Proposal Tugas Akhir

Implementasi Protokol Messaging Off-the-Record (OTR) pada Instant Messenger Berbasis Android(2076)

I MADE YOGY SUKMA PERMADI
5106100096

Dosen Pembimbing 1

ARY MAZHARUDDIN S
198106202005011003

Dosen Pembimbing 2

BASKORO ADI PRATOMO
510000003

DAFTAR

NCC

IBS

RPL

HASIL SIDANG

OK

REVISI

TOLAK

JURUSAN TEKNIK INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI
INSTITUT TEKNOLOGI SEPULUH NOPEMBER SURABAYA

USULAN TUGAS AKHIR

IDENTITAS PENGUSUL

Nama : I Made Yogy Sukma Permadi
NRP : 5106100096
Dosen Wali : Ahmad Saikhu, S.Si, M.T.

JUDUL TUGAS AKHIR

"Implementasi Protokol Messaging Off-the-Record (OTR) pada Instant Messenger Berbasis Android"

LATAR BELAKANG

Pengiriman pesan instan adalah suatu metode komunikasi yang bersifat real-time. Pengiriman pesan pada protokol XMPP yang digunakan oleh Google Talk dilakukan dengan melakukan transaksi paket antara client dengan server. Google Talk tidak menenkripsikan stream Jabber (XMPP) yang melalui jaringannya, akan tetapi menggunakan sebuah non standar yang tidak didokumentasikan untuk mengautentikasi stream yang akan dilayani oleh Google Talk service, dimana Google Talk service mengambil sebuah token dari sebuah *secure web server*. Aplikasi Google Talk client selain dari messenger client yang dikembangkan sendiri oleh Google perlu untuk mengamankan stream yang akan mereka kirimkan ke server Google menggunakan TLS sebelum mengirimkan passwordnya agar mereka berada dalam kondisi terenkripsi pada keseluruhan sesi[6].Oleh karena itu, untuk meningkatkan keamanan pesan (stream), maka diimplementasikan suatu sistem enkripsi pada client (aplikasi *instant messenger*).

Algoritma kriptografi yang akan digunakan pada perangkat lunak adalah OTR (Off-the-Record) yang menyediakan enkripsi yang kuat untuk komunikasi lewat aplikasi *instant messenger*. OTR mengkombinasikan[3] algoritma enkripsi AES (algoritma kunci simetris yang terbukti memiliki performa yang sangat baik ketika diimplementasikan pada software dan hardware karena kecepatannya tinggi dan kebutuhan memory RAM yang sedikit)[4] dan protokol pertukaran kunci (kunci publik dan kunci privat) Diffie-Hellman. Untuk pertukaran kunci publik dan kunci privat digunakan algoritma Diffie-Hellman sebagai implementasi dari suatu secure channel sehingga pertukaran kunci dapat dilakukan antara kedua user yang berkomunikasi dengan aman[5]. Perangkat

lunak dikembangkan dalam bahasa Java menggunakan API *Smack* kemudian diimplementasikan pada mobile phone berplatform android[1][2][7].

RUMUSAN MASALAH

Permasalahan yang diangkat dalam menyelesaikan tugas akhir ini adalah sebagai berikut:

1. Bagaimana membangun software *instant messenger client* berprotokol XMPP dalam bahasa Java menggunakan API *Smack* sebuah XMPP library *open source* untuk *instant messaging*.
2. Bagaimana mengimplementasikan algoritma AES pada perangkat lunak pengirim pesan instan untuk mengenkripsi pesan yang dikirim dan kemudian melakukan proses dekripsi terhadap pesan kiriman tersebut yang berisi ciphertext sehingga dapat ditampilkan ke user dalam plaintext.
3. Bagaimana mengimplementasikan algoritma pertukaran kunci (kunci public dan kunci privat) Diffie-Hellman antara user yang saling berkomunikasi.
4. Bagaimana menguji keamanan sistem enkripsi yang telah diimplementasikan pada perangkat lunak.

BATASAN MASALAH

Asumsi dan ruang lingkup permasalahan yang dikerjakan dalam Tugas Akhir ini adalah:

1. Menggunakan Android SDK untuk pengembangan aplikasi pada mobile phone.
2. Menggunakan IDE Eclipse dengan ADT (Android Development Tools) plugin sebagai editor sekaligus emulator.
3. Menggunakan *Smack* API untuk implementasi protokol pengiriman pesan XMPP.
4. Aplikasi ini hanya menyediakan koneksi ke satu *instant messaging service* Google Talk (hanya bisa login jika sudah mempunyai *account* Google talk) dan hanya bisa berkomunikasi dengan user lain yang juga memiliki Google Talk account.

TUJUAN PEMBUATAN TUGAS AKHIR

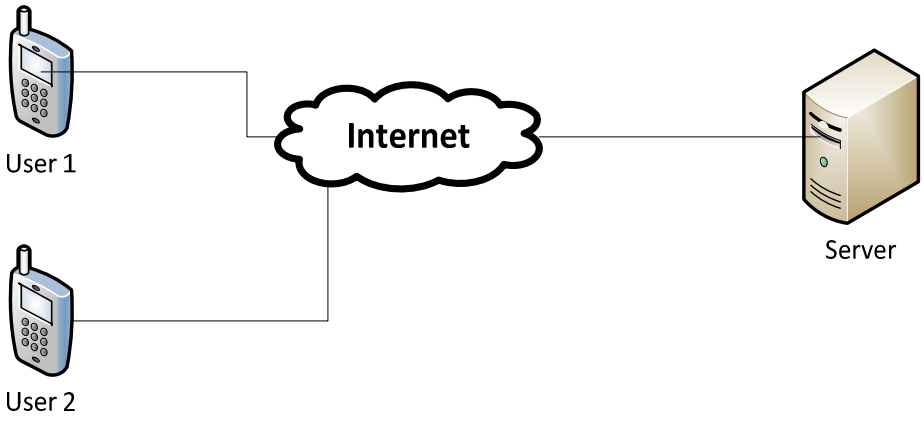
Tujuan dari pembuatan tugas akhir ini adalah membuat aplikasi pengiriman pesan pada protokol XAMPP yang digunakan oleh Google Talk dimana dibuat suatu kondisi

yang aman dari penyadap saat dua user yang saling berkomunikasi lewat proses enkripsi dan dekripsi pesan.

MANFAAT PEMBUATAN TUGAS AKHIR

Manfaat yang dapat diambil dari aplikasi yang dibangun pada tugas akhir ini adalah menambahkan suatu fitur keamanan pada aplikasi instant messenger dimana aplikasi seperti ini sering menjadi sasaran untuk disadap dari pihak ketiga yang tidak diinginkan oleh dua user yang saling berkomunikasi.

DESAIN APLIKASI



METODOLOGI

Langkah-langkah yang akan ditempuh dalam pengerjaan Tugas Akhir ini adalah:

1. **Pemahaman Sistem dan Studi Literatur**
   Mempelajari proses bisnis yang terjadi dan juga berbagai macam literatur tentang konsep-konsep yang berkaitan dengan rumusan masalah, antara lain konsep pembuatan perangkat lunak pada perangkat mobile dan konsep lain yang berhubungan.
2. **Pengumpulan dan analisis data**
   Dalam tahap ini akan dilakukan pengumpulan dan analisis terhadap data-data yang dibutuhkan.
3. **Perancangan Perangkat Lunak**
   Tahap ini merupakan tahapan analisis dan desain perangkat lunak yang akan dikembangkan dengan mengacu pada proses bisnis dan data yang telah diperoleh dan dianalisis pada tahapan sebelumnya.
4. **Implementasi**
   Pada tahap ini akan dilakukan proses pembuatan perangkat lunak yang akan dikembangkan.
5. **Ujicoba dan Evaluasi**
   Melakukan ujicoba dan evaluasi prototipe perangkat untuk mencari masalah yang mungkin timbul, mengevaluasi jalannya program, dan mengadakan perbaikan jika ada kekurangan.
6. **Pembuatan Buku Tugas Akhir**
   Pada tahap terakhir ini disusun buku sebagai dokumentasi dari pelaksanaan Tugas Akhir.

DAFTAR PUSTAKA

1. *Android News Website.* (2007) (diakses tanggal 12 April 2011) http://www.androidforums.com/
2. Mulyadi (2010). *Membuat Aplikasi untuk Android*. Multimedia Center Publishing.
3. Nikita Borisov, Ian Goldberg, Eric Brewer (2004). *Off-the-Record Communication, or, Why Not To Use PGP*. Workshop on Privacy in the Electronic Society. (diakses tanggal 12 April 2011).
4. Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson, Tadayoshi Kohno, Mike Stay (2000). *The Twofish Team's Final Comments on AES Selection* (diakses 12 April 2011)
5. Keith Palmgren. (2006) *Diffie–Hellman Key Exchange – A Non-Mathematician's Explanation.* NetIP
6. *Google Talk Center at BigBlueBall.* (2009) (diakses tanggal 12 April 2011)

http://www.bigblueball.com/im/googletalk/
7. *Smack Documentation.* (2008) (diakses tanggal 12 April 2011) http://www.igniterealtime.org/builds/smack/docs/latest/documentation/

JADWAL KEGIATAN

Tugas akhir ini diharapkan bisa dikerjakan menurut jadwal sebagai berikut:

No	Tahapan	Bulan				
		1	2	3	4	5
1	Pemahaman Sistem & Studi Literatur					
2	Pengumpulan & Analisis Data					
3	Perancangan Perangkat Lunak					
4	Pembuatan Perangkat Lunak					
5	Uji Coba dan Evaluasi					
6	Penyusunan Buku TA					

LEMBAR PENGESAHAN

Surabaya, 27 Oktober 2010

Menyetujui,

Pembimbing I

Ary Mazharuddin S, S.Kom, M.Comp.Sc
NIP.19810620 200501 1 003

Pembimbing II

Baskoro Adi Pratomo, S.Kom, M.Kom
NIP. 510000003