Chapter 13
Role-Based Access Control for Mobile Computing and Applications

Yaira K. Rivera Sánchez
University of Connecticut, USA

Steven A. Demurjian
University of Connecticut, USA

Joanne Conover
University of Connecticut, USA

Thomas P. Agresta
University of Connecticut Healthcare Center, USA

Xian Shao
University of Connecticut, USA

Michael Diamond
Pomona College, USA

ABSTRACT

The proliferation of mobile devices has changed the way that individuals access digital information with desktop applications now performed seamlessly in mobile applications. Mobile applications related to healthcare, finance/banking, etc., have highly sensitive data where unsecure access could have serious consequences. This chapter demonstrates an approach to Role-Based Access Control (RBAC) for mobile applications that allows an information owner to define who can do what by role, which is then enforced within a mobile application's infrastructure (UI, API, server/database). Towards this objective, the chapter: motivates the usage of RBAC for mobile applications; generalizes the structure and components of a mobile application so that it can be customized by role; defines a configurable framework of locations where RBAC can be realized in a mobile application's infrastructure; and, proposes an approach that realizes RBAC for mobile security. To demonstrate, the proposed RBAC approach is incorporated into the Connecticut Concussion Tracker mobile application.

DOI: 10.4018/978-1-7998-0417-8.ch013

INTRODUCTION

The proliferation of mobile devices in all aspects of daily living has fundamentally altered the way that individuals interact with mobile applications. Evidence includes: the worldwide shipments of 1.9 billion phones and 230 million tablets outpacing PC/laptop sales (300 million estimate) (Gartner, 2015; Cisco, 2014); a report of smartphone usage in the U.S. where 64% of adults own a Smartphone, 42% own a Tablet, and 32% own an e-reader (Pew Research Center, 2012; Smith, 2015); and, predictive statistics that tablet users will surpass 1 billion worldwide in 2015 (eMarketer, 2015) and total devices will exceed 12.1 billion by 2018 (Radicati, 2014). Mobile applications now span a broad spectrum of complexity, including games, social networking, email, web browsing, financial management, health and fitness, pharmaceutical, etc. For both personal and business usage, there is a need to protect secure information ranging from protected health information (PHI) and personally identifiable information (PII) to confidential work product that is displayed, accessed, modified, and stored. Mobile health (mHealth) applications in healthcare and fitness are numerous and diverse: tracking medications (myCVS (CVS Pharmacy, 2015), MedWatcher (2012), etc.); personal health records (PHR) (CAPZULE PHR (Capzule, 2012), MTBC PHR (2011), etc.); fitness applications that work with phones and wearables (Cohen, 2015); Apple's HealthKit app (iOS 9, 2014) and the Google Fit fitness tracker (Google Play, 2013), to track activity, heart rate, blood pressure, etc. (Kelly, 2014); and, Apple's ResearchKit (Apple, 2015), an open source framework for mobile applications to support medical research. Patients also seek to have access via their mobile devices to the electronic medical records (EMRs) utilized by medical providers and health information technology (HIT) systems that contain medical testing results (Care360, 2014) or results from imaging testing (My Imaging Records App, 2013). All of these systems 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.

To augment the usability of these mHealth applications, there is also a desire by patients to attain privacy control to different individuals at varying levels of granularity over their electronic health and fitness information in various locations (Caine & Hanania, 2013). For a given patient, this effort highlights the potential recipients of the information (e.g., primary physicians, spouse, family, emergency medical providers, etc.) and the type of information to be controlled (e.g., contact info, current conditions, medications, recent test results, genetic information, etc.). In such a setting, patients are also interested in actually defining specific fine-grained access control by role (Sujansky, Faus, Stone, & Brennan, 2010), for example: a family member may view my medication list (but not all of them), a medical provider may view my medication list and history of hospital visits (but not modify), my personal physician may both view and modify my health care and fitness data, etc. These efforts highlight a strong need to achieve fine grained role-based level of security to allow patients to define who can see and/or modify what portions of their health/fitness data, where the mobile application itself can be customized based on role to meet the permission definition provided by the patient (Peleg, Beimel, Dori, & Denekamp, 2008). Securing information of mHealth applications for a diverse set of stakeholders may benefit from the usage of role-based access control (RBAC) (Ferraiolo & Kuhn, 1992). Such an inclusion allows permissions established by the information owner to be defined for other authorized users by role and use this as a basis to have the mobile application deliver only authorized information, and permitted view and/or modify capabilities. Note also that RBAC has been heavily adopted in healthcare, where a recent published literature review (Fernández-Alemán, Señor, Lozoya, & Toval, 2013) had 35 efforts utilizing access control methods and 27 of these specifically utilized RBAC.