Telegram, secure messaging

Francisco Luque Sánchez - María de Mar Ruiz Martín

Universidad de Granada

fluque1995@correo.ugr.es - mariadel52@correo.ugr.es

October 30, 2015

Presentation index

Introduction

Telegram is a safe instant messaging application. Features:

- Secure
- Encrypted
- Own transport protocol (MTProto)
- Multiplatform
- Cloud-based
- Open source
- Powerful APIs (provided by Telegram team)
- Free "forever"

Telegram security

Telegram uses different features for secure messaging and message encryption

- MTProto message encryption
- Private chatting
  - End-to-end encrypted messages
  - Self-destruction for messages

MTProto protocol

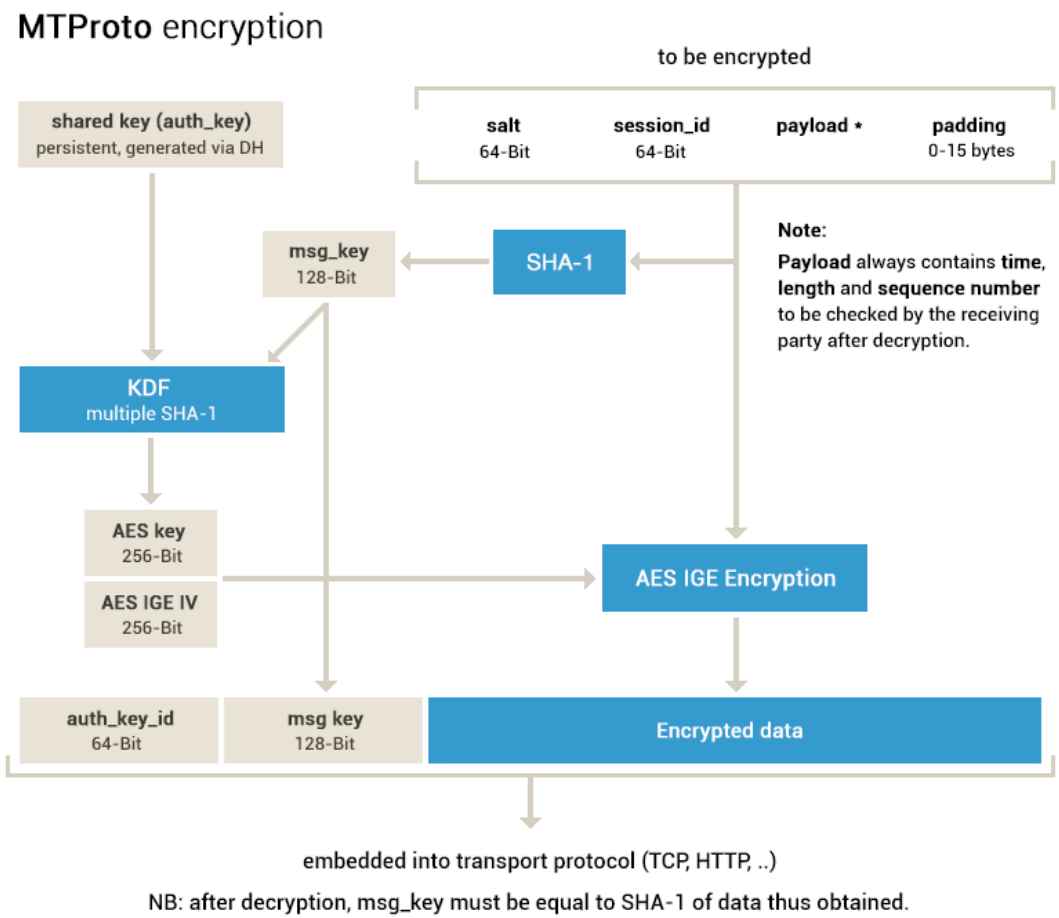
Transport and encryption protocol created by Telegram team (invented by Nikolai Durov, PhD Saint Pertersbourg Univ.). It allows multi-platform usage and file sending in every format. Based on:

- 256-bits symmetric AES encryption
- RSA 2048 encryption
- Diffie-Hellman key exchange

MTProto detailed description

Telegram haking contest: They will pay 300000 $ to the Telegram Encryption cracker

MTProto encryption schema



End-to-end encrypted messages - secret chats

Completely secure chats

Messages encrypted end-to-end (Encrypted by sender and decrypted by receiver)

No one is allowed to see the content of those messages, including Telegram team

They are not stored in Telegram cloud (you will only have access from the device of origin or destiny)

News: Iran blocked Telegram App after spy request

Self destruction for messages

Secret chat feature

Messages and files are deleted after a period of time

They are deleted from sender and receiver

Not stored on their servers

Everything you delete is deleted forever. Except for cats.
We never delete your funny cat pictures, we love them too much.

Telegram developer team

Open Source and APIs

Almost the whole code is open source, except for some code from the server (Keep calm! They promise they will release it soon)

APIs for applications and Bots

Application API

Wonderful client application API

They give us everything we need to create our own Telegram client

Telegram API documentation

Code of official Apps is released on github

Android App code

Bots API

Community started creating bots not supported by Telegram

Due to fast success of some of them, they decided to create an official Bots API

Now, Bots are really powerful tools

ETSIIT Bot source code

Q: What can I do with bots?

Telegram: Do virtually anything. Except for dishes — bots are terrible at doing the dishes.

The End.

github repository: https://github.com/pacron/telegram_beamer