Mobile Security Support for Android Developers

BSc Thesis – First Presentation

Dominik Briner

University of Bern (SCG), 15/01/2019
Outline

Android ICC Security Smells

Security Smell Detectors in Android Studio

More Security Support in Android Studio
Android ICC Security Smells

Android App Issues
Relevance

Android #1 mobile OS
*(market share > 85%)*

Personal devices
*(store a lot of sensitive data)*
GLOBAL MOBILE DATA GROWTH
TOTAL MONTHLY GLOBAL MOBILE DATA TRAFFIC (UPLOAD & DOWNLOAD), IN EXABYTES (BILLIONS OF GIGABYTES)

MONTHLY MOBILE DATA USED BY THE AVERAGE SMARTPHONE WORLDWIDE: 2.9GB

Android ICC Security

*Intent object*  →  Java object including ICC action to perform

*Intent filters*  →  Listeners for ICC requests

*Implicit intent*  →  User selects desired listener
ICC Security Threats

Denial of Service  Intent Spoofing  Intent Hijacking
Consequences

- Downtime
- Espionage / Blackmailing
- Data Leaks
Security Smell Detectors in Android Studio

Android Studio Security Smell Quickfixes
Security Smell Detection

IntelliJ platform

12 smells covered using Android Lint

Displays warning messages
```java
private String getSM(String id) {
    Uri.Builder urlBuilder = new Uri.Builder();
    urlBuilder.setAuthority("edu.ksu.cs.malicious.settings");
    urlBuilder.appendEncodedPath("/user/sms/");
    urlBuilder.appendPath(String.valueOf(id));

    Cursor cursor = getContentResolver().query(urlBuilder.build(), projection, null, selectionArgs, sortOrder);
    if (cursor != null && !cursor.moveToFirst()) {
        String str = cursor.getString(cursor.getColumnIndexOrThrow(Columns.CONTENT));
        return str;
    }
    return null;
}
```
Developers ignore warnings due to

Overwhelming information
Overwhelming complexity
Missing resources
Solution: Quickfixes

Quick & easy to apply

Powerful
Issue #1: Lack of context

Some fixes are not trivial

Require user input or can hardly be solved at all
Examples

Set `android:taskAffinity` to empty

Add missing `Context.revokeUriPermission()`

Where?

Input by user, add timer, just create method, ...
Issue #2: Implementation

Missing documentation

Integration with Android Lint
More Security Support in Android Studio

Existing Concepts & Novel Ideas
Computer Programming To Be Officially Renamed “Googling Stackoverflow”

Washington DC – The IEEE have produced a report today where they strongly recommend that from now on, the discipline of Computer Programming should be officially renamed to “Googling Stackoverflow”.

Evolution?

9 years of “progress”
Contrary perception

“IDEs are just glorified text editors”

vs

Embedded debugger, version control support, build tools, testing facilities, ...
Contrary perception

“IDEs are just glorified text editors”

vs

Embedded debugger, version control support, testing facilities, ...
The idea

Use of contextual knowledge

Customizable tool window

Separation of concern
(e.g. security, resilience, ...)

public boolean notNothing(String str) {
    return str.equals("Nothing");
}
Immediate benefits for developers

- Access to more relevant information
- Personal feedback
- Extensible

Proof-of-Concept available
Future Proposals

Vendor maintained topic datasets

Remote interaction with external “security professionals”

Live collaboration with team members on sensitive code
Next Steps

Progressing on *quickfixes* and *mock features*

Usability *tests*

Collecting *more feature ideas*

*Evaluation*
Summary

Quickfixes

Mitigating missing resources

Selection of approach is non-trivial

Context

An awful lot of ideas

How far can we go using the context?