


MONASH University
MONASH INFORMATION TECHNOLOGY

HUMANISE

# CHARACTERISING SENSOR LEAKS IN ANDROID APPS

Professor John Grundy, Dr Xiaoyu Sun,
Dr Xiao Chen and Professor Li Li

## At a glance

### Background

Mobile phone sensor misuse is one of the major causes of privacy leaks and security issues in Android applications.

### Goal

Regulate the use of mobile phone sensors to prevent malicious attackers from exploiting them.

### Strategies

- Design a prototype tool SEEKER (Sensor leak finder) that leverages static analysis to detect sensor leaks.
- Apply SEEKER to analyse Android apps on a larger scale.
- Demonstrate SEEKER's effectiveness in evaluating detecting sensor leaks.

## Key outcomes

### Tool feasibility and effectiveness

SEEKER proved capable of automatically detecting sensor leaks in Android apps, with malware apps presenting a higher risk of sensor leaks than benign ones.

### Characterised sensor leaks

The accelerometer leaked the most sensor data, with major sources being SensorManager#getDefaultSensor(int) and SensorEvent#values used to infer PIN numbers.

### Proven efficiency

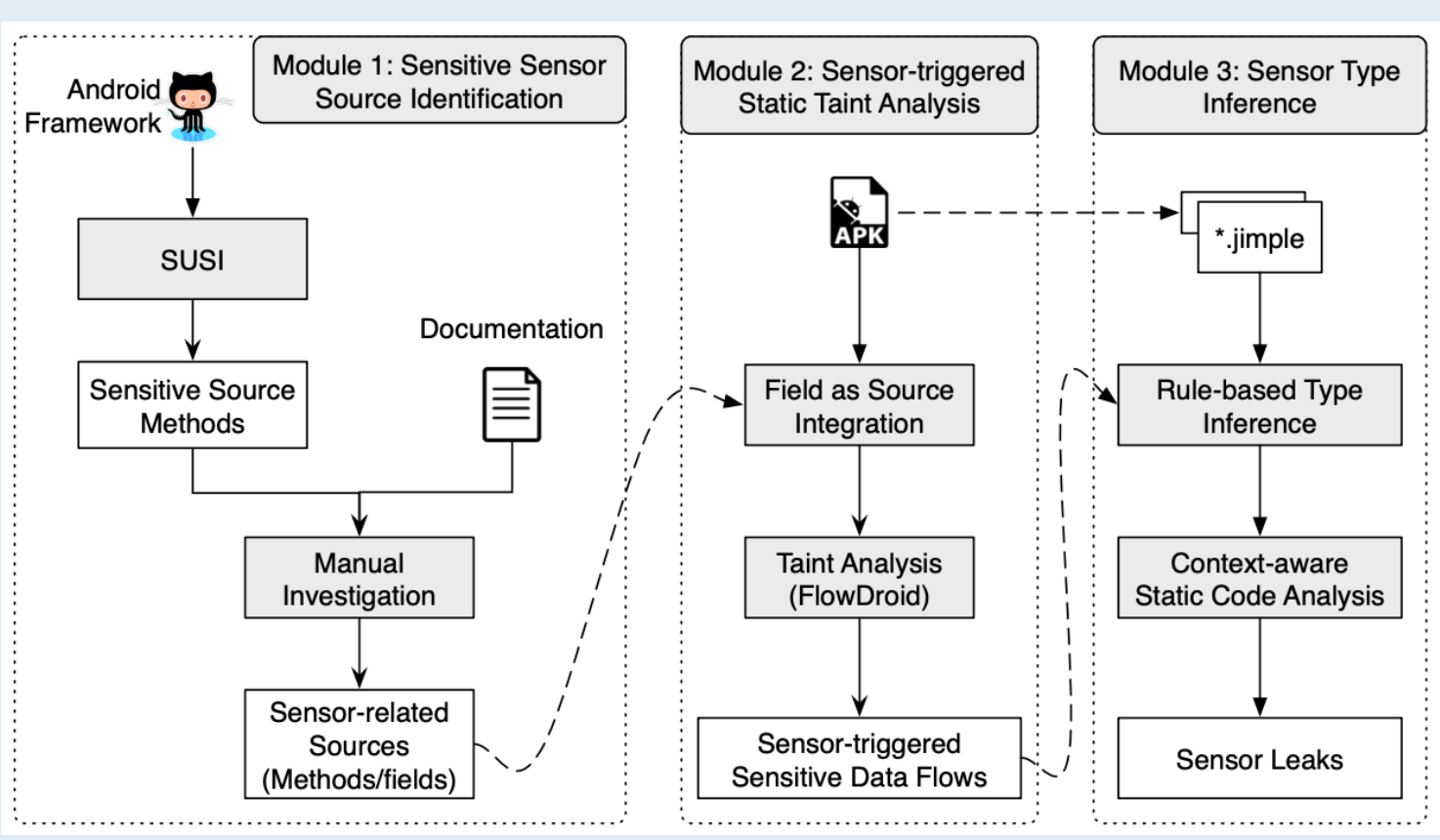
It took SEEKER an average of 177.09 seconds to detect sensor leaks in one app.

# How SEEKER works

The first module, Sensitive Sensor Source Identification, identifies sensor-related sources that access and obtain data.

The Sensor-triggered Static Taint Analysis module extends the state-of-the-art tool FlowDroid to facilitate sensor-related data leak detection.

The last module, Sensor Type Inference, identifies the types of sensors that are leaking information.




# Learn more

To discover more about this project,
contact Dr Xiaoyu Sun or scan the QR code.

# Acknowledgements

This project is funded by the Australian Research Council Laureate Fellowship FL190100035. We would like to acknowledge the participants who completed the survey to assist with our research.

**www.monash.edu/it/humanise-lab**

Australian Government
Australian Research Council