

Keamanan dalam Jaringan GPRS

Dibuat untuk memenuhi tugas mata kuliah:

EC-5010 Keamanan Sistem Informasi

Oleh:

L. Lintaka (132 99 013)

Departemen Teknik Elektro
Institut Teknologi Bandung
2004

Abstrak

Secara umum *Mobile IP* dapat dikatakan sebagai *mobilized internet*, yaitu layanan koneksi internet yang dipakai oleh perangkat komunikasi bergerak seperti telepon selular dan PDA. Pengguna (*subscriber*) harus memiliki akses ke operator yang mendukung layanan ini. Operator harus sudah memiliki jaringan selular 2.5G seperti GPRS/EDGE, atau sudah memiliki lisensi jaringan 3G (UMTS/CDMA2000). GPRS adalah jaringan yang paling umum digunakan di Indonesia untuk memperoleh akses internet kecepatan tinggi.

Dengan adanya jaringan GPRS pengguna dapat terhubung dengan jaringan internet dengan kecepatan tinggi pada perangkat bergerak (telepon selular, PDA). Tidak berbeda dengan koneksi internet biasa, masalah keamanan data di GPRS menjadi topik bahasan tersendiri. Untuk menjaga keamanan, pihak operator biasanya menggunakan *VPN (Virtual Private Network)* untuk menghubungkan perangkat bergerak pengguna dengan jaringan operator. Namun hal ini tidak menjamin keamanan data pengguna. Data bisa saja dibajak oleh sesama pengguna, karena memakai VPN yang sama.

Biasanya billing dan autentifikasi server terletak pada VPN yang sama dengan pengguna. Hal ini bisa dieksploitasi oleh pengguna, sehingga bisa merubah tagihan billing internet atau malah membuat autentifikasi yang baru sehingga bisa membuat gratis tagihan internetnya.

Kejahatan secara umum di internet seperti *hacking* dengan mempergunakan jaringan GPRS akan susah dilacak keberadaannya. Pelaku tidak mudah diketahui walaupun banyak meninggalkan jejak. Walaupun operator mempunyai *LBS (Location Base Server)* pelaku akan susah dicari karena pelaku dapat dengan mudah berpindah-pindah tempat. Pelaku dapat dengan mudah berganti-ganti operator dan membuang akses operator lama (*tinggal mengganti SIM Card*). Kalaupun operator mengidentifikasi berdasar kode unik perangkat bergerak yang dipakai (*IMEI* pada telepon selular), pelaku tinggal mengganti telepon selular yang baru.

1. Pendahuluan

Mobile IP secara umum bisa dikatakan sebagai *mobilized internet*, yaitu koneksi internet untuk perangkat bergerak seperti telepon selular, *PDA*, dan perangkat bergerak lainnya. Secara umum perangkat bergerak yang mendapatkan alamat IP (*Internet Protocol*), alamat IP tersebut bisa dikatakan sebagai *Mobile IP*. Sebagai contoh adalah penggunaan dial up lewat CSD dengan menggunakan telepon selular akan mendapatkan alamat IP dinamis.

Menurut standard *Mobile IP* (RFC 2002), yang diajukan oleh IETF (*Internet Engineering Task Force*), *Mobile IP* membuat perangkat yang terhubung ke internet akan mendapat alamat IP yang sama walaupun berpindah jaringan IP-nya (misal berpindah gateway). Dengan *Mobile IP* ini pengirim data tidak perlu tahu alamat IP penerima data. Tidak semua perangkat bergerak yang mendapat nomor IP bisa dikatakan sebagai *Mobile IP*.

GPRS (*General Packet Radio Service*) adalah teknologi yang digunakan dalam jaringan GSM untuk menangani komunikasi data. Dalam jaringan *GPRS* digunakan teknologi *Mobile IP* untuk menyampaikan pesan dari gateway yang menangani paket data GSM ke gateway yang menangani konversi paket data GSM ke paket data TCP/IP atau sebaliknya.

Di Indonesia jaringan selular yang banyak dipakai adalah GSM. Hampir sebagian besar operator GSM telah meningkatkan layanan mereka dengan menambah layanan *GPRS*. Dengan layanan *GPRS* pengguna (*subscriber*) bisa terhubung ke internet, mendownload e-mail, chatting, browsing, dll. Selain itu dengan adanya *GPRS* operator bisa menambah layanan *MMS* (*Multimedia Messaging Service*) yaitu layanan pengiriman data multimedia (suara/film) antar telepon selular.

Dalam proposal yang diajukan untuk tugas mata kuliah ini, penulis mengajukan judul 'Keamanan Jaringan dalam *Mobile IP*'. Isi dari proposal tersebut sebenarnya membahas tentang keamanan dalam jaringan *GPRS*. Untuk menghindari kerancuan antara definisi *Mobile IP* secara umum dan definisi yang menurut IETF, sehingga penulis merubah judul tugas menjadi 'Keamanan dalam Jaringan *GPRS*'. Makalah ini membahas tentang masalah keamanan apa yang bisa terjadi dalam jaringan *GPRS*, disertai dengan beberapa studi kasus keamanan pada jaringan *GPRS* salah satu operator GSM di Indonesia.

Makalah ini hanya membahas tentang keamanan yang berkaitan dengan jaringan *GPRS*. Apa saja kelemahan dalam jaringan *GPRS*? Kemungkinan apa saja yang bisa terjadi bila ada seseorang memanfaatkan kelemahan itu? Dan bagaimana kemungkinan menghindarinya.

2. Jaringan GPRS

2.1. Apa Itu GPRS?

GPRS yang termasuk dalam kelas 2.5 G adalah standard komunikasi data di jaringan GSM yang kecepatan transfernya mencapai 115 kbps. Dengan adanya GPRS ini jaringan GSM bisa memisah paket data kecepatan tinggi dengan suara.

Dengan adanya GPRS ini pengguna bisa terus terkoneksi ke internet. Pengguna tidak perlu dial up terus menerus ketika akan melakukan koneksi ke internet. Tagihan internet tidak berdasar lama waktu penggunaan internet namun berdasar banyaknya data yang dikirim/diterima.

2.2. Alasan Teknis Penggunaan GPRS

Sebelum ada pengembangan transmisi data lewat GPRS, transmisi data GSM sangat lambat, hal ini dikarenakan kanal radionya yang bersifat tunggal dan berkecepatan rendah, dan diperuntukkan khusus bagi setiap pengguna data selama durasi komunikasi (*dedicated*). Komunikasi yang bersifat *dedicated* ini menyebabkan operator harus menyediakan sambungan yang banyak agar semua pemakai bisa melakukan komunikasi data. Hal ini membuat biaya perawatan dan penambahan sambungan bagi operator semakin mahal.

GPRS menggunakan teknologi *packet switching* memungkinkan semua pengguna dalam sebuah sel dapat berbagi sumber-sumber yang sama; dengan kata lain para pelanggan menggunakan spektrum radio hanya ketika benar-benar mentransmisikan data. Efisiensi penggunaan spektrum pada akhirnya berarti kinerja yang lebih baik dan biaya yang lebih rendah. GPRS dapat menawarkan laju data sampai 115 kbps atau lebih.

GPRS disebut teknologi 2.5 G karena merupakan langkah awal menuju teknologi transfer data kecepatan tinggi lewat jaringan nirkabel (3G). Sehingga sering disebut-sebut sebagai teknologi kunci untuk data bergerak. Secara rinci ada beberapa faktor yang menjadi pertimbangan bahwa GPRS merupakan teknologi kunci untuk data bergerak, yakni;

- mampu memanfaatkan kemampuan cakupan global yang dimiliki GSM (2G)
- memperkaya utiliti investasi untuk perangkat GSM yang sudah ada

- merupakan teknologi jembatan yang bagus menuju generasi ke 3
- berbasis paket data yang lebih efisien dalam penggunaan sumber daya
- memiliki laju data sampai 115 kbps yang berarti dua kali lipat daripada koneksi 'dial up' 56 kbps yang berlaku

Dengan adanya GPRS ini operator GSM dapat menambah layanan bagi para pengguna. Pengguna tidak hanya bisa melakukan komunikasi suara namun juga bisa melakukan komunikasi data. Beberapa layanan yang berkembang dengan adanya jaringan GPRS ini antara lain:

- MMS (*Multimedia Messaging System*), dengan MMS ini pengguna bisa mengirimkan pesan dalam bentuk multimedia (suara, klip video, gambar)
- *Traffic Monitoring*, dengan layanan ini pengguna bisa melihat keadaan lalu lintas di suatu tempat secara *real time*, dengan maksud agar mengetahui daerah mana yang macet dan daerah mana yang lalu lintasnya sepi.
- VOIP (*Voice Over IP*), layanan ini biasanya digunakan antar pengguna PDA. Pemakai PDA pertama harus menginstal suatu program terlebih dahulu baru bisa menggunakan VOIP. Teknologi ini akan efektif bila tarif GPRS dihitung secara *flat*, sehingga walaupun banyak data yang ditransfer namun harga yang dibayarkan tetap sama.

2.3. Arsitektur Umum Jaringan GPRS

Gambar 2.1 adalah arsitektur jaringan GPRS secara umum. Dalam gambar di bawah terlihat bahwa jaringan GPRS merupakan bagian dari jaringan GSM (beberapa bagian dalam jaringan GPRS dipakai untuk komunikasi suara). Berikut penjelasan bagian-bagian dalam gambar tersebut:

MS – Mobile Station

MS dapat dikatakan perangkat selular yang terhubung langsung dengan jaringan GSM, yaitu *SIM (Subscriber Identify Module) Card* dan perangkat keras seperti telepon selular, PDA, perangkat komputer yang terhubung menggunakan jaringan GPRS. Untuk selanjutnya

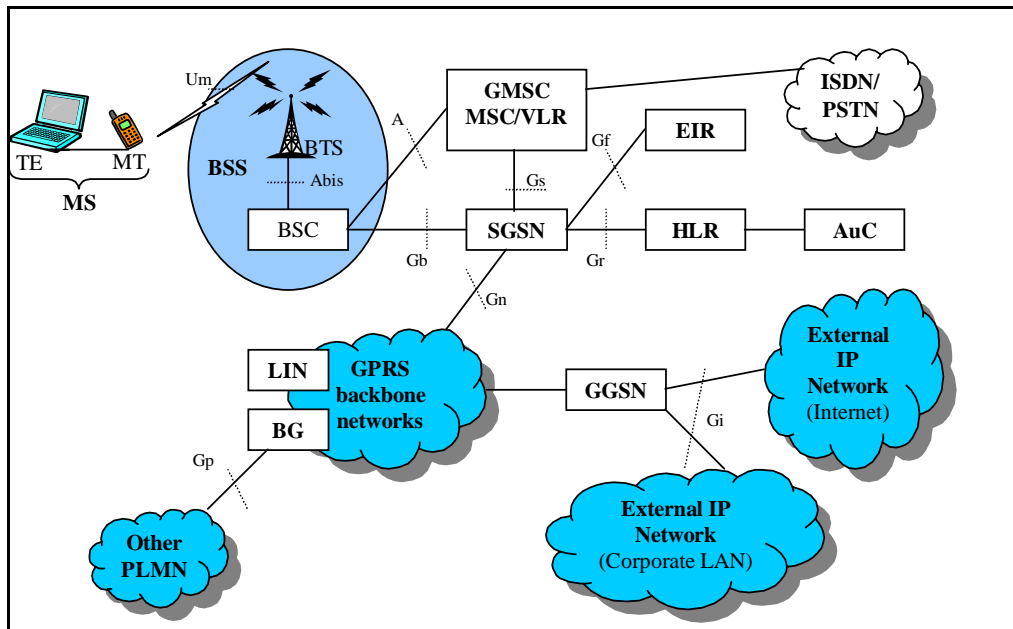
dalam tulisan ini yang dimaksud dengan MS adalah lebih mengarah kepada komputer yang terhubung ke jaringan GPRS dengan menggunakan GPRS Modem (telepon selular).

BSS – Base Station System

BSS terdiri dari BTS (*Base Transceiver Station*) dan BSC (*Base Station Controller*). Di BSS sinyal radio dari BSS akan diterima oleh BTS dan selanjutnya diteruskan ke BSC. BSC menangani sinyal yang dikirimkan oleh beberapa BTS.

HLR – Home Location Register

HLR adalah database yang menyimpan data pengguna jaringan GPRS. Informasi yang disimpan dalam HLR misalnya APN (*Access Point Name*).



Gambar 2.1 Arsitektur Jaringan GPRS

VLR – Visitor Location Register

VLR adalah database yang berisi informasi semua MS yang sedang terhubung dengan GPRS.

SGSN – Serving GPRS Support Node

SGSN adalah komponen utama jaringan GPRS. SGSN akan meneruskan paket data dari/ke MS.

GGSN – Gateway GPRS Support

GGSN juga merupakan komponen utama jaringan GPRS. GGSN mengubah paket data GSM dari SGSN menjadi paket TCP/IP. GGSN dan SGSN digunakan sebagai penghitung pembayaran pemakaian internet.

EIR – Equipment Identity Register

EIR adalah database yang berisi data tentang perangkat bergerak. Dalam EIR bisa berisi data-data IMEI dari telepon selular yang diperbolehkan/tidak diperbolehkan memakai GPRS.

AuC – Authentication Center

AuC adalah database yang berisi informasi pengguna yang diperbolehkan memakai jaringan GPRS. AuC merupakan bagian dari HLR.

GPRS backbone networks

GPRS backbone network adalah intranet dari jaringan GPRS. GPRS backbone networks adalah *IP based*.

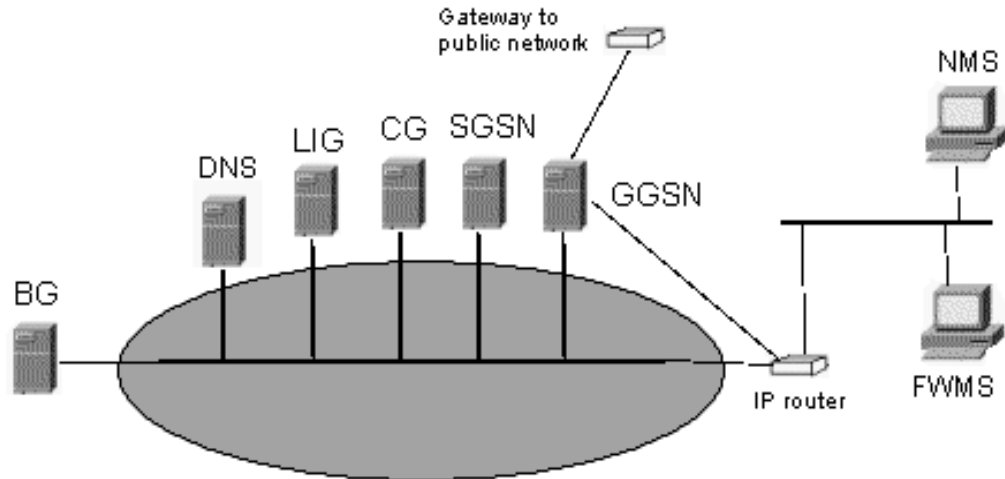
2.4. Arsitektur Jaringan GPRS Backbone

Bagian yang paling penting dari jaringan GPRS adalah SGSN dan GGSN. Walaupun dua bagian ini secara fisik bisa dijadikan dalam satu server, namun untuk menjaga keamanan dan reabilitasnya, biasanya oleh pihak operator didistribusikan dalam jaringan GPRS *backbone*. Dengan distribusi ini dalam mengimplementasikan server-server akan lebih fleksibel. Arsitektur bisa dirancang sedemikian rupa disesuaikan dengan keadaan di masa depan, misal ada penambahan server baru tidak akan merubah keseluruhan sistem.

Gambar 2.2 merupakan penjabaran dari bagian jaringan GPRS *backbone* (dalam gambar 1.1 hanya digambarkan sebagai satu blok saja). Berikut penjelasan dari blok-blok dari gambar 2.2.

CG - Charging Gateway.

Charging Gateway bertugas menghitung informasi banyaknya paket data yang lewat dan kemudian mentotal biaya pemakaian data. Total data ini dikirim ke sistem billing. Di sistem billing akan dihitung biaya pemakaian GPRS pengguna.



Gambar 2.2 Arsitektur Jaringan GPRS Backbone

BG - Border Gateway.

Border Gateway menghubungkan jaringan GPRS antar operator sehingga komunikasi data melalui operator berbeda bisa dilakukan. BG ini secara teori adalah bagian yang paling aman dan paling efisien, hal ini berguna agar transfer data antar jaringan operator yang berbeda terjadi secara cepat dan aman.

DNS - Domain Name Sever

Server yang menyediakan layanan merubah *logical name* ke alamat IP atau sebaliknya. DNS selain mengubah alamat IP untuk jaringan internet, juga mengubah alamat IP untuk jaringan lokal GPRS sendiri. Untuk jaringan lokal biasanya digunakan mengubah alamat APN ke alamat IP.

LIG - Lawful Interception Gateway

Bagian ini berguna untuk menyimpan data trafik spesifik untuk tiap-tiap pengguna. LIG berisi informasi (*log*) trafik data yang ditransfer oleh pengguna. Hal ini berguna bila ada masalah keamanan (kejahatan internet) yang dilakukan melalui jaringan GPRS. Pihak

operator bekerjasama dengan pihak berwajib bisa menganalisis log tersebut dan menentukan pengguna mana yang melakukan kejahatan lewat jaringan GPRS.

IP routers and switches

Digunakan untuk menghubungkan segmen yang berbeda dari jaringan GPRS network. Digunakan untuk level aplikasi seperti SNMP, HTTP, Telnet.

Firwall and Network Management Stations (FNMS & NMS)

Firewall digunakan untuk mencegah jaringan GPRS dari serangan dari luar.

3. Keamanan Jaringan GPRS

Dalam membahas mengenai masalah keamanan dalam suatu jaringan ada 3 topik utama yang harus diperhatikan. Topik bahasan tersebut adalah *confidentiality*, *integrity* dan *availability*.

- *Confidentiality*, berarti data-data dalam jaringan harus aman dari tangan-tangan yang tidak berhak. Untuk menjaga data agar bisa memenuhi target *confidentiality*, data sebelum ditransmisikan dalam jaringan dienkripsi terlebih dahulu.
- *Integrity*, berarti data-data yang melewati jaringan harus tetap dalam keadaan utuh dan mengandung informasi yang sesungguhnya seperti pada saat dikirimkan. Data tidak boleh rusak di tengah jalan, sehingga untuk menjaga agar data tidak hilang/rusak harus ada *error checking* terlebih dahulu, baik pada saat/setelah melakukan enkripsi data, pada saat/setelah melakukan transfer data.
- *Availability*, berarti data-data dalam jaringan harus bisa diakses oleh yang berhak tanpa tenggang waktu. Data tidak boleh terlambat atau malah tidak dapat diakses sama sekali.

Khusus untuk jaringan GPRS, dalam menjabarkan topik bahasan keamanan jaringan diatas, bisa dijabarkan dalam beberapa sub bahasan. Sub bahasan pertama adalah siapa saja yang berpotensi untuk mengacaukan masalah keamanan (penyerang), selanjutnya teknik-teknik apa saja yang bisa dilakukan penyerang untuk mengacaukan keamanan. Sub bahasan yang utama adalah bagian mana saja dalam jaringan GPRS yang berpotensi untuk dikacaukan.

3.1. Penyerang

Ada dua kategori utama yang berpotensi untuk menjadi penyerang dalam keamanan jaringan GPRS. Kategori yang pertama adalah penyerang dari luar, penyerang ini berasal dari luar operator dan dari luar pengguna jaringan GPRS. Yang termasuk dalam kategori yang pertama ini antara lain:

- *Cracker; cracker* mengarah ke penyerang yang berasal dari jaringan di luar jaringan lokal GPRS, biasanya berasal dari jaringan Internet. *Cracker* ini biasanya mempunyai tujuan untuk merusak sistem, atau hanya sekedar pamer kemampuan teknis saja. Namun tidak jarang *cracker* ini mempunyai motif ekonomi dengan mencuri data-data dari jaringan GPRS dan menjualnya ke pihak lain.
- Sub Kontraktor; sub kontraktor adalah pihak ketiga yang biasanya dikontrak oleh pihak operator untuk memasang atau mengupgrade jaringan selular. Pihak ini biasanya tidak berniat untuk melakukan untuk melakukan perusakan, namun bila pihak ini melakukan keteledoran dalam melakukan pemasangan jaringan, bisa menyebabkan masalah keamanan yang cukup fatal. Sub kontraktor bisa menjadi penyerang yang sangat potensial, mereka mempunyai akses ke jaringan dan bisa saja mengambil data-data penting dari pihak operator dan menjualnya ke operator yang lain.
- Rekanan; rekanan ini adalah pihak ketiga yang menyediakan dukungan penuh agar jaringan GPRS berjalan dengan semestinya, seperti ISP (*Internet Service Provider*). ISP menyediakan akses jaringan lokal GPRS ke jaringan internet. Sama seperti sub kontraktor, pihak rekanan biasanya tidak berniat melakukan perusakan namun karena rekanan memegang salah satu kunci jalannya jaringan GPRS, bisa saja mereka menjadi perusak yang potensial.
- Pihak Keamanan; pihak keamanan ini bisa dari pihak kepolisian atau pihak militer. Pihak keamanan ini bisa melakukan pencurian data secara diam-diam (menyadap) di jaringan GPRS dengan segala macam teknik. Pencurian ini biasanya berhubungan dengan operasi intelejen. Selain itu pihak keamanan sering melakukukan *jamming* (mengacaukan sinyal GSM), sehingga sinyal GSM dalam area tertentu sinyalnya menghilang. Aksi *jamming* ini biasanya berlangsung pada saat arak-arakan orang penting di jalan-jalan protokol dengan alasan keamanan orang penting yang sedang diarak.

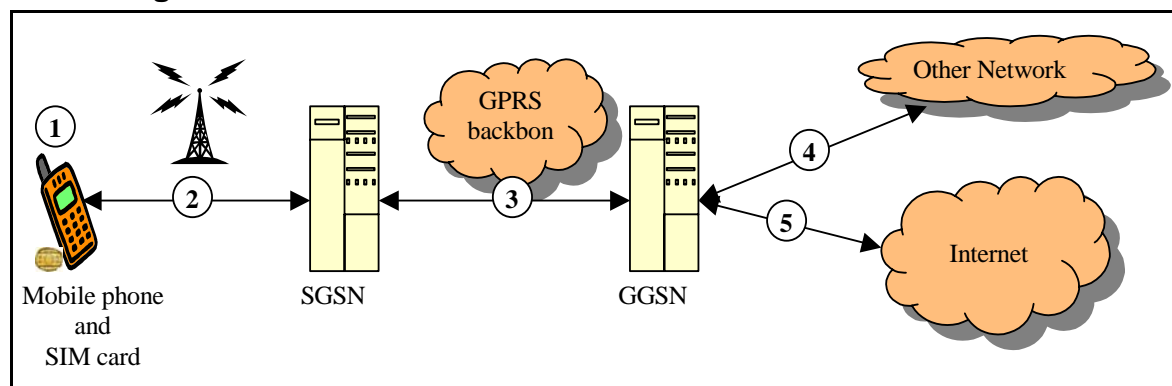
Kategori yang kedua adalah penyerang dari dalam jaringan GPRS itu sendiri. Penyerang ini bisa berasal dari sesama pengguna GPRS ataupun dari pihak operator GPRS sendiri. Dari pihak operator GPRS bisa berupa pekerja yang dengan sengaja membocorkan data-data ke pihak lain dengan motif tertentu (misalnya: ekonomi).

3.2. Teknik Penyerangan

Dari penjelesan di atas tentang pihak-pihak yang berpotensi melakukan penyerangan jaringan GPRS, dapat diperoleh sedikit informasi teknik-teknik dalam melakukan penyerangan. Teknik-teknik penyerangan ini sebenarnya bertujuan untuk menyerang salah satu atau beberapa topik bahasan keamanan yaitu *confidentiality*, *integrity* dan *availability* data. Berikut adalah beberapa teknik yang bisa dilakukan penyerang dalam jaringan GPRS:

- Pencurian; pencurian di sini yang dimaksud adalah pencurian benda secara fisik seperti pencurian telepon selular, SIM Card, PDA, PC. Pencuri bisa mengambil data-data yang ada dalam benda yang dicurinya, atau menggunakan SIM Card curian untuk mengakses jaringan GPRS sehingga tidak usah membayar tagihan.
- *Jamming*; seperti telah diterangkan di atas, *jamming* adalah aksi untuk mengacaukan sinyal GSM di suatu tempat. Dengan teknik ini sinyal GSM bisa di-*ground*-kan, sehingga sinyal GSM tidak bisa ditangkap sama sekali.
- DOS (*Denial Of Service*); teknik penyerangan ini bisa membuat jaringan GPRS tidak bisa diakses karena salah satu atau beberapa server yang diserang menjadi *crash*. Cara untuk membuat server *crash*, biasanya dengan mengirim paket yang berukuran besar dan terus menerus ke sebuah server. Karena paket yang diterima jumlahnya sangat besar, sehingga server tidak mampu melayani lagi dan akhirnya *crash*.
- *Eavesdropping*; teknik ini adalah teknik untuk menyadap aliran data dalam jaringan GPRS. Biasanya teknik ini menggunakan menggunakan program tertentu yang diletakkan di sebuah server, program tersebut dapat menyalin aliran data dan salinan tersebut dikirim ke penyerang.

3.2. Jaringan GPRS



Gambar 3.1. Masalah keamanan dalam jaringan GPRS

Masalah keamanan dalam jaringan GPRS dapat dibagi dalam 6 bagian besar:

- Keamanan yang berhubungan dengan MS (SIM Card, telepon selular, PDA, PC)
- Keamanan jaringan antara MS dan SGSN. Ini termasuk keamanan sinyal di udara ketika terjadi komunikasi antara MS dan BSS
- Keamanan jaringan GPRS *backbone*. Biasanya terjadi antara pada komunikasi antara SGSN dan GGSN.
- Keamanan antara operator jaringan operator yang berbeda.
- Keamanan antara GGSN dan jaringan luar (Internet).
- Keamanan jaringan GPRS secara umum

Keamanan di MS (*Mobile Station*)

Seperti telah dijelaskan di atas, perangkat-perangkat yang termasuk dalam MS adalah SIM Card, telepon selular, PDA, komputer/laptop (terhubung ke jaringan GPRS menggunakan GPRS modem). Di bagian ini, yang paling masalah keamanan yang paling sering muncul adalah pencurian barang secara fisik, misalnya kehilangan telepon selular, PC (*Personal Computer*). Selain pencuri bisa menggunakan SIM Card yang asli secara langsung untuk mengambil pulsanya, pencuri bisa mengkloning SIM Card. Kemudian pencuri tersebut mengembalikan SIM Card yang asli ke pemiliknya. Selanjutnya pencuri memakai SIM Card tersebut untuk melakukan koneksi GPRS secara gratis karena yang membayar tarif GPRS adalah pemilik SIM Card yang aslinya. Selain itu pencuri juga bisa mengambil data-data penting yang ada di MS.

Pengaksesan MS oleh pihak-pihak yang tidak bertanggung jawab juga sangat berbahaya. Sebagai contoh, misalnya komputer diakses oleh yang jahat, dan sengaja menjalankan trojan. Ketika komputer itu dijalankan dan terhubung ke internet lewat jaringan GPRS, trojan tersebut bisa diperintah untuk meng-*capture* segala data yang dihasilkan dan otomatis mengirimkan hasil *capture*-an ke alamat e-mail seseorang.

Keamanan antara MS dan SGSN

Dalam bagian ini data dari MS akan dibawa ke jaringan *GPRS Backbone*, melewati BSS (BTS, BSC) dan akhirnya ke SGSN. Antara MS dan BSS, data ditransmisikan lewat

gelombang radio. Di bagian inilah aksi *jamming* dilakukan. Sebenarnya kebanyakan aksi *jamming*, dilakukan untuk menjaga keamanan fisik, seperti di rumah sakit untuk menghindari interferensi peralatan kesehatan dengan sinyal telepon selular. Aksi ini mengakibatkan *availabilty* jaringan GPRS tidak bisa dipenuhi. *Jamming* akan lebih berbahaya bila dilakukan oleh orang yang tidak bertanggung jawab (misal: teroris), yang dengan aksinya mengakibatkan jaringan GPRS di satu kota lumpuh (dalam rangka melancarkan aksi terornya).

Di BSS, penyerang bisa menyadap aliran data yang lewat sebelum akhirnya dikirimkan ke SGSN. Penyerang akan lebih mudah melakukan *eavesdropping*, bila mempunyai akses ke BSS, misal subkontraktor atau malah pegawai operator selular tersebut.

Keamanan jaringan GPRS *backbone*

GPRS *backbone* adalah server-server yang terletak di antara SGSN dan GGSN (bab 2.4). Teknik penyerangan yang bisa dilakukan adalah *eavesdropping* di setiap server. Penyadapan paling memungkinkan dilakukan di LIG, yang memang server tersebut menyimpan semua data yang lewat di jaringan GPRS.

Pengubahan data yang paling memungkinkan adalah di CG, yang bertugas untuk menghitung billing tarif GPRS. Dengan motif ekonomi, seseorang bisa mengubah data billing atau mengubah program billing sehingga khusus untuk koneksi GPRS dari orang tersebut, penghitungan tarifnya berubah.

Jaringan GPRS *backbone*, adalah jaringan IP *based* sehingga sangat rentan terhadap serangan DOS (*Denial Of Service*), baik serangan dari jaringan internet atau dari jaringan internal. Serangan DOS dari jaringan internet biasanya susah untuk dilakukan, karena ada *firewall* di antara jaringan lokal GPRS dengan jaringan internet. Yang paling memungkinkan adalah serangan DOS dari jaringan internal sendiri, bisa dari salah satu atau lebih komputer yang tersambung ke jaringan GPRS *backbone*.

Keamanan antara jaringan operator yang berbeda

Di bagian ini server yang paling berperan adalah BG (*Border Gateway*), server ini menjadi perantara antara dua operator. Di BG ini terdapat *firewall* yang menjaga keamanan agar jaringan lokal operator yang satu tidak dapat mengakses jaringan yang tidak berhak. Bila *firewall* ini bisa ditembus, pihak yang tidak berhak dari operator yang lain bisa mendapat akses ke operator yang terhubung.

BG juga sangat rentan terhadap *eavesdropping*, dengan memasang program tertentu pemasang bisa menyadap alur data yang lewat antar operator. Perbedaan QoS (*Quality of Service*) pada jaringan tiap operator juga bisa mengakibatkan tingkat *availabilty*-nya menurun. Bila salah satu jaringan ada yang lebih lambat *transfer rate*-nya maka *transfer rate* total antar jaringan akan mengikuti yang lebih lambat.

Keamanan jaringan antara GGSN dan jaringan internet

Penyerang utama yang ada di bagian ini adalah pihak-pihak yang ada di internet. Dari jaringan internet penyerang dapat dengan mudah melumpuhkan GGSN dengan *distributed DOS*. TeknikDOS ini menggunakan banyak komputer yang telah diatur sedemikian rupa sehingga mengirim trafik ke GGSN secara bersamaan dan dalam jumlah yang besar.

Biasanya untuk mencegah masuknya penyerang ke jaringan lokal GPRS, antara GGSN dan jaringan internet ada *firewall*. Namun firewall kurang baik atau penyerang dari internet bisa melakukan serangan ke dalam jaringan lokal GPRS dengan mudah.

Keamanan jaringan GPRS secara umum

Yang dimaksud kewanaman jaringan secara umum di sini adalah masalah keamanan dari jaringan GPRS dipandang secara menyeluruh tidak per bagian-bagian. Sebagai contoh, penyerang dari dalam jaringan GPRS (*subscriber*), akan susah dilacak keberadaannya. Walaupun data-data MS (nomor IMEI, data SIM Card) telah dicatat, penyerang dapat dengan mudah mengganti MS. Selain itu penyerang dapat dengan mudah berpindah-pindah tempat.

Ada teknik lain yang bisa merugikan pihak yang diserang. Pihak yang diserang akan membayar tagihan internet dari traffic yang tidak dipakainya. Teknik ini bisa dilakukan oleh subscriber lain dengan melakukan *ping* ke alamat IP pihak yang diserang. Pihak yang diserang akan me-*replay ping* tersebut dan akan terkena biaya penggunaan traffic. Untuk mendapatkan alamat IP tersebut penyerang bisa melakukan *mass scanning* pada alamat-alamat IP yang diperkirakan dipakai oleh pengguna lain.

Pengguna akan dianggap sebagai satu LAN (*Local Area Network*) oleh pengguna lain. Hal ini akan berbahaya bila antar pengguna tidak ada *firewall* yang menghalangi koneksi langsung antar pengguna. Virus semacam virus sasser (menyebarkan lewat lubang keamanan sistem operasi), bisa saja menyebar ke pengguna lain. Atau dengan teknik mirip virus ini, pengguna lain bisa mengontrol komputer korban selama korban terkoneksi ke jaringan GPRS.

Program-program yang didownload dari internet bisa membahayakan subscriber bila program tersebut telah disusupi kode-kode virus atau trojan. Virus atau trojan juga dikirimkan lewat e-mail, bila *subscriber* membuka e-mail tersebut, virus bisa otomatis berjalan.

4. Mengamankan Jaringan GPRS

Mengamankan jaringan GPRS di sini, lebih diarahkan pada teknik-teknik pencegahan serangan masalah. Bahasan berikut adalah beberapa teknik yang biasa dilakukan oleh operator jaringan GPRS untuk mengamankan jaringan GPRS.

4.1. Keamanan MS

Keamanan MS di sini tentu saja adalah tanggung jawab pengguna jaringan GPRS. Pengguna harus bisa menjaga barang-barang miliknya agar tidak dicuri orang atau dipakai oleh orang yang tidak berhak. Pengguna wajib menjaga agar komputer yang terhubung jaringan GPRS tidak terkena virus atau trojan akibat mendownload e-mail atau mendownload program bervirus. Cara untuk mencegah agar tidak terkena virus/trojan, dengan rajin mengupdate data anti virus terbaru.

Khusus untuk keamanan data SIM Card, operator juga punya tanggung jawab besar. SIM Card harus dienkripsi sedemikian rupa agar susah untuk diduplikat (*clone*).

4.2. Keamanan Fisik Jaringan GPRS

Keamanan fisik di sini adalah keamanan hardware-hardware yang terhubung ke jaringan GPRS, misalnya BTS dan server-server. Keamanan fisik di sini seharusnya merupakan tanggung jawab operator. Ruangan yang berisi server-server penting harus dijaga dan dipastikan menyala selama 24 jam setiap harinya serta hanya orang yang berhak saja yang boleh memasukinya.

4.3. Firewall

Firewall bisa berupa software atau hardware yang akan menjaga lalu lintas data dan memastikan data tersebut aman untuk dilewatkan. *Firewall* berisi set-set aturan yang menentukan suatu data boleh lewat atau tidak. Sebagai contoh misalnya traffic dari jaringan

luar (internet) yang tidak sesuai aturan tidak boleh melewati jaringan jaringan lokal GPRS. Firewall ini diletakkan di antara GGSN dan Internet.

Firewall juga diletakkan di BG yang menghubungkan antara dua jaringan operator. *Firewall* ini digunakan untuk melindungi jaringan GPRS, dari *traffic* yang bisa membahayakan salah satu atau kedua jaringan. Selain itu *firewall* digunakan untuk mencegah pengaksesan komputer subscriber yang satu dengan yang lain. *Traffic* dari pengguna yang satu yang diarahkan ke pengguna yang lain akan dimatikan oleh *firewall*.

4.4. Virtual Private Network (VPN)

VPN adalah suatu teknik untuk membuat jalur komunikasi lebih aman dan privasi terjaga. Dengan adanya VPN ini jaringan akan seperti jaringan *private*, walaupun jalur yang dipakai untuk koneksi adalah jaringan *public* (internet). Data yang lewat jaringan VPN pertama kali dienkripsi terlebih dahulu baru kemudian didekripsi pada sisi penerima.

Pada jaringan GPRS VPN digunakan untuk mengamankan data dari MS ke jaringan GPRS. Dengan adanya VPN data dari/ke MS akan lebih aman karena selama transfer, data selalu dalam keadaan terenkripsi. Selain itu VPN digunakan antara GGSN dan *Corporate IP Network*.

5. Studi Kasus

Pada tulisan ini studi kasus dilakukan untuk mengetest apakah jaringan GPRS yang ada sudah benar-benar aman. Studi kasus ini selain berupa studi literatur juga melakukan uji coba. Jaringan GPRS yang akan diujicoba adalah jaringan GPRS IM3 Smart, dengan alasan tarif GPRS-nya paling murah dibanding kartu prabayar lain, sehingga dalam melakukan percobaan tidak banyak memakan biaya. Studi kasus ini dilakukan dengan metode yang aman, artinya tidak membahayakan pihak lain baik itu pengguna lain atau operator sendiri. Penulis tidak akan melakukan *scanning* terhadap server-server milik operator atau hal-hal yang akan merusak server operator.

5.1. SIM Card Clone

SIM Card Clone adalah bagian dari masalah keamanan di MS. Beberapa *authentication algorithm* (misal: COMP128-1) SIM Card GSM bisa ditembus dengan alat tertentu sehingga seluruh data dalam SIM Card bisa dipindahkan ke SIM Card lain. Di sini penulis tidak mencoba apakah SIM Card IM3 Smart bisa di-*clone* atau tidak. Penulis melakukan studi kasus dari pengalaman seseorang. Penulis memperoleh informasi dari sebuah forum (<http://www.forumponsel.com>), ada orang yang berhasil men-*clone* SIM Card IM3 Smart walaupun memakan waktu relatif lebih lama dibanding men-*clone* SIM Card yang lainnya. Orang tersebut mampu membuat duplikat SIM Card IM3 Smart dengan SIM Master 4 (Gambar 5.1).



Gambar 5.1. SIM Master 4

SIM Master 4 mempunyai modul SIM Card sendiri yang diberi nama SIM Magics, yang mampu menyimpan 8 buah SIM Card sekaligus. Menurut salah satu pengunjung forum yang mengaku penjual alat ini, mereka menjual seharga Rp 475.000,- dan berani memberi garansi bahwa semua SIM Card GSM di Indonesia mampu diclone.

Dengan alat ini seseorang dapat dengan mudah menduplikat SIM Card. Sangat berbahaya, bila alat ini jatuh ke tangan orang yang jahat. Orang itu bisa menduplikat SIM Card curian dan mempergunakannya untuk kepentingan dirinya sendiri (misal: menghabiskan pulsanya) atau malah menjual SIM Card duplikatnya.

5.2. GSM Jamming

Seperti telah dijelaskan di atas, jaringan GPRS merupakan bagian dari jaringan GSM. Jadi bila terjadi aksi GSM *Jamming* di suatu tempat maka otomatis jaringan GPRS di tempat itu tidak berfungsi. Penulis tidak mencoba apakah *jamming* bisa berhasil untuk jaringan GSM IM3 Smart, namun penulis berhasil menemukan bahwa alat ini bisa dibeli secara bebas. Hal ini tentu saja sangat berbahaya tentunya bila dipakai orang jahat yang sengaja mematikan jaringan GSM di suatu daerah tertentu.

Dari sebuah situs penjual GSM *Jammer* dari Israel (<http://www.netline.co.il>), diperoleh informasi bahwa ada beberapa tipe GSM *Jammer*, dari yang ukuran fisiknya sebesar PDA, sampai ke yang ukurannya sebesar kardus *Indomie* yang jangkauannya sampai beberapa kilometer. Berikut gambar diperoleh penulis untuk *jammer*, yang paling kuat daya jangkauannya yang diproduksi perusahaan tersebut.



Gambar 5.2. C-Guard VHP: Very High Power Cell Phone Jammer

C-Guard VHP adalah *jammer* dengan daya yang kuat. Daya jangkauannya mencapai 3 km. Mampu menjamming seluruh *frekuensi band* dari GSM (900/1800/1900 Mhz). Karena jaringan GSM IM3 Smart termasuk dalam frekuensi 1800 Mhz, maka dengan alat ini dimungkinkan jaringan GSM IM3 Smart untuk terkena *jamming*.

5.3. Ujicoba Keamanan Jaringan GPRS

Pada ujicoba jaringan GPRS kali ini penulis, hanya ingin melihat apakah *firewall* di jaringan GPRS IM3 Smart berjalan baik atau tidak. Yang akan diujicoba adalah *firewall* antara GGSN dengan jaringan Internet, dan *firewall* antar *subscriber*. Dua bahasan ini yang paling memungkinkan untuk dicoba tanpa menimbulkan kerugian pihak lain.

Setting GPRS yang dipergunakan adalah setting standard untuk koneksi GPRS lewat IM3 Smart. Setting koneksi untuk MS adalah:

- APN : www.indosat-m3.net
- Username : gprs
- Password : im3

Firewall antara GGSN dengan jaringan internet

Setelah terkoneksi ke jaringan GPRS, MS mendapat alamat IP dynamic 10.18.5.26. Di sini terlihat bahwa alamat IP yang diperoleh adalah alamat IP internal jaringan GPRS. Cara untuk memastikan apakah terdapat firewall di antara GGSN dan jaringan internet, yaitu dengan melihat alamat IP apa yang dipakai ketika sedang browsing di internet. Dengan menggunakan *tool* untuk melihat informasi alamat IP di internet, diperoleh informasi sebagai berikut: "Your IP : 202.155.46.5".

Dari data di atas, diperoleh informasi bahwa koneksi GPRS ke internet akan dikenali sebagai 202.155.46.5. Jaringan internet di luar tidak bisa mengenali alamat IP internal yang dipakai untuk melakukan koneksi. Di sini terlihat bahwa *firewall* antara GGSN dan jaringan internet berjalan dengan baik.

Firewall antar subscriber

Untuk mengujicoba hal ini diperlukan dua MS yang kedua-duanya terhubung secara bersamaan ke jaringan GPRS. Untuk MS yang baru diperoleh alamat IP internal 10.18.1.8 (sistem operasi yang dipakai kedua MS adalah Microsoft Windows). Dalam ujicoba ini,

seharusnya traffic yang ditujukan ke MS lain tidak boleh lewat, *firewall* akan men-*drop* traffic yang lewat.

Tahap pertama, diujicoba apakah mengirim traffic lewat perintah ping ke MS lain bisa atau tidak. Dari MS yang bernomor IP 10.18.1.8, dengan menggunakan perintah: “`ping -t 10.18.5.26`”, dicoba untuk mengirim paket data ke 10.18.5.26. Agar terlihat jelas perbedaan antara traffic sebelum ada *ping* dan sesudah *ping*, MS dengan alamat IP 10.18.5.26, dibiarkan dalam keadaan *idle*. Hasil dari percobaan ini, MS yang tadinya *idle* merespon *ping* tersebut, dan akhirnya terjadi lonjakan *traffic* di 10.18.5.26 padahal tidak ada aktivitas apapun.

Percobaan di atas menghasilkan informasi bahwa terdapat lobang keamanan yang bisa dieksploitasi subscriber lain, yaitu bisa mengirimkan *traffic* ke MS lain yang sedang terhubung ke jaringan GPRS. Penyerang bisa melakukan scanning alamat IP mana saja yang sedang online dengan cara mem-*ping range* IP dynamic yang disediakan bagi *subscriber*. Kemudian penyerang bisa mengirimkan paket-paket yang besar ke MS yang ditemuinya. Hal ini bisa membuat MS lain menjadi crash, atau paling tidak akan membayar biaya data dari paket yang tidak perlu (*note*: billing GPRS dihitung berdasar banyaknya traffic yang dikirim/diterima).

Percobaan selanjutnya apakah mengakses port-port tertentu dari MS lain bisa atau tidak. Dalam percobaan ini, penulis membuka port 80 (http) untuk MS di alamat IP 10.18.5.26. Selanjutnya lewat web browser, dari MS dengan alamat IP 10.18.1.8 dibuka <http://10.18.5.26>. Hasil dari percobaan ini, *web server* dari 10.18.5.26 bisa diakses dari 10.18.1.8.

Dari percobaan di atas menunjukkan kemungkinan besar tidak ada *firewall* yang menghalangi *traffic* antar subscriber. Kalau hal ini benar penyerang bisa melakukan *scanning port* pada MS yang ditemuinya, dan bila menemukan port yang lemah dapat dengan mudah mengeksploitasinya. Selain itu penyerang bisa memanfaatkan lubang keamanan sistem operasi MS, dengan mengirimkan virus sejenis virus Sasser. Penyerang bisa mengubah kode virus Sasser agar bekerja hanya di jaringan GPRS saja, misal dengan mengeset agar melakukan otomatis scanning pada jaringan internal GPRS saja. Mirip dengan virus Sasser yang asli, setelah ditemui sistem operasi yang berlobang, virus ini akan mengeksploitasi MS yang diserangnya dan menyuruh untuk melakukan download dan menjalankan program tertentu dari internet. Dengan begitu MS yang baru akan terjangkit virus tersebut dan melakukan penyebaran ke MS yang lainnya.

6. Kesimpulan

GPRS merupakan teknologi 2.5 G yang kecepatan transfer datanya tergolong tinggi. Jaringan GPRS dibuat untuk memperbaiki kecepatan transfer data dari jaringan GSM. Jaringan GPRS namun merupakan bagian dari jaringan GSM. Bila jaringan GSM tidak berfungsi maka otomatis jaringan GPRS juga tidak bisa berfungsi.

Dalam jaringan GPRS terdapat dua kategori utama yang berpotensi menjadi penyerang. Selain penyerang dari dalam jaringan (*subscriber* lain, pegawai operator), orang di luar operator juga berpotensi, misalnya pihak ketiga yang melaksanakan *upgrade* jaringan.

Ada beberapa teknik yang bisa digunakan untuk menyerang jaringan GPRS. Teknik-teknik ini antara lain DOS, *eavesdropping*, *jamming*, dan pencurian. Teknik-teknik tersebut bisa dilakukan di beberapa bagian jaringan GPRS.

Menjaga keamanan jaringan GPRS bukan semata-mata tanggung jawab pihak operator saja, pengguna juga wajib menjaga keamanan data-datanya sendiri yaitu dengan cara menjaga MS agar tidak dicuri orang atau tidak digunakan oleh orang yang tidak berhak.

Jaringan GPRS IM3 Smart memiliki kelemahan pada sistem *firewall* antar *subscriber*. *Firewall* tersebut tidak berjalan dengan baik atau malah tidak ada sama sekali. Pengguna lain dapat mengirim paket data ke *subscriber* lain yang sedang online lewat jaringan GPRS. Pengguna lain yang mendapatkan paket data tersebut akan membayar data-data yang tidak perlu.

Jaringan GPRS IM3 Smart tidak mem~~firewall~~ akses port ke MS pengguna lain. Hal ini bisa sangat berbahaya bila MS yang diakses mempunyai kelemahan (misal, terdapat lubang keamanan di sistem operasi). Penyerang bisa mengeksploitasi MS tersebut sehingga merugikan pihak lain.

Daftar Pustaka

Geir Stian Bjåen & Erling Kaasin, "Security in GPRS", Master Thesis in Information and Communication Technology, May 2001, <http://siving.hia.no/ikt01/ikt6400/ekaasin/Master%20Thesis%20Web.htm>

Hadi Jayani, "Pengalaman Cloning Kartu SIM GSM", Desember 2003, http://www.interdimension.org/sim_card_cloning/

Jussi Rautpalo, "GPRS Security - Secure Remote Connections over GPRS", Helsinki University of Technology, http://www.hut.fi/~jrautpal/gprs/gprs_sec.html

Netline.co.il, "Cell Phone Jammer by Netline Communication Technologies", <http://www.netline.co.il>

RFC 2002 - IP Mobility Support, rfc2002.txt

SourceO2.com, "GPRS", http://www.sourceo2.com/O2_Developers/O2_technologies/GPRS/default.htm

Sunomo, "GPRS: Komunikasi Data Melalui Jaringan Komunikasi Bergerak", Oktober 2000, <http://www.elektroindonesia.com/elektro/tel33a.html>