Analisis Keamanan *Voice Over Internet Protocol* (VOIP)*Menggunakan PPTP dan ZRTP*

Jupriyadi[1], Dwi Prastantio Putra[2], Syaiful Ahdan[3]
[1,3]Program Studi Teknologi Informasi, Universitas Teknokrat Indonesia, Lampung
[2]Program Studi Informatika, Universitas Teknokrat Indonesia, Lampung
e-mail: [1]jupriyadi@teknokrat.ac.id,[2]prastantio.26193@gmail.com,
[3]syaifulahdan@teknokrat.ac.id

Abstrak

Voip merupakan teknologi komunikasi berbasis internet yang dapat melewatkan data, suara dan video. Sisi keamanan penggunaan voip perlu diperhatikan karena memungkinkan beberapa komunikasi yang dilakukan bersifat rahasia dan data yang melewati jaringan juga memungkinkan untuk di sadap. Salah satu teknik yang dapat dilakukan untuk mengamankan komunikasi voip adalah menggunakan enkripsi pada aplikasi voip atau melewatkan trafik voip melalui VPN. Pada penelitian ini dilakukan pengujian terhadap voip tanpa menggunakan sistem keamanan, voip menggunakan *Zimmermann Real Time Transport Protocol* (ZRTP), dan voip dilewatkan melalui VPN untuk melihat sisi keamanannya. Berdasarkan hasil penelitan yang dilakukan diperoleh hasil bahwa perlu diterapkan sistem keamanan voip agar data voip tidak bisa disadap. Tanpa menggunakan sistem keamanan data voip berupa suara dapat disadap dengan mudah, sedangkan dengan menggunakan sistem keamanan data voip tidak dapat sadap. Penggunaan ZRTP pada aplikasi voip dan voip yang dilewatkan melalui VPN membuat data yang dikirim menjadi diacak sehingga meskipun data dapat dicapture namun suaranya tidak dapat didengarkan.

Kata kunci— keamanan voip, PPTP, virtual private network, ZRTP

Abstract

Voip is an internet-based communication technology that can pass data, voice and video. The security side of using voip needs to be considered because it allows some communication to be carried out confidentially and data that passes through the network is also possible to be tapped. One technique that can be done to secure VoIP communication is to use encryption on the VoIP application or pass VoIP traffic through VPN. In this research, testing on voip without using a security system, voip uses Zimmermann Real Time Transport Protocol (ZRTP), and voip is passed through VPN to see the security side. Based on the results of research conducted obtained results that need to be implemented voip security system so that voip data can not be tapped. Without using a voip data security system in the form of voice can be tapped easily, while using a voip data security system cannot be tapped. The use of ZRTP on voip and voip applications that are passed through VPN makes the data sent to be encrypted so that even though the data can be captured, the sound cannot be heard.

Keywords—*voip security,PPTP,* A,*virtual private network, ZRTP*

1. PENDAHULUAN

Seiring pesatnya perkembangan jumlah komputer yang saling terhubung dengan lainnya dan yang biasa disebut dengan jaringan komputer, maka munculah teknologi-teknologi baru, yaitu teknologi yang saling menghubungkan komputer di dunia, yang memungkinkan untuk dapat saling bertukar informasi dan data, bahkan dapat saling berkomunikasi dan bertukar informasi berupa gambar atau video[1][2]. Perkembangan jaringan komputer yang semakin pesat memungkinkan untuk melewatkan trafik suara melalui jaringan komputer atau yang biasa disebut VoIP (*Voice Over Internet Protocol*). Voip banyak digunakan karena lebih murah dibandingkan dengan biaya telpon konvensional sehingga dapat digunakan dalam sebuah instansi [3][4].

Teknologi VoIP merupakan teknologi yang menawarkan layanan transmisi data suara secara langsung (real time) dengan menggunakan Internet Protocol [5]. Akan tetapi komunikasi VoIP tidak memiliki jaminan keamanan terhadap data pada komunikasi suara yang sedang berlangsung, tidak menutup kemungkinan pihak lain yang tidak berwenang melakukan penyadapan terhadap komunikasi tersebut, seperti : pembajakan terhadap isi data (sniffing) ataupun tidak dapat mengakses server dikarenakan server kelebihan muatan *(denial of service*).

Penanggulangan dari beberapa hal tersebut adalah dengan pengimplementasian metode keamanan data terhadap layanan VoIP, diantaranya dengan implementasi keamanan protokol VPN PPTP dan ZRTP (Zimmermann Real Time Transport Protocol)[6]. “VPN merupakan jaringan public yang menekankan pada keamanan data dan akses global melalui internet” (Putranto. 2009). Penggunaan Virtual Private Network (VPN) merupakan salah satu alternatif untuk mengirimkan voice, yang bersifat private atau aman, karena penggunaan koneksi yang telah terenkripsi serta penggunaan private keys, certificate, username atau password untuk melakukan authentikasi dalam membangun koneksi [7][8]. ZRTP (Zimmermann Real-Time Transport Protocol) menghasilkan shared secret antara initiator dan responder yang kemudian digunakan untuk menghasilkan kunci Secure RTP (SRTP). ZRTP menggunakan pertukaran kunci Diffie-Hellman yang menegosiasikan kunci untuk mengenkripsi suara pada komunikasi VoIP. Pertukaran kunci tersebut yang akan menjaga suara atau komunikasi yang sedang berlangsung dari serangan pada komunikasi VoIP. Sehingga enkripsi yang dihasilkan adalah end to end antara pemanggil dan penerima.

2. METODE PENELITIAN

Dalam melaksanakan penelitian, dibutuhkan perangkat keras dan perangkat lunak yang dapat dilihat pada tabel berikut ini.

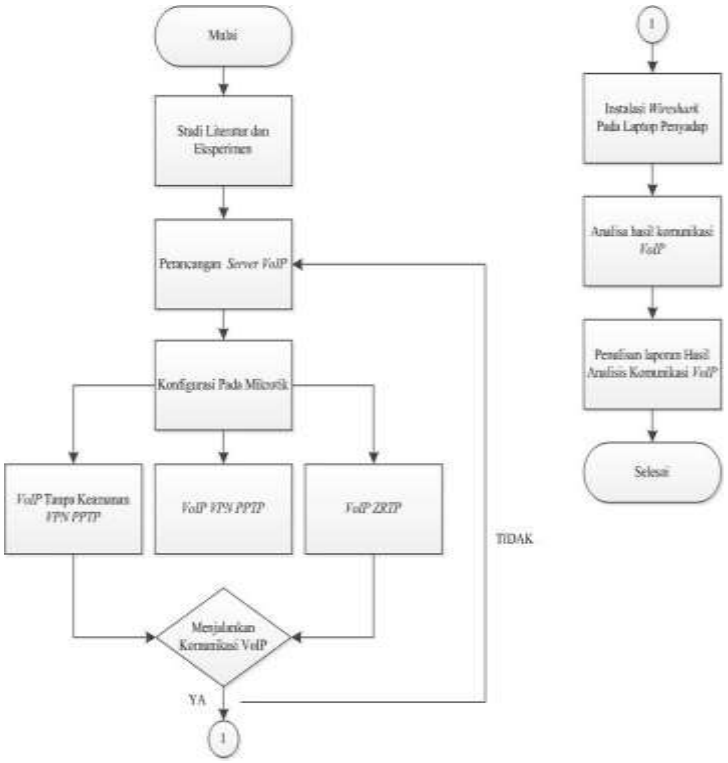
Tabel 1 Spesifikasi perangkat keras

Perangkat Keras	***Client***	***Server***
Processor	Core i3 – 2,20 GHz	*AMD A10 7700k – 3,4 GHz*
Memory	*2 GB DDR 3*	*4 GB*
Harddisk	*250 GB*	*250 GB*
Operating System	*Windows 7*	*Ubuntu 12.04*
Router		

Tabel 2 Perangkat lunak yang digunakan

Nama Perangkat	Perangkat Lunak	Keterangan
VoIP Server	*Asterisk*	Sebagai komunikasi antar *client VoIP* dan *server VoIP*.
Mikrotik	*VPN PPTP*	Sebagai *VPN server* yang berfungsi membuat *tunnel Host-to-Host.*
Client	*Zoiper*	Sebagai *VoIP client*
Penguji	*Wireshark*	Sebagai *packetsniffer, RTP (Realtime Transfer Protocol) decoder*, dan *RTP Player*

Dalam melaksanakan penelitian, tahapan yang dilakukan penulis berdasarkan flowchart seperti tampak pada gambar 1 berikut ini.

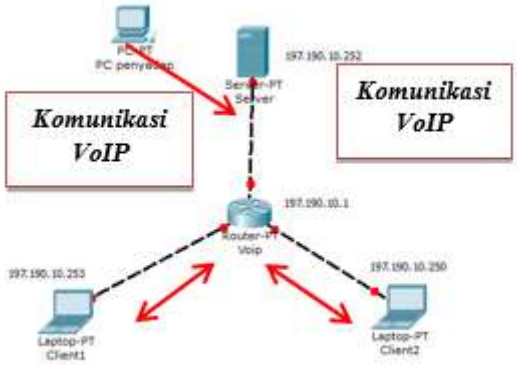


Gambar 1 Tahapan eksperimen yang dilakukan

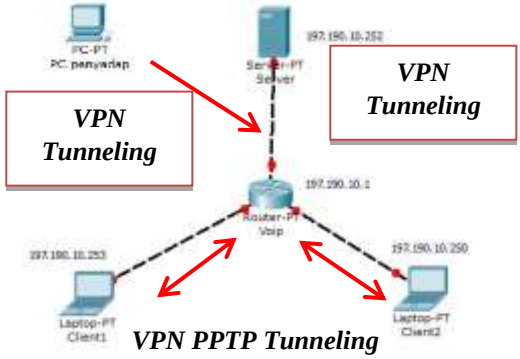
2. 1. Desain Pengujian

Dalam melakukan pengujian dilakukan 3 (tiga) skenario pengujian yaitu 1) Pengujian VOIP tanpa menggunakan sistem keamanan (gambar 2); 2) Pengujian VOIP menggunakan sistem keamanan ZRTP (gambar 3); 3) Pengujian VOIP menggunakan sistem keamanan PPTP (gambar 4)

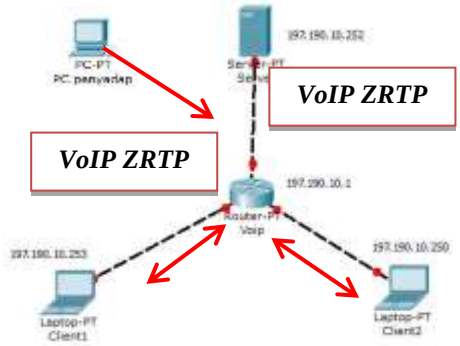
.



Gambar 2 Topologi pengujian *VoIP* tanpa keamanan



Gambar 3 Topologi pengujian *VoIPVPN PPTP*



Gambar 4 Topologi pengujian *VoIPZRTP*

Pada ketiga gambar tersebut nantinya akan di lakukan penyadapan sebagai pengujian keamanan, penyadapan dilakukan untuk menangkap data pada komunikasi yang sedang berlangsung antara *Client1* dengan *Client2*. Pengujian dilakukan menggunakan beberapa skenario. Skenario tersebut dibuat dengan tujuan untuk membuktikan keamanan *VoIP* pada sistem yang berbeda yang ditampilkan pada tabel berikut.

Tabel 3 Skenario Pengujian

No	Sistem VoIP	Pengujian
1	Tanpa menggunakan sistem keamanan	Dilakukan penyadapan paket menggunakan wireshark
2	Menggunakan keamanan PPTP	Dilakukan penyadapan paket menggunakan wireshark

3	Menggunakan keamanan ZRTP	Dilakukan penyadapan paket menggunakan wireshark

2. 2. Instalasi VoIP Server

VoIP server adalah komputer yang menyediakan layanan VoIP. VoIP server yang digunakan yaitu Asterisk yang berjalan pada sistem operasi Ubuntu 12.04 LTS [9]. Kebutuhan hardware dari VoIP server adalah sebagai berikut (tabel 4).

Tabel 4 Spesifikasi *Hardware VoIP Server*

Perangkat Keras	Spesifikasi
Processor	*1.6*
Memory	*4 GB*
Harddisk	*250 GB*
Operating System	*Ubuntu 16.04 LTS*
Ethernet	✓
Mouse	✓
Keyboard	✓
Monitor	✓

2. 2. 1. Installasi Server Asterisk

Installasi *Asterisk*dimulai dengan cara perintah "apt-get". Langkah untuk installasi *Asterisk*adalah sebagai berikut:

a. Pada terminal, ketik perintah ***sudo apt-get install asterisk***.
b. Untuk menjalankan *Asterisk*, gunakan perintah ***#service asterisk start*** pada terminal.

2. 2. 2. Pembuatan SIP ID

SIP ID digunakan sebagai pengalamatan pada *VoIP*[10]. Pengalamatan *SIP ID* yang digunakan yaitu sebagai berikut:

Tabel 5 Daftar SIP ID yang digunakan

IP Address	*SIP ID*	Keterangan
197.190.10.253	2001	*User* A (pras 1)
197.190.10.250	2002	*User* B (pras 2)

Pembuatan *SIP ID* pada *Asterisk* dilakukan dengan cara mengedit *file"/etc/asterisk/sip.conf"*. *File sip.conf* merupakan *file* konfigurasi dari *Asterisk*dan memiliki tipe *XML*, berikut ini adalah langkah dalam pembuatan *SIP ID:*

a. Pada terminal, buka file *sip.conf* dengan menggunakan perintah *nano /etc/asterisk/sip.conf*
b. Untuk menambahkan SIP 2000 pada */etc/asterisk/sip.conf* berikut konfigurasinya.

```
[general]
Port = 5060
Context = other
Bindaddr = 0.0.0.0
Srvlookup=yes
Allow=all

[2000]
Type=friend
Context=phones
Username=2000
Secret=1234
Host=dynamic
Nat=no
Directmedia=no
Dtmfmode=rfc2833
Allow=ulaw
Allow=alaw
Allow=gsm
```

c. Untuk menambahkan SIP ID 2001 berikut konfigurasinya,

```
[2001]
Type=friend
Context=phones
Username=2001
Secret=12345
Host=dynamic
Nat=no
Directmedia=no
```

```
Dtmfmode=rfc2833                    Allow=alaw
Allow=ulaw                          Allow=gsm
```

Simpan *file* dengan cara menekan tombol *"Ctrl+x"*, lalu mengetikkan karakter "Y" kemudian Enter.Setelah pembuatan *SIP ID* pada *Asterisk* dilakukan maka tahapan selanjutnya ialah membuat *file extensions* pada *asterisk* dengan cara mengedit *file"/etc/asterisk/extensions.conf"*, berikut *file extensions* ini adalah langkah dalam pembuatan *:*

```
[others]
[phones]
Exten =>2000,1,Answer()
Exten => 2000,n,Dial(SIP/2000)
Exten => 2000,n,Hangup

Exten => 2001,1,Answer()
Exten => 2001,n,Dial(SIP/2001)
Exten => 2001,n,Hangup
```

2. 3. Implementasi VoIP Client

Komputer *client* dapat menggunakan layanan *VoIP* melalui aplikasi *VoIPclient*. Aplikasi *VoIP client* yang digunakan adalah *phonerlite* versi 2.42. Spesifikasi dari perangkat keras yang digunakan yaitu:

Tabel 6 Kebutuhan perangkat keras c*lient*

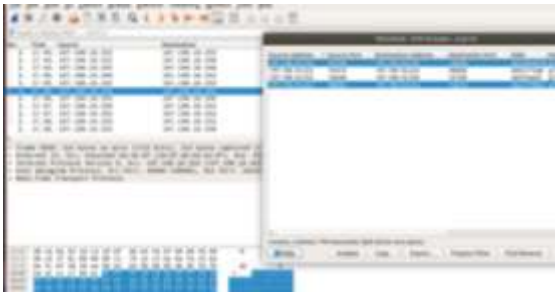
Hardware	Spesification
Processor	2,20 *GHz*
Memory	2048 *MB*
Harddisk	500 *GB*
Operating System	*Windows 7 Ultimate*
Audio Microphone / Speaker	✓

3. HASIL DAN PEMBAHASAN

3.1. Pengujian *VoIP* Tanpa Pengamanan

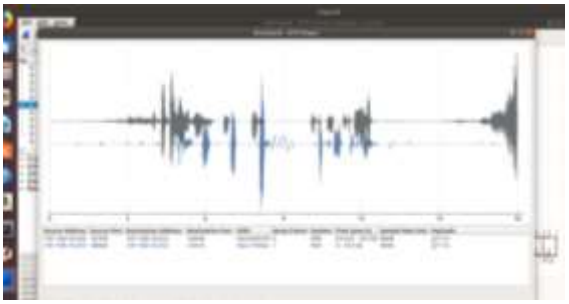
Untuk melihat keamanan *VoIP* dapat dilakukan setelah kita mendapatkan paket *RTP* dari *sniffing packet* yang dilakukan pada proses sebelumnya menggunakan aplikasi *wireshark*. Untuk langkah pengujian performa dapat dijelaskan seperti berikut:

a. Pada file hasil penyadapan, pilih tab *RTP Streams* kemudian *Analyze*. Akan muncul tampilan seperti gambar berikut.



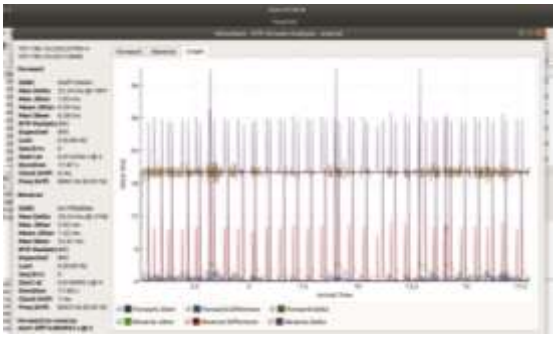
Gambar 5 Wirehark untuk menyadap *RTP Stream*

b. Pada gambar 6 dapat dilihat bahwa komunikasi *VoIP* yang berlangsung tanpa keamanan dapat di sadap dan di *capture* hasil komunikasi berupa suara saat komunikasi antar client.



Gambar 6 Hasil sadapan di putar menggunakan *RTP Player*

c. Pada gambar 7 dapat dilihat secara jelas statistik dari grafik komunikasi *VoIP* yang sedang berlangsung tanpa keamanan komunikasi.



Gambar 7 *RTP Stream Analysis Graph*

3.2. Pengujian VoIP VPN PPTP

Pada skenario ini dilakukan pengujian sebelum komunikasi *VoIP* berlangsung pada dasarnya sama seperti pengujian sebelumnya. Untuk langkah mengaktifkan mode keamanan *VPN PPTP* dan penyadapan pada *VoIP client* dapat dijelaskan seperti berikut:

a. Koneksikan laptop *client* dalam mode jaringan *VPN PPTP*, hubungkan *VPNPPTP* pada *notification area*, lalu klik *connect*, masukkan *username* serta *password* seperti yang telah dibuat pada *VPN PPTPserver* pada *mikrotik*. Tunggu proses *verifying username* and *password* selesai, kemudian terkoneksi seperti gambar dibawah ini.

Gambar 8 *ClientVPN PPTP Connected*

b. Setelah itu lakukan panggilan antar *user* Client1 dengan Client2 seperti pengujian yang dilakukan sebelumnya.
c. Kemudian setelah *wireshark* dari laptop *attacker* menangkap paket dari komunikasi tersebut, maka akan terlihat paket *RTP* seperti gambar dibawah ini.

Gambar 9 Penyadapan menggunakan wireshark terhadap paket *VPN PPTP*

d. Untuk melihat *stream audio* pilih *Telephony VoIP Call*, kemudian akan tampil seperti gambar dibawah ini.

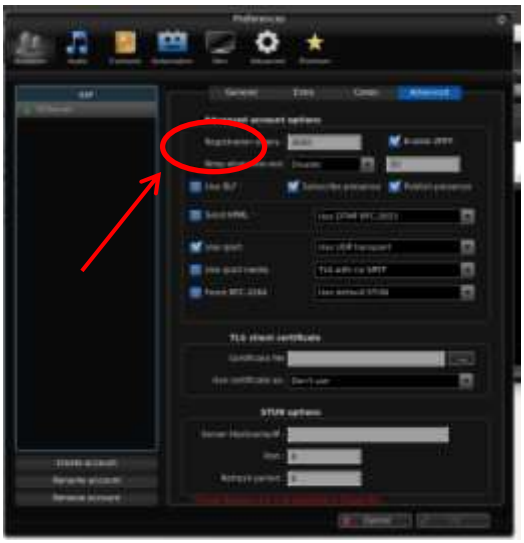
Gambar 10 Deteksi Komunikasi *VoIP VPN PPTP*

e. Pada tampilan tersebut tidak ada komunikasi *VoIP* yang terdeteksi, jadi *SIP* tidak terdeteksi.

3.3. Pengujian Keamanan VoIP ZRTP

Pada skenario ini dilakukan pengujian sebelum komunikasi *VoIP* berlangsung pada dasarnya sama seperti pengujian sebelumnya. Untuk langkah mengaktifkan mode keamanan *ZRTP* dan penyadapan pada *VoIP client* dapat dijelaskan seperti berikut:

a. Aktifkan mode *ZRTP* pada aplikasi *zoiperuserclient*1 dan *client*2, lalu mulai komunikasi antar *user* seperti skenario sebelumnya. Untuk mengaktifkan mode *ZRTP* dapat dilihat seperti gambar dibawah, ceklist *ZRTP* lalu *ok*.



Gambar 11 *ZRTP* Pada *ZOIPER*

b. Pada penyadapan *wiresharkakan* tampil *fileRTP* yang dilindungi oleh protokol *ZRTP*, seperti gambar dibawah ini. Bukti bahwa protokol *ZRTP* mengamankan paket *RTP* dalam komunikasi *VoIP*.

Gambar 12 Komunikasi *ZRTP* Pada *Wireshark*

c. Untuk membuktikan keamanan *ZRTP* pada *RTP*, pilih menu *Telephony* kemudian pilih *VoIP Call*, kemudian *Play Streams*. Akan tampil seperti gambar dibawah.

Gambar 13 Deteksi Komunikasi *ZRTP*

d. Untuk mendengarkan *audio* dari *RTP Stream* tersebut klik *icon play*.
e. Audio percakapan antar *userclient*1 dengan *client*2 tidak dapat didengarkan..

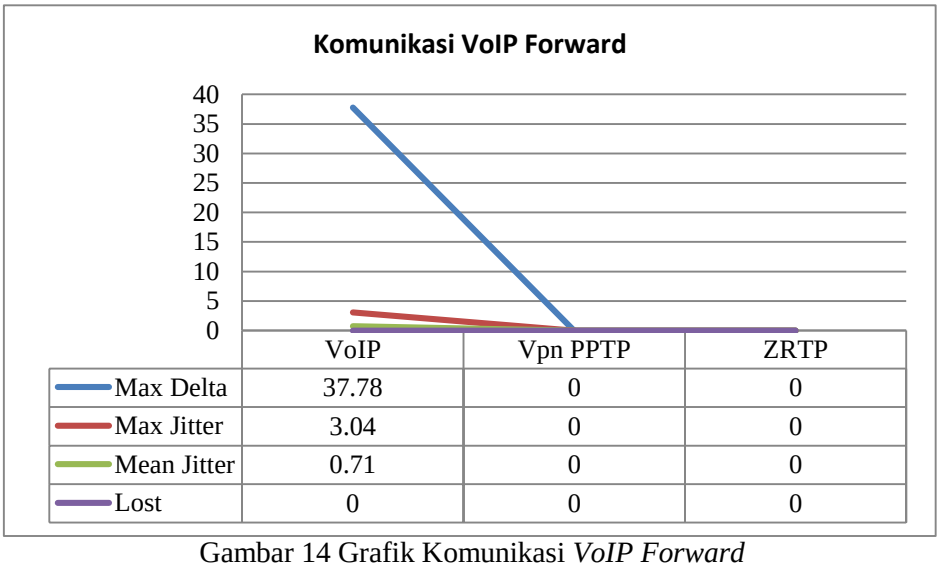
3.4. Analisis Keamanan VoIP

Analisis performa dilakukan dengan melakukan perbandingan dan pengukuran terhadap parameter-parameter pada komunikasi *VoIP* yang telah di bangun dan diambil data dari implementasinya yang telah diperoleh dari pengujian ke tiga sistem komunikasi *VoIP* tersebut.

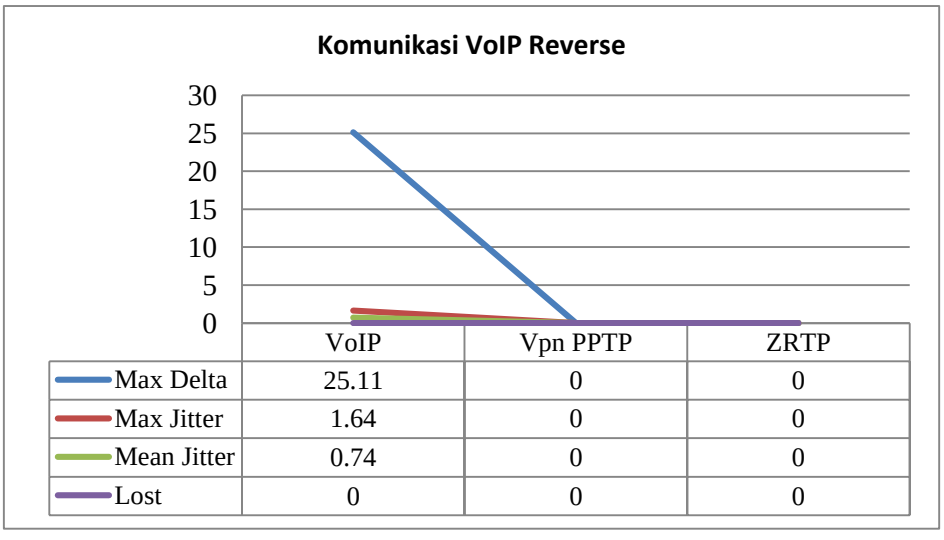
Tabel 7 Perbandingan *VoIP*

Pengujian	Capture	
	Deteksi Voip	RTP Stream
VoIP	Terdeteksi	Terdeteksi
VoIP dengan ZRTP	Terdeteksi	Tidak terdeteksi
VoIP dengan VPN PPTP	Tidak terdeteksi	Tidak terdeteksi

Berikut ini adalah data yang diperoleh terhadap performa komunikasi VoIP forward dan reverse dari penyadapan yang dilakukan menggunakan wireshark.



Gambar 14 Grafik Komunikasi *VoIP Forward*



Gambar 15 Grafik Komunikasi *VoIP Reverse*

4. KESIMPULAN

Setelah melakukan serangkaian implementasi pembangunan *VoIP* dan pengujian dengan skenario yang telah dijelaskan pada bab sebelumnya, dapat disimpulkan sebagai berikut :

1. Sistem keamanan yang paling baik adalah menggunakan VPN PPTP karena komunikasi tidak terdeteksi saat dilakukan penyadapan.
2. Sistem komunikasi *VoIP* tanpa keamananapabila diserang dapat mengetahui hasil komunikasi yang sedang berlangsung dan di *capture* hasil suara berdasarkan *VoIP Call Detect* dan *RTP Player*
3. Sistem komunikasi *VoIP VPN PPTP* apabila diserang tidak dapat mengetahui hasil komunikasi yang sedang berlangsung dan di *capture* hasil suara berdasarkan *VoIP Call Detect* dan *RTP Player*
4. Sistem komunikasi *VoIP ZRTP* apabila diserang dapat mengetahui hasil komunikasi yang sedang berlangsung tetapi tidak dapat di *capture* hasil suara berdasarkan *RTP Player*

5. SARAN

Perlu dilakukan penelitan lanjutan untuk mengetahui performa dari penerapan masing-masing sistem keamanan. Seberapa besar pengaruh penerapan sistem keamanan terhadap kinerja dari komunikasi VoIP.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada tim peneliti yang bekerjasama membuat penelitian ini dan Universitas Teknokrat Indonesia yang selalu mendukung untuk penelitian ini.

DAFTAR PUSTAKA

[1] Arta, Y., 2014. *"Asterisk : Implementasi VoIP Pada Biro Administrasi Informatika Teknologi Universitas Islam Riau",* Jurnal SAINS Vol.4 No.1 Januari. ISSN : 2252-9608.

[2] Izmail, M.N., 2010. *"Analysis of Secure Real Time Transport Protocol on VoIP Over Wireless LAN in Campus Environment",* International Journal on Computer Science Engineering, Vol.2 No.3. ISSN : 0975-3397.

[3] Manggau, F.X., Mangera, P., dan Loppies, S., 2012. *"Layanan Suara Berbasis Intranet Pada LAN Universitas Musamus Merauke",* Jurnal Ilmiah Mustek Anim Ha Vol.1 No.1 April. ISSN : 2089-6697.

[4] Rudiansyah., Herlawati., dan Sari, Puspita, E., 2013*, "Perancangan Voice Over Internet Protocol (VoIP) Menggunakan Virtual Private Network (VPN) Pada Pt Care Technologies".* Jurnal Techno Nusa Mandiri Vol. IX No.1 Maret.

[5] Budianto, E., Rachmawati, R.Y., dan Andayanti, D., 2015. *"Implementasi VoIP Menggunakan ZRTP, G.729A, Dan FreeSWITCH"*, Jurnal JARKOM, Vol.3 No.1 Desember. ISSN : 2338-6313.

[6] Callas, J., et al. 2011. *"ZRTP : Media Path Key Agreement for Unicast Secure RTP",* Internet Engineering Task Force (IETF) RFC 6189, ISSN : 2070-1721.

[7] Habibi, Ahmad., dan Arifin, Samsul., 2009. *"Membangun Jaringan Virtual Private Network (VPN) Dengan Metode Tunneling Menggunakan Mikrotik Untuk Komunikasi Lokal Di STMIK PPKIA Pradnya Paramita Malang".* Jurnal Teknologi Informasi STMIK PPKIA Volume 6 No. 2.

[8] Octavia, H., 2013. *"Unjuk Kerja Penerapan Teknologi VoIP Pada Jaringan VPN (Virtual Private Network)",* Jurnal Elektron, Vol.5 No.2 Desember. ISSN : 2085-6989.

[9] Datarkar, T., Bobade, N.P., and Gaikwan, M.A., 2015. *"Voice Over Internet Protocol (VoIP) Based On Asterisk",*International Journal of Applied Research June 2015. ISSN : 2394-5869.

[10] Setiawan, Budi, Eko., 2012. *"Analisa Quality Of Services (QOS) Voice Over Internet Protocol (VoIP) Dengan Protokol H.323 Dan SessionInitial Protocol (SIP)".* Jurnal Ilmiah Komputer dan Informatika (KOMPUTA) Volume 1 No. 2, Oktober. ISSN : 2089-9033