Chapter 62
Towards User Authentication Requirements for Mobile Computing

Yaira K. Rivera Sánchez
University of Connecticut, USA

Steven A. Demurjian
University of Connecticut, USA

ABSTRACT

The emergence and ubiquity of mobile computing has placed powerful capabilities in one's hand providing a wide range of applications such as email, calendar, photos, browsers, social network, communication, shopping, health and fitness, games etc., which were once restricted to traditional platforms. Such applications on a single mobile device raise critical security issues related to managing identity, re-authenticating users that stay active for long periods of time, protecting sensitive PII and PHI against access and misuse, insuring secure transactions, and protecting the physical device. This chapter explores user authentication requirements for mobile computing by: evaluating alternative user authentication requirements in order to make recommendations on their usage in authentication; identifying authentication methods used in mobile healthcare applications; and proposing a set of requirements for user authentication to handle the situation when a user seeks to be securely authenticated across a set of applications that are placed into context within a framework.

INTRODUCTION

Mobile computing platforms have greatly increased in the marketplace. By the end of 2013, globally, 6% of the population owned a tablet and 22% owned a smartphone (Jeggenstuen, 2013). In the United States, by the end of 2014, there was a 63.5% penetration rate (eMarketer, 2013). Such growth leads to the reduction of traditional desktop and laptop sales (Gartner, 2014). As individuals rapidly change the ways they access data and information, there is a profound impact on the way that users must be

DOI: 10.4018/978-1-7998-1204-3.ch062

authorized and authenticated. Accessing data and executing apps on a mobile platform is substantially more dynamic than traditional computing on laptops and desktops. A mobile device user may have a myriad of open applications including email accounts (corporate, Gmail, yahoo, etc.), browsers, social network apps (Facebook, Twitter, LinkedIn, etc.), communication apps (Skype, Snapchat, SMS, etc.), shopping apps (Amazon, JCPenney, Walgreens, etc.), health and fitness apps (CVS Health, Microsoft HealthVault, MyQuest, etc.), games, etc. In such a setting, users are often logged onto and authenticated to all of these apps simultaneously and move among them throughout the day, providing them with the ability to store, exchange, and view both personally identifiable information (PII) and personal health information (PHI). The drawback is the need for users to be authenticated on each individual application and often re-authenticated during sessions that can last for long periods of time. The challenge in this situation is to deliver a means for user authentication for mobile computing in order to provide a more seamless experience for users.

As a result, for a user to manage his/her personal information in several domains, we need to find a secure means while maintaining their privacy. Therefore, the challenge is a need to provide a cohesive means of user authentication that can cross all of these different domain boundaries with high availability of data, while still providing the necessary level of security and privacy. Our approach to such a challenge is to identify existing frameworks, standards, types of access control, and authentication methods that can identify requirements for user authentication for mobile devices and applications that would then be able to interact and share information with other mobile, cloud, and computing applications for a given domain. In the case of healthcare, health information technology (HIT) systems have emerged (e.g., electronic medical records (EMRs), practice management systems (PMSs) and personal health records (PHRs)), due to the American Recovery and Reinvestment Act (ARRA) of 2009 (U.S. Department of Education, 2010), all which must adhere to the Health Insurance Portability and Accountability Act (HIPAA) (HHS.gov, 2013) for the security, availability, transmission, and release of a patient's medical information. Note that an EMR is the primary means for making patient information electronically available to medical providers for healthcare. This wide adoption of HIT allows individuals to track their own health data independent of their provider. For example, the fitness market has exploded with wearable fitness devices that link to mobile applications, e.g., Apple has a new HealthKit app (Apple iOS 9, 2014) that utilizes a dashboard to manage health and fitness data while Google has the Fit fitness tracker (Real IT Experts, 2013). Both have pushed strongly into the smartwatch market to track activity, heart rate, blood pressure, etc. (Kelly, 2014) and these and other apps must be able to securely exchange HIPAA protected information back and forth with mobile applications for both patients and medical providers. In such a scenario, the same information is stored in different ways in diverse HIT systems and other applications, and this information must be staged back and forth to a mobile device and be protected from theft and misuse while simultaneously allowing a user to share the data with authorized medical providers and others, such as family members.

In support of this, the main focus of this work is to identify the requirements and capabilities that are needed to support user authentication that allows a person utilizing a mobile device to gain access to protected information from multiple input sources (cloud services, other users, other apps, etc.), with the health care domain as a test-bed. This chapter identifies and explains user authentication requirements for mobile computing that offers a high degree of security assurance and that is able to facilitate the aforementioned discussion on the access, usage, and sharing of information among users. In order to support user authentication in mobile computing there are key security concepts to be considered. In terms of *credentials*, mobile applications have long used passwords as a main means of access, with recent OS