KEAMANAN JARINGAN PADA APLIKASI ELECTRONIC PAYMENT MENGGUNAKAN PROTOKOL SSL BERBASIS ALGORITMA ENKRIPSI RSA 1024 BIT DAN RC-4 128 BIT

Gustommy Bisono[1], Agus Virgono[2], R. Rumani[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Pembayaran elektronik sekarang sudah menjadi seperti gaya hidup dan kebutuhan bagi sebagian masyarakat, terutama masyarakat perkotaan yang menginginkan pola bertransaksi yang praktis dan cepat. Dengan berkembangnya teknologi di bidang jaringan internet, suatu proses pembelian dan pembayaran melalui internet sudah bukan hal yang asing lagi.

Masalah terpenting dalam jaringan komputer adalah masalah keamanan data yang dikirimkan. Pelaku kejahatan memanfaatkan celah keamanan yang ada untuk dimasuki dan melakukan manipulasi data. Pihak penjahat itu bisa saja berniat untuk sekedar mencari tahu saja, atau juga bisa mencuri berbagai macam hal seperti uang, data rahasia, dll.

Secure Socket Layer (SSL) merupakan suatu protokol yang telah dikembangkan dan dipergunakan untuk mengatasi permasalahan keamanan yang mengancam proses transaksi menggunakan jaringan internet. SSL didukung pula dengan penyediaan fasilitas enkripsi yang cukup memadai dan dilengkapi dengan sebuah proses handshaking dan pengiriman data yang cukup aman untuk mengatasi berbagai kejahatan jaringan internet yang ada.

Dengan adanya kejahatan cyber yang berkembang di jaringan internet, maka tugas akhir ini akan menganalisa sistem keamanan yang mampu disediakan oleh sistem tersebut, meliputi simulasi serangan dan juga analisa yang disusun berdasarkan referensi yang sudah ada.

Sistem keamanan yang diimplementasikan ternyata bisa memenuhi parameter-parameter keamanan internet yaitu confidentiality, authority, authentication, integrity, dan non-repudiation. Sistem dengan protokol SSL ini juga sanggup mengantisipasi simulasi serangan man-in-the-middle dan juga masih aman terhadap serangan brute-force dalam waktu beberapa tahun ke depan. Kelemahan yang bisa diketahui dari sistem ini adalah masih rentan terhadap serangan denial of service, yang bisa membuat performa jaringan server menjadi sangat sibuk, dan bisa membuat kegagalan dalam transaksi rata-rata sebesar 2,31 % dari 15000 simulasi transaksi.

Kata Kunci : enkripsi, pembayaran elektronik, keamanan jaringan, SSL

Abstract

Electronic payment has now become a life style and needs for some community, especially for urban society that expect a practical and fast transaction. Within the development in technology in the computer network, especially with the existence of internet access, an online payment is now become popular. Even people now can use this online service to buy things from other country with only use their personal computer connected on internet access.

The most important thing in computer network is the security in sending data, there are so many cyber crimes we had heard from any media. Criminals use the security fissure to be interrupted and then doing some data manipulations. Those criminals may just want to look at something, or may steal anything like money, secret data, etc.

Secure Socket Layer (SSL) is a protocol that is developed and used to prevent the security problems that could threat transaction process through internet access. SSL is supported also with a good encryption facility and also completed with a secure handshaking and data transfer to solve the existence of internet network crime.

Within the existence of cyber crime in the internet, so this final project will analyze the security system that is provided by the system, including attack simulation and analysis that is compiled based on the exist references.

The implemented security system is able to provide the security parameters, they are confidentiality, authority, authentication, integrity, and non-repudiation. The SSL protocol is also able to anticipate man-in-the-middle attack simulation and still secure enough from brute-force attack in the next several years. The weakness of the system is the susceptibility from denial of service attack, that could make the network performance of the server is being very busy, and could make 2,31 % transaction failure from 15000 transaction simulation.

Keywords : encryption, electronic payment, network security, SSL

BAB I
PENDAHULUAN

1.1 LATAR BELAKANG

Gaya hidup masyarakat modern sekarang semakin membutuhkan suatu kemudahan dalam berbagai hal, termasuk dalam hal transaksi pembayaran. Sekarang, semua pihak PERBANKAN sudah menyediakan fasilitas kartu pintar untuk pelanggannya, dimana pelanggan tidak perlu lagi membawa uang untuk keperluan pembayaran suatu transaksi di tempat-tempat perbelanjaan. Hampir semua pusat perbelanjaan juga sudah menerima pembayaran melalui kartu pintar, bahkan banyak yang memberikan penawaran penjualan yang menarik jika melakukan transaksi dengan kartu pintar.

Permasalahan utama di dalam sebuah sistem jaringan pembayaran elektronik adalah masalah keamanan data yang dikirimkan, dimana banyak sekali pihak-pihak yang melakukan kriminalitas dunia maya (internet). Dengan adanya masalah itu, maka di dalam suatu sistem pembayaran elektronik harus ada suatu sistem keamanan di jaringan komputernya.

Sebuah sistem pembayaran elektronik juga terdiri dari sebuah sistem jaringan komputer yang akan mengirimkan permintaan transaksi dari berbagai cabang ke sentral, dan sistem ini harus mempunyai kinerja yang handal, terutama dalam mengatasi kejahatan pengiriman data antara klien-server.

Dalam mengatasi kejahatan yang bisa berupa pencurian data maupun manipulasi data oleh penjahat, maka akan dirancang dan dianalisa sebuah sistem keamanan yang bisa menjaga keamanan pengiriman data dari klien-server, sehingga proses pembayaran elektronik akan bisa dilakukan dengan aman.

1.2 TUJUAN DAN KEGUNAAN

1.2.1 Tujuan

Tujuan dari penelitian ini adalah untuk merancang sebuah sistem keamanan aplikasi pembayaran elektronik dalam sistem jaringan komputer klien-server, dan membuat suatu sistem basis data untuk penyimpanan dan pemrosesan sistem pembayaran elektronik yang terpusat.

1.2.2 Kegunaan

Kegunaan dari penelitian tugas akhir ini adalah untuk mempermudah dan mengamankan suatu aplikasi transaksi pembayaran dengan sistem jaringan komputer yang aman dan handal, sehingga dapat digunakan untuk menggantikan cara pembayaran dengan uang kontan.

1.2.3 Parameter Pengujian Analisis

Untuk mendukung analisa terhadap sistem yang dibuat penulis, maka penulis akan menggunakan parameter-parameter berikut untuk diuji:

1. Parameter keamanan data terhadap serangan pihak lain yang tidak bertanggung jawab.
2. Parameter kegagalan sistem (*Denial of Service*).
3. Parameter kecepatan sistem dalam bertransaksi dari awal proses hingga transaksi berhasil dilakukan.
4. Parameter Performansi Komputer dan Jaringan Komputer Klien dan *Server*.
5. Parameter kerahasiaan data yang dikirim (*Confidentiality*).
6. Parameter keutuhan pesan (*Integrity*) dari serangan data di tengah pengiriman data.
7. Parameter keabsahan (*Authentication*), baik keabsahan klien maupun *server*.
8. Parameter Otoritas (Authority) data, sehingga data hanya bisa diubah oleh pihak yang punya otoritas atau kewenangan terhadap data itu.
9. Parameter *Non-Repudiation*, bahwa pengirim seharusnya tidak bisa mengelak bahwa dialah yang benar-benar mengirim pesan.

1.3 PERMASALAHAN

1.3.1 Rumusan Masalah

Hal-hal yang akan dibahas dalam Tugas Akhir ini adalah:

1. Perancangan keamanan jaringan komputer yang handal untuk sistem pembayaran elektronik menggunakan input data nomor ID kartu pintar dan nominal pembelanjaan.
2. Perancangan *basis data* yang handal untuk menangani data dalam jumlah yang besar.
3. Perancangan perangkat lunak yang handal dan mudah dioperasikan yang akan digunakan untuk pengoperasian simulasi sistem.

1.3.2 Batasan Masalah

Agar pengerjaan tugas akhir ini mendapatkan hasil yang optimal, maka masalah akan dibatasi sebagai berikut :

1. Tugas akhir ini dikhususkan membuat sistem keamanan dan perangkat lunak pada sistem jaringan komputer klien-*server* untuk aplikasi pembayaran elektronik dengan inputan data nomor ID dari kartu pintar dan nominal pembelanjaan.
2. Hanya akan dibuat perancangan jaringan dari klien ke *server*, dengan jumlah server hanya ada 1 buah.
3. Tidak akan dibahas mengenai *reader/writer* kartu pintar maupun *tag/transponder*-nya.
4. Pada simulasi, inputan data akan dilakukan dengan komputer untuk menguji kehandalan sistem keamanan dan basis data.
5. Pengujian kehandalan sistem akan dilakukan dengan software jaringan (WireShark 1.02).
6. Teknik kriptografi yang akan digunakan adalah teknik simetris (RC-4), teknik asimetris (RSA), fungsi *hash* (SHA-1 dan MD5), tanda tangan digital, dan sertifikat digital, dan semua teknik kriptografi tersebut akan digunakan pada satu protokol SSL (*Secure Socket Layer*).
7. Sistem dititikberatkan menggunakan sistem operasi windows XP SP2.
8. Sistem dititikberatkan pada keamanan data yang dikirimkan.

9. Masalah keamanan yang berhubungan dengan pengamanan komputer maupun media penyimpanan yang berada di klien maupun server tidak akan dibahas.
10. Sistem dan perangkat lunak akan dibangun menggunakan bahasa pemrograman Java 2 *Standard Edition* 1.6 dan Netbeans 5.5.
11. Sistem basis data akan dibangun dengan menggunakan perangkat lunak MySQL 4.0.12.

1.4 METODA PENELITIAN

1.4.1 Bentuk Penelitian

Bentuk penelitian dari tugas akhir ini adalah berupa perancangan dan implementasi perangkat lunak untuk keamanan jaringan dan basis data yang handal untuk sistem Pembayaran Elektronik dengan menggunakan kartu pintar. Sehingga, data yang jumlahnya banyak akan bisa diproses dan transaksi akan berlangsung dengan aman dan cepat.

1.4.2 Teknik Pengumpulan Data

Pengumpulan data dilakukan dengan cara :

1. Studi literatur dan kajian-kajian yang berkaitan dengan masalah-masalah yang ada pada Tugas Akhir ini.
2. *Browsing* data-data pendukung melalui internet.
3. Diskusi secara langsung dengan pembimbing Tugas Akhir dan pihak-pihak yang lebih berpengalaman.

1.5 SISTEMATIKA PENULISAN TUGAS AKHIR

BAB I : PENDAHULUAN

Bab ini membahas latar belakang masalah, tujuan dan kegunaan, batasan masalah, metoda penelitian, dan sistematika penulisan yang digunakan dalam pembuatan tugas akhir.

BAB II : LANDASAN TEORI

Berisi teori-teori dasar pembahasan umum tentang sistem keamanan jaringan komputer dan perangkat lunak yang digunakan.

BAB III: PERANCANGAN SISTEM

Bab ini akan membahas perancangan perangkat lunak, keamanan jaringan dan basis data untuk pendukung sistem pembayaran elektronik yang akan dibuat.

BAB IV: SIMULASI DAN ANALISIS

Pada bab ini dibahas tentang simulasi uji fungsi dan performansi perangkat lunak dengan kasus-kasus tertentu, serta analisis yang menunjang permasalahan pada simulasi yang sudah dilakukan.

BAB V : PENUTUP

Berisi kesimpulan dan saran berdasarkan analisa dan pembahasan pada bab-bab sebelumnya.

Telkom University

BAB V
PENUTUP

5.1 Kesimpulan

1. Sistem mampu mengatasi serangan *Man-in-the-middle* sehingga jika ada pihak yang memalsukan sertifikat (*man-in-the-middle*), tidak akan terjadi pertukaran data antara klien dan *server*. Sehingga penyerang tidak akan mendapatkan apapun.
2. Sistem masih bisa bertahan terhadap serangan *brute force*, karena waktu pemecahan kunci algoritma yang sangat lama, yaitu 9×10^{19} tahun untuk algoritma RC-4 128 bit, dan kunci RSA 1024 bit masih aman untuk digunakan hingga tahun 2010 tanpa penggantian kunci.
3. Sistem bisa memenuhi parameter kerahasiaan data (*Confidentiality*), keutuhan data (*Integrity*), otentikasi, otoritas data, dan *Non-repudiation*.
4. Kegagalan sistem yang terjadi saat simulasi terjadi karena adanya keterbatasan aplikasi *server* dalam menerima laju banyak data dan datang dengan sangat cepat.

5.2 Saran

1. Diperlukan penggantian sertifikat digital secara berkala setiap tahun sekali pada masing-masing pihak.
2. Kelemahan pada aplikasi bisa diperbaiki pada sistem antrian (*buffer*) pada saat pembuatan aplikasi *server*.

DAFTAR PUSTAKA

[1] Adriana, Tiffany. KRIPTOGRAFI DAN PEMANFAATANNYA PADA RSA DAN MD5. (online). Available : http://www.informatika.org/~rinaldi/Matdis/2006-2007/Makalah/Makalah0607-126.pdf

[2] Cahyono, Setiono. Panduan Praktis Pemrograman Database Menggunakan MySQL dan Java. Informatika, Bandung, 2006.

[3] Harold, Elliotte Rusty. *Java Network Programming 2nd edition.* O'Reilly , California. 2000.

[4] Keizer, Gregg. 2008. New blackmailing Trojan encrypts files using high-grade 1024-bit RSA key. (online). Available : http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9094818

[5] Kurniawan, Yusuf Ir.,MT. Kriptografi. Informatika, Bandung, 2004.

[6] Prasetyo, Didik Dwi. 150 Rahasia Pemrograman Java . PT Elex Media Komputindo, Jakarta, 2007.

[7] Setiawan, Iman Budi. 1999 . SMARTWALLET–JAVA WALLET BERBASIS SMARTCARD DAN PROTOKOL SET. (online). Available: www.geocities.com/amwibowo/resource/rut6/set-cardholder-smartcard.pdf

[8] Wawancara gatra kepada Onno W. Purbo . 2000. (online). *available:* http://stream.plasa.com/onno/gfe/view.php?file=artikel_indonesia_1/network/network-security/wawancara-gatra-network-security-03-08-2000.txt