**JARAMOGI OGINGA ODINGA UNIVERSITY**

**OF SCIENCE AND TECHNOLOGY**

**SCHOOL OF INFORMATICS AND INNOVATIVE SYSTEMS**

**PROJECT TITLE:**

SSL/TLS CERTIFICATE TRACKING IN REVEALING FORGED CERTIFICATES

 **PRESENTED BY:**

NGARI EUSTUS MUTUGI

ADMISSION No: I 132/0877/2013

**AN APPLICATION PROJECT REPORT SUBMITTED IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR OF** **SCIENCE IN COMPUTER SECURITY AND FORENSICS**

**©2016**

**SUPERVISORS**

MR. ABUONJI PAUL

**Abstract.**

SSL/TLS (Secure Sockets Layer/Transport Layer Security) Certificate Tracking in Revealing Forged Certificates is based on implementing two chrome based security solutions meant set to uncover and evade the threats that results from unencrypted connections or by use of a forged SSL/TLS certificates. To ensure that the client browser connects via encrypted HTTPS (Secure HyperText Transfer Protocol) connections we have come up with a way to ensure that all user requests shall be redirected to HTTPS. Also, through monitoring of SSL/TLS certificate we will be able to verify the integrity of the certificate. Moreover, there are trackers to website that handles user data or have the ability to gather client related data. These trackers if they set to connect over HTTP unencrypted connection they may compromise the security of the of the client regardless the ability of the client to connect over secure HTTPS connections. Therefore, there was a need to connect the trackers mandatory over HTTP + SSL (HTTPS) encrypted connection.

The development of the security solution was made possible by the utilization of agile methodology and in our case Scrum Methodology proved to be useful. The software development took 35 days despite the change requests made. This was made possible by the adoption of Scrum in the software development process.

Strict SSL and Cert Monitor chrome browser extensions and application respectively, provides the user with added security features in your browsing experience and greatly improves your privacy online. This is also made as transparent and automatic as possible. Development was majorly done on the chrome browser as it the leading in usage statistics to date (Dec 2016). The chrome app and extensions should be deployed to any web user to help fight against man-in-the-middle attacks that are faced daily by every internet user and many a times without his/her consent. The information provided by my chrome extensions can allow the user to easily validate the security of his/her browsing experience. My chrome app and extension have the advantage of being lightweight, informative, and simple to install.