Implementasi Keamanan Mqtt dengan Protocol Augpake untuk Mencegah Serangan Man In The Middle

Prabowo Nofieldi[1], Vera Suryani[2]

School of Computing, Telkom University, Bandung

[1]prabowonofieldi@student.telkomuniversity.ac.id, [2]verasuryani@telkomuniversity.ac.id

Abstraksi

Implementasi MQTT telah banyak digunakan di area IoT (Internet of Things) sebagai protokol transport pengiriman pesan, dimana proses MQTT mencakup protokol yang ringan dengan kompleksitas rendah, daya rendah, dan pencetakan kaki rendah dalam penerapannya. Dengan standar OASIS MQTT, keamanan yang diberikan sudah mampu menjaga keamanannya seperti SLL/TSL yang membutuhkan validasi keamanannya. Dengan keamanan yang diberikan dapat memberikan kerentanan dan serangan MITM (Man in The Middle) pada protokol MQTT. Pada makalah ini penulis memfokuskan pada keamanan protokol MQTT dengan mengimplementasikan metode AugPAKE yang pada penelitian sebelumnya telah dilakukan pada area mesin virtual ubuntu 64bit dan raspberry Pi 2 model B dan penulis ingin membuktikan keamanan pada area OS yang berbeda yaitu OS Windows dan OS Kali Linux. serta menggunakan broker terbaru yaitu Mosquitto v.2.1. Pada tulisan ini penulis akan fokus menjaga keamanan Protokol MQTT dengan mengimplementasikan metode AugPAKE pada Mosquitto v.2.1 sebagai broker di area OS Windows dan OS Kali Linux. Dengan menggunakan metode AugPAKE, setiap proses dalam protokol MQTT tidak memerlukan validasi untuk keamanannya dan tetap menjaga keamanan data yang dikirim.

Kata kunci: AugPAKE, MQTT, Man in The Middle, Internet of Things