ABSTRAKSI

Kelas on-line adalah metode *e-learning* yang menggunakan teknologi VoIP sebagai layanan dasarnya. Kelas on-line mendukung revolusi sistem perkuliahan yang lebih efektif dan efisien dari kuliah di kelas konvensional atau sebagai pendukung pelaksanaan kuliah di kelas konvensional, dimana proses kuliah dapat dilakukan tanpa harus bertatap muka secara langsung antara pengajar dosen dengan mahasiswa. Sehingga apabila dosen atau mahasiswa berhalangan untuk hadir di kelas konvensional masih tetap dapat mengajar dan mahasiswa bisa mendapat materi kuliah dari tempat ia berada. VoIP memang memberikan layanan yang lebih fleksibel, dengan biaya yang lebih murah daripada PSTN, akan tetapi VoIP lebih riskan terhadap serangan hacker dan virus.

Untuk mendukung implementasi kelas *on-line,* perlu dilakukan pengamanan dengan meminimalkan *trade-off* sekuriti QoS yang terjadi. Salah satu cara adalah dengan menggunakan IPsec VPN (Virtual Private Network) dengan algoritma enkripsi Blowfish. Blowfish sendiri telah diketahui sebagai salah satu metoda algoritma enkripsi yang cukup kuat dan cepat dalam proses enkripsi-dekripsi, sehingga algoritma ini lebih handal dipandang dari segi *delay, packet loss,* dan *jitter* daripada 3DES dan AES. Selain itu sampai sekarang belum ada metode *cryptanalysis* yang efektif bekerja pada algoritma Blowfish.

Pada emulasi yang telah dilakukan, pada sisi keamanan, MITM tidak dapat mengakses server bahkan melakukan ping sekalipun. Serangan DoS yang dilancarkan MITM ke PC admin pun tidak berhasil setelah menggunakan sistem VPN. Selain itu paket IP yang tertangkap wireshark pada PC MITM mempunyai payload yang sudah terenkripsi sehingga sulit untuk melakukan analisis lebih lanjut dan hal ini mencegah seseorang untuk melakukan *eavesdropping / tapping.* Untuk sisi performansi, terjadi penurunan QoS pada sisi *throughput, delay, jitter,* dan *packet loss*. Pada skenario VoIP yang menggunakan codec G711 μ-law didapatkan penurunan performansi rata-rata total sekitar 23% - 34% dan 37% - 69% pada skenario Video Streaming menggunakan codec MPEG-4. Pada saat dilakukan perbandingan, Blowfish mempunyai performansi lebih unggul 3% - 12% dari AES dan 3DES.

Kata kunci : IPsec, VPN, Blowfish