UNIVERSITÉ DU
LUXEMBOURG

Static and Dynamic Software Security Analysis

Project

Prof. Jacques Klein & Marco Alecci

2024

Within this project, you will apply the concepts learned throughout the course in the context of Android applications by analyzing real-world Android apps. Your focus will be directed towards key segments of Android apps, such as critical components or areas with a higher potential for risk. This will allow you to gain hands-on experience in performing targeted analysis techniques. This project consists of two main sections. Details of each section are provided below.

Requirements:
The project must be completed exclusively using automated techniques. **Manual analysis is not allowed unless explicitly requested.** You may use either the Virtual Machine provided in the labs or your own environment. If you choose the latter, you will be responsible for setting up all dependencies and ensuring that all the programs you intend to use function correctly.

Section 1: Introduction to FlowDroid for Taint Analysis

Throughout this course, we have discussed various types of program analysis, including **Taint Analysis**. Taint Analysis is a method for tracking how data flows within a program, which is particularly useful for identifying security vulnerabilities and potential data leaks. For this project, you will use FlowDroid, a leading tool for performing Taint Analysis on Android applications. In the shared drive link provided at the end of this document, you will find **10 Android APK files**. Your task is to analyze these APKs using FlowDroid to identify potential data leaks, modifying the timeout parameter for each analysis. You will then compare and discuss the differences in results. Here is a breakdown of what you have to do:

- **Research Android App Components**: Begin by reviewing the components of Android applications (e.g., Activity) and their respective lifecycles. You may refer to the official Android documentation or other reputable resources.
- **Understand FlowDroid and Configuration Options**: Familiarize yourself with the FlowDroid tool and its configuration settings, specifically those related to timeout adjustments.
- **Identify Sources and Sinks**: Review the concepts of ”sources” and ”sinks” in Taint Analysis. Select appropriate sources and sinks for your analysis to track potential data leaks accurately.
- **Run FlowDroid Analysis**: For each APK, perform three separate analyses by setting different timeout values—1 minute, 5 minutes, and 20 minutes. Each APK should thus be analyzed three times.
- **Document Hardware and Configuration**: In your report, include the specifications of the hardware used for your analysis (e.g., CPU, RAM, etc.) and provide details of the FlowDroid configuration options used, explaining the purpose of each.
- **Analyze and Discuss Results**: Based on your findings using the 20-minute timeout:
  - Present the ”raw numbers,” i.e., the number of potential data leaks reported by FlowDroid for each APK.
  - Describe any potential data leaks identified across different apps (limit to no more than 10).
  - Assess whether each potential data leak is genuine. Based on the app’s expected behavior, do you consider this data flow to be normal or a data leak? Justify your reasoning.
- **Evaluate the Impact of Timeout**: Examine the effect of the timeout setting on results. Are the ”raw numbers” consistent across different timeouts? Do the potential data leaks you previously described persist when the timeout is shorter? If results differ, suggest possible reasons for these variations.
- **[Optional] Repeat with Different Hardware Setup**: For an extra challenge, perform the same analyses on a different hardware setup (e.g., adjusting the memory in a Virtual Machine or using a different laptop). Compare and discuss any differences in the results across these setups.

Section 2: Privacy Requirements Compliance Checking in Android Apps
Imagine you are a security analyst tasked with assessing whether an Android app complies with certain privacy requirements derived from regulations such as the GDPR. For this analysis, you may select one of the 10 apps provided in Section 1. You will focus on verifying compliance with the following two requirements:

1. **R1:** Information related to the user's device location must not be sent outside the app.
2. **R2:** The user should have the ability to delete their account.

For the first requirement (**R1**), you should use FlowDroid to analyze the app, selecting appropriate sources and sinks to determine if any location-related information is sent outside the app. For the second requirement (**R2**), you have flexibility in your approach. You can use static analysis (e.g., FlowDroid), dynamic analysis, AI, large language models (LLMs), or a combination of methods. Manual analysis (e.g., inspecting the Smali code after decompiling the APK) is allowed only to gain insights for developing your automated approach. The final goal is to determine whether the app provides a mechanism for account deletion.

In your project report, be sure to include the following:

- A detailed explanation of the strategy used for **R1 & R2**.
- The results of your analysis for **R1**.
- The findings for **R2**, based on your chosen approach.

Deliverables:

- A project report (no more than six pages) detailing the analysis of the selected Android app. You may include one additional page if you complete the optional task at the end of Section 1. The report should include:
  - **Description of the Analysis Setup used in Section 1:** A summary of the hardware and software configuration used, including all relevant FlowDroid configuration options.
  - **Results of Section 1 Analysis:** Findings from the Taint Analysis, including observed data leaks, a discussion on whether these leaks are expected behavior, and an analysis of how different timeout settings affected results.
  - **Compliance Check for Section 2:** Results and insights regarding the two privacy requirements (R1 and R2), including the method used for each requirement and any challenges encountered.
  - **Conclusion and Observations:** Key takeaways from the project, including any limitations of the analysis approach and suggestions for possible future works.
- All the source code for the implemented analysis.
- A presentation showcasing the project's findings and results. On the day of the presentation, you will have 10 minutes for the presentation, plus 5 minutes for questions.

Timeline:

- Projects will be presented on 9/12/2024 and 16/12/2024 during the lecture time slots.

  A Google Sheet for registering your time slot will be provided on Moodle.

App link:

- Click here to access the apps

Resources:

- FlowDroid paper: `https://orbilu.uni.lu/bitstream/10993/20223/1/far+14flowdroid.pdf`
- Android apps essentials: `https://developer.android.com/guide/components/fundamentals`

➠ If you have any questions, please get in touch with us at: **marco.alecci@uni.lu**.