PERANCANGAN PROTOKOL SMS BANKING

Herdyanto Soeryowardhana – NIM : 13505095

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if15095@students.if.itb.ac.id

Abstrak

Makalah ini membahas tentang perancangan protokol *SMS Banking*. *SMS banking* merupakan suatu layanan perbankan melalui jalur elektronik yang memungkinkan para nasabah bank tertentu untuk melakukan berbagai transaksi perbankan melalui fasilitas *SMS* pada telepon seluler. Layanan ini bertujuan untuk memberi kemudahan kepada nasabah dalam memperoleh informasi keuangan dan melakukan transaksi dimanapun dan kapanpun tanpa harus mengunjungi ATM (Anjungan Tunai Mandiri) atau bank tempat mereka menjadi nasabah.

Penggunaan *SMS* untuk keperluan transaksi perbankan memerlukan perencanaan dan implementasi yang baik. Hal ini dilakukan untuk melindungi para nasabah dari berbagai ancaman keamanan yang muncul dari oknum-oknum yang tidak bertanggung jawab. Saat ini terdapat berbagai ancaman keamanan terhadap sistem *SMS Banking* seperti *SMS spoofing*, kemungkinan pencurian pesan antara telepon seluler dan *BSS (Base Station Subsystems)*, ketiga datang dari personil operator telepon seluler yang dapat dengan mudah membaca isi log dari pesan *SMS* yang dikirim oleh pengguna layanan, berupa pengiriman pesan kepada server *SMS* provider dengan berpura-pura sebagai aplikasi *mobile banking* dan sebagainya.

Oleh karena itu, untuk mengatasi berbagai ancaman tersebut perlu diimplementasikan suatu protokol *SMS banking* yang relatif aman. Protokol adalah suatu kumpulan aturan yang mengatur cara suatu pelayanan diberikan. Penggunaan protokol *SMS banking* yang tepat dan baik dapat meningkatkan tingkat keamanan layanan tersebut.

***Kata kunci**: SMS Banking,* Protokol, *SMS*.

1. Pendahuluan

Fasilitas pada telepon genggam yaitu *SMS* (*Short Message Service*) sudah digunakan oleh masyarakat luas. Menurut data Asosiasi Telepon Seluler Indonesia (ATSI) pada Agustus 2008, jumlah pengguna telepon seluler tercatat sebanyak 120 juta nomor. Telepon seluler pada saat ini sudah menawarkan berbagai fasilitas seperti *SMS*, percakapan telepon melalui *video* dan *GPRS* (*General packet radio service*) untuk mengakses internet. Diantara fasilitas-fasilitas tersebut, *SMS* merupakan salah satu fasilitas standard yang didukung oleh telepon seluler termurah saat ini. *SMS* adalah suatu layanan pengiriman pesan singkat melalui telepon genggam. *SMS* juga merupakan favorit para pengguna telepon seluler. Hal ini dapat dilihat dari survei yang dilakukan oleh Nielsen Mobile di Amerika pada kuartal 2 tahun 2008. Survei ini menunjukkan bahwa pelanggan telepon seluler di Amerika Serikat lebih banyak menggunakan *SMS* dibanding melakukan percakapan telepon. Hal ini dapat terjadi salah satunya adalah karena tarif *SMS* relatif lebih murah dibandingkan tarif percakapan telepon. Selain itu, berbagai kemudahan ditawarkan oleh *SMS*, mulai dari pengunduhan nada dering, permintaan berbagai informasi, sampai dengan transaksi perbankan atau *SMS banking*.

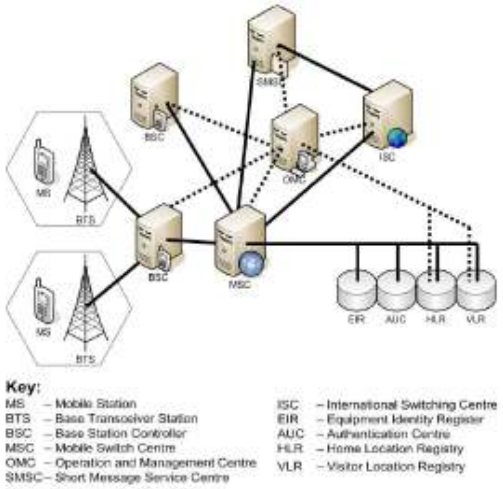
SMS banking merupakan suatu layanan perbankan melalui jalur elektronik yang memungkinkan para nasabah bank tertentu untuk melakukan berbagai transaksi perbankan melalui fasilitas *SMS* pada telepon seluler. Layanan ini bertujuan untuk memberi kemudahan kepada nasabah dalam memperoleh informasi keuangan dan melakukan transaksi dimanapun dan kapanpun tanpa harus mengunjungi ATM atau bank tempat mereka menjadi nasabah. Layanan ini sudah ditawarkan oleh berbagai bank di

Indonesia. Fasilitas-fasilitas yang ditawarkan dalam layanan ini hampir sama dengan layanan ATM (Anjungan Tunai Mandiri) pada umumnya, kecuali dalam fasilitas penarikan uang tunai.

Penggunaan *SMS* untuk keperluan transaksi perbankan memerlukan perencanaan dan implementasi yang baik. Hal ini dilakukan untuk melindungi para nasabah dari berbagai ancaman keamanan yang muncul dari oknum-oknum yang tidak bertanggung jawab. Saat ini terdapat berbagai ancaman keamanan terhadap sistem *SMS Banking*. Antara lain *SMS spoofing*, kemungkinan pencurian pesan antara telepon seluler dan *BSS (Base Station Subsystems)*, ketiga datang dari personil operator telepon seluler yang dapat dengan mudah membaca isi log dari pesan *SMS* yang dikirim oleh pengguna layanan, berupa pengiriman pesan kepada server *SMS* provider dengan berpura-pura sebagai aplikasi *mobile banking* dan sebagainya.
Salah satu cara untuk mengatasi bahaya penipuan yang telah dijelaskan sebelumnya adalah dengan merancang suatu protokol *SMS banking* yang relatif aman. Secara definitif protokol adalah suatu kumpulan aturan yang mengatur cara suatu pelayanan diberikan. Protokol SMS banking yang dimaksud di makalah ini mengarah kepada mekanisme pengiriman pesan *SMS* yang aman antara telepon seluler, *SMS gateway*, dan *server* bank. Protokol ini juga menerapkan berbagai teknologi kriptografi antara lain, algoritma pertukaran kunci seperti Diffie Hellman, algoritma enkripsi simetri seperti AES *(Advanced Encryption Standard)* dan algoritma enkripsi asimetri seperti RSA. Kegunaan algoritma pertukaran kunci adalah untuk mempertukarkan suatu kunci rahasia antara dua orang atau lebih. Algoritma asimetri menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi pesan yang berbeda sedangkan pada algoritma simetri, kunci yang digunakan adalah sama. Penerapan protokol *SMS banking* yang relatif aman diharapkan dapat mengurangi serta melindungi data-data pribadi para nasabah dari berbagai bahaya penipuan dan pencurian oleh oknum-oknum tertentu.

2. Arsitektur Keamanan GSM

Global System For Mobile Communication (GSM) adalah standard yang terkenal untuk telepon genggam di dunia. Gambar 1. menunjukkan struktur dasar untuk arsitektur GSM. GSM memberikan layanan SMS dan GPRS (*General Packet Radio Service*)



Gambar 1 Strukutur Arsitektur GSM

Jaringan inti GPRS adalah suatu bagian yang terintegrasi dari jaringan GSM. Jaringan tersebut berada di atas lapisan jaringan GSM dengan tambahan simpul-simpul untuk menangani *packet switching*. GPRS juga menggunakan beberapa elemen-elemen jaringan GSM yang sudah ada yang diantaranya sudah termasuk *Base Station Subsystem* (BSS), *Mobile Switching Centers* (MSC), *Authentication Centers* (AUC), dan *Home Location Registers* (HLR) yang sudah ada.

3. Ancaman Keamanan

3.1 Masalah dengan Algoritma Autentikasi A3/A8

A3/A8 adalah suatu istilah yang digunakan untuk mendeskripsikan mekanisme yang digunakan untuk mengautentikasikan suatu alat genggam pada suatu jaringan telepon seluler. A3 dan A8 secara aktual bukan merupakan algoritma enkripsi, namun merupakan *placeholder*. Algoritma yang secara umum digunakan dalam A3/A8 adalah COMP128. COMP128 telah dipecahkan oleh Wagner dan Goldberg dalam waktu kurang dari satu hari.

3.2 Masalah dengan algoritma A5

Algoritma A5 digunakan untuk mencegah *casual eavesdropping* dengan mengenkripsi komunikasi antara alat genggam dan BSS. Terdapat 3 macam algoritma A5 yaitu A5/0, A5/1 dan A5/2.

3.3 Memanipulasi alamat asli

SMS spoofing adalah suatu serangan yang melibatkan suatu pihak ketiga yang mengirim

pesan SMS yang terlihat seperti dari pihak yang terpercaya. Dimungkinkan untuk mengganti alamat asli pada *header* SMS dengan suatu string alfanumerik. Hal tersebut dapat menyembunyikan alamat pengirim dan pengirim dapat mengirimkan pesan palsu dan melakukan serangan *masquerading*.

3.4 Enkripsi SMS

Format data yang umum untuk SMS adalah plainteks. Enkripsi dilakukan pada saat tranmisi adalah hanya antara *Base Tranceiver Station* (BTS) dan *Mobile Station*. Enkripsi *End-To-End* tidak ada dan algoritma yang digunakan adalah A5 yang telah terbukti tidak aman.

4. Rancangan Protokol

Protokol yang dirancang terdiri atas 2 fase yaitu fase *handshaking* dan fase pertukaran data. Fase *handshaking* dibuat agar proses autentikasi antara nasabah dengan bank dapat berlangsung lebih aman. Fase pertukaran data dibuat agar pada proses pertukaran data transaksi *SMS Banking* yang berlangsung berjalan lebih aman. Selain itu, dibuat juga struktur pesan yang khusus agar proses ekstraksi pesan lebih mudah dilakukan. Struktur pesan yang dibuat berbeda antara fase *handshaking* dan fase pertukaran data.

4.1. Struktur Pesan

Pesan *SMS* yang telah diamankan dibagi menjadi beberapa bagian untuk memudahkan dalam pemeriksaan keamanan yang dibutuhkan untuk protokol. Struktur pesan antara fase handshaking dan fase pertukaran pesan dibuat berbeda agar proses pemeriksaan dapat lebih mudah.

4.1.1. Fase *Handshaking*

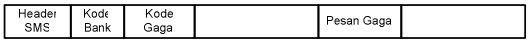
Pada fase ini dibuat 3 struktur pesan yang sama, namun isi dari bagian-bagian pesan tersebut dibuat berbeda. Struktur pesan-pesan tersebut antara lain struktur pesan dari nasabah, struktur pesan berhasil dari server dan struktur pesan gagal dari server.

Berikut penjelasan mengenai isi dari ketiga struktur pesan *SMS*:

- Header *SMS* : berisi header *SMS* yang memang merupakan standard *GSM*.
- Kode Bank: kode unik dari bank yang berguna untuk menghindari SMS palsu.
- Kode Nasabah: kode unik milik nasabah.
- Nilai X Diffie Helman: Nilai X dalam Diffie Helman.
- Nilai Y Diffie Helman: Nilai Y dalam Diffie Helman.
- PIN Nasabah: PIN (*Personal Identification Number*) milik nasabah.
- Nomor Seri Perangkat Lunak
- Pesan Berhasil: isi pesan berhasil
- Pesan Gagal: isi pesan gagal
- Kode Berhasil: kode yang menandakan bahwa proses berhasil
- Kode Gagal: kode yang menandakan bahwa proses gagal.

Gambar 2 Struktur Pesan dari Nasabah

Gambar 3 Struktur Pesan Berhasil dari Server



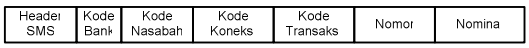
Gambar 4 Struktur Pesan Gagal dari Server

4.1.2. Fase Pertukaran Data

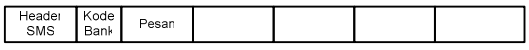
Pada fase ini dibuat 2 struktur pesan yang sama, namun isi dari bagian-bagian pesan tersebut dibuat berbeda. Struktur pesan-pesan tersebut antara lain struktur pesan berhasil dari nasabah dan struktur pesan dari server.

Berikut penjelasan mengenai isi dari kedua struktur pesan *SMS*:

- Header *SMS* : berisi header *SMS* yang memang merupakan standard *GSM*.
- Kode Bank: kode unik dari bank yang berguna untuk menghindari *SMS* palsu.
- Kode Nasabah: kode unik milik nasabah.
- Pesan: isi pesan
- Kode Koneksi: suatu kode sesi nasabah.
- Kode Transaksi: kode transaksi *SMS* banking yang dilakukan oleh nasabah.
- Nomor: nomor rekening dalam transaksi.
- Nominal: jumlah nominal dalam transaksi.



Gambar 5 Struktur pesan dari nasabah



Gambar 6 Struktur Pesan dari Server

4.2. Mekanisme Protokol

4.2.1. Fase Handshaking

Fase ini terdiri atas beberapa tahapan yaitu:

a) Nasabah memasukkan x Diffie Hellman, Kode Nasabah, dan *PIN*.
b) Perangkat lunak membangkitkan X Diffie Hellman dari nilai x yang dimasukkan oleh nasabah.
c) Perangkat lunak membangkitkan pesan yang berisi Kode Bank, Kode Nasabah, nilai X Diffie Hellman, Nomor Seri Perangkat Lunak dan PIN Nasabah.
d) Perangkat Lunak mengenkripsi pesan dengan cipher asimetri menggunakan kunci publik server
e) Perangkat Lunak mengirim pesan *SMS* ke server
f) Server menerima pesan *SMS* dari nasabah, mendekripsi pesan menggunakan kunci privat server
g) Server memilih Kunci Diffie Helman berdasarkan kesepakatan dengan nasabah sesuai kode nasabah yang diterima dan menghitung nilai Y Diffie Helman.
h) server mengautentikasi nasabah dengan memeriksa kode bank, kode nasabah, kesesuaian kunci simetri yang dibangkitkan berdasarkan nilai X Diffie Helman, pin nasabah dan nomor seri perangkat lunak.
i) Jika pesan gagal diautentikasi maka server membuat pesan gagal ke nasabah.
j) Jika pesan berhasil maka server akan membuat pesan yang berisi kode berhasil, Kunci Diffie Helman yang terpilih, dan kode bank
k) Server mengenkripsi pesan dengan cipher asimetri menggunakan kunci publik klien dan mengirim pesan SMS kepada nasabah.
l) Perangkat Lunak menerima pesan, mendekripsi pesan menggunakan kunci privat klien dan mengautentikasi kode bank.
m) Perangkat Lunak memeriksa kode bank, menghitung kunci simetri menggunakan Y Diffie Helman server dan mencocokkan dengan kunci simetri yang dihitung dengan nilai X pada nasabah
n) Jika terautentikasi dengan baik maka nasabah siap untuk melakukan transaksi perbankan

4.2.2. Fase Pertukaran Data

Fase ini terdiri atas beberapa tahapan yaitu:

a) Nasabah memasukkan sintaks sesuai transaksi yang diinginkan atau dapat juga memilih untuk mengakhiri sesi setelah transaksi tersebut.
b) Perangkat Lunak membuat pesan yang berisi kode bank, kode nasabah, kode transaksi sesuai sintaks, nomor serta nominal yang diinginkan.
c) Perangkat Lunak mengenkripsi pesan dengan algoritma Rijndael menggunakan kunci simetri yang didapatkan dari tahap handshaking.
d) Perangkat Lunak mengirim pesan *SMS* ke server
e) Server menerima pesan dari nasabah, mendekripsi pesan menggunakan algoritma Rijndael serta kunci simetri.
f) Server mengautentikasi nasabah dengan memeriksa kode bank, kode nasabah, serta melakukan *parsing* terhadap kode koneksi, kode transaksi, nomor dan nominal.
g) Jika pesan berhasil maka server akan melakukan proses transaksi yang tersebut.
h) Jika gagal, maka server tidak akan melakukan proses transaksi dan server akan mengirimkan pesan *SMS* kepada Nasabah tanpa melakukan enkripsi.
i) Server mengirim pesan *SMS* kepada nasabah yang berisi laporan transaksi yang telah dilakukan dan mengenkripsi pesan dengan algoritma rijndael menggunakan kunci simetri.
j) Perangkat lunak mendekripsi pesan dengan algoritma rijndael menggunakan kunci simetri.
k) Nasabah dapat melihat laporan pesan yang dikirim oleh bank
l) Jika terautentikasi dengan baik maka nasabah siap untuk melakukan transaksi perbankan

5. Kesimpulan

Teknologi GSM telah terbukti memiliki berbagai ancaman keamanan. Oleh karena itu, untuk mengatasi berbagai ancaman tersebut dibuatlah suatu protokol *SMS banking* yang relatif aman yang menggabungkan beberapa teknologi kriptografi yaitu algoritma pertukaran kunci, algoritma simetri, algoritma asimetri dan juga dengan pembuatan struktur pesan *SMS* yang sudah diamankan sehingga mengurangi kemungkinan bocornya informasi yang sensitif nasabah dan pihak bank serta mengurangi berbagai kemungkinan ancaman-ancaman keamanan pada transaksi *SMS Banking* tersebut.

DAFTAR PUSTAKA

[1] Marguerite Reardon (2008). Americans Text More Than They Talk <*http://news.cnet.com/8301-1035_3-10048257-94.html*>
Tanggal Akses: 10 Maret 2009, 15:25.

[2] Roike Sinaga (2008). Lebaran, Saatnya Operator Seluler Menangguk Untung. <*http://www.antara.co.id/arc/2008/8/31/lebaran-saatnya-operator-seluler-menangguk-untung*>
Tanggal Akses: 10 Maret 2009, 15:30.

[3] Luciana Spica Almilia, Antomy Nova Giarta (2007). Perspektif Nasabah Perbankan atas kehadiran *SMS banking* dan *WAP banking* sebagai sistem informasi perbankan yang bernilai tambah.

[4] Pieter Streicher (2008). *SMS* Phising On The Increase. <*http://www.bizcommunity.com/Article/196/78/26041.html*>
Tanggal Akses: 10 Maret 2009, 15:45.

[5] Rinaldi Munir (2009). IF3058 Kriptografi.

[6] Subhash Mehta (2003). Academic's Dictionary Of Computers. Academic India Publishers.