Telematics and Informatics xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

Telematics and Informatics

journal homepage: www.elsevier.com/locate/tele

Conceptual framework for the security of mobile health applications on Android platform

Muzammil Hussain[a], A.A. Zaidan[b,*], B.B. Zidan[b], S. Iqbal[a], M.M. Ahmed[c], O.S. Albahri[b], A.S. Albahri[b]

[a] Department of Computer Science, School of Systems and Technology, University of Management and Technology, Lahore, Pakistan
[b] Department of Computing, Faculty of Arts, Computing and Creative Industry, Universiti Pendidikan Sultan Idris, Tanjong Malim, Perak, Malaysia
[c] Department of Computer Science, Capital University of Science and Technology (CUST), Islamabad, Pakistan

ABSTRACT

Mobile Health (mHealth) applications are readily accessible to the average user of mobile devices, and despite the potential of mHealth applications to improve the availability, affordability and effectiveness of delivering healthcare services, they handle sensitive medical data, and as such, have also the potential to carry substantial risks to the security and privacy of their users. Developers of applications are usually unknown, and users are unaware of how their data are being managed and used. This is combined with the emergence of new threats due to the deficiency in mobile applications development or the design ambiguities of the current mobile operating systems. A number of mobile operating systems are available in the market, but the Android platform has gained the topmost popularity. However, Android security model is short of completely ensuring the privacy and security of users' data, including the data of mHealth applications. Despite the security mechanisms provided by Android such as permissions and sandboxing, mHealth applications are still plagued by serious privacy and security issues. These security issues need to be addressed in order to improve the acceptance of mHealth applications among users and the efficacy of mHealth applications in the healthcare systems. Thus, this paper presents a conceptual framework to improve the security of medical data associated with Android mHealth applications, as well as to protect the privacy of their users. Based on the literature review that suggested the need for the intended security framework, three-distinct and successive phases are presented, each of which is described in a separate section. First, discussed the design process of the first phase to develop a security framework for mHealth apps to ensure the security and privacy of sensitive medical data. The second phase is discussed who to achieve the implementation of a prototypic proof-of-concept version of the framework. Finally, the third phase ending discussed the evaluation process in terms of effectiveness and efficiency for the proposed framework.

1. Introduction

mHealth apps are hereby defined as software programs that provide health related services through smartphones and tablets (Organization, 2011). mHealth is an emerging field which has the potential to make healthcare professionals more efficient, increase patient satisfaction and reduce the healthcare cost (Mat Kiah et al., 2014a,b). The general concept of mHealth includes medical apps.

* Corresponding author.
E-mail address: aws.alaa@gmail.com (A.A. Zaidan).

https://doi.org/10.1016/j.tele.2018.03.005
Received 29 November 2017; Received in revised form 28 February 2018; Accepted 6 March 2018

There are several types of medical apps, some are using external devices such as medical sensors, and some apps are using smartphone resources, such as the camera for the treatment of the patient. The use of mHealth apps among physicians and patients has grown significantly since the introduction of mobile phones. Physicians can access patients' data and medical knowledge at the point of care, and they can also monitor patient health through mHealth apps. The sensitive nature of these apps' purpose and consequence of use – in relation to human health – impose several questions about their reliability, authority, and compliance to regulations. Aside from the functional requirements, issues related to non-functional requirements have also to be addressed, such as the usability of the apps by users from different age groups. In particular, it soon became clear that mHealth apps carry substantial risks to the security of user's sensitive medical data as well as their privacy (Gill et al., 2012). Developers of these apps are usually unknown, and users are unaware of how their data are being managed and used. In mHealth, users can easily enhance the functionalities of their smartphones by connecting them to external devices, such as medical devices, sensors and credit card readers. This introduces many new threats along with the useful applications in various domains, including healthcare information systems and retail (Avancha et al., 2012; Murthy and Kotz, 2014; Istepanian et al., 2006; Anokwa et al., 2012; Naveed et al., 2014). Android is an operating system based on Linux for mobile devices. Android platform provides a rich application framework that allows developers to build innovative apps in the Java language environment. Android is a multi-user system in which each app is considered an individual user, and is given a unique user ID (UID). Every app runs in its own Linux process and uses a separate virtual machine to be isolated from other apps. In this way, Android platform implements the principle of *least* privilege. That is, each app, by default, can only access those components that are required to do its own work. mHealth apps operate on mobile platforms, and because the Android operating system is chosen as the target platform in this article, there is a need to investigate its structure as well as its security model in detail.

In order to protect user data, system resources (including the network) and apps themselves, Android platform provides the following extra security features: security at the OS level through the Linux kernel's secure inter-process communication (IPC), application sandbox, application signing, and the Android permission model. Recently, researchers have been actively involved in the study of mHealth apps, in particular their security and privacy. For example, Mitchell et al. (2013) investigated the security and privacy challenges of mHealth apps; He et al. (2014) raised the security concerns of Android mHealth apps; and Plachkinova et al. (2015) proposed a taxonomy of mHealth apps' security and privacy concerns. Nevertheless, beyond the identification and investigation of the problem itself, there is no actual solution for the security and privacy of mHealth apps specifically, except one policy framework (Mitchell et al., 2013). This framework provides some guidelines to secure mHealth apps; however, these policies are not enough and even not implemented to secure mHealth apps. In addition, Android-provided security features are still insufficient to protect user data against few security attacks that are equally applicable to mHealth apps and their data, such as side channel threats, privilege escalation attacks, sensors-based covert channels and DMB attacks (Naveed et al., 2014; He et al., 2014; Davi et al., 2011; Al-Haiqi et al., 2014). mHealth apps are a new and revolutionary development in healthcare system, and a huge number of people can access this new system at a very low cost.

Considering the great utility and impact of this phenomenal development, and the detrimental effect that security and privacy issues might cause to its successful deployment, those issues in mobile health applications on Android platform need to be addressed to improve mHealth apps' effectiveness and alleviate any barriers to their rapid integration into the healthcare system. The main theme of this article is the security and privacy of mHealth apps on Android smartphones. This theme involves two main research components: the security of Android smartphones, and the incorporation of mHealth apps' security within Android security model. Then, figure out the weak points and consequently proposed a new methodology as a solution are discussed as demonstrated in our study framework in Fig. 1. The remaining sections of this paper are organized as follows. Section 2 describes the mobile health applications on android platform. Section 3 reports discussion of three distinct and successive phases. Section 4 concludes the conclusion.

2. Mobile health applications on Android platform

This section provides necessary background information on the concepts of the Android platform and the security issues at the intersection of mhealth and android platform. The section is divided into two sub-sections. Section 3.1 is providing a complete background on the Android architecture, and what has been done to secure this platform. While, the section 3.2 reviews the most relevant works in the literature on the threats to mHealth apps, and provides a critical assessment of their security and privacy. This section also summarizes the existing solutions to address those issues. The focus of the section is directly related to the research in this article, which attempts to contribute and propose a novel solution to the said issues.

2.1. The Android platform and its security

The main goal of this study is to protect sensitive information of mHealth apps and their user. mHealth apps operate on mobile platforms, and because the Android operating system is chosen as the target platform in this study, there is a need to review its structure as well as its security model in detail. This section briefly presents the details of Android OS, its components, the possible types of communication in the system, and the supported security mechanisms.

2.1.1. Android system architecture

Android is a Linux based operating system developed primarily for mobile devices (e.g., smartphones or tablets) circa 2003 by Android Inc. (Elgin, 2005). Soon after, Google acquired this company in 2005. Google commenced the first Android device in October 2008, and thenceforth it maintains the development of the operating system, as well as its marketing and support. Google also