Chapter 5
Trust Profiling to Enable Adaptive Trust Negotiation in Mobile Devices

Eugene Sanzi
University of Connecticut, USA

Thomas P. Agresta
University of Connecticut Health Center, USA

Steven A. Demurjian
University of Connecticut, USA

Amanda Murphy
Canisius College, USA

ABSTRACT

In order to secure mobile devices, there has been movement to trust negotiation where two entities are able to establish a measure of mutual trust, even if no prior contact between either entity has existed in the past. This chapter explores adaptive trust negotiation in a mobile environment as a means to dynamically adjust security parameters based on the level of trust established during the negotiation process thereby enhancing mobile security. To accomplish this, the chapter proposes a trust profile that contains a proof of history of successful access to sensitive data to facilitate identification and authentication for adaptive trust negotiation. The trust profile consists of a set of X.509 identity and attribute certificates, where a certificate is added whenever a user via a mobile application makes a successful attempt to request data from a server where no relationship between the user and server has previously existed as a result of trust negotiation. Our approach allows the user to collect an ever-growing amount of profile data for future adaptive trust negotiation.

INTRODUCTION

As the shift towards mobile device and application usage over traditional PCs as a dominant computing platforms occurs (Gartner, 2015), criminals are increasingly focusing on mobile devices as a means to steal data from unsuspecting users (Montopoli, 2013). Despite the surge in mobile device attacks, several industries are increasingly relying on mobile devices (West, 2012). There has been an emphasis on securing banking and financial platforms (Herzberg, 2003) with users adapting payments via mobile devices, as evidenced by Apple Pay, Google Wallet, and Samsung Pay. The ubiquity of mobile devices

DOI: 10.4018/978-1-5225-0945-5.ch005

in our daily lives has been led by the fitness and healthcare industries both for individuals monitoring their fitness activities and medical conditions such as: family members, care givers, etc.; and primary physicians, psychiatrists, on-call physicians, nurses, therapists, specialists, pharmacists, etc., seeking to access patient-collected fitness/health data in their daily activities. The healthcare industry is increasingly relying on mobile devices for quick and easy access to patient records via mHealth (Himiss, 2014) apps during treatment (Ventola, 2014) with an estimate that 80% of doctors rely on mobile devices in a report (Lewis, 2011) to access an electronic medical record (EMR) (Conn, 2014). In fact, a recent report (Aitken, n.d.) highlights 43,700+ medical apps in the Apple app store, with 69% apps targeting consumers/patients and 31% for use by medical providers. Apple has a separate category for Medical apps (iTunes, n.d.) and there has been a study comparing medical apps for both iOS and Android platforms (Seabrook, et al., 2014). Healthcare/medical apps for consumers and medical providers require a high degree of security due to the presence of protected health information (PHI) and personally identifiable information (PII).

To secure mobile devices, there has been increasing focus on *trust negotiation* (van der Horst T. W., Sundelin, Seamons, & Knutson, 2004), a procedure whereby two entities are able to establish a measure of mutual trust, even if no prior contact between either entity has existed in the past. *Adaptive trust negotiation* refers to the ability to dynamically adjust security parameters based on the level of trust established during the negotiation process. When a user via a mobile device attempts to access a server, a series of agreed upon credentials (e.g. attribute certificates) are exchanged to establish trust. The server vets the certificate, then determines if the user is trustworthy and the level of access to be allowed. Work by (Ryutov, Zhou, Neuman, Leithead, & Seamons, 2005) presents a framework for the adaptive trust negotiation process using a combination of TrustBuilder and the GAA-API (n.d.) for users to establish trust with online businesses based on the number and value of past purchases, to allow the user to make larger purchases of increasing value.

The usage of trust negotiation in healthcare information technology (HIT) systems was introduced by (Vawdrey, Sundelin, Seamons, & Knutson, 2003) and augmented by including additional assurance when accessing the EMR of a hospital (Elkhodr, Shahrestani, & Cheung, 2011) or employing trust negotiation to confirm the requestor's status as a licensed physician (Vawdrey, Sundelin, Seamons, & Knutson, 2003). One objective of this chapter is to explore the feasibility and utility of adaptive trust negotiation and its suitability for the healthcare domain, particularly for mHealth apps. Specifically, we expand existing capabilities in adaptive trust negotiation's ability to authorize users by increasing the granularity of security measures that can be utilized in an HIT system. For example, the remote server will be able to access portions of the medical provider's health record access history (i.e., a trust profile) to EMRs or other HIT systems that are exposed by the provider in the presented credentials. If the remote server grants access, the medical provider receives new identity and attribute certificates to augment the existing credentials that can be utilized as proof/history of successful access to PHI and PII for a future trust negotiation.

The adaptive trust negotiation process incorporating the trust profile in this chapter requires the user to present his/her authorizations (vetted set of credentials) to sensitive data from different systems that he/she has been successfully accessing over time. This history of user access is passed as a credential during the trust negotiation process, allowing past secure access to inform future access. A *Trust Profile* is created and modified over time to assemble a history of the successful access to serve as proof of past access to sensitive data. In support of the Trust Profile, the user has a *digital wallet* containing proof and history via new identity and attribute certificates detailing access by the user to sensitive data. A *Trust*