IMPLEMENTASI KRIPTOGRAFI PADA E-COMMERCE

Revi Fajar Marta – NIM : 13503005

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail: if13005@students.if.itb.ac.id

Abstrak

Makalah ini membahas tentang implementasi kriptografi pada teknologi e-commerce. E-commerce merupakan sebuah sarana untuk melakukan transaksi keuangan secara online. Sarana ini berkembang pesat sejak awal penggunaannya di tahun 1970an. Saat itu e-commerce hanya berkisar pada dokumen komersial seperti order pembelian atau *invoice* secara elektronik. Kini e-commerce telah mencakup transaksi kartu kredit, enterprise resource planning, dan lain sebagainya.

Salah satu metode pengamanan dalam jaringan adalah penggunaan teknologi Secure Socket Layer (SSL). Teknologi ini memungkinkan client membangun koneksi yang aman dan terenkripsi dengan server. Selain itu ada pula teknologi Sertifikat Digital yang memungkinkan client mengetahui apakah halaman situs yang diaksesnya asli atau palsu. Kedua teknologi ini kemudian disatukan untuk memfasilitasi e-commerce agar aman dan menghindarkan user dari rasa waswas.

Ada beberapa hal yang harus disiapkan untuk mengamankan e-commerce. Dari sisi server adalah ketersediaan tekmologi SSL, Digital Certificate, enkripsi data, dan sebagainya. Untuk dapat menggunakan teknologi ini ada langkah-lankah tertentu yang harus ditempuh. Sementara dari sisi client adalah kesiapan client/browser untuk menandingi kemampuan server, seperti kemampuan browser dalam menjalankan SSL.

Banyak ancaman yang mengintai para pengguna e-commerce. Salah satunya adalah phishing. Kejahatan ini memanfaatkan penggunaan situs palsu untuk menipu pengguna e-commerce sehingga bila si pengguna mengakses situs tersebut informasi-informasi penting dari dirinya dapat dicuri oleh si pelaku kejahatan. Kejahatan ini selain mengandalkan teknologi juga mengandalkan ketidakhati-hatian pengguna dalam mengakses situs e-commerce.

Sebenarnya faktor keamanan e-commerce tidak hanya bergantung pada canggihnya teknologi yang digunakan, tetapi lebih menitikberatkan pada kehati-hatian dan ketelitian pengguna e-commerce dalam menjaga informasi dirinya dan memperhatikan apa saja yang ia akses di internet. Yang menentukan teknologi itu aman atau tidak bukan hanya teknologi yang dipakai, tetapi juga kesiapan sumber daya manusia dalam menggunakannya.

***Kata kunci**: e-commerce, electronic commerce, SSL, Secure Socket Layer, Transport Layer Security, Digital Certificate*.

1. Pendahuluan

Electronic Commerce

Electronic Commerce (disebut juga EC, -commerce, atau ecommerce) utamanya terdiri atas distribusi, pembelian, penjualan, pemasaran, dan jasa atas produk atau jasa melalui system elektronik seperti Interner dan jaringan computer lainnya. Dari sudut pandang industri teknologi informasi e-commerce dapat diartikan aplikasi bisnis elektronik yang ditujukan pada transaksi komersial, dalam konteks ini, dapat melibatkan transfer dana elektronik, *supply chain management*, *e-marketing*, *online marketing*, *online transaction processing*, *electronic data interchange* (EDI), sistem manajemen inventori terotomasi, dan system koleksi data terotomasi. *Electronic commerce* umumnya menggunakan teknologi komunikasi elektronik *World Wide Web*, pada beberapa poin di siklus transaksi, meski tentu saja *electronic commerce* banyak pula bergantung pada teknologi selain *Worl Wide Web*, seperti basis data, *e-mail*, dan teknologi nonkomputer

lainnya, seperti transportasi untuk produsk-produk yang dijual melalui *e-commerce*.

Perkembangan

Pengertian frase "*electronic commerce*" telah berubah dalam 30 tahun terakhir. Pada awalnya, "*electronic commerce*" berarti pemfasilitasan transaksi komersial secara elektronik, biasanya menggunakan teknologi *Electronic Data Interchange* (EDI) dan *Electronic Fund Transfer* (EFT), di mana keduanya diperkenalkan di akhir 1970an, contohnya untuk mengirim dokumen komersial seperti order pembelian atau *invoice* secara elektronik.

Kata "*electronic*" atau "e" pada frase "*e-commerce*" merujuk pada teknologi/system; sementara kata "*commerce*" merujuk pada model bisnis tradisional. E-commerce didefinisikan sebagai set lengkap dari berbagai proses yang mendukung aktivitas komersial/bisnis pada sebuah jaringan. Di tahun 1970an dan 1980an, ini melibatkan juga analisis informasi. Pertumbuhan dan penerimaan kartu kredit, *Automated Teller Machine* (ATM) dan *telephone banking* di era 1980an juga merupakan salah satu bentuk e-commerce. Namun, pada era 1990an ke depan, ini termasuk juga system *enterprise resource planning* (ERP), *data mining*, dan *data warehousing*.

Pada era *dotcom*, muncul aktivitas baru yang disebut "Web Commerce"; pembelian produk barang dan jasa melalui World Wide Web, biasanya dengan koneksi yang aman (HTTPS, protocol server khusus yang mengenkripsi data pemesanan rahasia untuk perlindungan terhadap konsumen) dengan *e-shopping cart* dan layanan pembayaran elektronik, seperti otorisasi pembayaran menggunakan kartu kredit.

Kini, e-commerce mencakup aktivitas dan proses bisnis yang sangat luas, mulai dari e-banking, manufaktur lepas pantai, hingga e-logistics. Kebergantungan yang terus bertumbuh dari industri modern terhadap proses bisnis yang dapat dilakukan secara elektronik memberikan dorongan terhadap pertumbuhan dan perkembangan system pendukungnya, termasuk system backend, aplikasi, dan middleware. Contohnya adalah jaringan broadband dan serat optik, software manajemen supply chain, software customer relationship management, system control inventori, dan software *accounting* keuangan.

Pada saat Web mulai popular di kalangan umum pada tahun 1994, banyak jurnalis dan orang-orang terpelajar meramalkan Bahwa e-commerce akan menjadi salah satu sector ekonomi utama. Namun, butuh sekitar 4 tahun untuk protocol keamanan (seperti HTTPS) untuk dapat berkembang hingga mencukupi kebutuhan serta digunakan secara umum. Kemudian, antara tahun 1998 dan 2000, beberapa bisnis di Amerika Serikat dan Eropa Barat mengembangkan situs-situs web elementer.

Meskipun banyak perusahaan "pure e-commerce" menghilang pada masa kejatuhan dot-com di tahun 200 dan 2001, banyak retailer menyadari bahwa perusahaan tersebut telah mengidentifikasi tempat berharga di dalam pasar dan mulai memasukkan kemampuan e-commerce ke dalam situs-situs mereka. Contohnya, setelah kejatuhan toko online Webvan, dua supermarket tradisional, Albertsons dan Safeway, memulai layanan e-commerce di mana para konsumen dapat memesan produk secara online.

Kemendesakan e-commerce juga secara signifikan menurunkan halangan untuk masuk dalam penjualan berbagai jenis produk; dengan demikian banyak industri rumahan dapat menggunakan fasilitas internet untuk memasarkan dan menjual produk-produknya kepada pembeli.

Sertifikat Digital

Serangan umum yang terjadi pada kunci publik tanpa identitas adalah penyamaran (impersonation attack). Seseorang yang memiliki kunci publik orang laindapat menyamar seolah-olah dialah pemilik kunci itu. Serangan semacam ini adalah masalah yang muncul dari penggunaan kriptografi kunci publik. Contohnya, dalam teknologi e-commerce, pembayaran transaksi dilakkan dengan menggunakan kartu kredit. Pelanggan mengiriman informasi kartu kreditnya yang bersifat rahasia melalui website pedagang online. Selama pengiriman, informasi kartu kredit tersebut dilindungi dengan cara mengenkripsinya dengan kunci publik pedagang online. Bagaimana pelanggan itu memastikan bahwa website pedagang online tersebut memang benar milikpedagan online dan bukan website pihak lain yang menyamar sebagai website pedagang asli dengan tujuan untuk mncuri informasi kartu kredit.

Untuk menjawab masalah di atas, solusinya adalah dengan memberikan sertifikat digital pada kunci publik. Sertifikat digital dikeluarkan (issued) oleh pemegan otoritas sertifikasi (Certification Authority atau CA).

CA biasanya adalah institusi keuangan (seperti bank) yang terpercaya. Sertifikat digital adalah dokumen digital yang berisi informasi sebagai berikut:

1. nama subjek (perusahaan/individu yang disertifikasi)
2. kunci publik si subjek
3. waktu kedaluarsa sertifikat (expire time)
4. informasi relevan lain seperti nomor seri sertifikat, dan lain-lain.

CA membangkitkan nilai hash dari sertifikat digital tersebut (misalnya dengan fungsi hash satu arah MD5 atau SHA), lalu menandatangani nilai hash tersebut dengan menggunakan kunci privat CA.

Contoh sebuah sertifikat digital: Bob membawa kunci publiknya dan mendatangi CA untuk meminta sertifikat digital. CA mengeluarkan sertifikat digital dan menandatangani sertifikat tersebut dengan cara mengenkripsi nilai hash dari kunci publik Bob (atau nilai hash dari sertifikat digital keseluruhan) dengan menggunakan kunci privat CA. Contoh isi sertifikat digital dan tanda tangan digital dari CA kira-kira seperti Gambar 1.

I hereby certify that the public key

12487547268000477FC766E987234AB458DD2342568FF34868763538967676DCA

Belongs to

Bob Anderson

12345 University Avenue

Barkeley, CA234652

e-mail: **bob@barkeley.com**

Expiration Date: 13 Jul 2021

Tanda tangan digital: Nilai hash (SHA) dari sertifikat digital yang dienkripsi dengan menggunakan kunci privat CA.

Gambar 2. Contoh sebuah sertifikat digital.

Jadi, sertifikat digital mengikat kunci publik dengan identitas pemilik kunci publik. Sertifikat ini dapat dianggap sebagai “surat pengantar” dari CA. Supaya sertifikat digital itu dapat diverifikasi, maka kunci publik CA harus diketahui secara luas. Seseorang yang memiliki kunci publik CA dapat memverifikasi bahwa tanda tangan di dalam suatu sertifikat itu sah dank arena itu mendapat jaminan bahwa knci publik di dalam sertifikat itu memang benar. Salah satu CA, VeriSign, Inc. adalah CA yang terkemuka.

Sertifikat digital sendiri tidak rahasia, tersedia secara publik, dan disimpan oleh CA di dalam certificate repositories. Salinan sertifikat tersebut juga dimiliki oleh pemohon sertifikat. Bob mungkin meletakkan sertifikat tersebut di dalam homepage-nya, dengan link ke halaman web yang menyatakan: klik ini untuk melihat sertifikat kunci publikku. Hasil klik akan memperlihatkan sertifikat digital dan tanda tangan dari CA.

Misalkan Alice mengakses homepage Bob untuk mendapatkan kunci publik Bob. Misalkan Carol berhasil memintas (intercept) request Alice (client) ke homepage Bob (server), sehingga request tersebut masuk ke homepage Bob palsu (yang dibuat oleh Carol, tujuan memintas adalah agar Alice mengira Carol adalah Bob, sehingga Carol dapat memperoleh informasi rahasia dariAlice, misalnya kunci). Carol sudah meletakkan sertifikat digitalnya di dalam halaman web palsu,tapi jika Alice membaca sertifikat tersebut dia langsung paham bahwa dirinya sedang tidak berkomunikasi dengan Bob karena identitas Bob tidak terdapat di dalam sertifikat tersebut.

Misalkan Carol berhasil mengubah homepage Bob, mangganti kunci publik Bob di dalam

sertifikat digital dengan kunci publiknya. Tetapi, jika Alice meng-hash sertifikat digital tersebut, dia memperoleh nilai hash yang tidak sama dengan nilai hash yang dihasilkan jika tanda tangan digital diverifikasi dengan kunci publik CA. Karena Carol tidak mempunyai kunci privat CA, maka Carol tidak dapat membangkitkan tanda tangan digital dari sertifikat Bob yang sudah diubah tersebut. Dengan cara ini, Alice dapat meyakini bahwa dia memiliki kunci publik Bob dan bukan kunci publik Carol. Lagipula, skema ini juga tidak membutuhkan CA harus online untk melakukan verifikasi.

Adanya atribut waktu kedaluarsa pada sertifikat digital dimaksudkan agar pengguna mengubah kunci publik (dan kunci privat pasangannya) secara periodic. Makin lama penggunaan kunci, makin besar peluang kunci diserang dan dikriptanalisis. Jika pasangan kunci tersebut diubah, maka sertifikat digital yang lama harus ditarik kembali (revoked). Pada sisi lain, jikakunci privat berhasil diketahui pihak lain sebelum waktu kedaluarsanya, sertifikat digital harus dibatalkan dan ditarik kembali, dan pengguna arus mengganti pasangan kuncinya.

Bagaimana CA memberitahu ke publik bahwa sertifikat digital ditarik? Caranya mudah saja. CA secara periodic mengeluarkan CRL (Certificate Rovocation List) yang berisi nomor seri sertifikat digital yang sudah ditarik. Sertifikat digital yang sudah kedaluarsa otomatis dianggap tidak sah lagi dan ia juga dimasukkan dalam CRL. Dengan cara ini, maka CA tidak perlu memberitahu perubahan sertifikat digital kepada setiap orang.

Sayangnya, keberadaan CRL menyebabkan pengguna yang memakai sertifikat digital harus memiliki CRL untuk memvalidasi apakah sertifikat tersebut telah ditarik. Sebagai alternatif CRL adalah Online Certification Status Protocol (OCSP), yang memvalidasi sertifikat secara real time.

2. Secure Socket Layer (SSL)

Secure Socket Layer merupakan teknologi yang telah lama dipakai dalam jaringan internet. Usianya kini lebih dari sepuluh tahun. SSL merupakan salah satu teknologi yang paling banyak dipakai. SSL adalah teknologi yang matang dan stabil tapi tidak berarti SSL menjadi jawaban bagi semua permasalahan keamanan dalam e-commerce.

Secure Socket Layer (SSL) adalah protocol yang digunakan untuk browsing web secara aman. Dalam hal ini, SSL bertindak sebagai protocol 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 dikembangkan oleh Netscape Communications pada tahun 1994, dan menjadi protokol yang umum digunakan untuk komunikasi aman antara dua computer pada internet. SSL dibangun ke dalam beberapa web browser (termasuk Netscape Communicator dan Internet Explorer). Ada beberapa versi SSL, versi 2 dan versi 3. Namun, versi 3 paling banyak digunakan saat ini.

Untuk memastikan apakah Internet Explorer sudah siap menjalankan protokol SSL, klik dari IE:

Tools → Internet Options → Advanced

Lalu cari pilihan Security, kemudian periksa apakah SSL versi 2.0 atau SSL versi 3.0 telah diberi tanda ceklis (Gambar 2).

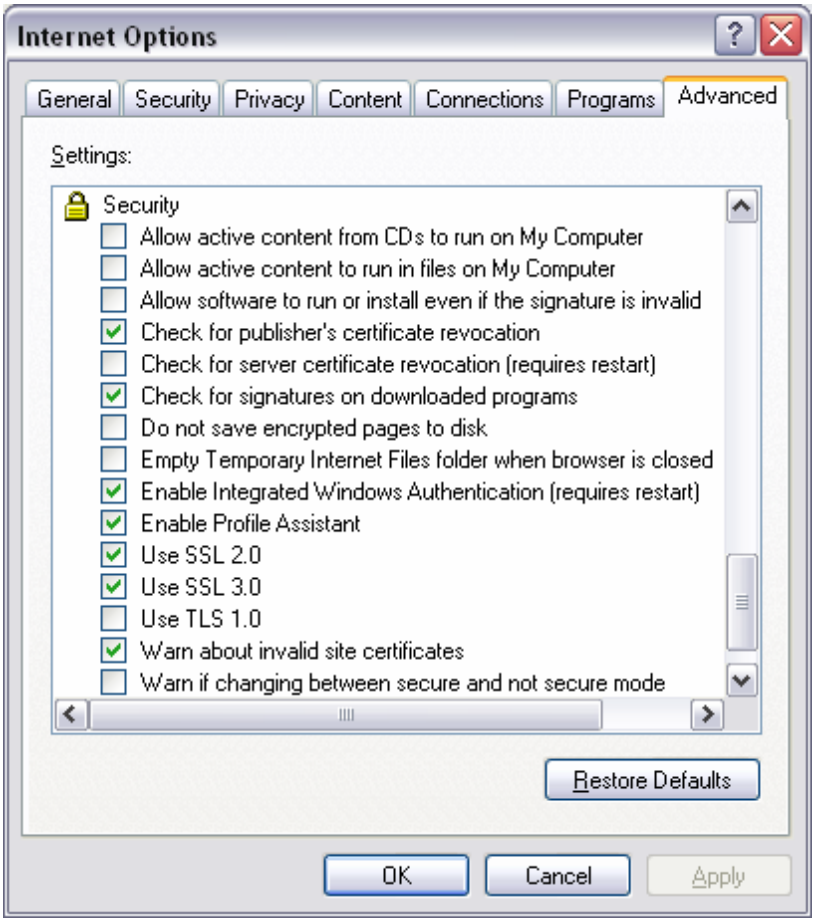
SSL beroperasi antara protokol komunikasi TCP/IP (Transmission Control Protocol/Internet Protocol) dan aplikasi (lihat Gambar 3). SSL seolah-olah berlaku sebagai lapisan (layer) baru antara lapisan Transport (TCP) dan lapisan aplikasi. TCP/IP adalah standard protokol yang digunakan untuk menghubungkan komputer dan jaringan dengan jaringan dari jaringan yang lebih besar, yaitu internet.

Application (HTTP, FTP, Telnet)
Security (SSL)
Transport (TCP)
Network (IP)
Data Link (PPP)
Physical (modem, ADSL, cable TV)

Gambar 3. Lapisan dan protokol untuk browsing dengan SSL.

Di dalam standar komunikasi di internet, pesan dari pengirim dilewatkan melalui socket (port khusus yang menerima dan mengirim informasi dari jaringan dengan mode byte stream). Socket kemudian menerjemahkan

pesan tersebut melalui protokol TCP/IP (Transmission Control Protocol/Internet Protocol).



Gambar 2. Opsi penggunaan SSL pada fitur security di dalam Internet Explorer.

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 sebuahpesan diberi nomor secara sekuensial. IP bertanggung jawab untuk merutekan paket (lintasan yang dilalui paket), dan setiap paket mungkin menempuh rute yang berbeda di dalam internet. Tujuan sebuah paet ditentukan oleh IP address, yaitu nomor yang digunakan untuk mengindentifikasi sebuah komputer pada sebuah jaringan.

Pada sisi penerima, TCP memastikan bahwa suatu paket sudah sampai, menyusunnya sesuai nomor urut, dan menentukan apakah paket tiba tanpa mengalami perubahan (misalnya berubah kasena physical error selama transmisi). Jika paket mengalami perubahan atau ada data yang hilang, TCP meminta pengiriman ulang. Bila semua paket dari pesan berhasil mancapai 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).

Cara Kerja TCP/IP (menggunakan SSL)

Dari penjelasan sebelumnya dapat diketahui 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 public dengan menggunakan algoritma RSA dan sertifikat digital untuk mengotentikasi server di dalam transaksi san 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.

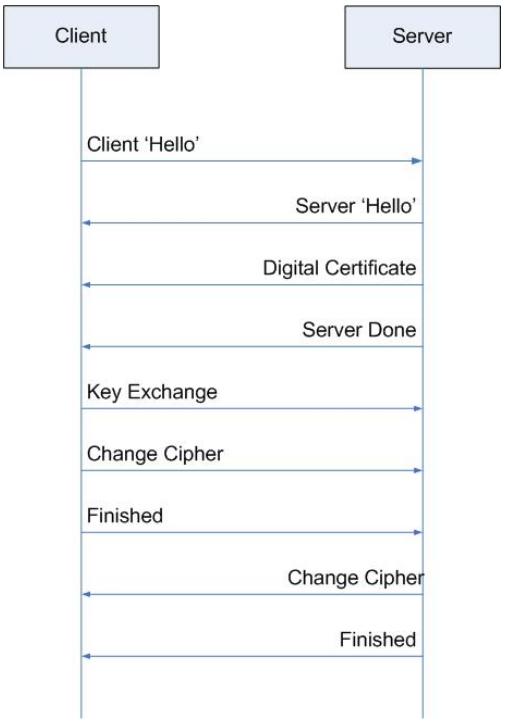
Perlu dicatat bahwa SSL adalah protokol client-server, yang dalam hal ini web browser adalah client dan website adalah server. Client yang memulai komunikasi, sedangkan server memberi respon terhadap permintaan client. Protokol SSL tidak bekerja kalau tidak diaktifkan terlebih dahulu (biasanya dengan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

1. Sub-protokol handshaking

Sub protokol handshaking diperlihatkan pada Gambar 4. Dari gambar tersebut terlihat bahwa SSL dimulai dengan pengiriman pesan Hello dari client ke server. Server merespon dengan mengirim pesan Hello dan sertifikat digital untuk otentikasi.

Sertifikat digital berisi kunci public server. Di dalam browser client terdapat daftar Certification Authority yang dipercaya. Jika sertifikat digital ditandatangani oleh salah satu Certification Authority di dalam daftar tersebut, maka client dapat memverifikasi kunci publik server. Setelah prose otentifikasi selesai, server mengirimkan pesan server done kepada client.

Selanjutnya, client dan server menyepakati session key untuk melanjutkan transaksi melalui proses yang disebut key exchange. Session key adalah kunci rahasia yang digunakan selama transaksi. Nantinya, komunikasi antara client dan server dilakukan dengan menggunakan session key ini. Data yang akan ditransmisikan sienkripsi terlebih dahulu dengan session key melalui protokol TCP/IP. Proses key exchange diawali dengan client mengirim nilai acak 384-bit yang disebut premaster 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. SSL mendukung banyak algoritma enkripsi, antara lain DES, IDEA, RC2, dan RC4. Sedangkan untuk fungsi hash, SSL mendukung algoritma SHA dan MD5.



Gambar 4. Sub-protokol handshaking untuk membangun koneksi yang aman.

Client mengirim pesan bahwa ia sudah selesai mambangun sub-protokol. Server merespon client dengan mengirim pesan 8 dan 9 (change cipher dan finished). Sampai di sini, proses pembentukan kanal yang aman sudah selesai. Bila sub-protokol ini sudah terbentuk, maka http:// pada URL akan berubah menjadi https:// (http secure). Proses SSL yang cukup panjang ini menyebabkan sistem menjadi lambat. Oleh

karena itu, SSL diaktifkan hanya bila client membutuhkan transmisi pesan yang benar-benar aman.

2. Sub-protokol SSL Record

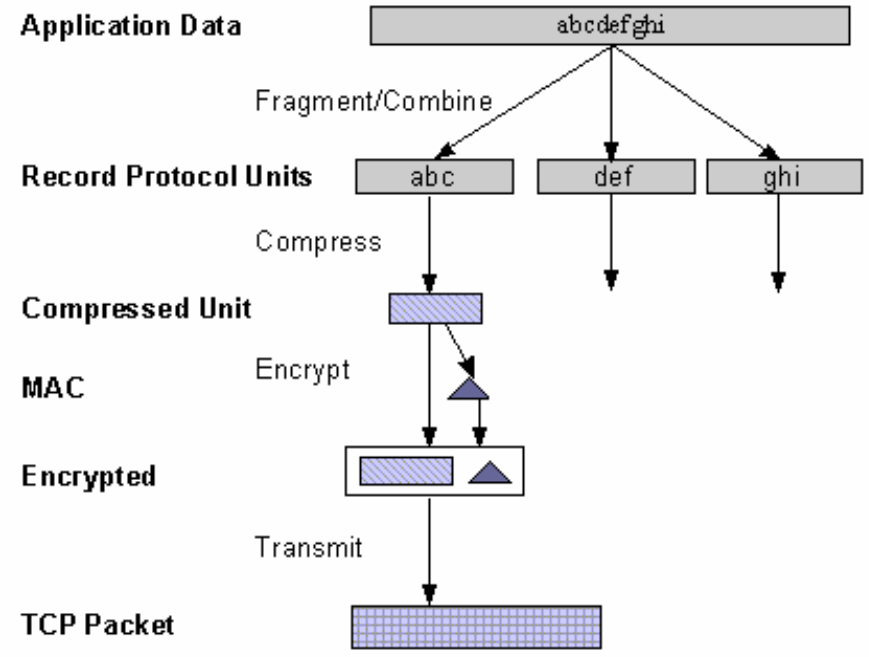
Setelah kanal yang aman terbentuk, client dan server menggunakannya untuk menjalankan sub-protokol kedua (SSL Record) untuk saling berkirim pesan. Misalnya client mengirim HTTP request ke server, dan server menjawab dengan mengirim HTTP response.

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:

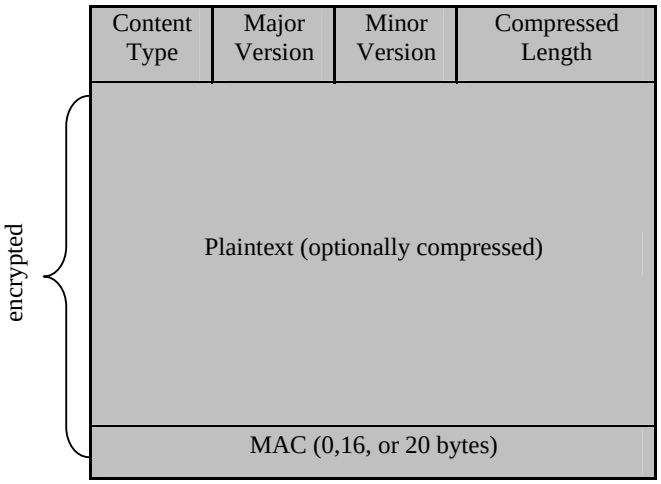
1. Pesan dipecah menjadi sejumlah blok (fragment) yang masing-masing panjangnya 16KB; setiap blok diberi nomor urut sekuensial.
2. Setiap blok kemudian dikompresi, lalu hasil kompresi disambung (concate) dengan session key.
3. kemudian, hasil dari langkah 2 di atas di-hash dengan algoritma MD5 (atau 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 seimetri (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.



Gambar 5. Pembungkusan pesan oleh SSL Record.



Gambar 6. Pembungkusan pesan oleh SSL Record.

Proses pembungkusan pesan oleh sub-protokol SSL record diperlihatkan pada Gambar 5. Format SSL Record ditunjukkan pada Gambar 6.

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 pesanan suatu barang,, informasi tersebut mungkin didekripsi dan disimpan di dalam server pedagang sampai pesanan barang tersebut diantar. Jika server tidak aman dan data di dalamnya tidak dienkripsi, pihak yang tidak berhak dapat saja mengakses informasi rahasia tersebut.

Piranti keras, seperti kartu *peripheral component interconnect* (PCI) yang dirancang untuk digunakan di dalam transaksi SSSL, dapat dipasang ke dalam web server untuk memproses transaksi SSL, sehingga mengurangi waktu pemrosesan dan memungkinkan server bebas mengerjakan tugas-tugas lain.

Pada tahun 1996, Netscape Communications Corp. mengajukan SSL ke IETF (Internet Engineering Task Force) untuk standardisasi. Hasilnya adalah TLS (Transport Layer Security). TLS dijelaskan di dalam RFC2246. TLS dapat dianggap sebagai TLS versi 3.1, dan implementasi pertamanya adalah pada tahun 1999.

Wireless Transprt Layer Security (WTLS) adalah protokol keamanan data untuk Wireless Application Protocol. WAP adalah standar untuk komunikasi nirkabel (wireless) pada telepon mobile dan peralatan nirkabel lainnya. WTLS mengamankan kanal untuk komunikasi antara peralatan nirkabel dan server aplikasi.

3. Implementasi SSL dalam E-Commerce

Dengan fasilitas pertukaran data secara aman yang disediakan oleh SSL, teknologi ini banyak diadopsi oleh berbagai bisnis online di seluruh dunia.

Ada 3 metode dasar untuk membuat sbuah website E-Commerce yang aman menggunakan SSL:

1. Dengan membeli solusi SSL lengkap, termasuk sertifikat, dari vendor yang bonafid. Vendor-vendor ini menyediakan server yang telah dikonfigurasi secara penuh dan pemilik bisnis hanya tinggal membangun situs di atas server tersebut. Beberapa vendor menyediakan pula solusi Web-building.
2. Dengan membeli ”space” dari sebuah web-hosting di salah satu servernya yang elah mnyediakan fasilitas SSL. Ini disebut juga Co-Lo atau jasa hosting Co-Location. Perusahaan-perusahaan ini biasanya memiliki banyak server diberbagai lokasi dan memiliki koneksi internet yang cepat. Co-Lo dapat pula menangani

registrasi domain dan mengurus sertifikat digital.

3. Dengan mambangun solusi sendiri. Di internet banyak Web Server open source dan aplikasi SSL yang tersedia secara gratis. Namun Sertifikat Digital masih harus dibeli secara terpisah.

Piranti-piranti yang dibutuhkan adalah sebagai berikut:

1. Sebuah server untuk difungsikan sebagai Web Server e-commerce.
2. Sebuah server redundant untuk difungsikan sebagai server mirror.
3. Firewall untuk melindungi jaringan internal.
4. Database server untuk menyimpan data untuk web server.
5. Backup device/server untuk menyimpan data backup dari database.
6. Cryptogaphic accelerator card, item opsional dan hanya dibutuhkan untuk menangani request halaman antara 300-500 halaman per detik pada web server. Karena SSL (dan TLS) memiliki fungsi kriptografis, berarti dibutuhkan kekuatan prosesor yang besar untuk menanganinya. Kartu ini dapat mengurangi beban kerja prosesor CPU dan meningkatkan kinerja web server.

Dengan melengkapi berbagai piranti di atas, server telah siap untuk menjalankan SSL. Namun, ada 3 hal lagi yang harus dipersiapkan agar SSL dapat berjalan, yaitu:

1. Sertifikat Digital SSL, dapat dibeli dari berbagai penyedia Sertifikat Digital (Certification Authority) terpercaya, seperti VeriSign, GTE CyberTrust, dan lain-lain.
2. Domain Name, salah satu syarat untuk mendapatkan Sertifikat Digital.
3. IP Address statis, syarat untuk mendapatkan Sertifikat Digital.

Sertifikat Digital tersedia dalam dua jenis, yaitu Sertifikat Digital private dan shared. Sertifikat Digital berjenis private hanya dijual ke perusahaan-perusahaan besar yang telah memiliki kredibilitas tinggi dengan domain name terkualifikasi dan IP address static. Sementara Sertifikat Digital berjenis shared ditujukan untuk perusahaan yang melakukan outsource dalam bisnisnya, seperti menitipkan server di Co-Lo.

4. Berbagai Ancaman pada E-Commerce

Karena berbagai informasi penting seperti identitas, alamat, nomor kartu kredit, dan informasi lainnya dipertukarkan pada fasilitas E-Commerce, teknologi ini pun tidak lepas dari perhatian para penjahat cyber yang berusaha mendapatkan banyak keuntungan meskipun harus melanggar hukum.

Metodenya pun bermacam-macam, seperti penyerangan pada teknologi internet umumnya.

Salah satu yang cukup sering dilakukan adalah *phishing*. Phishing berarti meniru suatu halaman website hingga menyerupai aslinya dengan tujuan mendapatkan informasi penting dari pelanggan situs asli.

Para pelaku phishing membuat situs palsu ini semirip mungkin dengan aslinya. Tidak hanya isinya, nama domainnya pun dibuat mirip hingga pengguna yang salah memasukkan domain ke web browser akan memasuki situs palsu (misalnya memalsukan **http://www.klik-bca.com** dengan membuat situs **http://www.click-bca.com**; perhatikan namanya yang hanya berbeda tipis dan dapat membingungkan masyarakat umum) dan informasi-informasi pribadinya akan dapat jatuh ke tangan pihak-pihak yang tidak berhak.

Cara mencegah kejahatan E-Commerce tidak jauh dengan pencegahan teknologi informasi lainnya, yaitu dengan menitikberatkan pada faktor sumber daya manusia yang menggunakannya. Meskipun manusia dapat mambuat teknologi secanggih-canggihnya dan seaman-amannya, teknologi tersebut akan lumpuh ketika penggunanya tidak berhati-hati dalam menggunakannya.

5. Kesimpulan

E-Commerce saat ini telah menjadi bagian penting dari kehidupan masyarakat, terutama mereka yang telah terbiasa dengan teknologi komputer dan jaringan. Untuk orang-orang yang tinggal jauh dari pusat kota besar atau pusat perbelanjaan, layanan ini bisa menjadi kebutuhan sehari-hari. Barang-barang dapat dipesan dan diantar ke rumah tanpa harus pergi ke pusat kota dan menghabiskan waktu di perjalanan. Ini tidak terbatas pada belanja saja.

Tagihan kartu kredit, telepon, dan transaksi keuangan lainnya dapat dilakukan dari lauyar komputer.

Sayangnya layanan yang menjanjikan kemudahan ini tidak luput dari incaran para pencuri, yang kini telah merambah dunia digital. Tidak semua website e-commerce dapat dinyatakan aman, sehingga data-data personal yang sensitif seperti nomor kartu kredit dan lain sebagainya dapat jatuh ke tangan pihak-pihak yang tidak berhak. Ini menimbulkan rasa waswas bagi para pelaku e-commerce.

Untuk mengatasi hal tersebut digunakan teknologi Secure Socket Layer yang mengimplementasikan kriptografi kunci publik dan memungkinkan koneksi yang aman ke website. Selain itu ada pula teknologi sertifikasi digital sehingga para pengguna tidak akan tertipu dengan website palsu.

Namun, semua teknologi tersebut tidak akan ampuh bila si pengguna ceroboh dalam memakai fasilitas e-commerce. Kehati-hatian dan ketelitian manusia tetap diperlukan untuk mendukung teknologi keamanan sehingga dapat berjalan dengan semestinya.

6. Pustaka

Cryptography for Dummies. Chebby Chobb. Wiley Publishing. 2004.

***http://en.wikipedia.org**. Desember 2006.*

***http://www.verisign.com**. Desember 2006.*

***http://www.ssl.com**. Desember 2006.*