БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Кафедра телекоммуникаций и информационных технологий

Аннотация к дипломной работе

ПЕРЕДАЧА КРИПТОГРАФИЧЕСКИ ЗАЩИЩЕННЫХ СООБЩЕНИЙ МЕЖДУ УСТРОЙСТВАМИ НА БАЗЕ ОС ANDROID

Тарликовский Дмитрий Андреевич

Научный руководитель – старший преподаватель Попко Е.Е.

2020

РЕФЕРАТ

Дипломная работа 40 страниц, 23 рисунка (схемы, диаграммы), 1 таблица, 24 источника.

SMS-СООБЩЕНИЯ; ANDROID; ШИФРОВАНИЕ; УЯЗВИМОСТЬ;

Объекты исследования – шифрованная передача и хранение SMS-сообщений.

Цель работы – провести анализ существующих уязвимостей. На основании анализа разработать приложение для операционной системы Android, позволяющего отправлять и хранить зашифрованные сообщения.

В данной дипломной работе рассмотрены проблемы протокола SS7, изучен масштаб проблемы нарушения конфиденциальности в актульном до сегодняшнего дня сервисе, а также приведен пример применяющейся до сих пор атаки.

Была сделана попытка реализовать шифрование SMS–сообщений по упрощенной схеме, аналогичной той, что используется в мессенджерах. Как результат, было получено приложение шифрующее отправляемые и хранимые сообщения. Данное приложение требует дальнейшей доработки и расширения функционала, однако на данном этапе оно уже выполняет поставленную перед ним задачу.

РЭФЕРАТ

Дыпломная работа 40 старонак, 23 малюнка (схемы, дыяграмы), 1 табліца, 24 крыніцы.

SMS-ПАВЕДАМЛЕННІ; ANDROID; ШЫФРАВАННЕ; СЛАБЫЯ МЕСЦЫ

Аб'ект даследавання – шыфраваная перадача і захоўванне SMS-паведамленняў.

Мэта работы - правесці аналіз існуючых уразлівасцяў. На падставе аналізу распрацаваць прыкладанне для аперацыйнай сістэмы Android, якое дазваляе адпраўляць і захоўваць зашыфраваныя паведамленні.

У дадзенай дыпломнай працы разгледжаны праблемы пратаколу SS7, вывучаны маштаб праблемы парушэння прыватнасці ў актульном да сённяшняга дня сэрвісе, а таксама прыведзены прыклад ужыўной дагэтуль атакі.

Была зроблена спроба рэалізаваць шыфраванне SMS-паведамленняў па спрошчанай схеме, аналагічнай той, што выкарыстоўваецца ў паведамляльніке. Як вынік, было атрымана прыкладанне якое шыфруе паведамленні, якія адпраўляюцца і захоўваюцца. Дадзенае прыкладанне патрабуе далейшай дапрацоўкі і пашырэння функцыяналу, але на даным этапе яно ўжо выконвае пастаўленую перад ім задачу.

ABSTRACT

The degree work 40 pages, 23 figures (diagrams, diagrams), 1 table, 24 sources.

SMS; ANDROID; ENCRYPTION; VULNERABILITY

The objects of the work are encrypted transmission and storage of SMS messages.

The purpose of the research is to analyse existing. Based on the analysis, develop an application for the Android operating system that allows you to send and store encrypted messages.

In this thesis the problems of SS7 protocol are considered, the scale of the problem of confidentiality violation in the actual service up to now is studied, and also an example of the attack which is used up to now is given.

An attempt was made to implement encryption of SMS messages using a simplified scheme similar to that used in messengers. As a result, an application encrypting sent and stored messages was received. This application requires further development and expansion of functionality, but at this stage it is already fulfilling its task.