Jenis dan Cara Penanggulangan Ancaman pada Keamanan Teknologi Perbankan

Eko Riswanto[1], Herliana[2], Jumadi[3], Kuntoro Primadiantoro[4]
Program Studi Ilmu Komputer
Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Gadjah Mada, Yogyakarta.

[1]riswantoeko@yahoo.com, [2]lea_poenya86@yahoo.com, [3]mas.ajum@gmail.com, [4]kuntoroprimadiantoro@gmail.com

A. Pendahuluan

Ada beberapa hal di dunia perbankan yang berpotensi untuk dikembangkan lebih lanjut dengan perkembangan ekonomi yang mulai banyak berbasis pada teknologi informasi. Tentunya di luar hal-hal yang sudah umum di dunia perbankan saat ini, seperti infrastruktur ATM bersama dll. Secara umum akan ada dua(2) hal besar di dunia perbankan yang dapat terasa manfaatnya,

1. Interaksi di sisi customer/client.
2. Beberapa isu interaksi/clearing antar bank.

Hal yang paling kritis dalam aplikasi keuangan/perbankan terutama adalah masalah security. Kegagalan sisi keamanan jaringan akan dapat menyebabkan kerugian yang tidak sedikit bagi industri perbankan. Secara umum ada empat(4) aspek keamanan jaringan, yaitu:

1. *Penetration testing*
2. *Certificate Authority / PKI*
3. *Vulnerability Testing*
4. *Managed Security Services*

Masing-masing aspek akan mencakup yang yang cukup kompleks, misalnya, aspek Penetration Testing meliputi *Active Content Monitoring/ Filtering, Intrusion Detection–Host Based, Firewall, Intrusion Detection–Network Based, Authorization, Air Gap Technology, Network Authentication, Security Appliances*. Aspek *Certificate Authority/Public Key Infrastructure* meliputi hal

Certificate Authority, File & Session Encryption, VPN & Cryptographic Communications, Secure Web Servers, Single Sign On, *Web Application Security*.

Sebagian besar dari teknologi keamanan jaringan sebetulnya tersedia secara terbuka(*open source*). Misalnya untuk *certicicate authority*/PKI, biasanya menggunakan openSSL; Untuk *secure web transaction* biasanya digunakan *standard secure* HTTP(https); untuk membangun *Virtual Private Network* antar bank biasanya digunakan *Free Secure Wide Area Network*(FreeSWAN). Semua biasanya tersedia di berbagai distribusi Linux.

Dengan menguasai teknik keamanan jaringan dan mampu membuat aman-nya jaringan maka bukan mustahil kita dapat lebih mengeffisienkan infrastruktur *backoffice* industri perbankan. Bukan mustahil kita dapat menggunakan infrastruktur yang berbasis Internet dan IntraNet sebagai backbone infrastruktur per bankan. Terutama untuk menjangkau bank-bank cabang atau bank bergerak di daerah urban, sub-urban bahkan daerah rural dan remote jika di inginkan, Purbo O.W (2001).

Di sisi pelanggan/pengguna jasa bank, perkembangan teknologi tidak kalah menarik. Secara umum ada dua(2) teknologi yang menjadi basis interaksi dunia perbankan dengan pelanggannya agar dapat dilakukan transaksi secara *on-line* dan transaksional, yaitu,

1) Selular Telepon.
2) Internet

Secara umum telepon selular menjadi lebih menarik karena jumlah pelanggan yang lebih bahkan menurut CSFB, Indonesia termasuk mempunyai potensi rangking sangat besar bagi pertumbuhan pengguna selular. Tentunya akan bertambah pilihan lagi dengan semakin banyaknya operator yang menggelar infrastruktur selular. Purbo O.W (2001)

Internet banking, melalui *web* dan *e-mail*, dapat menjadi fasilitas transaksi terutama untuk *corporate customer* karena pada hari ini cukup banyak kantor yang sudah *on-line* 24 jam ke internet. Teknologi keamanan jaringan yang dijelaskan di atas juga telah cukup mapan, terutama jika digunakan enkripsi dengan panjang kunci 128 bit pada akses *web* bertumpu pada teknologi OpenSSL; 1024 bit pada transaksi *e-mail* bertumpu pada teknologi GnuPG di tambah teknologi *One Time Password*, cukup handal untuk menjamin keamanan transaksi. Seperti hal-nya *corporate banking* lainnya sangat di untungkan karena transaksi yang diproses tidak banyak tapi mengalirkan uang dengan berjumlah sangat besar. Transaksi jenis ini justru yang paling menguntungkan untuk dunia perbankan karena termasuk kategori transaksi *Business To Business* (B2B).

Berbeda dengan *InterNet Banking*, pada *end-user* atau *customer* biasa, aplikasi yang jelas-jelas akan menjangkau banyak massa adalah *Short Message Services*(SMS) yang jelas akan menjangkau banyak sekali pelanggan. Salah satu keuntungan dengan adanya teknologi selular bagi dunia pelanggan adalah sistem authentikasi yang sudah *built-in* dalam infrastruktur telepon selular. Authentikasi akan sangat memudahkan bagi dunia perbankan untuk melakukan mapping antara pelanggan/client antara dunia perbankan dengan dunia selular melalui nomor telepon dan nomor *account*.

Ada cukup banyak forum open standar untuk transaksi SMS, MMS, WAP yang menstandarisasi teknologi *messaging* antar pengguna selular telepon, untuk para pelaku yang ingin membuat sendiri *gateway* WAP dan SMS dengan menggunakan solusi *open source* yang terbuka dapat berekperimen dan mencobanya.

Adanya *Internet Banking* dan *Mobile Banking* akan menjadi lebih semarak lagi dengan ada kerjasama yang cukup erat antara dunia perbankan, operator selular, operator Internet dengan berbagai *service provider*, *software house* untuk mengembangkan aplikasi yang lebih terintegrasi dari berbagai layanan.

Contoh sederhana, memberikan informasi perbankan, apakah itu kurs valuta asing, bunga bank, proses peminjaman uang, bunga deposit dll melalui SMS, e-mail, Web.

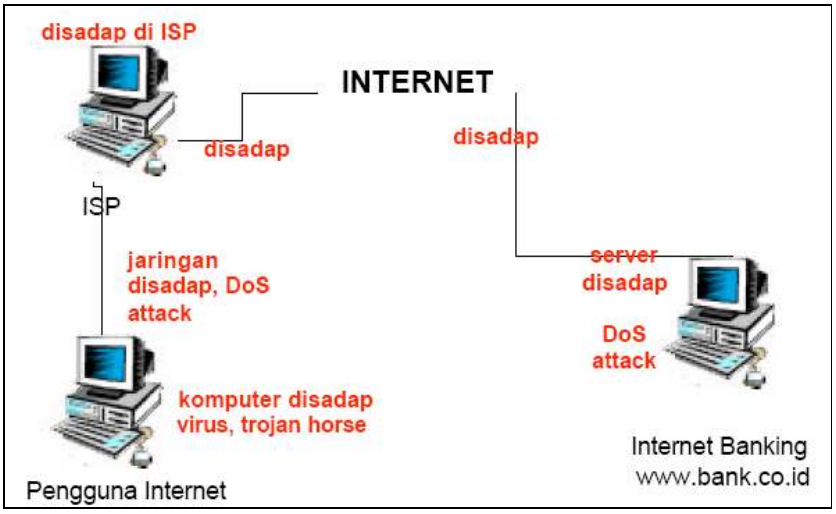
Pada tingkat yang lebih kompleks mendukung transaksi pembelian barang, penjualan barang dengan transaksi keuangan melalui SMS, tidak hanya tergantung pada mekanisme kartu debet atau kartu kredit yang biasa. ini merupakan indikasi perkembangan menuju *mobile commerce*. Tentunya dibutuhkan *service provider* atau *software house* yang mampu membangun *payment gateway* terutama melalui SMS antara bank, penjual dan pembeli. Terutama karena *mobile commerce* termasuk kategori transaksi *business to customer* (B2C).

B. Jenis ancaman dan penanggulangan

1) Keamanan Teknologi *Internet Banking*(i-banking)

a) Ancaman pada sistem keamanan *intenet banking*

Pada dasarnya layanan Internet Banking menggunakan Internet sebagai media komunikasi, maka keamanan dari layanan Internet Banking bergantung kepada keamananan dari Internet. Internet pada mulanya dikembangan di lingkungan akademis (pendidikan dan penelitan). Teknologi Internet yang digunakan saat ini bergantung kepada sebuah teknologi yang disebut IP (Internet Protocol) versi 4. IPv4 ini memiliki beberapa kelemahan ditinjau dari segi keamanan yang sudah diperbaiki di versi 6 (IP v6). Namun sayangnya IPv6 belum lazim dipergunakan.



Gambar 1. Titik rawan dalam hubungan internet

Secara umum hubungan antara pengguna Internet dan penyedia layanan *Internet Banking* dapat dilihat pada gambar 1. Pengguna terhubung ke Internet melalui layanan *Internet Service Provider* (ISP), baik dengan menggunakan modem, DSL, cable modem, wireless, maupun dengan menggunakan leased line. ISP ini kemudian terhubung ke Internet melalui network provider (atau upstream). Di sisi penyedia layanan Internet Banking, terjadi hal yang serupa. Server Internet Banking terhubung ke Internet melalui ISP atau *network provider* lainnya. Gambar 1 juga menunjukkan beberapa potensi lubang keamanan (*security hole*).

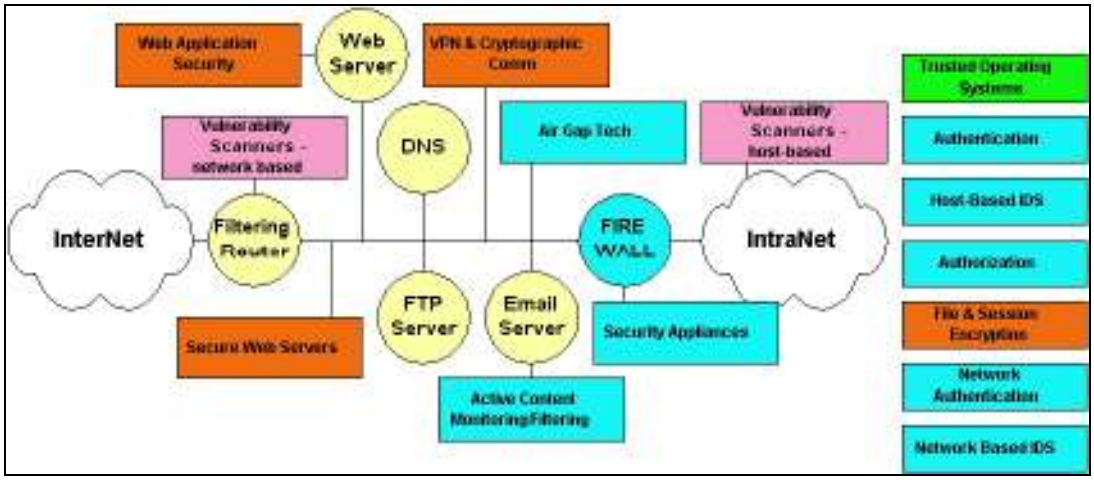
Di sisi pengguna, komputer milik pengguna dapat disusupi virus dan trojan horse sehingga data-data yang berada di komputer pengguna (seperti nomor PIN, nomor kartu kredit, dan kunci rahasia lainnya) dapat disadap, diubah, dihapus, dan dipalsukan. Contoh virus SirCam yang beredar saat ini membuktikan bahwa datadata dari harddisk pengguna dapat tersebar ke seluruh dunia melalui email tanpa diketahui oleh pengguna yang bersangkutan. Virus SirCam mengirimkan file-file dari harddisk tanpa sepengetahuan pemilik computer yang terkena virus SirCam ini. Implikasinya adalah data-

data rahasia (misal data pelanggan, business proposal/plan) yang kita simpan dalam komputer dapat bocor.

Jalur antara pengguna dan ISP dapat juga di sadap. Sebagai contoh, seorang pengguna yang menggunakan komputer di lingkungan umum (*public facilities*) seperti di Warung Internet (warnet) dapat disadap informasinya oleh sesame pengguna warnet tersebut (atau pemilik warnet yang tidak bertanggung jawab) ketika dia mengetikkan data-data rahasia melalui web.

Di sisi ISP, informasi dapat juga disadap dan dipalsukan. Sebagai contoh bila sistem keamanan dari sang ISP ternyata rentan, dan dia kebobolan, maka mungkin saja seorang cracker memasang program penyadap (sniffer) yang menyadap atau mengambil informasi tentang pelanggan ISP tersebut.

Di sisi penyedia jasa, dalam hal ini bank yang menyediakan layanan Internet Banking, ada juga potensi lubang keamanan. Berbagai kasus tentang keamanan dan institusi finansial sudah dilaporkan. Misalnya, ada kasus di Amerika serikat dimana seorang cracker berhasil masuk ke sebuah institusi finansial dan mengambil data-data nasabah dari berbagai bank yang berada dalam naungan institusi finansial tersebut. Di Indonesia sendiri ada "kasus" domain "plesetan" klikbca.com yang sempat membuat heboh.



Gambar 2. Arsitektur keamanan jaringan

Selain serangan yang bersifat penyadapan masih banyak jenis serangan lain seperti pemalsuan dan bahkan meniadakan servis (*Denial of Service attack*).

b) Penanggulangan Ancaman pada sistem keamanan *internet banking*

Ada usaha pengamanan yang dapat digunakan untuk meningkatkan tingkat keamanan dan pada saat yang sama meningkatkan kepercayaan (trust) dari nasabah. Secara teknis sistem dapat diproteksi dengan menggunakan *firewall, Intrusion Detection System* (IDS), dan produk *cryptography* (untuk encryption dan decryption seperti penggunaan SSL). Selain hal teknis yang tidak kalah pentingnya adalah usaha untuk meningkatkan awareness (baik dari pihak management, operator, penyelenggara jasa, sampai ke nasabah), membuat policy (procedure) yang baik dan mengevaluasi sistem secara berkala.

Penanggulangan potensi penyerangan keamanan sitem *internet banking,* diantaranya;

[1] *IP spoofing* diantisipasi dengan penyaringan oleh router;

[2] *User name spoofing*, sistem otentikasi mencegah seseorang dari berpura-pura menjadi user lain dengan memerlukan sandi untuk mengakses bank, transmisi semua password terenkripsi, dan menggunakan *encrypted one-time* "*cookies*" untuk mempertahankan state yang telah disahkan

[3] Upaya untuk Crack Database Otentikasi (*Attempts to Crack Authentication Database*), Informasi *account* pelanggan yang disimpan pada database server yang terlindungi di belakang firewall dan database tidak dapat di-download dari Internet.

[4] Serangan berbasis web server (*Web Server Based Attacks*), Serangan terhadap Netscape Commerce Server adalah digagalkan karena lingkungan chroot-ed dan karena proses "*outside*" yang tidak bisa melihat apa-apa pada proses "*inside*". Firewall hanya mengizinkan mail untuk melewati dan menggunakan SMTP filter. Setiap mesin minimal dikonfigurasi untuk hanya melakukan tugasnya, dan tidak lebih.

Pengamanan di atas pada prinsipnya merupakan usaha untuk memenuhi aspek keamanan seperti *authentication, confidentiality / privacy, non-repudiation, dan availability*. Adanya pengamanan ini tidak membuat sistem menjadi 100% aman akan tetapi dapat membuat sistem dipercaya (*trusted*). Potensi lubang keamanan dapat dianggap sebagai resiko. Maka masalah ini dapat diubah menjadi masalah *risk management*.

2) Keamanan Teknologi *Mobile Banking*(m-banking)

a) Ancaman pada sistem keamanan *mobile banking*

Dalam dekade terakhir, jumlah pengguna perbankan online meningkat pesat. Hal ini menyebabkan banyak pengembang untuk menyelidiki metode yang lebih nyaman bagi pelanggan untuk melakukan remote transaksi perbankan. *Mobile banking* merupakan

skema nyaman baru pelanggan untuk melakukan transaksi, dan diperkirakan akan meningkat sebagai meningkatnya jumlah pengguna telepon seluler. Perkembangan teknologi *mobile banking* bertujuan membangun aplikasi untuk perangkat portabel yang memastikan aman pengguna dapat mengirim informasi perbankan melalui Jaringan GSM. Solusi *mobile banking* maju memberikan platform bagi pengguna untuk bank dengan menggunakan SMS dan GPRS. Tetapi ada beberapa lubang keamanan pada sistem *mobile banking*, masalah yang dimaksud sebagai berikut:

[1] Masalah jaringan GSM: **Masalah dengan algoritma otentikasi A3/A8**. Algoritma ini adalah istilah yang digunakan untuk menjelaskan mekanisme yang digunakan untuk mengotentikasi handset pada jaringan telepon selular. A3 dan A8 sebenarnya tidak algoritma enkripsi, tapi *placeholder*. Dalam A3/A8 algoritma yang umum digunakan adalah COMP128. Algoritma COMP128 rusak oleh Wagner dan Goldberg dalam waktu kurang dari satu hari. Hal ini menimbulkan kekhawatiran GPRS memiliki sebagai yang aman mekanisme komunikasi. Setelah cracking COMP128 Wagner dan Goldberg melanjutkan untuk membuktikan bahwa adalah mungkin untuk mendapatkan Nilai Ki, sehingga sehingga memungkinkan untuk melakukan kloning SIM.

Masalah dengan algoritma A5, Algoritma A5 yang digunakan untuk mencegah *casual eavesdropping* dengan mengenkripsi komunikasi antara stasiun bergerak (handset) dan BSS(*Base Station subsystem*). Kc adalah nilai Ki dan RAND dimasukkan ke dalam algoritma A5. Nilai Kc adalah kunci rahasia yang digunakan dengan algoritma A5 untuk enkripsi antara stasiun bergerak dan BSS.

Attack on the RAND value*,* Ketika AUC(*Authentication Center)* berupaya untuk otentikasi kartu SIM, nilai RAND yang dikirim ke kartu SIM dapat dimodifikasi oleh penyusup gagal

otentikasi. Hal ini dapat menyebabkan penolakan serangan layanan.

[2] Keamanan masalah dengan SMS: Ide awal untuk penggunaan SMS itu dimaksudkan agar pelanggan dapat mengirim pesan non-sensitif di seluruh jaringan GSM terbuka. Reksa otentikasi, enkripsi teks, *end-to-end* keamanan, nonrepudiation dihilangkan selama desain arsitektur GSM. Pada bagian ini kami mendiskusikan beberapa masalah keamanan menggunakan SMS. ***Forging Originator's Address,*** SMS *spoofing* adalah serangan yang melibatkan pihak ketiga mengirimkan pesan SMS yang tampaknya dari pengirim. Hal ini dimungkinkan untuk mengubah originator *field* alamat dalam *header* SMS ke yang lain alfa-numerik *string*. Hal ini dapat menyembunyikan alamat pengirim aslinya, dan melakukan tipuan serangan *masquerading*.

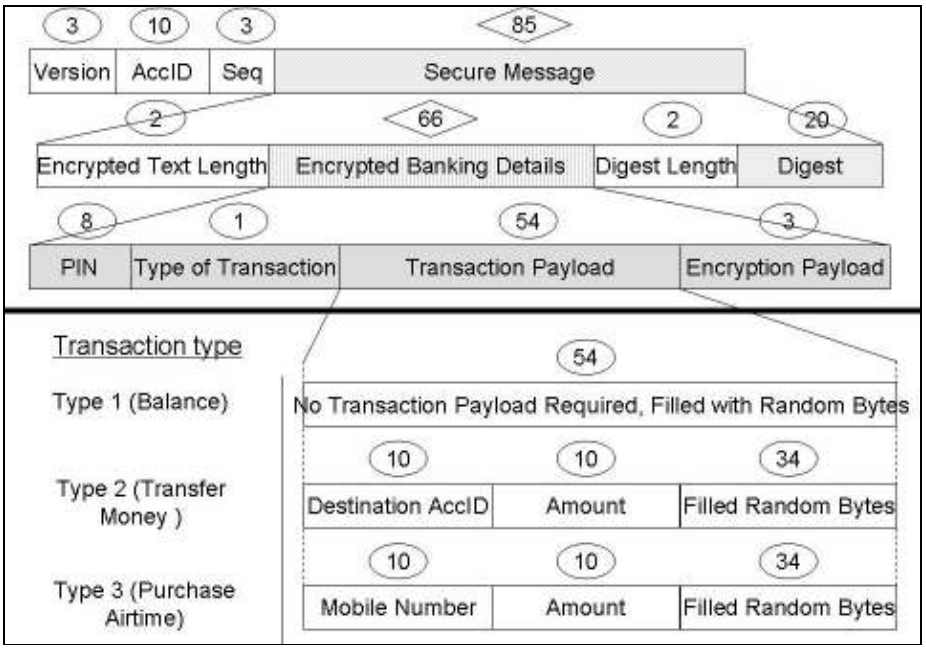
SMS Encryption, Data Format default untuk pesan SMS adalah dalam plaintext. Enkripsi hanya terlibat selama transmisi adalah enkripsi antara stasiun base transceiver dan stasiun mobile. Enkripsi *end-to-end* saat ini tidak tersedia. Algoritma enkripsi yang digunakan adalah A5 yang terbukti rentan. Oleh karena itu algoritma yang lebih aman diperlukan.

[3] Masalah keamanan dengan Implementasi *current* GPRS: S***ecurity issues with present implementations that use WAP,*** Implementasi mobile banking saat ini yang menggunakan WAP telah terbukti sangat aman, tetapi terdapat beberapa lubang yang dapat menyebabkan komunikasi tidak aman. Beberapa lubang meliputi: Tidak ada enkripsi end-to-end antara klien dan bank server. Ada *end-to-end* untuk enkripsi antara klien dan Gateway dan antara Gateway dan Server Bank. Untuk mengatasi ini, server bank dapat memiliki Access Point Name (APN) sendiri di salah satu jaringan GPRS. APN ini akan berfungsi sebagai Gateway WAP untuk bank. Oleh

karena itu klien akan dihubungkan langsung ke bank tanpa ketiga pihak di tengah komunikasi. Kriptografi kunci publik kunci ukuran yang ditawarkan oleh WTLS standar tidak cukup kuat untuk memenuhi aplikasi persyaratan keamanan WAP saat ini. Mengingat rendah kekuatan pengolahan perangkat genggam, ukuran kunci telah telah dibatasi. Anonymous suite pertukaran kunci yang ditawarkan oleh *WTLS handshake* tidak dianggap aman. Baik klien maupun server otentikasi. Bank harus menyediakan fungsionalitas untuk melarang opsi ini dari *handshaking*. **S*ecurity issues associated with using the plain GPRS network,*** Jaringan Inti GPRS terlalu umum, tetapi tidak melayani untuk beberapa perbankan persyaratan keamanan. Beberapa persyaratan termasuk; Kurangnya pemegang rekening atau bank otentikasi. Bank dapat memberikan APN yang unik untuk mengakses server Bank, tetapi tanpa ini atau beberapa orang lain mekanisme otentikasi dapat menyamar sebagai Bank. Semua masalah ini menimbulkan kekhawatiran fabrikasi baik informasi bank atau pemegang rekening informasi, Penyediaan fungsi untuk menghindari modifikasi data dan memastikan integritas data baik untuk pemegang rekening dan Bank. Metode untuk memenuhi kerahasiaan data antara stasiun bergerak dan server bank telah terbukti lemah, dan operator jaringan dapat melihat informasi rekening pemegang. Hal ini menimbulkan masalah keamanan baik bagi bank dan pemegang rekening. Bank tidak dapat membuktikan bahwa pemegang rekening melakukan tindakan spesifik dan pemegang rekening tidak dapat membuktikan bahwa bank melakukan tindakan tertentu. GPRS menyediakan fasilitas penanganan session, tetapi tidak menangani Bank sesi khusus; ini dapat menyebabkan inkonsistensi pada bank samping mengangkat isu-isu keamanan.

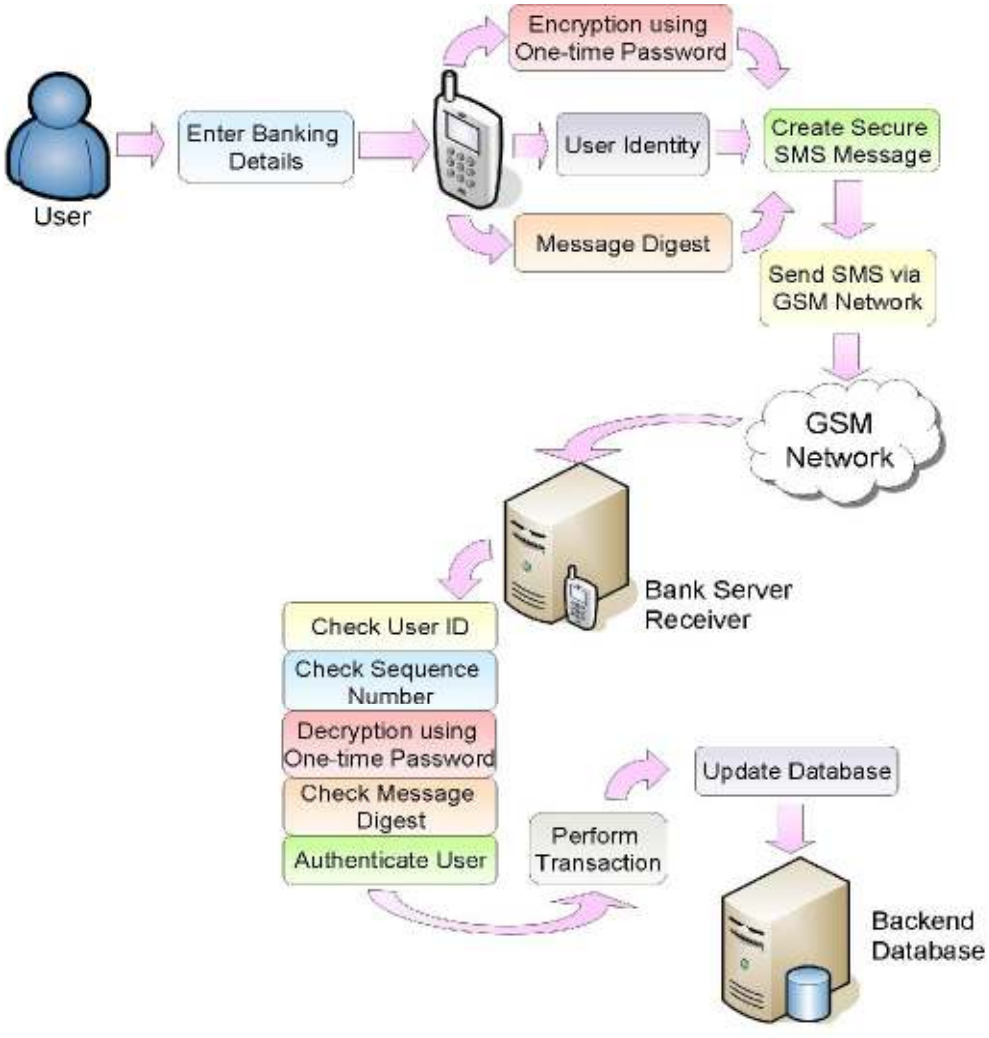
b) Penanggulangan ancaman pada sistem keamanan *mobile banking*

[1] Solusi keamanan SMS, Solusi ini menyediakan protokol messaging aman yang menggunakan SMS. Protokol pesan aman mengatasi keamanan yang ada kekurangan dalam arsitektur GSM. Protokol pesan telah telah terintegrasi dengan sistem mobile banking sehingga dapat meningkatkan keamanan SMS banking. Protokol SMS yang aman meliputi; ***Message Structure***, Pesan SMS dijamin dibagi menjadi beberapa bidang untuk mengakomodasi untuk berbagai pemeriksaan keamanan yang diperlukan untuk protokol. Untuk mempermudah pemahaman tentang struktur pesan, Gambar 3 menunjukkan gambaran struktur untuk pesan SMS yang aman. Angka-angka di atas field adalah jumlah minimum byte diperlukan untuk setiap field dalam pesan. Jumlah byte untuk setiap bidang dapat ditingkatkan tergantung pada pelaksanaan persyaratan.



Gambar 3. Struktur pesan SMS yang aman

Protocol Sequence, Pada jaringan GSM, pesan SMS akan dikirim secara asynchronous ke penerima, karena protokol ini SMS Secure adalah asynchronous. Gambar 4 di bawah ini menggambarkan ikhtisar SMS protokol aman. Kita dapat mempertimbangkan protokol Secure SMS akan dibagi menjadi dua bagian. Bagian pertama adalah generasi pesan. Ponsel menghasilkan pesan dan mengirimkannya ke server. Bagian kedua adalah pesan pemeriksaan keamanan. Server membaca diterima pesan, decode isi dan melakukan pemeriksaan keamanan. subbagian berikut menjelaskan setiap bagian dari protokol.



Gambar 4. Review Protokol SMS

Generating and Sending Secure SMS Messages, Telepon selular menangkap semua informasi keamanan yang diperlukan dari pengguna. Informasi ini digunakan untuk menghasilkan SMS pesan aman yang akan dikirim ke server. Aplikasi mobile telah preset versi pola byte, pola ini dimasukkan ke dalam pesan. Nilai hash pesan nomor yang dapat memastikan pesan integritas untuk sisi penerima. Persyaratan mempertahankan integritas pesan adalah bahwa setidaknya sebagian isi yang digunakan untuk menghitung pesan digest perlu dienkripsi. Hal ini dapat memastikan integritas pesan karena jika pesan disadap, penyerang tidak dapat menggunakan isi terenkripsi untuk menghasilkan lain dicerna. Validasi integritas tidak akan lulus jika ada bagian dari pesan asli diubah. Bidang konten yang harus terenkripsi tergantung pada kebutuhan pengembang. Protokol tersebut mensyaratkan bahwa pesan memiliki beberapa rincian identifikasi untuk tidak dienkripsi. Hal ini untuk penerima untuk mengidentifikasi identitas pemegang rekening. Algoritma yang digunakan untuk enkripsi harus simetris algoritma enkripsi. Kunci yang digunakan untuk enkripsi dihasilkan dari waktu satu-password yang dimasukkan oleh pengguna. Yang satu kali password hanya diketahui oleh server dan pengguna. Setelah aplikasi selesai memproses isi keamanan, isi ditempatkan dalam pesan SMS sesuai dengan struktur pesan yang dijelaskan pada bagian Struktur pesan. Pesan SMS dikirim ke server melalui jaringan GSM.

Receiving and Decoding Secure SMS Message, Ketika server menerima pesan dari jaringan selular, rusak pesan ke bawah sesuai dengan struktur yang diuraikan dalam Pesan bagian Struktur. Server memeriksa versi pertama untuk pola byte. Jika versi benar, diasumsikan bahwa pesan cocok untuk aman SMS protokol. Selanjutnya, server membaca *account* identifier dari pesan dan memeriksa apakah *account identifier* ada di database server. Setelah ini, server akan mengambil arus urutan nomor untuk account yang diberikan identifier. Server memeriksa apakah nomor urutan

membaca dari pesan cocok dengan nomor urutan membaca dari database server. Jika keamanan di atas memeriksa semua berlalu, server hasil untuk mengambil password satu kali dari database. Password diindeks oleh *account* pengenal dan nomor urutan. Setelah itu server menggunakan password diambil sebagai kunci dekripsi untuk memecahkan kode isi dienkripsi. Jika dekripsi yang berhasil, maka password yang digunakan satu kali dibuang dan urutan *counter* server untuk *account* yang akan bertambah dengan nilai dari 1. Setelah dekripsi, server membaca isi yang aman yang diperlukan untuk perhitungan message digest. Pesan digest dihitung dengan menggunakan algoritma yang sama dengan algoritma digunakan oleh aplikasi mobile. Server membandingkan dua *digests* untuk integritas pesan. Jika pesan tidak terbukti memiliki telah diubah, maka server akan mengambil PIN (*account* pemegang password pribadi) dari pesan dan membandingkannya terhadap pemegang rekening PIN dari database server. Jika semua pemeriksaan keamanan di atas berlalu, server melakukan permintaan transaksi.

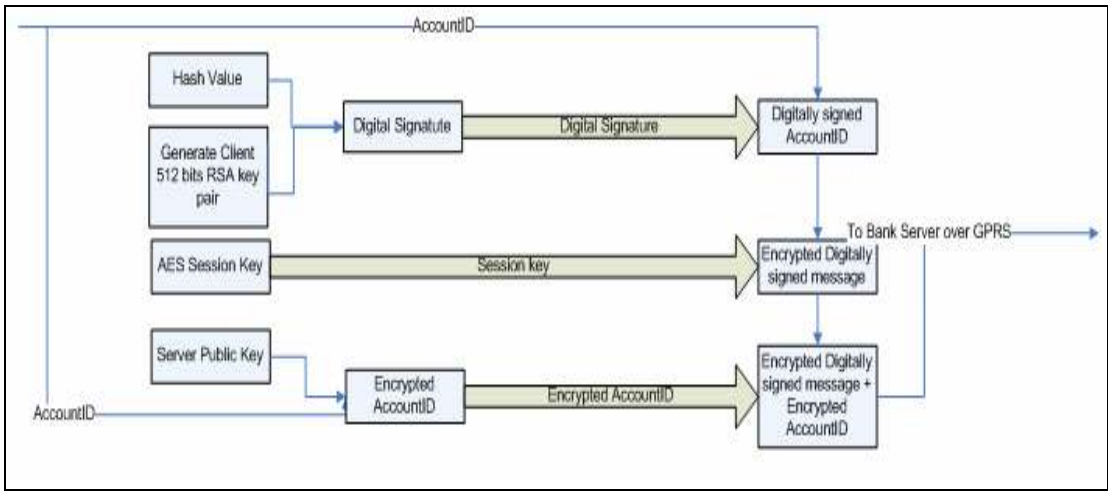
[2] Solusi Keamanan GPRS,

Beberapa protokol GPRS menggunakan sistem kriptografi untuk memberikan solusi keamanan, adapun protokol yang dimaksud adalah: ***Client Protocol Initialization***, Ketika klien start-up aplikasi mobile suatu waktu, menghasilkan pasangan kunci RSA 512 bit. Setelah kunci yang telah dihasilkan klien mengirimkan kunci publik ke server. Kunci ini digunakan dalam protokol untuk membuat tanda tangan digital untuk klien. Tanda tangan digital tersebut diverifikasi oleh server menggunakan publik klien dikirim kunci; hal ini di gunakan mengotentikasi pesan yang dikirim oleh mobile client. Untuk menyelesaikan inisialisasi protokol klien klien menghasilkan PBE AES kunci sesi dengan menggunakan password klien.

User Authentication, Otentikasi dilakukan dalam dua bagian yang berbeda, yang pertama otentikasi dilakukan oleh perangkat

mobile dan yang kedua oleh bank. Ketika seorang pengguna mendaftar untuk menggunakan layanan perbankan server sertifikat ditandatangani menggunakan password klien disertakan sebagai bagian dari aplikasi. Sertifikat ini digunakan untuk mengotentikasi account dudukan di telepon. Ketika pengguna memasukkan password telepon aplikasi menghasilkan kunci AES menggunakan password ini. Menggunakan kunci aplikasi upaya untuk mengambil kunci publik server di sertifikat server, jika server kunci publik akan diambil berhasil otentikasi klien awal selesai; lain yang klien diminta untuk memasukkan kembali password. Yang penting klien hanya diizinkan tiga kali login, jika login gagal di tiga upaya akun tersebut akan diblokir. Otentikasi pengguna kedua dilakukan oleh server, client mengirimkan dienkripsi kliennya ID akun. Server kemudian mendapatkan password dari database dan membuat ulang kunci AES, jika bisa berhasil decode pesan terenkripsi maka klien dikonfirmasi.

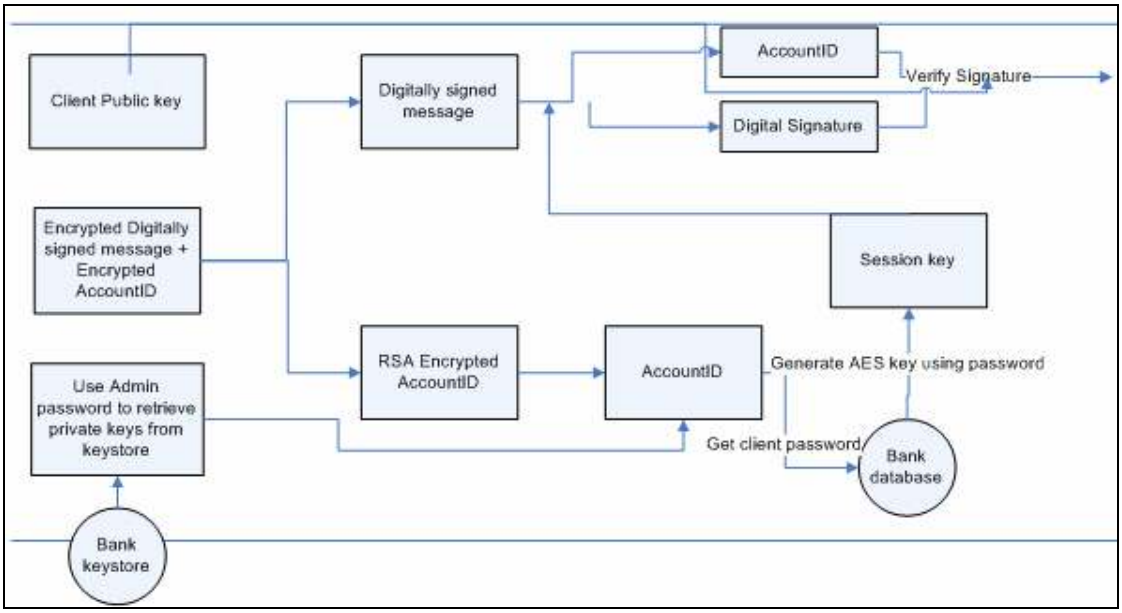
SGP handshake (Client), Handshake SGP melibatkan pengepakan dan mengirim SGP Penuh paket ke server dan server bisa berhasil decode pesan tersebut dan menghasilkan kunci sesi. Gambar 5 di bawah ini menggambarkan mengemas paket SGP Penuh.



Gambar 5. Packing SGP Pesan

Packing dari paket SGP Penuh dimulai-dari dengan klien hashing account klien ID menggunakan SHA-1, ID account hashed ini kemudian dienkripsi menggunakan kunci klien swasta di-order untuk membuat klien tanda tangan digital. Tanda tangan digital ini kemudian digabungkan ke ID account untuk membuat message digest. Hal ini dilakukan untuk memungkinkan server untuk mendeteksi modifikasi data yang dikirim oleh klien. Message digest ini kemudian dienkripsi menggunakan AES dihasilkan sesi kunci, untuk menghindari penyadapan dari pihak ketiga. Aplikasi mobile kemudian mengenkripsi klien s ID account menggunakan server kunci publik. ID akun ini digunakan oleh server untuk mengambil password klien. Terakhir ID dienkripsi akun dan pesan terenkripsi digest di rubah dan dikirim ke bank server.

SGP handshake (Server), Ketika klien membuat koneksi dengan server, yang pertama pesan server adalah klien menerima kunci publik. Setelah klien menerima kunci publik, server mengharapkan untuk menerima pesan SGP Penuh. Ketika server menerima SGP penuh pesan yang membagi pesan ke dalam pesan terenkripsi digest dan ID account dienkripsi. Menggunakan kunci pribadinya server mengambil ID account yang dikirim, dan pada gilirannya mengambil klien password dari database. Jika server gagal untuk mendekripsi pesan, atau jika ID account yang dikirim tidak ada dalam database-nya server mengirimkan pesan kesalahan ke klien. Gambar 6 di bawah ini menunjukkan bagaimana server membongkar dan memverifikasi SGP Penuh paket yang dikirim oleh klien.



Gambar 6. *Unpacking* dan verifikasi SGP pesan

Server kemudian menghasilkan session key menggunakan password yang diambil; session key digunakan untuk mendekripsi message digest yang terenkripsi. Jika server gagal untuk mendekripsi *message digest*, maka server akan mengirimkan pesan kesalahan ke klien, selain lain itu *message digest* dikonversi ke pesan asli dan tanda tangan digital klien. Akhirnya ia memverifikasi pesan asli dengan tanda tangan digital yang dikirim, jika pesan di tanda tangan digital sama dengan *message digest* aslinya maka suite cipher dibentuk dengan sukses. Untuk melengkapi *handshake,* server mengirim sebuah jalur yang dibangun untuk pesan ke klien, inilah sinyal pesan kepada klien bahwa jalur aman dibuat.

Daftar Pustaka

Chikomo K., Chong M. K., Arnab A., Hutchison A., *Security of Mobile Banking.* Data Networks Architecture Group, Department of Computer Science, University of Cape Town, South Africa.

Hammond N., *Secure Internet Commerce: Design and Implementation of the security Architecture of Security First Network Ban, FSB.,* NJH Security Consulting Inc., Atlnata.

Purbo O. W., *E-Banking.*

Rahardjo B., 2001, *Aspek Teknologi dan Keamanan dalam Internet Banking.* INDOCISC.

Yang Y.J., 1997. *The Security of Electronic Banking.* Proceeding. NISSC.