ABSTRACT

Instant messaging has grown to become a very important means of communication among organization staff and among individuals outside an organization. The problem with this form of communication is that some of the instant messaging applications send the messages in plain text, meaning that intruders can easily intercept the packets and read their content. To address these shortcomings, end to end encryption has been developed. Unfortunately, this protocol only protects data on transit and does not secure data at the endpoint device interface. The purpose of this research thesis was therefore to develop a port –based algorithm for securing the instant messages at the device interface. The required data for this research included plain text and enciphered messages exchanged between the client and the server. Therefore, an experimental research design involving a prototyping approach was employed. The port-based algorithm borrowing from the port –based authentication was designed to operate at the application layer. To achieve this, an Jcreator integrated development environment was selected and it was in this environment where the proposed algorithm was coded. The concept of port based authentication was employed so that the port-hopping attacks against the developed algorithm were minimized by effectively securing the chosen communication ports. Due to the heavy usage of virtualization in data centers, the proposed algorithm was run in a client-server virtualized environment. The output of this analysis was presented in figures for easier interpretation. The research findings showed that some instant messaging applications such as telegram offered no protection at all. However, WhatAapp and Facebook messenger employed end to end encryption which lacked endpoint security. The results further indicated that the Java API contained a list of classes for networking, I/O, programming and GUI that facilitated a development of secure instant messaging applications. Therefore these APIs were used in-conjunction with port numbers and IP addresses to develop an algorithm that encapsulated data at the endpoint devices. The evaluation of these algorithms confirmed that valid split knowledge was required before the endpoint data could be deciphered. This research work contributed to the security of instant messaging by enforcing endpoint security that is missing the current end to end protocol. It is therefore recommended that this algorithm be incorporated as extension of end to end security.