ABSTRACT

On-line class is an e-learning method that uses VoIP and Video Streaming technology as the basic service. On-line class support lecturing system that more effective and efficient than conventional lecturing because the lecturing process allow lecturer and the students to attend the class without directly face to face. So, if lecturers have obstacle for attending the conventional class, the lecturer may access the class On-line class server to give the students some lecture materials in the place where he or she stand. VoIP gives more flexible services with lower cost compared with PSTN, however VoIP has more risk on virus and hacker attack.

Because of that, there must be a one way out to secure VoIP packet data with minimized trade-off between security and QoS. Using IPsec VPN (Virtual Private Network) with Blowfish encryption algorithm is one of many choices to secure VoIP packet data. Blowfish itself is known as strong and fast encryption algorithm on encryption-decryption process, so this algorithm is better than 3DES and AES on delay, packet loss, and jitter. In the other hand, there are no documented cryptanalysis methods that effectively working in this algorithm.

From the emulation that has been done before, on the security side, MITM can't gain access to the servers or even pinging because there is no access right planted on its PC. DoS attack that unleashed by MITM to admin's PC isn't work after VPN system enabled. In the other side, the captured IP packets on MITM's wireshark have their payload encrypted and difficult to do some further analysis with its payload and it is also avoid someone to do some eavesdropping / tapping activity. On performance side, the QoS (delay, jitter, packet loss, and throughput) is decreased approximately 23% - 34% on VoIP with G711 μ-law codec and 37% - 69% on Video Streaming with MPEG-4 codec. When compared, Blowfish is more efficient 3% - 12% than AES and 3DES.

Keyword: IPsec, VPN, Blowfish