ABSTRAK

Komunikasi *one-way* berupa video saat ini semakin mudah digunakan. Salah satu layanan yang mempermudah akses komunikasi tersebut adalah *Internet Protocol Tele Vision* (IPTV). Dengan kemudahan layanan berbasis *packet switch* yang sudah masuk di seluruh wilayah di dunia semakin mempermudah akses dari layanan IPTV. Regulasi dari IPTV, yang membutuhkan performansi tinggi, membuat layanan ini diminati oleh masyarakat luas. Namun, mudahnya akses dari layanan tersebut membuat tingkat keamanan yang digunakan perlu dianalisis lebih lanjut.

Salah satu penggunaan keamanan jaringan adalah penggunaan *Secure Socket Layer* (SSL). Protokol ini mampu mengenkripsi data yang akan dikirimkan menuju *client* atau pengguna, dengan metode *SSL Handshake*, dimana metode ini memberikan sistem yang hampir sama dengan *connection-oriented*. Penggunaan SSL ini lebih tertuju pada penggabungan antara SSL dengan *HyperText Transfer Protocol* (HTTP), dimana komunikasi ini terjadi saat pengguna layanan IPTV melakukan sesi *login* saat akan memasuki *website* yang disediakan oleh *server*. Dengan sistem ini, maka penggunaan protokol *Real-Time Transport Protocol* (RTP) pada layer *Application* tidak membebani performansi dari pengiriman data antara *server* dengan *client*. Sebagai pengujian keamanan dari layanan IPTV, penelitian ini menggunakan 5 serangan secara bertahap, yaitu *Distributed Denial-of-Service* (DDoS), *IP Spoofing*, *Man-in-the-Middle Attack: Video Hijacking, Heartbleed Bug,* serta satu kombinasi dari *IP Spoofing-Distributed Denial-of-Service* (DDoS)-*Man-in-the-Middle Attack: Video Hijacking,* dengan *hacker* atau *pentest* bukan berasal dari penguji sendiri.

Dalam tugas akhir ini, analisis penelitian diambil dari 3 skenario: menggunakan program VLC, menggunakan *web page-interface*, serta menggunakan *web-page-interface* setelah diserang oleh *pentest* atau *hacker*, dengan *routing protocol* berupa *Open-Shortest Path First* (OSPF) dan menggunakan *Protocol Independent Multicast* (PIM) sebagai pengelompokan alamat IP video. Dari hasil ini didapatkan rata – rata nilai sebelum serangan terjadi (hanya menggunakan VLC) adalah 3.40734 Mbit/s, 4.31384 Mbit/s, dan 1.31656 Mbit/s untuk *throughput*, 0.974 ms, 0.938 ms, dan 0.899 ms untuk *end-to-end delay*, 0.0085 µs, 0.0093 µs, 0.0110 µs untuk *mean jitter*, serta 0% *packet loss* untuk video 1 dan 3, dan 0.93% untuk video 2, dan nilai rata – rata sebelum serangan terjadi (menggunakan *web page* dan *HTTPS*) adalah 3.62284 Mbit/s, 6.04867 Mbit/s, dan 1.33368 Mbit/s untuk *throughput*, 0.971 ms, 0.926 ms, dan 1.008 ms untuk *end-to-end delay*, 0.1188 µs, 0.0271 µs, 0.0048 µs untuk *mean jitter*, serta 0% *packet loss* untuk semua video. Sedangkan nilai rata – rata setelah serangan berbeda – beda, tergantung dari jenis serangan yang dilancarkan.

Kata kunci: IPTV, *Secure Socket Layer*, Performansi Serangan