Why are Developers Struggling to Put GDPR into Practice when Developing Privacy-Preserving Software Systems?

Abdulrahman Alhazmi, Nalin Asanka Gamagedara Arachchilage
La Trobe University, Australia

Introduction

- Software developers find it difficult to incorporate privacy into the software applications they develop or take GDPR (General Data Protection Regulations) law into account.
- This may lead them to develop software applications that open up privacy breaches.
- Previous research has attempted to investigate why developers cannot embed privacy into applications, but not considering GDPR principles in full.
- To investigate the issue in-depth, there is a need for comprehensive study that investigates why developers cannot embed privacy into applications taking GDPR principles on-board.

Contribution

Our study contributes to helping develop privacy-preserving software systems, taking GDPR on board. If developers comply with GDPR principles, potential privacy breaches may reduce.

Therefore, as the first step, we conducted an interview study to investigate developers on the challenges they face when embedding privacy into software applications taking GDPR principles into consideration.

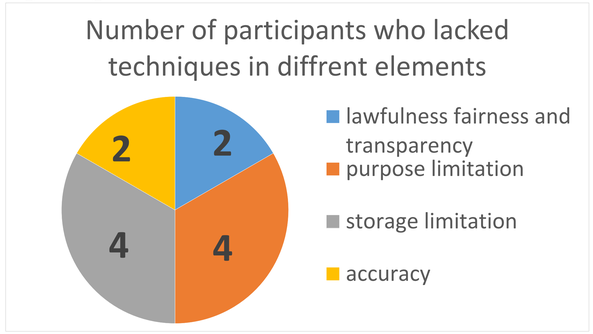
Methodology

- We conducted interviews with six developers who were identified on LinkedIn.
  - Males = 4
  - Females = 2
- The interviews were conducted remotely via Zoom.
- We gave participants a scenario and its UML diagrams, which were developed reflecting GDPR principles.
- We used the grounded theory technique to collect and analyse the participants' descriptive answers. Some of the answers were 'yes/no' and did not require grounded theory to analyse.
- Responses from all the participants were analysed. Three coding schemes were applied to the data collected. This was important as it enabled us to capture all the issues that developers face.

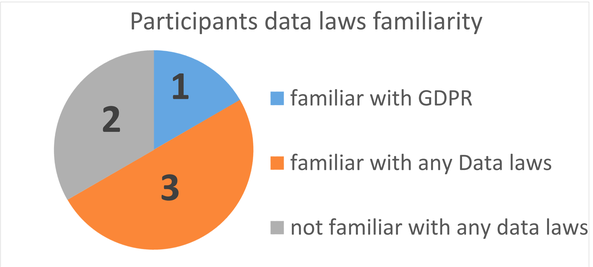
Results

The study findings revealed that two major issues that prevent developers from embedding privacy using GDPR principles. The issues were:

- Lack of good techniques to implement GDPR principles as shown below.



- Not familiar with GDPR law and lacked proper guidelines to implement it represented in the graph below.



Discussion and Recommendations

- The universal standard of GDPR law should be made available, so software creators can follow (irrespective of the country they belong to or the software application they develop for) while maintaining consistency; all nations should adopt and enforce it to enable developers familiarize themselves with the law and be bound by it.
- GDPR law should be accompanied by guiding techniques for each principle to ensure effective implementation of the principles and to prevent developers from using substandard techniques.
- Developers should be given formal knowledge of the GDPR law (i.e. principles), processes and techniques to apply them when developing privacy-preserving software systems.

Further Research

- We are planning to conduct qualitative this study with more participants, investigating why software developer cannot develop software applications that preserve user privacy.
- In addition, we are aiming at identifying tools, techniques and processes that are required for them to put GDPR into practice.

References

- A. Senarath and N. A. Arachchilage, "Why devel-opers cannot embed privacy into software systems? an empirical investigation," in Proceedings of the 22nd International Conference on Evaluation and Assessment in Software Engineering 2018, pp. 211–216, 2018.
- S. Schwerin, "Blockchain and privacy protection in the case of the european general data protection regulation (gdpr): a delphi study," The Journal of the British Blockchain Association, vol. 1, no. 1, p. 3554, 2018.
- A. Senarath and N. A. G. Arachchilage, "A data minimization model for embedding privacy into software systems," Computers & Security, vol. 87, p. 101605, 2019.

Contact Information

- Abdulrahman Alhazmi, Nalin A. G. Arachchilage

20509556@students.latrobe.edu.au
nalin.asanka@latrobe.edu.au