Static Analysis for Android GDPR Compliance Assurance

Mugdha Khedkar *(Heinz Nixdorf Institute, Paderborn University)*

mugdha.khedkar@upb.de @KhedkarMugdha

Problem

- Android apps collect and process personal data.
- Privacy by Design [1] and GDPR [2] need app developers to use state-of-the-art technical measures to protect their users' privacy.
- App developers may need assistance in writing privacy-aware code.

Observations

Privacy Disclosure

- A recent study by Mozilla [3] has revealed discrepancies between the information disclosed in Google Play's data safety section and Android app's privacy policies.

Tool Support

- Tools that bridge the legal and technical aspects of data protection are required.
- Such tools seek to help app developers reason about data protection.
- They can also assist GDPR auditors in conducting *source code audits.*

Static Analysis

- Checks the whole source code before execution.
- Widely used to ensure "Security by Design".
- Can potentially be used for ensuring data protection in Android apps.

Research Questions

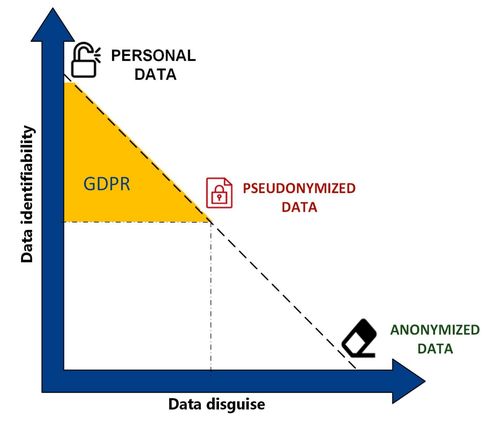
RQ1 How can we bridge the gap between legal privacy statements and the technical measures Android apps use for data protection?

RQ2 Which static analysis methods can be used to diagnose and explain data protection issues?

RQ3 To what extent can static analysis aid privacy-aware Android app development and auditing?

Challenges

Data	Category
Passport no.	Directly identifiable!!
Password	Access data
Pincode	Indirectly identifiable



1. ***Classifying input data***
2. ***Detecting data disguise***
3. ***Examining data manipulation***
4. ***Displaying analysis results***

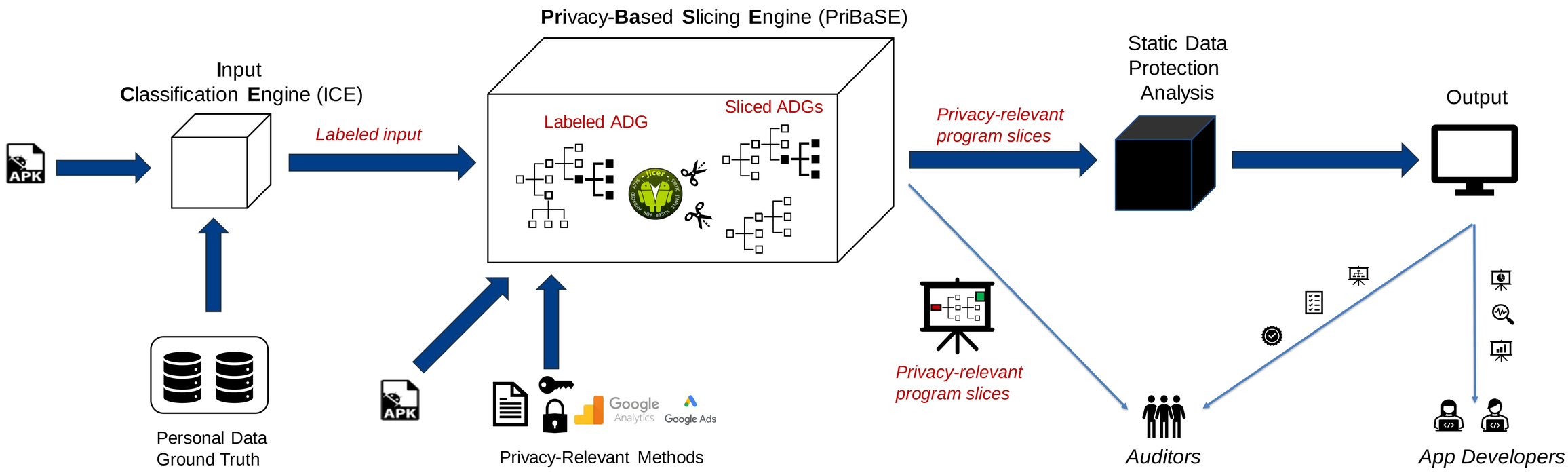
Proposed Workflow

Design an ***Input Classification Engine*** which labels sources of personal data in an Android app.

Extend Jicer [4] to label and slice the Application Dependence Graph (ADG) and represent flow of personal data. ***(RQ1)***

Implement a static analysis approach which examines personal data manipulation. ***(RQ2)***

Display results and evaluate analysis on Android apps. ***(RQ3)***



[1] Ann Cavoukian et al. 2009. Privacy by design: The 7 foundational principles. Information and privacy commissioner of Ontario, Canada 5 (2009), 12

[2] https://eur-lex.europa.eu/legal-content/ EN/TXT/PDF/uri=CELEX:32016R0679

[3] https://foundation.mozilla.org/en/campaigns/googles-data-safety-labels/

[4] F. Pauck and H. Wehrheim, "Jicer: Simplifying Cooperative Android App Analysis Tasks," *2021 IEEE 21st International Working Conference on Source Code Analysis and Manipulation (SCAM)*, Luxembourg, 2021, pp. 187-197, doi: 10.1109/SCAM52516.2021.00031.

Fill this short survey to help us with our research!!!