A platform to develop a secure instant messaging using jabber protocol

Problem statement: Open Source technologies are interesting in that they allow free experimentation and integration by anyone and anywhere. A Jabber user can control presence with very little effort. Another user, regardless of external platform, must subscribe to your presence. You have the choice of rejecting or accepting the subscription at the time it is submitted. Approach: Other applications of this system were yet to be discovered. Jabber is a work in progress; the community learns and creates applications of the protocol/platform on an almost daily basis. This study aimed to implement a security algorithm for developed instant messaging. Results: The objective was to make sure that flow of data from client application or computer is not tapped by a hacker and also to make it difficult for a network data sniffer to explore the situation. In this study there were many aspects must be understood such as: Jabber protocol, programming language and security aspect. For this reason it was proposed to develop a new secure connection and makes sure that the connection between clients and server is safe and secure when the instant massage had been transferred using jabber protocol. Conclusion/Recommendations: To develop a new secure connection for instance message using jabber protocol or other names, the Extensible messaging and presence protocol had been used. To make it secure the open secure socket layer will be used for general-purpose encryption. In this study the methodology used to solve security threats like: The ability to control access to IM applications, audit and archive IM conversation, the ability to lockout unauthorized IM and peer-to-peer file sharing connections and Encryption.