

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

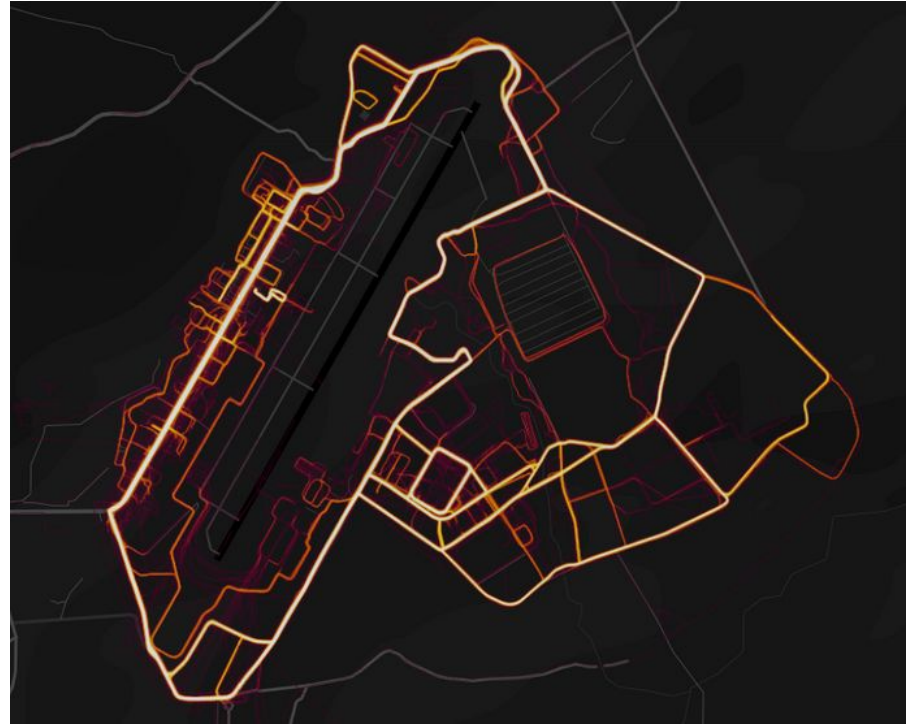
Android ICC Security Smells

Android App Issues

Relevance

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

Personal devices
(*store a lot of sensitive data*)



JAN
2018

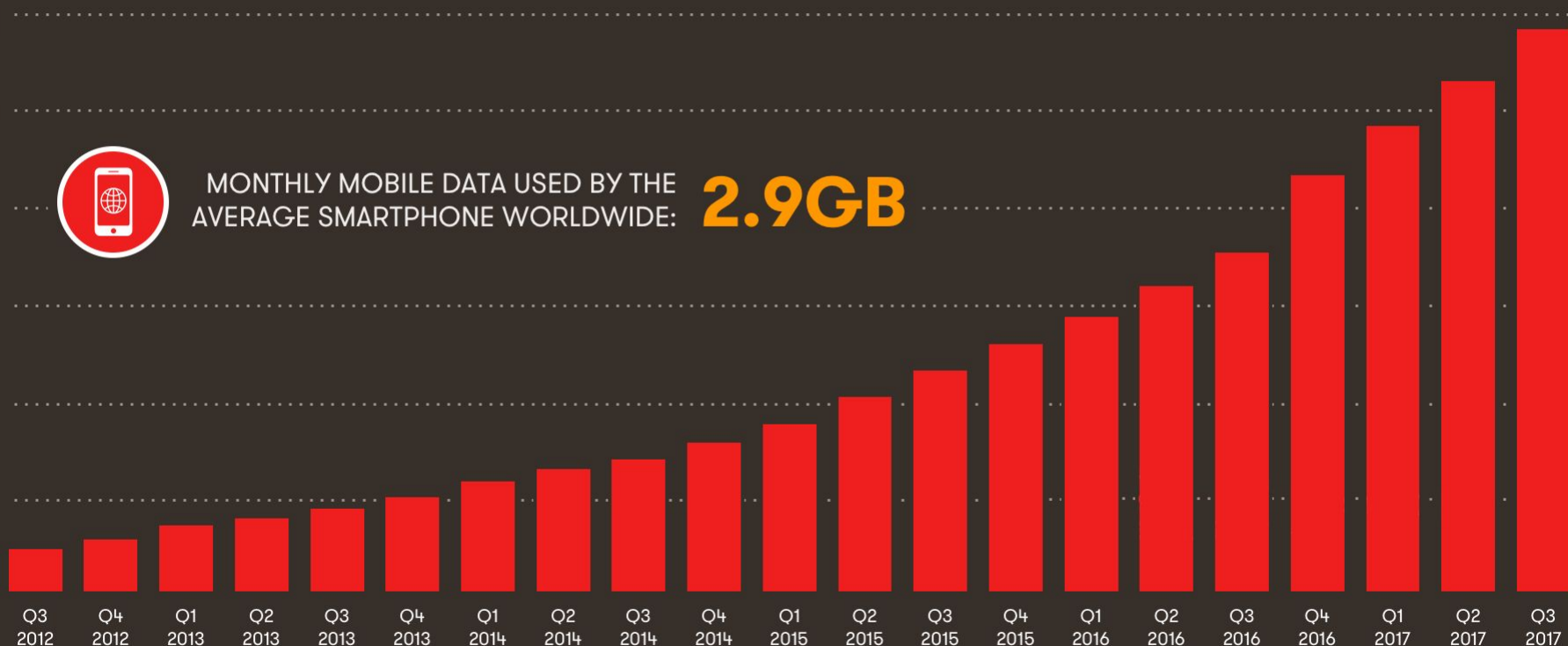
GLOBAL MOBILE DATA GROWTH

TOTAL MONTHLY GLOBAL MOBILE DATA TRAFFIC (UPLOAD & DOWNLOAD), IN EXABYTES (BILLIONS OF GIGABYTES)



MONTHLY MOBILE DATA USED BY THE
AVERAGE SMARTPHONE WORLDWIDE:

2.9GB



SOURCE: ERICSSON MOBILITY REPORT, NOVEMBER 2017.



Hootsuite™

we
are
social

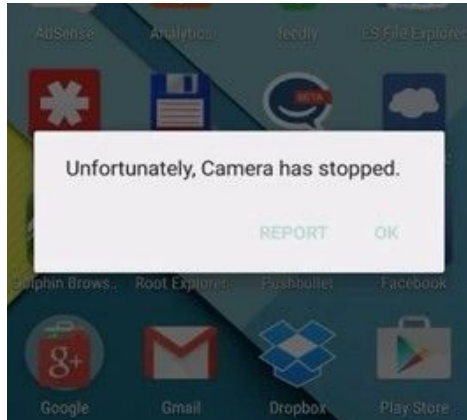
Android ICC Security

Intent object → Java object including ICC action to perform

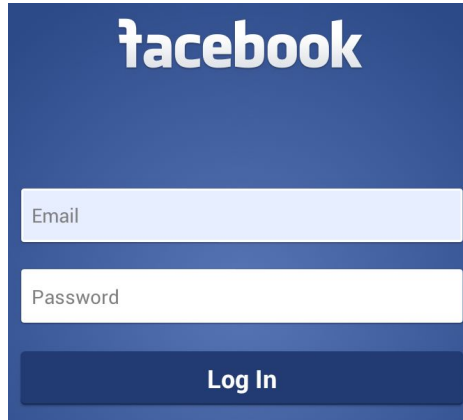
Intent filters → Listeners for ICC requests

Implicit intent → User selects desired listener

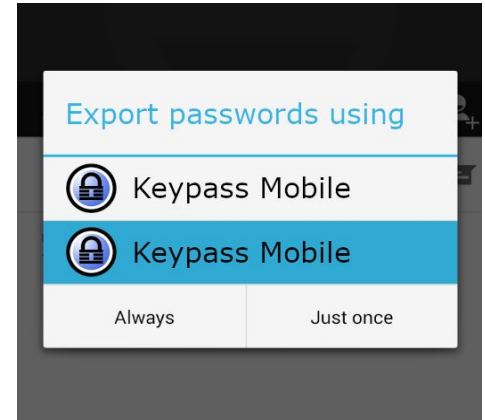
ICC Security Threats



Denial of Service



Intent Spoofing



Intent Hijacking

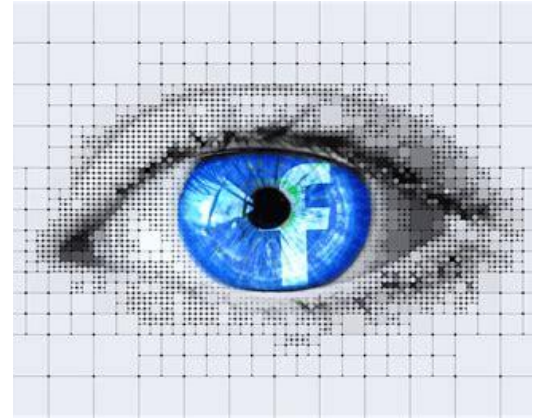
Consequences



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

Malicious [C:\git\4_Forks\android-app-vulnerability-benchmarks\ICC\InadequatePathPermission-InformationExposure-Lean\Malicious] - ...\app\src\main\java\edu\ksu\cs\malicious\MalActivity.java [app] - Android Studio

File Edit View Navigate Code Analyze Refactor Build Run Tools VCS Window Help Lint

Malicious > app > src > main > java > edu > ksu > cs > malicious > MalActivity

AndroidManifest.xml MalActivity.java

Project

app

manifests

AndroidManifest.xml

java

edu.ksu.cs.malicious

MalActivity

res

Gradle Scripts

37

String[] selectionArgs = new String[]{"1"};

38

Cursor cursor = getContentResolver().query(uri, projection: null, selection: null, selectionArgs, sortOrder: null);

39

if (cursor != null && cursor.moveToFirst()) {

40

TextView tv = (TextView) findViewById(R.id.ssnDisp);

41

tv.setText(cursor.getString(columnIndex: 1));

42

cursor.close();

43

}

44

}

45

}

46

@

47

private String getSSN(String id) {

48

Uri.Builder uribuilder = new Uri.Builder();

49

uribuilder.authority("edu.ksu.cs.benign.userdetails");

50

uribuilder.appendEncodedPath("/user/ssn");

51

uribuilder.scheme("content");

52

String[] selectionArgs = new String[]{id};

53

Cursor cursor = getContentResolver().query(uribuilder.build(), projection: null, selection: null, selectionArgs, sortOrder: null);

54

if (cursor != null && cursor.moveToFirst()) {

55

String str = cursor.getString(columnIndex: 1);

56

cursor.close();

57

return str;

58

}

59

return null;

60

}

61

}

62

MalActivity > getSSN()

Build Sync

Build: completed successfully at 14/01/2019 13:21

Run build C:\git\4_Forks\android-app-vulnerability-benchmarks\ICC\InadequatePathPermission-InformationExposure-Lean\Malicious

Load build

Configure build

Calculate task graph

Run tasks

7s 520ms

6s 330ms

42ms

1s 647ms

1s 755ms

2s 828ms

Device File Explorer

11

Event Log

51:38 CRLF UTF-8 Context: <no context>

Malicious [C:\git\4_Forks\android-app-vulnerability-benchmarks\ICC\InadequatePathPermissionExposure-Lean\Malicious] - ...app\src\main\AndroidManifest.xml [app] - Android Studio

FileEditViewNavigateCodeAnalyzeRefactorBuildRunToolsVCSWindowHelpLint

Malicious > app > src > main > AndroidManifest.xml

AndroidAndroidManifest.xmlMalActivity.java

Project

app

manifestsAndroidManifest.xml

java

edu.ksu.cs.malicious

MalActivity

res

Gradle Scripts

AndroidManifest.xml

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

<!-- <uses-permission

android:name="edu.ksu.cs.benign.permission.sensitive"

android:protectionLevel="normal" />-->

<uses-permission

android:name="edu.ksu.cs.benign.permission.generic"

android:protectionLevel="normal" />

application

android:allowBackup="false"

android:icon="@mipmap/ic_launcher"

android:label="Malicious"

android:supportsRtl="true"

android:theme="@style/AppTheme">

<activity android:name=".MalActivity">

<intent-filter>

<action android:name="android.intent.action.MAIN" />

<category android:name="android.intent.category.LAUNCHER" />

</intent-filter>

</activity>

</application>

</manifest>

manifest > application

TextMerged Manifest

Inspection Results: of 'Project Default' Profile on Project 'Malicious'

Android 6 warnings

Lint 6 warnings

Correctness 2 warnings

Internationalization 2 warnings

Security 1 warning

SM12: Common Task Affinity | Consider setting the task affinity of your app explicitly to an empty value 1 warning

AndroidManifest.xml 1 warning

SM12: Common Task Affinity | Consider setting the task affinity of your app explicitly to an empty value

Usability 1 warning

Java 1 warning

Suppress

android:theme="@style/AppTheme">

<activity android:name=".MalActivity">

<intent-filter>

<action android:name="android.intent.action.MAIN" />

<category android:name="android.intent.category.LAUNCHER" />

</intent-filter>

</activity>

</application>

</manifest>

Security Smell Inspection

Inspection Results

TODO

Logcat

Build

Terminal

Event Log

App is not indexable by Google Search; consider adding at least one Activity with an ACTION-VIEW intent filter. See issue explanation for more details. SM12: Common Task Affinity | Consider setting the task affinity of your app explicitly to a... 13:5 CRLF UTF-8 Context: <no context>

```












18         android:theme="@style/AppTheme">
19             <activity android:name=".MalActivity">
20                 <intent-filter>
21                     <action android:name="android.intent.action.MAIN" />
22
23                     <category android:name="android.intent.category.LAUNCHER" />
24                 </intent-filter>
25             </activity>
26         </application>
27
28     </manifest>

```

manifest > application

Text Merged Manifest

Inspection Results: of 'Project Default' Profile on Project 'Malicious' x

- 

Android 6 warnings
 - 
Lint 6 warnings
 - 
Correctness 2 warnings
 - 
Internationalization 2 warnings
 - 
Security 1 warning
 - 
SM12: Common Task Affinity | Consider setting the task affinity of your app explicitly to an empty value 1 warning
 - 

AndroidManifest.xml 1 warning
 - SM12: Common Task Affinity** | Consider setting the task affinity of your app explicitly to an empty value
 - 
Usability 1 warning
 - 
Java 1 warning

Suppress v

```


        android:theme="@style/AppTheme">
        <activity android:name=".MalActivity">
            <intent-filter>
                <action android:name="android.intent.action.MAIN" />

                <category android:name="android.intent.category.LAUNCHER" />
            </intent-filter>
        </activity>
    </application>

</manifest>

```

Security Smell Inspection

 Inspection Results

 TODO

 Logcat

 Build

 Terminal

13

App is not indexable by Google Search; consider adding at least one Activity with an ACTION-VIEW intent filter. See issue explanation for more details. SM12: Common Task Affinity | Consider

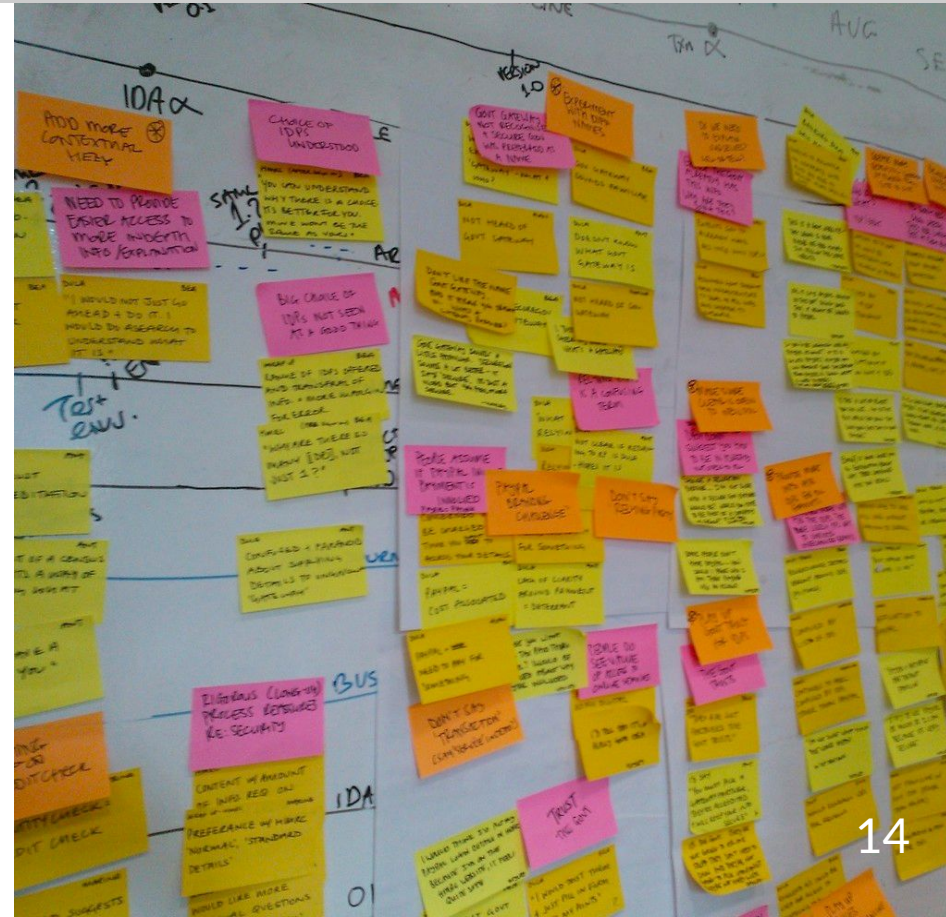
Developers ignore

warnings due to

Overwhelming information

Overwhelming complexity

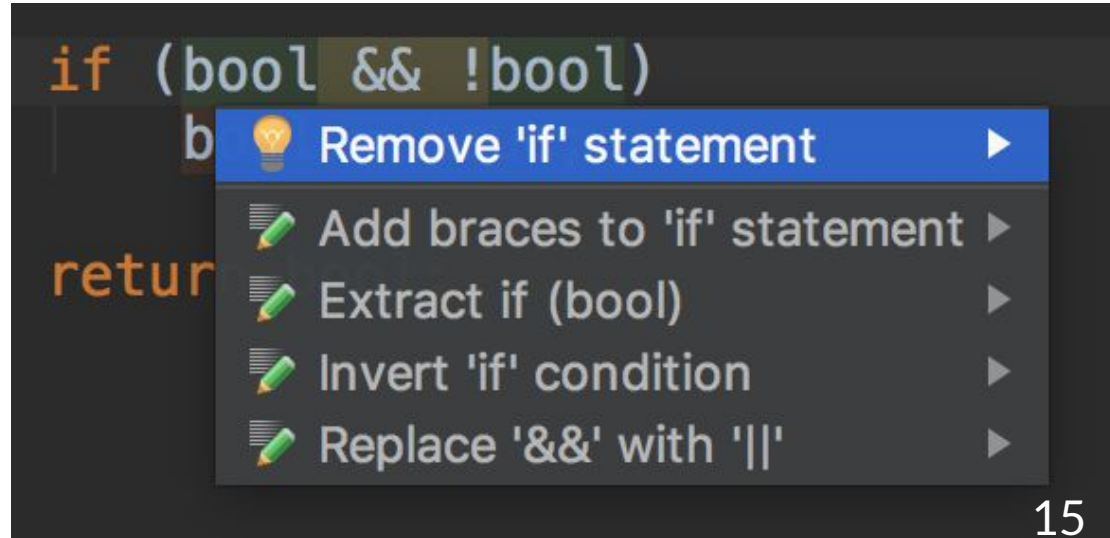
Missing resources



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”

101k
SHARES



Facebook

101k



Twitter



Google+

0



LinkedIn

0



Reddit

0

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”



```
command.process.processingFinished=Bylo úspěšně zpracováno {0} záznamů.  
  
feedListing.1.title=Newsfeed  
feedListing.eventBrowser.dateCreated=Datum vytvoření  
feedListing.eventBrowser.userName=Událost vyvolal  
feedListing.eventBrowser.idAggregatedTarget=Id cílového objektu  
feedListing.eventBrowser.targetType=Typ cílového objektu  
feedListing.eventBrowser.operationType=Typ provedené operace  
feedListing.eventBrowser.dataType=Kontener dat  
feedListing.show.title=Detail  
  
feedDetail.1.title=Detail záznamu v newsfeedu  
feedDetail.dateCreated.title=Datum vytvoření  
feedDetail.userName.title=Událost vyvolal  
feedDetail.idAggregatedTarget.title=Id cílového objektu  
feedDetail.targetType.title=Typ cílového objektu  
feedDetail.operationType.title=Typ provedené operace  
feedDetail.dataType.title=Kontener dat  
feedDetail.jsonData.title=Data
```

year 2010

```
@RequestMapping(value = "/api/users", method = RequestMethod.GET)  
public  
@ResponseBody  
String listUsersJson(ModelMap model) throws JSONException {  
    JSONArray userArray = new JSONArray();  
    for (User user : userRepository.findAll()) {  
        JSONObject userJSON = new JSONObject();  
        userJSON.put("id", user.getId());  
        userJSON.put("firstName", user.getFirstName());  
        userJSON.put("lastName", user.getLastName());  
        userJSON.put("email", user.getEmail());  
        userArray.put(userJSON);  
    }  
    return userArray.toString();  
}  
  
@RequestMapping(value = "/add", method = RequestMethod.POST)  
public String addUser(@ModelAttribute("user") User user,  
    BindingResult result) {  
    userRepository.save(user);  
    return "redirect:/";  
}  
  
@RequestMapping("/delete/{userId}")  
public String deleteUser(@PathVariable("userId") Long userId) {  
    userRepository.delete(userRepository.findOne(userId));  
    return "redirect:/";  
}
```

year 2019

Contrary perception

“IDEs are just glorified text editors”

vs

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

Contrary perception

“IDEs are just glorified

vs

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

**DOESN'T
MATTER!**

The idea

Use of contextual knowledge

Customizable tool window

Separation of concern

(e.g. security, resilience, ...)


```
40  public boolean notNothing(String str) {  
41      return str.equals("Nothing");  
42  }
```

Main > notNothing()

Dynamic Infos Security



There are no known security issues for "String.equals()".

Refresh



6: TODO



Terminal

Dynamic Infos



Event Log

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?