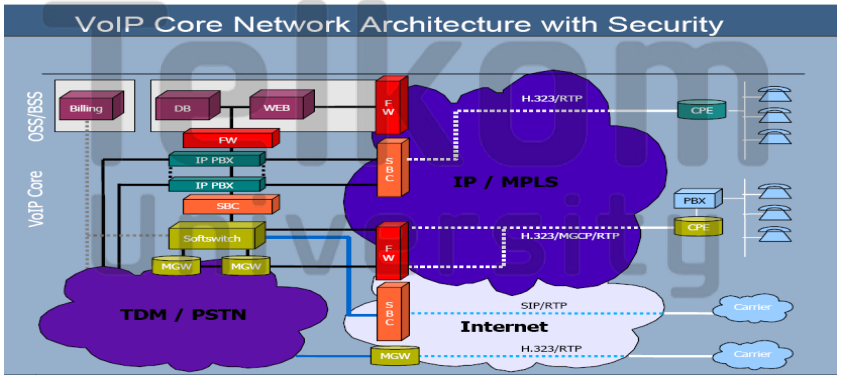
Dimensi pengamanan :

1. ***Access Control***
2. **Authentication**
3. **Communication secuirty**
4. **Avaibility**

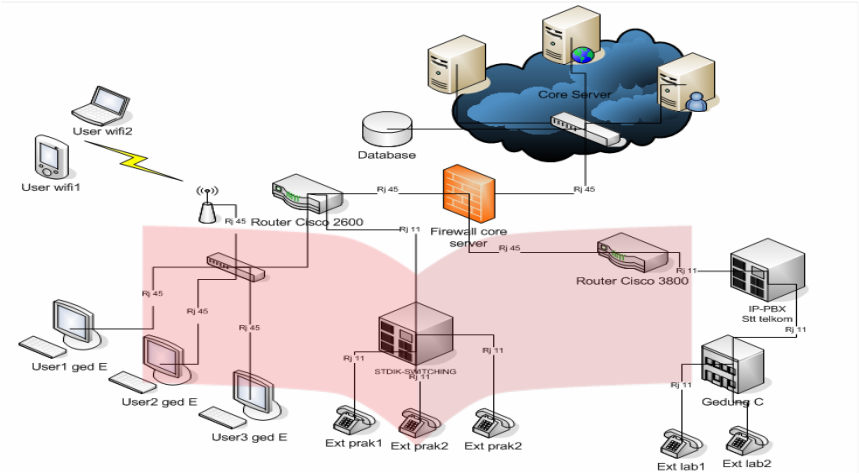
Dan tidak membahas enkripsi dan ENUM secara mendalam agar tujuan Tugas Akhir ini tidak melebar.

1.5 PEMODELAN

Pada gambar di bawah adalah skenario umum dalam arsitektur VoIP pada umumnya protokol-protokol yang digunakan adalah H.323, SIP, IAX2, megaco, dll. sedangkan pada gambar kedua adalah pemodelan yang akan di lakukan untuk menganalisa dan berfokus pada protokol SIP



Gambar 1.1 Model jaringan umum



Gambar 1.2 Model jaringan implentasi

1.6 METODOLOGI

- Studi literature atau studi pustaka dengan mengumpulkan dan memplajari buku-buku,

  tutorial, artikel dan referensi lain yang terkait dengan materi terutama mengenai konfigurasi server VoIP, topologi jaringan, protokol yang di gunakan SIP serta keamanan jaringan.
- Melakukan percobaan dengan mengujikan aspek-aspek security pada jaringan yang dibagun untuk melihat dampak sebelum dan sesudah mengimplentasikan sistim keamanan
- Diskusi dan konsultasi dengan dosen pembimbing, millis-milis dan pihak-pihak lain untuk mendapatkan pengarahan dalam pengerjaan tugas akhir ini.

1.7 SISTEMATIKA PENULISAN

BAB I PENDAHULUAN

Membahas tentang latar belakang, perumusan masalah, batasan masalah, tujuan, metodologi, dan sistematika penulisan.

BAB II DASAR TEORI

Membahas tentang sircuit switch dan packet switch, NGN, teori VoIP, OSI layer, keamanan server, protokol-protokol yang digunakan.

BAB III KONFIGURASI JARINGAN VOIP PADA NGN

Merancang konfigurasi sebagai medium analisa kemanan VoIP dalam mengemulasi jaringan NGN.

BAB IV ANALISA ASPEK KEAMANAN VOIP PADA NGN

Membahas tentang keamanan jaringan VoIP (asterisk) terhadap vulnarbility di NGN.

BAB V KESIMPULAN DAN SARAN

Berisi kesimpulan yang didapat dari pembahasan dan analisa bab sebelumnya, juga saran yang yang di butuhkan untuk pengembangan selanjutnya.

BAB V
Simpulan dan Saran

5.1 Simpulan

Dari semua percobaan dan emulasi yang telah dilakukan maka disini penulis akan menuliskan kesimpulan yang di dapat tentang aspek kemanan VoIP pada NGN yaitu sebagai berikut :

Dengan penggunaan enkripsi pada payload data voice dalam aplikasi VoIP terbukti dapat menurunkan tingkat *vulnarbility* khususnya pada ancaman seperti *eavesdropping* atau *traffic snifing*

Diperlukan sikap waspada kepada administrator untuk mengamati traffik yang mencurigakan Pada jaringan yang terhubung, karena ancaman bisa datang kapan dan dalam jenis apa saja, seperti ***Flooding*** dan ***spoofing*** yang dapat menggagu kinerja sistem dengan memblack list IP address yang mencurigakan tersebut, hal ini bisa terlihat jika dalam suatu jaringan suatu paket berulang lebih dari 11-13 kali karena waktu regristrasi dari sebuah user adalah 3600 detik sebelum time out

Kelebihannya RTP dapat menggunakan berbagai *port* sembarang mulai dari 1024 sampai 65,534. Masalah akan muncul juga jika terjadi pertambahan volume panggilan (call volume). *voice traffic* dapat mempengaruhi kinerja proses *load* di *firewall*, disini *voice traffic* dapat mengetahui *voice packet* dilakukan pesan dari SIP, Jika jumlah *call* bertambah banyak, firewall akan bekerja keras (*delaying packet*)

Perubahan pada konfigurasi default pada aplikasi VoIP dapat menurunkan tingkat resiko serangan burce attack untuk mendapatkan username dan password yang legal pada suatu server atau provider

Jika komunikasi VoIP melibatkan dua jaringan yang berbeda seperti internet dan PSTN maka endpoint vulnarbelity tidak lagi server tapi juga gateway sebagai interface yang menghubungkan jaringan yang berbeda

5.2 Saran

Untuk pengembangan dan pembelajaran lebih lanjut ada beberapa saran yang penulis ingin sampaikan berkenaan faktor keamanan VoIP:

1. Menganalisa aspek-aspek keamanan yang di standarkan ITU-T X.805 yang lain seperti Non- repudation, Data Confidentiality and Data integrity
2. Mencoba untuk menerapkan jenis enkripsi yang berbeda untuk pengamanan payload data voice pada aplikasi VoIP
3. Mencoba untuk mengimplementasikan standar keamanan untuk teknologi VoIP seperti TLS dan SRTP
4. Menggunakan *platform* dan konfigurasi jaringan yang mensupport aspek keamanan pada aplikasi yang diberikan seperti VoIP yang bersifat *realtime*

Daftar Pustaka

[1]. Lawencki Pawel, Master thesis VoIP Security in Public Network, Alcatel-Lucent, February 2007

[2]. Orrblad Joachim, Master of Science thesis Altenatives to Mikey/SRTP to secure VoIP. KTH Microelectronics and Information Technology, Stockholm,March 2005.

[3]. Luthra Amit, Waqas Ashraf. Master thesis Security of VoIP System. Technical University of Denmark, Denmark, August 2005.

[4]. William Patrick.M,Next Generation Networks for Voice Services: History, Design and Policy Implications. Universidade Tecnica de Lisboa, March 2005.

[5]. Indra Martinus S. Mekanisme dan implentasi keamanan pada Session Initiation.ITB, 2004

[6]. Tu Jiashun.Next Generation Network Security,ZTE, Geneva ,2005.

[7]. ITU-T; Focus Group, Next Generation Network Proceedings.2005

[8]. Mark Spencer - Digium Inc.; Home page of Asterisk software - an open source, freeware implementation of IP PBX; *http://www.asterisk.org*, January 2007

[9]. Endler David, Collier Mark . Voice Over IP Security Secrets and Solutions, McGraw-Hill,2007

[10] Collier Mark D. Session Initiation Protocol (SIP) Vulnerabilities,IPComm,2006

[11] Febriato Stevi, Implentasi IP PBX di STT Telkom,Bandung, oktober 2007