Privacy Mindset for Developing Internet of Things Applications for Social Sensing: Software Engineering Challenges

Charith Perera
charith.perera@ieee.org

Athanasios Vasilakos
Lulea University of Technology, Sweden
athanasios.vasilakos@ltu.se

ABSTRACT

Social sensing aims to collect sensory data by using human population as sensor carriers (e.g., location), sensor operators (e.g., taking photos), and sensors themselves (e.g., Twitter). The Internet of Things (IoT) applications facilitate social sensing tasks. However, designing and developing IoT applications is much more complicated than designing and developing desktop, mobile, or web applications. The IoT applications require both software and hardware (e.g., sensors and actuators) to work together on multiple different type of nodes (e.g., micro-controllers, system-on-chips, mobile phones, single-board computers, cloud platforms) with different capabilities under different conditions.

CCS CONCEPTS

•Hardware →Sensor applications and deployments; •Security and privacy →*Human and societal aspects of security and privacy;*

KEYWORDS

Internet of Things, Privacy, Privacy Mindset, Software Engineering

ACM Reference format:
Charith Perera and Athanasios Vasilakos. 2016. Privacy Mindset for Developing Internet of Things Applications for Social Sensing: Software Engineering Challenges. In *Proceedings of The 2nd International Workshop on Social Sensing, Pittsburgh, PA USA, April 2017 (SocialSens 2017),* 1 pages.
DOI: http://dx.doi.org/10.1145/3055601.3055621

1 PROBLEM DOMAIN

Such engineering complexities have forced software engineers to put most of their efforts towards addressing other challenges such as interoperability and modifiability, resulting in privacy concerns being often overlooked. However, IoT applications, especially which are focused on social sensing, collect and analyse personal data that can be used to derive sensitive information about individuals. Therefore, designing privacy aware IoT applications are critical. In order to achieve this, it is important to develop *Privacy mindset* among software engineers. The notion of *Privacy mindset* is similar to *Security mindset* [3].

Privacy mindset encourages software engineers to think about privacy awareness of their IoT applications at early design phases, not as an after thought. Privacy need to be treated as a first class citizen in IoT application development processes. Privacy mindset can only be developed by providing strong guidance to the software engineers and by reducing the effort and time required to embed privacy protecting measures into IoT applications. There are few different research work that have been proposed in order to guide software engineering processes.

Privacy foundation principles [1], *Privacy design strategies* [1], *Privacy by Design (PbD) guidelines* [2], *Privacy Patterns*, and *Privacy Tactics* aim to provides different levels of guidance to software engineers as show in Figure 1. *Privacy Patterns*, inspired by design patterns, describe high-level structures and behaviours of software systems as the solution to multiple system requirements. They are complex compositions of privacy tactics. *Privacy Tactics*, inspired by tactics, are design decisions that improve individual privacy quality attributes. They are the most fundamental building blocks.

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
SocialSens 2017, Pittsburgh, PA USA
© 2017 ACM. 978-1-4503-4977-2/17/04…$$15.00
DOI: http://dx.doi.org/10.1145/3055601.3055621

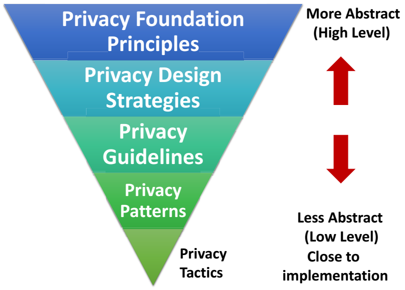
Privacy Foundation Principles
Privacy Design Strategies
Privacy Guidelines
Privacy Patterns
Privacy Tactics
More Abstract (High Level)
Less Abstract (Low Level) Close to implementation

Figure 1: From high level principles to low level tactics

2 RESEARCH DIRECTIONS

We need develop an unified PbD design framework that incorporates not only high level principles, but all the way to patterns and tactics. Then, we need to build automated (or at least semi-automated) tools that can help software engineers to apply privacy protecting measures into their IoT applications. Different types of tools will be required to support different phases of the IoT application life-cycle (e.g., design, runtime) and different components (e.g., edge nodes, gateway nodes, cloud nodes).

REFERENCES

[1] George Danezis, Josep Domingo-Ferrer, Marit Hansen, Jaap-Henk Hoepman, Daniel Le Métayer, Rodica Tirtea, and Stefan Schiffner. 2014. *Privacy and Data Protection by Design - from policy to engineering.* Technical Report. European Union Agency for Network and Information Security (ENISA). 1–79 pages.

[2] Charith Perera, Ciaran Mccormick, Arosha Bandara, Blaine A. Price, and Bashar Nuseibeh. 2016. Privacy-by-Design Framework for Assessing Internet of Things Applications and Platforms. In *The 6th International Conference on the Internet of Things.* 83–92.

[3] C Severance. 2016. Bruce Schneier: The Security Mindset. *Computer* 49, 2 (feb 2016), 7–8. DOI: http://dx.doi.org/10.1109/MC.2016.38