A Privacy-Aware Wearable Framework

Muhammad Mohzary
Advance Information Security and Privacy Lab,
Department of Computer Science
Kent State University, OH
mmohzary@kent.edu

Kambiz Ghazinour
Advance Information Security and Privacy Lab,
Department of Computer Science
Kent State University, OH
kghazino @kent.edu

ABSTRACT

With the exceptional evolution in smartwatch capabilities to monitor users' daily activities, privacy concerns increase for the smartwatch users who must disclose their sensitive personal information in order to have access to application services. Recently, studies have stated that collected information, even in aggregated form, is sufficient to infer users' behavior. Therefore, sharing such information may lead to privacy leakage not expected by the users. This research proposes a privacy-aware wearable framework to protect smartwatch users' sensitive information. The proposed framework consists of a friendly user interface and an access control model. The user interface is designed to allow smartwatch users to express their privacy preferences for each application; the access control model is developed to enforce privacy policies as defined by the data collector and smartwatch user. The Tizen platform is used to conduct two experiments on a group of participants to examine the efficiency of the proposed framework. Finally, a survey is conducted to study participants' privacy feeling towards the proposed privacy-aware framework and to measure the demand for such tool and its usability.

1. INTRODUCTION

Wearable devices play a core role in enhancing the quality of life for everyone because of their distinctive capabilities of collecting users' vital signs in real time. Wearable devices like smartwatches have many applications which can perform many computing tasks that can be seen on laptops and mobile devices. Additionally, they can communicate seamlessly with other devices like smartphones to synchronize users' information. Unfortunately, despite all the useful features smartwatches currently have, users still have no control over the collected data which negatively affects their privacy.

Smartwatch platforms such as watchOS, Android, and Tizen, provide developers with standardized APIs to collect users' personal information [1]. For example, the platform Tizen provides HumanActivityMonitor API which allows developers to manage human activity data from various sensors on the smartwatch [2]. Collected information from sensors like Pedometer or GPS can be used to infer the behavior of users [1].

Currently, three issues must be addressed. First, smartwatch users cannot easily select their privacy preferences on their data. Second, applications give users two options which are to accept or refuse privacy terms, if users decline to accept the terms, they cannot use applications. Third, there is no framework that can support flexibility to run applications based on privacy policies as defined by the data collector and smartwatch users.

The purpose of this research is to assist smartwatch users in being aware of how their personal information will be used after collection. In addition, it aims to enforce applications to work based on privacy policies as defined by the data collector and smartwatch user.

2. PROPOSED WORK

This research proposes a privacy-aware framework to protect smartwatch users' sensitive information.

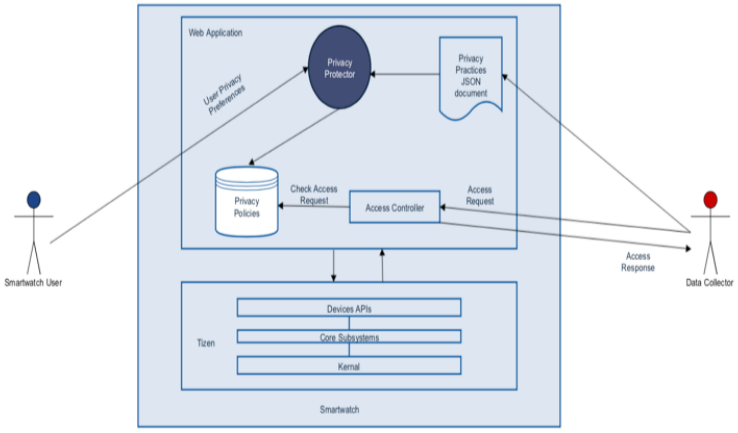

Figure 1. Proposed privacy-aware wearable framework.

Subsequently, we designed a graphical user interface based on design principles and guidelines for wearable devices to deliver a better user experience for our app [4] [5]. It represents data privacy taxonomy elements that are proposed in [3]. With this GUI, smartwatch users can express their privacy preferences for each application. Moreover, we built an access control model to receive application requests to access sensors information and enforce privacy policies as defined by the data collector and smartwatch user. The Tizen platform is used to develop and examine the efficiency of the proposed framework.

3. EXPERIMENTS

This is an ongoing research and for our initial phase, we used the Tizen platform to conduct two experiments on a group of participants. In the first experiment, a malicious application is built to collect their private information such as heart rate, step counts, and GEO-data from the GPS sensor. Their data is anonymized in the database to protect their privacy. Each participant is given a smartwatch with the malicious app installed on it. Then, they use the smartwatches for two days. Next, they are allowed to see the data that is collected by the malicious app. In the second experiment, the same participants use the proposed privacy-aware framework with the malicious app. After they return the smartwatches, they are presented with the collected data and they see how much data is protected using the privacy-aware model compared to the first experiment.

4. REFERENCES

[1] T. Yan, Y. Lu, and N. Zhang, "Privacy Disclosure from Wearable Devices," In Proceedings of the 2015 Workshop on Privacy-Aware Mobile Computing, New York, NY, USA, 2015, pp. 13–18.

[2] "API Reference - Web Application - | Tizen Developers." [Online]. Available: https://developer.tizen.org/development/api-references/web-application. [Accessed: 04-Apr-2018].

[3] K. Barker et al., "A Data Privacy Taxonomy," In Dataspace: The Final Frontier, 2009, pp. 42–54.

[4] Design Principles | Tizen Developers." [Online]. Available: https://developer.tizen.org/design/wearable/design-principles. [Accessed: 25-May-2018].

[5] "Design for Wear OS," Android Developers. [Online]. Available: https://developer.android.com/design/wear/. [Accessed: 25-May-2018].