Security evaluation for Instant Messaging encryption algorithms

Peter S. Nyakomitta, Dr. Silvance O. Abeka, Dr. Solomon O. Ogara

Abstract

Instant messaging applications such as Whats App, Facebook Messenger, Telegram and Skype provide a convenient means of passing information among company employees. Fueled by the bring your own device (BYOD) trend, organizations are allowing employees to access crucial information. The security flaws in such tools can create fear among the users leading to their slow uptake due to the leakage of organization sensitive information and attacks such as BEARST and POODLE. The rationale of this study provides a security evaluation of the current state-of- art on instant messaging encryption algorithm. The study deployed a survey approach as the master plan to throw light on the algorithms and their cons such as; Text secure, can encrypt chat messages but can also allow users to exchange unencrypted SMS and MMS messages with people who did not have Text Secure; Double ratchet algorithm, combines public key infrastructure in its operation, hence bringing in the challenges of key management; Off-the- record messaging, an extra symmetric key is derived during authenticated key exchanges that can be used for secure communication, hence also suffers from the key management constraints of public key infrastructure; Perfect forward secrecy intended to prevent the compromise of a long-term secret key from affecting the confidentiality of past conversations. However, forward secrecy cannot defend against a successful cryptanalysis of the underlying ciphers being used, since a cryptanalysis consists of finding a way to decrypt an encrypted message without the key, and forward secrecy only protects keys, not the ciphers themselves and Transport Layer Security / Secure Socket Layer algorithms however, have been shown to be easily compromised, for example exploiting initialization Vector chaining in Cipher Block Chaining weakness using a known plaintext attack and algorithm flaws in SSL v3. These security weakness in the current instant messaging encryption algorithms necessitates the development of port-based algorithm For protecting the information both in transit and at the endpoint. In this work, a security evaluation of these encryption algorithms given.

Keywords: Instant Messaging Applications, Algorithms, Attacks