Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 98 (2016) 205 – 210

Procedia
Computer Science

The 7th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2016)

A Privacy-aware Platform for Sharing Personal Information on Wearable Devices

Kambiz Ghazinour *, Wesley Delp, Jimmy Gross, Ali Taheri Moghadam, Timothy Strawbridge, Jake Tobin

Advanced Information Security and Privacy Lab, Department of Computer Science, Kent State University, Kent, Ohio, USA

Abstract

Personal information (PI) embodies a wide and sometimes fuzzy spectrum of user privacy and security concerns. Recently, with the rapid progression in mobile technologies, a new frontier with both opportunities and vulnerabilities has come to fruition. Multitudes of personal fitness devices are able to capture data at any time, storing it on users' mobile devices. Third party developers can access this data, raising questions about the security of users' sensitive information, in addition to privacy concerns related to the possibly identifiable nature of the data. Frameworks such as Apple's HealthKit provide terms to developers, which restrict what can be done with personal user information. However, the wording of these frameworks is largely vague, and sharing settings within the OS are restrictive. In order to provide users with a more customizable and informative user-interface, as well as developers with a framework for requesting access to health data, a new standard must be created. We propose a model able to store privacy predicates for each piece of health information requested. We also propose a new platform, allowing users to select privacy settings in an efficient and informative manner. It is imperative that a uniform and scalable solution be put in place such that the privacy and security of personal and potentially identifiable health data remains an utmost concern. Our implementation provides a method to meet these concerns.

Peer-review under responsibility of the Program Chairs

Keywords: Privacy; Health info; JSON; Wearable device;

* Corresponding author. *E-mail addresses:* kghazino@kent.edu

Peer-review under responsibility of the Program Chairs
doi:10.1016/j.procs.2016.09.033

1. Introduction

The information collection capabilities of mobile and wearable technologies have continuously expanded over time. The current privacy options available for use in mobile and wearable devices do not allow an individual to know with certainty how sensitive information will be used or for how long that information will be stored [1]. The legal framework that regulates and protects an individual's health information has remained since 2009 [2]. Improvements in health information collection coupled with the aforementioned static legal framework has created a difficult situation for developers in knowing when the health information being collected is protected under law and when it is not [3]. Inadequate protection of semi/quasi-identifying sensitive personal information may lead to unauthorized individuals using information to identify individuals, which poses a threat to user privacy and security. Reducing the security and privacy related uncertainty created by the current trends of technological progress and legislative gridlock for both individuals and developers is the problem we aim to solve.

There is previous research work in the areas of privacy policy languages, such as XACML [4] and the privacy taxonomy [1]. XACML uses XML to implement a role based access control model (RBAC). RBACs provide a framework that protects both providers and collectors of data from unauthorized access to that data [5]. However, the XML backbone of XACML is not ideal for mobile technologies because XML usage is too resource intensive for mobile hardware [6]. The privacy tuple developed by Barker et al provides a framework in which individuals can gain information on how their data is being used (purpose), who is able to access the data (visibility), the level of detail of the data provided (granularity), and how long the data may be stored (retention).

To protect the privacy of users of mobile applications and wearable technology, and to ensure that developers can communicate privacy settings and their implications to their users, we propose a user interface that visualizes the taxonomy proposed by Barker et al. [1] and is supported by a standardized JSON schema. The work presented in [7] and [11] addresses a Privacy Policy Visualization Model (PPVM). However, this work does not provide a model that translated to a mobile user interface. In this work, we have developed an interface that communicates the privacy information of the taxonomy model to the user in a manner that is usable within the limitations of a mobile or wearable interface. The JSON schema that we propose is both modern and lightweight. It ensures that sensitive data can be kept secure using best security practices and can be easily be implemented by developers. We plan to examine the efficacy of our proposed model as future research direction.

2. Proposed Platform

To the best of our knowledge there is currently no clear method to identify how information collected by mobile devices is used, and given that many applications require at least some information to function, users may be unwillingly giving access to PI. For example, the current workflow supported by Apple's HealthKit framework involves a user opening a third-party application before being transported to the system settings screen. This screen presents the user with a binary selection for each data point. This is a slightly tedious process as there is no uniform way of selecting preferences within the third-party app, and no way for the developer to communicate the purpose for using the data.

Our solution to this issue is be a new system-oriented UI for privacy preference selection. On initial startup of a third-party application, the device would trigger the application's bundled JSON to be loaded into our proposed interface. The user could then select preferences for each individual data object. Once the user has selected his or her preferences, the edited JSON data object communicates with the third-party application as to the user's intended settings and the application launches accordingly.

3. Implementation: Creating JSON API

In order to protect the user, certain steps concerning the security aspect of personal information must be followed. Users expect their data in a typical use case to be secure and protected. The security and authenticity of this data is a critical priority in any information system, even more so when this data is of a personal nature.

A. The first step in capturing data is conceptualizing and designing how it will be stored. This becomes important when complex relationships among datasets exist. We designed our system to be able to integrate with