IMPLEMENTASI PROTOKOL INSTANT MESSAGING KEY EXCHANGE PADA SECURE INSTANT MESSAGING

Skripsi

oleh
ABDIEL BRAMANTYO
22084515

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2013

IMPLEMENTASI PROTOKOL INSTANT MESSAGING KEY EXCHANGE PADA SECURE INSTANT MESSAGING

Skripsi

Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

ABDIEL BRAMANTYO
22084515

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2013

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

IMPLEMENTASI PROTOKOL INSTANT MESSAGING KEY EXCHANGE PADA SECURE INSTANT MESSAGING

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 9 September 2013

ABDIEL BRAMANTYO
22084515

HALAMAN PENGESAHAN

IMPLEMENTASI PROTOKOL INSTANT MESSAGING KEY EXCHANGE PADA SECURE INSTANT MESSAGING

Oleh: ABDIEL BRAMANTYO / 22084515

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 16 Agustus 2013

Yogyakarta, 30 Agustus 2013
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, SKom.,M.Cs
2. Junius Karel, M.T.
3. Antonius Rachmat C., SKom.,M.Cs
4. Joko Purwadi, M.Kom

Dekan	Ketua Program Studi
(Drs. Wimmie Handiwidjojo, MIT.)	(Nugroho Agus Haryono, M.Si)

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa atas berkat, rahmat, dan karunianya sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul "Implementasi Protokol Instant Messaging Key Exchange Pada Secure Instant Messaging" dengan baik.

Penulisan laporan ini merupakan kelengkapan dan pemenuhan dari salah satu syarat dalam memperoleh gelar Sarjana Komputer. Selain itu, penulisan laporan Tugas Akhir ini juga bertujuan untuk melatih mahasiswa agar dapat menghasilkan suatu karya yang dapat dipertanggungjawabkan secara ilmiah, sehingga dapat bermanfaat bagi penggunanya.

Dalam menyelesaikan penelitian dan laporan Tugas Akhir ini, penulis telah banyak menerima bimbingan, saran, dan masukkan dari berbagai pihak, baik secara langsung maupun secara tidak langsung. Untuk itu dengan segala kerendahan hati, pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada :

1. Bapak Willy Sudiarto Raharjo, SKom.,M.Cs. selaku dosen pembimbing I yang pertama yang selalu sabar dalam membimbing penulis dalam mengerjakan penelitian dan penyusunan laporan Tugas Akhir.
2. Bapak Junius Karel, S.Si., M.T. selaku dosen pembimbing II yang selalu sabar dan baik membimbing penulis dalam mengerjakan penelitian dan penyusunan laporan Tugas Akhir.
3. Keluarga dan saudara yang selalu memberikan doa dan dukungannya kepada penulis dalam menyelesaikan Tugas Akhir.
4. Rekan-rekan penulis yang dengan senang hati memberikan arahan, saran, dan, sharing dalam pengerjaan Tugas Akhir maupun penulisan laporan Tugas Akhir.
5. Pihak lain yang tidak dapat penulis sebutkan satu per satu, sehingga Tugas Akhir ini dapat terselesaikan dengan baik.

Penulis menyadari bahwa penelitian dan laporan Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca sekalian.

Akhir kata penulis meminta maaf bila ada kesalahan dalam penyusunan laporan maupun sewaktu penulis melakukan penelitian Tugas Akhir. Semoga penelitian dan laporan Tugas Akhir ini dapat berguna bagi kita semua.

Yogyakarta, Agustus 2013

Penulis

INTISARI

Penggunaan teknologi komunikasi dalam kehidupan manusia semakin berkembang. Kita bisa berkomunikasi secara global tanpa terbatas geografis dan waktu. *Instant Messaging* (IM) merupakan salah satu dari banyak layanan komunikasi yang sering banyak dipakai oleh banyak orang. *Instant Messaging* memungkinkan seseorang untuk berkomunikasi dengan orang lain secara *real-time* melalui *internet* maupun *intranet*. Masalah muncul ketika *Instant Messaging* digunakan untuk mengirim pesan yang bersifat rahasia atau strategis. Mayoritas layanan *Instant Messaging* tidak memperhatikan aspek keamanan dari pesan dan otentikasi pengguna. Sistem *instant messaging* saat ini masih rentan terhadap *sniffing* atau suatu proses penyadapan memanfaatkan paket *sniffer* atau teknologi sejenis oleh pihak yang tidak berkepentingan untuk mengetahui informasi didalamnya.

Untuk mengatasi permasalahan tersebut, diperlukan suatu cara untuk menyamarkan informasi yang dikirim oleh *user*. Pada penelitian ini akan dibangun sebuah *instant messaging* yang mengimplementasikan protokol *Instant Messaging Key Exchange* untuk mengamankan komunikasi antar *user*.

Hasil dari penelitian ini, komunikasi antara *client* dan *server* yang sebelumnya dapat dengan mudah diketahui isi informasinya karena informasi yang dikrimkan berupa *plaintext*, sehingga pesan yang sebelumnya dikirim dalam bentuk *plaintext* diganti dengan pesan yang terekripsi atau *ciphertext* saat dikirimkan, sehingga walaupun paket data dapat disadap oleh pihak lain, namun informasi didalamnya tidak dapat dibaca dengan mudah.

Kata Kunci : *Instant Messaging, Instant messaging key exchange, sniffing,* protokol

DAFTAR ISI

DAFTAR GAMBAR

BAB 1
PENDAHULUAN

1.1. Latar Belakang

Instant Messaging (IM) merupakan salah satu dari banyak layanan komunikasi yang sering banyak dipakai oleh banyak orang. Kehadiran *Instant Messaging* beberapa tahun belakangan ini telah menjadi fenomena yang sangat besar. *Instant Messaging* memungkinkan seseorang untuk berkomunikasi dengan orang lain secara *realtime* melalui *internet* maupun *intranet*. Dikarenakan *Instant Messaging* hanya membutuhkan sedikit *bandwith*, sehingga membutuhkan *cost* yang rendah daripada menggunakan telepon. Berdasarkan kemudahan tersebut, kalangan bisnis mulai melihat *Instant Messaging* sebagai alternatif sarana komunikasi. Saat ini ada beberapa aplikasi *Instant Messaging* yang cukup popular di kalangan pengguna *internet* diantaranya adalah Yahoo! Messanger, ICQ, MSN Messenger, dan AIM.

Masalah muncul ketika *Instant Messaging* digunakan untuk mengirim pesan yang bersifat rahasia atau strategis. Mayoritas layanan *Instant Messaging* tidak memperhatikan askpek keamanan dari pesan dan otentikasi pengguna. Sistem *Instant Messaging* saat ini masih rentan terhadap *sniffing* atau suatu proses penyadapan memanfaatkan paket *sniffer* atau teknologi sejenis oleh pihak yang tidak berkepentingan untuk mengetahui informasi didalamnya. Melihat beberapa kekurangan dari *Instant messaging*, maka pada penelitian ini akan dibahas protokol keamanan yang dapat diterapkan untuk mengamankan informasi yang ditransmisikan pada *instant messaging* dengan menggunakan protokol *Instant Messaging Key Exchane* (IMKE) yang diperkenalkan oleh Mohammad Mannan.

1.2. Rumusan Masalah

Masalah yang dibahas dalam penelitian ini adalah :

1. Bagaimana mengimplementasikan protokol *Instant Messaging Key Exchange* (IMKE) dalam membangun sebuah sistem *secure instant messaging*.

1.3. Batasan Masalah

Sistem yang akan dibangun ini memiliki batasan-batasan masalah yang meliputi :

- Pertukaran informasi melalui *instant messaging* hanya berupa pesan teks atau yang sering disebut dengan chatting.
- Hanya akan diimplementasikan pada desktop di dalam *Local Area Network.*
- Model chat sistem bersifat privat.
- Proses *secure chatting* hanya berlangsung pada saat *client* melakukan komunikasi privat dengan *client* lain.

1.4. Tujuan Penelitian

Tujuan dari penelitian ini antara lain :

- Membangun aplikasi *secure instant messaging* dengan mengimplementasikan protokol *Instant Messaging Key Exchange*.
- Meneliti dan menganalisa bahwa protokol *Instant Messaging Key Exchange* (IMKE) dapat diterapkan untuk mengamankan informasi yang ditransmisikan pada *instant messaging*.

1.5. Metodologi Penelitian

Metodologi atau pendekatan yang digunakan dalam penyusunan Tugas Akhir ini adalah :

- Studi Pustaka

Studi pustaka dilakukan dengan cara membaca buku, jurnal, modul dan semua yang berhubungan dengan protokol keamanan *Instant Messaging Key Exchange*. Segala informasi atau data yang dikumpulkan dari bahan tercetak, baik secara manual ataupun *online* termasuk dalam metode ini.

- Perancangan Sistem dan Implementasi

  Metode ini dilakukan dengan cara merancang arsitektur sistem, antarmuka, dan prosedural sistem. Setelah itu mengimplementasikan protokol *Instant Messaging Key Exchange* ke dalam sistem yang dibangun.

- Pengujian

  Metode ini dilakukan dengan cara menguji kinerja dari sistem yang dibangun dan analisa hasil.

1.6 . Sistematika Penulisan

Sitematika penulisan tugas akhir ini akan terbagi dalam lima bab dengan urutan penulisan sebagai berikut

BAB 1 PENDAHULUAN pada bab ini yang berisi Latar Belakang, Rumusan Masalah, Batasan Masalah, Tujuan Penelitian, Metode Penelitian, dan Sistematika Penulisan.

BAB 2 TINJAUAN PUSTAKA pada bab ini terdiri dari dua bagian utama, yaitu Tinjauan Pustaka dan Landasan Teori.

BAB 3 PERANCANGAN SISTEM pada bab ini mencakup analisis teori-teori yang digunakan, dan bagaimana menerapkannya ke dalam sistem yang akan dibuat.

BAB 4 IMPLEMENTASI DAN ANALISIS SISTEM pada bab ini memuat hasil riset / implementasi, dan pembahasan dari riset tersebut yang bersifat terpadu.

BAB 5 KESIMPULAN DAN SARAN pada bab ini terdiri dari kesimpulan dan saran-saran untuk pengembangan sistem.

Selain berisi bab-bab utama tersebut, skripsi ini juga dilengkapi dengan Intisari , Kata Pengantar, Daftar Isi, Daftar Tabel, Daftar Gambar, Daftar Pustaka dan Lampiran.dan Lampiran.

BAB 5
KESIMPULAN DAN SARAN

5.1. Kesimpulan

Setelah dilakukan penelitian dan pengujian sistem yang telah dibuat, dapat disimpulkan bahwa:

1. *Instant messaging* yang telah dibuat dengan mengimplementasikan protokol *instant messaging key exchange* dapat mengamankan proses komunikasi antar *client*. Walaupun paket data yang ditransmisikan dapat dicapture oleh *software packet sniffer,* namun informasi yang didapat tidak dapat dibaca dengan mudah atau tersamarkan. Hal ini karena pesan yang sebelumnya dalam bentuk *plaintext* diubah kedalam *ciphertext* sebelum ditransmisikan ke penerima.

5.2. Saran

Untuk pengembangan lebih lanjut, saran yang dapat diberikan adalah sebagai berikut :

1. Untuk penelitian selanjutnya, dalam penerapan protokol *instant messaging* dapat dilakukan lebih lanjut dalam mengamankan tipe data berbeda dengan yang penulis teliti yang dalam penelitian ini yang hanya berupa teks. Tipe data lain yang dapat dilakukan penelitian lebih lanjut antara audio, citra atau video yang tentu saja dengan *file size* yang lebih besar dari data teks.
2. Dapat mengimplementasikan protokol *Instant Messaging Key Exchange* terhadap protokol instant messaging yang telah ada seperti pada protokol jabber.

DAFTAR PUSTAKA

Candradinata, M.M. (2010). Implementasi Enkripsi Simetris Data Encryption Standard Pada Web Based instant Messanging Berbasis Protokol Jabber. Diakses 15 November dari http://sinta.ukdw.ac.id/.

Listiyono, Hersatoto. (2009). Implementasi Algoritma Kunci Public Pada Algoritma Rsa. *Dinamika Informatika*. Semarang: Universitas Stikubank, Vol 1, 95-99.

Menezes, A.J., Oorschot, P.C.V., & Vastone, S. (1997). *Handbook of Applied cryptography*. Florida: CRC PressLLC.

Munir, R. (2005). Penggunaan Tanda-Tangan Digital Untuk Menjaga Integritas Berkas Perangkat Lunak. *Seminar Nasional Aplikasi Teknologi Informasi*. Yogyakarta, F-31-F34.

Mannan, M & Oorschot, P.C.V. (2006). A Protokol for Secure Public Instant Messaging, Financial Cryptography and Data Security. Ottawa: School of Computer Science Carleton University.

Riadhy, R. Sistem Enkripsi Instant Messaging (IM) Berbasis Tray Dengan Menggunakan Algoritma RSA. Diakses 20 Maret dari http://www.slideshare.net/rizkyriadhy/jurnal-sistem-enkripsi-instant-messaging-rizky-riadhy.

Sadikin, R. (2012). *Kriptografi Untuk Keamanan Jaringan*. Yogyakarta: Andi Offset.

Schneier, B. (1996). *Applied Cryptography*. New York: John Willey and Sons, Inc. 2nd Edition.

Tom, S.D., & Johnson, S. (2007).*Cryptography for Developers*. Rockland: Syngress Publishing, Inc.