Demo Abstract: PARROT: Privacy by Design Tool for Internet of Things

Nada Alhirabi
School of Computer Science and Informatics, Cardiff University
Cardiff, UK
King Saud University, Saudi Arabia
AlhirabiN@cardiff.ac.uk

Omer Rana
School of Computer Science and Informatics, Cardiff University
Cardiff, UK
RanaOF@cardiff.ac.uk

Charith Perera
School of Computer Science and Informatics, Cardiff University
Cardiff, UK
PereraC@cardiff.ac.uk

***Abstract*—The design process for applications that make use of Internet of Things (IoT) can be more complex than for desktop, mobile or web-based platforms. IoT applications typically collect and analyse personal data categorised as *sensitive*. These data may be subject to a higher degree of protection under data privacy laws. We present PARROT (PrivAcy by design tool foR inteRnet Of Things) – an interactive IoT application design tool for privacy-aware IoT applications. PARROT enables developers to consider privacy compliance during the design process and provides real-time feedback on potential privacy concerns that may need to be considered. From a privacy compliance perspective, PARROT incorporates privacy-specific design features into the IoT application from the beginning rather than retrospectively.**

***Index Terms*—Internet of Things, Privacy by Design, Software Design, Data Protection, Privacy Law, GDPR, Usable Privacy**

I. INTRODUCTION AND MOTIVATION

Internet of Things (IoT) applications generate and process large amounts of data, which need to be transferred to devices for processing. As the size and frequency of generation of this data increases, an efficient architecture is needed to deal with this data. To enable end-users to use these applications regularly, it is necessary to design End-User Development (EUD) techniques that align more closely with user needs. Interactivity may also make such applications and software tools more intuitive for users (both lawyers and developers in our case). It is necessary for EUD techniques to more closely capture real-time collaboration instead of a static user experience.

Researchers have been using privacy-enhancing technologies (PETs) and privacy-by-design (PbD) concepts to minimise privacy risks in data processing systems. These approaches must align with legal privacy requirements, such as those set out in the General Data Protection Regulation (GDPR). Data protection-by-design (DPbD) must ensure that privacy-related requirements are considered in the design and development of data processing systems [1]. Cavoukian [2] identified the importance of including PbD into the design of information technologies and systems. Despite the efforts made in the PbD area, most people have limited knowledge of (potentially substantial) privacy risks in an online environment. Many users find it difficult and time-consuming to fully understand privacy policies and their impact on their work. There is a need for a tool that enable privacy requirements to be more clearly identified [3] [4] [5]. This tool should also offer an intuitive and user-friendly interfaces to assist software developers in deciding how to include privacy into their system design.

II. APPROACH

We used a number of semi-structured interviews to understand privacy requirements of users, including collaboration with a privacy lawyer. This led to the design and implementation of PARROT. A prototype of PARROT was then evaluated to see if developers considered privacy requirements during the design process.

A. Study 1: Understanding Privacy Breakdowns

The goal of this study was to understand privacy challenges considered by developers. To design our tool we recruited 18 full-stack developers to examine their understanding of privacy through a series of semi-structured interviews. We then ran an IoT application design exercise for an IoT health use case, *Diabetes treatment and monitoring*, to understand their approach of integrating privacy within the software design process. We collaborated with a privacy lawyer and other legal professionals to identify privacy breakdowns between developers and privacy professionals. Our results helped us to identify potential areas to consider for the design of IoT applications.

B. Study 2: Operationalisation

This study aimed to apply operationalisation techniques for the designs produced in study one. We applied the design notations that were analysed in study one using the four Enact design principles: provide multiple viewpoints, maintain a single source of truth, reveal the invisible, support design by enaction [6]. Since Enact principles claimed to reduce the breakdown between designers and developers, we wanted to test whether the same principles could help us to reduce breakdowns between developers and privacy professional.

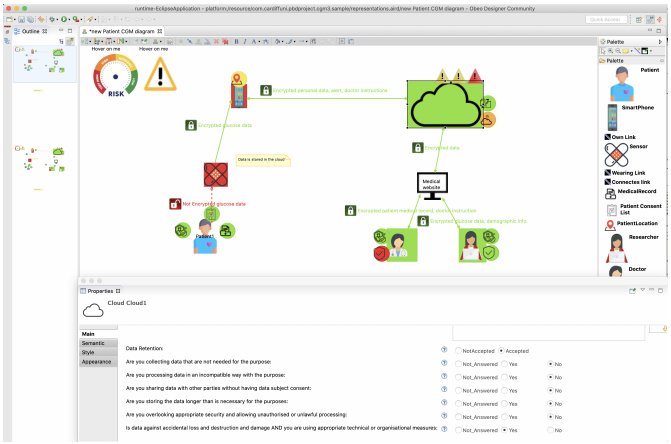

Fig. 1. PARROT interface. The design area is in the middle. At the right, there is the palette to drag and drop in the design area. At the bottom are properties where a developer configures privacy properties by answering multiple questions related to the selected node or sub-node. Each risk is colour to reflect a degree of privacy/security risk. Red: very high risk; Orange: high risk; Yellow: moderate risk; Green: low risk.

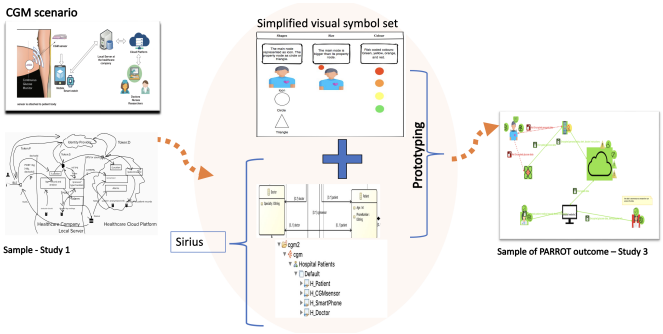

Fig. 2. Integrating privacy using PARROT (right) and without PARROT (left) for the Continuous Glucose Monitoring (CGM) use-case.

C. Study 3: Prototyping and Evaluation

In this study, we created an initial prototype of PARROT to test the effectiveness of privacy design principles in the context of healthcare. After that, we evaluated the tool in a controlled lab study with multiple developers. A privacy lawyer interpreted the resulting designs for privacy. Our goal is to implement an interactive tool to complement the designs produced in study one. We implemented the prototype using Sirius (eclipse.org/sirius), an online modelling tool, to test the effectiveness of the design principles. Sirius gives us the ability to build a domain-specific modelling tool, starting from building a custom domain model, as shown in Figure 1. This prototype was intended to be used as a privacy assistant, based on the results of study two. We then tested the prototype in a controlled lab study with 24 developers, and with support of a privacy lawyer. The result is used to determine whether these developed designs using the prototyped tool are more privacy-aware than the previous designs produced in study one. Figure 2 shows that using PARROT to represent privacy risks visually is more effective than using text.

III. Lessons Learned

Our findings provide insights into how developers perceive PARROT. Since adding privacy properties to a design can also add additional cost, we evaluated if the prototype features were considered by users as disruptive, difficult to use or time-consuming using the Likert scale. Overall, most of the developers found PARROT useful. We also used Microsoft's reaction words to evaluate the usability of the tool. The majority of the participants found the tools to be useful, helpful, easy to use and effective. In addition, our study results show that IoT applications designed with PARROT addressed privacy issues better and managed to reduce some of the breakdowns identified earlier. We also found that PARROT reduces the workload of the privacy lawyer. Moreover, we found that PARROT is equally useful for both expert and novice developers despite their level of experience.

IV. Demonstration Description

To demonstrate our tool, we use a *diabetes treatment and monitoring* scenario to demonstrate how the proposed tool will help IoT system developers better incorporate privacy measures at design time. In this sample use case, we have a researcher working in a healthcare company with many diabetes patients. Both doctor and researcher need the collected data from a Continuous Glucose Monitoring (CGM) device worn by patients for medical follow-up or analytical purposes. The challenge here is for the software developers to build the system while applying privacy principles and rules to their designs – which PARROT could offer. This demo will show the running tool (Demo Video). It will demonstrate the simplified visual notation that we have implemented to support the PbD concept. We will present the interactivity while configuring privacy properties with real-time feedback using colour coding. Additionally, the demo will illustrate that privacy configuration could be carried out at two levels: at the node and sub-node levels. For example, the phone could be the node with privacy constraints, such as collecting data that does not match the purpose of use. The location is the sub-node that could have specific privacy issues, such as sharing the exact location even if it is unnecessary.

References

[1] Lee A Bygrave. Data protection by design and by default: deciphering the EU's legislative requirements. *Oslo Law Review*, 4(2):105–120, 2017.

[2] Abhik Chaudhuri and Ann Cavoukian. The Proactive and Preventive Privacy (3P) Framework for IoT Privacy by Design. *EDPACS*, 57(1):1–16, 2018.

[3] Charith Perera, Mahmoud Barhamgi, and Massimo Vecchio. Envisioning tool support for designing privacy-aware internet of thing applications. *IEEE Internet of Things Magazine*, 4(1):78–83, 2021.

[4] Charith Perera, Mahmoud Barhamgi, Arosha K Bandara, Muhammad Ajmal, Blaine Price, and Bashar Nuseibeh. Designing privacy-aware internet of things applications. *Information Sciences*, 512:238–257, 2020.

[5] Nada Alhirabi, Omer Rana, and Charith Perera. Security and privacy requirements for the internet of things: A survey. *ACM Trans. Internet Things*, 2(1), Feb 2021.

[6] Germán Leiva and et al. Enact: Reducing designer–developer breakdowns when prototyping custom interactions. *ACM Transactions on Computer-Human Interaction (TOCHI)*, 26(3):1–48, 2019.