Mobile Privacy Leakage Detection and Prevention

Saeed Ibrahim Saeed Alqahtani[1,2] *

[1]University of Surrey, UK [2]Taibah University, Saudi Arabia

Introduction

It has been shown that **mobile apps leak** different types of **information about users without their awareness**, e.g., device identifiers (IMEI, Device ID) , data collected by sensors (cameras, microphones, accelerometers, GPS devices, etc.), personal communication data (messages, contacts, browsing history) [1].

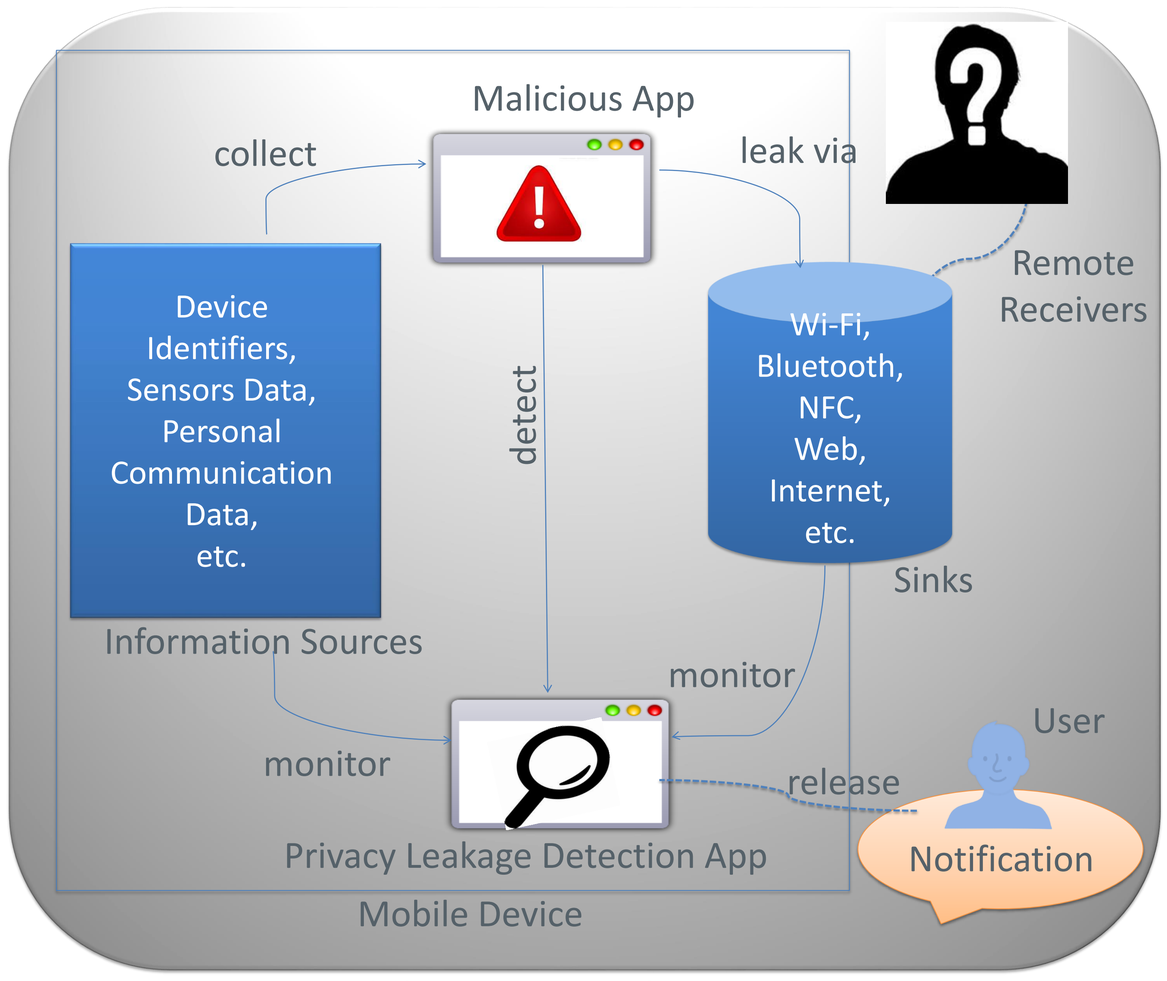
The main technical approach followed by mobile privacy leakage tools is to detect unauthorised and suspicious information flows from monitored information sources to sinks [1], where a "sink" is an interface allowing information to go out of the mobile device.

Identified Research Problems:

•Many mobile privacy leakage detection tools use a **limited and static** list of information sources.

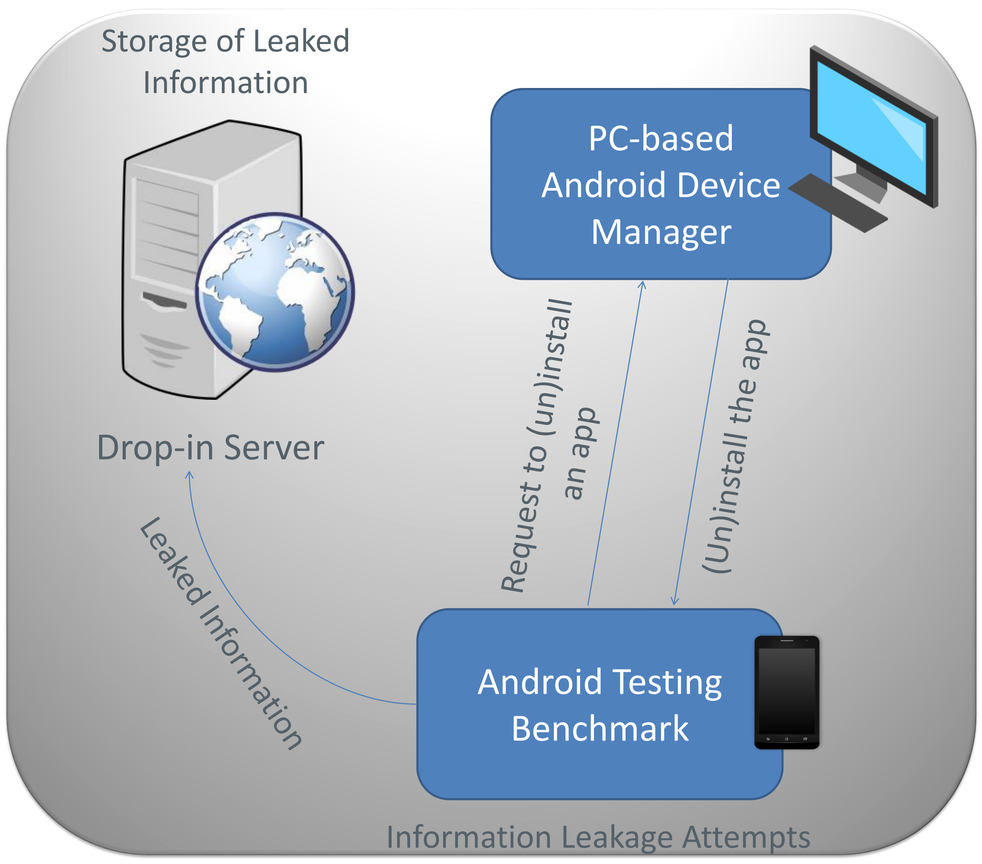
•Almost all mobile privacy leakage detection tools simply produce a notification for **every** detected leakage and leave further actions to end users who often feel annoyed / confused about the next step.

•Little work has been done on how leaked private information is actually used by leaking mobile apps and receivers of such information in real world [2].



Mobile Privacy Leakage Scenario

PhD Research Plan



Benchmarking System

Short-Term Goal

Developing a benchmarking system for Android devices which can be used to analyse privacy leakage detection apps in a **(semi-) automated** manner. Android devices are targeted due to the **openness** of the Android OS.

Benchmarking System Design

▪**An Android app** programmed to **simulate leakage** of different types of private information.
▪**A drop-in server receiving the leaked information** from the Android mobile app.
▪**A PC-based Android device manager** handling **automatic (un)installation** of each tested app during the testing process (which cannot be done by the Android app running inside the testing device due to Android security policies).
▪**A test profile creator** distributed between the Android app and the PC-based Android device manager for **defining the actual testing tasks**.

What Tools to Test?

Tools are collected from:
• Google Play and Google search
• Major third-party Android markets
• Cyber security product vendors and service providers (e.g. Anti-Virus vendors)
• Data leakage protection and Android forensics tools

163 collected so far, and more to be collected in future.

Medium-Term Goals

1. Extending Information Sources

This research plans to extend the currently static and limited private information sources to cover more sources in a dynamic manner (e.g. files that may store private information) using machine learning techniques.

2. Improving User Experience

This research aims to improve the user's overall experience with mobile privacy protection in general. Current thoughts include the following: a) developing "smarter" filters to show users fewer notifications and rank them in a more user-relevant manner; b) employing machine learning techniques to learn from users' feedback to notifications to optimise the above "smarter" filters; c) providing more useful tips to users for further actions against leakage.

Long-Term Goal

While our medium-term goals focus on the first two identified research problems more, which are largely passive approaches (detecting, notifying, and blocking), for the long term, this research plans to look at **active** approaches to attack the third identified research problem by introducing **forensic elements** e.g. honeypots and data watermarking technologies.

References

[1] M. Haris, H. Haddadi, and P. Hui, "Privacy leakage in mobile computing: Tools, methods, and characteristics," arXiv.org e-Print archive, arXiv:1410.4978v1, 2014
[2] W. Enck, "Defending users against smartphone apps: Techniques and future directions," in *Information Systems Security: 7th International Conference, ICISS 2011, Kolkata, India, December 15-19, 2011, Proceedings*, *Lecture Notes in Computer Science*, vol. 7093, pp. 49-70, Springer, 2011

* Supervised by Dr Shujun Li (principal) and Prof Anthony T.S. Ho (secondary).