Encrypted SMS App: Reliable Data Security (RDS)

Lt Col Rahul Dutt Sharma

Abstract: *Reliable Data Security (RDS) is an android mobile app that encrypts the SMS using AES-256 bit Encryption technique thereby making optimum utilization of existing civil mobile infrastructure as per the military/government department's requirement. It is a server-independent mobile app with no third party software/tool. In addition to transmitting encrypted SMS, RDS is integrated with in-built GPS to transfer own geo-location in encrypted format.*

Keywords: Encryption, mobile security, Encrypted SMS, AES-256, OTP based authorization, Own geo-location, Files locker

1. Introduction

Most of the places nowadaysare covered by cell phone providers thus, its data facility like SMS/ text chat has proved to be fastest method of data transmission. But, these SMS are transmitted in plain text and are prone to easy interception by legal/ illegal agencies. Similarly, chat apps like whatsapp, wechat, viberetc have their servers installed abroad with a massive network of engineers & technicians involved which makes the chat susceptible to interception.

2. Requirement

Defence/Government organizations have dynamic & urgent data requirement from remote locations. With growing dependence on mobiles, even government personnel have also started using SMS service being fastest method of data transmission. It is prudent to use existing civil mobile network provided it is encrypted and has high level of security embedded. This requirement laid the foundation of project 'Reliable Data Security' to develop a mobile app for securing SMS during and after its transmission over mobile networks and to password protect data in the mobile phones. Use of SMS facility becomes more pertinent with free SMS packs available these days.

3. Equipments Affected

Android mobile handsets on civil or private mobile network.

4. Brief Description

Reliable Data Security (RDS) is anandroid mobile application for securing SMS over cellular networks and password protect data in mobile phones. It uses AES-256 bit encryption for encrypting/decrypting SMS during and after its transmission.Various additional features like files/folder locking, integration with in-built GPS and own location plotting on Google maps make it a complete package for use by personnel operating in highly secure environment with confidential data.

5. SalientFeatures

RDS mobile app as a package comprises of following features:

a) Only authorized users are allowed to install the app. Authentication based on OTP derived from IMEI of authorized users only.
b) AES-256 bit Encryption/Decryption in text messages using sender defined passphrase (Symmetric Key).
c) Folders/Files Locker to hide data in handset.
d) Integration with in-built GPS to display and SMS own location(LAT/LONG).
e) Integration with Google maps to show own location on maps.
f) Provide protection from decompilation.

6. Details of Utilisation

RDS app has been implemented successfully on almost all android based handsets and on various android versions ranging from Android 2.2 to 10.**This app lays foundation for development of other apps** to transmit time critical and confidential information in encrypted and secure way. The basic encryption feature of the app may form the core of any other mobile app that requires authenticated users to transmit encrypted messages.

7. Sources of Innovation

Indigenous programming of more than 20,000 lines of code in Javalanguage has been carried out to develop the app. It entails intensive research work from internet on latest encryption techniques and its implementation.