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:	2025-09-24
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.

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 addition 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 state-of-the-art 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

As the usage of mobile applications increases and the centralization of information is more intensified, more internet connections 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 the outbound connections.

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 1.1.

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

1.1 Some section...

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.

Nam dui ligula, fringilla a, euismod sodales, sollicitudin vel, wisi. Morbi auctor lorem non justo. Nam lacus libero, pretium at, lobortis vitae, ultricies et, tellus. Donec aliquet, tortor sed accumsan bibendum, erat ligula aliquet magna, vitae ornare odio metus a mi. Morbi ac orci et nisl hendrerit mollis. Suspendisse ut massa. Cras nec ante. Pellentesque a nulla. Cum sociis natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Aliquam tincidunt urna. Nulla ullamcorper vestibulum turpis. Pellentesque cursus luctus mauris.

Nulla malesuada porttitor diam. Donec felis erat, congue non, volutpat at, tincidunt tristique, libero. Vivamus viverra fermentum felis. Donec nonummy pellentesque ante. Phasellus adipiscing semper elit. Proin fermentum massa ac quam. Sed diam turpis, molestie vitae, placerat a, molestie nec, leo. Maecenas lacinia. Nam ipsum ligula, eleifend at, accumsan nec, suscipit a, ipsum. Morbi blandit ligula feugiat magna. Nunc eleifend consequat lorem. Sed lacinia nulla vitae enim. Pellentesque tincidunt purus vel magna. Integer non enim. Praesent euismod nunc eu purus. Donec bibendum quam in tellus. Nullam cursus pulvinar lectus. Donec et mi. Nam vulputate metus eu enim. Vestibulum pellentesque felis eu massa.

Quisque ullamcorper placerat ipsum. Cras nibh. Morbi vel justo vitae lacus tincidunt ultrices. Lorem ipsum dolor sit amet, consectetuer adipiscing elit. In hac habitasse platea dictumst. Integer tempus convallis augue. Etiam facilisis. Nunc elementum fermentum wisi. Aenean placerat. Ut imperdiet, enim sed gravida sollicitudin, felis odio placerat quam, ac pulvinar elit purus eget enim. Nunc vitae tortor. Proin tempus nibh sit amet nisl. Vivamus quis tortor vitae risus porta vehicula.

Fusce mauris. Vestibulum luctus nibh at lectus. Sed bibendum, nulla a faucibus semper, leo velit ultricies tellus, ac venenatis arcu wisi vel nisl. Vestibulum diam. Aliquam pellentesque, augue quis sagittis posuere, turpis lacus congue quam, in hendrerit risus eros eget felis. Maecenas eget erat in sapien mattis porttitor. Vestibulum porttitor. Nulla facilisi. Sed a turpis eu lacus commodo facilisis. Morbi fringilla, wisi in dignissim interdum, justo lectus sagittis dui, et vehicula libero dui cursus dui. Mauris tempor ligula sed lacus. Duis cursus enim ut augue. Cras ac magna. Cras nulla. Nulla egestas. Curabitur a leo. Quisque egestas wisi eget nunc. Nam feugiat lacus vel est. Curabitur consectetuer.

Suspendisse vel felis. Ut lorem lorem, interdum eu, tincidunt sit amet, laoreet vitae, arcu. Aenean faucibus pede eu ante. Praesent enim elit, rutrum at, molestie non, nonummy vel, nisl. Ut lectus eros, malesuada sit amet, fermentum eu, sodales cursus, magna. Donec eu purus. Quisque vehicula, urna sed ultricies auctor, pede lorem egestas dui, et convallis elit erat sed nulla. Donec luctus. Curabitur et nunc. Aliquam dolor odio, commodo pretium, ultricies non, pharetra in, velit. Integer arcu est, nonummy in, fermentum faucibus, egestas vel, odio.

Sed commodo posuere pede. Mauris ut est. Ut quis purus. Sed ac odio. Sed vehicula hendrerit sem. Duis non odio. Morbi ut dui. Sed accumsan risus eget odio. In hac habitasse platea dictumst. Pellentesque non elit. Fusce sed justo eu urna porta tincidunt. Mauris felis odio, sollicitudin sed, volutpat a, ornare ac, erat. Morbi quis dolor. Donec pellentesque, erat ac sagittis semper, nunc dui lobortis purus, quis congue purus metus ultricies tellus. Proin et quam. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos hymenaeos. Praesent sapien turpis, fermentum vel, eleifend faucibus, vehicula eu, lacus.

2 Background

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.

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 2016. doi: 10.1109/TrustCom.2016.0162.