

TUGAS AKHIR
EC7010 – Keamanan Sistem Lanjut

Dosen : Budi Rahardjo, MSc, PhD

KEAMANAN PADA GSM



Oleh:
Agus Heri S
23201060

PROGRAM STUDI TEKNIK ELEKTRO
BIDANG KHUSUS TEKNIK KOMPUTER
PROGRAM PASCASARJANA
INSTITUT TEKNOLOGI BANDUNG
2004

KEAMANAN PADA GSM

Abstrak

Tujuan keamanan pada sistem telekomunikasi seluler adalah untuk mengamankan suara dan data dalam transmisi dari *interception* (pelacakan) dan *fraud* (kecurangan) dari pihak-pihak yang tidak berhak. *Authentication* (pembuktian keaslian) dan enkripsi memastikan keamanan dalam jaringan GSM.

1. PENDAHULUAN

Kejahatan seluler mulai merebak pada saat seluler masih menggunakan sistem analog. Dimana baik voice dan data dari pelanggan seluler analog ditransmisikan tanpa menggunakan enkripsi, sehingga setiap orang dengan menggunakan radio all-band dapat mendengarkan / menyadap pembicaraan pada seluler. Bahkan dapat melakukan panggilan dengan memanfaatkan data pelanggan orang lain (cloning).

Tuntutan dari dunia industri bahwa sistem operator harus dapat memastikan bahwa pelanggan yang meminta pelayanan adalah valid (*Authentication*) dan pelanggan menginginkan akses yang memiliki privasi (kerahasiaan data), sebuah sistem yang lebih baik terasa sangat diperlukan. Komunikasi Global System for Mobile (GSM) yang merupakan sebuah standar baru muncul pada tahun 1982. Pada awalnya muncul di Eropa dan menggunakan frekuensi radio 900Mhz, sehingga biasa disebut GSM900. Dan kemudian menjadi standar untuk komunikasi seluler digital yang memiliki kewanaman yang lebih baik dibandingkan dengan sistem analog sebelumnya.

Perbandingan sistem GSM dengan sistem analog, sistem GSM menyediakan mekanisme keamanan dan *Authentication*. Keamanan sistem GSM adalah bagian dari kemajuan sistem digital, sejak speech coding algoritma mulai dipergunakan. Untuk menyadap informasi pada sistem GSM diperlukan alat tambahan yang lain, tidak hanya

bermodalkan radio all-band. Kemampuan *Authentication* dan enkripsi ditawarkan sistem GSM untuk memastikan keamanan pada sistem seluler.

Manakala informasi akan ditransfer melalui jaringan seluler keamanan merupakan masalah yang sangat penting dan bisa dijadikan sebagai objek untuk sebuah tindak kejahatan. Pada bagian berikutnya akan dijelaskan mengenai keamanan GSM dengan harapan dapat dimengerti keamanan system seluler tersebut.

2. JARINGAN GSM

Jaringan GSM adalah sitem jaringan digital yang aman dan di desain untuk menggantikan sistem analog. Banyak feature seperti algoritma yang lebih baik dan teknik enkripsi dipergunakan dalam sistem ini, untuk mendapatkan keamanan yang terkendali. Keamanan dalam sistem GSM terdiri dari tiga kategori fungsi yaitu :

Subscriber identity confidentiality (Kerahasiaan identitas pelanggan)

Subscriber identity authentication (pembuktian keaslian identitas pelanggan)

Signaling data and user data confidentiality (kerahasiaan pengiriman data dan data pelanggan) .

Keamanan dalam sistem GSM ini akan dibahas lebih lanjut dalam sub bab 2.4 Pelanggan pada jaringan diberi identitas yang unik oleh International Mobile Subscriber Identity (IMSI), bersama dengan secret key/kunci rahasia (Ki) yang unik untuk mobile device. Data yang sensitif tidak dipancarkan melalui path radio, melainkan menggunakan sebuah mekanisme yang disebut *Challenge and Respon*, yang berbasis pada enkripsi dan digunakan untuk melakukan *authentication*. Komunikasi suara menggunakan enkripsi yang memakai *random temporary generated ciphering key* (Kc).

2.1. Cryptography

Pada bagian ini akan membahas mengenai cryptography dengan penekanan pada feature yang ada pada sistem GSM.

2.1.1. Symmetric Algorithms

Algoritma Symmetric adalah algoritma dimana enkripsi dan dekripsi menggunakan kunci yang sama. Sebagai contoh, jika plaintext ditandai oleh variable P, ciphertext oleh C, enkripsi dengan kunci x oleh fungsi $E_x()$ dan dekripsi dengan kunci x oleh $D_x()$ kemudian algoritma symmetric secara fungsional diuraikan sebagai berikut :

$$C = E_x (P)$$

$$P = D_x (C)$$

$$P = D_x (E_x (p))$$

Algoritma enkripsi yang baik, keamana data terletak pada keamanan kunci. Contoh dari algoritma symmetric yang sudah cukup terkenal adalah Data Encryption Standard (DES). Enkripsi Algoritma symmetric dibagi menjadi block ciphers dan stream ciphers.

2.1.1.1. Block Ciphers

Seperti namanya, block ciphers enkrip atau dekrip data, dalam blok atau group bits. DES menggunakan kunci 64 bit dan proses data dalam 64 bit blok, menghasilkan 64 bits enkrip data untuk 64 bit input dan sebaliknya. Algoritma Blok lebih lanjut ditandai oleh mode operasinya, seperti Electronic code book (ECB), cipher block chaining (CBC) dan cipher feedback (CFB). CBC dan CFB adalah contoh mode operasi di mana encryption dari blok berurutan adalah bergantung pada keluaran satu atau lebih sebelum enkripsi. Mode inilah yang diinginkan sebab mereka memisahkan satu per satu koresponden antarablock ciphertext dan blok plaintext (seperti pada mode ECB). Blok Cipher diterapkan sebagai sebuah komponen dari stream cipher.

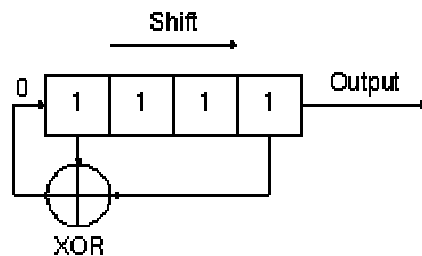
2.1.1.2. Stream Ciphers

Stream cipher beroperasi pada basis bit per bit, menghasilkan bit enkrip tunggal untuk sebuah bit plaintext. Umumnya stream cipher diimplementasikan seperti exclusive-or (XOR) dari data stream dengan keystream. Keamanan dari stream cipher ditentukan oleh properti keystream. Sebuah keystream yang acak/random akan efektif bila

diimplementasikan pada *unbreakable one time pad encryption* dan sebuah keystream yang deterministic dengan periode yang pendek akan memiliki keamanan yang kurang baik.

Linear Feedback Shift Registers (LFSRs) adalah sebuah komponen key dari banyak stream cipher. LFSRs diimplementasikan seperti sebuah shift register dimana bit yang kosong dihasilkan dari pergantian sebuah shift suatu fungsi state yang sebelumnya. Dengan pemilihan umpan balik yang tepat, LFSRs dapat berfungsi seperti pembangkit angka yang acak (pseudo-random number generators). LFSRS mempunyai kelebihan tambahan yaitu mudah diterapkan pada perangkat keras.

Panjang sequence maksimal (atau m-sequence) sama dengan $2^n - 1$ di mana n adalah derajat tingkat/pangkat shift register. Sebagai contoh, panjang maximal LFSR seperti ditunjukkan gambar 1. LFSR ini akan menghasilkan m-sequence yang periodik seperti berikut ini (1111, 0111, 1011, 0101, 1010, 1101, 0110, 0011, 1001, 0100, 0010, 0001, 1000, 1100, 1110).



Gambar 1. Empat Stage Linear Feedback Shift Register (LFSR)

Dengan maksud menghasilkan m-sequence, tap umpan balik dari LFSR harus berpasangan dengan polynomial modulo2 pangkat n . Desain stream cipher terdiri dari berbagai LFSRS dengan berbagai skema interkoneksi dan clocking. Algoritma GSM A5, digunakan untuk enkripsi suara dan signaling data pada GSM adalah stream cipher dengan based pada LFSRs controler pada clock tiga.

2.1.2. Public Key Algorithm

Algoritma public key ditandai oleh dua key, public dan private key, yang melaksanakan fungsi komplementer. Public dan private key adalah satu pasang, idealnya private key tidak mungkin disimpulkan dari public key, dimana public key dapat

didistribusikan secara terbuka. Data yang dienkripsi dengan public key hanya dapat didekripsi dengan private key pasangannya dan sebaliknya. Fungsi ini dapat ditunjukkan seperti berikut :

$$C = E_{pub}(P), P = D_{priv}(C)$$

$$C = E_{priv}(P), P = D_{pub}(C)$$

Contoh yang paling umum dari public key algorithm adalah RSA, singkatan dari penciptanya Rivest, Shamir dan Adleman.

2.1.3. One-Way Hash Function

Biasanya, fungsi hash satu arah menghasilkan panjang output yang tetap yang diberikan oleh arbitrary input. Keamanan fungsi hash satu arah di desain sedemikian rupa sehingga computationally tidak mungkin untuk menentukan masukan itu memberi nilai hash, atau untuk menentukan dua masukan unik dimana hash memiliki nilai yang sama. Contoh dari fungsi hash satu arah pada MD5 yang dikembangkan oleh Ron Rivest, dimana untuk menghasilkan nilai 128-bit hash, dan Secure Hash Algorithm (SHA) dikembangkan oleh National Institutes of Standards and Technology (NIST), yang menghasilkan 160-bit out put.

Suatu aplikasi yang khas dari fungsi hash satu arah adalah untuk menghitung sebuah "message digest" yang memungkinkan penerima untuk memverifikasi keaslian data dengan menyalin perhitungan itu dan membandingkan hasilnya. Keluaran Fungsi hash satu arah dienkripsi dengan suatu algoritma key public membentuk basis untuk tandatangan digital (digital signatures), seperti Algoritma Tandatangan Digital (DSA) milik NIST.

Sebuah key-dependent fungsi hash satu arah memerlukan suatu key untuk menghitung dan memverifikasi nilai hash. Ini sangat bermanfaat untuk tujuan authentication, dimana seorang pengirim dan penerima boleh menggunakan suatu key-dependent fungsi hash di dalam suatu skema challenge-response. Sebuah key-dependent fungsi hash satu arah dapat diimplementasikan dengan hanya menambahkan key tersebut kepada message dan menghitung nilai hash. Pendekatan yang lain adalah dengan

menggunakan sebuah block cipher dalam mode cipher feedback (CFB), dengan output yang telah dienkripsi pada block terakhir (memanggilnya pada mode CFB yang diberikan output blok yang bergantung pada output block sebelumnya). Algoritma A3 dan A8 dari GSM adalah key-dependent fungsi hash satu arah. Algoritma A3 dan A8 GSM adalah mirip dalam fungsi dan implementasi umum seperti algoritma tunggal yang biasa disebut COMP128.

2.2. Implementasi Keamanan GSM

Terdapat tiga elemen yang berbeda dimana mekanisme keamanan GSM diimplementasikan, yaitu : Subscriber Identity module (SIM), GSM handset dan jaringan GSM.

Subscriber Identity module (SIM)

SIM berisi IMSI, secret key yang unik (KI) untuk mobile device, ciphering key generating algorithm (A8), authentication algoritma (A3) dan Personal Identification Number (PIN). Algoritma authentication (A3) yang dipergunakan disini adalah untuk pilihan operator, sehingga operator dapat bekerja antar operator tanpa algoritma authentication dan secret key (ki) dengan operator yang lain.

GSM handset

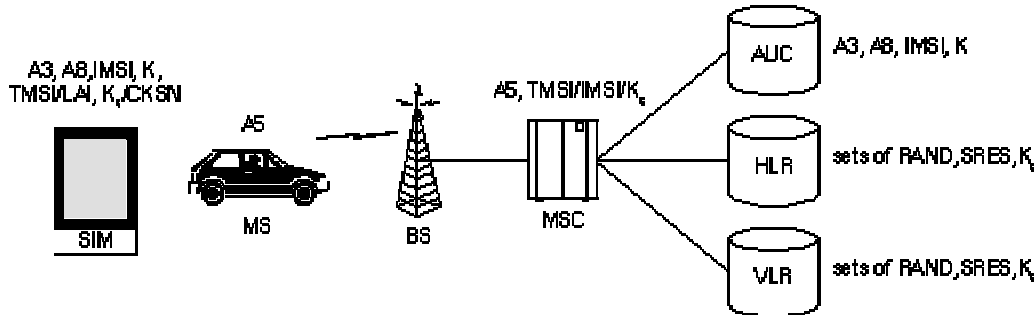
Handset berisi ciphering algoritma (A5), yang harus bekerja dengan cukup cepat sehingga diimplementasikan pada level hardware.

Jaringan GSM

Jaringan berisi enkripsi algoritma (A3, A5 dan A8)

Pada gambar 2 menunjukkan distribusi dari keamanan informasi yang terdiri dari tiga elemen; Subscriber Identity module (SIM), GSM handset atau MS dan jaringan GSM. Dalam jaringan GSM, keamanan informasi didistribusikan antar pusat Authentication (AUC), Home Location Register (HLR) dan Visitor Location Register

(VLR). AUC bertanggung jawab pembangkitan RAND, SRES dan Kc yang disimpan pada HLR dan VLR untuk subsequent yang berguna pada fungsi *authentication* dan proses enkripsi.



Gambar 2. Distribusi feature keamanan pada jaringan GSM

2.3. Algoritma Enkripsi GSM

Terdapat nomer dari algoritma enkripsi yang diimplementasikan pada GSM sistem :

A3 – Algoritma placeholder dari *authentication* GSM

A5 – Algoritma GSM stream chipper, dimana terdapat empat implementasi :

A5/0 – Dalam algoritma tidak terdapat enkripsi

A5/1 – Juga dikenal sebagai algoritma “strong over the air voice privacy”

A5/2 – Implementasi yang lebih lemah dari A5/1

A5/3 – Algoritma enkripsi baru yang diperkenalkan pada Juli 2002

GSM di desain untuk dipergunakan di Eropa Barat, dan regulasi export tidak mengijinkan teknologi yang asli dipergunakan di luar Eropa. Umumnya A5/1 dipergunakan oleh negara negara di Eropa dan A5/2 digunakan oleh negara negara diluar Eropa.

A8 – Algoritma Chiper key generating

Comp128 one way function yang saat ini dipergunakan pada jaringan GSM A3 dan A8. tetapi algoritma comp128 telah dapat dipecahkan. Algoritma ini telah dibuktikan untuk

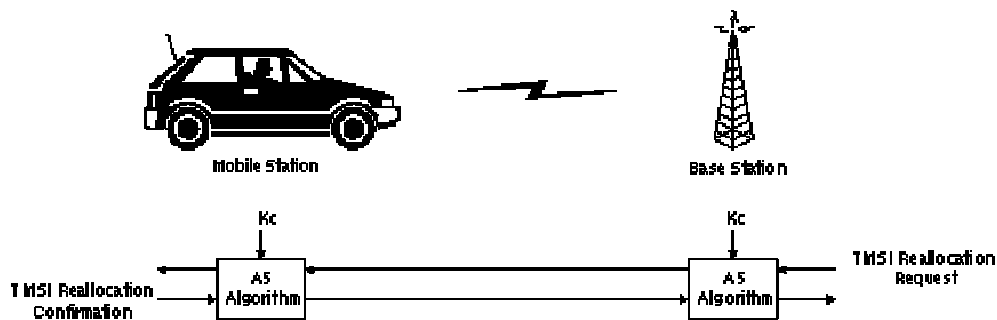
sebuah kesalahan sehingga secret key dapat dipecahkan dengan SIM level (2^{19} queries) dalam waktu empat jam.

2.4. Fungsi Keamanan GSM

Terdapat tiga kategori fungsi keamanan yang disediakan oleh sistem GSM, yaitu :

2.4.1. Subscriber identity confidentiality (anonymity)

Informasi pelanggan adalah hal utama yang harus dilindungi, dari kemungkinan pengganggu. Kebocoran dari transmisi pada radio juga harus dihindari. Hal ini dapat dilakukan dengan menggunakan Temporary Mobile Subscriber Identity (TMSI). Identitas asli dari pelanggan akan digunakan ketika pelanggan pertama kali meyalakan handsetnya, TMSI kemudian akan mulai aktif dijalankan. TMSI akan mengirim ke MS setelah melakukan prosedur authentication dan enkripsi. MS akan merespon dengan melakukan konfirmasi atas TMSI yang diterimanya. TMSI adalah valid/benar dalam lokasi dimana TMSI tersebut dikeluarkan. Proses alokasi atau realokasi TMSI seperti ditunjukkan pada gambar 3.



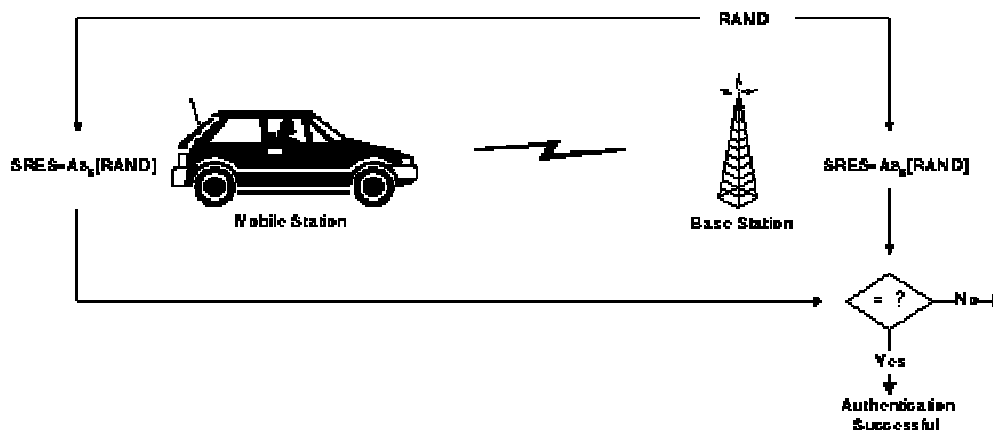
Gambar 3. Subscriber Identity Confidentiality

2.4.2. Subscriber identity authentication (Authentication)

Tujuan dari *authentication* adalah untuk mengidentifikasi pelanggan yang asli dan berhak pada operator jaringan, sehingga operator dapat memastikan tagihan ditujukan

kepada orang yang tepat. Oleh karena itu *authentication* yang handal perlu diimplementasikan untuk melindungi oprator dari kejahatan tagihan.

Ini dicapai dengan menggunakan mekanisme yang disebut “*Challenge and Response*”. Suatu *random challenge R* (acak 128 bits/ RAND) dikeluarkan dari jaringan ke mobile (MS). MS menghitung 32-bit signed response (SRES) yang berbasis enkripsi pada random number (RAND) dengan menggunakan algoritma *authentication (A3)* dan *secret key (Ki)* yang unik pada mobile, dan akan mengirim kembali 32 bit *Signed Response (SRES)* ke jaringan. Operator kemudian melakukan cek terhadap respon kepada challenge, dengan melakukan hal yang sama ke challenge, jika hasilnya adalah sama seperti respon yang diterima *authentication* telah berhasil. Jika nilai tidak sama koneksi akan diputus dan *authentication* gagal. Seperti ditunjukkan pada gambar 4.



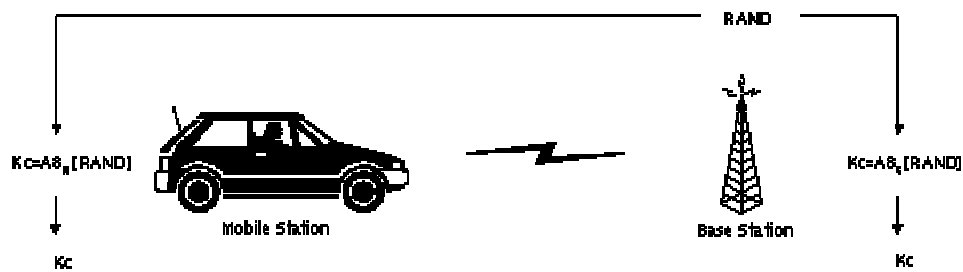
Gambar 4. Mekanisme GSM authentication

2.4.3. Signaling data and user data confidentiality (User data and signaling protection)

Setelah koneksi berlangsung (*establish*), semua transfer data yang melalui jaringan perlu untuk dilindungi. Informasi pengguna seperti SMS ditransfer pada sebuah mode paket *connectionless* melalui sebuah *signaling channel*, atau suara dan beberapa komunikasi bukan suara *establish* pada koneksi physical melalui interface radio, harus diamankan dengan sebaik baiknya.

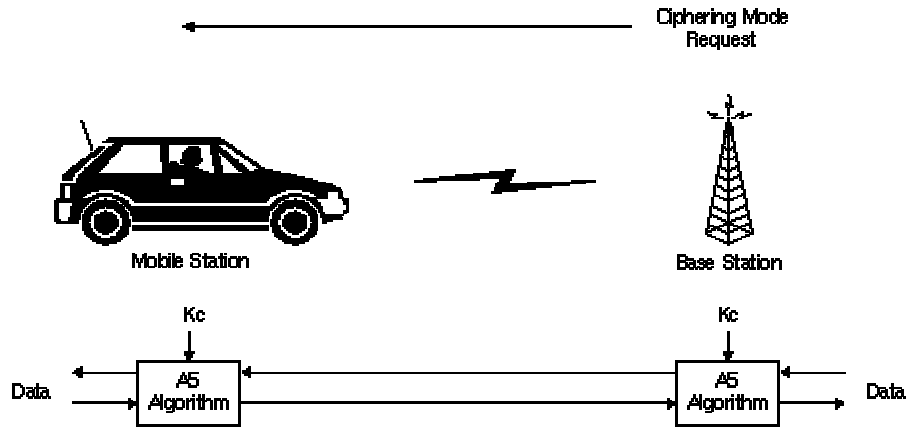
Untuk mencapai kerahasiaan, berbagai mekanisme pengamanan diperlukan seperti: metode chipering, key setting, proses enchipering dan dechipering serta sinkronisasi.

Setelah berhasil melakukan proses *authentication* seperti dijelaskan sebelumnya, baik mobile dan jaringan menggunakan algoritma A8 untuk *decrypt the response* agar dapat memperoleh 64 bits key Kc. Chipering key dihitung dengan menggunakan aplikasi yang sama Random Number (RAND) yang digunakan pada proses authentication. Oleh karena itu algoritma enkripsi A5 dan key Kc digunakan untuk enkripsi data yang dikirim melalui radio path dengan tujuan untuk mendapatkan privacy. Chipering key dapat dirubah pada waktu tertentu sesuai dengan desain jaringan dan pertimbangan keamanan. Pada gambar 5 memperlihatkan perhitungan dari chipering key (Kc).



Gambar 5. Mekanisme Chipering Key Generation

Key Kc akan disimpan dan digunakan dalam *mobile device* untuk transmisi sampai diupdate pada *authentication* yang akan datang. Hal ini juga penting bahwa *enchipering stream* pada sebuah end harus disinkronisasi dengan *dechipering stream* pada end yang lain. Mekanisme mode inisialisasi Chipering seperti diperlihatkan pada gambar 6.



Gambar 6. Mekanisme mode inisialisasi Chipering

3. Fraud

Fraud (kecurangan) adalah dimana sebuah kelemahan pada sistem yang dieksploitasi untuk mendapatkan keuntungan. Ada dua tipe dari fraud yaitu: *technical fraud* dan *procedural fraud*.

3.1. Technical fraud

Ini tipe fraud dimana kelemahan jaringan yang dimanfaatkan untuk membuat panggilan yang tanpa bayar (free Call). Sebagai contoh, servis panggilan seperti *call forwarding* atau *conference* dapat ditawarkan kepada pelanggan dengan mencuri *mobile device*-nya. Sistem switching atau billing (tagihan) dari jaringan sering dapat ditembus oleh para hacker, dimana *free call* atau keuntungan keuangan dapat dibuat. Pada beberapa kasus yang ekstrim sistem billing dan sistem routing dapat diambil alih oleh para hacker. Ukuran dari *fraud* untuk tipe ini adalah sangat tinggi, khususnya ketika modifikasi peralatan diperlukan. *Fraud* dapat diminimasi dengan melakukan desain *feature* yang baik dari awalnya.

3.2. Procedural fraud

Pada tipe ini *fraud* diakibatkan oleh eksploitasi pada kelemahan proses bisnis. Para attacker dapat memperoleh uang atau yang lain dari pengembalian keuntungan. Sebagai contoh, *free call* dapat dibuat dari pencurian *mobile device* dan menjual *call* kepada pihak ketiga dengan rate yang lebih rendah dari operator jaringan. Ukuran fraud untuk tipe ini terhitung lebih mudah dan lebih efektif costnya. ☺ Mau coba ?

4. Kesimpulan

Pada tugas ini menguraikan keamanan pada sistem GSM, terutama fungsi pada setiap feature keamanan. Bagaimanapun juga, sistem GSM bukanlah sistem yang sempurna, masih terdapat ancaman didalamnya. Operator jaringan harus melihat level keamanan dari *authentication* dan enkripsi, enkripsi yang lebih baik dari A3/A8 harus digunakan sebagai penggantinya.

Fraud (kecurangan) dapat terjadi karena adanya kolusi dengan orang dalam. Hal ini harus diketahui oleh pelanggan/konsumen sehingga mereka diharapkan untuk berhati-hati dalam memilih provider/penyedia jasa seluler.

Singkatan

A3	Authentication Algorithm
A5	Ciphering Algorithm
A8	Ciphering Key Generating Algorithm
AMPS	Advanced Mobile Phone System
AUC	Authentication Center
BS	Base Station
CBC	Cipher Block Chaining
CEPT	European Conference of Post and Telecommunication Administrations
CFB	Cipher Feedback
CKSN	Ciphering Key Sequence Number
DES	Data Encryption Standard
DSA	Digital Signature Algorithm
ECB	Electronic Code Book
ETSI	European Telecommunications Standards Institute
GMSK	Gaussian Minimum Shift Keying
GSM	Group Special Mobile
HLR	Home Location Register

IMSI International Mobile Subscriber Identity
Kc Ciphering Key
Ki Individual Subscriber Authentication Key
LAI Location Area Identity
LFSR Linear Feedback Shift Register
MoU Memorandum of Understanding
MS Mobile Station
MSC Mobile Switching Center
NIST National Institute of Standards and Technology1
OMS Operation and Maintenance Subsystem
RAND Random Number
RSA Rivest, Shamir, Adleman
SHA Secure Hash Algorithm
SRES Signed Response
TACS Total Access Communications System
TMSI Temporary Mobile Subscriber Identity
VLR Visitor Location Register

Daftar pustaka

1. David Margrave, "GSM Security and Encryption" online terdapat :
<http://www.hackcanada.com/blackcrawl/cell/gsm/gsm-secur/gsm-secur.html>
2. Fu-Yao Kevin Fang, GSM & GPRS security, Department of Computer Science
University of Cape Town.
3. The Clone, The GSM Security Technical White paper for 2002, online terdapat :
http://www.hackcanada.com/blackcrawl/cell/gsm/gsm_security.html.