SIM: A Smartphone-based Identity Management Framework and Its Application to Arkansas Trauma Image Repository

Mengjun Xie*, Umit Topaloglu†, Thomas Powell†, Chao Peng‡, Jiang Bian†
*Department of Computer Science
University of Arkansas at Little Rock
Little Rock, AR 72204, USA
Email: mxxie@ualr.edu
†Division of Biomedical Informatics
University of Arkansas for Medical Sciences
Little Rock, AR 72205, USA
Email: {UTopaloglu, TEPowell, jbian}@uams.edu
‡Software Engineering Institute
East China Normal University
Shanghai, 200062, China
Email: cpeng@sei.ecnu.edu.cn

***Abstract*—Secure and convenient user identity management is particularly important to the success of EMR, EHR, and PHR systems. Unfortunately, widely-used identity management mechanisms that solely rely on username/password are inadequate to meet the strong security and privacy requirements for protecting sensitive user information and medical data. Two-factor authentication approaches that are more convenient and user friendly than existing solutions have been given top priority in the healthcare sector where the majority of healthcare practitioners and patients are not tech-savvy. In this paper, we present a smartphone-based identity management framework—SIM—to enhance the security and usability of user identity management in healthcare information systems. SIM leverages the popularity and computational power of smartphone. Within the SIM framework, a person employs a smartphone to centrally store and manage her identity credentials and authenticates herself to healthcare applications using two-factor authentication without typing any identity credentials. Moreover, SIM provides patients with a patient-controlled authorization mechanism to help patients manage the accesses to their PHRs in a secure and convenient manner. Using an existing EMR system—Arkansas Trauma Image Repository—as an example, we demonstrate that SIM can be applied to a real-world healthcare information system to enhance its protection of user credentials and sensitive information.**

I. Introduction

Electronic medical records (EMRs), electronic health records (EHRs), and personal health records (PHRs) [1], [2] have gained significant popularity in the healthcare domain. According to [3], the use of EHR systems among office-based physicians has increased to 72% in 2012 in the United States. As a patient's EMRs/EHRs/PHRs carry sensitive personal information, their security and privacy have been mandated by legal and regulatory policies (e.g., the U.S. Health Insurance Portability and Accountability Act (HIPAA) [4] and European Data Protection Directive 95/46/EC). Therefore, it is imperative for hospitals and medical organizations to ensure accesses to EMRs/EHRs are securely authenticated and appropriately authorized; and it is desirable for a patient to have a convenient and secure mechanism through which she can enforce fine-grained authorization for accesses to her PHR information.

Secure and convenient user identity management that consists of both authentication and authorization, however, is very difficult. There exists significant diversity of healthcare information systems (HISs) deployed in a typical hospital or medical institution. As it is almost impossible for any vendor to provide a single integrated system that can suit all needs a hospital has, a hospital usually has tens if not hundreds of systems purchased from different vendors or developed in-house. For example, over one hundred commercial and internally developed EMR systems and HISs were used at the University of Arkansas for Medical Sciences (UAMS). User authentication is the root of user identity management, where a user submits her identity (most often represented by a pair of username and password) to the system and validates to the system she is who she claims to be. If the authentication succeeds, the system will then assign appropriate privileges to the user for accessing protected information based on the authorization rules. Without appropriate user authentication and authorization, the confidentiality of patient information and privacy protection of patients can be easily penetrated. However, the common practice of user identity management in many HISs is prone to security issues.

The most common authentication mechanism is the password-based authentication, where a user enters her username and password—a "secret" that should be well protected and only known to the owner—to validate her identity to the system. Despite its popularity, password-based authentication has many security issues in identity management[5], [6], [7]. Weak passwords and password reuse can significantly weaken the protection on sensitive data and user privacy, especially in

978-1-4799-1310-7/13/$31.00 ©2013 IEEE

the healthcare domain where the majority of doctors, nurses, staff, and patients are not tech-savvy. Writing down passwords on a sticky note and pasting it on a PC monitor, although strictly forbidden by best security practices, is still not unusual in medical environments [13]. Moreover, it is not uncommon for a healthcare practitioner to have different accounts for different HISs to perform daily tasks, which makes identity management even more difficult.

To remedy these issues, mainstream web browsers have introduced built-in password managers. And standalone password managers [8] such as 1Password, KeePass, LastPass, and Mitto become popular. However, a password manager alone does not provide sufficient security assurance of passwords due to insecure running environment [9], [10]. An Anti-Phishing Working Group (APWG) report shows that data stealing and generic Trojan malware comprises ~37% of all malware detected in the first quarter of 2013 [11], where the malware is designed to steal confidential personal information especially user accounts and passwords. According to a recent research study [12], those browser built-in password managers in all five mainstream web browsers could not prevent malware from stealing passwords in a PC environment.

Existing identity management schemes cannot effectively handle identity delegation, either. In clinical practices, physicians often need to delegate certain tasks to nurses or staff members. In other words, the delegate acts as the physician being delegated in performing those specific tasks. However, most of existing HISs do not support fine-grained owner-controlled delegation. In practice, the physician in need of delegation often has to give out her full identity credentials, e.g., username and password, to the delegate [13]. Evidently, it is necessary for the physician to change her identity after the delegation finishes, which usually is very inconvenient in practice, to prevent potential identity abuse. Therefore, it would be very beneficial for an identity management system to support identity delegation without revealing identity credentials.

Two-factor authentication (TFA) has gained increasingly interest in many sectors including healthcare as it offers much stronger security assurance than password only authentication. Existing TFA solutions usually require a user to carry a special electronic device such as RSA SecurID key fob as the second factor. Given the prominent advancement of smartphone technologies, we believe smartphone can be an excellent choice as the second factor in TFA. Compared to PCs, smartphones have a much smaller attack surface as they have new system designs from scratch that remove the legacy application issue and incorporate security consideration. The computing capacity distinguishes smartphones from "dumb" authentication devices such as smart cards, secure tokens and traditional cellphones. A wide spectrum of application libraries including cryptographic libraries are supported by smartphone systems, which offers greater flexibility in the design of an authentication scheme. Smartphones are usually carried around and well taken care of by their owners, which makes them a nice fit for carrying personal identities and being the secondary authentication factor. Last but not least, very different from all previous computing devices, smartphones integrate many hardware modules that can be leveraged for authentication (e.g., GPS, camera, fingerprint scanner, and NFC [14]).

In this paper, we present a smartphone-based identity management framework—SIM—to enhance the security and usability of user identity management in healthcare information systems. SIM leverages the popularity and computational power of smartphone. Within the SIM framework, a person employs a smartphone to centrally store and manage her identity credentials and authenticates herself to healthcare applications using two-factor authentication without typing any identity credentials. Moreover, SIM provides patients with a patient-controlled authorization mechanism to help patients manage the accesses to their PHRs in a secure and convenient manner. Using an existing EMR system—Arkansas Trauma Image Repository—as an example, we demonstrate that SIM can be applied to a real-world healthcare information system to enhance its protection of user credentials and sensitive information.

The rest of the paper is organized as follows. We first briefly introduce the background information of user authentication and the Arkansas Trauma Image Repository that will be used later as the application of our SIM framework. Then, we describe the SIM framework in detail. After that, we present the prototype implementation of SIM and its application to the Arkansas Trauma Image Repository. We conclude the paper in the end.

II. Background

A. Authentication Mechanisms

Two-factor authentication (TFA) requires the presentation of two or more authentication factors: something a user knows (e.g., a password), something a user has (e.g., a secure token), and something a user is (e.g., biometric characteristics). Using two factors as opposed to one factor generally delivers a higher level of authentication assurance. For example, passwords can be combined with security tokens such as RSA SecurID that implement one-time passwords for authentication. By using the second factor such as security tokens, password stealing is not sufficient for an adversary to gain access to the user's account. The recently released electronic prescriptions for controlled substances clarification by DEA[15] has incorporated the TFA requirement. With the popularity of mobile phone, a new category of TFA tools (e.g., Mobile-OTP [16]) transforms a PC user's mobile phone into a token device using either SMS messaging, an interactive telephone call, or via downloadable application to a smartphone. Since a user communicates with the remote server through two channels, the mobile phone becomes a two-factor, two-channel authentication mechanism. Google's 2-step verification is such a TFA with mobile phone example. A few mobile device-assisted authentication schemes [17], [18], [19], [20], [21] were proposed for protecting a user from either password stealing on an untrusted PC or phishing attacks. In those schemes, mobile devices are assumed to be trustworthy and able to perform certain computing operations such as hashing.

B. Arkansas Trauma Image Repository

The Arkansas Trauma Image Repository (TIR) [22], developed and maintained by the University of Arkansas for Medical Sciences (UAMS), is a state-wide imaging repository that aims to improve trauma decision and outcomes by sharing critical images between emergency departments. The TIR system

speeds up treatment from the point of injury to definitive care. For those trauma patients who need to be transferred from the first receiving hospital (e.g., a level III facility) to a definitive care hospital (e.g., a level I comprehensive trauma center), their CT (computerized tomography) or MRI (magnetic resonance imaging) scan images obtained in the initial treating facility are first sent to the TIR server, which then makes the information available to the tertiary receiving facility. This allows the specialist in the receiving hospital to view the films and begin to make clinical decisions and organize the care team ahead of the patient's arrival. Since its introduction in 2011, sixty-seven hospitals across Arkansas have been able to upload radiological images to the repository and forward those to the physician specialist who will provide care at the receiving facility. Over 5,000 such images have been forwarded [23].

The patient's hospital-to-hospital transfer is coordinated through the Arkansas Trauma Communications Center (ATCC), which operates a 24/7 call center with trained paramedics and nurses. Since it began operations through Oct. 31, 2012, the ATCC has facilitated 9,766 hospital-to-hospital transfers of trauma patients (1,029 major, 2,597 moderate, and 6,140 minor) [24].

III. Method

The SIM framework aims to simplify identity management while enhancing identity security. We use smartphone-based centralized identity management to achieve the former and smartphone-based two-factor authentication (TFA) to achieve the latter. To realize TFA, existing applications/services without TFA also need to be modified to incorporate the authentication of the second factor. Considering the large number of existing applications in the healthcare domain and user habits trained with those applications, an identity management server is introduced into the SIM framework, which takes the job of authenticating the second factor, trying to minimize the changes to existing applications. The SIM authentication protocol is designed to preserve already-developed application use experience and protect users from identity theft attacks launched by malware on PC. Under the SIM framework, a user can be securely authenticated to a remote application from any PC without typing her identity credentials (e.g., username/password) on that PC.

Suppose that a hospital has deployed SIM and users have their smartphones appropriately set up for SIM, that is, SIM mobile app has been correctly installed and appropriately configured and user's identity credentials (e.g., username and password) have been imported and stored by the app. The normal scenario of user authentication through SIM is as follows. When a physician wants to access an EMR application to check a patient's medical information, for example, view a CT image through web browser, she does not need to type her username and password on her working PC. Instead, she just needs to launch the SIM mobile app from her smartphone (The app is protected by a master password to prevent unauthorized accesses) and select the intended EMR application and account for login. After the physician completes selection and presses "confirm" button, the app will use her stored identity to log into the selected application and communicate with the special identity management server for authentication. Upon successful authentication, the physician will be notified of a message shown in the phone screen, instructing her to access the EMR application from her working PC with a one-time PIN. The purpose of the one-time PIN is two-fold: to prevent possible identity misuse/abuse and to achieve identity delegation. After typing the given PIN, the physician can access the application from PC web browser as usual. If the physician wants to delegate her task, e.g., asking a nurse to check the patient's lab report, she can simply push that PIN to the nurse's smartphone and then the nurse will be able to perform the task with the given PIN. If the physician needs to log in on another PC, e.g., the PC in the lab or patient room, she only needs to type in a new one-time PIN given by the mobile app on that PC. The smartphone app generates a new one-time PIN periodically, much similar to the RSA SecurID fob and Google Android Authenticator app.

In principle, the SIM framework consists of four types of software components:

- SIM-aware applications,
- an identity management server,
- a browser extension on the client PC, and
- an identity management application on the smartphone.

In SIM, the applications need to be aware of the two-factor authentication (TFA), which means existing applications need to be modified. If the application allows no change in its authentication flow, it works as usual but cannot take advantage of TFA. The identity management server is a critical component of SIM with important responsibilities. It is responsible for authenticating the second factor, communicating with different application servers, PCs, and smartphones through secure connections, maintaining authentication states, relaying confidential data, performing data encryption/decryption, etc. The browser extension is used to maintain secure channels between a web browser on PC and the identity management server so that user authentication token can be migrated to the web browser on PC in a user transparent manner. The smartphone identity management app is in charge of importing, changing, expiring identities and authenticating the user with the selected identity. The app also needs to perform password generation, data encryption/decryption operations.

In the remaining part of this section, we first describe the security assumptions and threat model for the SIM framework. Then we present the authentication protocol employed by SIM. Last we provide the security analysis of the authentication protocol.

A. Security Assumptions and Threat Model

The primary security goal of SIM is to protect sensitive user identity credentials (e.g., passwords, private keys, security tokens, etc) from being stolen by malware in an untrusted PC or by attackers who eavesdrop network communication traffic. To prevent man-in-the-middle and eavesdropping attacks, we assume that standard cryptographic mechanisms (e.g., SSL/TLS) are employed during authentication such that a secure communication channel is provided between the user's smartphone/PC and the remote server. The smartphone app will use cellular network instead of Wi-Fi for network communications as attacking the cellular network is much more difficult. We also assume that the certificates of the identity

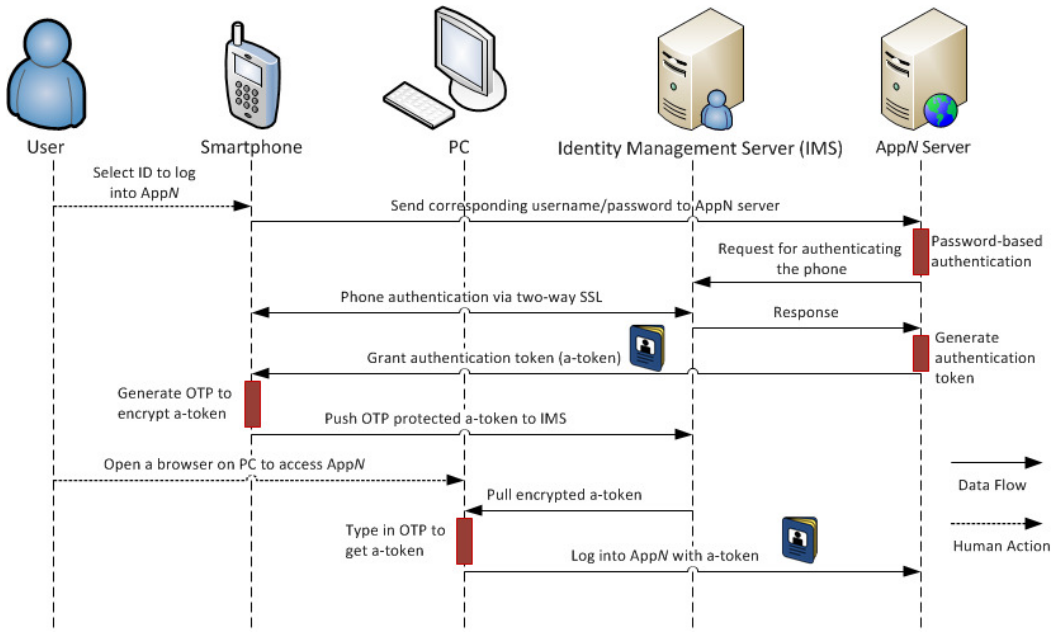

Fig. 1. The diagram of the authentication protocol

management server and application servers (either certified by the deployment domain, i.e., self-certified, or certified by a CA) are available to all users.

We assume that the identity management server is properly secured and available for access all the time (Denial-of-service attacks to the server are out of the scope of this paper). We also assume that user applications such as web browsers may be compromised but the operating systems (i.e., the kernels) of the user's PC and smartphone are secure. This is a reasonable assumption as today's operating systems such as Windows 7/8 and Android do not give administrative privileges to a normal user by default, which means the compromise of an application usually will not affect the operating system's security. The user's identity credentials are encrypted, stored, and managed by the smartphone application. The smartphone application is protected by a strong master password, much similar to the master password mechanism applied by the Firefox browser to its built-in password manager.

The password stealing attack through breaking the application server's password database is out of the scope of SIM. However, we note that the smartphone identity management app can generate different strong passwords for different EMR/EHR/PHR systems and prevent user from reusing passwords. Therefore, the breach of password database on one application server can only affect one user identity. SIM helps contain the damage caused by server-side security breach.

We assign the attacker the following capabilities. First, the attacker is capable of infecting the PC application (e.g., a web browser) with arbitrary malware such that she has full control over that application and the data and programs of that user account. However, the attacker can neither access the data owned by another user nor escalate her privilege to the administrator level. For the smartphone application, we assign the attacker a similar capability. Note that due to strong application isolation design of smartphone operating systems (e.g., each application runs with a different user identity in Android), malware compromising one application normally cannot gain access to another application's private data in smartphone. Second, the attacker may either obtain the user's master password for smartphone or gain the user's smartphone but not both.

B. Authentication Protocol

There is a one-time setup process for each smartphone to be used with SIM authentication. After appropriate installation, the smartphone application will generates a pair of public and private keys in a secure manner. The certificate of the user's identity will be securely generated (by a CA or the internal authentication service) and stored by the service. The certificate of a remote application service is certified by a CA and trusted by the smartphone application. This one-time setup in general can be done fairly quickly.

Figure 1 illustrates the authentication protocol used in the SIM. A user first launches the smartphone app by typing a master password on the phone's screen. Then she selects the remote application service she wants to log into and her corresponding identity (assuming a pair of username and password) for that service. The app will first establish a secure TCP connection via TLS or SSL with the intended application server (AppN) through a cellular network and then send the username and password to the server through the secure connection. The application server will invoke its authentication module to verify the username and password. Upon successful verification, the application server redirects the authentication request to the IMS that will authenticate the smartphone through the two-way SSL authentication. Then, the IMS returns a success response to the server. Now the AppN server confirms the identity, generates a special authentication token (a-token, usually implemented as an HTTP cookie) for the user, and returns the a-token back to the smartphone app. The app will generate a one-time password (OTP), use it to

encrypt the a-token, and push the OTP protected a-token onto the IMS. The app will also prompt user that she can access the AppN through a PC. After the browser is launched, the browser extension will instantly create a secure channel with the IMS (assuming the user has saved her IMS account and password in the extension) and pull the OTP protected a-token to the PC. After the user correctly inputs the OTP, the a-token will be decrypted and saved. From then on, the a-token will be sent with normal requests for accessing the AppN. As the a-token is valid, the access will be granted.

C. Security Analysis

SIM realizes two-factor authentication for a user with her smartphone (what a user has) and her identity to the application (what a user knows). The identities stored in the smartphone are protected by a strong master password. Either knowing the master password, capturing user identity on wire, or stealing the smartphone will not give an adversary the ability to access the user's accounts. In SIM, the smartphone application manages the creation, use, expiration of passwords in an automatic manner, which can effectively avoid common password risks including weak password, password reuse, and shoulder surfing. We note that social engineering attacks may still succeed where a user is willing to giving out her identity credentials such as username and password. SIM cannot prevent this type of attacks. However, this type of attacks can be mitigated by the two-factor authentication used in SIM.

Since user credentials are stored in the smartphone, smartphone itself may become the attack target and the security of SIM hinges on the security of the smartphone application. Although malware for mobile environments is expected to become a significant threat in next few years[25], [26], smartphone operating systems such as Android and iOS were designed with more security features such as mandatory application sandbox and strong application isolation [27]. The new system design and hardware enabled security features such as fingerprint verification can further enhance the security of smartphone. When fingerprint scanner becomes universal on smartphones, fingerprint should replace the app master password for protecting the data stored on the smartphone.

SIM can effectively defeat phishing attacks by the SSL/TLS mutual authentication between the smartphone and remote server and counter replay attacks by using the server provided nouce. In case of phone loss, sensitive data on the lost smartphone shall still be protected by the strong encryption, which cannot be decrypted without knowing the app master password. In addition, certain user credentials such as the certificates stored in the lost phone can be revoked.

SIM prevents user credentials from being accessed by malware in PC. However, malware may launch a session hijacking attack, in which the malware takes control of a user session after the user successfully establishes a session with the legitimate server. In a session hijacking attack, the malware may stealthily alter user transactions or perform unauthorized transactions. We note that assurance of transaction integrity is out of the scope of SIM. However, SIM can be used to mitigate session hijacking attacks. For example, SIM can be instructed to authenticate a user either periodically or upon the request of an important data operation (e.g., deleting a patient's medical record) during a session to make user keep alert to unauthorized data operations.

IV. Results

In this section, we first describe the implementation of current prototype and then detail how the SIM framework can be applied to an existing healthcare information system—Trauma Image Repository (TIR)—to embrace two-factor authentication and achieve patient-controlled authorization to her EHR.

A. Implementation

We have developed a functional proof-of-concept prototype that consists of an Android based identity management application, a web-based identity management server (IMS), and a Google chrome browser extension. A demo web-based healthcare application server is under development as existing production healthcare information systems are not allowed to be modified for the SIM framework and tested against our prototype. However, our prototype can work with existing EMR systems such as the TIR system without applying two-factor authentication that demands modifications to the existing application servers. The prototype allows a person to securely log into an application (e.g., TIR) from an Android smartphone without typing any password and then access the same application from a web browser on a PC instantly. The authentication token is securely relayed from the smartphone to the PC through the identity management server. Our current implementation is able to release a nontechnical person from the burden of password management and shield her from password stealing by malware in a PC.

We have implemented an identity management Android application which is able to (1) scan the QR code of a certificate from a display, decode, and save it; (2) generate a public/private key pair and transfer the public key to the remote server; (3) take a user's username and password from keyboard typing and encrypt them; and (4) communicate with IMS and application servers via the cellular network in authentication. The application has multiple Android activities and services, each responsible for one specific task such as taking password input, generating a public/private key pair, etc.

In the prototype implementation, real-time communications between the IMS and the browser extension are carried through an authenticated `socket.io` channel so that notifications can be pushed to the user as soon as an event has occurred. The Android application uses a master key to protect stored credentials. The app first authenticates to the identity management server for retrieving the server generated nonce and then computes the authentication key *aKey*, which is derived from the nonce and user's IMS password *password* using the Password-Based Key Derivation Function 2 (PBKDF2). Formally, *aKey* = PBKDF2_HMAC_SHA256 (*password*, *nonce*). We use a hash-based message authentication code (HMAC) function with a strong cryptographic hash function (SHA256) as PBKDF2's underlying pseudorandom function. The encryption/decryption routine uses the Advance Encryption Standard (AES) in cipher-block chain (CBC) mode of operation with the PKCS#7 byte padding method. We use 256-bit key size to match the output of the PBKDF2_HMAC_SHA256 function.

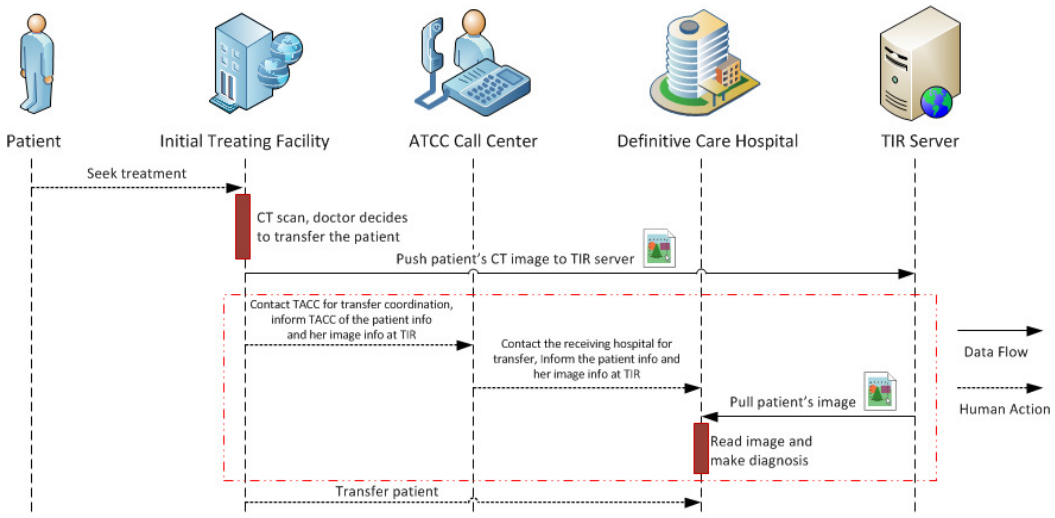

Fig. 2. Current Patient Transfer Procedure with TIR

B. Application of SIM to Trauma Image Repository (TIR) System

1) Current Use of TIR and Its Security Issue: As pointed out in Section II-B, the establishment of TIR has significantly facilitated the transfer of trauma patients in Arkansas. Figure 2 illustrates the general procedure of transferring a trauma patient from an initial treating facility to a definitive care hospital. The transfer is coordinated by the Arkansas Trauma Communications Center (ATCC) via their 24/7 call center. Once the patient takes a CT scan, her CT image can be uploaded to the TIR server directly from the modality. Then, the initial treating facility contacts the call center requesting a transfer. Upon receiving such a request, the ATCC call center will contact a upper-level trauma care center as the definitive care hospital and arrange the transfer. At the receiving hospital, the point-of-contact (POC) person distributes the patient information to the physician responsible for treating the patient. The physician then can pull the patient's CT image from the TIR server and make a diagnosis based on the image before the arrival of the patient.

The current TIR system only uses password-based authentication mechanism to protect its users' information, which is subjected to a variety of password related attacks. In addition, although a Role-based Access Control (RBAC) security model has been implemented in the TIR for controlling access to protected data, it is possible that a patient's images can be accessed by authenticated physicians with certain roles while none of them is authorized to access the images. Currently, the protection of patient privacy on TIR mainly relies on the policy and regulation. In other words, the access control is only enforced by the policy, not the system once a user logs in. Even if the system can log an unauthorized access to a patient's image by an authenticated user and trigger an audit report asking for immediate attention, the data has been accessed and patient privacy has been breached. Therefore, the images on TIR should be encrypted to protect patient's privacy. At the same time, encryption keys should be delivered promptly to the receiving hospital for quick diagnosis and treatment of patient.

2) Application of SIM to TIR: In this section, we describe how SIM can be applied to the TIR, a typical EMR system, to enhance the data security and patient privacy without sacrificing system usability. For clear presentation, we assume that all TIR users mentioned in the section are trustworthy and have been appropriately authenticated through SIM authentication protocol and their smartphones and working PCs maintain secure connections with the identity management server.

Figure 3 illustrates the patient transfer procedure within the SIM framework, which essentially corresponds to the rectangle area surrounded by red dashed line in Figure 2. Once the patient radiology image is uploaded to the TIR server, a staff member in charge of the TIR system at the initial treating facility will use the SIM application to generate a key on her smartphone. The key will be automatically pushed to the IMS once being generated. The staff member then accesses the TIR system through a web browser on her PC to instruct the data encryption operation. The IMS will fetch the image file from TIR, encrypt the image using the user-supplied key, and put encrypted image back to TIR. Then, the staff member sends the key protected by a one-time password (OTP) to the ATCC and contacts ATCC to request a patient transfer. The OTP protected key actually is first transferred to the IMS and then pushed to the ATCC staff member by the IMS. Through the phone call, the staff member at the initial facility notifies the call center of the patient information and OTP. With the OTP, the staff member at the call center can reveal the key and then re-encrypt the key with another OTP generated by her SIM application on her smartphone. After that, she calls the POC at the receiving hospital and notifies the POC of the patient information and OTP. At the same time, the OTP protected key will be relayed to the POC's smartphone through the IMS. Following the similar procedure, the key will finally be delivered to the treating physician's smartphone. Now the physician can get the encrypted patient image from the TIR through a web browser, decrypt that image with the received key, and make diagnosis decision based on the image. Note that all key and OPT generations, data encryption/decryption operations are done automatically and transparent to the user. The trauma patient transfer procedure keeps the same after

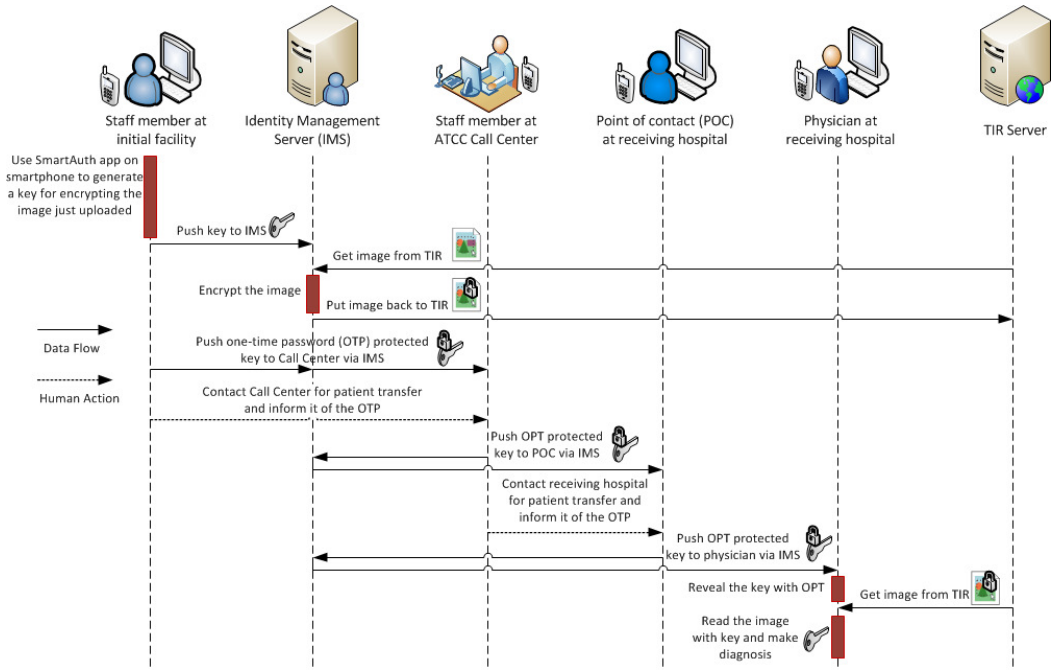

Fig. 3. SIM Augmented Patient Transfer Procedure with TIR

SIM is incorporated and operational overhead introduced is light. SIM users just need to carry their smartphones and type in OTP occasionally. However, those users do not need to remember many different pairs of username/password while enjoy stronger assurance of data security.

Two benefits manifest immediately after we apply SIM to the TIR system. First, every TIR user now is freed from the burden of remembering passwords and the worry of malware stealing identities. Second, patient images are protected by strong encryption from the very beginning and can only be accessed by authenticated and authorized persons.

V. Discussions

One key component of the continuity of care processes is the ability to transfer and share patients' medical records across different care facilities. The personal health record (PHR) system and the continuity of care record (CCR) have emerged to support this process. However, security and patient privacy issues have often been overlooked in the development of PHR systems. We can leverage the SIM framework to create a secure and patient-centric PHR environment. For example, a trauma patient may request a copy of her radiology images to be securely transferred from the TIR to a SIM-aware PHR system, where she controls and manages her own medical data. One one hand, a patient needs a convenient way to share part of her PHRs with physicians in another facility, e.g., transferring her CT images to her primary care physician (PCP) for a follow-up of the trauma. On the other hand, the patient might want to control the access to her medical information, e.g., not disclosing her psychiatric condition to her PCP.

Here we still use TIR as the example to briefly explain the aforementioned idea. Upon receiving a request for a copy of the patient's images, the staff member at the initial treating facility can register the patient with the IMS, and initiate the process of secure data exchange from TIR to the SIM-aware PHR system. An OTP will be generated and used to encrypt the patients' images before sending it to the PHR system. When the staff member starts the transfer process, the IMS will send a notification to the patient's registered smartphone by SMS. Once receiving the notification, the patient will install the SIM mobile app. The staff member will then contact the patient by phone and provide her the OTP. Now the patient can log into the PHR (i.e., using the normal SIM's authentication process), and provide the PHR system with the OTP she has received to claim the ownership of the transferred images and import the newly transmitted images into her account. The SIM-aware PHR system shall decrypt the images using the provided OTP and re-encrypt them with the master key the patient uses to encrypt all other PHRs in the PHR system. After that, the patient's radiology images become part of her PHRs in a secure manner. Similarly, the patient will also be able to use this process to transfer her medical data from the PHR system to another SIM-aware EMR/EHR system so that her other care-givers can access the information.

VI. Conclusion

In this paper, we have presented a smartphone-based identity management framework called SIM to simplify management of personal identities and enhance identity and data security for EMR/EHR/PHR systems. SIM enables a person to use a smartphone to centrally manage her identity credentials and authenticates herself using two-factor authentication without typing her credentials. SIM also provides patients with a patient-controlled access control mechanism to help patients manage the accesses to their PHRs. Using an existing EMR system–Trauma Image Repository–as an example, we have demonstrated how SIM can be applied to a real-world EMR system to enhance protection of user credentials and patient sensitive information. We have been implementing a

prototype system that is partially functional. We believe the testing deployment and user feedback will greatly improve the development of SIM.

ACKNOWLEDGMENT

The work described in this manuscript is supported by award UL1TR000039 through National Center for Advancing Translational Sciences (formerly UL1RR029884 through the NIH National Center for Research Resources). The content is solely the responsibility of the authors and does not necessarily represent the official views of the NIH.

Dr. Chao Peng is partially supported by the Innovation Program of Shanghai Municipal Education Commission, the Natural Science Foundation of China under Grant No.91118008 and Grant No.61232006, the national high-tech research and development plan of China under grant No.2011AA010101, and the Shanghai Knowledge Service Platform Project (No.ZF1213).

REFERENCES

[1] L. Poissant, J. Pereira, R. Tamblyn, and Y. Kawasumi, "The impact of electronic health records on time efficiency of physicians and nurses: A systematic review," Journal of the American Medical Informatics Association, vol. 12, pp. 505–516, Sep-Oct 2005.

[2] B. Dean, J. Lam, J. Natoli, Q. Butler, D. Aguilar, and R. Nordyke, "Use of electronic medical records for health outcomes research: A literature review," Journal of the American Medical Informatics Association, vol. 66, pp. 611–638, 2010.

[3] C. Hsiao and E. Hing, "Use and characteristics of electronic health record systems among office-based physician practices: United states, 20012012." NCHS Data Brief, pp. 1–8, Dec. 2012.

[4] "The health insurance portability and accountability act of 1996 (hipaa)," U.S. Department of Health & Human Sevices, 1996. [Online]. Available: http://www.hhs.gov/ocr/privacy/

[5] R. Lemos, "Passwords: the weakest link?" http://news.cnet.com/2009-1001-916719.html, May 2002.

[6] G. Spafford, "Security myths and passwords," http://www.cerias.purdue.edu/site/blog/post/password-change-myths/, April 2006.

[7] ——, "Passwords and myth," http://www.cerias.purdue.edu/site/blog/post/password-change-myths/, May 2006.

[8] K.-P. Yee and K. Sitaker, "Passpet: convenient password management and phishing protection," in Proceedings of the second symposium on usable privacy and security (SOUPS '06), 2006, pp. 32–43.

[9] M. Ciampa, "Are password management applications viable? an analysis of user training and reactions," in Proc. of ISECON, 2010.

[10] A. Herzberg and R. Margulies, "Forcing johnny to login safely: long-term user study of forcing and training login mechanisms," in Proceedings of the 16th European conference on Research in computer security (ESORICS'11), 2011, pp. 452–471.

[11] A.-P. W. G. (APWG), "Phishing attack trends report: 1st quarter 2013," Anti-Phishing Working Group (APWG), July 2013. [Online]. Available: http://docs.apwg.org/reports/apwg_trends_report_q1_2013.pdf

[12] R. Zhao and C. Yue, "All your browser-saved passwords could belong to us: a security analysis and a cloud-based new design," in Proceedings of the ACM Conference on Data and Applications Security (CODASPY) 2013, 2013.

[13] M. Peleg, D. Beimel, D. Dori, and Y. Denekamp, "Situation-based access control: Privacy management via modeling of patient data access scenarios," Journal of Biomedical Informatics, vol. 41, pp. 1028–1040, 2008.

[14] N. Forum, "What is nfc?" NFC Forum, Feb 2012. [Online]. Available: http://www.nfc-forum.org/aboutnfc/

[15] Drug Enforcement Administration, "Electronic prescriptions for controlled substances clarification," http://www.deadiversion.usdoj.gov/fed_regs/notices/2011/fr1019.htm, October 2011.

[16] "Mobile-opt: Mobile one time passwords." [Online]. Available: http://motp.sourceforge.net/

[17] D. Balfanz and E. W. Felten, "Hand-held computers can be better smart cards," in Proceedings of the 8th USENIX Security Symposium, August 1999, pp. 15–24.

[18] B. Parno, C. Kuo, and A. Perrig, "Phoolproof phishing prevention," in Proceedings of the 10th International Conference on Financial Cryptography and Data Security (FC 2006), ser. Lecture Notes in Computer Science, vol. 4107. Springer, 2006, pp. 1–19.

[19] S. Garriss, R. Cáceres, S. Berger, R. Sailer, L. van Doorn, and X. Zhang, "Trustworthy and personalized computing on public kiosks," in Proceedings of the 6th international conference on Mobile systems, applications, and services (MobiSys '08), 2008, pp. 199–210.

[20] M. Mannan and P. van Oorschot, "Leveraging personal devices for stronger password authentication from untrusted computers," Journal of Computer Security, vol. 19, no. 4, pp. 703–750, 2011.

[21] M. Mannan, B. H. Kim, A. Ganjali, and D. Lie, "Unicorn: Two-factor attestation for data security," in Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS 2011), October 2011.

[22] (2012, Jan) Trauma image repository. ARKANSAS DEPARTMENT OF HEALTH. [Online]. Available: https://tir.uams.edu/

[23] (2012) Arkansas trauma system update. State of Arkansas. [Online]. Available: http://www.healthy.arkansas.gov/programsServices/injuryPreventionControl/TraumaticSystems/Documents/trauma/Update/TraumaSystemUpdate.pdf

[24] (2012) Arkansas trauma system brochure. State of Arkansas. [Online]. Available: http://www.healthy.arkansas.gov/programsServices/injuryPreventionControl/TraumaticSystems/Documents/trauma/ArkansasTraumaSystemBrochure.pdf

[25] G. Lawton, "Is it finally time to worry about mobile malware?" Computer, vol. 41, no. 5, pp. 12–14, May 2008.

[26] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices, ser. SPSM '11. New York, NY, USA: ACM, 2011, pp. 3–14. [Online]. Available: http://doi.acm.org/10.1145/2046614.2046618

[27] W. Enck, M. Ongtang, and P. McDaniel, "Understanding android security," IEEE Security and Privacy, vol. 7, no. 1, pp. 50–57, Jan.-Feb. 2009.