SISTEM PENGAMANAN PADA GPRS

(GENERAL PACKET RADIO SERVICE)

PT. TELKOMSEL

Diajukan untuk memenuhi persyaratan
Mencapai Gelar sarjana Strata – 1
Fakultas Teknologi Industri

DISUSUN OLEH :

Erwin Harafan

01497 – 030

UNIVERSITAS MERCU BUANA
FAKULTAS TEKNOLOGI INDUSTRI
Jurusan Teknik Elektro
JAKARTA
2005

PERNYATAAN KEASLIAN KARYA TUGAS AKHIR

Saya yang bertandatangan dibawah ini :

Nama	:	Erwin Harafan
Nim	:	01497-030
Fakiltas	:	Teknologi Industri
Jurusan	:	Elektro
Program studi	:	Telekomunikasi

Dengan ini menyatakan bahwa karya tulis yang saya buat dengan judul

"SISTEM PENGAMANAN PADA GPRS
(GENERAL PACKET RADIO SERVICE) PT. TELKOMSEL"

Adalah hasil karya sendiri, kecuali yang saya nyatakan sebagai sumbernya dan belum pernah dipublikasikan untuk mendapatkan gelar sarjana di Universitas lain kecuali pada bagian-bagian sumber informasinya yang dicantumkan dengan cara referensi yang semestinya.

Jakarta, Februari 2005

(Erwin Harafan)

LEMBAR PENGESAHAN

Tugas akhir ini untuk melengkapi tugas-tugas dan memenuhi persyaratan dalam memperoleh gelar Sarjana Teknik, jenjang pendidikan Strata 1 (S-1), Jurusan Teknik Elektro Fakultas Teknologi Industri, Universitas Mercu Buana Jakarta.

Judul Tugas Akhir	:	SISTEM PENGAMANAN PADA GPRS (GENERAL PACKET RADIO SERVICE) PT. TELKOMSEL

Disusun oleh :

Nama	:	**Erwin Harafan**
NIM	:	01497-030
Jurusan	:	Teknik Elektro/Telkom
Fakultas	:	Teknologi Industri

Telah diperiksa dan disetujui untuk diajukan pada sidang Sarjana

Jakarta,

Pembimbing

Ir. A. Y. Syauki, MBAT

Mengetahui
Ketua Jurusan Teknik Elektro

Ir. Budi Yanto, MSC

ABSTRACT

Network system of General Packet Radio Service, GPRS is a new bearer service that developed in the GSM infrastructure, which a communications technology based on packet switch data. GPRS applies a packet radio principle to access to packet data network efficiently and high bit rate with several excess services. Technically this service allows new application and variation of services, the new set of application using GPRS service will be influenced by the level of security offered. Moreever, operating of GPRS is connected with other network, this scurity function is significant to ensure a secure transmition of data trought this network.

In this assignment will be discussed an issue that related with security system in GPRS service. Level of security from GPRS system in overall is defined by level of sub system security of its architechture. Therefore, the needs of analisys of every elements from GPRS infrastructure required, includes the entity and the interface. Discussion of security aspect in GPRS service that related with air interface and GPRS backbone network with their interconnection between GPRS backbone.

KATA PENGANTAR

Puji dan syukur Penulis panjatkan ke hadirat Allah SWT yang telah memberikan nikmat sehat dan juga kemudahan sehingga tulisan ini dapat terselesaikan. Shalawat dan salam juga Penulis curahkan kepada Rasulullah Muhammad SAW beserta keluarga dan sahabatnya.

Tugas akhir ini ditulis untuk memenuhi salah satu persyaratan dalam menyelesaikan pendidikan Strata 1 (S-1) pada jurusan Teknik Elektro Universitas Mercu Buana Jakarta.

Pada kesempatan ini Penulis ingin mengucapkan terima kasih yang sebesar-besarnya kepada :

1. Kedua Orang Tua saya, atas dukungan materil dan moril selama perkuliahan penulis.
2. Bpk. Dr. Ing. Mudrik Alaydrus, selaku koordinator Tugas Akhir dan Ketua jurusan Teknik Elektro Universitas Mercu Buana Jakarta.
3. Bpk. Ir. A.Y.Syauki, MBAT, selaku pembimbing tugas akhir yang telah memberikan arahan dalam penyelesaian tugas akhir ini
4. Bpk. Ir. Agus Irawan selaku pembimbing teknis yang telah memberikan bimbingan dan arahan dalam penyelesaian tugas akhir ini
5. Seluruh Dosen dan Staff karyawan jurusan Teknik Elektro.
6. Pimpinan dan Staff PT Telkomsel yang telah memberikan informasi sesuai dengan keburuhan dalam menyelesaikan tugas akhir ini

7. Rekan-rekan Mahasiswa Teknik Elektro Universitas Mercu Buana Khususnya angkatan 97 dan semua pihak yang telah membantu penulisan tugas akhir ini.
8. Komeng, Bonny, Wisnu, Iyul, Toto, Echa, Asep, Tatang, team XEROX, dan semua teman-teman yang telah membantu, yang tidak dapat penulis sebutkan satu persatu.
9. Rekan-rekan kerja CITY PARKING LIPPO SUPERMALL,Khususnya N.J. (071) dengan rasa cinta dan sayangnya, yang telah memberikan semangat dan perhatiannya

Penulis menyadari bahwa tulisan ini masih jauh dari sempurna, oleh karena itu adanya saran dan kritik yang membangun sangat diharapkan. Semoga tulisan ini dapat bermanfaat bagi siapa saja yang membacanya.

Jakarta,Oktober 2005

Erwin Harafan
01497030

PERPUSTAKAAN UMB

DAFTAR ISI

Halaman

LEMBAR PENGESAHAN

ABSTRAK iii

KATA PENGANTAR vii

DAFTAR ISI ix

DAFTAR GAMBAR xiii

DAFTAR ISTILAH xiv

BAB I PENDAHULUAN

1.1 Latar Belakang 1

1.2 Maksud dan Tujuan Penulisan 2

1.3 Batasan Masalah 3

1.4 Metode Penulisan 3

1.5 Sistematika Penulisan 4

BAB II LANDASAN TEORI

II.1. Pendahuluan 5

II.2 Sistem Komunikasi Seluler 6

II.2.1 Radius Sel 9

II.2.2 Roaming 10

II.2.3. Handover 10

II.2.3.1. Jenis-Jenis Handover 12

II.2.3.2. Tipe Handover 13

II.2.4. Pembelahan Sel 14

II.2.5. Alokasi Frekuensi 15

II.2.6. Frekuensi Reuse 15

II.2.7. Interferensi 16

II.2.7.1. Cochannel Interference 17

II.2.7.2. Adjacent Channel Interference 17

II.3 Arsitektur GSM 18

II.3.1. Base Station System (BSS) 19

II.3.1.1. Mobile Station (MS) 19

II.3.1.2. Base Transciever Station (BTS) 19

II.3.1.3. Base Station Controler (BSC) 20

II.3.2. Network Swithcing System 20

II.3.2.1. Mobile Switching Center 20

II.3.2.2. Home Location Register (HLR) 21

II.3.2.3. Visitor Location Register (VLR) 21

II.3.2.4. Authentic Center (AuC) 21

II.3.2.5. Equepment Identity Register (EIR) 22

II.3.3. Operating Support System (OSS) 22

II.4. Data Switching 23

BAB III SISTEM PENGAMANAN PADA GPRS

III.1. Pendahuluan 15

III.2. Universal Subcriber Identity Module (USIM) 28

III.3. Fungsi Keamanan Pada Interface Udara 29

III.3.1. Aspek Kemanan pada Sistem Kemanan GPRS 30

III.3.1.1. Kerahasiaan 30

III.3.1.2. Otentikasi *(Authentication)* 31

III.3.1.3. Ketersediaan *(Availability)* dan Integritas *(Integrity)* 31

III.3.1.4. Pengaturan Akses *(Acces Control)* 31

III.3.1.5. Sistem Kriptografi 32

III.3.1.6. Enkripsi dan Dekripsi 32

III.3.2. Kerahasiaan Data dan Pensinyalan antara MS dan SGSN 33

III.3.2.1. Metode Penyandian 34

III.3.2.2. Key Setting 34

III.3.2.3. Titik Awal Proses Chipering 35

III.3.2.4. Sinkronisasi 36

III.3.3. Kerahasiaan Identitas Pelanggan 37

III.4. Keamanan Pada Backbone GPRS 39

III.4.1. GPRS Tunnel Protocol (GTP) 40

III.4.2. IP Roating 40

III.4.3. Pengaman IP *(IP Security)* 41

III.4.3.1. Security Asociation 42

III.4.3.2. IP Encapsulating Security Payload (ESP) 43

III.4.4. Manajemen Pertukaran Kunci 44

III.4.5. Interkoneksi Antar Jaringan Backbone GPRS 45

III.4.6. Firewall 47

III.5. Analisis Aspek Keamanan pada Layanan GPRS 50

III.5.1. Analisis Aspek Keamanan pada Interface Udara 52

III.5.2. Analisis Keamanan pada MS dan Kartu SIM 53

III.5.3. Analisisi Keamanan pada Backbone GPRS 56

III.6. Contoh Kasus 59

BAB IV GENERAL PACKET RADIO SERVICE

IV.1. Pendahuluan 61

IV.2. Penggunaan CSD dan PSD 62

IV.3. Arsitektur Jaringan GPRS 65

IV.3.1. Serving GPRS Support Node (SGSN) 66

IV.3.2. Gateway GPRS Support Node (GGSN) 66

IV.3.2.1. Billing System 67

IV.3.2.1. Fungsi Otentikasi 67

VI.3.2.3. Fungsi Registrasi 67

IV.3.3. Elemen-Elemen dari Jaringa GPRS 68

IV.3.3.1. Base Station System (BSS) 68

IV.3.3.2. Network Switching System (NSS) 68

IV.3.3.3. Jaringan Backbone GPRS 69

IV.3.3.4. Interkoneksi antar Jaringan Backbone GPRS 70

IV.3.3.5. Border Gateway (BG) 70

IV.4. Coding Scheme 71

IV.4.1. Coding Scheme, CS-1 dan CS-2 72

IV.4.2. Pemilihan Coding Scheme 72

BAB V KESIMPULAN DAN SARAN

V.1. Kesimpulan 77

V.2. Saran 77

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR RIWAYAT HIDUP

DAFTAR GAMBAR

	Halaman
1. Gambar 2.1. Multiple Access FDMA dan TDMA	 8
2. Gambar 2.2. Sistem GSM dengan TDMA	 9
3. Gambar 2.3. Roaming pada Subscriber	 10
4. Gambar 2.4. Handover antar BTS dalam satu BSC dan MSC	 12
5. Gambar 2.5. Handover antar BTS dan BSC dalam satu MSC	 13
6. Gambar 2.6. Handoff antar BTS, BSC dan MSC	 13
7. Gambar 2.7. Pembelahan Sel	 14
8. Gambar 2.8. Alokasi Frequency Channel GSM	 15
9. Gambar 2.9. Adjacent Channel Interference	 18
10. Gambar 2.10. Arsitektur Jaringan GSM	 23
11. Gambar 2.11. Jaringan Transmisi Circuit Swithed dan Pcket Swithed	 25
12. Gambar 3.1. Key Setting	 35
13. Gambar 3.2. Proses Sinkronisasi Chipering dan Dechipering	 36
14. Gambar 3.3. Interkoneksi antar Jaringan Backbone GPRS	 47
15. Gambar 4.1. Arsitektur Jaringa GPRS	 65
16. Gambar 4.2. Block RLC Konstruksi CS-1 dan CS-2	 72
17. Gambar 4.3. Grafik Perbandingan CS terhadap C/I	 73
18. Gambar 4.4. Grafik Perbandingan CS terhadap Besar Paket Data	 75

DAFTAR TABEL

Halaman

1. Tabel 4.1. Parameter untuk GPRS Coding Schemes 73

DAFTAR ISTILAH

AuC	= Authentication Centre
BAS	= Billing Administration System
BEC	= Backward Error Correction
BG	= Border Gateway
BSC	= Base Station Controller
BSS	= Base Station System
BSSGP	= Base Station System GPRS Protocol
BTS	= Base Transceiver System
CG	= Charging Gateway
CSD	= Circuit Switched Data
DNS	= Domain Name Servers
EDGE	= Enhanced Date rate for GSM Evolution
EIR	= Equipment Identity Register
ETSI	= European Telecommunication Standar Institute
FDMA	= Frequency Division Multiple Access
FEC	= Forward Error Corection
GGSN	= Gateway GPRS Support Node
GPRS	= General Packet Radio Sytem
GSM	= Global System for Mobile
GTP	= GPRS Tunnelling Protocol
HLR	= Home Location Register

HSCSD	= High Speed Circuit Switched Data
IMEI	= International Mobile Equipment Identity
IMT 2000	= International Mobile Telecommunication 2000
ISDN	= Integrated Service Digital Network
ITU	= International Telecommunication Union
LAN	= Local Area Network
LLC	= Logical Link Control
MAC	= Medium Access Control
MCC	= Mobile Country Code
MNC	= Mobile Network Code
MS	= Mobile Station
MSC	= Mobile Switching Centre
MSIN	= Mobile Subscriber Identification Number
NAT	= Network Address Translation
NSAPI	= Network layer Service Acces Point Identifier
NSS	= Network and Switching Subsystem
OSS	= Operation SubSystem
PCS	= Personalization Centre for SIMs
PIN/PUK	= Personal Identification Number/ PIN Unblocking Key
PLMN	= Public Land Mobile Network
PSTN	= Public Switch Telephone Network
RLC	= Radio Link Control
SAPI	= Service Access Point Identifier

SGSN = Serving GPRS Support Node

SIM = Subscriber Identity Module

SMS = Short Message Service

SNDCP = SubNetwork Dependent Convergence Protokol

TCP/IP = Transmission Control Protocol/ Internet Protocol

TDMA = Time Division Multiple Access

TID = Tunnel ID Format

TLLI = Temporary Logical Link Identity

TRAU = Transcoder Unit

UMTS = Universal Mobile Telecommunication System

VLR = Visitor Location Register

WAP = Wireless Application Protocol