Kajian mengenai Serangan dan Celah Keamanan pada Internet Banking beserta SSL sebagai Kriptografi Pengamanannya

Hendy Sutanto - 13507011
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if17011@students.if.itb.ac.id

***Abstrak* — Socket Secure Layer (SSL) adalah protokol yang digunakan untuk browsing web secara aman. Dalam hal ini, SSL bertindak sebagai protokol yang mengamankan komunikasi antara client dan server. Protokol ini memfasilitasi penggunaan enkripsi untuk data yang rahasia dan membantu menjamin integritas informasi yang dipertukarkan antara website dan web browser.**

SSL mengimplementasikan kriptografi kunci-publik dengan menggunakan algoritma RSA dan sertifikat digital untuk mengotentikasi server di dalam transaksi dan untuk melindungi informasi rahasia yang dikirim antara dua buah socket. Server selalu diotentikasi, sedangkan client tidak harus diotentikasi oleh server. Server diotentikasi agar client yakin bahwa ia mengakses situs web yang sah (dan bukan situs web palsu yang menyamar seolah-olah benar ia adalah server yang asli). Client tidak harus diotentikasi oleh server karena kebanyakan server menganggap nomor kartu kredit sudah cukup untuk mengotentikasi client.

Internet banking merupakan sebuah layanan perbankan dengan media komunikasi internet yang disediakan oleh bank untuk para nasabahnya. Dengan layanan ini, para nasabahnya dapat melakukan berbagai aktivitas perbankan tanpa perlu beranjak dari tempat duduk. Mulai dari pengecekkan saldo, transfer uang, hingga pembelian pulsa telepon pun sudah dapat dilakukan.

***Index Terms* — Internet banking, RSA, SSL**

I. PENDAHULUAN

Internet telah menjadi bagian yang tidak dapat dipisahkan dari kehidupan manusia dewasa ini. Segala aspek yang berhubungan dengan sistem informasi sudah beralih dari yang tadinya masih menggunakan pencatatan manual menjadi model elektronik di mana data dan informasi disimpan dalam bentuk digital dan didistribusikan dengan media jaringan atau internet. Hal ini meningkatkan kemudahan orang dalam berkomunikasi maupun bertransaksi, misalnya saja untuk transaksi keuangan.

Belasan tahun yang lalu, segala transaksi keuangan harus dilakukan dengan mendatangi bank tempat nasabah mena-bung. Namun dengan adanya teknologi seperti *internet banking*, *mobile banking*, dan SMS *banking*, nasabah sangat dimudahkan karena bisa melakukan transaksi keuangan di manapun dan kapanpun.

Sayangnya dengan kemudahan itu, ancaman serangan terhadap internet banking juga sangat besar, mulai dari ancaman di sisi *client* apabila ada *keylogger*, *trojan*, atau *spyware* yang terdapat pada komputer nasabah, ancaman selama data dikirimkan dari client ke server dengan *sniffer* sehingga memung-kinkan penyadapan data yang dikirim, hingga ancaman pada sisi *server*.

Oleh karena itu, kriptografi memiliki peran dalam menjaga keamanan informasi yang berlangsung dalam proses transaksi pada *internet banking* ini, salah satunya adalah dengan SSL (*secure socket layer*). SSL digunakan untuk menyandikan komunikasi antara web browser nasabah dengan web server bank. Cirinya,situs bank yang diakses memiliki alamat https (s singkatan dari secure), bukan http seperti situs-situs biasa.

Penyandian menggunakan sertifikat SSL 128 bit yang dikeluarkan oleh lembaga resmi seperti Cybertrust atau Verisign. Sertifikat ini mempunyai masa berlaku satu atau dua tahun. Setelah masa berlaku habis, maka bank akan memperbarui dan menggunakan sertifikat baru.

II. DASAR TEORI

Socket Secure Layer (*SSL*) adalah protokol yang digunakan untuk *browsing web* secara aman. Dalam hal ini, SSL bertindak sebagai protokol yang mengamankan komunikasi antara *client* dan *server*. Protokol ini memfasilitasi penggunaan enkripsi untuk data yang rahasia dan membantu menjamin integritas informasi yang dipertukarkan antara *website* dan *web browser*.

SSL beroperasi antara protokol komunikasi *TCP / IP* (*Transmission Control Protocol/Internet Protocol*) dan aplikasi. *SSL* seolah-olah berlaku sebagai lapisan (*layer*) baru antara lapisan transpor (*TCP*) dan lapisan aplikasi. *TCP / IP* adalah standard protokol yang digunakan untuk menghubungkan komputer dan jaringan dengan jaringan dari jaringan yang lebih besar, yaitu internet.

A. Cara kerja TCP / IP (tanpa SSL)

Kebanyakan transmisi pesan di internet dikirim sebagai kumpulan potongan pesan yang disebut **paket**. Pada sisi pengiriman, paket-paket dari sebuah pesan diberi nomor secara sekuensial. *IP* bertanggung jawab untuk merutekan paket (lintasan yang dilalui oleh paket), dan setiap paket mungkin menempuh rute yang berbeda di dalam internet, Tujuan sebuah paket ditentukan oleh *IP address*, yaitu nomor yang digunakan untuk mengidentifikasi sebuah komputer pada sebuah jaringan.

Pada sisi penerima, *TCP* memastikan bahwa suatu paket sudah sampai, menyusunnya sesuai nomor urut, dan menentukan apakah paket tiba tanda mengalami perubahan (misalnya berubah karena *physical error* selama transmisi). Jika paket mengalami perubahan atau ada data yang hilang, *TCP* meminta pengiriman ulang. Bila semua paket dari pesan berhasil mencapai *TCP / IP*, pesan tersebut kemudian dilewatkan ke *socket* penerima. *Socket* tersebut menerjemahkan pesan kembali menjadi bentuk yang dibaca oleh aplikasi penerima (contoh aplikasi adalah *HTTP*, *FTP*, *Telnet*).

B. Cara kerja TCP / IP (dengan SSL)

Dari penjelasan di atas dapat dilihat bahwa pada dasarnya *TCP / IP* tidak memiliki pengamanan komunikasi yang bagus. Bahkan *TCP* tidak cukup canggih menentukan bilamana suatu paket berubah karena diubah oleh pihak ketiga (musuh), karena paket yang diubah tersebut dapat dianggap oleh *TCP* sebagai paket yang benar. Pada transaksi yang menggunakan *SSL*, *SSL* membangun hubungan (*connection*) yang aman antara dua *socket*, sehingga pengiriman pesan antara dua entitas dapat dijamin keamanannya.

SSL disusun oleh dua sub-protokol:

1. *SSL handshaking*, yaitu sub-protokol untuk membangun koneksi (kanal) yang aman untuk berkomunikasi,
2. *SSL record*, yaitu sub-protokol yang menggunakan kanal yang sudah aman. *SSL Record* membungkus seluruh data yang dikirim selama koneksi.

SSL mengimplementasikan kriptografi kunci-publik dengan menggunakan algoritma RSA dan sertifikat digital untuk mengotentikasi *server* di dalam transaksi dan untuk melindungi informasi rahasia yang dikirim antara dua buah *socket*. *Server* selalu diotentikasi, sedangkan *client* tidak harus diotentikasi oleh *server*. *Server* diotentikasi agar *client* yakin bahwa ia mengakses situs *web* yang sah (dan bukan situs *web* palsu yang menyamar seolah-olah benar ia adalah *server* yang asli). *Client* tidak harus diotentikasi oleh *server* karena kebanyakan *server* menganggap nomor kartu kredit sudah cukup untuk mengotentikasi *client*.

Perlu dicatat bahwa *SSL* adlaah protokol *client-server*, yang dalam hal ini *web browser* adalah *client* dan *website* adalah *server*. *Client* yang memulai komunikasi, sedangkan *server* memberi respon terhadap permintaan *client*. Protokol *SSL* tidak bekerja kalau tidak diaktifkan terlebih dahulu (biasanya dengan meng-klik tombol yang disediakan di dalam *web server*).

C. Internet Banking

Internet secara resmi sudah menjadi landasan untuk melakukan bisnis. Ada dua makna atau arti dari internet, yaitu teknologinya dan jaringannya. Teknologi Internet adalah teknologi komunikasi yang berbasisis pada protokol TCP/IP. Saat ini juga teknologi internet mencakup pengguna web browser sebagai user interface. Sementara itu pengertiaan Internet sebagai jaringan adalah internet sebagai salah satu jaringan komputer yang terbesar di dunia. Jaringan Internet sendiri pada mulanya hanya dapat digunakan untuk keperluan akademis (penelitian dan pendidikan). Namun sejak tahun 1995 Internet sudah boleh dipergunakan untuk keperluan bisnis. Sejak saat itulah Internet mulai menjadi media komunikasi data yang populer.

Internet banking merupakan sebuah layanan perbankan dengan media komunikasi internet yang disediakan oleh bank untuk para nasabahnya. Dengan layanan ini, para nasabahnya dapat melakukan berbagai aktivitas perbankan tanpa perlu beranjak dari tempat duduk. Mulai dari pengecekkan saldo, transfer uang, hingga pembelian pulsa telepon pun sudah dapat dilakukan. Berbagai kelebihan yang dapat diperoleh baik nasabah maupun bank dari layanan Internet Banking antara lain:

1. **Business expansion**
   Mempermudah perluasan daerah operasi bank. Dengan Internet banking, bank, 2 layanan perbankan dapat diakses dimana saja dan kapan saja, tanpa perlu membka kantor cabang baru.
2. **Customer loyalty**
   Nasabah akan merasa lebih nyaman untuk melakukan aktivitas perbankannya tanpa harus membuka akun di bank yang berbeda-beda di berbagai tempat.
3. **Revenue & cost improvement**
   Biaya untuk memberikan layanan ini dapa lebih murah dibandingkan dengan membuka kantor cabang baru.
4. **Competitive advantage**
   Dengan membuka layanan Internet Banking, Bank akan memiliki keuntungan lebih dibandingkan dengan kompetitor lain dalam melayani nasabahnya.

Pada intinya, aspek keamanan komputer mempunyai beberapa lingkup yang penting, yaitu:

1. **Privacy & Confidentiality**
   Hal yang paling penting dalam aspek ini adalah usaha untuk menjaga data dan informasi dari pihak yang tidak diperbolehkan mengkasesnya. Privacy lebih mengarah kepada data-data yang sifatnya privat. Sebagai contoh, email pengguna yang tidak boleh dibaca admin. Sedangkan confidentiality

berhubungan dengan data yang diberikan kepada suatu pihak untuk hal tertentu dan hanya diperbolehkan untuk hal itu saja. Contohnya, daftar pelanggan sebuah ISP.

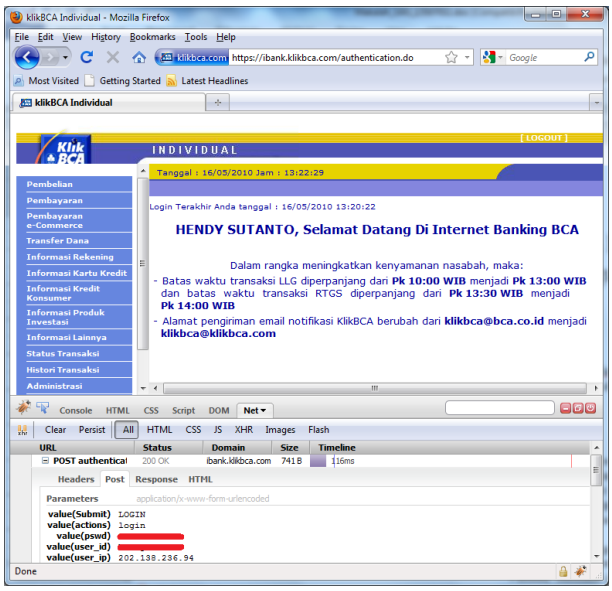
2. **Integrity**
   Aspek ini mengutamakan data atau informasi tidak boleh diakses tanpa seizin pemiliknya. Sebagai contoh, sebuah email yang dikirim pengirim seharusnya tidak dapat dibaca orang lain sebelum sampai ke tujuannya.
3. **Authentication**
   Hal ini menekankan mengenai keaslian suatu data/informasi, termasuk juga pihak yang memberi data atau mengaksesnya tersebut merupakan pihak yang dimaksud. Contohnya seperti penggunaan PIN atau password.
4. **Availability**
   Aspek yang berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sebuah sistem inofrmasi yang diserang dapat menghambat ketersediaan informasi yang diberikan.
5. **Access Control**
   Aspek ini berhubungan dengan cara pengaksesan informasi. Hal ini biasanya berhubungan dengan klasifikasi data (public, private confidential, top secret) & user (guest, admin, top manager, dsb.), mekanisme authentication dan juga privacy. Seringkali dilakukan dengan menggunakan kombinasi user ID/password dengan metode lain seperti kartu atau biometrics.
6. **Non-Repudiation**
   Hal ini menekankan agar sebuah pihak tidak dapat menyangkal telah melakukan transaksi atau pengaksesan data tertentu. 3 Aspek ini sangat penting dalam hal e-commerce. Sebagai contoh, seseorang yang mengirim email pemesanan barang tidak dapat disangkal telah mengirim email tersebut.

III. Serangan dan Celah Keamanan Internet Banking

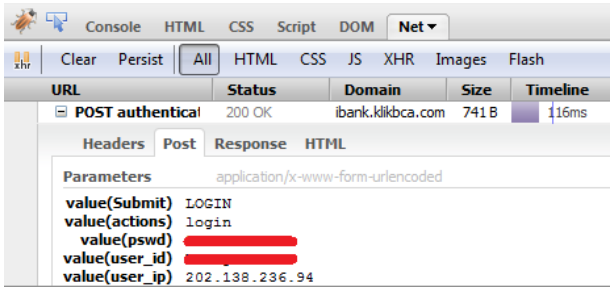
A. Post data menggunakan Mozila Firefox

Penulis melakukan suatu eksperimen untuk mengecek tingkat keamanan situs *internet banking* yang terkenal di Indonesia, yaitu klikbca. Pada halaman *login*, *user* diminta memasukkan username dan password, sekilas *form* ini terlihat sudah cukup aman dan tidak ada orang lain yang dapat mengetahui username dan password kita. Namun dengan bantuan tools *firebug* sebagai *add-on* pada *web browser Mozilla Firefox*, penulis menemukan bahwa *username* dan *password* yang diketikkan tadi bisa dilihat langsung pada *firebug*.

Tips untuk aman dari celah keamanan ini, sebaiknya gunakan *web browser* lain yang lebih aman, dan jangan biarkan ada orang lain yang menggunakan komputer anda.



Gambar 1. *Screenshot* klikBCA dengan Mozilla Firefox dan *add-on firebug*



Gambar 2. Data yang dikirim dari halaman login ke halaman utama klikBCA

B. Typo Site

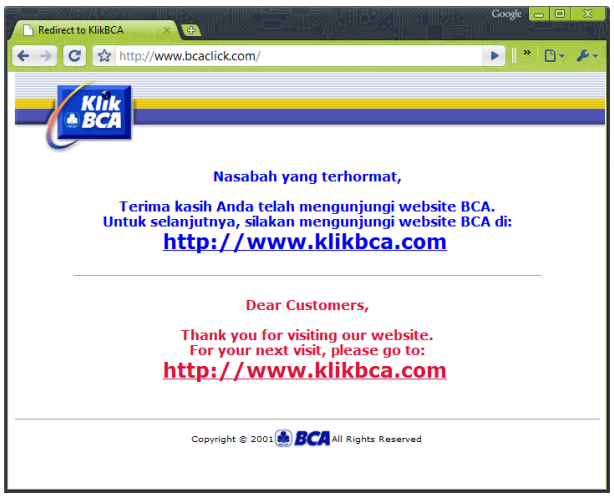
Typo site adalah situs perangkap yang dibuat oleh hacker, yang mengharapkan nasabah salah mengetikkan url situs Internet Banking sehingga navigasi terarah ke situs palsu hacker yang sudah disiapkan sama seperti situs asli.

Contoh salah ketik misal: situs asli adalah bank.com tapi nasabah salah mengetikkan bang.com. Tanpa disadari oleh nasabah, dia akan memasukkan user id dan pin yang akan direkam oleh hacker di situs palsu, kemudian navigasi akan diteruskan ke situs asli. Ciri utama jika kita kesasar di typo site adalah munculnya peringatan dari browser bahwa sertifikat *SSL* tidak valid atau bahkan situs tidak menggunakan https tetapi http biasa.

Tips untuk terhindar dari modus ini adalah tambahkan situs i-bank ke *bookmark* atau *favorite browser*, dan selalu kunjungi dari sana. Jangan pernah mengunjungi situs i-bank dari *link* yang disediakan oleh situs ketiga, seperti toko online, karena beresiko dibelokkan ke situs palsu.

Gambar 3. Halaman asli www.klikbca.com

Gambar 4. Halaman palsu www.bcaclick.com



Gambar 5. Halaman palsu www.bcaclick.com yang sudah ditangani oleh pihak BCA dan di-*redirect* ke halaman yang sebenarnya

B. Keylogging

Teknik ini biasanya digunakan oleh hacker di komputer umum yang penggunanya banyak bergantian. Misalnya di komputer warnet. Hacker akan memasang software keylogger di komputer tersebut, dan berharap ada nasabah internet banking yang mengakses di komputer tersebut. *Software keylogger* atau *keystroke logger* adalah software yang merekam semua karakter keyboard yang ditekan oleh pengguna komputer. Software ini berjalan di background dan biasanya tidak disadari oleh pengguna awam bahwa aktifitasnya sudah direkam oleh orang yang berniat jahat. Di lain waktu si hacker akan melihat hasil jebakannya dan jika beruntung barangkali akan memperoleh user id dan pin nasabah yang kemudian digunakan untuk mengakses layanan *Internet Banking*. Tips supaya terhindar dari modus ini, mudah saja: selalu gunakan komputer pribadi untuk mengakses *Internet Banking*.

Untuk mencegah hardware keylogger, pengguna atau penyedia layanan Internet Banking dapat memaksimalkan fitur *virtual keyboard*. Karena dengan fitur ini, keylogger tidak dapat merekam hasil ketikan karena tidak melalui port atau kabel keyboard. Fitur ini sudah digunakan pada layanan *Internet Banking* CitiBank.

Untuk mencegah perangkat lunak keylogger, dapat menggunakan perangkat lunak antivirus dan firewall yang selalu ter-update. Karena jika tidak ter-*update*, akan percuma. Karena beberapa keylogger dapat mematikan anti virus. Hindari untuk mengakses Internet Banking dari tempat – tempat umum, seperti warnet, dll. Karena aspek keamanan yang biasanya minimalis.

C. Phishing

Phishing adalah cara-cara penipuan yang dilakukan oleh hacker untuk mendapatkan informasi rahasia seorang nasabah seperti user id dan pin. Contohnya misal dengan berpura-pura sebagai pegawai bank yang meminta data-data nasabah dengan berbagai alasan, mengirim *email* kepada nasabah yang berisi *login screen* dan meminta nasabah untuk *login*. Tips untuk terhindar: jangan mudah percaya kepada siapapun yang meminta anda untuk memberikan data, bank tidak pernah meminta hal-hal tersebut melalui *email* atau telepon.

D. Virus dan spyware

Belakangan pernah ditemukan virus yang jika menginfeksi komputer korban, akan memata-matai komputer korban, dan akan mengirimkan data penting korban ke pembuat virus/spyware. Tips: selalu update antivirus dan selalu berhati-hati saat menjelajah internet dan menerima attachment email tak dikenal.

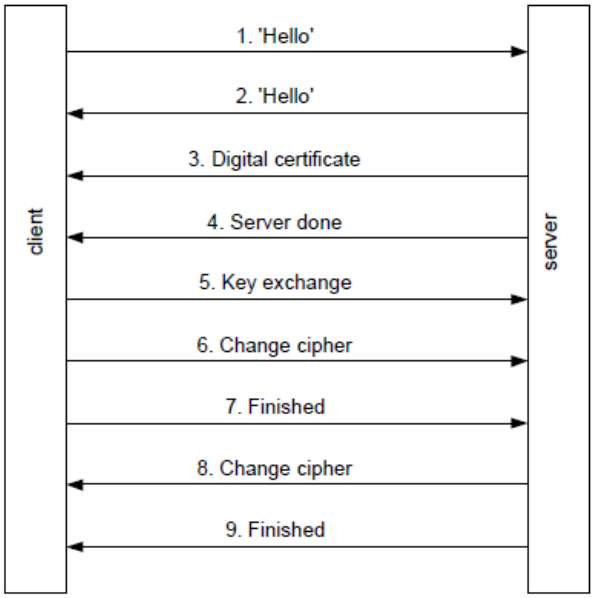
IV. CARA KERJA SSL

Seperti yang sudah dijelaskan pada teori singkat, *SSL* disusun oleh dua buah sub-protokol, yakni *SSL handshaking* dan *SSL record*.

A. Sub-protokol handshaking

Sub-protokol handshaking diperlihatkan pada Gambar 6. Dari gambar tersebut terlihat bahwa SSL dimulai dengan pengiriman pesan Hello dari client ke server (1). Server merespon dengan mengirim pesan Hello (2) dan sertifikat digital ke client untuk otentikasi (3).

Sertifikat digital berisi kunci publik server. Di dalam browser client terdapat daftar CA yang dipercaya. Jika sertifikat digital ditandatangi oleh salah satu CA di dalam daftar tersebut, maka client dapat memverifikasi kunci publik server. Setelah proses otentikasi selesai, server mengirimkan pesan server done (4) kepada client.



Gambar 6. Sub-protokol handshaking untuk membangun koneksi yang aman

Selanjutnya, client dan server menyepakati session key untuk melanjutkan transaksi melalui proses yang disebut keynexchange (5). Session key adalah kunci rahasia yang digunakan selama transaksi. Nantinya, komunikasi antara client dan server dilakukan dengan menggunakan session key ini. Data yang akan ditansmisikan dienkripsi terlebih dahulu dengan session key melalui protokol TCP/IP.

Proses exchange key diawali dengan client nilai acak 384-bit yang disebut premater key kepada server. Nilai acak ini dikirim dalam bentuk terenkripsi (dienkripsi dengan kunci publik server). Melalui perhitungan yang cukup kompleks, client dan server menghitung session key yang diturunkan dari premaster key.

Setelah pertukaran kunci, client dan server menyepakati algoritma enkripsi (6). SSL mendukung banyak algoritma enkripsi, antara lain DES, IDEA, RC2, dan RC4. Sedangkan untuk fungsi hash, SSL mendukung algoritma SHA dan MD5.

Client mengirim pesan bahwa bahwa ia sudah selesai membangun sub-protokol (pesan 7). Server merespon client dengan mengirim pesan 8 dan 9.

Sampai di sini, proses pembentukan kanal yang aman sudah selesai. Bila sub-protokol ini sudah terbentuk, maka http:// pada URL berubah menjadi https:// (http secure)

Proses SSL yang cukup panjang ini sistem menjadi lambat. Oleh karena itu, SSL diaktifkan hanya jika client memerlukan transmisi pesan yang benar-benar aman.

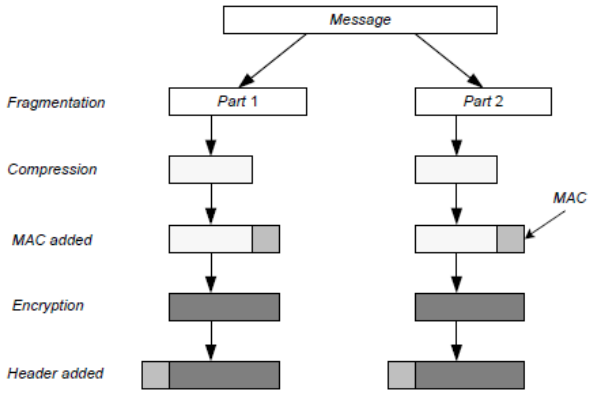
B. Sub-protokol record

Setelah kanal yang aman terbentuk, client dan server menggunakannya untuk menjalankan sub-protokol kedua (SSL record) untuk saling berkirim pesan. Misalnya client mengirim HTTP request ke server, dan server menjawab dengan mengirim HTTP response.

Pesan dari client ke server (dan sebaliknya) dikirim dalam bentuk terenkripsi (pesan dienkripsi dengan menggunakan session key). Tetapi, sebelum pesan dikirim dengan TCP/IP, protokol SSL melakukan proses pembungkusan data sebagai berikut:

1. Pesan dipecah menjadi sejumlah blok yang masing-masing panjangnya 16 KB; setiap blok diberi nomor urut sekuensial.
2. Setiap blok kemudian dikompresi, lalu hasil kompresi disambung (concate) dengan session key;
3. Kemudian, hasil dari langkah 2 di atas di-hash dengan algoritma MD5 (atau algoritma hash lain yang disepakati). Nilai hash ini ditambahkan ke setiap blok sebagai MAC (Message Authentication Code). Jadi, MAC dihitung sebagai berikut: MAC = Hash(session key, compressed data block)
4. Hasil dari langkah 3 kemudian dienkripsi dengan algoritma kriptografi simetri (misalnya RC4).
5. Terakhir, hasil dari langkah 4 diberi header (2 atau 3 byte), baru kemudian dikirim melalui koneksi TCP/IP aman yang terbentuk sebelumnya.

Proses pembungkusan pesan oleh sub-protokol SSL record diperlihatkan pada Gambar 7.



Gambar 6. Pembungkusan pesan oleh SSL record

Setelah data sampai di tempat penerima, sub-protokol SSL ini melakukan proses berkebalikan: mendekripsi data yang diterima, mengotentikasinya (dengan MAC), mendekompresinya, lalu merakitnya.

Meskipun SSL melindungi informasi yang dikirim melalui internet, tetapi ia tidak melindungi informasi yang sudah disimpan di dalam server pedagang (merchant). Bila pedagang online menerima informasi kartu kredit atas suatu pesanan barang, informasi tersebut mungkin di-dekripsi dan disimpan di dalam server pedagang sampai pesanan barang diantar. Jika server tidak aman dan data di dalamnya tidak dienkripsi, pihak yang tidak berhak dapat aja mengakses informasi rahasia tersebut.

V. KESIMPULAN

Internet banking yang sudah sangat terkenal di kalangan masyarakat, ternyata tidak seaman itu, begitu banyak celah keamanan mulai dari sisi pengguna, sisi client, sisi server, maupun sisi jaringan. Meskipun pihak bank telah berusaha meningkatkan keamanan internet bankingnya dengan menggunakan token (seperti keyBCA) dan menggunakan SSL pada situs internet bankingnya, kejahatan cyber yang dilakukan oleh para hacker tidak henti-hentinya semakin meningkat dalam hal kualitas maupun kuantitas. Maraknya kegiatan phishing maupun pembuatan situs palsu dengan alamat situs yang sangat mirip merupakan salah satu bukti nyatanya.

VII. UCAPAN TERIMA KASIH

Penulis mengucapkan banyak terima kasih kepada seluruh pihak yang terlibat dalam pembuatan makalah ini. Pertama-tama kepada Bapak Rinaldi Munir selaku dosen pengajar mata kuliah IF3058 Kriptografi, bimbingan dan ajaran beliau menjadi dasar utama terselesaikannya makalah ini. Tidak lupa penulis juga mengucapkan terima kasih kepada semua pihak yang menjadi referensi makalah ini.

REFERENSI

[1] Munir, Rinaldi, "Kriptografi", Institut Teknologi Bandung, 2009.
[2] http://www.cert.or.id/~budi/articles/internet-banking-bi-1.pdf
tanggal akses : 14 Mei 2010
[3] http://www.klikbca.com/corporate/learn.html?p=264
tanggal akses : 15 Mei 2010
[4] http://dhidik.wordpress.com/2009/04/14/keamanan-internet-banking/
tanggal akses : 15 Mei 2010
[5] http://go-kerja.com/aplikasi-keamanan-internet-pada-internet-banking/
tanggal akses : 16 Mei 2010
[6] http://rizyasanjaya.blogspot.com/2010/02/aspek-keamanan-internet-banking.html
tanggal akses : 16 Mei 2010
[7] http://mamanatrixie.multiply.com/photos/album/79#
tanggal akses : 16 Mei 2010

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 16 Mei 2010

Hendy Sutanto
13507011