



UNIVERSITAS INDONESIA

**ANALISIS SISTEM KEAMANAN
UNTUK MOBILE WIMAX**

SKRIPSI

**SJAIFUL RIJAL
06 06 04 2916**

**FAKULTAS TEKNIK UNIVERSITAS INDONESIA
PROGRAM STUDI TEKNIK ELEKTRO
DEPOK
DESEMBER 2008**



UNIVERSITAS INDONESIA

**ANALISIS SISTEM KEAMANAN
UNTUK MOBILE WIMAX**

SKRIPSI

Diajukan sebagai salah satu syarat untuk memperoleh gelar sarjana teknik

**SJAIFUL RIJAL
06 06 04 2916**

**FAKULTAS TEKNIK UNIVERSITAS INDONESIA
PROGRAM STUDI TEKNIK ELEKTRO
DEPOK
DESEMBER 2008**

HALAMAN PERNYATAAN ORISINALITAS

Skripsi ini adalah hasil karya saya sendiri,
dan semua sumber baik yang dikutip maupun dirujuk
telah saya nyatakan dengan benar.

Nama : Sjaiful Rijal

NPM : 0606042916

Tanda Tangan :

Tanggal : 22 Desember 2008



HALAMAN PENGESAHAN

Skripsi ini diajukan oleh :
Nama : SJAIFUL RIJAL
NPM : 0606042916
Program Studi : Teknik Elektro
Judul Skripsi : ANALISIS SISTEM KEAMANAN
UNTUK MOBILE WIMAX

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Sarjana Teknik pada Program Studi Teknik Elektro, Fakultas Teknik, Universitas Indonesia

DEWAN PENGUJI

Pembimbing : Dr. Ir. Muhammad Asvial, M.Eng (.....)

Penguji : Ir. Gunawan Wibisono, M.Sc., PhD (.....)

Penguji : Fitri Yuli Zulkifli, ST., M.Sc. (.....)

Ditetapkan di : Depok

Tanggal : 22 Desember 2008

UCAPAN TERIMA KASIH

Puji syukur saya panjatkan kepada Allah SWT, karena atas berkat dan rahmat-Nya, saya dapat menyelesaikan skripsi ini. Penulisan skripsi ini dilakukan dalam rangka memenuhi salah satu syarat untuk mencapai gelar Sarjana Teknik pada Departemen Teknik Elektro Fakultas Teknik Universitas Indonesia. Saya menyadari bahwa, tanpa bantuan dan bimbingan dari berbagai pihak, dari masa perkuliahan sampai pada penyusunan skripsi ini, sangatlah sulit bagi saya untuk menyelesaikan skripsi ini. Oleh karena itu, saya mengucapkan terima kasih kepada:

- (1) Dr. Ir. Muhammad Asvial, M.Eng, selaku dosen pembimbing yang telah menyediakan waktu, tenaga, dan pikiran untuk mengarahkan saya dalam penyusunan skripsi ini.
- (2) Ibu tercinta, yang tak terhitung cinta kasihnya, hanya inilah yang bisa saya berikan untuk kado di hari ibu tahun ini. Bapak, atas dedikasinya pada pendidikan saya serta kakak, adik dan seluruh keluarga atas dukungannya yang tak pernah berhenti.
- (3) Sahabat-sahabat setia dan saudara seperjuangan : Taqin, DAS, Awan, teman-teman seluruh angkatan beserta segenap civitas akademika Universitas Indonesia.
- (4) Berbagai elemen baik di dunia nyata maupun dunia maya yang telah memberikan inspirasi, motivasi dan apresiasi yang teramat banyak untuk saya sebutkan satu-persatu

Akhir kata, saya berharap Allah SWT berkenan membalas segala kebaikan semua pihak yang telah membantu. Semoga skripsi ini membawa manfaat bagi pengembangan ilmu.

Depok, 22 Desember 2008

Penulis

**HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI
TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS**

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini:

Nama : Sjaiful Rijal
NPM : 0606042916
Program Studi : Teknik Elektro
Departemen : Teknik Elektro
Fakultas : Teknik
Jenis karya : Skripsi

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Noneksklusif** (*Non-exclusive Royalty-Free Right*) atas karya ilmiah saya yang berjudul :

Analisis Sistem Keamanan Untuk Mobile WiMax

beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan memublikasikan tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Depok
Pada tanggal : 22 Desember 2008
Yang menyatakan

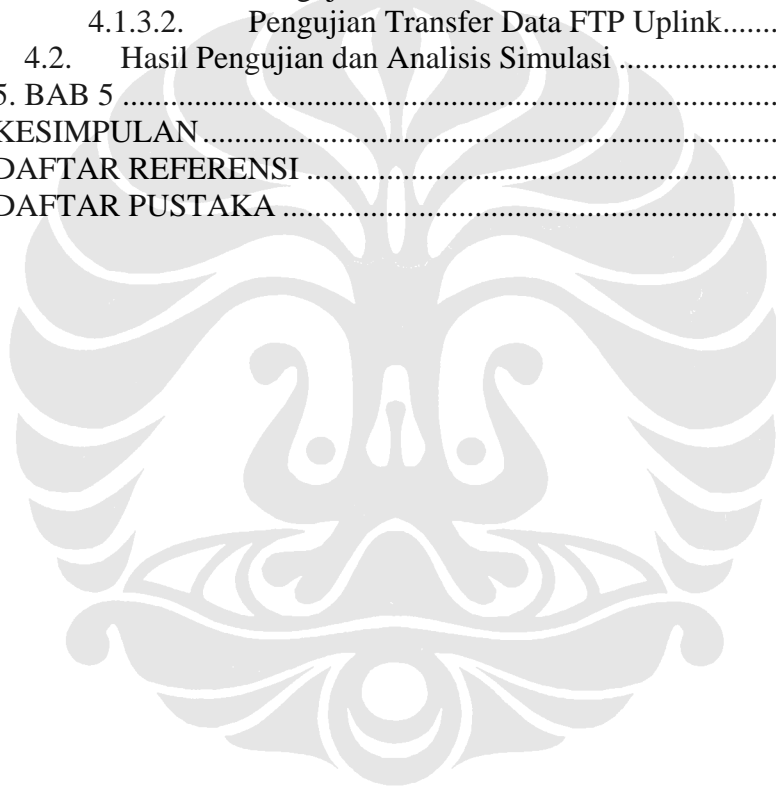
(Sjaiful Rijal)

DAFTAR ISI

Halaman

HALAMAN JUDUL.....	i
HALAMAN PERNYATAAN ORISINALITAS.....	ii
HALAMAN PENGESAHAN.....	iii
UCAPAN TERIMA KASIH.....	iv
HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI.....	v
ABSTRAK.....	vi
ABSTRACT.....	vii
DAFTAR ISI.....	viii
DAFTAR GAMBAR.....	x
DAFTAR TABEL.....	xi
DAFTAR TABEL.....	xi
1. BAB 1.....	1
PENDAHULUAN.....	1
1.1. LATAR BELAKANG.....	1
1.2. TUJUAN PENULISAN.....	1
1.3. BATASAN MASALAH.....	2
1.4. SISTEMATIKA PENULISAN.....	2
2. BAB 2.....	4
DASAR TEORI SISTEM KEAMANAN MOBILE WIMAX.....	4
2.1. Pengenalan WiMax.....	4
2.2. Lapisan Protokol WiMax.....	5
2.3. Aspek Jaringan.....	6
2.4. MAC Protocol Data Unit (MPDU).....	7
2.5. Security Association (SA).....	9
2.6. Kriptografi.....	10
2.6.1. Panjang Kunci.....	12
2.6.2. Kriptografi Kunci Rahasia dan Kunci Publik.....	13
2.6.2.1. Kriptografi Kunci Rahasia.....	14
2.6.2.2. Kriptografi Kunci Publik.....	14
2.6.3. Penyandian Blok.....	15
2.6.3.1. Electronic Code Book (ECB).....	16
2.6.3.2. Cipher Block Chaining (CBC).....	16
2.6.3.3. Cipher Feedback (CFB).....	17
2.6.3.4. Output Feedback (OFB).....	18
2.7. Proses Pengamanan.....	18
2.7.1. Memulai Koneksi.....	18
2.7.2. Autentikasi.....	20
2.7.3. Pertukaran Kunci Data.....	21
2.7.4. Privasi Data.....	22
3. BAB 3.....	25
PERANCANGAN SISTEM.....	25
3.1. Deskripsi Umum Sistem.....	25
3.2. Perangkat Yang Digunakan.....	26
3.2.1. Stasiun Utama.....	26

3.2.2.	Stasiun Pelanggan	28
3.3.	Metode Sistem Keamanan yang Digunakan	30
3.4.	Program Simulasi Sistem Keamanan	30
3.4.1.	Platform Perangkat Lunak Simulasi.....	31
3.4.2.	Diagram Alir Perangkat Lunak Simulasi	31
3.4.2.1.	Diagram Alir Enkripsi.....	32
3.4.2.2.	Diagram Alir Dekripsi.....	33
4. BAB 4		34
ANALISIS DAN PENGUJIAN SISTEM.....		34
4.1.	Hasil Pengujian dan Analisis Sistem	34
4.1.1.	Pengujian dan Analisis Pemindaian Frekuensi	34
4.1.2.	Pengujian dan Analisis Autorisasi	35
4.1.3.	Pengujian dan Analisis Transfer Data FTP	37
4.1.3.1.	Pengujian Transfer Data FTP Downlink.....	39
4.1.3.2.	Pengujian Transfer Data FTP Uplink.....	41
4.2.	Hasil Pengujian dan Analisis Simulasi	41
5. BAB 5		45
KESIMPULAN		45
DAFTAR REFERENSI		46
DAFTAR PUSTAKA		47



DAFTAR GAMBAR

Halaman

Gambar 2.1 Lapisan Protokol WiMax	5
Gambar 2.2 Arsitektur Jaringan WiMax	6
Gambar 2.3 MAC PDU	7
Gambar 2.4 Generic MAC Header.....	8
Gambar 2.5 Struktur BRH PDU	9
Gambar 2.6 Gambar Proses Enkripsi dan Dekripsi	12
Gambar 2.7 Kriptografi simetris	14
Gambar 2.8 Kriptografi Asimetris	15
Gambar 2.9 Mode Operasi ECB	16
Gambar 2.10 Mode Operasi CBC	17
Gambar 2.11 Mode Operasi CFB	18
Gambar 2.12 Proses koneksi.....	19
Gambar 2.13 Proses Autentikasi	20
Gambar 2.14 Proses Pertukaran Key	21
Gambar 2.15 Diagram Blok Pengenkripsian Payload.....	24
Gambar 3.1 Diagram Jaringan WiMax	26
Gambar 3.2 Perangkat Base Station WiMax.....	28
Gambar 3.3 CPE Motorola tipe wolverine	29
Gambar 3.4 CPE Motorola tipe badger.....	30
Gambar 4.1 Pemindaian Akses Poin WiMax yang Tersedia	34
Gambar 4.2 Hasil Tes Ping dari CPE ke EMS Pada Saat CPE Belum Melakukan Inisiasi	35
Gambar 4.3 Hasil Pengujian Status Autentikasi Terminal Pengguna WiMax	36
Gambar 4.4 Hasil Tes Ping Dari CPE ke Server EMS Pada Saat Status Tersambung	37
Gambar 4.5 Status Koneksi Sebelum Melakukan FTP	38
Gambar 4.6 Hasil Tes Ping Dari CPE ke Server FTP	39
Gambar 4.7 Trafik Saat Pengujian FTP Downlink	39
Gambar 4.8 Status MAC Pada CPE Saat Melakukan FTP	40
Gambar 4.9 Trafik Saat Transfer Data FTP Uplink.....	41
Gambar 4.10 Tampilan Program Simulasi.....	42

DAFTAR TABEL

Halaman

Tabel 2.1 Field-field GMH	8
Tabel 2.2 Field-field BRH.....	9
Tabel 3.1 Daftar Spesifikasi Perangkat Akses Poin WiMax.....	27
Tabel 3.2 Daftar spesifikasi perangkat CPE	28

