BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Instant Messaging (IM) saat ini mengalami perkembangan yang cukup pesat pada jaringan *user*, karena kemampuannya mengirimkan pesan secara singkat dan cepat antara pengguna telekomunikasi. IM menjadi perangkat yang sangat penting untuk industri di seluruh dunia. IM digunakan di dalam penjadwalan *(scheduling meeting)*, pertukaran informasi bisnis dan informasi *client* dan lain-lain. IM telah dikembangkan pada sektor-sektor khusus atau antar penyedia layanan seperti *American online Instant Messenger* (AIM), MSN dan Yahoo. Pada tahun 1998 muncul protokol IM yang bersifat *open source* yang terkenal dengan protokol Jabber.

Jabber mulai dapat perhatian publik ketika didiskusikan antar pengembang pada *website Slashdot* pada bulan Januari 1999. Pada Mei 2000, protokol Jabber diluncurkan sebagai protokol yang bersifat *open source* berdasarkan referensi server dan saat ini tidak dapat saling dipertukarkan.

Jabber menggunakan arsitektur *client-server*, bukan arsitektur *peer-to-peer* seperti yang digunakan pada sistem IM lainnya. Protokol Jabber menggunakan format pesan *Extensible Markup Language* (XML). Format dokumen XML menjadi bahasa generik yang digunakan pada berbagai aspek komunikasi, karena sifatnya yang berbasis teks, mudah dibaca oleh manusia, maka aplikasi yang berbasis XML mudah untuk di-*debug* atau melewati *firewall*.

Protokol Jabber menggunakan standar XML. Standar ini adalah terbuka dan diterima secara luas untuk mendukung transaksi berbasis internet. Dengan karakteristik berbasis teks dan bersifat terbuka tersebut, maka kelemahan pada XML ini dapat membuka peluang terhadap serangan dan gangguan keamanan pada data. Oleh karena itu, demi melindungi data dari ancaman keamanan diperlukan penerapan mekanisme keamanan agar data dapat terjaga.

Protokol Jabber telah berkembang menjadi protokol yang sangat atraktif karena bersifat *open source* dan dapat diterima secara luas. Siapapun dapat membuat atau mengembangkan protokol Jabber secara fungsional tanpa memodifikasi protokol inti dengan hanya melakukan *maintainance* interoperabilitas dengan *client* IM lainnya seperti Yahoo dan MSN. Penggunaan teknologi IM Jabber semakin meningkat, oleh karena itu perlu ditingkatkan kebutuhan proteksi terhadap informasi.

Aktifitas komunikasi antar *client* tersebut harus melewati beberapa titik (*node*) agar dapat sampai ke *client* lainnya. Oleh karena itu data yang dikirim dapat disadap oleh pihak yang seharusnya tidak berhak menerima data tersebut. Tentu hal ini sangat berbahaya, karena bisa jadi percakapan yang dilakukan berisi data-data penting dan rahasia. Demi mengamankan data yang dikirim ini, maka diterapkanlah mekanisme keamanan agar data tidak dapat terbaca oleh pihak ketiga.

Diperlukan pemilihan penggunaan mekanisme keamanan yang tepat sesuai dengan kondisi lingkungan jaringan komputer yang digunakan. Mekanisme keamanan ini akan berpengaruh terhadap kinerja *server* tersebut dalam melayani *client*. Dengan menggunakan mekanisme keamanan yang tepat, akhirnya dapat dihasilkan pula *server*

Jabber dengan kinerja yang maksimal.

Dalam penelitian ini, akan dibahas sistem keamanan protokol Jabber pada sisi *client* dan kemampuan untuk membuat protokol Jabber yang sudah ada menjadi lebih aman melalui jaringan berdasarkan *library* kriptografi atau berdasarkan standar *library* yang *open source* sebagai tulang punggung untuk mengamankan perintah-perintah yang ada pada Jabber.

1.2 Perumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan sebelumnya, maka diajukan masalah umum adalah implementasi dan perbandingan beberapa metode sistem keamanan pada server Jabber terkait dengan *open source*, *network througput*, dan jumlah *user* yang dapat terkoneksi secara bersamaan (*connected simultaneuos user*) yang dihasilkan. Dalam penelitian ini server Jabber yang digunakan adalah **Ejabberd-1.1.3.**

1.3 Batasan Masalah

Percobaan ini dibatasi oleh hal-hal yang terkait dengan kemampuan, kecepatan dan keamanan transfer data. Hal ini dilakukan untuk lebih memfokuskan pada masalah yang akan menjadi bahan analisa dalam pembuatan laporan. Batasan-batasan itu sebagai berikut:

1. Perangkat lunak *(software)*

   Pemilihan perangkat lunak berperan dalam kemampuan fungsional Jabber server tersebut. Pada percobaan kali ini penulis menggunakan *software* ejabber.1.13 (versi stabil) karena mendukung sistem keamanan *stream encryption* dan *stream authentication.*

2. Perangkat Keras (*hardware*)

   Komputer yang digunakan sebagai server percobaan adalah Intell Celeron 1.7 GHz dengan NIC berjenis Rtl8900. Kelak perangkat keras juga akan berpengaruh pada performa server. Hasil pengujian kemungkinan akan berbeda apabila menggunakan jenis *hardware* yang lain.

3. Pengujian kemampuan server Jabber

   Dalam melakukan percobaan ini, penulis memanfaatkan jaringan intranet di bagian IT-departement STMIK Amikom Yogyakarta. Strategi pengujian kemampuan server dengan melakukan uji performa (*benchmark*) melalui layanan koneksi nirkabel di STMIK Amikom Yogyakarta.

4. Perbandingan pengaruh sistem keamanan

   Sistem keamanan yang digunakan yaitu sistem keamanan *stream encryption*; SSL dan TLS. Serta sistem keamanan *stream authentication* yaitu; SASL dan Digest-MD5, terhadap *open source* dan *network throughput* dalam melayani beberapa *client* dalam jumlah tertentu secara bersamaan.

Dari uraian diatas, maka dalam uji coba ini yang menjadi titik perhatian utama adalah membandingan besar *open source* dan *network throughput* yang dihasilkan oleh server Jabber yang menggunakan beberapa mekanisme keamanan yang berbeda.

Penelitian ini menggunakan Sistem Operasi Linux **Slackware 11**, dan perangkat lunak *open source*, **ejabberd-1.1.3** sebagai server Jabber, **tsung-1.2.2** sebagai alat *benchmark*.

1.4 Maksud dan Tujuan

Tujuan dari penulisan skripsi adalah untuk melihat performa perangkat lunak Server Jabber sebagai IM server dalam jaringan lokal (intranet) dengan menggunakan beberapa sistem keamanan yang berbeda. Dengan mendapatkan hasil penelitian tersebut, dapat disimpulkan penggunaan mekanisme sistem keamanan yang tepat pada server Jabber untuk lingkungan jaringan intranet.

1.5 Metode Penulisan Skripsi

Adapun metode penelitian yang digunakan oleh penulis adalah:

1. Metode observasi

   Yaitu pengumpulan data dengan pengamatan secara langsung pada obyek yang diteliti untuk memperoleh informasi yang tepat dan sistematis.

2. Metode kepustakaan

   Yaitu pengumpulan data dengan cara membaca berdasarkan kepustakaan yang mana dimaksudkan untuk mendapatkan konsep teori mengenai masalah yang diteliti, serta mencari sumber data dengan mencari di internet dan perpustakaan.

3. Metode eksperimen

   Yaitu melakukan percobaan dengan mengimplementasikan Jabber server pada jaringan intranet dan melakukan proses *benchmark*ing untuk memperoleh hasil pengukuran yang obyektif berdasarkan metode sistem keamanan baik *stream encryption* maupun *stream auntentication*

1.6 Sistematika Penulisan Skripsi

BAB I. PENDAHULUAN

Menguraikan latar belakang masalah, perumusan masalah, batasan masalah, maksud dan tujuan penulisan skripsi, metode penulisan skripsi, serta sistematika penulisan skripsi.

BAB II. TINJAUAN PUSTAKA

Membahas mengenai tinjauan pustaka protokol Jabber/XMPP, landasan teori sistem keamanan pada server Jabber dan model jaringan intranet yang digunakan.

BAB III. DESAIN PENELITIAN

Dalam bab ini dibahas cara penulis melakukan uji pengukuran kemampuan dengan menggunakan sistem keamanan yang berbeda dan obyek penelitian adalah jaringan intranet di STMIK Amikom Yogyakarta.

BAB IV. ANALISIS HASIL PENGUJIAN DAN PEMBAHASAN

Memberikan hasil analisis dari server yang digunakan, membahas mengenai cara pengukuran (*benchmark*) server beserta variabel-variabel pengukurannya.

BAB V. PENUTUP

Dalam bab ini berisikan kesimpulan dari penelitian dan saran-saran yang ditujukan pada pihak yang terkait.