University of Passau
Faculty of Computer Science and Mathematics

Chair of Computer Engineering
Prof. Dr. Stefan Katzenbeisser

Master's Thesis
in
Computer Science

Android Threat Detection Through Passive VPN Monitoring and IP Reputation Analysis

Shayan Rostamzadeh
111769

Date:	2025-09-29
Supervisors:	Prof. Dr. Stefan Katzenbeisser
	Dr. Ing. Nikolaos Athanasios Anagnostopoulos
Advisor:	Nico Mexis

Rostamzadeh, Shayan
Theresienstrasse 8
94032, Passau

ERKLÄRUNG

Ich erkläre, dass ich die vorliegende Arbeit mit dem Titel „Android Threat Detection Through Passive VPN Monitoring and IP Reputation Analysis“ selbstständig, ohne unzulässige Hilfe und ohne Benutzung anderer als der angegebenen Quellen und Hilfsmittel verfasst habe und dass alle wörtlich oder sinngemäß übernommenen Stellen als solche kenntlich gemacht sind.

Mit der aktuell geltenden Fassung der Satzung der Universität Passau zur Sicherung guter wissenschaftlicher Praxis und für den Umgang mit wissenschaftlichem Fehlverhalten vom 31. Juli 2008 (vABlUP Seite 283) bin ich vertraut.

Ich erkläre mich mit einer Überprüfung der Arbeit unter Zuhilfenahme von Dienstleistungen Dritter (z.B. Anti-Plagiatssoftware) zur Gewährleistung der einwandfreien Kennzeichnung übernommener Ausführungen ohne Verletzung geistigen Eigentums an einem von anderen geschaffenen urheberrechtlich geschützten Werk oder von anderen stammenden wesentlichen wissenschaftlichen Erkenntnissen, Hypothesen, Lehren oder Forschungsansätzen einverstanden.

.....
(Name, Vorname)

Translation of German text (notice: Only the German text is legally binding)

I hereby confirm that I have composed the present scientific work entitled “Android Threat Detection Through Passive VPN Monitoring and IP Reputation Analysis” independently without anybody else’s assistance and utilising no sources or resources other than those specified. I certify that any content adopted literally or in substance has been properly identified and attributed.

I have familiarised myself with the University of Passau’s most recent Guidelines for Good Scientific Practice and Scientific Misconduct Ramifications of 31 July 2008 (vABlUP page 283).

I declare my consent to the use of third-party services (e.g. anti-plagiarism software) for the examination of my work to verify the absence of impermissible representation of adopted content without adequate attribution, which would violate the intellectual property rights of others by claiming ownership of somebody else’s work, scientific findings, hypotheses, teachings or research approaches.

Supervisor contacts:

Prof. Dr. Stefan Katzenbeisser
Chair of Computer Engineering
University of Passau
Email: stefan.katzenbeisser@uni-passau.de
Web: https://www.fim.uni-passau.de/en/computer-engineering/

Dr. Ing. Nikolaos Athanasios Anagnostopoulos
The chair of your second advisor professor
University of Passau
Email: nikolaos.anagnostopoulos@uni-passau.de
Web: https://www.anagnostopoulos.academy/

Abstract

Mobile devices are becoming more and more immersed in our daily lives, making them attractive targets for threats such as malware, data exfiltration, and unauthorized access and even end-points for APTs (Advanced Persistent Threat) in a huge number of companies that comply with with BYOD (Bring Your Own Device) policy for cost reduction and personal convenience. The comprehensive use of mobile devices in sensitive and vital business operations highlights the necessity of advanced monitoring and threat detection mechanisms.

While existing tools like PCAPdroid and Ant-Monitor provide traffic analysis and monitoring capabilities, they often lack integration with real-time threat recognition. This project exhibits the design and implementation of an Android-based threat detection application that leverages the android VPNService API to capture and intercept network/internet traffic. This comes alongside the functionality to map associated packets to originating device applications. This thesis project incorporates AbuseIPDB. A well-known platform dedicated to helping users and administrators combat the spread of hackers, spammers, and abusive activity on the internet. This incorporation is to assess the maliciousness of destination IP addresses in the outgoing internet packets, notifying the user of the corresponding potential risk(s) that the application can introduce.

This application is developed as a complementary extension to PCAPdroid that lacks live threat detection and analysis of network/internet traffic. It utilizes the passive packet-capture capabilities of PCAPdroid and employs AbuseIPDB capabilities to bridge the gap between packet capture and live threat analysis combined with the latest modern user interface approaches.

This application receives the outgoing IP address, application UIDs to extract the app-specific information alongside other useful data in the form of a PCAPNG file via a local TCP Server from PCAPdroid and subsequently transmits and inquiry to AbuseIPDB to evaluate the maliciousness of outbound traffic.

Threat Detector illustrates an ability to identify suspicious connections with minimal performance and storage overhead, highlighting it as a potent and practical tool to enhance mobile security, privacy and user awareness.

Contents

1 Introduction

Modify the text below

should i implement the deviations from the first idea of the app?

1.1 Background and Motivation

In today's connected world, mobile devices have evolved from simple communication intermediaries to vital hubs not only for personal use but also professional activities. They have undoubtedly become personal assistance, banking platforms, health trackers and entertainment centers, and also professional workstations. Smartphones, Tablets, and other similar portable devices now store sensitive information such as personal messages, financial intel, business-related documents and login credentials. Nowadays as mobile devices are increasingly integrating with enterprise businesses and consequently their associate networks through policies such as BYOD (Bring Your Own Device), we see them more frequently being subjected to cyber attacks including mobile malware, unauthorized access, data exfiltration, Advanced Persistent Threats (APTs), etc. This widespread adaption of mobile technology and its undeniable integration in our daily personal and professional lives in combination with users and companies reliance have considerably expanded the attack surface for adversaries. Additionally, the on-going increase in the use of mobile devices to access sensitive corporate and financial resources also amplifies the potential damage an intrusion can lead to. This means that the security landscape of mobile platforms is therefore, both dynamic and highly critical. Thus, it requires solutions and approaches that continuously adapt to such evolving threats while ensuring practicality.

1.2 Problem Statement

Most of enterprise network systems belong to a pool of PCs (Personal computers) and servers. Therefore, the majority of traditional cybersecurity measures often focus on such systems. However, the integration and usage of mobile devices in enterprise networks introduce unique challenges that require a different approach. The diversity of mobile devices' operating systems, varying security and privacy policies, constant updates and patches, and openness of certain app-ecosystems complicate protecting mobile devices. Among mobile operating systems, Android has gained the most popularity and market

share due to its open-source nature and flexibility to be implemented in various environments. However, Android's open-source architecture, alongside its fragmented ecosystem and, in a lot of cases, its inconsistent update policies make it in particular considerably susceptible to attacks. These lead malicious actors to utilize various application-level and network-based attacks and also abuse hardware and software vulnerabilities to compromise user's privacy and the organization's security.

It is worth mentioning that the traditional endpoint security solutions such as anti-malware software, often lead to inadequate results for mobile devices including android phones. Many are based on signature recognition, and operate reactively meaning they typically identify malware signatures after the infection completely took place. Moreover, they are incapable of monitoring the full scope of the device's network and its behaviour. Furthermore, android system suffers from an invisibility gap. Even though android has a sandboxing mechanism which provides isolation between running applications, it also limits the visibility of network activities associated with each app. This simply means that users and more importantly administrators cannot easily determine which of the running applications is connecting to external servers, nor they can evaluate the legitimacy of the established connections.

Consequently, there is a significant need for a real-time, lightweight monitoring solution that not only captures the traffic, but also identifies suspicious patterns stacked with the capability to map each of those activities to specific applications. This gives the users and administrators the visibility, without which, organizations might remain at risk of covert data leakage and eventually exposure to malicious infrastructure.

1.3 Existing Solutions and Their Limits

This paper is not the first to introduce defensive and preventive solutions to offensive security attempts made by malicious actors. However, it acts as a complementary extension for previously designed solutions such as PCAPdroid and Ant-Monitor that function on unrooted devices based on android's VpnService mechanism. Such tools represent vital insights into how applications interact with local and external servers, letting the user perform forensic analysis of network traffic and point out potential anomaly-indicating behaviours. While current solutions for mobile threat detection and network monitoring are well established and offer the foundation for capabilities such as network traffic analysis, application activity monitoring, and anomaly detection, they often

- **Lack real-time threat detection and automated integration of threat intelligence:** Neither of the mentioned monitoring tools implement automated checks against malicious IP databases or incorporate a reputation assessment service. As a result, threat identification relies heavily on the expertise the user possesses and the manual processing of analysing each and every IP address.
- **Have limited real-time protection:** While they are really effective in packet capture, they do not provide the user with any sort of alerts regarding suspicious activities.
- **Dump the device traffic as a PCAP file and send it remotely for further analysis (e.g. to Wireshark):** This ensures the inevitable need for an external inspection system/application to allocate the IP address and the network connections to a white or black list.
- **Have limited user accessibility:** These tools as shown later in this paper, often present raw data packets. This can be significantly overwhelming for users without any technical background. The lack of intuitive, well-designed interfaces, and actionable insights introduce restrictions to adapting such applications with daily lives and

limit their use to only research contexts.

- **Lack blocking capabilities:** The mentioned tools among other existing ones do not typically support active traffic blocking capabilities, leaving the user without any mitigating countermeasures once the threat is detected.

The complexity of mobile threats that are on continues growth and the aforementioned gaps highlight the vital necessity of a solution that not only makes uses of monitoring capabilities provided by mobile platforms (e.g android's VpnService), but also delivers actionable, intelligence-driven, and user-friendly insights.

1.4 Research Objectives

This thesis aims to design and evaluate a threat detection application for android devices that addresses some of the above-mentioned limitations.

From the applications mentioned above, PCAPdroid has been chosen as the underlying solution that provides not only the capabilities to passively sniff app-specific network traffic but also presents application metadata. According to its official website PCAPdroid is an open source network capture and monitoring tool for android devices which works without root privileges.

The common use cases of PCAPdroid include:

- Analyze the connections made by the apps installed into the device, both user and system apps.
- Dump the device traffic as a PCAP and send it remotely for futher analysis (e.g. to Wireshark).
- Decrypt the HTTPS/TLS traffic of a specific app PCAPdroid leverages the android VpnService to receive all the traffic generated by the android apps. No external VPN is actually created, the traffic is processed locally by the app.

This application alongside the real-time threat detection provided by the project presented in this paper will expand the possibilities and ease the user interaction and notification in case of malicious activities.

As the usage of mobile applications increases in business constellations and the centralization of information is more intensified, more internet connections and data transfer take place. This would potentially open some doors for the adversaries to abuse these connections for their own benefit while user privacy is completely neglected. A huge threat that connection of mobile applications with internet brings along, is data exfiltration. Data exfiltration is an underlying concept for most of the applications to function correctly since their logic relies on connection to a back-end server via internet. This however, can theoretically endanger user privacy if user's consent is not taken into consideration. This could take place by utilizing internet packets' outbound connections. The mobile threat detection application developed in this thesis addresses data transfer specifically. These challenges are addressed by combining real-time internet traffic monitoring, UID-to-application mapping, and finally threat intelligence integration.

By leveraging the android's VpnService API the application-specific packets are inspected, their correlation with app-generated traffic is established and as the last step, the suspicious IP (Internet Protocol) addresses are cross-referenced with external thread detection databases such as AbuseIPDB. Using this approach the visibility of potential malicious activities is enhanced and also some actionable insights are provided that eventually can

assist users and organizations to mitigate risks and potential vulnerabilities before the escalate into various security incidents.

This thesis contributes to the field of mobile and android cybersecurity by illustrating an effective methodology for an app-level threat detection and intelligence, real-time monitoring, and also proactive risk management solution. The results and findings of this project, emphasizes both the potential and the limitations mobile threat detection systems and also represents a foundation for future work, research and actions in securing android devices in our increasingly complex and hyperconnected environments.

In order to start using this template, change the values inside `thesis.tex` to your liking. *It is strongly advised to only change what is necessary (language, names etc.).* Please also remember to remove the "REMOVE ME LATER" part when you are done. Below you can find some examples of important LaTeX-commands.

This is a cited text [1].

Add more content

This is a reference to Chapter 7 and Section 1.5.

We can also add code such as in **??**.

You can also include and reference figures and tables such as Figure 1.1 and Table 1.1. Notice how the table cannot be placed using the "h" specifier and thus uses the "t" specifier instead?

Figure 1.1: Captions for figures are usually placed below. The German logo of the University of Passau.

URLs can be added for example like this: `https://www.fim.uni-passau.de/technische-informatik/`.

Table 1.1: Captions for tables are usually placed above. φ denotes the Euler totient function, by the way.

x	$\varphi(x)$
1	1
2	1
3	2
4	2
5	4
6	2

1.5 Some section...

2 Background

Show the PCAPdroid app and info about it from its website in the background section or similar

add the trial to make the VPN myself and the attempt to use android VpnService and the difficulties it has brought

3

Related Work

4

Architecture/System Design

5 Implementation

6 Evaluation and Discussion

7 Conclusion

In the conclusion, all the main results are summarised once again. Here, experiences made can also be described. At the end of the summary, an outlook can also follow, which presents the future development of the topic dealt with from the author's point of view.

A

Appendix

List of Figures

List of Tables

Bibliography

[1] Benjamin Taubmann, Noelle Rakotondravony, and Hans P. Reiser. CloudPhylactor: harnessing mandatory access control for virtual machine introspection in cloud data centers. In *2016 IEEE Trustcom/BigDataSE/ISPA*, pages 957–964, Aug 2025. doi: 10.1109/TrustCom.2016.0162.