HANOI UNIVERSITY OF SCIENCE AND TECHNOLOGY

GRADUATION THESIS

Android Malware Scanner

ĐẶNG PHÚC HIẾU
hieu.dp194759@sis.hust.edu.vn

Major: Information Technology

Supervisor: Doctor Nguyễn Đức Toàn ______________

Signature

School: Information and Communications Technology

HANOI, 12/2024

ACKNOWLEDGMENTS

First and foremost, I would like to express my sincere gratitude to the Board of Directors and all the faculty members of Hanoi University of Science and Technology for providing me with the opportunity and support throughout my academic journey.

I am particularly indebted to my advisor, PhD. Nguyen Duc Toan, for their invaluable guidance, patience, and support during the process of completing this thesis. Their expertise and insightful suggestions greatly contributed to the success of my work.

I also wish to extend my heartfelt thanks to my classmates, who have always been by my side, sharing experiences and providing assistance during our studies and research. Your friendship and solidarity have been a great source of encouragement for me.

Finally, I am deeply grateful to my family, whose unwavering support and encouragement have been my constant motivation. Your sacrifices, love, and faith in me have helped me overcome numerous challenges and obstacles.

Though this thesis may have its limitations, I hope it will serve as an important milestone in my future career. I sincerely thank everyone who has supported and accompanied me throughout the past five years.

ABSTRACT

As Android continues to dominate the global mobile landscape, the rise of malicious applications poses significant threats to user privacy and security. This project introduces Androlyzer, an advanced Android malware analysis framework engineered to deliver in-depth security assessments for APK files.

Harnessing the power of cutting-edge technologies like Django and Bootstrap, Androlyzer integrates static and dynamic analysis to uncover vulnerabilities, detect malware, and evaluate the overall security posture of Android applications. The framework generates detailed, actionable reports, equipping developers and security professionals with the insights needed to mitigate risks effectively.

Designed with modern architecture, Androlyzer combines Django for a powerful backend with a sleek, lightweight frontend to ensure rapid deployment, high scalability, and seamless integration into diverse security workflows. Its API-driven automation capabilities make it an indispensable tool for CI/CD pipelines, streamlining security in secure development lifecycles.

This project seeks to redefine mobile application security by providing an open-source, robust solution to combat Android malware. Androlyzer empowers researchers and developers to enhance app resilience, safeguard user data, and strengthen the Android ecosystem against evolving threats.

Student

(Signature and full name)

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1. INTRODUCTION

1.1 Motivation

The Android operating system has become the most widely used platform in the mobile world, but this growth has also brought significant security challenges. Malicious applications continue to pose serious threats to user privacy and data security. As malware becomes more sophisticated, it is increasingly difficult to detect and mitigate these threats using traditional methods.

This problem is particularly important for developers and organizations that rely on Android applications, as security vulnerabilities can lead to data breaches, loss of user trust, and financial damages. However, existing tools often lack the detailed analysis and flexibility needed to address these challenges effectively.

To tackle this issue, this project introduces Androlyzer, a framework designed to analyze Android files. By performing both static and dynamic analysis, Androlyzer helps identify malware, detect vulnerabilities, and assess the overall security of applications. The system generates detailed reports to assist developers and security professionals in improving the safety of their applications.

The goal of this project is to provide a practical tool that contributes to enhancing Android application security while also supporting the broader effort to create a safer mobile ecosystem.

1.2 Objectives and scope of the graduation thesis

1.2.1 Overview of Current Solutions

In the Android ecosystem, malware analysis has become increasingly important due to the growing prevalence of malicious applications. Current approaches to malware analysis can be divided into static and dynamic methods, each with its own strengths and limitations.

- Static Analysis: This method involves examining the structure, code, and resources of an application without executing it. Static analysis is efficient and can uncover embedded malicious code, permissions, and configurations. However, it struggles to detect runtime behaviors or obfuscation techniques used by advanced malware.
- Dynamic Analysis: This approach observes the behavior of an application during execution in a controlled environment. It can detect malicious activities such as unauthorized data exfiltration or suspicious API calls. While effective, dynamic analysis is resource-intensive, time-consuming, and often requires