Security Analysis of Telegram

6.857 Final Project

Hayk Saribekyan (hayks@mit.edu)
Akaki Margvelashvili (margvela@mit.edu)

May 17, 2017

Abstract

Telegram is a text messaging platform, with a secure messaging protocol called MTProto. The company was founded in 2013 and has more than 100 million active users. Telegram was created to allow users to have surveillance-proof communication. It claims to have the best security and privacy guarantees in the market. In this report we overview Telegram, discuss its protocol and compare it to similar products. We also exploit a leak on user availability and use it to predict when users are talking to each other.