Ministerul Educaţiei al Republicii Moldova

Universitatea Tehnică a Moldovei

Facultatea Calculatoare, Informatică și Microelectronică

Departamentul Informatică şi Ingineria Sistemelor

Admis la susţinere

Şef departament:

conf. univ., dr. Viorica Sudacevschi

_____

„ _ ”_____2020

INSTRUMENT PENTRU PREVENIREA VULNERABILITĂŢILOR PENTRU SO ANDROID

Teză de master în

Managementul aplicațiilor informaționale

Masterand: Dmitrii VRABIE (_____)

Conducător: Mihail PEREBINOS (_____)

Chişinău – 2020

ADNOTARE

Vrabie Dmitrii

INSTRUMENT PENTRU PREVENIREA VULNERABILITĂȚILOR DIN OS ANDROID.

Teza de master, Chișinău, 2020

Structura lucrării: introducere, 3 capitole, concluzie, 25 de surse bibliografice, 86 de pagini, 23 de figuri, 1 tabel, 2 anexe.

Cuvinte cheie: Android, vulnerabilitate, securitate, aplicație

Domeniul de studiu: securitatea sistemului de operare Android

Scopul: cercetarea securității sistemului de operare Android și crearea unui instrument pentru prevenirea vulnerabilităților în sistemul de operare Android, crearea unei aplicații care confirmă operativitatea instrumentului.

Sarcinile avansate:

1) Studiul și analiza vulnerabilităților și amenințărilor aplicațiilor mobile, precum și a aspectelor specifice a etapei actuale de dezvoltare a sistemului de operare Android în ceea ce privește securitatea;
2) Studierea și analizarea vectorului atacurilor asupra aplicațiilor mobile, precum și urgența creării instrumentelor de prevenire a vulnerabilităților pentru sistemul de operare Android;
3) Proiectarea, dezvoltarea și testarea unui instrument de prevenire a vulnerabilităților în sistemul de operare Android.

Metodologie de cercetare: documentație științifică, analiză a literaturii de specialitate, comparație, sinteză, generalizare. Metodele statistice de prelucrare a datelor.

Noutatea și originalitatea științifică: în cursul studiului, a devenit evidentă necesitatea creării unui instrument universal care să conțină diverse verificări de securitate.

Semnificația teoretică a studiului constă în fundamentarea metodologică a respectării securității informațiilor și crearea unui instrument de prevenire a vulnerabilităților din sistemul de operare Android.

Valoarea aplicativă: crearea unui instrument de prevenire a vulnerabilităților în sistemul de operare Android care include mai multe soluții gata pregătite și care acceptă o extindere ușoară a funcționalității.

Implementarea rezultatelor științifice: aplicarea instrumentului creat într-o aplicație care confirmă operativitatea și eficiența produsului creat.

АННОТАЦИЯ

Врабие Дмитрий

ИНСТРУМЕНТ ДЛЯ ПРЕДОТВРАЩЕНИЯ УЯЗВИМОСТЕЙ В ОС ANDROID.

Магистратская работа, Кишинёв, 2020

Структура работы: введение, 3 главы, вывод, 25 библиографических источников, 86 страниц, 23 рисунка, 1 таблица, 2 приложения.

Ключевые слова: Android, уязвимость, безопасность, приложение

Область изучения: Безопасность операционной системы Android

Цель магистратской работы: Изучение безопасности операционной системы Android и создание инструмента по предотвращению уязвимостей в ОС Android, создание приложение подтверждающего работоспособность инструмента.

Выдвинутые задачи:

1) Изучение и анализ уязвимостей и угроз мобильных приложений, а также изучение и анализ особенностей современного этапа развития операционной системы Android с точки зрения безопасности;
2) Изучение и анализ вектора атак на мобильные приложения, а также астуальности создания инструмента предотвращения уязвимостей для ОС Android;
3) Проектирование, разработка и тестирование инструмента по предотвращению уязвимостей в ОС Android.

Методология исследования: научная документация, анализ специализированной литературы, сравнение, синтез, обобщение. Статистические методы обработки данных.

Уникальности и новизна работы: в процессе исследования выяснилась необходимость создания универсального инструмента, содержащего в себе различные проверки безопасности.

Теоретическое знание исследования состоит в методологическом обосновании соблюдения информационной безопасности и создании инструмента по предотвращению уязвимостей в ОС Android.

Ценность работы: создании инструмента по предотвращению уязвимостей в ОС Android включающего в себя несколько готовых решений и поддерживающего лёгкое расширение функционала.

Применение научных результатов: использование созданного инструмента в приложении, подтверждающего работоспособность.

ANNOTATION

Vrabie Dmitrii

TOOL FOR PREVENTING VULNERABILITIES IN ANDROID OS.

Master's thesis, Chisinau, 2020

Thesis structure: introduction, 3 chapters, conclusion, 25 bibliographic sources, 86 pages, 23 figures, 1 table, 2 appendices.

Keywords: Android, vulnerability, security, application

Area of study: Android Operating System Security

Aim of the thesis: Studying the security of the Android operating system and creating a tool for preventing vulnerabilities in the Android OS, creating an application confirming the operability of the tool.

Study objectives:

1) The study and analysis of vulnerabilities and threats of mobile applications, as well as the study and analysis of the features of the current stage of development of the Android operating system in terms of security;
2) Studying and analyzing the vector of attacks on mobile applications, as well as the urgency of creating vulnerability prevention tools for the Android OS;
3) Design, development and testing of a vulnerability prevention tool in the Android OS.

Methodology of research: scientific documentation, analysis of specialized literature, comparison, synthesis, generalization. Statistical methods for data processing.

Uniqueness and newness of the work: in the course of the study, it became clear the need to create a universal tool containing various security checks.

The theoretical meaning of the research consists in the methodological substantiation of compliance with information security and the creation of a tool to prevent vulnerabilities in the Android OS.

Value of work: creating a vulnerability prevention tool in the Android OS that includes several ready-made solutions and supports easy extendibility of functionality.

Application of scientific results: applying of the created tool in an application to confirming operability.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Невозможно себе представить современный мир, в котором бы не было электричества, интернета и гаджетов. Всё это уже давно стало неотъемлемой частью повседневной жизни человека. Было бы крайне глупо утверждать, что все эти блага цивилизации, несут вред. Сколько возможностей появилось у людей благодаря интернету трудно подсчитать. Теперь людям чтобы увидеть друг друга, нужно всего лишь сделать пару касаний экрана их телефона. Чтобы поесть, что-либо уже не надо выходить в магазин, выбирать продукты, а потом готовить еду, достаточно просто запустить приложение и в течение часа курьер будет у порога. Но у всего есть своя цена и за все «удобства» нужно платить.

В данной работе, исследуется тема уязвимостей операционной системы Android, а также инструментов по предотвращению угроз возникновения взлома приложений. Об актуальности темы, крайне красноречиво говорит статистика. С каждым годом количество успешных атак растёт, несмотря на все усилия, прилагаемые разработчиками ОС. В результате чего, компании несут огромные убытки, клиенты подают судебные иски в связи с раскрытием их данных.

Работая непосредственно в сфере программирования для ОС Android, была возможность наблюдать, использования существующий методов разработки. В ходе этого было замечено, что многие программисты пренебрегают методами предотвращения угроз или просто не осведомлены. Что немаловажно, многие компании намеренно «забывают» о безопасности собственного продукта в угоду скорейшего запуска продукта на рынке. В качестве подтверждения вышесказанного, приведу пример, в котором было запущено приложение для социального мониторинга в Москве, позволяющее следить, где находится пользователь во время пандемии COVID-19. В результате некомпетентности разработчиков или спешке, в которой разрабатывался данный продукт, было реализованы решения, способные в будущем привести к значительным репутационным потерям и судебным издержкам. Причина была в том, что приложение отслеживало информацию о пользователе и передавало её в незашифрованном виде [1].

В рамках данной работы, исследовались различные уязвимости, которые можно применить к приложениям на операционной системе Android, актуальность применения мер по предотвращению последствий, причины их новых атак хакеров и методы борьбы с ними, а также описание процесса создания инструмента, способного помочь разработчикам избегать новых уязвимостей.

Первая глава, состоит из 2-х частей. В первой части, производится анализ уязвимости и угрозы мобильных приложений, их современное состояние, а также изучены этапы развития

операционной системы Android. Во второй главе производится анализ современного состояния проблем уязвимостей и угроз мобильных компьютерных систем, а также проблемы безопасности Android-приложений, их классификация и анализ. Кроме того, был произведён анализ актуальности создания инструмента предотвращения уязвимостей и выдвинуты цель и задачи работы.

Вторая глава посвящена анализу методов и средств борьбы с мобильным уязвимостями и векторов атак на мобильные приложения, также рассматриваются средства защиты, предоставляемые ядром и возможностями операционной системы. Особое внимание уделено изучению основных практик и методов предотвращения угроз мобильных устройств со стороны разработчиков. В результате анализа имеющиеся решений, их преимуществ и недостатков, был определён функционал, который будет внедрён в собственное решение.

В третьей главе, производится проектирование собственной библиотеки по предотвращению угроз возникновения взлома приложений ОС Android, портирующего приложения их разработка и тестирование. Также по результатам анализа, был намечен план развития и расширения библиотеки в будущем.

БИБЛИОГРАФИЯ

1. АЛИЗАР А. Приложение для слежки за москвичами “Социальный мониторинг” убрали из Google Play. https://habr.com/ru/news/t/495088/
2. Operating System Market Share Worldwide. URL: http://gs.statcounter.com/os-market-share.
3. APPLE INC. About the security content. http://support.apple.com/kb/HT6147
4. OWASP FOUNDATION. Owasp Mobile top 10. https://owasp.blogspot.com/2014/11/owasp-mobile-top-10.html
5. SWINHOE D. The 14 biggest data breaches of the 21st century. https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html
6. KREBSONSECURITY. Adobe breach impacted at least 38 million users. https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/
7. FRUHLINGER J. Marriot data breach FAQ: how did it happen and what was the impact. https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html
8. BUG BOUNTY PROGRAM. https://www.mozilla.org/en-US/security/bug-bounty/
9. COIMBRA A., CABRAL. D. Android developer roadmap. https://github.com/mobile-roadmap/android-developer-roadmap
10. GUARDSQUARE. Proguard. https://www.guardsquare.com/en/products/proguard
11. Robert C. Martin. GETTING A SOLID START. objectmentor.com
12. GITHUB. https://github.com/
13. RISK BASED SECURITY. https://www.riskbasedsecurity.com/2019/11/12/number-of-records-exposed-up-112/
14. CVDETAILS. https://www.cvedetails.com/top-50-products.php?year=0
15. XDA-DEVELOPERS. Android version distribution statistics now will only be available in Android Studio. https://www.xda-developers.com/android-version-distribution-statistics-android-studio/
16. SUMOLOGIC. What is an attack Vector? https://www.sumologic.com/glossary/attack-vector/

17. GOOGLE INC. Platform architecture. https://developer.android.com/guide/platform
18. GOOGLE INC. System and kernel overview. https://source.android.com/security/overview/kernel-security
19. PREEMTIVE. Why use obfuscation? https://www.preemptive.com/obfuscation
20. JODE. Jode. http://jode.sourceforge.net/
21. JAVAGUARD. JavaGuard. https://sourceforge.net/projects/javaguard/
22. PREEMTIVE. Preemtive. https://www.preemptive.com
23. ALEXANDR-BOWN S., ROLLINGS M. RootBeer. https://github.com/scottyab/rootbeer
24. ANDROID EMULATOR - https://developer.android.com/studio/run/emulator/?gclid=Cj0KCQjwzN71BRCOARIsAF8pjfgms8f4PJeTF_gpG3-i6BIjGG2MXxhbD0I9LnLeF3kFroAFkCpfVIQaAvUfEALw_wcB&gclsrc=aw.ds
25. KOTLIN EXTENSION FUNCTIONS - https://stackoverflow.com/questions/28294509/accessing-kotlin-extension-functions-from-java