



**Analisis Kinerja VoIP Client Siproid Dengan
Pengintegrasian Modul Enkripsi**

TESIS

**Oleh
Abdi Wahab
55410110009**

**PROGRAM MAGISTER TEKNIK ELEKTRO
PROGRAM PASCASARJANA
UNIVERSITAS MERCU BUANA
2012**

Abstrak

Jumlah pengguna VoIP di Indonesia masih kecil sekali, walaupun *cost* yang ditawarkan oleh VoIP lebih kecil dibandingkan dengan menggunakan telepon berpulsa. Salah satu alasannya adalah keamanan yang diberikan oleh penyedia layanan VoIP yang masih kurang. Pengguna VoIP belum mendapat layanan keamanan yang dapat menjamin keamanan komunikasi. Penelitian ini mencoba untuk mengamankan komunikasi antara pengguna VoIP dengan menggunakan modul enkripsi yang diintegrasikan dengan VoIP *client* Sipdroid yang berjalan di *smartphone* Android. Hal ini dimungkinkan oleh pengguna VoIP karena hanya VoIP *client* yang dapat diakses oleh pengguna VoIP.

Hasil yang diperoleh setelah dilakukan integrasi dengan modul enkripsi menggunakan tiga buah skema enkripsi yaitu AES, DES, dan RC4, Sipdroid mampu menahan serangan pasif dari penyadapan informasi (*eavesdropping*) selama terjadi komunikasi. Dan hasil dari pengukuran QoS terdapat peningkatan *delay* sebesar 0.01 ms dan tidak terjadi perubahan yang signifikan terhadap *throughput* dan *packet loss*, untuk *throughput* yang dihasilkan berkisar di 78 kbps, dan untuk *packet loss* rata-rata adalah 0.8 %. Akan tetapi terdapat *noise* yang mengikuti komunikasi pada Sipdroid yang terintegrasi dengan modul enkripsi akibat skew gelombang dari penambahan waktu proses ketika enkripsi.

Kata kunci: VoIP, VoIP *Client*, Enkripsi.

Abstract

The number of VoIP users in Indonesia is still very small, although the cost offered by VoIP is smaller than by using pulsed phone. One reason is the security provided by VoIP service providers still weak. VoIP users do not have a security service that can guarantee the security of communications. This study attempts to secure the communication between VoIP users using encryption module integrated with a VoIP client Sipdroid that runs on Android smartphone. This is one of way to secure the communications that can be access by VoIP users, adding the encryption module to VoIP client.

The results obtained after the integration with the encryption module with three encryption schemes, AES, DES, and RC4, Sipdroid able to prevent passive attacks from eavesdropping of information during the communication. And The result of QoS measurements are an increase in delay of 0.01 ms and no significant changes in the throughput and packet loss, for the throughput range at 78 kbps, and average of packet loss is 0.8%. However, there is noise on the communication that follow Sipdroid integrated with the encryption module, due to the wave skew from the extra time when the encryption process happens.

Key Words: VoIP, VoIP client, Encryption

PERNYATAAN

Saya yang bertandatangan di bawah ini menyatakan dengan sebenar-benarnya bahwa seluruh tulisan dan pernyataan dalam Tesis ini:

Judul : Analisis Kinerja VoIP Client Siproid Dengan
Pengintegrasian Modul Enkripsi

Nama : Abdi Wahab

NIM : 55410110009

Program : Pascasarjana Program Magister Teknik Elektro

Tanggal : Maret 2012

Merupakan hasil studi pustaka, penelitian lapangan, dan karya saya sendiri dengan bimbingan Pembimbing yang ditetapkan dengan Surat Keputusan Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana.

Tesis ini belum pernah diajukan untuk memperoleh gelar magister pada program sejenis di perguruan tinggi lain. Semua informasi, data, dan hasil pengolahannya yang digunakan, telah dinyatakan secara jelas sumbernya dan dapat diperiksa kebenarannya.

Jakarta, Maret 2012

ABDI WAHAB

PENGESAHAN TESIS

Judul : Analisis Kinerja VoIP Client Siproid Dengan
Pengintegrasian Modul Enkripsi

Nama : Abdi Wahab

NIM : 55410110009

Program : Pascasarjana Program Magister Teknik Elektro

Tanggal : Maret 2012

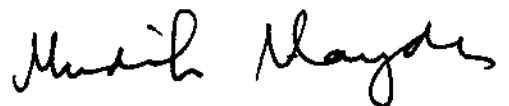
Mengesahkan :

Direktur Pascasarjana



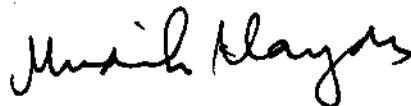
Prof. Dr. Didik J. Rachbini

Ketua Program Studi
Magister Teknik Elektro



Dr.-Ing. Mudrik Alaydrus

Pembimbing Utama



Dr.-Ing. Mudrik Alaydrus

KATA PENGANTAR



Alhamdulillah, segala puji syukur kepada Allah SWT atas segala rahmat dan hidayah-Nya sehingga penulisan tesis dengan judul: **Analisis Kinerja VoIP Client Siproid Dengan Pengintegrasian Modul Enkripsi** dapat diselesaikan dengan baik. Penulisan ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Magister Teknik Program Studi Teknik Elektro, kekhususan Manajemen Telekomunikasi pada Universitas Mercu Buana.

Penyelesaian Tesis ini tak lepas dari bantuan berbagai pihak. Dengan segala kerendahan hati, kami menghaturkan terima kasih yang sebesar-besarnya kepada :

1. Dr.-Ing. Mudrik Alaydrus selaku Ketua Program Studi Magister Teknik Elektro Universitas Mercu Buana.
2. Dr.-Ing. Mudrik Alaydrus sebagai dosen Pembimbing yang telah banyak meluangkan waktu untuk memberikan pengarahan, diskusi dan bimbingan serta persetujuan sehingga kami menyelesaikan tesis ini dengan baik.
3. Segenap dosen dan staf Program Studi Magister Teknik Elektro Universitas Mercu Buana.
4. Kedua orang tua atas segala doa restunya selama ini sehingga kami dapat melalui setiap rintangan dengan selamat dan penuh kesabaran. Semoga Allah SWT juga memberikan keselamatan dunia dan akhirat kepada keduanya, Amin.
5. Istri, adik dan anak-anak atas dorongan dan doanya.
6. Segenap teman-teman Program Studi Magister Teknik Elektro Universitas Mercu Buana.

Begitu pula ucapan terima kasih kepada semua pihak yang tidak sempat kami sebutkan satu per satu atas jasa-jasanya dalam membantu dan menumbuhkan gairah optimisme kami, baik secara langsung maupun tidak langsung.

Dengan menyadari berbagai kekhilafan yang bukan tidak mungkin akan terdapat dalam tulisan ini, penulis sangat mengharapkan adanya kritik dan saran yang bersifat membangun terhadap Tesis ini. Akhir kata dengan segala kerendahan hati penulis berharap semoga Tesis ini dapat bermanfaat bagi penelitian-penelitian selanjutnya.

Jakarta, Maret 2012

Penulis

Daftar Isi

JUDUL LUAR	i
JUDUL DALAM.....	ii
Abstrak.....	iii
Abstract.....	iv
Pernyataan.....	v
Pengesahan Tesis.....	vi
Kata Pengantar	vii
Daftar Isi	viii
Daftar Gambar.....	xii
Daftar Tabel	xiv
Daftar Istilah.....	xv
BAB 1 Pendahuluan	1
1.1 Latar Belakang	1
1.1 Tujuan dan Sasaran	3
1.2 Perumusan Masalah.....	3
1.3 Batasan Masalah.....	4
1.4 Sistematika Penulisan.....	5
BAB 2 Kajian Pustaka	6
2.1 Penelitian Terkait	6
2.2 Sipdroid.....	7
2.3 Konsep Kriptografi.....	7
2.3.1 DES (<i>Data Encryption Standard</i>).....	8
2.3.2 AES (<i>Advanced Encryption Standard</i>).....	8
2.3.3 RC4 (<i>Rivest Cipher 4</i>).....	9

2.4	<i>Java Cryptography Extension (JCE)</i>	9
2.5	Layanan Keamanan (<i>Security Services</i>)	9
2.6	Penyerangan Keamanan (<i>Security Attacks</i>).....	11
2.6.1	Penyerangan Pasif.....	11
2.6.2	Penyerangan Aktif.....	12
2.7	Pengukuran Kinerja.....	12
2.7.1	Kualitas Layanan (<i>Quality of Service (QoS)</i>).....	12
2.7.2	Mean Opinion Score (MOS).....	14
2.8	Pengujian Alpha (<i>Alpha Testing</i>).....	14
BAB 3	Metodologi Penelitian.....	15
3.1	Studi Literatur.....	17
3.2	Integrasi Siproid dengan Modul Enkripsi.....	17
3.2.1	Perancangan Modul Enkripsi pada VoIP Client Siproid.....	17
3.2.2	Analisa Arsitektur Siproid.....	18
3.2.3	Perancangan Integrasi Modul Enkripsi pada VoIP Client Siproid.....	20
3.3	Perancangan <i>Test Bed</i> Untuk VoIP.....	25
3.4	Skenario Pengujian.....	26
3.4.1	Skenario Pengujian menggunakan Layanan Keamanan (<i>Security Service</i>).....	26
3.4.2	Skenario Pengujian menggunakan QoS (<i>Quality of Service</i>).....	26
3.4.3	Skenario Pengujian Menggunakan MOS (<i>Mean Opinion Score</i>).....	27
3.4.4	Skenario Simulasi Penyerangan.....	28
3.5	Pembahasan Hasil Pengujian.....	29
3.6	Kesimpulan dan Saran.....	29

BAB 4	Hasil dan Pembahasan	30
4.1	Implementasi Pengintegrasian Modul Enkripsi pada Sipdroid.....	30
4.1.1	Implementasi Kelas Security.java pada Sipdroid	31
4.1.2	Tampilan Sipdroid UMB dengan modul enkripsi.....	33
4.2	Pengambilan Data dari Test Bed.....	37
4.2.1	Proses pengambilan Data Dari Komunikasi VoIP	37
4.3	Hasil Pengujian Menggunakan Parameter Layanan Keamanan (Security Services).....	40
4.3.1	Hasil Pengujian <i>Data Confidentiality</i>	40
4.3.2	Hasil Pengujian <i>Data Integrity</i>	42
4.3.3	Hasil Pengujian <i>Availability</i>	43
4.4	Pengujian Kualitas Layanan (<i>Quality of Service (QoS)</i>).....	44
4.4.1	Hasil Pengujian <i>Packet Loss</i>	44
4.4.2	Hasil Pengujian <i>Delay</i>	46
4.4.3	Hasil pengujian <i>Throughput</i>	48
4.4.4	Hasil Pengujian dengan <i>Mean Opinion Score (MOS)</i> Tahap Pertama	50
4.4.5	Hasil Pengujian dengan <i>Mean Opinion Score (MOS)</i> Tahap Kedua	52
4.5	Simulasi Penyerangan	54
4.6	Pembahasan.....	55
4.6.1	Pembahasan hasil Pengujian.....	55
4.6.2	Pembahasan dengan Penelitian yang Terkait.....	57
BAB 5	Kesimpulan dan Saran	59
5.1	Kesimpulan	59
5.2	Saran	60

Daftar Pustaka	61
Lampiran	63

Daftar Gambar

Gambar 1.1 Persentase perusahaan pengguna internet berdasarkan aktifitas internet yang dilakukan (sumber: hasil survei penggunaan teknologi TIK di sektor bisnis Indonesia 2011 oleh Kominfo)	1
Gambar 2.1 Penggambaran Penelitian Terkait dengan Penelitian ini	6
Gambar 3.1 Metodologi penelitian pada penelitian ini	15
Gambar 3.2 Arsitektur Sipdroid	18
Gambar 3.3 Arsitektur Sipdroid Modifikasi	19
Gambar 3.4 Rancangan Integrasi Modul Enkripsi dengan Sipdroid	20
Gambar 3.5 Proses Integrasi Modul Enkripsi JCE dengan Sipdroid	21
Gambar 3.6 Diagram aktifitas Sipdroid yang asli	22
Gambar 3.7 Diagram aktifitas Sipdroid yang telah dimodifikasi.....	23
Gambar 3.8 Diagram kelas integrasi modul keamanan dengan Sipdroid.....	24
Gambar 3.9 Diagram RTP	24
Gambar 3.10 <i>Test bed</i> jaringan VoIP yang akan dibangun	25
Gambar 3.11 Simulasi Penyerangan.....	28
Gambar 4.1 Pemilihan skema enkripsi AES pada hasil integrasi modul enkripsi	31
Gambar 4.2 Sipdroid Normal.....	34
Gambar 4.3 Hasil Sipdroid UMB.....	35
Gambar 4.4 Menu tampilan Atur Kunci	35
Gambar 4.5 Tampilan Pilihan Algoritma Enkripsi	36
Gambar 4.6 Tampilan Kunci Enkripsi.....	37
Gambar 4.7 Proses Penangkapan paket data saat proses komunikasi VoIP di test bed	38
Gambar 4.8 Hasil berkas pcap yang dibuka di Wireshark Desktop.....	38
Gambar 4.9 Tampilan RTP Stream yang tertangkap Wireshark.....	39
Gambar 4.10 Hasil Analisa RTP stream di Wireshark.....	40
Gambar 4.11 Gambar hasil decode RTP pada Sipdroid normal	41
Gambar 4.12 Gambar hasil decode RTP pada Sipdroid dengan modul enkripsi..	42
Gambar 4.13 Hasil pengukuran <i>Packet Loss</i>	44
Gambar 4.14 Rata-rata <i>Packet Loss</i>	45

Gambar 4.15 Hasil Pengukuran <i>Delay</i>	46
Gambar 4.16 Rata-rata <i>Delay</i>	47
Gambar 4.17 Hasil Pengukuran <i>Throughput</i>	48
Gambar 4.18 Rata-rata <i>Throughput</i>	49
Gambar 4.19 Hasil Pengujian MOS	50
Gambar 4.20 Hasil Rata-rata MOS	51
Gambar 4.21 MOS Sipdroid Normal dan Sipdroid UMB AES	53
Gambar 4.22 Rata-rata MOS Sipdroid Normal dan Sipdroid UMB AES.....	54
Gambar 4.23 Arsitektur Sipdroid UMB dengan Skema Enkripsi AES.....	56

Daftar Tabel

Tabel 2.1 Parameter QoS Jaringan	12
Tabel 2.2 Nilai MOS yang direkomendasikan ITU-T	14
Tabel 3.1 Korelasi antara metode, perangkat, parameter, dan hasil pada penelitian ini	16
Tabel 4.1 Hasil Pengujian pada Data Confidentiality	41
Tabel 4.2 Hasil Pengujian Data Integrity	42
Tabel 4.3 Hasil Pengujian Availability	43
Tabel 4.4 Tabel Rata-rata <i>Packet Loss</i>	45
Tabel 4.5 Rata-rata Delay	47
Tabel 4.6 Rata-rata <i>Throughput</i>	49
Tabel 4.7 Rata-rata MOS	51
Tabel 4.8 Rata-rata MOS Sipdroid Normal dan Sipdroid UMB AES	53
Tabel 4.9 Hasil Simulasi Penyerangan	55

Daftar Istilah

- Android: Sistem operasi buatan Google, yang awalnya dikhususkan untuk dijalankan di *handset*.
- Data stream: seurutan signal koheren yang diencode secara digital (paket data) digunakan untuk mengirimkan atau menerima informasi yang dalam proses pengiriman.
- Framework: dalam dunia perangkat lunak dikenal sebagai susunan kepastakaan atau kelas-kelas yang dapat digunakan kembali untuk mengembangkan sebuah perangkat lunak baru.
- RTP: protokol yang dijadikan standar untuk format paket audio dan video melalui jaringan berbasis IP.
- SIP: kepanjangan dari *Session Initiation Protocol*, merupakan protokol yang digunakan untuk mengatur sesi komunikasi, seperti panggilan suara dan video.
- VoIP: kepanjangan dari *Voice Over Internet Protocol*, yaitu teknologi untuk melakukan komunikasi melalui layanan IP.
- VoIP Client: aplikasi *softphone* untuk melakukan komunikasi melalui jaringan VoIP.
- Wireshark: perangkat untuk menganalisa protokol pada jaringan.