CERIAS

The Center for Education and Research in Information Assurance and Security

Privacy-Enhancing Features of IdentiDroid

Daniele Midi, Oyindamola Oluwatimi, Bilal Shebaro, Elisa Bertino

Problem and Motivations

Many privacy concerns for smartphones users
Identity, location, movement, habits, etc...

Anonymous communication technologies (Onion routers such as Tor, Secure VPN services such as Hotspot Shield, and more) can help... But are users *really* anonymous?

Applications may still release real information without user knowledge:

Re-identification of the user and/or device
Through Device ID, MAC addresses, ... or even Accounts, Contacts, Location ...

IP address hiding and secure communication channels are not enough

The ***least privilege*** *principle* is not enough: apps store self-identifying information

Motivating example

Using Tor on Android	Tor is doing its job...	User is still re-identified
Pandora accesses: Device ID, Contacts Angry Birds accesses: Location, Device ID	... transferring all this data anonymously!	Tor is not enough to fully protect the user's privacy.

Requirements

1. Applications should not be able to **bypass** restrictions enforced by the solution
2. No modification of application's **source code** should be needed
3. Anonymity restrictions should be fully **customizable per application**
4. The approach should not cause **significant delays** in the device functionality

Sensitive Data and Permissions

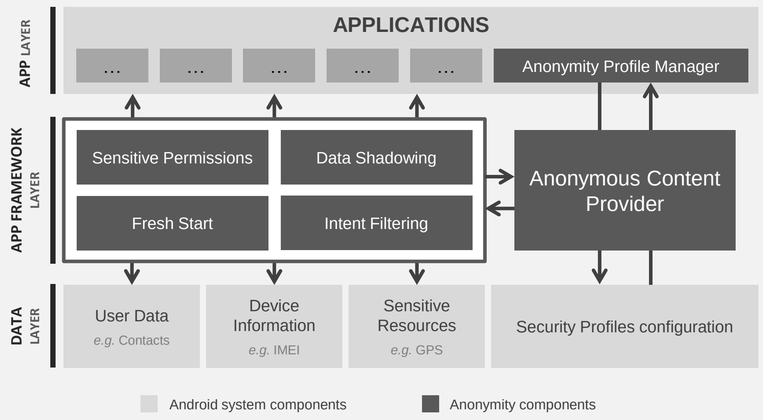
System Information
It consists of all the information concerning the system state and identity.
- Android_ID
- IMEI or CDM or ESN
- Current Cell Location
- Phone Number
- IP Address

User Data
It consists of common data generated by the user, such as contacts and SMSs.
- Contacts
- Photo Albums
- SMS
- Bookmarks/History

Resources
It consists of resources provided by the device, such as camera and GPS.
- Camera
- Location
- WiFi MAC Address

Application Data
It consists of the data stored and managed autonomously by the applications.
- Files (read/write file storage)

ARCHITECTURE AND COMPONENTS



A · Data Shadowing Manager

Supports the user in choosing the identifying information that needs to be hidden from selected apps.

Randomizes returned data and resources.

Conceals the actual information about the user and/or device.

B · Sensitive Permission Manager

Controls the access of apps to sensitive permissions by dynamic revocation at runtime.

Prevents apps from accessing identifying information during an anonymous session.

Keeps permissions available during non-anonymous sessions.

Fresh Start feature

Part of both solutions.

Prevents apps from leaving any identifying information or traces within their own data storage.

Apps appear as running on a device for the first time.
Existing app data can't be used to identify the device or the user.

Intent Filtering feature

Part of both solutions.

Manages messages exchanged between apps, to block the identifying data sharing.

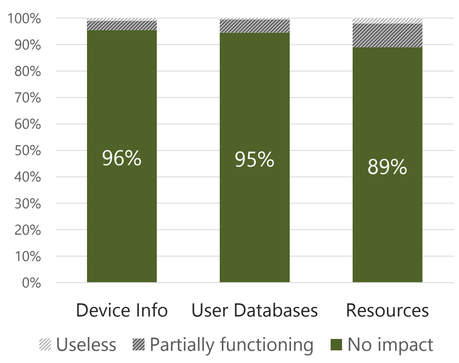
Prevents colluding apps from circumventing anonymity through message exchanges.

IdentiDroid Profile Manager

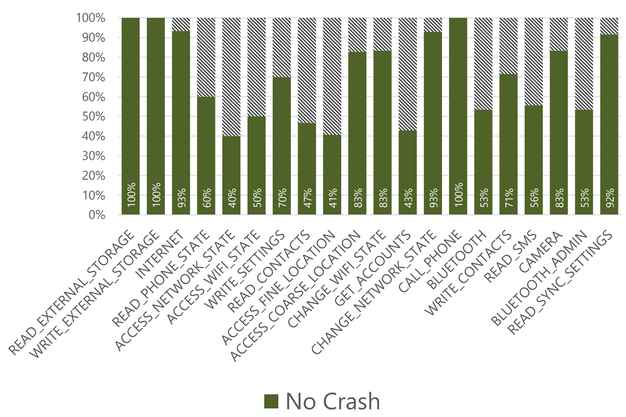
Tool for configuring *profiles*, sets of customized anonymity configurations for every installed Android application.

Experimental Analysis

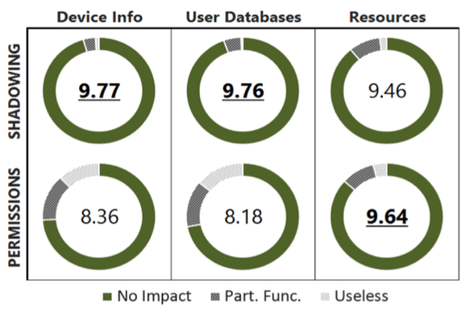
Impact of Data Shadowing on Apps



Impact of Permission Revoking on Apps



Shadowing vs. Permission Mgmt.



Conclusions and Future Work

Anonymous networks on smartphones are not enough.

Applications aren't ready to be anonymous.

IdentiDroid is necessary for anonymity, security and privacy.

Combine the permission and shadowing solutions for better trade-off.

WE PLAN TO:

- Introduce **guidelines** on how to build applications that can effectively function anonymously.
- Investigate IdentiDroid's effectiveness against applications that make use of **native libraries**.
- Study vulnerabilities in applications that have **unprotected APIs**.

CERIAS

PURDUE UNIVERSITY