Semi-automated Discovery of Server-Based Information Oversharing Vulnerabilities in Android Applications

ISSTA '17

Title

1

Introduction

Introduction

SIFON

Server-based InFormation OvershariNg

```
tv0.setText("First Name:");
tv1.setText(p.firstName);
tv2.setText("Last Name:");
tv3.setText(p.lastName);
```

JSON representation

```
{"firstName": "Donald",
 "lastName": "Knuth",
 "email": "donald.k@spambox.us"}
```

Listing 1: JSON representation of a user profile.

Java Model

```
public class Profile {
  public String firstName;
  public String lastName;
  public String email; }
```

Deserialization

```
InputStream is = getProfileInputStream();
Reader r = new InputStreamReader(is);
Profile p = new Gson().fromJson(r,Profile.class);
```

2

System Overview

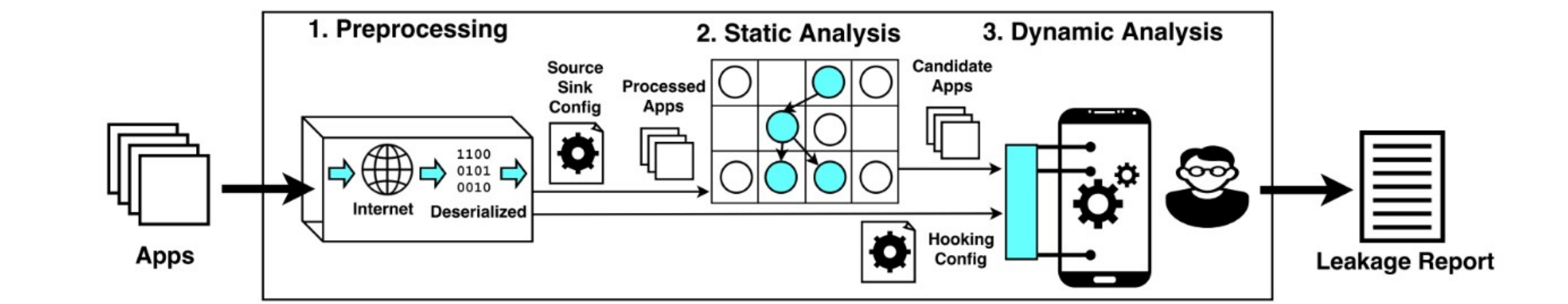
System Overview

Preprocessing

01

02

Static Analysis



03

Dynamic Analysis

3

Methodology

Preprocessing

INTERNET permission

Serialization library

Gson

Obfuscation

Signature matching

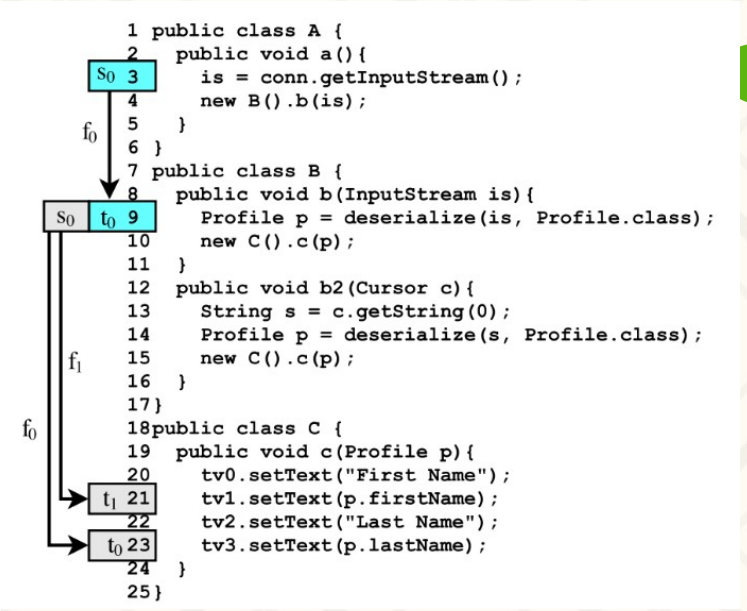
Static Analysis

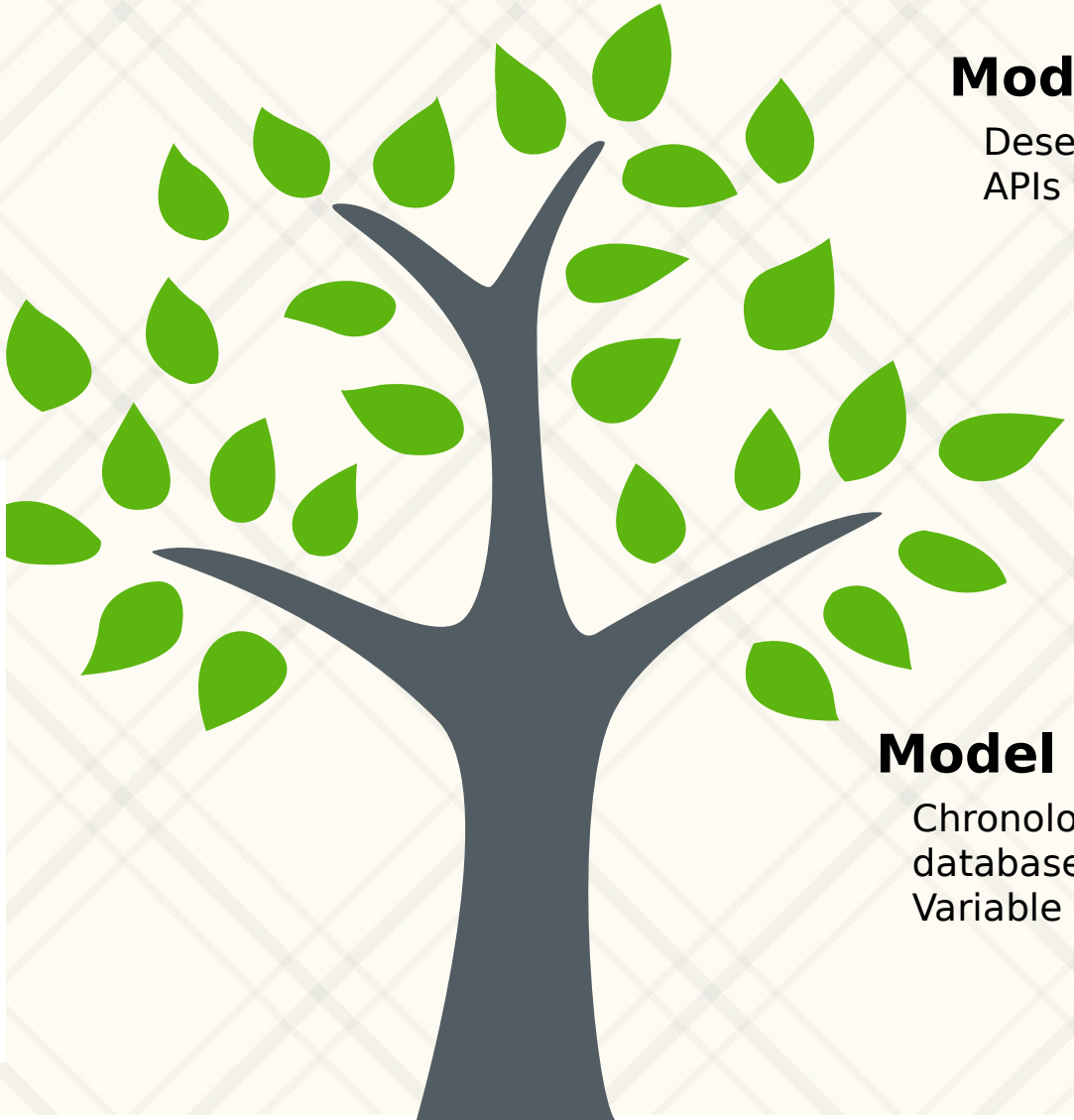
sCFG

flowdroid

Model Deserialization

Network API(sources)
Call sites of deserialization libraries(sinks)





Model Field Identification

Deserialization points(sources)
APIs that render text in UI (sinks)

Model Field Classification

Chronology of Data Breaches database
Variable name

Dynamic Analysis

Hooking

Xposed

Application seeding

Manually(user account creation)

UI Exploration

As a real user

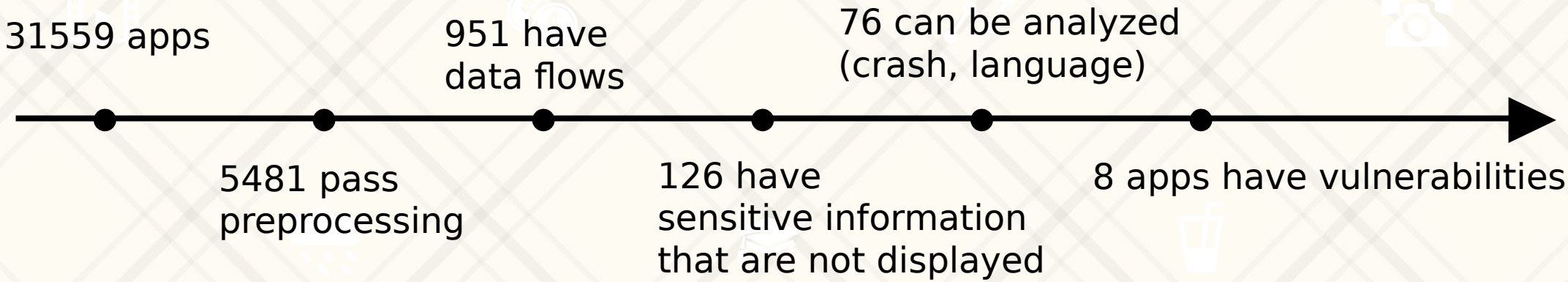
Vulnerability Confirmation

Data flows exist at run time

4

Evaluation

单击此处添加标题



Apps	Leaked Data	Number Installs
App A	first and last name, DOB, last action*, ZIP, gender*, user ID*, email, profile status	10,000 - 50,000
App B	email, home page, street, ZIP code, phone number	10,000 - 50,000
App C	Client OS*, email*, friend list*, user ID*, latitude, longitude	10,000 - 50,000
App D	latitude, longitude, last action	5,000 - 10,000
App E	Phone number	1000 - 5000
App F	userRelationID, latitude*, longitude*	500 - 1,000
App G	address, DOB, phone number, email*, deviceOS, Facebook ID, encrypted latitude, longitude, and password	100-500
App H	DOB, hashed password, last login, user type	100 - 500

5

Conclusion