Guiding App Developers on Privacy and Security Design Matters

Majid Hatamian
Chair of Mobile Business & Multilateral Security
Goethe University Frankfurt
majid.hatamian@m-chair.de
www.hatamian.net

12th June 2019 – Rome, Italy
IPEN Workshop 2019

mobile business

Outline

1. Introduction
2. App Developers Guide
3. Summary

Outline

1. Introduction
2. App Developers Guide
3. Summary

Did app privacy improve after GDPR?

Nurul Momen, Majid Hatamian (*Member, IEEE*), Lothar Fritsch

Abstract— What are the effects of the GDPR on consumer apps? This article presents an analysis of app behavior before and after the regulatory change in data protection in Europe. Based on long-term data collection, we present differences in app permission use and expressed user concerns and discuss their implications. In May 2018, the General Data Protection Regulation (GDPR) changed the data protection obligations of the information industry with European Union customers substantially. One should expect to find changes in code, program behavior and data collection activities. To investigate this expectation, we analyzed data about Android apps' request and use of permissions to access sensitive group of data on smartphones, and collected user reviews. Our data shows an overall reduction of both permissions used and of expressed user concern. However, in some areas apps have increased access or user complaints while in addition, many apps carry with them several unused access privileges.

Index Terms— Apps, data protection, GDPR, information privacy, survey,

1 Introduction

In May 2018, stronger regulation of the processing of personal data became law in the European Union, known as the General Data Protection Regulation (GDPR) [1]. The expected effect of the regulation was better protection of personal data, increased transparency of collection and processing, and stronger intervention rights of data subjects, with some authors claiming that GDPR will change the world, or at least that of data protection regulation [2]. The GDPR had a two-year (2016–2018) implementation period that followed four years of preparation. Now, in January 2019, three quarters of a year have passed since the implementation of GDPR.

Has GDPR had an effect on consumer software, then? Has the world of code changed, too? Did the GDPR have a measurable effect on mobile apps behavior? How should such a change in behavior be measured?

In our study, we decided to use two indicators for measurement: Android dangerous permission privileges and sources. We monitored app permission access request data in March 2017. To compare, we installed a subset of the post-GDPR version of the respective apps in December 2018 and ran a one-week data collection campaign. The data collection was done with the A-ware data capture app described in [3], [4]. The data is stored in an on-line collection database [5].

Figure 2 shows how we organized the collection of three different types of data from the Google Play server, from the app manifest and from observing apps at run time.

Permissions are Android's access control mechanism that regulates an app's access to various system resources. To retrieve data protected by dangerous permissions, the app code contains a declaration of the permissions requested by the app programmers in its manifesto. Upon the apps' first presentation to the operating system, the user of the device is prompted to confirm the app's permission request. If the user consents, the app stores the

Introduction
Problem Definition

- Users are more concerned

- Apps are still greedy

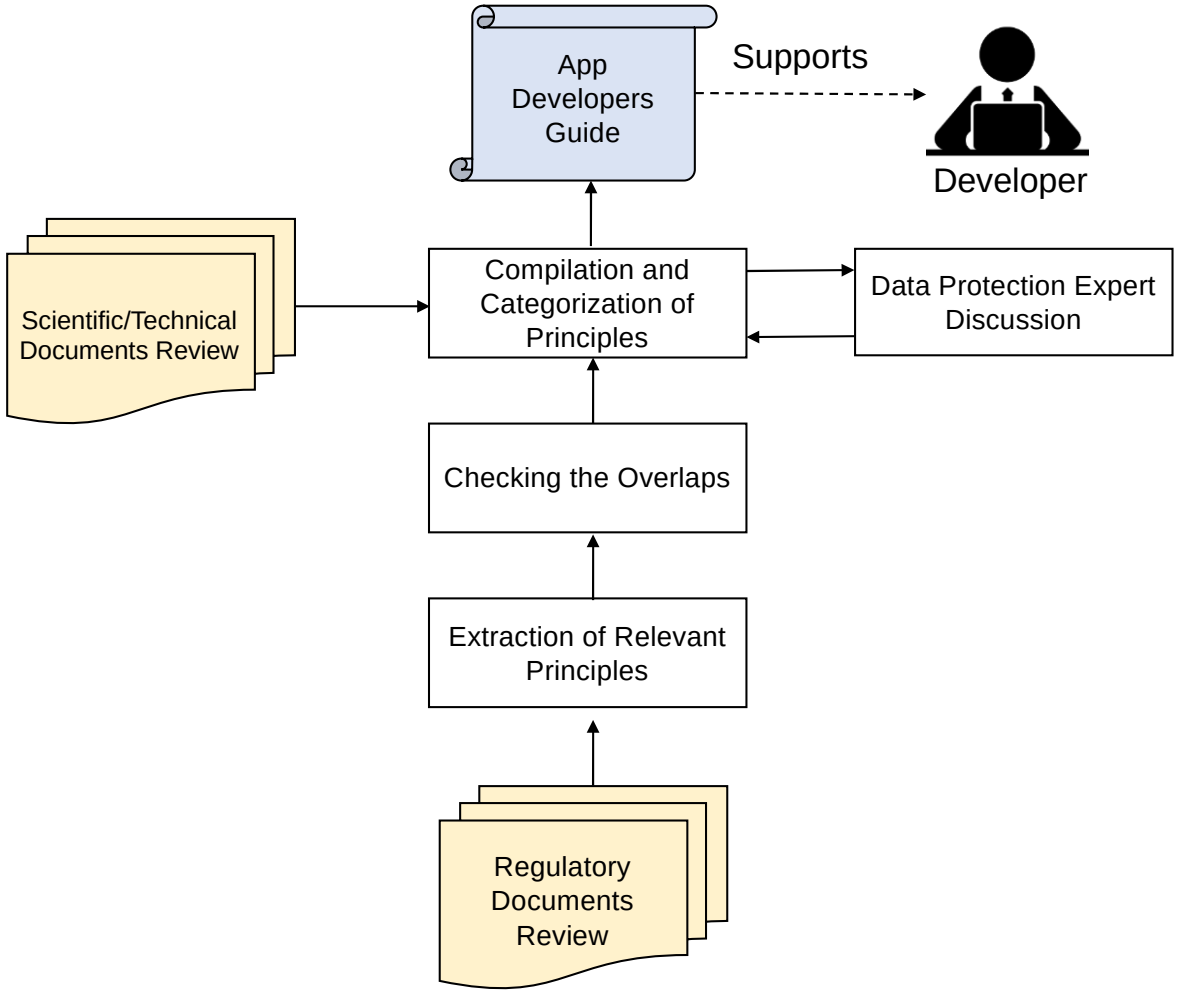
Outline

1. Introduction
2. App Developers Guide
3. Summary

App Developers Guide

- National and international bodies
- Legal and technical documents
- Institutes and authorities
- Not only *what* to do, but also *how* to do it

App Developers Guide



App Developers Guide

Privacy & Security Design Principles Catalog

- Purpose limitation & Data minimization
- Unlinkability
- Storage limitation
- Transparency
- Integrity & Confidentiality
- Accountability
- Intervenability

App Developers Guide

Privacy & Security Design Principles Catalog

- Purpose limitation & Data minimization
- Unlinkability
- Storage limitation
- Transparency
- Integrity & Confidentiality
- Accountability
- Intervenability

- Sharing limitation
- 3rd parties & 3rd countries
- 3rd party content

App Developers Guide

Privacy & Security Design Principles Catalog

- Purpose limitation & Data minimization
- Unlinkability
- Storage limitation
- Transparency
- Integrity & Confidentiality
- Accountability
- Intervenability

- Anonymization
- Pseudonymization

App Developers Guide

Privacy & Security Design Principles Catalog

- Purpose limitation & Data minimization
- Unlinkability
- Storage limitation
- Transparency
- Integrity & Confidentiality
- Accountability
- Intervenability

- Data retention
- Data accuracy

App Developers Guide

Privacy & Security Design Principles Catalog

- Purpose limitation & Data minimization
- Unlinkability
- Storage limitation
- Transparency
- Integrity & Confidentiality
- Accountability
- Intervenability

- Ex-ante measures
- Ex-post measures

App Developers Guide

Privacy & Security Design Principles Catalog

- Purpose limitation & Data minimization
- Unlinkability
- Storage limitation
- Transparency
- Integrity & Confidentiality
- Accountability
- Intervenability

- Sharing security
- Storage security
- Unauthorized access prevention
- Safeguard measures
- Secure payment
- Device & OS

App Developers Guide

Privacy & Security Design Principles Catalog

- Purpose limitation & Data minimization
- Unlinkability
- Storage limitation
- Transparency
- Integrity & Confidentiality
- **Accountability**
- Intervenability

→

- Internal procedures
- Data Protection Impact Assessments (DPIAs)

App Developers Guide

Privacy & Security Design Principles Catalog

- Purpose limitation & Data minimization
- Unlinkability
- Storage limitation
- Transparency
- Integrity & Confidentiality
- Accountability
- Intervenability

- User's rights
- User's consent

mobile business

Outline

1. Introduction
2. App Developers Guide
3. Summary

Summary

- Promises do not match actions
  - Absolute freedom!
- There is a gap between privacy regulation and implementation of real world app privacy practices
  - The presented guide catalog may help filling it.

Chair of Mobile Business & Multilateral Security

Majid Hatamian, Ph.D. candidate

Goethe University Frankfurt

E-Mail: majid.hatamian@m-chair.de

WWW: www.hatamian.net

www.m-chair.de