

Project Proposal Final - 2200897 Kai Probert

by Kai Probert

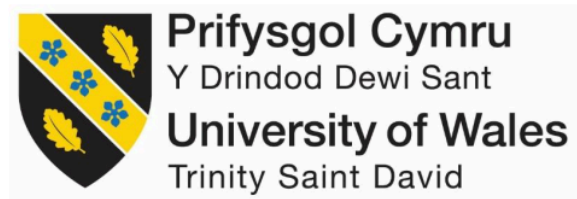
Submission date: 21-Oct-2024 12:54AM (UTC+0100)

Submission ID: 240729941

File name: 41764_Kai_Probert_Project_Proposal_Final_-_2200897_Kai_Probert_586419_1234840702.docx
(145.47K)

Word count: 1592

Character count: 8373



A Study of the analysis and investigation of Mobile Android Malware

by

Kai Probert 2200897

Supervisor: Nitheesh Kaliyamurthy

Project submitted as part of the requirements for the
award of

*BSc (Hons) Computing (Computer Networks and
Cybersecurity)*

April 2025

Introduction

Project Area

The mobile device market has grown exponentially since the late 2000s. It has revolutionized the digital world allowing people to access any information they require at the touch of a button, alongside revolutionising the world of communication. However, the exponential market explosion and modern-day reliance on mobile platforms has allowed threat actors to maliciously target the market. Especially on platforms like Android, known for its open-source nature. This has led to massive growth on mobile malware development.

I will be focusing on malware that targets android mobile devices, the aim of the project is in considering modern day mobile devices, their uses and what different malware does to target those features and its users. This project will contribute to the evolving field of cybersecurity by completing analysis on malware using static and dynamic methods of investigation. I will also discuss mitigation methods for user protection, what exists and what could be developed in future. For example, using machine learning and AI to analyse for example like creating a machine learning model to identify and classify malware much faster and more accurately than traditional methods^[1].

The specific problem to be investigated is investigating and analysing the specifics of android based malware, due to its open-sourced nature allowing more specialised attacks and finding ways that the malware attacks devices most commonly, allowing us to find more sophisticated methods of stopping these attacks from being possible and patching them. An obvious example of this is users lack of security awareness.

Objectives and aims of this project are investigating malware and identifying attack vectors most commonly exploited by malware. This knowledge will be used to propose better defence and security methods for those exploited vectors.

- **Specific:** Analyse different types of mobile malware, focusing on their behaviour and the methods used to gain access and control to mobile devices.
- **Measurable:** Investigate multiple malware families and identify their behaviours.
- **Achievable:** Use android emulators to have a safe secured environment to then use malware analysis tools using both static and dynamic methods of investigation.
- **Relevant:** Address the growing requirements for better malware security on android devices due to it being the largest market share OS for mobile.
- **Time-bound:** Complete the analysis and reporting within the constraints of my submission time, including periodic reviews by my supervisor.

This project is worth creating due to the growing market of android mobile devices that are big targets by threat actors, yet there are less tools and methodologies than the significant number of threats and mobile devices face.

To make sure this project is a success, I will need to have detailed analysis of the multiple malware families I will be conducting research on, ensuring that I use real-world scenarios and applicable methods in my research and applied investigation.

Literature Review

The rapid growth in the mobile market has led to a major increase in mobile based malware, designed to exploit and/or steal data from its victims. The fight between defensive security and offensive malware designed by threat actors is an ongoing back and forth fight constantly demanding new methods of detection and prevention.

Malware is becoming increasingly sophisticated making use of more complex evasion methods to avoid detection like obfuscation and polymorphic behaviour to keep the malware constantly changing to avoid traditional detection means.^[2] Threat actors are also becoming more thoughtful about their attacks, now targeting devices for banking information and access to banking apps in the recent mainstream. Ransomware becoming a major player in the malware market with large organizations being targeted by hacking groups, encrypting company data for a large ransom. The average ransom payment in 2020 was around 310k USD. Up 171% from the previous year, it has become the main avenue for Threat Actors.^[3]

The ever-changing malware landscape requires constant vigilance for new malware variants that target people and systems in different ways. New methods constantly need to be evaluated and implemented to slow down the evolution of malware. More advanced malware methods like ransomware are constantly changing their attack vectors and infection methods so new research and tools constantly have to be created and developed to find more efficient ways of protecting users.^[3] Making use of machine learning as a new tool to find more automated ways that can prevent and identify malware faster than humans is something that is new to the cyber security bubble but could prove extremely useful in time if enough research is done into finding the most efficient and cost effective methods.^[4]

The justification for this project lies in the need for more research into different malware families and what we can do better to prevent them from doing an increasing amount of damage. Identifying trends in malware to better prepare for an increase in specific methods of attack. Also evaluating different tools to see how they compare against different types of malwares, allowing us to further understand how we should make use of different methods and tools to find the best way to investigate malware types.^[5] Bridging the research gap to allow other researchers more information and how different malware types are interacted by different tools and how they can affect user systems.

Project Design

I will be using emulators / virtual machines for this project to allow me to complete this project with less risk to my personal network and machine. I will also airgap my machine to make sure there is no risk to my network. Using emulators like QEMU or Genymotion are both open source and designed with malware analysis in mind. I will likely use these or something to a similar affect.

For my project, I will be conducting different types of analysis to allow me to make clearer and proven effective methods of analysis against mobile malware types. I will conduct static analysis to examine the structure of the malware, so I can disassemble the code and analyse it without requiring execution. One program I will use for this is IDA, a disassembler and debugger that I can use to find the code structure. I could also use Ghidra for this. Androguard will also be used to disassemble and extract any and all API calls for investigation. I could also use MobSF, which provides a web interface to allow me to analyse that way, it is also capable of generating reports, which I may find useful in the future for comparisons.

I will also conduct Dynamic analysis of the malware to find any malicious activities the malware may try to conduct that would not be identified using static methods. Using a tool like Cuckoo for sandboxing, allowing me to run the malware in an isolated environment safely allowing me to analyse the malware. Using tools like Frida to analyse running apps and processes, to identify more dynamic features of malware.

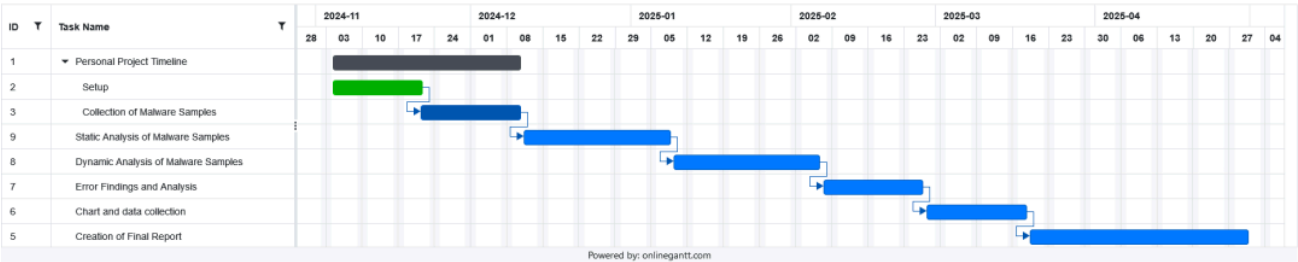
I can also use cloud-based analysis methods like using Virus Total (VT) to gain a quick overview from other antivirus engines to see how they classify each piece of malware. This can allow me to cross-compare based on my own findings.

I will conduct analysis of the data I compile from my research, I will be compiling feature extraction, so I can evaluate their similarities to other malware and helping me to classify the malware. Where necessary I will collect qualitative data that I can then use to analyse trends and potential counter measures to what I find. I can then compile this data into the relevant formats (graphs etc.) Doing error analysis will be a must, as I can find errors that the tools have made or myself, and explain ways of avoiding these errors and learning from them in the future, making sure that other people do not make these same mistakes.

I will also complete behaviour analysis using tools like androidprocmon, an open-source fork of process monitor that will allow me to complete monitoring on an android device. I possibly could also make use of Wireshark, a powerful packet sniffing tool that will allow me to see in detail what the malware is trying to do.

Resources / Planning

I will deliver at the end of this project a report that details all of my considerations and implementations of malware analysis. It will include actual personal generated results, my findings, any metrics, contributions and limitations. I will include visualisations of my findings and behavioural reports from my analysis.



I will require a malware database which I can use for analysis, using publicly available datasets from multiple sources.

References

[1]
Q. Xu, D. Zhao, S. Yang, L. Xu, and X. Li, "Android Malware Detection Based on Behavioral-Level Features with Graph Convolutional Networks," vol. 12, no. 23, p. 4817, Dec. 2023, doi: 10.3390/electronics12234817.

[2]
P. Faruki, R. Bhan, V. Jain, S. Bhatia, N. El Madhoun, and R. Pamula, "A Survey and Evaluation of Android-Based Malware Evasion Techniques and Detection Frameworks," vol. 14, no. 7, p. 374, Jul. 2023, doi: 10.3390/info14070374.

[3]
N. Kshetri and J. Voas, "Ransomware: Pay to Play?," vol. 55, no. 3, pp. 11–13, Mar. 2022, doi: 10.1109/MC.2021.3126529.

[4]
S. Peng, L. Cao, Y. Zhou, J. Xie, P. Yin, and J. Mo, "Challenges and Trends of Android Malware Detection in the Era of Deep Learning," pp. 37–43, Dec. 2020, doi: 10.1109/ISCI50694.2020.00014.

[5]

J. Gennari and D. French, "Defining malware families based on analyst insights," pp. 396–401, Nov. 2011, doi: 10.1109/THS.2011.6107902.

Project Proposal Final - 2200897 Kai Probert

GRADEMARK REPORT

FINAL GRADE

GENERAL COMMENTS

67 / 100

PROJECT PROPOSAL – ACCA6020 INDEPENDENT PROJECT

Student Kai Probert Mark 67

Intro / A&O (400 words)		
Project title; Identification of a specific problem to be investigated; Well-defined aims and SMART objectives; Explaining why this project is worth doing; Discussion of what the project needs to do in order to be a success; Description any deliverables that will be produced at the end of the project	20	14
Project Title and the idea aligns well. Following are my recommendations		
To Do:		
+ Your Aim should be a broad statement on what you want to achieve. The aim must tell the reader what the		

end result is likely to be. It doesn't need to specify how, but it need to clarify the work on focus. + Objectives must be a breakdown of your aim into Specific, Measurable, Achievable, Relevant, and Time-bound tasks.		
Background to the Project / Literature Review (400 words)		
Description of how the work to be done by in the project relates to the work identified in the literature review; Discussion of any ethical issues raised by the project Identifying what has already been done within the field; Topic familiarity; Brief literature review using appropriate sources – 6-8 journal papers and book chapters rather than just websites; Selection of relevant models & concepts Literature review done. However, more adequate literatures, critical appraisals could have added value to the work. Literatures on Open Source Mobile Forensics Tools could have given insights. To Do: + Define Keywords and Search for Literatures ScienceDirect, ACM, and IEEE (Accessible via UWTSD Library)	20	10

+ Review literatures that focus on recent malware attacks in Mobile Phones, approach in Mitigating etc. + Identify what is the problem these literatures are addressing? + Explain the problem with details like the type of malwares, its operations, tools to detect, mitigation steps etc. + Identify the Gap. + Clearly state how your project will address this gap or to experiment this malware attacks.		
Project Design (500 words)		
Clear statement of which development methods are to be used and why they are appropriate; Clear statement of which tools are to be used and why they are appropriate; Clear description of how data collected will be analysed In order to work on your design (different types of analysis), you must do a proper Literature review to under the different types of analysis. Addressed the tools and environments. However, it could have been presented well.	30	24

Resources / Planning (200 words)		
List of any deliverables; Clear diagram showing both timing and resource use; Completed ethics form; Limited and relevant appendices Done	15	11
Document Presentation		
Correct spelling, grammar and punctuation; Flow of narrative/fluency; Coherence; Word processed ; Correct use of referencing with bibliography; Strict word limit Presented well	15	8
TOTAL	100	67

PAGE 1

PAGE 2

PAGE 3

PAGE 4

PAGE 5
