Detecting Android ICC Security Smells

BSc Thesis - Presentation #2

Patrick Frischknecht

29.05.2018

SCG UniBe

Relevance of Android Security

Android smartphone market share > 85%

Used for sensitive applications (e-banking, healthcare, etc.)

Ambitions

Easy to use JIT feedback tool

Detection of common ICC security smells

Evaluation on real world applications

Android Lint

```
public class CustomWebViewClient extends WebViewClient {

    @Override
    public void onReceivedSslError(WebView view, final SslErr
        handler.proceed();
```

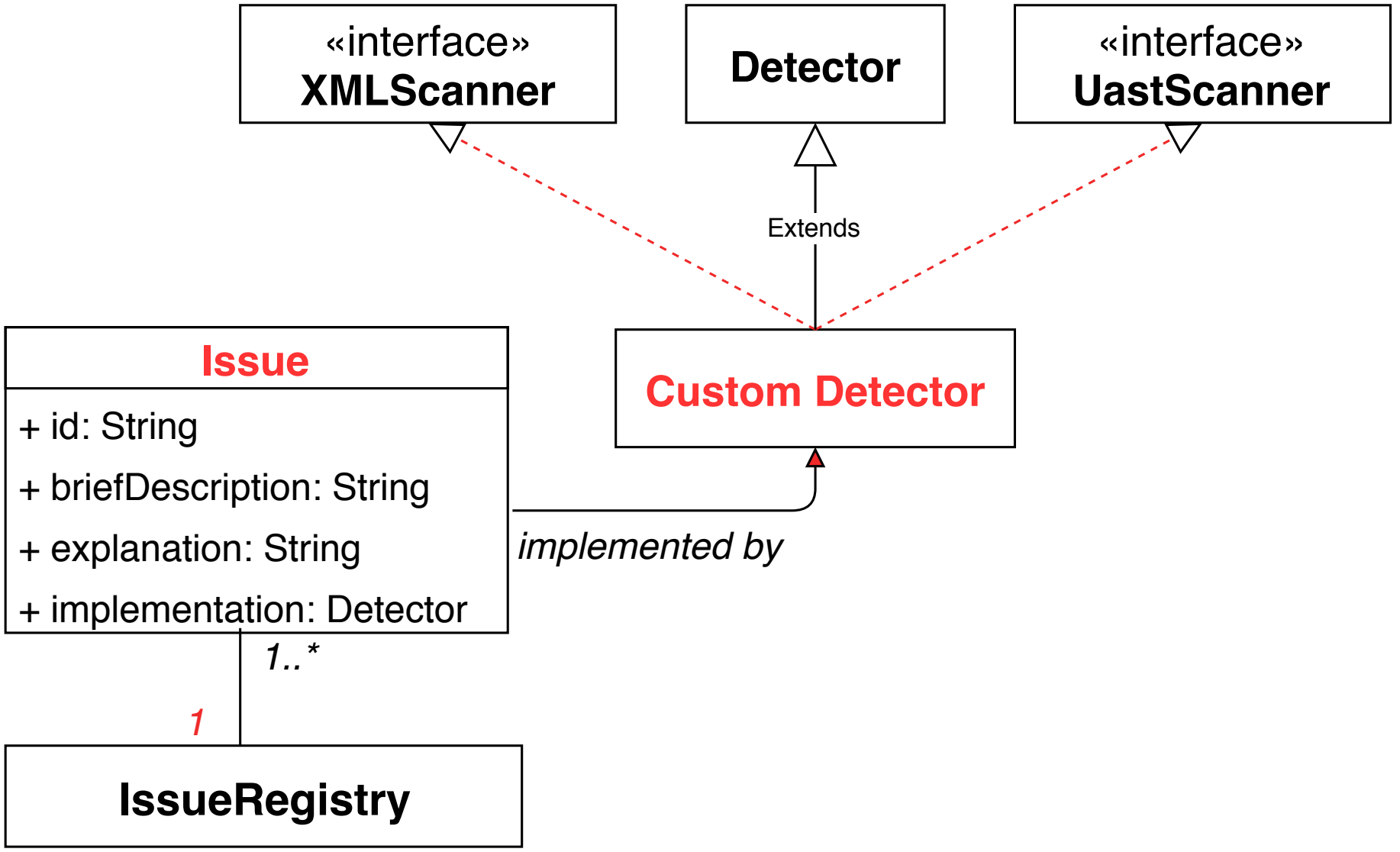
onReceivedSslError which always proceeds more... (Strg+F1)

Static JIT analysis framework

Integrated into Android Studio

Foundation of our extension

Android Lint Architecture



Detected ICC-Smells

Persisted Dynamic Permission	Custom Scheme Channel	Incorrect Protection Level
Unauthorized Intent	Sticky Broadcast	Slack WebViewClient
Broken Service Permission	Insecure Path Permission	Broken Path Permission Precedence
Unprotected Broadcast Receiver	Implicit Pending Intent	Common Task Affinity

Android ICC Overview

Intent: Message object

Activity: Main user interface component

Service: Handles background tasks

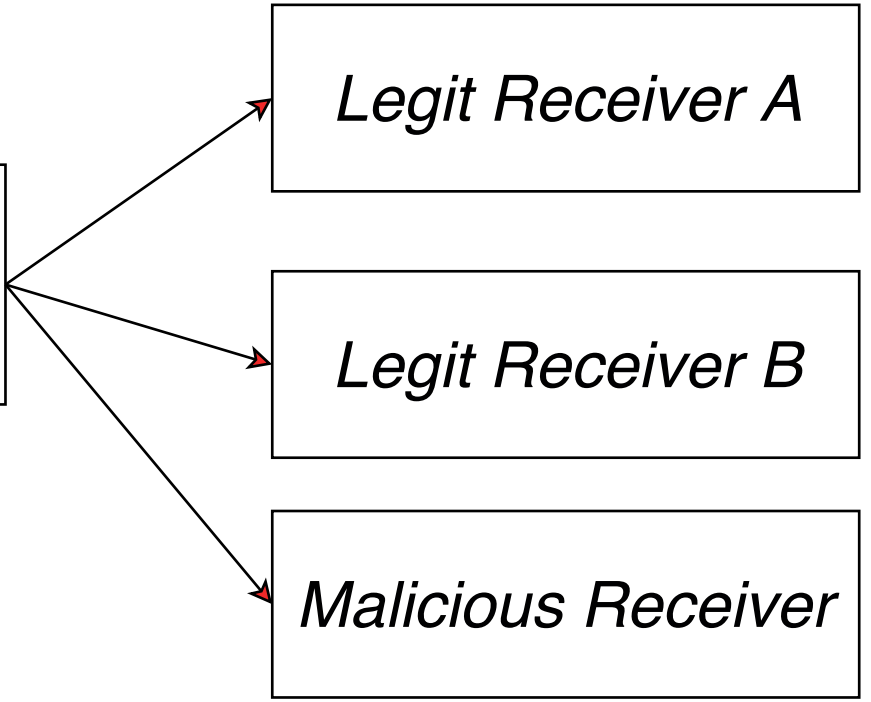
BroadcastReceiver: Reacts on system or app events

Unauthorized Intent

Implicit Intent
(Broadcast)

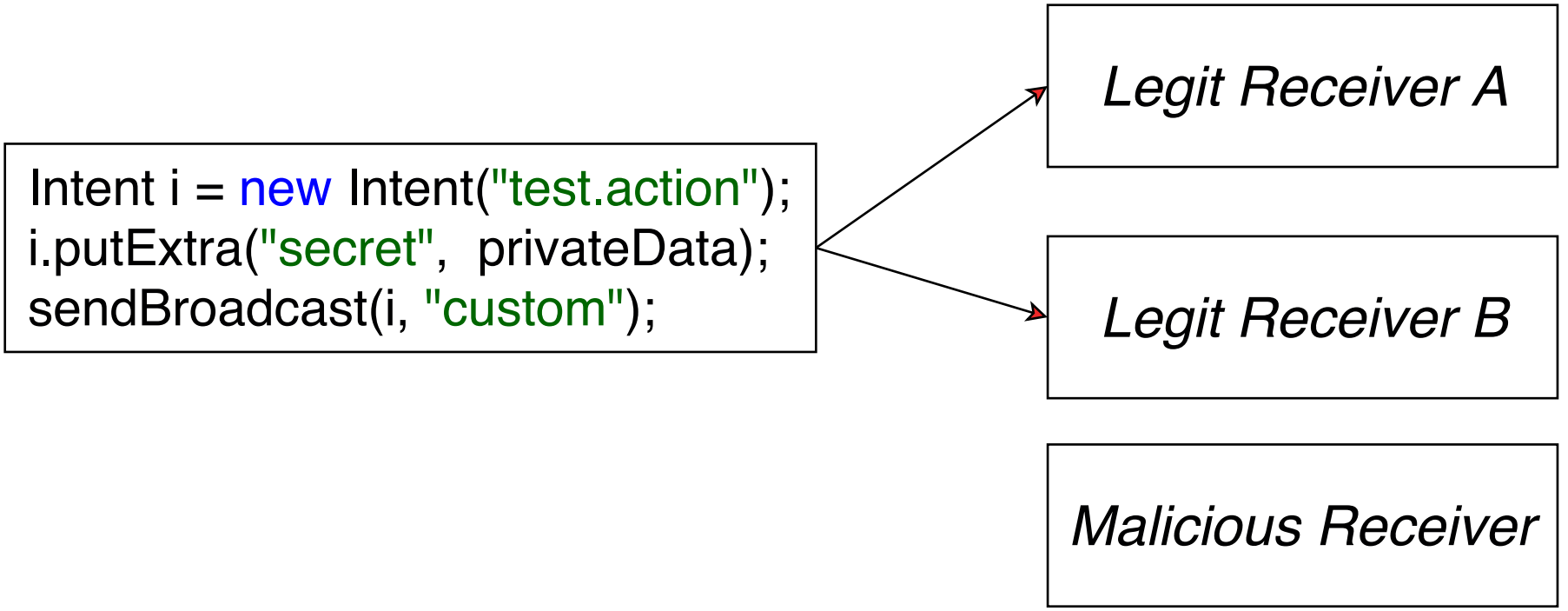
Received by every *matching receiver*

```
Intent i = new Intent("test.action");
i.putExtra("secret",  privateData);
sendBroadcast(i);
```



Mitigation

Receiver requires "custom" *permission*



Demo

Demo 1: Unauthorized Intent

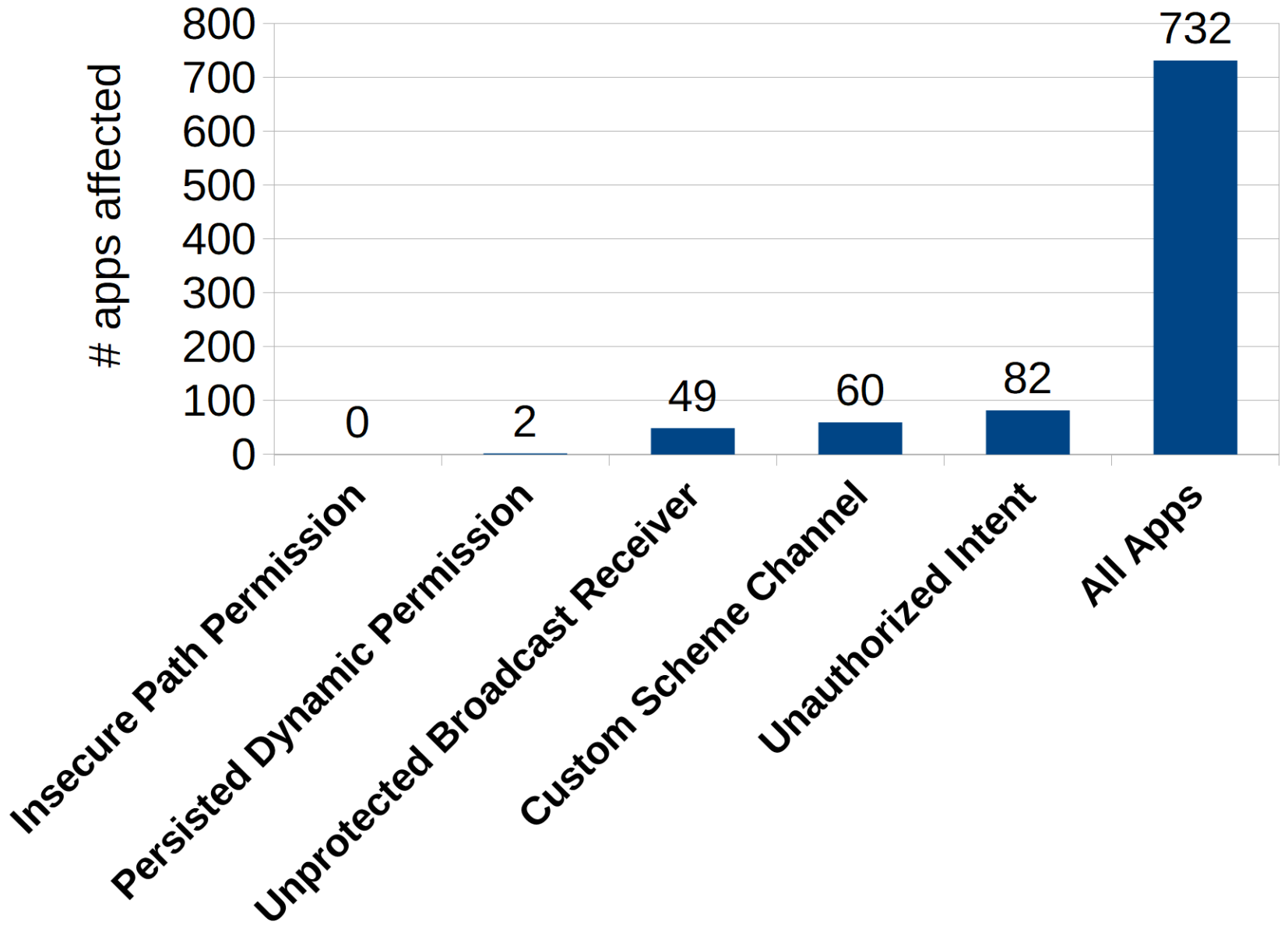
Evaluation

~700/100 apps analyzed
in batch / manual mode

Fixed occuring crashes and improved detection

Studied smell prevalence and distribution

Smell Prevalence



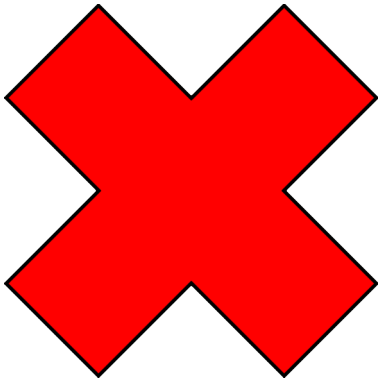
Lessons Learned

Android Lint

Easy to extend effectively
(Documentation sometimes bad)

Lessons Learned

```
Intent intent = new Intent(SHOW_PROGRESS);
intent.putExtra("show", show);
intent.putExtra("recording", recording);
intent.putExtra("sec", sec);
intent.putExtra("phone", phone);
context.sendBroadcast(intent);
```



Wrong implementation of in-app communication (Intra-app communication rare, mostly opening browser)

Future Work

Quickfixes

Taint Analysis for Android Lint

Usability Study

Summary

Android Lint

ICC Security Smells

Demo

Evaluation

Lessons Learned

Future Work