IMPLEMENTASI JARINGAN AD-HOC UNTUK PEMANFAATAN LIMA TEKNIK DASAR KRIPTOGRAFI SEBAGAI PENGACAKAN DATA AUDIO MENGGUNAKAN MATLAB

TUGAS AKHIR

Diajukan sebagai salah satu syarat
Untuk memperoleh gelar Ahli Madya dari
Politeknik Universitas Andalas Padang

Oleh :

HARRYO AZANOF
BP : 05075030

Program Studi Teknik Telekomunikasi
Jurusan Teknik Elektro

POLITEKNIK UNIVERSITAS ANDALAS
PADANG
2009

ABSTRAK

Perkembangan teknologi komunikasi yang semakin pesat selalu diikuti dengan perkembangan tindak kejahatan. Namun hal ini tidak diikuti oleh perkembangan sistem keamanan terutama file audio. Pada tugas akhir ini penulis mencoba memberikan salah satu solusi dengan memanfaatkan teknik dasar yang selama ini mendasari perkembangan metoda pengamanan data yaitu kriptografi yang dapat digunakan dan dikembangkan pada data audio. Sebagai pembuktian sistem ini, penulis menrealisasikannya pada jaringan wireless Ad-Hoc yang selama ini sangat rentan terhadap serangan dan memiliki tingkat keamanan yang masih rendah. Interface yang sederhana dengan fitur record audio secara langsung yang dilengkapi menu help yang menarik, memudahkan user untuk menggunakan aplikasi ini. Dalam pembuatan aplikasi ini digunakan Matlab versi 7.

Keyword: Kriptografi, Audio, Ad-Hoc

BAB I

PENDAHULUAN

1.1. Latar Belakang

Kemajuan teknologi di bidang Teknologi Informasi dan Telekomunikasi memungkinkan jutaan orang pengguna komputer di seluruh dunia terhubung dalam satu dunia *maya* yang dikenal sebagai *cyberspace* atau internet. Begitu juga ribuan organisasi seperti perusahaan, lembaga negara, lembaga keuangan, militer dan sebagainya tidak terlepas dari pengaruh berkembangnya dunia IT. Berbagai layanan dan fasilitas diberikan seperti *web*, *electronic mail* (*e-mail*), *newsgroups*, *chat* dan sebagainya.

Cara pengamanan data yang dapat digunakan, misalnya dengan adanya *kriptografi*. Ketika suatu pesan ditransmisikan dari suatu tempat ke tempat lain, isi pesan tersebut kemungkinan dapat disadap oleh pihak lain. Dalam *kriptografi*, untuk menjaga keamanan pesan, data atau pesan yang dikirimkan melalui jaringan akan disamarkan atau diubah menjadi kode yang tidak dimengerti oleh orang lain sedemikian rupa sehingga walaupun data tersebut dapat dibajak, tetapi tetap tidak akan bisa dimengerti oleh pihak yang tidak berhak.

Dalam perkembangan teknik *kriptografi*, jenis pesan yang diacak adalah text. Hal ini dikarenakan kebanyakan masyarakat lebih banyak menggunakan pesan text dalam berkomunikasi. Namun dalam perkembangannya, pesan text sudah jarang digunakan semenjak munculnya komunikasi suara. Perkembangan ini dibuktikan dengan adanya komunikasi *celluler* seperti GSM (*Global System*

for Mobile telecommunication) dan CDMA (*Code Division Multiple Access*), serta munculnya VoIP (*Voice Internet Protocol*) pada jaringan internet.

Perkembangan metoda dan berbagai teknik *kriptografi* pada masa sekarang tidak terlepas dari dasar yang menjadi landasan munculnya teknik tersebut. Sebagai dasar dalam mengembangkan suatu teknik modern, perlu dikembangkan untuk kelanjutannya. Teknik dasar ini yaitu *substitusi*, *blocking*, *permutasi*, *ekspansi* dan pemampatan. Jika teknik dasar ini digunakan lebih baik, maka tingkat keamanan data akan semakin meningkat. Selain itu, dengan menggunakan teknik modern yang telah disebarluaskan akan lebih mudah dalam pemecahan. Untuk itulah digunakan penggabungan yang lebih kompleks tingkat pengamanan data semakin tinggi.

Jaringan komputer yang menggunakan *wireless frekuensi* 2,4 GHz sudah mulai banyak digunakan. Penggunaannya yang selama ini digunakan mengharuskan *user* untuk terkoneksi dengan sebuah *access point* untuk dapat berkomunikasi dengan *user* lain yang terkoneksi dengan *access point* yang sama. Komunikasi jaringan *wireless* 2,4 GHz dapat dibentuk dengan membentuk jaringan baru yang disebut modus *Ad-Hoc*. Modus ini dapat membentuk *topologi mesh* dimana setiap *user* dapat terhubung langsung ke *user* lain tanpa harus menggunakan *access point*.

Kelemahan dari jaringan dengan menggunakan modus ini adalah seorang *user* lebih mudah untuk melakukan pembajakan. Baik itu untuk *sharing* data maupun dalam memanfaatkan fasilitas jaringan seperti aplikasi LAN-VoIP pada Net-Meeting. Untuk itu, diperlukan pengamanan pada modus ini.

BAB V

PENUTUP

5.1. Kesimpulan

1. Dengan memanfaatkan lima teknik dasar *kriptografi* pada data *audio*, data *audio* yang ditransmisikan terutama pada jaringan *Ad-Hoc* dapat dijaga dari penyadapan langsung.
2. Pengacakan dengan menggunakan data *sampling audio* tidak sempurna karena memerlukan waktu yang cukup besar untuk memproses data dan juga tidak dapat menjaga stabilitas data secara penuh.
3. Data *audio* yang ditransmisikan pada jaringan *Ad-Hoc* dapat dipertahankan dan kerusakan terjadi tidak terlalu mengganggu untuk dikembalikan ke *plain audio*.
4. Data *audio* yang berbentuk *stereo* sulit untuk dipertahankan karena harus memperhitungkan perbedaan setiap *channel stereo*.

5.2. Saran

1. Diharapkan transmisi yang digunakan langsung, tidak adanya penyimpanan data *audio* sebelum pengiriman untuk meningkatkan keamanan data *audio* yang akan dikirimkan.
2. Pengacakan tidak menggunakan titik *sampling* tapi pemotongan *audio* dengan *delay* yang sangat pendek untuk menjaga kualitas dan stabilitas data.
3. Sistem ini tidak menjaga stabilitas data *stereo*, diharapkan selanjutnya dapat mempertahankan data *stereo*.

DAFTAR PUSTAKA

Arhami, Muhammad, Anita Desiani. 2005. *Pemograman Matlab*. Andi Yogyakarta. Yogyakarta

Ariyus, Dony. 2005. *Computer Security*. Andi Yogyakarka. Yogyakarta

Hahn, Brian, Daniel T. Valentine. 2007. *Essential Matlab for Engineers and Scientists third edition*. Elsevier. Ltd. Oxford

http://lecturer.eepis-its.edu/
tribudiLN_SIP_Prakrev_01_Speech_prak_Lamp_MatlabAudio.pdf

http://en.wikipedia.org/wiki/Analog-to-digital_converter

http://en.wikipedia.org/wiki/Digital-to-analog_converter

http://en.wikipedia.org/wiki/Digital_signal_processing

http://www.mathwork.com

Kester, Walt. 2004. *Analog Digital Conversion Handbook*. Analog Devices, Inc. United State of America

Kurniawan, Yusuf. 2004. *Kriptografi, Keamanan Internet dan Jaringan Komunikasi*. Informatika Bandung. Bandung

Mukodin, Didin. *Tinjauan tentang Enkripsi dan Dekripsi, suatu teknik pengamanan data dengan penyandian RSA*. Jakarta.

Paulus, Erick, Yessica Nataliani. 2007. *GUI Matlab*. Andi Yogyakarta. Yogyakarta

Sugiharto, Aris. 2006. *Pemograman GUI dengan Matlab*. Andi Yogyakarta. Yogyakarta.

S'to. 2007. *Wireless Kung Fu Networking & Hacking*. Jasakom. Jakarta