

ASPEK TEKNOLOGI DAN KEAMANAN DALAM INTERNET BANKING¹

Budi Rahardjo²
PT INDOCISC – <http://www.indocisc.com>
Email: budi@indocisc.com
Agustus 2001

Dunia Perbankan tidak berbeda dengan industri lainnya dimana teknologi Internet mulai menjadi merasuk dan bahkan sebagian sudah menjadi standar *de facto*. Internet Banking mulai muncul sebagai salah satu servis dari Bank. Servis ini mulai menjadi tuntutan dari sebagian nasabah bank, sama halnya dengan servis ATM dan phone banking. Akan aneh jika sebuah bank tidak memiliki ATM. Demikian pula tidak lama lagi akan aneh jika sebuah bank tidak memiliki Internet Banking meskipun jumlah pengguna Internet di Indonesia masih sedikit.

Tuntutan ini datangnya dari nasabah yang menginginkan servis cepat, tersedia setiap saat (24 jam/hari, 7 hari/minggu), nyaman, dan murah. Hal ini dapat diberikan oleh layanan Internet Banking. Namun dibalik kemudahan dan kenyamanan tersebut terdapat aspek keamanan. Dalam sebuah survey oleh Ernst & Young tentang *Information Security* diperoleh informasi bahwa 66% responden mengatakan *security* dan *privacy* merupakan penghambat lebih besarnya penggunaan *electronic commerce*.

Di lain pihak, apabila sebuah bank tidak melakukan internet banking, maka dia mengambil resiko untuk tidak berpartisipasi. Internet banking memberikan beberapa keuntungan yang lebih besar dibandingkan resikonya. Adapun keuntungan tersebut antara lain:

- *Business expansion*. Dahulu sebuah bank harus memiliki sebuah kantor cabang untuk beroperasi di tempat tertentu. Usaha ini memerlukan biaya yang tidak kecil. Kemudian hal ini dipermudah dengan hanya meletakkan mesin ATM sehingga dia dapat hadir di tempat tersebut. Kemudian ada phone banking yang mulai menghilangkan batas fisik dimana nasabah dapat menggunakan telepon untuk melakukan aktivitas perbankannya. Sekarang ada Internet Banking yang lebih mempermudah lagi karena menghilangkan batas ruang dan waktu. Layanan perbankan sebuah bank kecil dapat diakses dari mana saja di seluruh Indonesia, dan bahkan dari seluruh dunia.
- *Customer loyalty*. Nasabah, khususnya yang sering bergerak (mobile), akan merasa lebih nyaman untuk melakukan aktivitas perbankannya tanpa harus membuka account di bank yang berbeda-beda di berbagai tempat. Dia dapat menggunakan satu bank saja.

¹ Materi Seminar Internet Banking di *Banking Research and Regulation Directorate*, Bank Indonesia, "Internet Banking: Implementasi & Tantangannya ke Depan", 13 Agustus 2001.

² Konsultan security pada PT INDOCISC, peneliti pada Pusat Penelitian Antar Universitas bidang Mikroelektronika (PPAUME) ITB.

- *Revenue and cost improvement.* Biaya untuk memberikan layanan perbankan melalui Internet Banking dapat lebih murah daripada membuka kantor cabang.
- *Competitive advantage.* Bank yang tidak memiliki mesin ATM akan sukar berkompetisi dengan bank yang memiliki banyak mesin ATM. Maukah anda membuka account di bank yang tidak memiliki mesin ATM? Demikian pula bank yang memiliki Internet Banking akan memiliki keuntungan dibandingkan dengan bank yang tidak memiliki Internet Banking. Dalam waktu dekat, orang tidak ingin membuka account di bank yang tidak memiliki fasilitas Internet Banking.
- *New business model.* Internet Banking memungkinkan adanya bisnis model yang baru. Layanan perbankan baru dapat diluncurkan melalui web dengan cepat.

Makalah ini akan mengulas aspek teknologi dan keamanan (security) dari Internet Banking.

Teknologi Internet

Internet secara *de facto* sudah menjadi landasan untuk melakukan bisnis.

Ada dua makna atau arti dari “Internet”, yaitu teknologinya dan jaringannya. *Teknologi Internet* adalah teknologi komunikasi yang berbasis kepada protokol TCP/IP. Saat ini juga teknologi Internet mencakup penggunaan web browser sebagai user interface. Sementara itu pengertian *Internet sebagai jaringan* adalah Internet sebagai salah satu jaringan komputer yang terbesar di dunia. (Ada jaringan komputer lain yang bukan Internet, seperti misalnya jaringan privat dari beberapa perusahaan yang besar.)

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.

Beberapa hal yang menyebabkan jaringan dan teknologi Internet populer sebagai media komunikasi data

- Cakupannya yang luas (seluruh dunia)
- Implementasinya relatif lebih murah dibandingkan dengan menggunakan jaringan atau fasilitas lainnya, misalnya menggunakan *Value Added Network (VAN)* sendiri. Untuk menjadi bagian dari Internet kita cukup dengan hanya menghubungkan sistem ke koneksi Internet terdekat, misalnya melalui *Internet Service Provider (ISP)*. Jika kita menggunakan VAN, maka kita harus menggelar jaringan sendiri (dan ini cukup mahal).
- Teknologi Internet yang terbuka (*open standard*) sehingga tidak tergantung kepada satu vendor tertentu. Implementasi teknologi Internet, TCP/IP, tersedia di semua platform komputer (Microsoft Windows, Apple, UNIX, Linux, dan lain-lainnya).
- Penggunaan web browser mempercepat pengembangan dan peluncuran (*deployment*) aplikasi serta mengurangi *learning curve* dari pengguna. Modal utama dari seorang pemakai adalah kemampuan menggunakan web browser.

- Teknologi Internet juga memungkinkan konvergensi berbagai aplikasi menjadi satu. Sebagai contoh, saat ini telah dimungkinkan untuk mengirimkan data, suara, dan bahkan gambar melalui satu media Internet. Hal ini sering disebut dengan istilah konvergensi. Implikasinya adalah perusahaan dapat menghemat biaya dan dapat mengintegrasikan kesemua layanan dalam satu media.

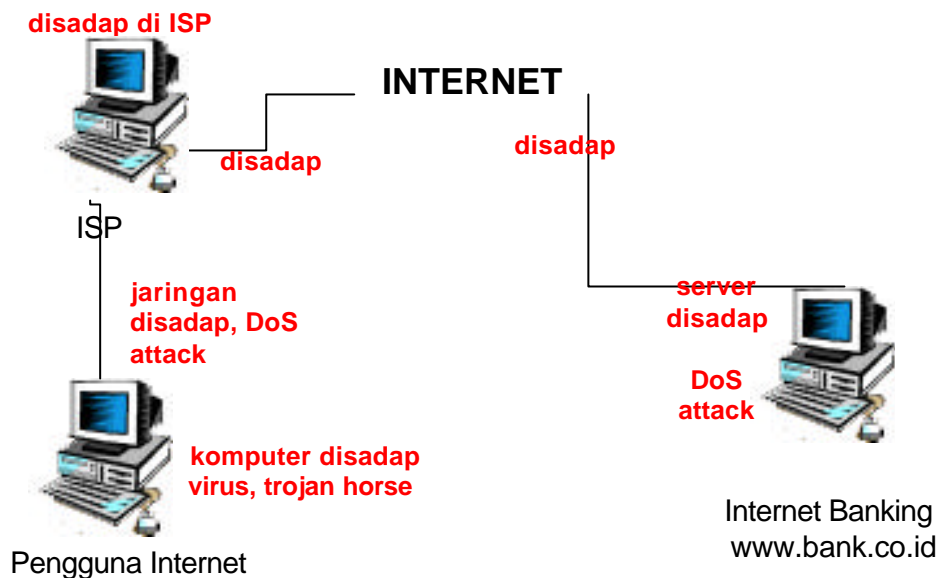
Selain memiliki keuntungan-keuntungan di atas sebetulnya teknologi Internet memiliki beberapa masalah. Beberapa masalah ini antara lain:

- Sifat aplikasi web yang *connectionless*. Banyak aplikasi web-based bersifat *connectionless* sehingga agak sukar untuk aplikasi-aplikasi yang membutuhkan sifat *connection-oriented* seperti aplikasi yang dibutuhkan oleh aplikasi dengan keamanan tinggi. Biasanya aplikasi yang membutuhkan keamanan melakukan *authentication* pada awal sesinya. Kemudian untuk selanjutnya, selama sesi tersebut, pengguna dapat memberikan perintah sesuai dengan level akses yang dimilikinya. Aplikasi semacam ini agak sukar (bukannya tidak bisa, namun lebih sukar) diimplementasikan dalam sistem yang memiliki sifat *connectionless* seperti kebanyakan aplikasi web.
- Tingkat keamanan yang dipertanyakan. Salah satu kendala dari layanan Internet Banking adalah ketidak-percayaan akan amannya layanan ini. Hal ini berlaku secara umum untuk layanan *electronic commerce* (e-commerce). Masalah ini akan dibahas pada bagian terpisah.

Keamanan Internet

Dikarenakan layanan Internet Banking menggunakan Internet sebagai media komunikasi, maka keamanan dari layanan Internet Banking bergantung kepada keamanan dari Internet. Pada bagian ini akan dibahas sedikit tentang keamanan Internet. Penjelasan yang lebih lengkap mengenai topik ini dapat dibaca pada buku-buku yang tertera di bagian Referensi.

Internet pada mulanya dikembangkan di lingkungan akademis (pendidikan dan penelitian). 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 di 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*³ yang beredar saat ini membuktikan bahwa data-data dari harddisk pengguna dapat tersebar ke seluruh dunia melalui email tanpa diketahui oleh pengguna yang bersangkutan.

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 sesama 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.

³ Virus *SirCam* mengirimkan file-file dari harddisk tanpa sepengetahuan pemilik komputer yang terkena virus *SirCam* ini. Implikasinya adalah data-data rahasia (misal data pelanggan, *business proposal/plan*) yang kita simpan dalam komputer dapat bocor.

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.

Selain serangan yang bersifat penyadapan masih banyak jenis serangan lain seperti pemalsuan dan bahkan meniadakan servis (Denial of Service attack). Makalah ini tidak membahas serangan-serangan tersebut meskipun efek yang ditimbulkan oleh serangan tersebut cukup dahsyat juga.

Pengamanan

Tulisan di atas mungkin membuat orang menjadi takut dengan layanan Internet Banking. Pihak nasabah takut accountnya disalahgunakan orang lain. Sementara itu, pihak bank takut membuat lubang keamanan dari sistem yang sudah dimilikinya. Lantas harus bagaimana?

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.

Pengamanan di atas pada prinsipnya merupakan usaha untuk memenuhi aspek keamanan seperti *authentication*, *confidentiality* / *privacy*, *non-repudiation*, dan *availability*. (Karena terbatasnya ruang dari makalah ini, pembaca dipersilahkan membaca buku yang tertera pada bagian referensi.)

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.

Penutup

Lubang keamanan (*security hole*) akan selalu ada. Hal ini bisa diamati dari situs web yang melaporkan adanya lubang keamanan setiap hari!. Namun bisnis tidak dapat berhenti karena adanya potensi lubang keamanan. Seperti halnya sebuah rumah, dia akan tetap memiliki pintu dan jendela meskipun pintu dan jendela ini dapat digunakan oleh pencuri. Yang dapat kita lakukan adalah meningkatkan tingkat kesulitan untuk masuk dengan menggunakan pengamanan-pengamanan, seperti menggunakan kunci (dalam kasus rumah), firewall & IDS (dalam kasus server Internet). Adanya proteksi ini membuat kita dapat hidup dengan lebih baik. Demikian pula, layanan Internet Banking mudah-mudahan dapat memberikan

kenyamanan nasabah dalam melakukan kegiatan perbankannya tanpa mengorbankan sisi keamanannya.

Bahan Bacaan

1. Budi Rahardjo, “Keamanan Sistem Informasi Berbasis Internet”, PT Insan Infonesia, PT INDOCISC, 2001. Buku ini berisi dasar-dasar *security* dan dapat diambil (download) secara gratis dari <http://budi.insan.co.id>
2. Kevin Paulsen, “Mass web banking hack probed: Intruder cracks network handling 300 banks across the U.S.”, 6 Juli 2001. Artikel di Security Focus. <http://www.securityfocus.com/news/222>