Mobile Application Development, Usability, and Security

Sougata Mukherjea
IBM, India

A volume in the Advances in Multimedia and Interactive Technologies (AMIT) Book Series

www.igi-global.com

Published in the United States of America by
IGI Global
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA, USA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Names: Mukherjea, Sougata, 1965- editor.
Title: Mobile application development, usability, and security / Sougata Mukherjea, editor.
Description: Hershey PA : Information Science Reference, [2017] | Series: Advances in multimedia and interactive technologies | Includes bibliographical references and index.
Identifiers: LCCN 2016033134| ISBN 9781522509455 (h/c) | ISBN 9781522509462 (eISBN)
Subjects: LCSH: Mobile apps. | Application software--Development--Management. | Application program interfaces (Computer software)
Classification: LCC QA76.76.A65 M596 2017 | DDC 005.35--dc23 LC record available at https://lccn.loc.gov/2016033134

This book is published in the IGI Global book series Advances in Multimedia and Interactive Technologies (AMIT) (ISSN: 2327-929X; eISSN: 2327-9303)

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

For electronic access to this publication, please contact: eresources@igi-global.com.

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*

Profile is a subset of the user's digital wallet that can change based on a user's location and the type of data the user is attempting to access. The Trust Profile is independent of any particular mobile device and travels with the user and changes in response to the user's attempts to access sensitive data on multiple systems at different locations over time. From a practical perspective, the Trust Profile consists of a set of identity and attribute certificates, where a certificate is added to the trust profile 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 independent of the domain. These certificates adhere to the X.509 (n.d.) standard for identity and attribute certificates. Consider a physician utilizing a mHealth app for accessing patient data: from an EMR at the physician's primary practice, from an EMR that the physician utilizes when he spends one day at a local city clinic, from an EMR that is in a hospital where a physician sees his patients, etc. Since all of these various accesses to patient data are on different EMRs, the physician's Trust Profile is constantly updated to record a history of the successful PHI accesses.

The Trust Profile is stored in a form that is presentable on behalf of the user to other, unrelated systems with similar sensitive data that the user is interested in gaining access (to which he/she has not been previously explicitly authorized to). The Trust Profile is compatible with mobile devices and allows a user to make requests to new, previously unknown systems. Additionally, the Trust Profile submitted by a user (the requestor) must be supported by an adaptive trust infrastructure via a set of interacting components including: a component to verify the structure and content of a Trust Profile; a component to determine the authenticity of the Trust Profile with respect to the user/credentials; a component to match the Trust Profile against a defined security policy of the receiving system; a component to deliver the sensitive data from the source to the requestor; and, a component to generate/add a record of the transaction to the Trust Profile. A presented Trust Profile contains credentials and the degree of access (create, read, update, and delete) which will be allowed to the requestor. To demonstrate the feasibility of our work, we utilize the Connecticut Concussion Tracker (CT^2) mHealth app, a joint effort between the Departments of Physiology and Neurobiology, and Computer Science & Engineering at the University of Connecticut, in collaboration with faculty in the Schools of Nursing and Medicine. CT^2 was developed in support of a newly passed law on concussions to be tracked for kindergarten through high school in Connecticut (State of Connecticut, n.d.).

This chapter contains 5 sections. The *Background* section discusses the healthcare domain and adaptive trust negotiation in conventional and mobile computing. The *Trust Profiling for Adaptive Trust Negotiation* section defines and explains our approach to Trust Profiles that extends adaptive trust negotiation for supporting mobile devices/applications. Next, the *Design and Prototyping of Trust Profiles* section implements the capabilities of Trust Profiles through an extension to the mHealth CT^2 app in support of an adaptive trust negotiation process that has been added to the CT^2 server. Then, the *Future Trends* section explores the areas of single sign-on (SSO) (Yu, Wang, & Mu, 2012), biometrics (Biometrics, n.d.), spatio-temporal access control (Ray & Toahchoodee, 2007), and their impact on securing mobile authentication procedures. Finally, the *Conclusion* section highlights the chapter contributions.

BACKGROUND

Background for the chapter is divided into five areas via examples in healthcare: *role-based access control (RBAC)* to identify the user by role and the nature of accessible sensitive data; *identity certificates* as a set of credentials he/she has accumulated from accessing sensitive data; *attribute certificates* that

encode user credentials in a verifiable and claimable format; *trust agents* that offload computationally intensive operations from the mobile device to an external server; and, related trust models.

RBAC provides a set of permissions, roles, and users (Ferraiolo, Sandhu, Gavrila, Kuhn, & Chandramou, 2001). Permissions are a set of actions that one may take in regards to objects (data) with operations to create, read, update, and/or delete data. In healthcare, these permissions involve reading a patient's medical data, inserting new records into a patient's history, or reading a patient's insurance information with roles for nurses, physicians, billing staff, or secretaries. Each role contains only the permissions necessary to perform the associated job, e.g., an employee attempting to access billing data under the doctor role would not have the proper permission and would be denied access. Each user of the system is assigned one or many roles, but is limited to one role for any session. One major extension to RBAC provides functionality for role delegation (Na & Cheon, 2000), where the owner of a role may receive the ability to permit another user to act in their stead with respect to a subset of their permissions. RBAC has been a popular choice for access control within HIT systems (Fernández-Alemán, Señor, Lozoya, & Toval, 2013).

Identity certificates (Housley, Polk, Ford, & Solo, 2002) uniquely identify the certificate owner through cryptographic means in a public key infrastructure (PKI) using the X.509 standard. In PKI, a certificate authority (CA) disseminates an identity certificate to a user after he/she first proves their identity through traditional means (e.g., driver's license, birth certificate, passport, email from administrator of owned domain, etc.). The CA provides a cryptographic signature on the certificate that indicates that they endorse the user's claim to that identity and that the contents of the certificate have not been altered since the signature was created. If the certificate is verified, the system performing verification accepts the identity certificate if the system trusts the CA that signed it. The user's ownership of the certificate is proved via public/private key cryptography. The user's public key is listed within the certificate while the private key is kept secret by the user. To provide proof of ownership, the user can decrypt messages encrypted with his/her public key and provide responses encrypted with the private key that the associated public key is able to decrypt. In this chapter, the identity certificate can uniquely identify unknown entities and confirm that the unknown holder is in fact a member of the medical community. This virtual identity is utilized as an anchor point for a verifiable medical record access record history as credentials in the trust negotiation process.

Attribute certificates (Farrell & Housley, 2002) store data in a key-value pair format and are associated with an identity certificate through its serial number, which is unique inside the signing organization (the issuer), and the issuer. The attribute certificate is signed by an attribute authority (AA) in a manner similar to an identity certificate. An identity certificate may have one or more attribute certificates associated with it, but each attribute certificate is associated with one identity certificate. Similar to the identity certificate, the information within an attribute certificate contains a digital signature computed at the time of creation by the AA. During certificate verification, if the signature on the attribute certificate is found to be valid, the information within is trusted if the AA is trusted. The separation between the identity certificate and attribute certificate facilitates the addition of information that augments the identity of the holder without requiring reverification of the holder's identity. A more specialized, short-lived version of the attribute certificate referred to as the rule certificate may be generated that records the user's actual permissions on the HIT system for the current session (Mavridis, Georgiadis, Pangalos, & Khair, 2001). In healthcare, an attribute certificate might contain: role (e.g., primary physician, nurse, pharmacist, etc.), permissions (e.g., whether the holder is allowed to delegate responsibilities), or authorization (e.g., when the holder is allowed to access sensitive data).

Trust agents (van der Horst T. W., Sundelin, Seamons, & Knutson, 2005) are software components that are able to perform the trust negotiation process for others. A *local agent* runs on the device initiating or receiving a request to begin the trust negotiation process. A *remote agent* performs the same task but runs on a different device, performing the trust negotiation process on behalf of the device that desires trust. The trust negotiation process requires a substantial amount of computational power for the involved cryptographic processes. While a traditional PC's only bottleneck is the PC's ability to complete many cryptographic calculations quickly, mobile devices must be also be able to compute the calculations while maximizing battery life using less powerful CPUs. To address this issue, mobile devices can leverage surrogate trust negotiation (Sundelin, July 2003) where a trusted base station performs trust negotiation. In healthcare, a trust agent could operate as a software module running on a trust negotiation server owned by a healthcare organization that the mobile device contacts to perform the trust negotiation phase. *Generic software agents* may be used by medical servers receiving trust negotiation requests to generate new certificate-based credentials, offloading the responsibility of guarding the private key and signing certificates to a trusted third party.

Trust in this chapter represents the ability for two entities to: believe the authenticity of one another's credentials, utilize those credentials to ascertain whether each individual is entitled to privileged information, and believe that each will handle sensitive data appropriately once exchanged. Many different trust models have been proposed. (Artz & Gil, 2007) surveys a wide range of trust and trust distribution techniques, including trust in the accuracy of the information released (e.g. search engine results). The work also explores policy-based trust (users possess credentials that must be matched to security policies) and reputation-based trust (user behavior is inferred from past actions). (Sabater & Sierra, 2005) reviews different models of trust and classifies by: the conceptual model (cognitive vs. game theory); the information source (direct, witness, sociological, prejudice); the visibility type (global vs. subjective); the granularity (single context vs. multiple context); agent behavior (cheating not considered, agents can hide or bias information, agents can lie); the type of exchanged information; and the trust value. This work notes that the diversity of trust models creating trust in different domains makes it difficult to classify each model according to this criteria. As an example, our approach utilizes information sources from direct experience information, which is the access history the user presents as proof of past data access, and prejudice information, which is the role the user chooses to initiate the request. Direct experience is defined as trust values that are provided directly from the entity the user is initiating the request to, or other members of the community (other healthcare organizations). Prejudicial information is inferred based on the user's "group". For example, a hospital employee with an X-ray technician role cannot access the patient's billing data, but it can be inferred that the release of past X-ray data may be warranted if requested.

TRUST PROFILING FOR ADAPTIVE TRUST NEGOTIATION

In this section, we describe the trust profile, its usage, and the architecture required to enable adaptive trust negotiation in systems, demonstrated via the healthcare domain. In this context, trust is the ability of the two entities to believe one another, and that each will take proper responsibility in the handling of sensitive data. Companies that improperly disclose medical data stand to lose money and customers' trust. However, the proper dissemination of medical data is paramount in patient care/treatment and medical research. A *trust profile* is the entity that is constructed to support the adaptive trust negotia-

tion process by providing a set of access history-based credentials that a data requestor and data holder exchange to establish trust. In the approach detailed in this chapter, a healthcare stakeholder builds a set of credentials into a trust profile over the course of his/her medical career, allowing him/her to build trust with the various HIT systems containing the data he/she needs.

The remainder of this section introduces and explains trust profiling for adaptive trust negotiation in four parts. In part one, we overview the trust profile and the negotiation process. Next, in part two, we examine the physical structure of the trust profile and the supporting network architecture. Part three discusses the trust profile processing which is decomposed into three components (validation, security policy, and data collection and delivery) that reads the trust profile and decides whether data will be disseminated. Lastly, part four has a comprehensive healthcare example of trust profile utilization leveraging the concepts presented in the first three parts.

Trust Profile and Negotiation Process

In part one of this section of the chapter, we present the trust profile and negotiation process that requires a set of credentials that are passed between the two entities attempting to establish trust. In previous works (Elkhodr, Shahrestani, & Cheung, 2011) (Vawdrey, Sundelin, Seamons, & Knutson, 2003), the credentials are based on what the user is (e.g., physician, billing agent) whereas this work allows for more fine grained control that tunes user access by adding credentials that detail actions that the user has been allowed to take in the past (e.g., access patient A's complete medical history, access a hospital's available public health data). This allows implementations of security policies that have more options with PHI disclosure. Based on the user's access history, the system may decide to: deny access if the user does not meet basic requirements for access (such as a physician attempting to access protected mental health data); allow access but trigger an extra layer of auditing (such as an alert being issued to an auditor when an unknown E.R. doctor requests medical data regarding a patient he/she has never treated); or allow access to the data (such as in the event a doctor who is an employee of the institution is treating a patient he/she has already treated, but is currently working in a remote location).

The attribute certificate, as introduced in the background section, is a container for records of user access while the identity certificate is a unique virtual identity that the user can claim ownership of. A user presents identity and attribute certificates that encode the trust profile, readable by the trust negotiation server of the HIT system (e.g., EMR), along with a request for the exact data needed. The HIT system's trust negotiation server determines certificate authenticity and ownership using PKI, then extracts the medical record access history of the user from the attribute certificate. The HIT system's trust negotiation server decides the level of access the user is allowed and generates new certificates that detail which records the user is allowed to access. The security policy reacts to the request dynamically and adjusts which credentials are required. For instance, a family physician requesting updates on his/her patient's medical record from other medical stakeholders (e.g., OB/GYN, podiatrist, dentist, cardiologist, etc.) that the patient has recently seen for treatment would be expected to present a medical record access history indicating that he/she has successfully authenticated and been granted access to the patient's medical history in the past.

Each stakeholder (e.g., primary physicians, psychiatrists, on-call physicians, nurses, therapists, specialists, pharmacists, etc.) in the healthcare domain that is expected to require access to secure HIT systems is granted the ability to build and maintain a trust profile. An initial trust profile is granted by the healthcare institution that employs the stakeholder, thus endorsing the professional's status as a trusted

member of the medical community. Should the stakeholder leave the healthcare institution, his/her trust profile remains valid and moves with him/her as a permanent record of the access afforded to him/her by the institution. When joining a new healthcare institution with its own EMR, the stakeholder is granted additions to the trust profile indicating that this new institution also endorses his/her trustworthiness and begins recording requests for access into the trust profile. Additionally, when requesting medical data from HIT systems of healthcare institutions where there is no preexisting relationship between the owner of the system and the person requesting access, in the event that the trust negotiation phase is successful, the HIT system adds its own entries to the user's trust profile. This behavior allows practicing stakeholders to gradually build a permanent trust profile over the course of his/her medical career with trust endorsements from many different institutions that demonstrates a history of successful access of sensitive data in varied HIT systems. In the event that the physician requires access to medical data from an unknown healthcare institution, the physician can use this trust profile to obtain assurance that he/she is trusted by trustworthy entities.

Trust Profile Structure

In part two of this section of the chapter, we describe the trust profile's structure. The structure of the trust profile is a series of identity and attribute certificates which together form the physician's digital wallet. When a user is successful in trust negotiation with an unknown HIT system, the system requests a new public key from the user and generates an identity certificate that is utilized in future communication with the server. The server also generates and signs an attribute certificate containing records of access that is attached to the identity certificate. Thus, the user has verifiable proof of access to these records that can be utilized as credentials in attempts to access healthcare data residing at other healthcare organizations. In the case of mobile devices, the certificates may be stored locally on the device, or stored with a remote agent that can perform the trust negotiation procedure and generate the necessary public-private key pairs on behalf of the mobile device. A *medical authority*, similar to the certificate authority described in the *Background* section, is responsible for verifying that the HIT systems are certified, maintained by licensed healthcare providers, and proper security procedures are followed on the certificate processing and signing servers. Medical authorities establish trust between the healthcare organizations' HIT systems that endorse the trust profiles of those who have been allowed access to patient records as shown in Figure 2. Mutual trust must be established between the HIT systems through medical authorities to enable the trust negotiation process; in order for the HIT systems to trust the authenticity of the user's trust profile, the HIT system that signed it must be trusted.

While a later section of the chapter provides a detailed real-world example, for the reader to be able to understand the concepts in the rest of this section, a brief example is provided. To begin, a sample Physician Trust Profile is shown in Figure 1. The Physician has multiple roles (Physician that sees patients at the Family Health Center, Researcher and Professor at the UConn Health Center (UCHC) that includes the medical school, and Radiologist at St. Francis hospital that assesses imaging tests) that generate appropriate attribute certificates that are associated with X.509 certificates issued by the aforementioned health organizations. Note that each X.509 certificate in Figure 1 has one or more attribute certificates that represent the role of the user within the organization (e.g., UCHC has two attribute certificates for the roles Research and Professor). The Physician presents his trust profile containing the multiple certificates to a new health organization (Hartford Hospital) that he needs to have access to for treating one of his patients at St. Francis Hospital. Now suppose that a physician attempts to access a patient's health

Figure 1. A sample physician trust profile

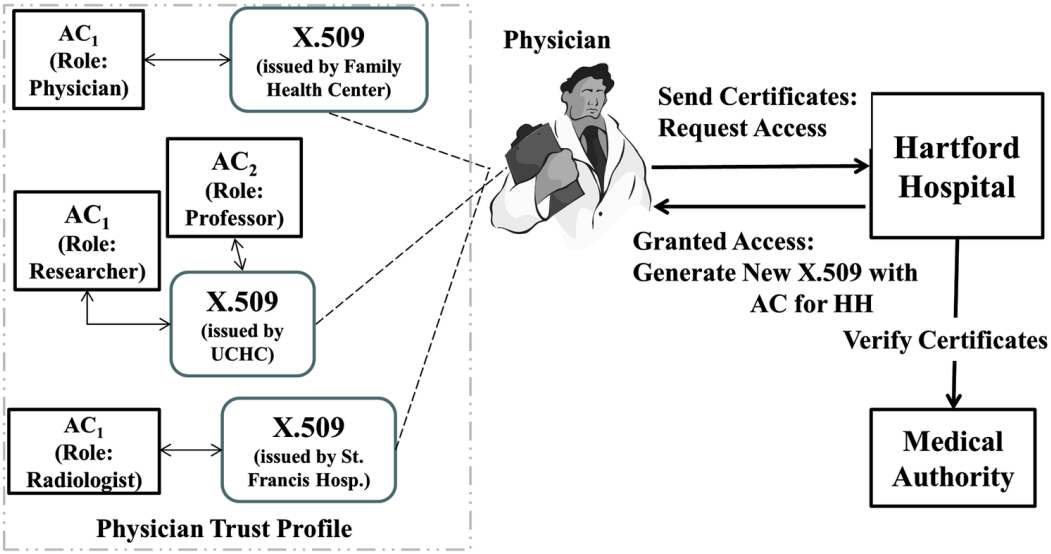
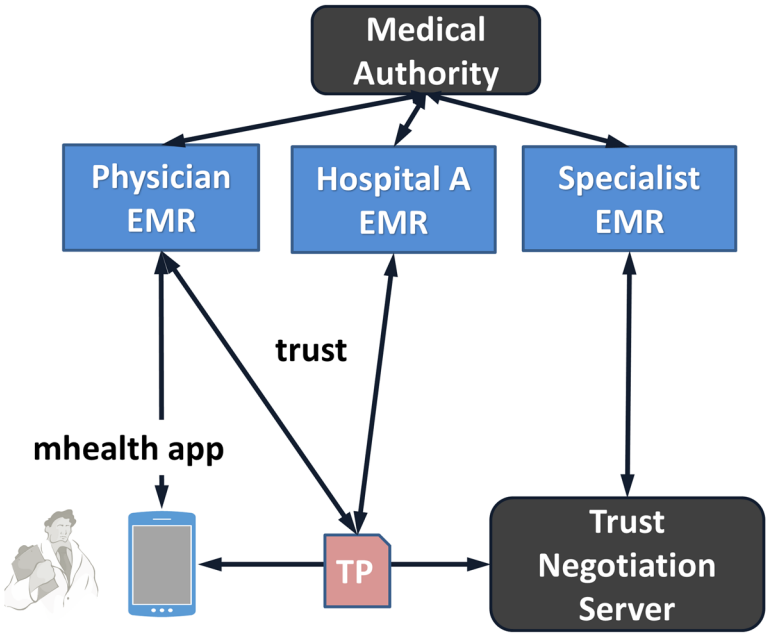


Figure 2. Trust profile process



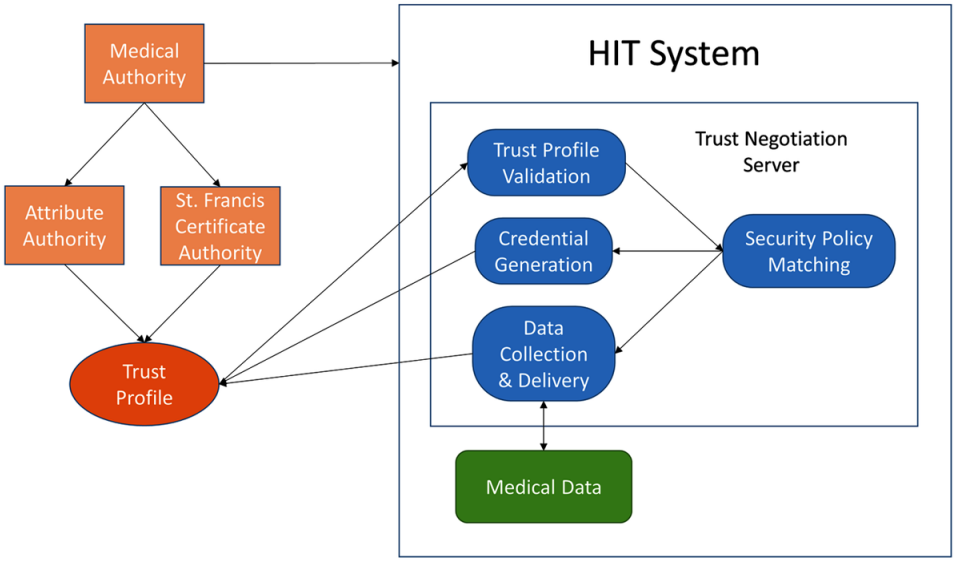
data in the EMR at his/her local practice using a mobile health (mHealth) application on his/her mobile device and discovers that the patient has recently visited an unknown specialist for a related condition; this is shown in Figure 2. In such a situation, the mHealth application used by the physician will present his/her trust profile to the specialist's EMR through a remote agent running on a trust negotiation server maintained by his/her hospital. The physician's trust profile details: previously successful attempts of

the physician accessing patient data at his/her local EMR; and, patient data the physician has previously accessed from other specialists. The trust negotiation server for the specialist's EMR will read the presented trust profile, determine its legitimacy, decide the level of access to be authorized to the physician, and determine which additional actions the system must execute to ensure data integrity and security. If the attempt at access is successful, the specialist's server automatically returns to the physician a new set of digital credentials that the physician can add to his/her Trust Profile.

Trust Profile Process

In part three of this section of the chapter, the *trust profile process* is presented by explaining its three components as shown in Figure 3: *validation* to ensure that the credentials within the user's certificates are correct and have not been modified; *security policy* to enforce a set of requirements on the presented credentials; and, *data collection and delivery* to retrieve the PHI data and transfer it securely to the user. When a physician is attempting to access information from multiple HIT systems (EMRs), in order to identify the correct location(s), a medical record discovery service such as a master patient index (MPI) is utilized. MPI is a uniform index that is able to cross reference a patient's medical data that is stored in multiple HIT systems (EMRs) in support of health information exchange (HIE) (HIS, n.d.). The physician sends a request for healthcare data and an appropriate subset of his/her trust profile. Recall from Figure 2, the physician is attempting to obtain a copy of his/her patient's medical records at a specialist's office EMR, where his/her trust profile provides proof that he/she has treated this patient before by showcasing successful authorizations to the patient's data in the Family Medical Center and St. Francis Hospital EMRs. The HIT system (specialist's office EMR) receives the trust profile and passes it to the healthcare organization's trust negotiation server, which completes trust profile processing and adaptive trust negotiation on its behalf.

Figure 3. Trust components and their interdependencies



The trust negotiation server's *validation component* as shown in the upper middle of Figure 3 is responsible for performing analysis on the presented trust profile and determining its authenticity. The *validation component* begins by checking the user's identity certificates for validity; verifying that the certificate has not been altered and checking that the signer is trusted. A challenge is sent to the physician's trust agent utilizing public key cryptography to prove that the physician is the rightful owner of the record. A successful response indicates that the physician is the rightful owner of the identity certificate and thus the trust profile specified in the associated attribute certificates. The associated attribute certificates are checked to ensure that they have not been altered, and that the associated attribute authority (AA) is trusted. The trust negotiation component now knows that: the trust profile is valid, the information contained within is trustworthy, and the user responsible for initiating the connection is the rightful claimant to the presented trust profile. The healthcare data request (to an EMR) and the information within the attribute certificate are extracted and sent to another subcomponent of the trust negotiation component that matches the trust profile to a security policy.

The *security policy component* as shown on the right of Figure 3 receives the user's request and the extracted attributes from the validation component. The security policy contains all rules that govern the security policy component's responses to the requestor. The security policy component matches the trust profile against the policy and decides the requestor's level of access to the data and which other necessary actions the HIT system will undertake to ensure data security. The enacted policy differs depending on the nature of the request and other attributes present in the trust profile. For example, a physician working in the E.R. requesting data to treat a patient that arrived from an automobile accident would cause the HIT system to enact a policy that requires indications that the physician has accessed data under the role of an E.R. physician, but the requirement that the physician has treated the patient before is relaxed (since it is likely the patient has not been treated by that E.R. physician previously). Since there is no indication in the trust profile that the physician has treated this patient previously, the security policy component would dispatch an audit notification to an auditor for later verification. Once the security policy component has completed this process, the request is passed to the data collection and delivery component in the bottom of Figure 3. However, if the user's credentials do not match the security policy, the trust negotiation server sends a message to the user stating that the request is denied.

The *data collection and delivery component* shown in the bottom middle of Figure 3 is only enabled in the case when a user is successful in the trust negotiation process. The data collection and delivery component is responsible for: creating a secure record of the transaction for the user to add to his/her digital wallet, collecting the requested medical data, performing any additional actions required by the security policy, and securely delivering the requested data to the user as shown in Figure 3. If the user does not possess an identity certificate from this institution, the component requests a public key from the user. The user generates a public-private key pair, using a remote agent, from his/her mobile device and sends the public key to the server. The trust negotiation server creates a certificate signing request and forwards it to the institution's certificate authority (CA), as shown in Figure 2. The data collection and delivery component utilizes the institution's AA to create an attribute certificate that encodes records of access for the data that is to be sent the user, e.g., this would be creating the attribute certificate for Hartford Hospital from Figure 1 or for the request to the Specialist EMR in Figure 2. This process is represented by the credential generation in the middle of Figure 3. The component collects the requested healthcare data from the institution's HIT system, e.g., a specific EMR at an institution. This data may reside in a data warehouse, the institution's EMR, or a separate staging server for shareable medical data. The generated certificates and data are transferred to the user. When the transfer has completed

the connection may be terminated. The user then adds the certificates to the digital wallet and is able to read the medical data.

At any point during this process, the data collection and delivery component may be required to perform some ancillary action as required by the security policy. As healthcare data is protected by laws such as HIPAA and hospitals have significant financial investment in the generation of medical data (through MRIs, X-rays, or other analysis), the ability to fine-tune how an HIT system responds to a request for healthcare data is required. The security policy may require logging the transaction in a low risk audit log, in a high risk audit log, or dispatching a notification that a high risk transaction has occurred. As audit logs tend to be large and difficult to review (AHIMA, 2011), this ability working in tandem with a multi-level auditing system greatly assists in discovering and performing actions regarding mishandled data.

Healthcare Example

In this section, we present a comprehensive healthcare example in trust profiling and negotiation, shown in Figure 4. Suppose that Jane with a physician role is working at Family Medicine Center (FMC) and St. Francis Hospital (SFH). Jane has received one identity certificate from FMC where she works in ambulatory care, and one identity certificate from SFH where she works as a practicing physician. Jane also possesses attribute certificates for the physician role under each identity certificate. Note that these different certificates are shown in the upper portion of Figure 5 in Jane's current trust profile (smaller dashed box). Since Jane is known as a physician at both FMC and SFH, her access to the EMR of each is unrestricted, with improper access being determined through audits of the EMR's data access logs. Over the course of Jane's career at these healthcare organizations, she accesses PHI from the EMR of each organization utilizing a mHealth application provided for her appointments with patients, and each access is recorded in her trust profile, encoded in attribute certificates attached to the appropriate identity certificate, which travels with Jane to each organization.

Figure 4. The trust profile pre-negotiation process for Jane with Hartford Hospital

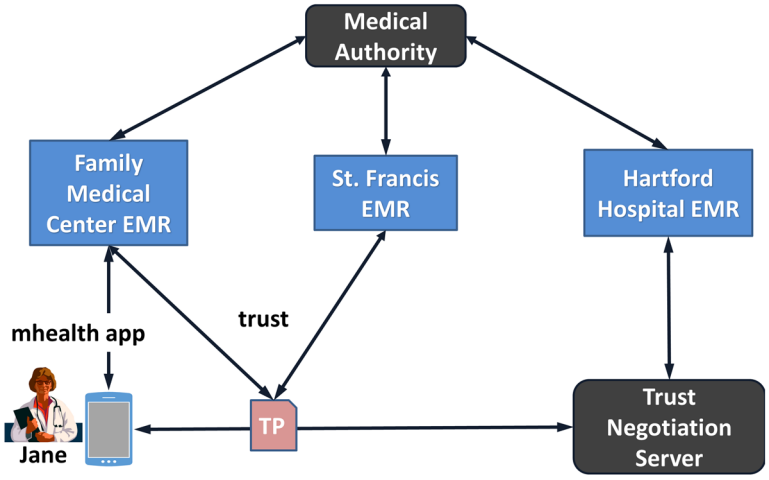
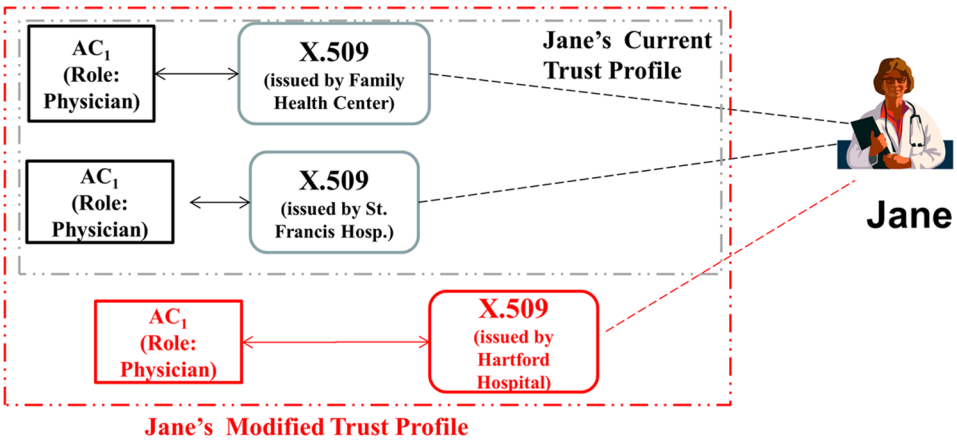


Figure 5. The trust profile post-negotiation process for Jane with Hartford Hospital



Jane is treating a patient that she has seen previously at FMC. The patient has recently received cardiology treatment from The Henry Low Heart Center at Hartford Hospital (HH). HH has never had previous contact with Jane, and Jane has never had previous contact with HH. Jane locates the patient's new PHI through a MPI and determines that she needs access to her patient's records in the EMR at HH to treat the patient. Through her mHealth application, a request for trust negotiation is initialized to HH's HIT system for data regarding the patient's cardiology treatment including medical notes by the treating physician and tests such as electrocardiograms or cardiac ultrasounds. The identity of the EMR is verified as belonging to HH through a TLS/SSL verification of its X.509 certificate and the medical authority's certificate. Jane selects portions of her trust profile indicating that she: has successfully accessed the patient's health data from FMC's EMR, is affiliated with SFH, and has a long history of accessing data in St. Francis' EMR utilizing a mHealth application,. The mHealth application selects the certificates within Jane's digital wallet that contain records of the selected history in the trust profile and sends them to HH's EMR.

HH's EMR receives the certificates and forwards them and the request to its trust negotiation server. At this point, the process completes the actions of the validation component (prior section and Figure 3) which requests proof of ownership to Jane, which is forwarded to Jane's trust agent. The validation component successfully reads the messages and completes the validation process by extracting the trust profile from the attribute certificates and passes the trust profile to the security component. In the next step, the security component reads the request and determines that to release the requested data, the trust profile must contain at least one record of the owner in a physician, specialist, or nursing role; Jane has physician role usage for FMC and SFC EMRs. Additionally, if the trust profile indicates that the owner has accessed the patient's medical data elsewhere, the transaction will be marked as low risk and recorded in a low risk audit log; Jane has accessed the patient's data in the FMC EMR. Conversely, if there is no indication of patient treatment by Jane, the transaction will be marked as high risk, recorded in a high risk audit log, and an e-mail will be sent to HH's auditor. A subsequent check will be initiated to see if there is any other evidence that would warrant granting Jane access, e.g., the trust profile indicates that the Jane has accessed health records under her physician role, including health records for many other

patients in two EMRs. In this case, the security component could decide that this is sufficient evidence to allow Jane to have access to the HH EMR for the patient whose data is being requested.

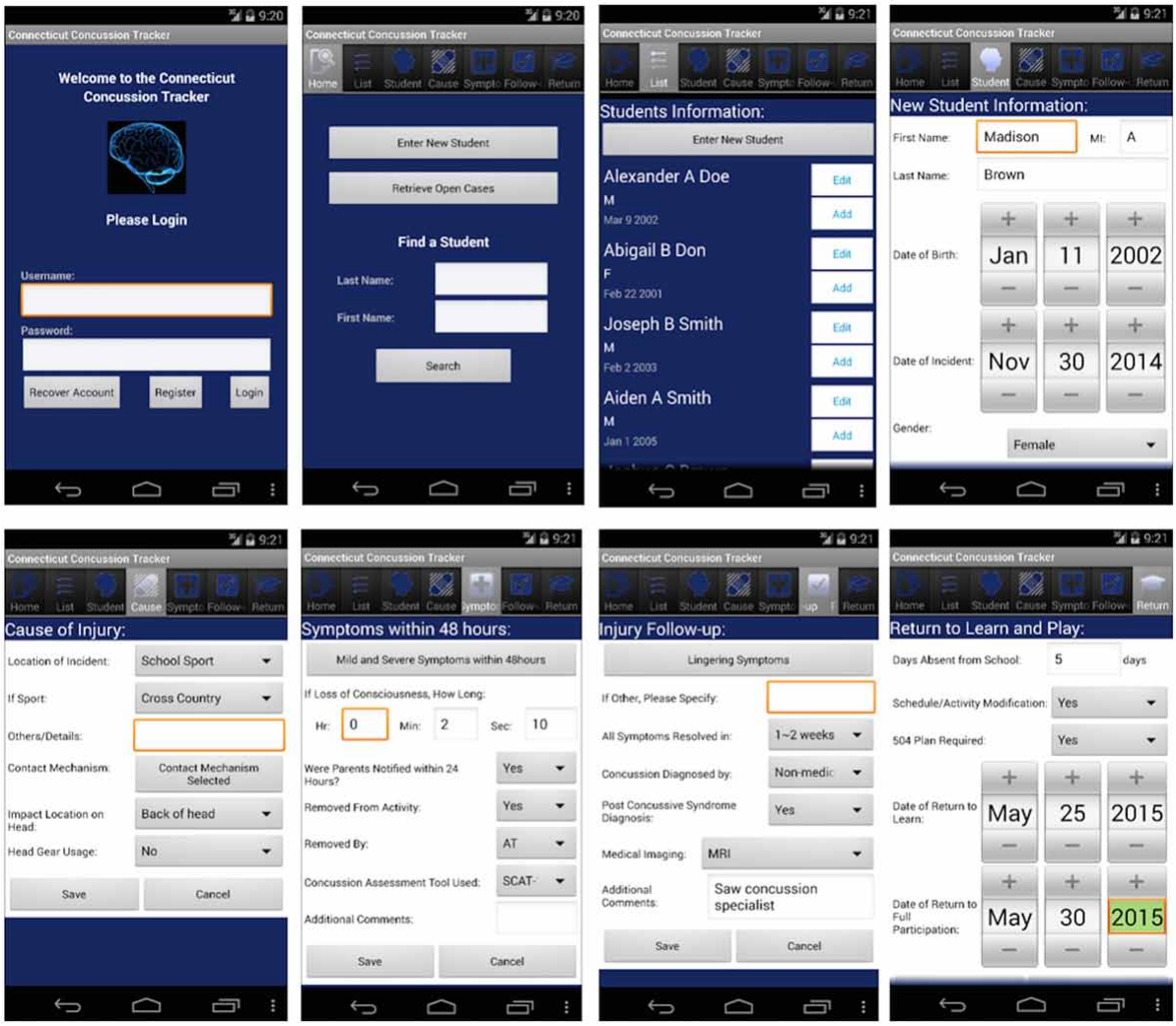
In the final step, the data collection and delivery component creates a record of access granted to the HH EMR during the trust negotiation process. Since this is the first request for access by Jane to the HH's EMR, the data collection and delivery component requests a public key from Jane. Jane's mobile device sends a request to the trust agent to generate a new public/private key pair and sends the public key to the data collection and delivery component, which creates a certificate signing request for a new X.509 identity certificate for HH for Jane and sends it to the local CA for signing. The new certificate is shown in the bottom portion of Figure 5 with the larger dashed box that includes the current and new certificates. The private key is added to Jane's digital wallet. The records of access for the data requested by Jane are encoded in attribute certificates signed by the AA, attached to the newly generated identity certificate, and are sent to Jane at which point she adds the certificates describing this new entry to her trust profile and digital wallet. In parallel, the data collection and delivery component contacts the HIT system (HH EMR), gathers the requested data, and sends the requested data and generated certificates back to Jane. Jane now possesses the requested data and the certificates detailing the access she has gained to HH's EMR. The identity and attribute certificates are added to Jane's trust profile, which now contains proof of access to EMRs owned by FMC, SFH, and the newly approved HH. In future requests for data through trust negotiation, Jane is able to present this new certificate as a credential.

DESIGN AND PROTOTYPING OF TRUST PROFILES

The trust profile functionality as presented in this chapter has been integrated into the Connecticut Concussion Tracker (CT^2) mHealth Android app as a proof of concept prototype. CT^2 tracks concussions for grades kindergarten through high school and is a collaboration between the Departments of Physiology and Neurobiology, and Computer Science & Engineering at the University of Connecticut and Schools of Nursing and Medicine. The CT^2 mHealth app shown in Figure 6 contains the login screen (first screenshot) and additional screens: find students (Home tab), all students are assigned to a user (List tab), add a new concussion incident (Student tab), enter information on the concussion (Cause tab), enter student symptoms within 48 hour (Symptom tab), record the status of the student over time (Follow-up tab), and indicate when student can return to various activities at school (Return tab).

The data collected by the CT2 mHealth app is stored in a remote server running a custom MySQL database that contains tables for: student records, records of a student's concussion incident, the school, symptoms of the concussion incident, follow-up information, and records for when the user is allowed to participate in activities. The server provides outside access to the database through a REST API written in PHP using Slim. To demonstrate the trust process, the installation has been augmented with a trust negotiation agent that accepts trust negotiation requests and performs the required certificate validation checks. Once the user's credentials sent by the CT2 mHealth app are accepted, the trust negotiation agent passes new test certificates back to the user, which the user has the option of adding to his/her certificate store, expanding his/her trust profile. The initial screen of CT2 mHealth (Figure 6) has been upgraded to support the adaptive trust process in the 1st screen in Figure 7.

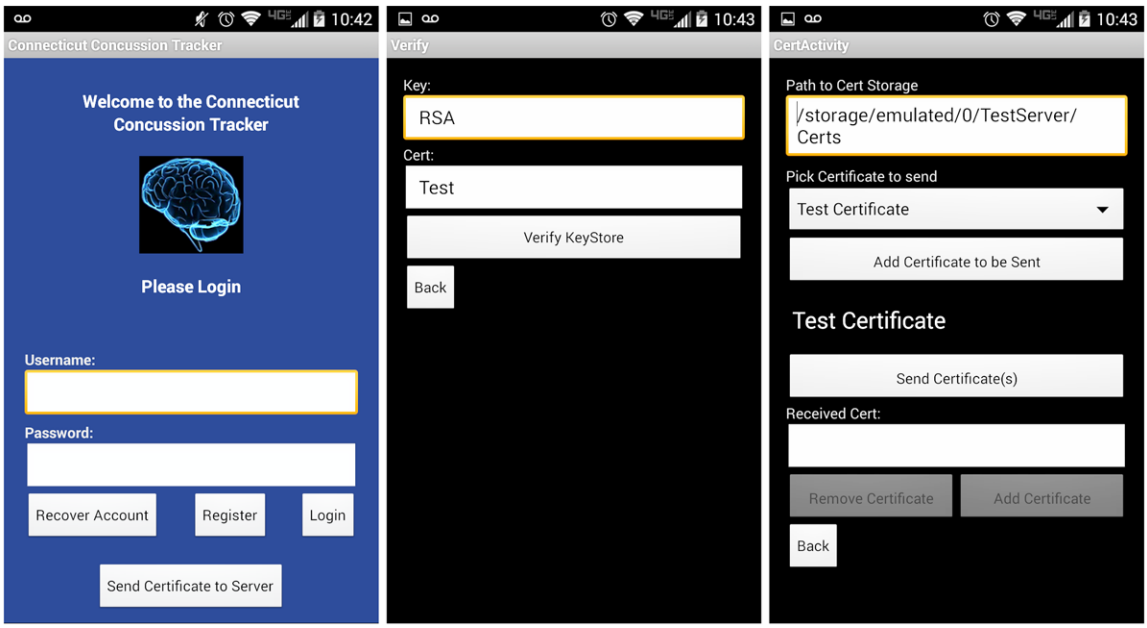
Figure 6. Select screens Connecticut concussion tracker (CT^2) app



The prototype trust profile has been developed as a series of attribute certificates attached to an identity certificate. The trust profile contains verifiable information (provided by the certificate signers) related to the specific concussion records the user has accessed in the past and the circumstances regarding access. The access records contain information on:

- The user's role (for CT^2 roles include Nurse, Athletic Trainer, Coach, and Parent).
- The user's action in regards to the data (for CT^2 read a concussion record, create a concussion record, edit a concussion record, etc.).
- The id of the specific record that was requested by/sent to the user (for CT^2, the concussion id of the record).

Figure 7. Trust negotiation screens in the modified CT² app



- The specific individual that that record is referring and the user's reason for access (for CT², the student id associated with the concussion id along with an action such as add a new symptom that showed up 48 hours or later).
- A timestamp detailing the time of access.

When the trust negotiation portion of the app is first run, the app generates necessary folder structures to hold the user's data (for CT2, a user with a role of Nurse, Coach, etc.). Within the prototype, the user's certificates reside on the mobile device in a KeyStore folder that the app reads during the credential selection phase. The trust negotiation agent is verified using standard SSL over an HTTPS connection. A successful connection indicates that the user has connected to the proper trust negotiation server. Certificates that a mobile device utilizes for verification of the trust negotiation agent are placed in a Trusted folder on the device rather than as a regular certificate on the device through the settings menu. When the trust negotiation component of the CT² mHealth app is first executed, the user has the option of creating a test public/private key pair and initial identity certificate for the trust negotiation process. These certificates are stored within the app folder in the KeyStore folder. Any new certificates created during the trust negotiation process and sent back to the user are processed by the mobile device and placed in a Certificates folder. The concussion data is received by the mobile app, processed, and displayed on the screens presented in Figure 6.

The CT² mHealth home screen shown in Figure 6 (1st screen, 1st row) provides options for a username/password combination, an account recovery option, and a login button. A user has been assigned a specific role (e.g., Nurse, Coach, etc.) that adjusts which screens in Figure 6 are available and whether or not a screen can be read or read/edited. In support of adaptive trust negotiation, the modified CT² mHealth app login screen in Figure 7 (1st screen) has a Send Certificate to Server button which sends the user with a given role to the first trust negotiation screen that verifies the user's trust store. The

validation process (see Figure 3 again) begins by testing for the existence of a public/private key pair owned by the user and the presence of a properly formatted public key certificate. If these two elements are not found on the device, the modified CT^2 mHealth app offers to create a test public/private key pair and a test certificate for the user, shown in screen 2 of Figure 7. If the public/private key pair and associated identity certificate are both present, the verification process checks for proper formatting of the certificate and the encryption keys to ensure that they are the proper format.

Once the personal keystore is verified, the CT^2 mHealth app continues on to screen 3 in Figure 7 where the user is able to select his/her preinstalled certificates (if no certificates were installed, then only the default test certificate is available). The user selects one or more certificates to be sent to the trust negotiation server from a dropdown box labeled "Pick Certificate to send". Once the user has selected the certificates, he/she presses the Send Certificate(s) button and the certificates are uploaded. This send command is transmitted to our trust negotiation server to proceed through the validation, security policy, and, data collection and delivery components shown in Figure 3. Upon completion, the server issues a new certificate to the mobile device. The app receives the new certificate and displays it in the Received Cert: box in Figure 7. The user can then decide to remove the certificate, or add it to his/her digital wallet for future trust negotiation attempts. Note that the changes that have been made to the CT^2 mHealth app are at a programmatic level; we had the available Android app code and server/MySQL that allowed us to make these changes. We are currently exploring a way to encapsulate our adaptive trust negotiation via trust profiles into a device level app that can easily be referenced and used by others apps that require only minimal changes.

The addition of a trust negotiation feature to this mHealth app greatly simplifies the process of obtaining or adding patient data to the CT^2 database. This allows users to access concussion information or insert relevant concussion data without the need for a lengthy pre-registration process. Since the app is intended to be used by many stakeholders across the state, including school teachers and coaches, the reduction in the amount of necessary account registrations will result in decreased work for system administrators and increased access to the app's features. The manual selection of certificates works well when the user access history is small, but as the user adds to the trust profile, it quickly becomes difficult to manage and choose the best set of credentials. A search filter could improve the user's ability to find credentials that match the server's policy. Additionally, support for credential access policies (Winsborough, Seamons, & Jones, 2000) could be extended to the trust profile and incorporated into the app. Credential access policies allow the user to specify the conditions under which a credential can be released. For instance, the user can specify that the five latest records in the trust profile that match the intended request as closely as possible (student, role under which data was accessed, etc.) are to be released. This would automate the process of credential selection, enabling the creation of an ever-growing trust profile without requiring the user to manage it directly during trust negotiation.

FUTURE TRENDS

In this section, we explore three future trends that have the potential to augment trust negotiation: *spatio-temporal access control* where a user's permissions are restricted based on his/her geographic location and time; *biometrics* that utilizes a user's unique biological data to determine identity; and *single sign-on (SSO)* to manage multiple virtual identities.

Spatio-temporal access control is an access control model where user permissions change as the user moves to different geographic locations at different times. For example, if a user moves from the Family Medical Center to St. Francis Hospital (see Figure 1 again), the permissions of the user would change from patient data in the EMR at the center to the EMR at St. Francis. Similarly, if the device were to leave the premises entirely, the device would lack the permissions to access the EMR. Location-based access control as an extension to RBAC in (Bertino, Catania, & Damiani, 2005) is combined with the user's login information to determine the time that a user is working. The user is only able to log in successfully if he/she is scheduled to work at the time of the request for data access. Both of these types of access control could be integrated into the trust profile to enhance the owner's credentials and automate the credential selection process. When the physician moves to St. Francis, the owner will be able to present those portions of the trust profile that demonstrate the physician's history of accessing patient data at Family Medical Center.

Biometrics are being integrated with mobile devices for unique identification via: fingerprint scans, retina scans, gait recognition (Mantyjarvi, Lindholm, Vildjiounaite, Makela, & Ailisto, 2005), touch patterns on a smartphone display (Xu, Zhou, & Lyu, 2014), knuckle patterns, accelerometer data, keystrokes (Hwang, Cho, & Park, 2009), and voice recognition (Baloul, Cherrier, & Rosenberger, 2012). A user must register his/her biometrics in advance before he/she can be authenticated. Biometric authentication introduces new issues should the user's biometrics become unavailable in the event of extensive injury or are stolen (Nexus, n.d.; CNN Money, 2015). Cancelable biometrics (Ratha, Connell, & Bolle, 2001) secures biometric data servers against attacks for users' biometric data by allowing users to revoke old biometric data and create new biometric data in the event that the server is compromised. This work has been extended to fingerprints (Ratha N., Connell, Bolle, & Chikkerur, 2006) and irises (Zuo, Ratha, & Connell, 2008) (Pillai, Patel, Chellappa, & Ratha, 2010). Biometrics may be used to provide additional assurance of identity during the trust negotiation process by acting as a passphrase to unlock the user's private keys.

*Single sign-on*enables a user to log in to multiple services with one log in without the difficulty of needing to remember multiple complex passwords from multiple services. During an SSO log in attempt, the user must authenticate with an SSO service, usually with a username/password combination. The SSO validates the user's identity and automatically logs him/her in to services where the user has authorized the SSO to manage account credentials on his/her behalf. Kerberos (Neuman & Ts'o, 1994) and Shibboleth are popular SSO systems utilized for log in to multiple servers in distributed systems. True SSO (Pashalidis & Mitchell, 2003) allows a many-to-many association between owned user identities and authenticated services. The multiple identities granted by a True SSO are useful for situations such as online shopping, where online stores may track user purchases that the user has purchased as a gift for someone else and adjust targeted ads accordingly. The True SSO multiple identity approach is akin to our digital wallet approach where a user obtains multiple identities from various healthcare organizations for use in authentication. There is current research in adapting SSO to healthcare such as (Heckle, Lutters, & Gurzick, 2008) that presented findings on the reaction of staff to the introduction of an SSO system in a hospital and (Mauro, Sunyaev, Leimeister, Schweiger, & Krcmar, 2008) that described a system to manage doctors' smart cards. SSO can simplify trust negotiation by performing the trust negotiation process as a trusted third party on behalf of the entities the user is attempting access resulting in a token the user can then present as credentials to the HIT systems he/she is attempting to access.

CONCLUSION

This chapter has presented *adaptive trust negotiation* in a mobile context and incorporated the concept of a *trust profile*. The *trust profile* provides detailed credentials that allows IT staff to create fine grained, adaptive security that can react dynamically via adaptive trust negotiation to protect sensitive data while still allowing data to be safely disseminated to legitimate users. Rather than basing the required credentials on what a user *is* (e.g., physician, nurse, psychiatrist), by knowing the actions that the user has been authorized to make, new organizations can better ascertain the user's level of trustworthiness and adjust its security policies accordingly in a dynamic fashion. The *Background* section briefly reviewed role-based access control, (the type of access a user may be allowed), identity certificates (a set of *trust profile* credentials), attribute certificates (to encode *trust profile* credentials in an endorsable format), and trust agents (to offload intensive cryptographic calculations to a more powerful server). The *Trust Profiling for Adaptive Trust Negotiation Section* described the trust profile in four parts: a general overview of the trust profile and its use in creating trust, the physical structure of the trust profile, a method for processing the trust profile in order to validate and extract the credentials contained within, and a healthcare example that describes the trust negotiation process and trust profile utilization. In *Design and Prototyping of Trust Profiles*, a prototype of our approach to trust negotiation in healthcare incorporated into the CT^2 concussion tracking mHealth app was presented. To complete the chapter, the *Future Trends* section discussed emerging trends in healthcare authentication and information exchange including: spatio-temporal access control, biometrics, and single sign-on.

REFERENCES

AHIMA. (2011, March). Security Audits of Electronic Health Information (Updated). *Journal of American Health Information Management Association*, *82*(3), 45–50.

Aitken, M. (n.d.). *Patient Apps for Improved Healthcare: From Novelty to Mainstream*. Retrieved from http://www.imshealth.com/portal/site/imshealth/menuitem.762a961826aad98f53c753c71ad8c22a/?vgnextoid=e0f913850c8b1410VgnVCM10000076192ca2RCRD

Artz, D., & Gil, Y. (2007, June). A Survey of Trust in Computer Science and the Semantic Web. *Journal of Web Semantics*, *5*(2), 58–71. doi:10.1016/j.websem.2007.03.002

Baloul, M., Cherrier, E., & Rosenberger, C. (2012). Challenge-based speaker recognition for mobile authentication. *2012 BIOSIG - Proceedings of the International Conference of the Biometrics Special Interest Group (BIOSIG)* (pp. 1-7). Darmstadt: IEEE.

Bertino, E., Catania, B., & Damiani, M. (2005). GEO-RBAC: A spatially aware RBAC. In *SACMAT '05 Proceedings of the tenth ACM symposium on Access control models and technologies* (pp. 29-37). Stockholm, Sweden: ACM.

Biometrics. (n.d.). *Biometrics*. Retrieved from http://dictionary.reference.com/browse/biometrics

CNN Money. (2015). *OPM hack's unprecedented haul: 1.1 million fingerprints*. Retrieved from http://money.cnn.com/2015/07/10/technology/opm-hack-fingerprints/

Conn, J. (2014). EHR makers' mobile medical apps grow in popularity. *Modern Healthcare*, *29*(November). Retrieved from http://www.modernhealthcare.com/article/20141129/MAGAZINE/311299981 PMID:25671868

Elkhodr, M., Shahrestani, S., & Cheung, H. (2011). *Enhancing the security of mobile health monitoring systems through trust negotiations. In Local Computer Networks (LCN), 2011 IEEE 36th Converence on* (pp. 754–757). Bonn: IEEE.

Farrell, S., & Housley, R. (2002, April). *An Internet Attribute Certificate Profile for Authorization*. Retrieved from The Internet Engineering Task Force (IETF®): https://www.ietf.org/rfc/rfc3281.txt

Fernández-Alemán, J., Señor, I., Lozoya, P., & Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *Journal of Biomedical Informatics*, *46*(3), 541–562. doi:10.1016/j.jbi.2012.12.003 PMID:23305810

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramou, R. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security*, *4*(3), 224–274. doi:10.1145/501978.501980

GAA-API. (n.d.). *Generic Authorization and Access-control API (GAA-API)*. Retrieved from http://gost.isi.edu/info/gaaapi/

Gartner. (2015). *Gartner Says Global Devices Shipments to Grow 2.8 Percent in 2015*. Retrieved from http://www.gartner.com/newsroom/id/3010017

Heckle, R., Lutters, W., & Gurzick, D. (2008). Network Authentication Using Single Sign-on: The Challenge of Aligning Mental Models.*Proceedings of the 2nd ACM Symposium on Computer Human Interaction for Management of Information Technology* (pp. 6:1-6:10). San Diego, CA: ACM. doi:10.1145/1477973.1477982

Herzberg, A. (2003, May). Payments and Banking with Mobile Personal Devices. *Communications of the ACM*, *46*(5), 53–58. doi:10.1145/769800.769801

Himiss. (2014). *How mHealth is Changing Health and Healthcare*. Retrieved from http://www.himss.org/ResourceLibrary/mHimssRoadmapLanding.aspx?ItemNumber=30562

Housley, R., Polk, W., Ford, W., & Solo, D. (2002, April). *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*. Retrieved from The Internet Engineering Task Force: http://www.ietf.org/rfc/rfc3280.txt

Hwang, S., Cho, S., & Park, S. (2009). Keystroke dynamics-based authentication for mobile devices. *Computers & Security*, *28*(1-2), 85–93. doi:10.1016/j.cose.2008.10.002

IHS. (n.d.). *Health Information Exchange and Master Patient Index*. Retrieved from https://www.ihs.gov/hie/index.cfm?module=dsp_hie_mpi

iTunes. (n.d.). *iTunes App Store Medical Apps*. Retrieved from https://itunes.apple.com/us/genre/ios-medical/id6020?mt=8

Lewis, N. (2011). 80% Of Doctors Use Mobile Devices At Work. *Information Week*, *21*(October). Retrieved from http://www.informationweek.com/mobile/80--of-doctors-use-mobile-devices-at-work/d/d-id/1100880

Mantyjarvi, J., Lindholm, M., Vildjiounaite, E., Makela, S.-M., & Ailisto, H. (2005). Identifying users of portable devices from gait pattern with accelerometers. *Acoustics, Speech, and Signal Processing, 2005. Proceedings. (ICASSP '05). IEEE International Conference on.* IEEE. doi:10.1109/ICASSP.2005.1415569

Mauro, C., Sunyaev, A., Leimeister, J., Schweiger, A., & Krcmar, H. (2008). A Proposed Solution for Managing Doctor's Smart Cards in Hospitals Using a Single Sign-On Central Architecture.*Hawaii International Conference on System Sciences, Proceedings of the 41st Annual* (pp. 2565-266). Waikoloa, HI: IEEE. doi:10.1109/HICSS.2008.33

Mavridis, I., Georgiadis, C., Pangalos, G., & Khair, M. (2001, January-March). Access Control based on Attribute Certificates for Medical Intranet Applications. *Journal of Medical Internet Research*, *3*(1), e9. doi:10.2196/jmir.3.1.e9 PMID:11720951

Montopoli, B. (2013). *For criminals, smartphones becoming prime targets*. Retrieved from http://www.cbsnews.com/news/for-criminals-smartphones-becoming-prime-targets/

Na, S., & Cheon, S. (2000). Role Delegation in Role-based Access Control.*Proceedings of the Fifth ACM Workshop on Role-based Access Control* (pp. 39-44). Berlin, Germany: ACM. doi:10.1145/344287.344300

Neuman, B., & Ts'o, T. (1994, September). Kerberos: An Authentication. *IEEE Communications Magazine*, *32*(9), 33–38. doi:10.1109/35.312841

Nexus. (n.d.). *Fingerprint security on Nexus devices*. Retrieved from https://support.google.com/nexus/answer/6300638?hl=en

Pashalidis, A., & Mitchell, C. (2003). A Taxonomy of Single Sign-On Systems. *8th Australasian Conference, ACISP. 2727*. Wollongong, Australia: Springer-Verlag Berlin Heidelberg.

Pillai, J., Patel, V., Chellappa, R., & Ratha, N. (2010). Sectored Random Projections for Cancelable Iris Biometrics. *Acoustics Speech and Signal Processing (ICASSP), 2010 IEEE International Conference on* (pp. 1838-1841). Dallas, TX: IEEE. doi:10.1109/ICASSP.2010.5495383

Ratha, N., Connell, J., & Bolle, R. (2001). Enhancing security and privacy in biometrics-based authentication systems. *IBM Systems Journal*, *40*(3), 614–634. doi:10.1147/sj.403.0614

Ratha, N., Connell, J., Bolle, R., & Chikkerur, S. (2006). Cancelable Biometrics: A Case Study in Fingerprints. *Pattern Recognition, 2006. ICPR 2006. 18th International Conference on, 4*. doi:10.1109/ICPR.2006.353

Ray, I., & Toahchoodee, M. (2007). A spatio-temporal role-based access control model.*Proceedings of the 21st annual IFIP WG 11.3 working conference on Data and applications security* (pp. 211-226). Redondo Beach, CA: Springer-Verlag.

Ryutov, T., Zhou, L., Neuman, C., Leithead, T., & Seamons, K. (2005). Adaptive Trust Negotiation and Access Control. *SACMAT '05 Proceedings of the tenth ACM symposium on Access control models and technologies* (pp. 139-146). New York: ACM.

Sabater, J., & Sierra, C. (2005, September). Review on computational trust and reputation models. *Artificial Intelligence Review*, *24*(1), 33–60. doi:10.1007/s10462-004-0041-5

Seabrook, H., Stromer, J. N., Shevkenek, C., Bharwani, A., Grood, J., & Ghali, W. A. (2014). Medical applications: A database and characterization of apps in Applie iOS and Android Platforms. *BMC Research Notes*, *7*(1), 573. doi:10.1186/1756-0500-7-573 PMID:25167765

SlimFramework. (n.d.). *Slim framework*. Retrieved from http://www.slimframework.com/

State of Connecticut. (n.d.). *An Act Concerning Young Athletics and Concussions*. Retrieved from http://www.cga.ct.gov/2014/act/pa/pdf/2014PA-00066-R00HB-05113-PA.pdf

Sundelin, T. L. (2003). *Surrogate Trust Negotiation: Solving Authentication and Authorization Issues in Dynamic Mobile Networks.* Brigham Young University.

van der Horst, T. W., Sundelin, T., Seamons, K. E., & Knutson, C. D. (2004). Mobile Trust Negotiation: Authentication and Authorization in Dynamic Mobile Networks. *Proc. of the Eighth IFIP Conference on Communications and Multimedia Security*.

van der Horst, T. W., Sundelin, T., Seamons, K. E., & Knutson, C. D. (2005). Mobile Trust Negotiation. In D. a. Chadwick (Ed.), *Communications and Multimedia Security* (Vol. 175, pp. 97–109). Springer. doi:10.1007/0-387-24486-7_7

Vawdrey, D. K., Sundelin, T. L., Seamons, K. E., & Knutson, C. D. (2003). Trust Negotiation for Authentication and Authorization in Healthcare Information Systems. *Engineering in Medicine and Biology Society, 2003. Proceedings of the 25th Annual International Conference of the IEEE* (pp. 1406-1409). IEEE.

Ventola, C. L. (2014, May). Mobile Devices and Apps for Health Care Professionals: Uses and Benefits. *Pharmacy and Therapeutics, 39*(5), 356-364. Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4029126

West, D. (2012) How Mobile Devices are Transforming Healthcare. *Issues in Technology Innovation*, *19*. Retrieved from http://www.brookings.edu/~/media/research/files/papers/2012/5/22-mobile-health-west/22-mobile-health-west.pdf

Winsborough, W. H., Seamons, K. E., & Jones, V. E. (2000). *Automated trust negotiation. In DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proceedings* (pp. 88–102). Hilton Head, SC: IEEE; doi:10.1109/DISCEX.2000.824965

X.509. (n.d.). *Standard*. Retrieved from https://tools.ietf.org/html/rfc5280

Xu, H., Zhou, Y., & Lyu, M. R. (2014). Towards Continuous and Passive Authentication via Touch Biometrics: An Experimental Study on Smartphones.*Symposium On Usable Privacy and Security (SOUPS 2014)* (pp. 187-198). Menlo Park, CA: USENIX Association.

Yu, J., Wang, G., & Mu, Y. (2012). Provably Secure Single Sign-on Scheme in Distributed Systems and Networks. *TRUSTCOM '12 Proceedings of the 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications* (pp. 271-278). Washington, DC: IEEE.

Zuo, J., Ratha, N., & Connell, J. (2008). Cancelable Iris Biometric. *Pattern Recognition, 2008. ICPR 2008. 19th International Conference on* (pp. 1-4). Tampa, FL: IEEE. doi:10.1109/ICPR.2008.4761886

KEY TERMS AND DEFINITIONS

Adaptive Trust Negotiation: Trust negotiation in which the request receiver adjusts its security policies based on the user's credentials.

Attribute Certificate: A structured tamper-resistant file that is associated with an identity through an identity certificate and that lists data in a key-value pairs.

Certificate Authority (CA): An entity endorsed by another authority that vets user identities and signs identity certificates.

Digital Wallet: A collection of credentials a user earns through being granted access to secure systems.

Electronic Medical Record (EMR): A collection of credentials a user earns through being granted access to secure systems.

Health Information Exchange (HIE): The sharing of health data between stakeholders over a secure medical network, or the computer system that facilitates data sharing.

Identity Certificate: A structured tamper-resistant file that is used to identify an individual and provide assurance for secure connections.

Root Authority: An entity that signs user certificates with a self-signed certificate, users must add the certificate to their certificate store to establish trust.

Trust Negotiation: The process two entities without prior contact undertake to establish trust based on credentials other than identity.