GSM Security

Ratih Hardiantina[1] , Siti Awaliyah[2], dan Sandra Syafwin[3]

Departemen Teknik Informatika
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung 40132

E-mail : if12045@students.if.itb.ac.id[1], if12051@students.if.itb.ac.id[2], if12075@students.if.itb.ac.id[3]

Abstrak

Artikel ini menjelaskan mengenai mekanisme pengamanan jaringan GSM. Mencakup prosedur – prosedur yang dilakukan untuk pengamanan komunikasi menggunakan jaringan GSM, beserta algoritma yang diterapkan untuk masing – masing prosedur yaitu algoritma A3, A5, dan A8. Ada beberapa prosedur yang dilakukan dalam pengamanan GSM, mulai dari otentikasi *Personal Identification Number* (PIN), otentikasi *Mobile Station* oleh jaringan, hingga pembangkitan kunci untuk mengenkripsi data yang ditransmisikan melalui jaringan GSM. Selain itu, dibahas pula mengenai contoh serangan yang mungkin dilakukan terhadap komunikasi GSM serta saran pengembangan sebagai solusi atas kelemahan – kelemahan yang dimiliki oleh mekanisme pengamanan jaringan GSM yang digunakan saat ini.

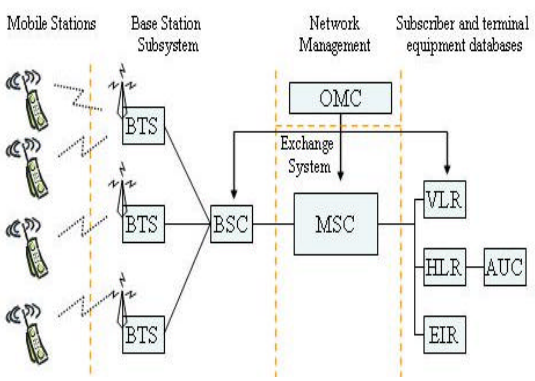
***Kata kunci**: GSM, otentikasi, serangan, algoritma A3, A5, dan A8*

1. Pendahuluan

Mobile phone digunakan oleh banyak user melalui *radio link*. Dengan *radio link*, siapapun dapat memantau *airwave* secara pasif. Oleh karena itu, sangat diperlukan teknologi pengamanan untuk memastikan kerahasiaan *phone call* user dan teks pesan (data) untuk mencegah penggunaan layanan GSM yang ilegal. Layanan yang disediakan oleh GSM adalah komunikasi suara, *Short Messaging Service (SMS)*, penungguan panggilan (*call waiting)*, pengalihan panggilan (*call forwarding)*, pemberian identitas saluran panggilan (*calling line identity)*, *circuit-switched data (packet-switched data with GPRS)* [4].

2. Pengamanan untuk GSM

Arsitektur GSM dapat dilihat pada ilustrasi gambar di bawah ini .



Gambar 1 Arsitektur GSM

Dari gambar di atas, dapat dilihat bahwa dalam berkomunikasi, telepon seluler, *mobile station* (MS), memanfaatkan layanan jaringan melalui *base station subsystem* yang terdiri dari beberapa *base*

transceiver station (BTS) dan sebuah *base station controller* (BSC) [5].

BSC akan terhubung dalam manajemen jaringan operator GSM.

Subsistem jaringan memanfaatkan basis data berikut untuk keperluan otentikasi dan keamanan [4]:

1) *Home Location Register* (HLR), basis data yang menyimpan seluruh informasi administratif dari tiap pelanggan jaringan GSM yang terdaftar, lengkap dengan lokasi terkini (*current location*) dari MS.
2) *Visitor Location Register* (VLR), melacak MS yang berada di luar *home network*, sehingga jaringan dapat dengan mudah mendeteksi keberadaan MS tersebut.
3) *Equipment Identity Register* (EIR), berisi daftar *International Mobile Equipment Identity* (IMEI) yang dibolehkan untuk menggunakan layanan jaringan.
4) *Authentication Center* (AuC), basis data yang berisi: *International Mobile Subscriber Identity* (IMSI), *Temporary Mobile Subscriber Identity* (TMSI), *Location Area Identity* (LAI), *dan Authentication Key* (Ki).

Ada beberapa cara yang dipakai dalam upaya melakukan pengamanan komunikasi jaringan GSM, yaitu :

a. *Personal Identification Number* (PIN) pada MS.
b. Otentikasi pengguna layanan.
c. Enkripsi pada GSM.
d. Penggunaan TMSI

***Personal Identification Number* (PIN) pada MS**.

Subscriber Identity Module (SIM) adalah sebuah *smartcard* yang dimasukkan ke dalam posel GSM. SIM memiliki nilai IMSI dan Ki, dimana IMSI adalah nilai unik untuk masing-masing *subscriber* di seluruh dunia dan Ki adalah kunci otentikasi 128-bit yang dibangkitkan secara acak.

Penggunaan kode PIN bertujuan untuk melindungi mengotentikasi SIM. PIN disimpan pada kartu SIM. Otentikasi dilakukan secara lokal, tanpa melibatkan jaringan.

Dilakukan dengan meminta PIN setiap kali MS dihidupkan. Jika pengguna melakukan tiga kali kesalahan ketika memasukkan PIN, maka pengguna akan diminta untuk memasukkan kode yang lebih panjang, yaitu *Personal Unblocking Key* (PUK).

Jika pengguna melakukan sepuluh kali kesalahan saat memasukkan PUK, maka SIM akan dikunci, dan pengguna harus meminta SIM yang baru dari operator jaringan GSM.

Otentikasi pengguna layanan.

Otentikasi pengguna dibutuhkan untuk mencegah pengguna yang tidak berhak memasuki jaringan dan mengklaim bahwa ia adalah *subscriber*. Jika hal ini terjadi, maka dengan mudahnya ada kemungkinan untuk membajak *account* seseorang dan berkedok seolah-olah ia adalah *account* tersebut.

Otentikasi pengguna dilakukan agar hanya pengguna yang terdaftar dan berhak saja yang dapat menggunakan layanan operator jaringan. Selain itu, digunakan agar tagihan dikenakan pada pengguna yang tepat, yang memang memanfaatkan layanan jaringan.

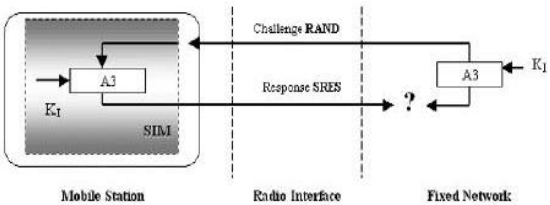
Algoritma yang digunakan dalam proses otentikasi pengguna layanan pada jaringan

GSM adalah algoritma A3. Algoritma ini tidak bersifat publik sehingga hanya antarmuka eksternalnya saja yang dispesifikasikan dalam GSM. Keamanan algoritma ini tergantung pada kunci rahasia *user Ki* yang beririsan antara *mobile phone* dan jaringan GSM. GSM sendiri tidak menspesifikasikan panjang nilai *Ki* sehingga penentuan panjang nilai *Ki* biasanya diserahkan sepenuhnya kepada pihak operator masing-masing. Namun, biasanya panjang kunci yang biasa digunakan oleh operator adalah 128 bit.

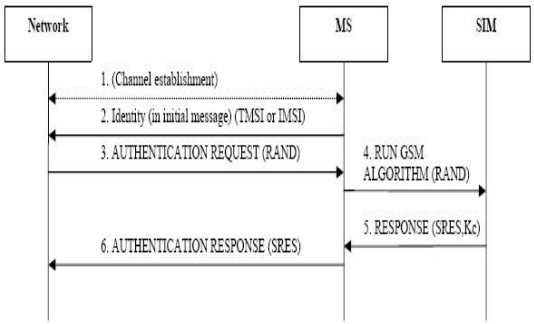
Adapun proses otentikasi pengguna menggunakan algoritma A3 adalah sebagai berikut :

i. Jaringan mengirim tantangan acak (RAND) kepada MS.
ii. MS melakukan enkripsi terhadap RAND dengan algoritma A3 dan kunci Ki, menghasilkan respon SRES. Proses ini dilakukan pula oleh jaringan.
iii. MS mengirim SRES kepada jaringan.
iv. Jaringan membandingkan SRES yang dihasilkannya dengan SRES yang diterima. Jika cocok, otentikasi berhasil.

Skema otentikasi pengguna dapat dilihat pada gambar di bawah.



Gambar 2 Skema Proses Otentikasi Pengguna



Gambar 3 Diagram Sekuens Otentikasi Pengguna

Dapat dilihat bahwa tidak ada pengiriman Ki karena mensubmit Ki ke jaringan tidaklah aman.Karena hal itulah proses otentikasi tidak dilakukan dengan membandingkan nilai Ki di SIM dan Auc, tapi dengan prosedur otentikasi yang telah dijelaskan.

Jika otentikasi gagal untuk pertama kalinya dan TMSI telah digunakan, maka jaringan akan memilih untuk kembali mengulangi proses otentikasi menggunakan IMSI.

Enkripsi pada GSM.

Selama terjadi komunikasi pada jaringan, semua data pengguna (seperti pesan teks dan panggilan) yang dipertukarkan melalui media udara dienkripsi terlebih dahulu untuk menjaga kerahasiaannya [2].

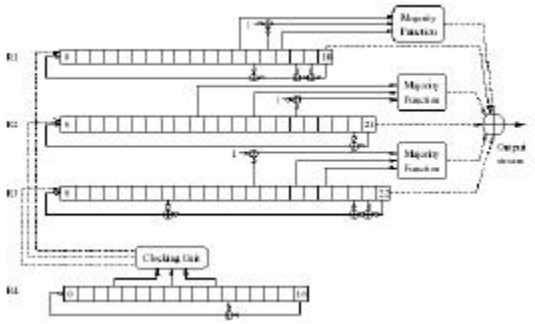
Sistem GSM menggunakan kriptografi simetri karena menggunakan sebuah kunci privat, yaitu Kc. Kunci Kc digunakan untuk enkripsi dan juga dekripsi. Kunci Kc ini hanya boleh diketahui oleh ponsel dan jaringan.

Algoritma yang digunakan untuk proses enkripsi ketika komunikasi data berlangsung adalah algoritma A5. Tidak seperti A3, deskripsi algoritma A5 ini merupakan bagian

dari GSM walaupun algoritma A5 sendiri tidak pernah dibuat publik.

Ada dua versi algoritma A5 yang sering digunakan dalam GSM, yakni A5/1 dan A5/2 yang merupakan stream cheaper. Selain itu, ada tambahan versi baru yang telah distandardisasikan tetapi belum digunakan di jaringan GSM yaitu algoritma A5/3. Algoritma ini didasarkan pada *block-cipher* pada algoritma KASUMI [2,3]. Algoritma A5/1 dan A5/2 merupakan algoritma pertama yang ditentukan standarnya oleh GSM dan dirancang berdasarkan sistem kontrol *clocking* LFSRs yang sederhana [3].

Algoritma A5/2 terdiri dari empat LFSR (Linear Feedback Shift Register) dengan panjang maksimum yakni : R1, R2, R3, dan R4. Register-register tersebut memiliki panjang 19 bit, 22 bit, 23 bit, dan 17 bit. Setiap register memiliki *tap* dan fungsi *feedback* dan untuk ploynomial tiap-tiap register adalah $x^{19} \oplus x^5 \oplus x^2 \oplus x \oplus 1$, $x^{22} \oplus x \oplus 1$, $x^{23} \oplus x^{15} \oplus x^2 \oplus x \oplus 1$, dan $x^{17} \oplus x^5 \oplus 1$. Untuk representasi register-register tersebut digunakan notasi [2, 4, 5, 17] dimana bit-bit dalam register yang terurut secara terbalik berkorespondensi dengan sebuah *tap* dengan indeks *len-i*-1, dimana *len* adalah ukuran register. Contoh: ketika R4 dikunci berdasarkan mekanisme penguncian (*clocking*), nilai XOR R4[17-0-1=16] dan R4[17-5-1=11] dihitung, baru kemudian registernya digeser satu bit ke kanan dan nilai hasil XOR tersebut ditempatkan di R4[0].



Gambar 4 Ilustrasi Algoritma A5/2

Pada algoritma A5/2, R1, R2, dan R3 dikunci dilakukan berdasarkan mekanisme penguncian (*clocking*) dengan aturan seperti yang dijelaskan pada gambar yakni R4 mengontrol penguncian (*clocking*) R1, R2, dan R3. Ketika penguncia terhadap R1, R2, danR3 dilakukan, bit-bit R4[3], R4[7], dan R4[10] merupakan input dari unit penguncian. Unit pengujian ini melakukan sebuah fungsi mayoritas pada bit-bit yang ada. R1 dikunci jika dan hanya jika R4[10] sesuai dengan mayoritas. R2 dikunci jika dan hanya jika R4[3] sesuai dengan mayoritas. R3 dikunsi jika dan hanya jika R4[7] sesuai dengan mayoritas. Setelah penguncian-penguncian terhadap register R1, R2, dan R3 dilakukan, baru kemudian R4 dikunci.

Setelah proses penguncian dilakukan, satu bit output sudah siap untuk dihasilkan pada A5/2. bit output merupakan fungsi non-linier dari status internal R1, R2, dan R3. setelah dilakukan inisialisasi 99 bit output dibuang dan 228 bit berikutnya digunakan sebagai *output key-stream.* Adapun proses inisialisasi status internal dilakukan sebagai berikut:

- ubah nilai seluruh LFSRs dengan nilai 0
- for 1:=0 to 63 do
  1. kunci seluruh LFSR
  2. $R1[0] \neg R1[0] \oplus Kc[i]$
  3. $R2[0] \neg R2[0] \oplus Kc[i]$
  4. $R3[0] \neg R3[0] \oplus Kc[i]$

5. $R4[0] \neg R4[0] \oplus Kc[i]$

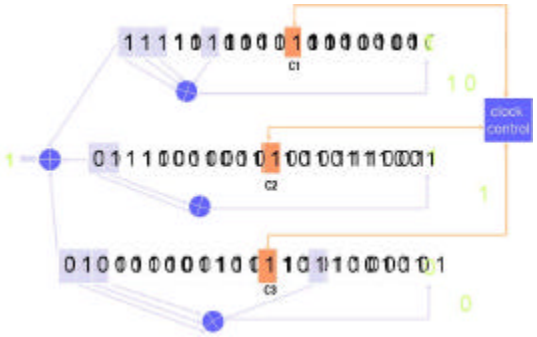
- for i:=0 to 21 do
  1. kunci seluruh LFSR
  2. $R1[0] \neg R1[0] \oplus f[i]$
  3. $R2[0] \neg R2[0] \oplus f[i]$
  4. $R3[0] \neg R3[0] \oplus f[i]$
  5. $R4[0] \neg R4[0] \oplus f[i]$

Dimana nilai *i* menunjukkan bit ke-*i* dari *session key Kc*[i] dengan panjang 64 bit, bit ke-*i* dari register dari register *Rj*[*i*], dan bit ke-*i* dari jumlah *frame* yang bersifat publik *f*[*i*].

Sedangkan proses pembangkitan *key-stream* adalah:

1. inisialisasi status internal dengan nilai *Kc* dan jumlah *frame*
2. Isikan nilai bit-bit R1[15], R2[16], R3[8], dan R4[10] dengan 1
3. jalankan algoritma A5/2 untuk 99 *clocks* dan abaikan outputnya
4. Jalankan algoritma A5/2 untuk 228 *clocks* berikutnya dan gunakan aoutputnya sebagai *key-stream*

Pada dasarnya algoritma A5/2 dibangun dengan kerangka yang sama dengan A5/1. Fungsi-fungsi *feedback* untuk register R1, R2, dan R3 pada A5/2 sama dengan fungsi *feedback* pada A5/1, begitu pula halnya dengan proses inisialisasi yang dilakukan A5/1 dan A5/2 serupa. Yang membedakan algoritma A5/1 dan A5/2 adalah A5/1 hanya terdiri dari tiga LFSR dengan panjang maksimum masing-masing R1, R2, R3 adalah 19 bit, 22 bit, dan 23 bit sehingga tidak ada pendefinisian untuk register R4 sehingga A5/2 juga harus melakukan inisialisasi R4 dan nilai satu bit pada tiap register harus diisikan dengan nilai 1 setelah dilakukan inisialisasi. Selain itu A5/2 membuang 99 bit output sementara A5/1 membuang 100 bit aoutput. Untuk lebih jelasnya, struktur internal algopritma A5/1 digambarkan melalui gambar berikut :



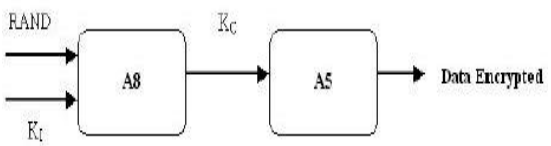
Gambar 5 Ilustrasi Algoritma A5/1

Namun, baik A5/1 maupun A5/2 telah berhasil dipecahkan oleh beberapa kriptanalis di dunia dengan menggunakan serangan yang dikenal sebagai *plaintext attack*.

Mekanisme enkripsi data adalah sebagai berikut [4]:

i. Memproses RAND, yang diterima pada saat akan melakukan otentikasi pengguna, dengan algoritma A8 dan Ki untuk menghasilkan kunci enkripsi Kc (*ciphering key*).
ii. Mengenkripsi *plaintext* dengan algoritma A5 dan kunci Kc untuk menghasilkan *ciphertext*, yang akan ditransmisikan melalui jaringan.

Skema untuk enkripsi dapat dilihat pada gambar berikut :



Gambar 6 Skema Enkripsi dalam GSM

Ketika algoritma A3 dijalankan pada proses otentikasi pengguna, sebenarnya pada saat yang sama algoritma A8 juga dijalankan.

Kc dibangkitkan pada saat dilakukan otentikasi pengguna. Untuk setiap panggilan, Kc yang dibangkitkan akan berbeda nilainya.

Kc hasil proses algoritma A8 disimpan ke dalam SIM dan terbaca oleh ponsel. Jaringan juga membangkitkan Kc dan mendistribusikannya kepada *base station*(BTS) yang menangani koneksi.

Penggunaan TMSI.
Selain kerahasiaan data, juga diperlukan kerahasiaan pengguna. Ketika jaringan mengalamatkan ke *subscriber* tertentu, atau selama proses otentikasi, nilai IMSI yang unik sebaiknya tidak diperlihatkan dalam bentuk plainteks sehingga seseorang yang melintas dalam komunikasi tidak dapat mengetahui keberadaan pengguna tertentu dalam area tertentu.

Karena IMSI bernilai unik, maka digunakan TMSI untuk mencegah pihak penyadap mengetahui identitas serta lokasi pengguna layanan yang sedang disadapnya. IMSI hanya dikirim jika diperlukan, misalnya pada saat SIM digunakan untuk pertama kali, serta jika terjadi kehilangan data di VLR.

TMSI ditentukan nilainya pada saat IMSI ditransmisikan ke AuC, yaitu saat SIM diaktifkan untuk pertama kalinya. TMSI digunakan oleh MS untuk melapor kepada jaringan atau pada saat inisialisasi panggilan.

Pada saat MS dimatikan, TMSI disimpan pada SIM untuk dipakai kembali pada waktu mendatang. Sedangkan jaringan menggunakan TMSI untuk berkomunikasi dengan MS. TMSI dikirim kepada MS setelah prosedur otentikasi pengguna dilakukan. Pemetaan TMSI ke IMSI yang berkoresponden, dilakukan oleh jaringan, tepatnya ditangani oleh VLR.

TMSI hanya valid di suatu *Location Area* (LA) tertentu. TMSI di *update* setidaknya setiap perubahan lokasi (ketika ponsel berganti LA atau setelah periode tertentu). TMSI juga dapat diuabah kapanpun oleh jaringan. TMSI dikirimkan dalam bentuk cipher

Contoh serangan terhadap keamanan GSM adalah :

Penduplikasian SIM
Serangan ini dilakukan dengan cara mengekstrak Ki dari SIM melalui serangan *side-channel.* Akan tetapi untuk serangan ini, diperlukan akses secara fisik terhadap SIM dan peralatan khusus[4,5].

Keamanan GSM tidak mencakup otentikasi BTS terhadap MS. Oleh karena itu, MS harus merespon setiap tantangan yang diajukan jaringan. Dengan menggunakan peralatan khusus, dapat dikirim tantangan yang berbeda – beda, kemudian dilakukan *cryptanalysis* terhadap respon untuk kemudian mengekstrak Ki dari SIM. Selama melakukan *cryptanalysis* sinyal dari BTS yang sah harus dalam keadaan mati.
Setelah nilai Ki didapat, dibuat sebuah kartu SIM dengan nilai Ki yang didapat tersebut.

3. Kesimpulan dan Saran Pengembangan

Kesimpulan

1. Algoritma yang digunakan untuk keamanan GSM adalah :
   - A3 : untuk otentikasi user.
   - A5 : untuk enkripsi pesan.
   - A8 : untuk menghasilkan *ciphering key*.

Semua algoritma tidak bersifat publik.

2. Ada anggapan bahwa algoritma yang digunakan lemah, sehingga dirahasiakan.

3. Telah banyak dilakukan *reverse engineering* terhadap Algoritma A5

Saran

1. Untuk pengembangan keamanan GSM, sebaiknya bukan terletak pada kerahasiaan algoritma, namun pada komputasi algoritma yang dibuat kompleks.

2. Salah satu cara untuk pengamanan, adalah dengan menggunakan ukuran *ciphering key* (Kc) yang cukup panjang. Sebagai informasi, ukuran Kc hanya 54 bit, ukurannya yang kecil sangat rawan terhadap serangan.

3. Pada mekanisme komunikasi melalui jaringan GSM, MS diotentikasi oleh BS, namun tidak ada otentikasi BS oleh MS. Kondisi yang demikian menyebabkan MS harus merespon semua tantangan (*challenge*) yang diajukan oleh BS. Hal ini rawan terhadap serangan *man in the middle*. Oleh karena itu, dalam protokol komunikasi GSM perlu ditambah prosedur otentikasi BS oleh MS.

[1] http://www.gsm-security.net/gsm-security-papers.shtml, diakses tanggal 27 Desember 2005.
[2] Quirke, Jeremy. *Security in the GSM System,* Aus Mobile, 2004.
[3] Barkan, Elad; Biham, Eli; Keller, Nathan. *Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication.*
[4] Suominen, Mikko. *GSM Security*, Helsinki University of Technology.
[5] Suominen, Mikko. *GSM Attacks,* Helsinki University of Technology.