A NOVEL ENCRYPTION METHODOLOGY TO ENHANCE SECURITY IN STOMP PROTOCOL

M. R. Bilal Ahamed

A dissertation submitted in partial fulfilment of the requirements for Bachelor of Engineering (Honours) degree in Software Engineering

Department of Computing

Informatics Institute of Technology, Sri Lanka

in collaboration with

University of Westminster, UK

2020

Abstract

As the era of Internet expanded the importance of connectivity arised. As a result, new inventions using Internet came into play, thereby technology becomes very fast and reachable day by day. All new devices which are invented are connected together over the network. Each and every device have multiple sensors, cameras and power consumptions which are built-in to do a specific or multiple task. This is when all devices turned into Internet of Things (IoT) which mostly rely on Internet in different modes. Now these devices are open over the Internet, thereby it can be accessed by anyone who can destroy the architecture layers and see through the data. As the main data transferring medium, message passing protocols are required. From this research it is provable that STOMP protocol has no security methodology made for its payload, thereby as a solution to this problem is by having an encrypted payload generated while transmitting over the network. This encryption will have the HMAC methodology to do the encryption process. As the final test result, it's guarantees that the payload sent on the wire cannot be brute forced and read.

Subject Descriptors:

Networking

Protocol Security

Client Server Architecture

Key Words:

Network Messaging Protocol, Message Encryption, Client Server, Socket