

# BAB I PENDAHULUAN

## 1.1. Latar Belakang

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*. Perkembangan jaringan komputer yang semakin pesat memungkinkan untuk melewati trafik suara melalui jaringan komputer atau yang biasa disebut *VoIP (Voice Over Internet Protocol)*.

“Teknologi (*Voice Over Internet Protocol*) *VoIP* merupakan teknologi yang menawarkan layanan transmisi data suara secara langsung (*real time*) dengan menggunakan *Internet Protocol*” (Eko Budi Setiawan. 2012). 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)*. “*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 autentikasi dalam membangun koneksi. *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. (Zimmermann, dkk. 2011)

Berdasarkan latar belakang diatas penulis mencoba untuk melakukan pengujian komunikasi *VoIP* dengan menggunakan metode keamanan *VPN PPTP* dan *ZRTP* untuk meminimalisir terjadinya penyadapan, maka penulis mengangkat judul skripsi “Analisis Keamanan *Voice Over Internet Protocol (VoIP) Over Virtual Private Network (VPN)*” dengan tujuan untuk mengetahui hasil pengujian komunikasi *VoIP* dengan menggunakan metode keamanan *VPN PPTP* dan *ZRTP* apabila dilakukan penyerangan pada saat komunikasi *VoIP* berlangsung.

## **1.2. Rumusan Masalah**

Berdasarkan latar belakang yang sudah diuraikan sebelumnya, maka penulis merumuskan permasalahan pada skripsi ini, yaitu:

1. Bagaimana membuat *VoIP* untuk keperluan komunikasi dengan menggunakan *VPN PPTP* dan *ZRTP* sebagai metode keamanan?
2. Seberapa besar pengaruh implementasi metode keamanan *VPN PPTP* dan *ZRTP* terhadap serangan yang dilakukan pada komunikasi *VoIP*?
3. Bagaimanakah hasil dari pengujian metode keamanan *VPN PPTP*, *ZRTP*, dan tanpa keamanan dalam layanan komunikasi *VoIP*?

### **1.3. Batasan Masalah**

Agar pembahasan masalah pada skripsi ini tidak menyimpang dari apa yang telah ditentukan serta untuk menyederhanakan masalah yang diulas maka diperlukan batasan-batasan masalah. Adapun batasan-batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Sistem keamanan *VoIP* yang diimplementasikan dalam penelitian ini ialah *VPN PPTP*, *ZRTP* dan tanpa keamanan.
2. Tidak membandingkan keunggulan masing-masing keamanan pada analisis komunikasi *VoIP*.
3. Penelitian dilakukan untuk menemukan perbedaan keamanan pada sistem komunikasi *VoIP* yang akan dibangun, tidak membahas secara mendalam mengenai algoritma enkripsi pada metode pengamanan yang akan diterapkan.

### **1.4. Tujuan Penelitian**

Tujuan penelitian ini adalah:

1. Mengetahui cara membuat *VoIP* untuk keperluan komunikasi dengan

menggunakan *VPN PPTP* dan *ZRTP* sebagai metode keamanan.

2. Mengetahui pengaruh penerapan keamanan *VPN PPTP* dan *ZRTP* terhadap suara yang dihasilkan pada *VoIP*.
3. Mengetahui hasil pengujian komunikasi *VoIP* dengan menggunakan metode keamanan *VPN PPTP* dan *ZRTP* apabila dilakukan penyerangan pada saat komunikasi *VoIP* berlangsung.

### **1.5. Manfaat Penelitian**

1. Mengetahui perbandingan keamanan dari implementasi dari metode keamanan pada sistem komunikasi *VoIP*.
2. Mengetahui cara kerja komunikasi *VoIP* dengan menggunakan metode *VPN PPTP*, *ZRTP* dan *VoIP* tanpa keamanan.

### **1.6. Sistematika Penulisan**

## **BAB 1 PENDAHULUAN**

Pendahuluan berisikan tentang latar belakang, rumusan masalah, batasan masalah, manfaat penelitian, tujuan penelitian, keaslian penelitian, dan sistematika penulisan.

## **BAB II TINJAUAN PUSTAKA**

Tinjauan pustaka berisi tentang hasil penelitian sebelumnya yang digunakan sebagai landasan teori. Selain itu juga memuat konsep-konsep dan teori-teori yang mendukung seperti *VoIP (Voice Over Internet Protocol)*, *VPN*

(*Virtual Private Network*), *PPTP (Point to Point Tunneling Protocol)*, dan metode pengukuran kualitas layanan *VoIP*.

### **BAB III METODE PENELITIAN**

Metode dan perancangan sistem memuat uraian tentang bahan dan peralatan penelitian, pengumpulan data, analisis dan rancangan penelitian, rencana implementasi dan pengujian, teknik pengolahan data dan analisis hasil yang akan digunakan.

### **BAB IV HASIL PENELITIAN DAN PEMBAHASAN**

Hasil penelitian dan pembahasan digunakan untuk mengetahui bagaimana objek penelitian tersebut dibangun, meliputi perancangan serta hasil yang diperoleh ketika dilakukan pengujian terhadap sistem yang dibangun.

### **BAB V KESIMPULAN**

Penutup berisi mengenai kesimpulan terhadap penelitian yang telah dilakukan dan saran peneliti yang dapat dilakukan dikemudian hari.

### **DAFTAR PUSTAKA**

### **LAMPIRAN**