BAB I

PENDAHULUAN

1.1. Latar Belakang Masalah

Berbagai macam layanan komunikasi saat ini banyak menggunakan penerapan kriptografi, misalnya *I-banking* ATM, kartu kredit, *web, e-mail, milis, newsgroup,* dan sebagainya. Dengan semakin maraknya orang memanfaatkan layanan komunikasi di internet tersebut, maka permasalahan pun bermunculan, seperti *spaming, spoofing, sniffing user* dan *password*, apalagi ditambah dengan adanya *hacker* dan *cracker*. Banyak administrator yang kemudian berusaha menyiasati bagaimana cara mengamankan informasi *Web server* yang dikomunikasikannya, atau menyiasati bagaimana cara mendeteksi keaslian dari informasi data *website* yang diterimanya berupa paket data *user* dan *password* [LiangIptek, 2007].

Sebagai contoh [SecureBank, 2008], [Rico, 2008], [Wenny, 2006] yang merupakan sebuah website yang berisikan transaksi e-commerce atau *web-web* di mana terdapat login *user* dan *password*-nya. *Hacker* atau *cracker* melakukan *sniffing/spoofing mode* dengan menggunakan *software-software* yang ada misal : *ettercap, ethereal, comodo*, dan sebagainya. Dikarenakan data yang dikirim masih berupa plaintext khususnya *user* dan *password* bisa terbaca dengan mudah tanpa adanya enkripsi.Teknik untuk membuat pesan tersebut tidak terbaca disebut enkripsi. Pesan yang tidak dapat dibaca tersebut disebut *ciphertext*. Proses yang

merupakan kebalikan dari enkripsi disebut sebagai deskripsi. Jadi deskripsi akan membuat *ciphertext* menjadi *plaintext* (informasi yang asli).

Kriptografi adalah ilmu dan praktik menjaga kerahasiaan dari pihak-pihak yang tidak dikehendaki baik saat penyampaian maupun penyimpanan informasi tersebut. Informasi yang hendak dilindungi itu disamarkan dengan menggunakan cara-cara dan kunci tertentu. Identitas pihak-pihak yang tidak berwenang atas informasi yang dienkripsi dapat dipastikan dengan kriptografi. Kriptografi tidak hanya menjaga kerahasiaan informasi, namun juga menjaga keutuhan dan keaslian informasi yang disampaikan.

Salah satu aplikasi kriptografi di jaringan internet adalah pengamanan situs dengan menggunakan protokol HTTPS (*Hypertext Transfer Protocol Secure*). HTTPS memungkinkan terjadinya akses dan transaksi melalui situs internet secara aman, misalnya dalam online banking, online shopping, login ke email host dan sebagainya.

Ketika menggunakan koneksi HTTPS, server menanggapi inisiasi koneksi oleh klien dengan menawarkan berbagai metode enkripsi yang dapat disokong. Klien lalu memilih metode koneksi, dan kedua belah pihak saling bertukar sertifikat untuk memastikan identitas masing-masing. Setelah itu, kedua belah pihak bertukar informasi yang telah dienkripsi. Namun sebelumnya, harus dipastikan keduanya menggunakan kunci yang sama dan bahwa koneksi yang digunakan tertutup.

Perkembangan internet begitu pesat dan kini telah menjadi suatu jaringan raksasa yang saling menghubungkan berbagai jaringan. Pemanfaatannya di bidang

bisnis menjadikan terjadinya pergeseran model. Dari bentukan komunitas pengguna internet yang cenderung berupa suatu *Gemainschaft* (kelompok masyarakat di mana anggotanya sangat terikat secara emosional dengan yang lainnya) dengan norma internal dan tradisi yang diatur berdasarkan status dan didorong oleh kecintaan, kewajiban serta kesamaan pemahaman dan tujuan, sekarang telah bergeser dan cenderung menjadi suatu *Gesselschaft* (ikatan-ikatan diantara anggotanya kurang kuat dan bersifat rasional) yang terdiri dari individu (organisasi) yang memiliki interest masing-masing yang saling berkompetisi untuk kepentingan material sehingga berbentuk pasar bebas. Dari pergeseran model tersebut perlu adanya penanaman sebuah pemikiran bahwa seorang administrator perlu membentuk dan menerapkan sekuriti *policy* yang tepat, menanamkan pemahaman sekuriti kepada seluruh pengguna yang ada di sekitarnya, mendefinisikan proses otentifikasi dan *firewall*, *design* jaringan yang aman dan deteksi perbaikkan bila terjadi kerusakan.

Pada bentuk pertama bisa dikatakan tak ada batasan antara privat dan publik, sedang pada yang kedua terjadi perbedaan secara jelas. Dengan adanya pergeseran tersebut dan makin banyaknya penggunaan *eCommerce* kebutuhan akan sekuriti mulai tampak dengan jelas. Banyak perusahaan yang awalnya menganggap remeh masalah ini akhirnya mengalami kerugian yang besar akibat kelalaian ini.

Tetapi pada kenyataannya, terutama dalam era Internet yang serba cepat ini. Sekuriti terbentuk dari suatu mata rantai yang akan memiliki kekuatan sama dengan mata rantai yang terlemah. Sistem sekuriti berbasiskan *CA* akan memiliki

rantai yang tak seluruhnya hanya merupakan sistem kriptografi namun manusia juga akan banyak terlibat dalam implementasi sistem nantinya.

Jadi masalah sekuriti pada infrastruktur Internet tidak saja terletak pada masalah teknologi dan ekonomi saja, tetapi juga menyangkut dengan keamanan suatu negara atau ketergantungan negara terhadap negara lain. Bukan saja sistem sekuriti dengan teknologi yang aman, tetapi juga pertimbangan bahwa pemanfaatan suatu teknologi tidak dibatasi oleh negera lain. Sebagai contoh USA dengan *ITAR (international traffic arms regulation)* -nya membatasi pemanfaatan jenis teknologi kriptografi tertentu.

Kompleksnya infrastruktur dari jaringan komputer secara global di mana proses pengaksesan suatu aplikasi-aplikasi berbasis web yang ada di internet akan melewati beberapa terminal-terminal. Terminal tersebut dapat berupa Internet *Service Provider* ataupun *router-router* yang ada pada *backbone internet*. Ini menyebabkan data yang ditransmisikan tidak langsung sampai pada tujuan. Hal tersebut menimbulkan kesempatan pihak yang tidak berwenang untuk mengakses data tersebut pada saat data melewati terminal-terminal yang ada pada jaringan komputer global. Hal tersebut merupakan faktor yang menyebabkan suatu ancaman yang menerangkan bahwa jalur yang disediakan internet pada saat ini tidak sepenuhnya adalah jalur yang aman [Onno W. Purbo, 1998] . Dari permasalahan tersebut dibutuhkan suatu *protokol* (sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer) yang dapat menjamin integritas dari data tersebut pada saat melewati suatu jaringan internet.

HTTPS (HyperText Transport Protocol Secure) sebagai salah satu secure protokol pada protokol *HTTP* yang banyak digunakan oleh institusi-institusi tertentu, khususnya pada perusahan-perusahan jenis *e-commerce* yang banyak melakukan transaksi melalui internet. HTTPS sendiri didukung oleh SSL yang berfungsi menjamin keamanan dalam pengiriman dan pengaksesan informasi lewat internet. Biasanya, hanya server yang mengalami otentikasi (untuk memastikan identitasnya). Sedangkan pengguna akhir (misalnya orang yang mengakses sebuah situs) tidak terotentikasi, namun mereka dapat mengetahui dengan jelas dengan siapa mereka berbagi informasi.

SSL menjamin kerahasiaan, kesatuan dan keaslian informasi yang terkait. Untuk menjaga kerahasiaan informasi, SSL menggunakan kriptografi. Sedangkan kesatuan informasi dimungkinkan terjadi dengan adanya digital signatures (tanda tangan digital). Keaslian informasi dijamin dengan penggunaan sertifikat.

1.2. Rumusan Masalah

Berdasarkan uraian yang telah diutarakan sebelumnya, maka dapat dibuat rumusan masalah sebagai berikut :

1. Bagaimana melakukan implementasi installasi *Web server* dengan menggunakan *secure protocol HTTPS ?*
2. Bagaimana perbedaan protokol *HTTP* dan *HTTPS ?*

1.3. Batasan Masalah

Agar permasalahan yang dihadapi tidak terlalu meluas maka perlu adanya batasan masalah. Adapun permasalahan yang akan diteliti adalah :

1. Pembahasan mengenai installasi dan kompilasi dari Operating Sistem dan software pendukung *SSL* yaitu *Open SSL* dan *Mod SSL*, *AMP* dengan *Web server Apache*.
2. Pembuatan *certificate* digital yang berisi kunci publik dan private menggunakan metode SSL, *certificate* ini juga berisi tentang identitas dan hal-hal lain yang berhubungan dengan pemilik *certificate* pada proses penginstallan.
3. Melakukan *attacking mode sniffing* pada aplikasi *Web server* yang menggunakan *HTTP* dan *HTTPS*.

1.4. Maksud dan Tujuan Penelitian

Berangkat dari permasalahan yang telah dirumuskan di atas, maka maksud dan tujuan penelitian ini antara lain :

1. Untuk memenuhi persyaratan kelulusan jenjang pendidikan Ahli Madya (A.Md) Komputer jurusan Teknik Informatika di Sekolah Tinggi Manajemen Informatika dan Komputer "AMIKOM" Yogyakarta.
2. Menjelaskan model struktur pengenkripsian protokol *HTTPS* dengan menggunakan *SSL*.

3. Membuat sebuah *Web server* dengan menggunakan protokol *HTTPS* dan kemudian membandingkannya dengan Web server yang hanya menggunakan protokol *HTTP*.
4. Menjelaskan kesimpulan dari hasil *attacking mode sniffing* terhadap *Web server* yang menggunakan *HTTP* dan *HTTPS*, untuk membuktikan perbedaan keamanan kedua protokol.

1.5. Manfaat Penelitian

Setelah tujuan dapat dicapai, maka manfaat yang diharapkan nantinya yang akan didapat dari penulisan tugas akhir ini, yaitu:

1. Dapat memberikan Informasi dan gambaran akan pentingnya keamanan dalam sistem jaringan
2. Membantu pengguna komputer jaringan untuk memilih dan menentukan sistem keamanan yang akan digunakan dalam web server.
3. Agar dapat mengetahui seberapa kemampuan teknik enkripsi data dengan menggunakan *SSL* pada *Web server*.
4. Membantu praktisi jaringan untuk membuat suatu *secure Web server* menggunakan *SSL* dan konfigurasinya.

1.6. Metodologi

Metodologi yang digunakan dalam penyusunan Laporan Akhir ini dapat dijelaskan sebagai berikut :

1. Studi literatur

   Adalah dengan mempelajari literatur – literatur yang berhubungan dengan sistem keamanan data, kriptografi, sertifikat dan web server *HTTPS.*

2. Diskusi

   Adalah dengan melakukan diskusi untuk membahas sertifikat dan web server *HTTPS* tersebut melalui *groups*, *mailing-list* dan *e-mail*.

3. Observasi

   Yaitu dengan melakukan pengamatan secara langsung, cermat, dan sistematis terhadap sebuah web server yang akan diamati.

1.7. Sistematika Penulisan

Penulisan laporan akhir ini dilaksanakan dengan langkah – langkah sebagai berikut :

BAB I : Membahas latar belakang, rumusan masalah, batasan masalah , maksud dan tujuan, manfaat, metodologi dan sistematika penulisan.

BAB II : Membahas tentang HTTPS secara umum, dasar-dasar sistem keamanan data dan kriptografi.

BAB III : Memaparkan gambaran umum objek penelitian.

BAB IV : Memaparkan hasil pembuatan sertifikat *HTTPS* dan analisis keamanan data menggunakan *HTTPS*.

BAB V : Membahas tentang kesimpulan dari analisis dan perencanaan serta saran bagi pengembangan selanjutnya.

I.8. Jadwal Penelitian

Tabel 1.1 Jadwal Penelitian

No	Waktu / Kegiatan	Bulan											
		Maret 2008				April 2008				Mei 2008			
		Minggu Ke :											
		I	II	III	IV	I	II	III	IV	I	II	III	IV
1	Pengumpulan data												
2	Analisis masalah												
3	Perancangan sistem												
4	Pembuatan sistem												
5	Pengujian sistem												
6	Penulisan laporan												