МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе

БЕЗОПАСНОСТЬ ДАННЫХ В ПРИЛОЖЕНИЯХ-МЕССЕНДЖЕРАХ

Корнеенко Диана Петровна

Научный
руководитель:
старший
преподаватель,
А. В. Кушнеров

2021

В дипломной работе 66 страниц, 8 рисунков, 8 источников, 1 приложение.

ШИФРОВАНИЕ, СЕКРЕТНЫЙ ЧАТ TELEGRAM, ПРОТОКОЛ MTPROTO, СКВОЗНОЕ ШИФРОВАНИЕ, ПРОТОКОЛ ДИФФИ-ХЕЛМАНА, AES, IGE, ФУНКЦИЯ KDF, КРИПТОАНАЛИЗ, КЛИЕНТ-СЕРВЕРНОЕ ПРИЛОЖЕНИЕ.

Объектом исследования данной работы является криптографический протокол MTProto для секретных чатов Telegram.

Целью дипломной работы является изучения, реализация и анализ протокола MTProto для секретных чатов Telegram.

Для достижения этой цели использовались следующие методы и инструменты: изучение официальной документации Telegram, редактор кода Microsoft Visual Studio, язык программирования C#, технология платформы .NET для создания графического интерфейса Window Forms.

В дипломной работе были получены следующие результаты:

1) Описана работа протокола MTProto, включающая в себя протокол Диффи-Хелмана для получения общего секретного ключа и обмен сообщениями с использованием сквозного шифрования.

2) Реализовано учебное клиент-серверное приложение, моделирующее работу протокола MTProto для секретных чатов Telegram с графическим интерфейсом на Window Forms.

3) Проанализированы основные атаки на протокол MTProto v1.0, а также выявлены пути их предотвращения. Проанализирован протокол MTProto v2.0, а также подробнее рассмотрена уязвимость данной версии протокола к атаке MitM.

Дипломная работа практическая. Ее результаты можно использовать для понимания работы протокола MTProto для секретных чатов Telegram, а также дальнейшего анализа криптостойкости данного протокола.

Дипломная работа выполнена, поставленные задачи решены в полном объеме, есть возможность для дальнейшего развития исследований.

Дипломная работа выполнена самим автором.

Thesis project is presented in the form of an explanatory note of 66 pages, 8 figures, 8 references, 1 application.

ENCRYPTION, TELEGRAM, MTPROTO PROTOCOL, END-TO-END ENCRYPTION, DIFFE-HELMAN PROTOCOL, AES, IGE, KDF FUNCTION, CRYPTOANALYSIS, CLIENT-SERVER APPLICATION

The research object of this thesis project is the MTProto cryptographic protocol for secret Telegram chats.

The purpose of this work is to study, implement and analyze the MTProto protocol for secret Telegram chats.

The following methods and tools were used to achieve the goal: study of the official Telegram documentation, Microsoft Visual Studio code editor, C # programming language, .NET platform technology for creating a Window Forms graphical interface.

The main results of the thesis project are as follows:

1) The operation of the MTProto protocol was described, which includes the Diffie-Hellman protocol for obtaining a shared secret key and exchanging messages using end-to-end encryption.

2) A training client-server application that simulates the operation of the MTProto protocol for secret Telegram chats with a graphical interface on Window Forms was built.

3) Analyzed the main attacks on the MTProto v1.0 protocol, and identified ways to prevent them. The MTProto v2.0 protocol has been analyzed, and the vulnerability of this version of the protocol to the MitM attack is considered in more detail.

This thesis project is a practical one. Its results can be used to understand how the MTProto protocol works for secret Telegram chats, as well as further analysis of the cryptographic strength of this protocol.

The thesis project is complete, all tasks have been successfully done, there is a possibility for further research and development.

The thesis project was done by the author himself.