

Configuration Manual

MSc Research Project MSc in Cybersecurity

Rajendra Yashwant Topare Student ID: 21222061

> School of Computing National College of Ireland

Supervisor: Mr. Vikas Sahni

National College of Ireland



MSc Project Submission Sheet

School of Computing

| Student Name: | Rajendra Yashwant Topare | | | |
|--------------------------------------|---|-------|---------|--|
| Student ID: | 21222061 | | | |
| Programme: | MSc in Cybersecurity | Year: | 2022-23 | |
| Module: | MSc Research Project | | | |
| Lecturer: Submission Due Date: | Mr. Vikas Sahni | | | |
| | 18/09/2023 | | | |
| Project Title: | A Technique to Steal OAuth Tokens in Android-Based Devices Using a Malicious Application | | | |

Word Count:741Page Count: 7

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

<u>ALL</u> internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Rajendra Yashwant Topare

Date: 16/09/2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

| Attach a completed copy of this sheet to each project (including multiple copies) | |
|---|--|
| Attach a Moodle submission receipt of the online project | |
| submission, to each project (including multiple copies). | |
| You must ensure that you retain a HARD COPY of the project, | |
| both for your own reference and in case a project is lost or mislaid. It is | |
| not sufficient to keep a copy on computer. | |

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

| Office Use Only | |
|----------------------------------|--|
| Signature: | |
| Date: | |
| Penalty Applied (if applicable): | |

Configuration Manual

Rajendra Yashwant Topare 21222061

1 Introduction

This document provides an overview of the system requirements and step-by-step instructions to create an Android application intended for stealing OAuth tokens from Android devices. The designed application is deployed on an Android device and an Android simulator on a laptop to provide a complete demonstration of token theft on both web and Android applications.

2 System Requirements

This section provides an overview of the hardware and software specifications required to perform the proposed task.

2.1 Hardware Details:

The implementation was carried out on a Samsung device and an Acer laptop, with the following device specifications:

Mobile details:

Model Name: Samsung M51 OS Name: Android 11.0 (Min. required – Android 6.0 Marshmallow)

Laptop details:

Model Name: Acer Aspire A514-54G OS Name: Microsoft Windows 11 – 11th Gen Intel® CoreTM i5

2.2 Software Details:

| Application | Version | Description |
|--------------------------------|---------------------|---|
| Name | | |
| Android Studio | Flamingo 2022.2.1 | It is used to design, build, and test Android applications ¹ . |
| Genymotion | 3.5 | It enables the testing and running of Android apps on a computer ² . |
| Programming Language - Java | Java 11 | Useful for creating Android applications due to its platform compatibility. |

¹ <u>https://www.genymotion.com</u>

² <u>https://developer.android.com/studio</u>

3 Implementation

3.1 Installation:

Android studio:

It is an open-source application that was downloaded from the Android Studio download page using the version which is compatible with the operating system.



Figure 1. Android Studio

Genymotion:

The most recent version of Genymotion was downloaded from its official website. After the download, the installer was executed, and afterwards, installation prompts allowed the installation location to be specified. Upon completion, the application was available for use enabling Android app emulation and testing.



Figure 2. Genymotion

3.2 Environment Setup:

After installing Android Studio successfully on the system, a new project with a name, programming language, and minimum SDK requirements has been created.

| <u> </u> | Navigate Code Refactor Build Run Iools VCS Window Help fbtokentheft-strings.xml [fbtokentheft.app.main] | |
|---------------|---|----------------|
| 🞽 New Project | | |
| Empty View | is Activity | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | DK API 23: Android 6.0 (Marshmallow) | |
| | Your app will run on approximately 97.7% of devices. Help me choose | |
| | Previous Next Cancel | <u>F</u> inish |

Figure 3. Creation of a new project in Android Studio.

3.3 Build Project:

The code is written in the Java programming language. After debugging the code and executing it successfully in the studio, the final APK was generated.

| 🗯 Eile Edit View Navigate Code Refactor Build Ryn Tools VCS Window Help - (btokentheft-stringssmil (btokentheft.app.main) | | | | | × |
|---|--|--|--|--|--|
| fbtokentheft) app) src) main) res) values) 🏭 | | | | | ર 📀 🗖 |
| 눈 🛎 Android 👻 😔 王 🛨 🗕 | - 🧿 MainActivity.java 🗵 🏭 AndroidManifest.xml 🗵 🚜 strings.xml 🐇 | | | | ¢ − 6 |
| Image: Second | Edit translations for all locales in the translations editor. <pre></pre> | Open editor Hide motification tion">Navigate home on">Navigate up scription">Nore options /string> eall'>See all ose_application">Choose an appg> rial">sans-serif rial">sans-serif rial">sans-serif aterial">sans-serif | | | 2 Device Manager 🐐 Restitutions 📽 Gradie 🕂 🕂 🖿 🖂 |
| res (generated) | resources string | | | | |
| Image: Constant successfully finish Image: Constant successfully finish < | app' on Pixel_3a_API_34_extension_level_7_x86_64. d in 985 ms. . naj.fbtokenthoft/com.raj.fbtokentheft.HainActivity" - <u>con Pixel 3a API_34_extension_level_7_x86_64</u> device 'Pixel_3a_API_34_extension_level_7_x86_64 [emu | | | | - □ Device Rie Explorer |

Figure 4. The project is running successfully in Android Studio.

| 🛎 <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>N</u> avigate <u>C</u> ode <u>R</u> efactor | <u>Build</u> R <u>un T</u> ools VC <u>S W</u> indow <u>H</u> | elp fbtokentheft - strings.xml [fbtokentheft.app.main] | | - 0 | × |
|---|--|--|--|---------|------------|
| fbtokentheft $ angle$ app $ angle$ src $ angle$ main $ angle$ res $ angle$ values $ angle$ $rac{d}{d}$ | | 🔨 🔺 app 💌 📑 samsung SM-G9550 💌 🕨 🖉 | | 🗓 🔍 🔍 🄇 | 2 |
| ू 🛎 Android 👻 😌 至 🛨 💠 | | | | | : 6 |
| | | ranslations editor. | | | |
| a Tidninesis | | Build APK(s) -8"?> | | | |
| ž ∨ i java | | | | | |
| Com.rai.fbtokentheft | | | | | |
| + | | | | | - * |
| com.raj.fbtokentheft (androidTest) | | | | | |
| com.raj.fbtokentheft (test) | | | | | |
| 🞼 java (generated) | | | | | |
| 🕆 🛅 res | | Select Build Variant abc_activitychooserview_choose_application">Choose an app | | | |
| > 🖿 drawable | | | | | |
| > Da layout | | | | | |
| > D mipmap | | | | | |
| | | | | | |
| a ctringe yml | 13 <string name="</td"><td></td><td></td><td></td><td></td></string> | | | | |
| > In themes (2) | 14 <string name="</td"><td>"abc_font_family_caption_material">sans-serif</td></string> | "abc_font_family_caption_material">sans-serif | | | |
| ✓ Di xml | 15 <string name="</td"><td>"abc_font_family_display_1_material">sans-serif</td></string> | "abc_font_family_display_1_material">sans-serif | | | |
| ackup_rules.xml | 16 <string name="</td"><td>"abc_font_family_display_2_material">sans-serif</td></string> | "abc_font_family_display_2_material">sans-serif | | | |
| data_extraction_rules.xml | 17 <string name="</td"><td></td><td></td><td></td><td></td></string> | | | | |
| res (generated) | 18 <string name="</td"><td>"abc_font_family_display_4_material">sans-serif-light</td></string> | "abc_font_family_display_4_material">sans-serif-light | | | |
| 월 👌 🗬 Gradle Scripts | 19 <string name="</td"><td>"abc_font_family_headline_material">sans-serif</td></string> | "abc_font_family_headline_material">sans-serif | | | |

Figure 5. Building APK in Android Studio.

3.4 Run Project:

After the APK was successfully generated, it has been deployed. In our case, the application was deployed on a compatible Android device and Genymotion's Android simulation environment.



Figure 6. Running the application on Genymotion.

References

Shehab, M. and Mohsen, F. (2014) 'Towards enhancing the security of OAuth implementations in smart phones', *Proceedings - 2014 IEEE 3rd International Conference on Mobile Services, MS 2014*, pp. 39–46. Available at: <u>https://doi.org/10.1109/MOBSERV.2014.15</u>.

Luo, T. *et al.* (2011) 'Attacks on WebView in the Android System', in *Proceedings of the 27th Annual Computer Security Applications Conference*. New York, NY, USA: Association for Computing Machinery (ACSAC '11), pp. 343–352. Available at: <u>https://doi.org/10.1145/2076732.2076781</u>.