PENGEMBANGAN VOIP MENGGUNAKAN ENKRIPSI BASE64

Bagus Budi Santoso, Erfan Rohadi

Program Studi Teknik Informatika, Jurusan Teknik Elektro, Politeknik Negeri Malang
[1]bagusbudi92@gmail.com, [2]erfanr@gmail.com

Abstrak

Komunikasi yang murah untuk dapat berkomunikasi dengan antar user. Selain murah dibutuhkan jalur komunikasi yang aman digunakan untuk dapat berkomunikasi. Komunikasi dikatakan aman adalah tidak adanya celah keamanan mengakibatkan komunikasi yang dilakukan dapat disadap. Dengan bertitik tolak dengan masalah yang terjadi, maka akan dicoba untuk membangun komunikasi jarak jauh berbasis Internet Protokol dengan menggunakan Internet sebagai jalur komunikasi bernama VoIP atau Voice Over Internet Protocol. Dengan keamanan menggunakan *stream cipher*

Kata kunci : komunikasi, keamanan, stream cipher

1. Pendahuluan

Seiring dengan berkembangnya teknologi internet menyebabkan hampir semua sistem komunikasi dan informasi di semua bidang menjadi lebih mudah dalam hal penggunaan serta pengembangan. Dengan terhubungnya komputer-komputer di dunia, memungkinkan untuk bertukar informasi dan komunikasi. Bahkan dapat saling bertukar informasi berupa gambar atau video. Perkembangan jaringan komputer yang semakin pesat ini memungkinkan untuk melewatkan data suara melalui jaringan komputer atau biasa yang disebut *Voice Over Internet Protocol* (*VoIP*). Media yang sudah banyak beredar sekarang banyak menggunakan teknologi itu dan biaya yang dikeluarkan dalam penggunaannya juga cukup besar, memanfaatkan teknologi yang sedang berkembang saat ini yaitu internet dan jaringan komputer sehingga dapat mendukung sistem komunikasi *voice* dan *video.*

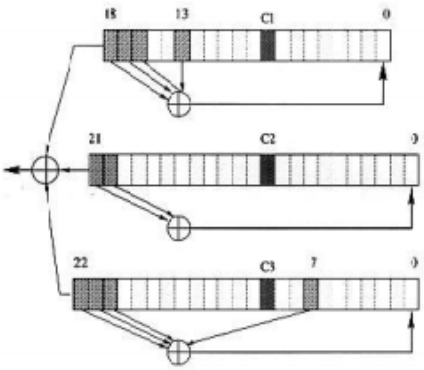
2. Tinjauan Pustaka

2.1 Komunikasi

Komunikasi adalah proses pengiriman (sending) dan penerimaan (receiving) pesan atau berita (informasi) antara dua individu atau lebih dengan cara yang efektif sehingga pesan yang dimaksud dapat dipahaami.

2.2 Stream Cipher

Metode yang digunakan untuk unit plaintext yang besar sedangkan stream cipher digunakan untuk blok data yang lebih kecil, biasanya ukuran bit. Proses enkripsi terhadap plaintext tertentu dengan algoritma block cipher akan menghasilkan ciphertext yang sama jika kunci yang sama digunakan. Dengan stream cipher, transformasi dari unit plaintext yang lebih kecil ini berbeda antara satu dengan lainnya, tergantungpada kapan unit tersebut ditemukan selama proses enkripsi.



Tiap bit yang berada pada posisi paling kanan pada tiap-tiap LFSR diberi nama sebagai bit ke-0. Untuk LFSR pertama, ketukan dikenakan pada bit ke- 13, ke-16, ke 17, dank ke-18. Untuk LFSR ke-2, ketukan dikenakan pada bit ke-20 dan ke-21. Untuk LFSR ke-3 ketukan dikenakan pada bit ke -7 , ke-20, ke-21, dank ke-22. Pada tiap satu clocked, tiap bit-bit ketukan yang dimiliki oleh masing-masing LFSR dilakenakan operasi XOR. Hasil operasi tersebut akan disimpan pada bit ke-0 untuk tiap LFSR

2.3 *Voice Over Internet Protocol*

Voice over Internet Protocol adalah Teknologi yang menjadikan media internet untuk bisa melakukan komunikasi suara jarak jauh secara langsung. Sinyal suara analog, seperti yang anda dengar ketika berkomunikasi di telepon diubah menjadi data digital dan dikirimkan melalui jaringan berupa paket-paket data secara real time. Dalam komunikasi VoIP, pemakai melakukan hubungan telepon melalui terminal yang berupa PC atau telepon biasa. Dengan bertelepon menggunakan VoIP, banyak keuntungan yang dapat diambil diantaranya adalah dari segi biaya jelas lebih murah dari tarif telepon tradisional, karena jaringan IP bersifat global.

Sehingga untuk hubungan Internasionaldapat ditekan hingga 70%. Selain itu, biaya maintenance dapat di tekan karena voicedan data networkterpisah, sehingga IP Phone dapat di tambah, dipindah dan di ubah. Hal ini karena VoIP dapat dipasang di sembarang *ethernet* dan *IP address*.

3. Design dan Implementasi

3.1 Analisis

Pada bagian ini akan ditunjukan design model dan struktur implementasi dari solusi yang ditawarkan.

3.1.1 Deskripsi Umum

Aplikasi ini adalah bentuk dari keamanan untuk VoIP dengan menggunakan enkripsi agar data berupa suara antar client tidakmudah di dengar.*Stream Cipher* merupakanalgoritma enkripsi simetri. Stream cipher dapat dibuat sangat cepat sekali, jauh lebih cepat dibandingkan dengan algoritma block cipher yang manapun dimana Satu stream cipher menghasilkan apa yang disebut suatu keystream (suatu barisan bit yang digunakan sebagai kunci). Proses enkripsi dicapai dengan menggabungkan keystream dengan plaintext biasanya dengan operasi bitwise XOR.

Aplikasi keamanan VoIP menggunakan metode *Stream Cipher* diharapkan dapat membantu *client* atau *user* untuk lebih aman menggunakan VoIP.

3.1.2 Arsitektur Sistem

Secara umum sistem akan bekerja dengan penulisan alamat ip dalam satu area (local) dan dapat saling terhubung satu dengan yang lain selama berada pada satu area

4. Uji Coba dan Evaluasi.

4.1 Spesifikasi Hardware

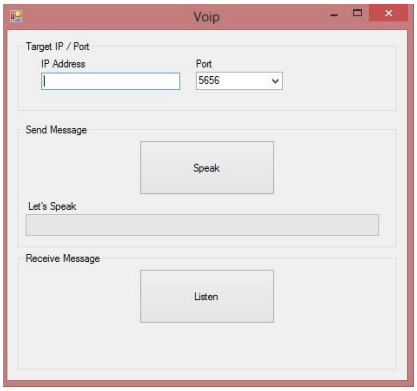
a. Processor, Intel(R) Core(TM) i3 CPU.
b. RAM, 2.00GB.

4.2 Spesifikasi Software

a. Microsoft Windows 8.1.
b. Microsoft Visual Studio 2010.
c. Microsoft .NET Framework 4.5.

4.3 Perancangan Proses

Pada bagian ini adalah proses utama yang ada pada aplikasi yang dibangun. Pada aplikasi ini terdapat proses penulisan ip yang digunakan.

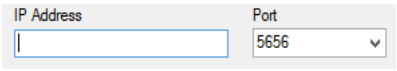


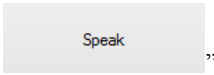
Gambar 1. Penulisan IP

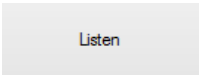
4.4 Proses Komunikasi

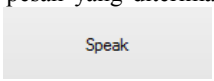
4.4.1 Komunikasi antar Client

Untuk melakukan proses menghubungi client tujuan adalah sebagai berikut :



1. Isi ip address tujuan yang ingin dihubungi dan pilih port yang ingin digunakan.
2. Klik 

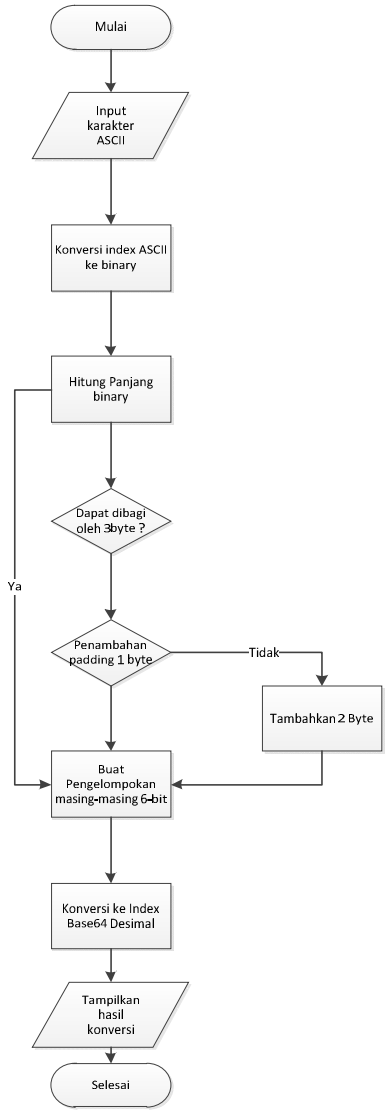
”Speak” untuk memulai record suara yang akan dikirim beserta filename yang diinginkan.
3. Klik 

“Listen”untuk menerima suara yang dikirimkan oleh pengirim dan suara yang dikirimkan oleh pengirim akan terdengar.
4. Jika ingin membalas pesan yang diterima maka dapat langsung klik 

untuk mengirim kembali balasan yang diinginkan.

Flowchart Alur Algoritma

Flowchart merupakan serangkaian bagian-bagian yang berfungsi untuk menerangkan alur dari jalannya algoritma. Dalam aplikasi voip ini algoritma yang di pergunakan Base64.



Gambar 2. Algoritma Umum Encoding

Berdasarkan Gambar 5.2, maka algoritma umum proses encoding dari ASCII ke Base64 dimulai dari input karakter ASCII lalu mengkonversikan *index* ASCII menjadi *biner* setelah menjadi biner, biner tersebut dihitung panjangnya dapat di bagi menjadi *3byte* jika bisa ditambahkan *padding*1 *byte* dibuatlah pengelompokan masing-masing menjadi 6 *bit* setelah itu akan terlihat hasil konversi.

5. Kesimpulan dan Saran

5.1 Kesimpulan

Dari aplikasi ini dapat diperoleh beberapa kesimpulan sebagai berikut :

a. Aplikasi ini dapat digunakan pada satu area network dan data diamankan menggunakan key private
b. Aplikasi yang dibangun pada artikel ini dapat membantu user untuk berkomunikasi langsung tanpa membayar

5.2 Saran

Pada penelitian ini aplikasi yang dibuat untuk mengamankan data berupa suara. Menjadi lebih efisien dapat dilakukan penelitian lanjutan dengan menggunakan *platform* Java yang lebih banyak pengguna dan sebaiknya menggunakan server untuk lebih terorganisir untuk user.

Daftar Pustaka:

Kurniawan, A. 2012. Network Forensics *Panduan Analisis dan Investigasi Paket Data Jaringan Menggunakan Wireshark*. Yogyakarta : Penerbit Andi.

Garrison, K. and Dempster B. 2006. *A Step-by-step guide to installing and running your home and office VOIP system*. Birmingham mumbai: Packt Publishing Ltd

Markus, F. and Norbert G. 2009. *Build and integrate Virtual Private Network using OpenVPN*. Birmingham mumbai: Packt Publishing Ltd

Henrik,I. 2009 *Session Initiation Protocol (SIP) and Another Voice Over IP (VoIP) Protocols and Applications*. Finland: Sesca technologies

Darmayuda, Ketut.2010. *Pemrograman Aplikasi Database Dengan Microsoft Visual Basic.NET* 2008.Bandung : Informatika

Febrian Wahyu, Adriana, Febry. 2012 "*Penerapan Algoritma Gabungan RC4 dan Base64 Pada Sistem Keamanan E-Commerce*"

Adriansyah, Yusuf. 2010. *Enkripsi Sederhana dengan Base64 dan Subtitusi Monoalfabetik ke Huruf Non-Latin. Makalah Mahasiswa* Teknologi Bandung.

Mesran, 2009. *Visual Basic*, Mitra wacana Media.

Binanto, 2010. "*Multimedia Digital Dasar Teori + Pengembangan,* Yogyakarta: Penerbit: Andi.

Madcoms. 2004. *Referensi Microsoft Visual Basic.Net*, Yogyakarta:Penerbit: Andi

Kurniawan dan Erick. 2010. *Cepat Mahir Visual Basic 2010*.Yogyakarta: Penerbit: Andi

S. Josefsson 2003**.** *The Base16, Base32, and Base64 Data Encodings*.

Ardiat, Badai. 2012. *Awal Mula MP3*. [Online] Tersedia: http://badaiardiat.blogspot.com/2009/07/awal-mula-mp3.html. [7 Oktober 2012]

http://www.theasciicode.com.ar/[diakses pada tanggal 17 juli 2014]