БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ ПРИКЛАДНОЙ МАТЕМАТИКИ И ИНФОРМАТИКИ
Кафедра технологий программирования

Аннотация к дипломной работе

Методы, инструменты реверс-инжиниринга и принципы защиты Android-приложения

Попова Анна Юрьевна

Научный руководитель – доцент, кандидат физико-математических наук Горячкин В.В.

Минск, 2022

РЕФЕРАТ

Дипломная работа, 51 с., 43 рис., 1 таблица, 2 приложения.

Ключевые слова: Вредоносные приложения, структура мобильного приложения, внедрение кода в приложение, обратная разработка, безопасность мобильного приложения

Объект исследования – методы, инструменты обратной разработки и обнаружение вредоносной вставки.

Цели работы – анализ строения мобильного приложения, описание способов вставки кода в приложение, исследование методов обнаружения вредоносной вставки в приложение.

Методы исследования – теоретические: изучение литературы, посвященной обратной разработке Android-приложения, а также изучение документации выбранного инструментария. Практические: применение изученных подходов для осуществления обратной разработки.

Область применения – разработка и безопасность мобильных приложений.

РЭФЕРАТ

Дыпломная праца, 50 с., 43 мал., 1 табліца, 2 дадаткі.

Ключавыя словы: Шкодныя мабільныя дадаткі, структура мабільнага дадатку, укараненне кода ў дадатак, зваротная распрацоўка, бяспека мабільнага дадатку

Аб'ект даследавання– метады, прылады зваротнай распрацоўкі і выяўленне шкоднай устаўкі.

Мэты працы – аналіз будынка мабільнага дадатку, апісанне спосабаў устаўкі кода ў дадатак, даследаванне метадаў выяўлення шкоднай устаўкі ў дадатак.

Метады даследвання– тэарэтычныя: вывучэнне літаратуры, прысвечанай зваротнай распрацоўцы Android-дадатку, а таксама вывучэнне дакументацыі абранага інструментара. Практычныя: ужыванне вывучаных падыходаў для ажыццяўлення зваротнай распрацоўкі.

Вобласць ужывання – распрацоўка і бяспека мабільных дадаткаў.

ABSTRACT

Graduate Work, 50 pages, 43 illustrations, 1 table, 2appendix.

Keywords: Malicious applications, mobile application structure, code injection into the application, reverse engineering, mobile application security

The object of research is methods, reverse engineering tools, and malicious insertion detection.

The purpose is analysis of the structure of the mobile application, description of ways to insert code into the application, research of methods for detecting malicious insertion into the application.

Methods of research are theoretical: study of the literature devoted to the reverse development of an Android application, as well as the study of the documentation of the selected toolkit. Practical: application of the studied approaches to reverse engineering.

Scope is development and security of mobile applications.