Analisis Keamanan Internet Banking Bank Mandiri

Fata Mukhlish[1]

Sekolah Teknik Elektro dan Informatika
Program Studi Teknik Informatika
Institut Teknologi Bandung
Jl. Ganesha 10 Bandung 40132

E-mail : if14084@students.if.itb.ac.id[1]

Abstraksi

Berbagai layanan perbankan diberikan Bank kepada nasabahnya demi kepuasan pelanggan. Salah satu layanan yang mulai banyak dilirik dewasa ini adalah layanan Internet Banking. Dengan layanan ini, nasabah dapat melakukan berbagai macam transaksi perbankan dengan lebih mudah, hanya dengan koneksi internet semata. Hal ini mempermudah para nasabah, terutama mereka yang selalu sibuk, dalam mengelola keuangan mereka.
Penggunaan akses internet dalam layanan ini mengharuskan keamanan data selalu terjaga dari pihak yang tidak bertanggung jawab. Oleh karena itu, layanan jenis ini menggunakan berbagai metode keamanan untuk menjaga privasi dan data nasabah. Pengamanan yang dilakukan biasanya meliputi penggunaan Secure Socket Layer (SSL, kriptografi Kunci Publik, dan Digital Signature. Namun, apakah dengan semua pengaman ini layanan ini sudah 100% aman?
Dalam makalah ini, penulis akan menganalisis keamanan data, metode yang digunakan dalam Internet Banking Bank Mandiri. Penulis juga akan melakukan pengujian terhadap keamanan data yang diterapkan pada layanan Internet Banking ini. Sehingga pada akhir makalah ini, akan disimpulkan berdasarkan pengujian yang dilakukan, mengenai kualitas pengamanan yang diterapkan pada layanan ini.

***Kata kunci** : internet banking, keamanan, Mandiri, keylogger, active sniffing, passive sniffing*

1. Pendahuluan

Di era ini, teknologi internet hampir mulai menjadi penggunaan yang wajib bagi segala aspek kehidupan. Begitu juga di dunia perbankan, penggunaan teknologi internet telah menjadi standar *de facto*. Dengan teknologi inilah bank dapat dengan mudah mengelola segala kebutuhan nasabah nya dengan lebih baik. Salah satunya dengan diberikannya sebuah layanan yang bernama Internet Banking.
Layanan Internet Banking merupakan salah satu jenis layanan yang disediakan oleh Bank. Layanan ini lahir dari tuntutan persaingan dunia perbankan dalam menjaring nasabah, selain itu juga merupakan salah satu keinginan dari nasabah itu sendiri yang menginginkan layanan perbankan yang mudah dan cepat, tersedia setiap saat, terjangkau, serta nyaman..
Akan tetapi, dibalik segala kenyamanan dan kemudahan yang diberikan layanan ini ada sebuah aspek yang harus sangat diperhatikan, yaitu aspek keamanan. Ernst & Young dalam sebuah survey mengenai Information Security mengemukakan bahwa 66% responden mengatakan *security* dan *privacy* merupakan aspek penghambat lebih besarnya penggunaan layanan yang berbasis *e-commerce* [2]. Banyak para nasabah masih merasa ragu untuk bertransaksi dengan menggunakan internet banking karena masih sangsi dengan keamanannya.
Dalam makalah ini akan dianalisis keamanan Internet Banking Bank Mandiri, salah satu layanan internet banking yang keamanannya sudah cukup baik.

2. Internet Banking

2.1. Deskripsi Singkat

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.

2.2. Kelebihan

Berbagai kelebihan yang dapat diperoleh baik nasabah maupun bank dari layanan Internet Banking antara lain:

a. **Business expansion**
   Mempermudah perluasan daerah operasi bank. Dengan Internet banking, bank,

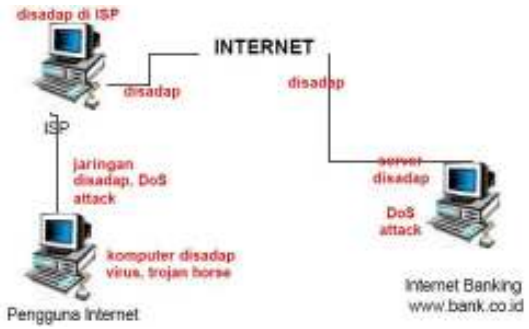
layanan perbankan dapat diakses dimana saja dan kapan saja, tanpa perlu membka kantor cabang baru.

b. **Customer loyalty**
   Nasabah akan merasa lebih nyaman untuk melakukan aktivitas perbankannya tanpa harus membuka akun di bank yang berbeda-beda I berbagai tempat.
c. **Revenue & cost improvement**
   Biaya untuk memberikan layanan ini dapa lebih murah dibandingkan dengan membuka kantor cabang baru.
d. **Competitive advantage**
   Dengan membuka layanan Internet Banking, Bank akan memiliki keuntungan lebih dibandingkan dengan kompetitor lain dalam melayani nasabahnya.
e. **New Business Model**
   Layanan ini memungkinkan adanya model bisnis yang baru.

3. Keamanan Internet

3.1. Gambaran Umum

Secara umum, hubungan koneksi internet dengan pengguna layanan internet Banking dapat dilihat pada gambar berikut:



Gambar 1: Kerawanan Internet

Dapat dilihat pada gambar 1, pengguna terhubung dengan jaringan internet melalui layanan *Internet Service Provider* (ISP). Biasanya, koneksi menggunakan modem, DSL, kabel modem, *wireless*, maupun dengan *leased line*. Lalu ISP akan menghubungakan pengguna ke internet melalui penyedia jaringan (*network provider*). Hal ini juga berlaku pada layanan Internet Banking. Server akan terhubung ke internet melalui ISP atau penyedia jaringan lainnya.

Dari gambar 1, dapat ditunjukkan pula potensi celah keamanan yang yang dapat terjadi. Dari sisi pengguna, komputer miliknya dapat disisipkan virus atau *Trojan* sehingga data – data di dalamnya dapat diubah atau diambil. Dari sisi ISP, apabila sistem keamanannya rentan, maka seorang *cracker* dapat menbobolnya dan dapat mengambil data pelanggan ISPnya. Dari sisi penyedia layanan Internet Banking pun juga terdapat potensi celah keamanan. Salah satu yang terjadi kasus di Amerika seorang *cracker* menjebol institusi keuangan dan mengambil data nasabah dari berbagai bank. Begitu pula dari sisi jalur ISP dan pengguna, biasanya hal ini terjadi di tempat umum, seperti warnet. Pengguna warnet dapat disadap informasinya dari pemilik warnet yang tidak bertanggung jawab.

3.2. Aspek Keamanan

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

a. **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.
b. **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.
c. **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*.
d. **Availability**
   Aspek yang berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sebuah sistem inofrmasi yang diserang dapat menghambat ketersediaan informasi yang diberikan.
e. **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.
f. **Non-Repudiation**
   Hal ini menekankan agar sebuah pihak tidak dapat menyangkal telah melakukan transaksi atau pengaksesan data tertentu.

Aspek ini sangat penting dalam hal *e-commerce*. Sebagai contoh, seseorang yang mengirim email pemesanan barang tidak dapat disangkal telah mengirim email tersebut.

4. Internet Banking Mandiri

4.1. Prosedur Pengaksesan Layanan

Untuk dapat menikmati layanan Internet Banking Mandiri, seorang nasabah harus mengikuti prosedur berikut:

a. Melakukan pendaftaran awal yang dapat dilakukan di ATM atau di Kantor Cabang Mandiri.
b. Nasabah akan mendapatkan Token PIN Mandiri, sebuah alat PIN *generator* dinamis yang digunakan untuk aktivasi setiap aktivitas perbankan menggunakan Internet Banking.
c. Melakukan aktivasi Internet Banking Mandiri. Dilakukan pada situs resmi Bank Mandiri.
d. Nasabah akan mendapatkan *user ID* dan PIN yang dibuat pada langkah c. Nasabah sudah dapat login ke layanan, untuk melakukan aktivasi Token PIN Mandiri.

4.2. Metode Keamanan

Layanan ini menggunakan beberapa metode keamanan terkini seperti:

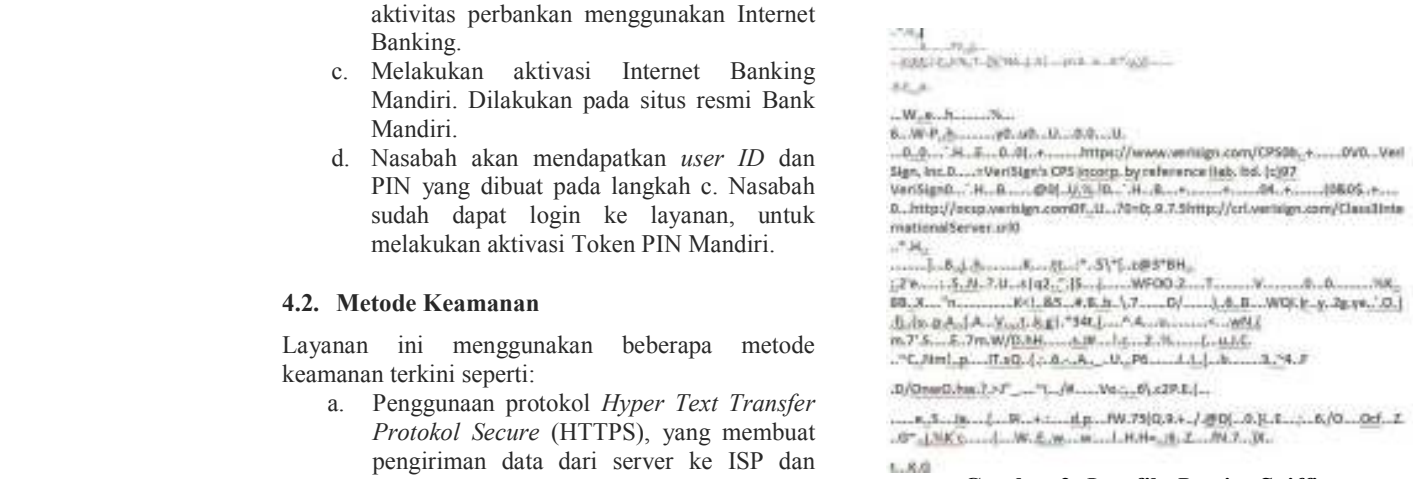
a. Penggunaan protokol *Hyper Text Transfer Protokol Secure* (HTTPS), yang membuat pengiriman data dari server ke ISP dan klien berupa data acak yang terenkripsi.
b. Penggunaan teknologi enkripsi *Secure Socket Layer* (SSL) 128 bit, dari Verisign. Dengan SSL inilah, transfer data yang terjadi harus melalui enkripsi SSL pada komunikasi tingkat *socket*.
c. Penggunaan *user ID* dan PIN untuk login ke layanan Internet Banking ini.
d. Penggunaan metode *time out session*, yang menyebabkan bila setelah 10 menit nasabah tidak melakukan aktivitas apapun, akses tidak berlaku lagi.
e. Penggunaan PIN Mandiri untuk setiap aktivitas perbankan. PIN ini di-*generate* dari Token PIN Mandiri.

5. Pengujian Keamanan

Secara umum, hal yang paling sering diserang para penyusup untuk masuk ke dalam sebuah situs yang terproteksi adalah dengan mendapatkan akses masuknya, atau sisi Autentikasi. Karena hanya dengan mengetahu *user ID* dan *password* kita dapat melakukan apapun yang kita inginkan. Dalam pengujian keamanan layanan ini, penulis akan mencoba melakukannya dengan dua cara, yaitu dengan menggunakan perangkat lunak *keylogger* dan proses *sniffing*.

5.1. *Passive* Snifing

Snifing merupakan sebuah aksi penyadapan paket data yang dikirimkan sebuah computer ke server tertentu. Terdapat dua jenis aksi *sniffing*, yaitu *passive* dan *active*. Perbedaannya hanyalah jika *active* melakukan aksi perubahan paket data dalam melakukan *sniffing*, sedangkan *passive* tidak. Kali ini penulis akan mencoba melakukan *passive sniffing* dengan bantuan perangkat lunak Wireshark.
Dengan perangkat lunak ini, penulis melakukan *sniffing* dan mengambil paket data yang berasal dari korban yang mengakses Internet Banking Mandiri. Dalam log file yang direkam Wireshark, penulis mendapatkan bahwa data yang terambil terenkripsi.



Gambar 2: Log file *Passive Sniffing*

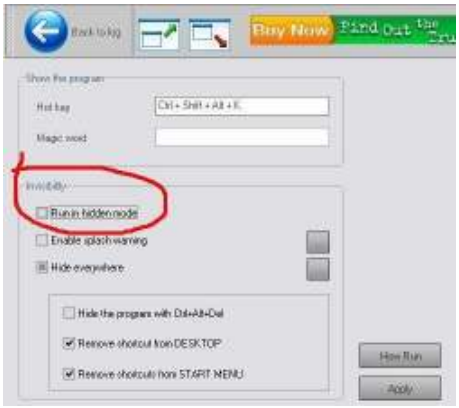
Hal ini disebabkan karena penggunaan SSL dari Internet Banking Mandiri sehingga walaupun paket data terambil, data yang bisa terbaca hanya data acak.

5.2. *Keylogger*

Keylogger merupakan sebuah produk yang dapat mengetahui aktivitas apa saja yang terjadi padakomputer yang isisipinya. Pembuat produk ini berargumen bahwa *keylogger* sangat berguna untuk memantau perkembangan kerja karyawan perusahaan, mengetahui apa yang dilakukan anak ketika brosing di Internet dan sebagainya.
Jenis kelogger ada 2 yaitu, perangkat lunak & hardware. Keduanya mempunyai tujuan yang sama dengan karakteristik yang berbeda. Jenis hardware biasanya dipasang secara fisik pada computer, merekam segala aktivitas yang diketikkan *keyboard*. Sedangkan jenis perangkat lunak, diinstal di sistem operasi kompueter dan dijalankan, biasanya secara tersembunyi. Kali ini penulis akan mencoba untuk merekam aktivitas dengan menggunakan perangkat lunak KGB *Keylogger* ang dapat didapatkan secara

di *www.refog.com*. Perangkat lunak ini dapat berjalan secara hidden mode (tidak terdapat dala *Task Manager*), dan dapat diakses hanya dengan shortcut tertentu. Langkah-langkah yang dilakukan:

a. Melakukan instalasi KGB *Keylogger*.
b. Jalankan *keylogger*, jika perlu dalam hidden mode.



Gambar 3: KGB dalam hidden mode

c. Nyalakan browser untuk mengunjungi situs Bank Mandiri.
d. Login ke Internet Banking Mandiri, dengan *user ID* dan PIN.

Gambar 4: Login Internet Banking

e. Terakhir, buka *keylogger*, dalam lognya akan tercatat *user ID* dan *password* yang sebelumnya dimasukkan.

Gambar 5: Rekaman *user ID* dan *password*

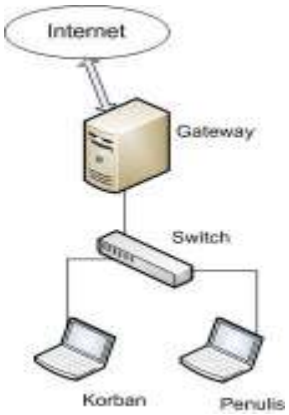
Dapat terlihat bahwa *keylogger* mendapatkan *user ID* dan *password* dengan mudah, yaitu "enygma135" dan "657345". Dengan info ini penyusup dengan mudah langsung mengakses akun nasabah yang dimaksud.

Hal yang lebih berbahaya adalah jika perangkat lunak ini disisipi ke dalam komputer korban. Salah satu caranya dengan mengelabuinya dengan file permainan atau gambar. Hal ini bisa dilakukan dengan perangkat lunak seperti Fearless *Keylogger*, perangkat lunak sejenis dengan KGB *Keylogger* yang dapat membuat file .exe yang dapat disisipi ke komputer korban.

5.3. *Active Sniffing*

Proses ini menggunakan metode serangan *Man-In-The-Middle* dan juga peracunan ARP dengan bantuan perangkat lunak Cain & Abel. Sebagai studi kasus, penguji akan melakukan *sniffing* terhadap komputer korban dengan spesifikasi:

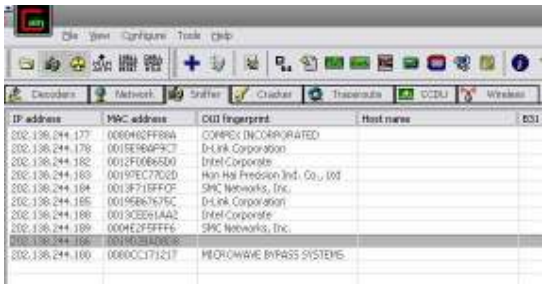
- Korban
  IP *address* : 202.138.244.186
  MAC *address* : 0019D2BADBD8
- Penulis
  IP *address* : 202.138.244.190
  MAC *address* : 0018DEB0DCFB
- Gateway
  IP *address* : 202.138.244.177
  MAC *address* : 0080482FF88A



Gambar 6: Kondisi Jaringan

Untuk langkah-langkahnya sebagai berikut:

a. Aktifkan *sniffer* Cain & Abel untuk menangkap IP *address* komputer korban dan komputer gateway.



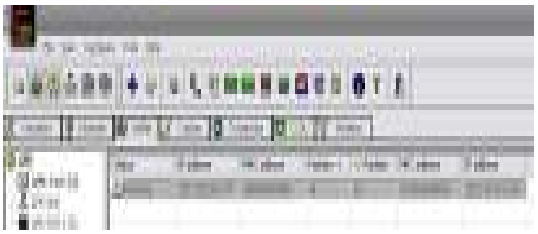
Gambar 7: *Sniffing* IP & MAC *address*

b. Pada komputer penulis, jika diketikkan perintah **arp –a** pada *command prompt* maka akan muncul:

```
Interface: 202.138.244.190 --- 0x3
Internet Address      Physical Address
202.138.244.177       00-80-48-2f-f8-8a
202.138.244.186       00-19-d2-ba-db-d8
```

Hal ini menandakan bahwa komputer penulis telah berkomunikasi dengan korban dan gateway.

c. Selanjutnya, penulis akan melakukan peracunan ARP, sehingga komputer korban yang ingin menghubungi gateway, pada kenyataannya malah menghubungi komputer penulis. Agar tidak diketahui korban, maka penulis akan melakukan *IP forwarding*, sehingga paket komputer ke gateway, akan diteruskan, begitu juga sebaliknya. Penulis melakukan dengan bantuan sniffer Cain & Abel.



Gambar 8: Poisoning ARP oleh Cain & Abel

d. Pada komputer korban, jika diketikkan perintah **arp –a** maka akan muncul:

```
Interface: 202.138.244.186 --- 0x3
Internet Address        Physical Address
202.138.244.177         00-18-DE-B0-DC-FB
202.138.244.190         00-18-DE-B0-DC-FB
```

Terlihat bahwa MAC *address* 202.138.244.177 berubah menjadi 0018DEB0DCFB yang sebenarnya merupakan MAC *address* komputer penulis, bukan komputer gateway.

e. Selanjutnya tinggal menunggu korban mengakses layanan Internet Banking Mandiri. Begitu korban login, maka secara otomatis Cain & Abel akan segera merekam aktivitas ini dan menyimpannya dalam log file yang berbentuk file text. Dan begitu penulis buka log file tersebut,

Gambar 9: Log File Sniffer

Dalam gambar terlihat kata yang diperbesar dan ditebalkan bahwa log file mencatat *user ID* = "ENYGMA135" dan *password* "267898". Dan penulis pun dapat dengan mudah *user ID* dan *password* korban.

Perlu diperhatikan bahwa metode *sniffing* jenis ini dapat dikategorikan sebagai *cyberlaw,* jika penggunaannya tidak pada tempatnya. Penulis melakukan pengujian ini dengan menyadap *user ID* dan *password* akun milik penulis sendiri. Sudah tentu gambar, contoh *user ID* dan *password* yang terdapat dalam makalah ini tidak berlaku. Pengujian hanya dilakukan untuk menunjukkan celah keamanan pada Internet Banking Mandiri.

6. Kesimpulan Pengujian & Saran

6.1. Kesimpulan

Dari kedua pengujian yang dilakukan dapat diambil kesimpulan sebagai berikut:

a. Aksi passive sniffing bahwa paket data yang dikirimkan terenkripsi. Sehingga daa yang terbaca hanya data acak.
b. Dengan *keylogger* informasi penting dapat direkam dengan mudah. Hal ini sangat rawan terjadi jika pengaksesan terjadi di tempat umum (warnet,dll)terutama dengan *keylogger* hardware.
c. Penggunaan *keylogger* dapat dikamuflase dengan file lain (gambar,game) yang mempermudah penyusup mendapatkan data korban.
d. Dengan proses *active sniffing*, penyadapan dapat dilakukan dengan lebih mudah dan tidak mudah terdeteksi.

6.2. Saran

Beberapa saran dari penulis untuk meminimalisir celah keamanan antara lain:

a. 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.
b. 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.
c. Hindari untuk mengakses Internet Banking dari tempat – tempat umum, seperti warnet, dll. Karena aspek keamanan yang biasanya minimalis.

d. Untuk mencegah terjadinya poisoning ARP, maka solusi yang dapat dilakukan dengan mengimplementasi security pada switch, tetapi hanya switch manageable yang dapat melakukannya, bukan switch jenis biasa.
e. Cara lain untuk mencegah poisoning ARP adalah dengan mencegah ARP cache pada komputer berubah, dengan cara mengubahnya menjadi ARP cache statik. Caranya dapat menggunakan perintah **arp –s** pada *command prompt*.
f. Untuk meminimalisir terjadinya proses *sniffing*, gunakan protokol yang mengenkripsi data pada transfer datanya seperti HTTPS, IPSec, SMB Signing, dll.

Semua saran diatas sama sekali tidak menjamin bahwa keamanan menggunakan Internet Banking akan selalu aman 100%. Saran hanya dilakukan untuk meminimalisir celah keamanan yang berpotensi terjadi.

7. Daftar Referensi

[1] Munir, Rinaldi, *Kriptografi*, Institut Teknologi Bandung, 2006.

[2] Rahardjo, Budi, *Keamanan Sistem Informasi Berbasis Internet*, PT Insan Infonesia, PT INDOCISC, 1998-2005.

[3] Rahardjo, Budi, *Aspek Teknologi dan Keamanan dalam Internet Banking*, PT INDOCISC, 2001.

[4] http://free.vlsm.org/v17/com/ictwatch/paper/paper009.htm

[5] http://www.bankmandiri.co.id

[6] S'to, Seni Teknik Hacking 2, Jasakom, 2007

[7] http://www.verisign.com/ssl/ssl-information-center/