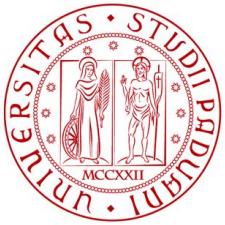
Mobile Security

Università degli studi di Padova



UNIVERSITÀ DEGLI STUDI DI PADOVA

SPRITZ SECURITY & PRIVACY RESEARCH GROUP

DIPARTIMENTO MATEMATICA

Overview

- Introduction
- FlowDroid
- Practical Demo

Introduction - Taint Analysis

Information flow analysis → we analyze the flow of information inside the app

Can be used to track the creation and use of “tainted” data

- Sensitive data
- Dangerous data

Smarter than the static analysis performed by MobSF

Taint Analysis - Sources and Sinks

We define Sources and Sinks

Source → Taints the data
Sink → Uses the tainted data

Taint analysis finds connections between sources and sinks

Taint Analysis - Taint propagation

Some operations may propagate the taint

For example String concatenation → the concatenated string contains the tainted data

Taint Analysis - example


```
Intent i = new Intent();
String tainted = source();
i.putExtra("data", tainted);
sink(i);
```

Taint Analysis - example


```
Intent i = new Intent();
String tainted = source();
i.putExtra("data", tainted);
sink(i);
```

`source()` creates the taint

Taint Analysis - example


```
Intent i = new Intent();
String tainted = source();
i.putExtra("data", tainted);
sink(i);
```

`i` now is tainted!

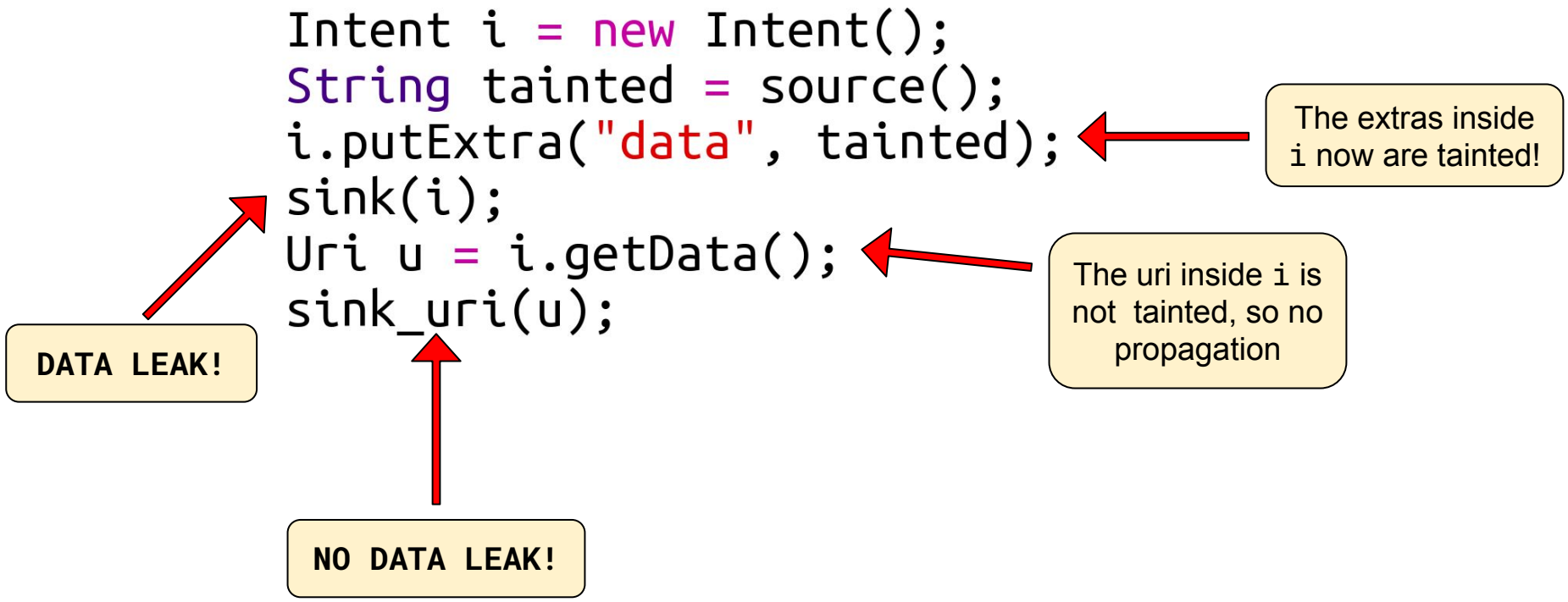
Taint Analysis - example


```
Intent i = new Intent();
String tainted = source();
i.putExtra("data", tainted);
sink(i);
```

i now is tainted!

DATA LEAK!

EXTRA: Field Taint Propagation



FlowDroid

Static taint analysis tool for Android

Analyzes compiled apks → acts at the bytecode level

Widely used in academia as well as industry

Can be used as a library or as a standalone tool

FlowDroid - command line interface

Needs the android.jar file

Uses a txt configuration with the list of sources and sinks

Demo time!

Conclusion

We talked about taint analysis and saw how it can be used to detect different kinds of vulnerabilities

- Data leaks
- SQL injections

FlowDroid CLI can be used for most cases → The library is more flexible, so it should be used for more complex cases