Usable Protection to Healthcare Application

Li Yang
University of Tennessee at Chattanooga
615 McCallie Avenue
Chattanooga, TN 37403
1 423 425 4392
Li-Yang@utc.edu

Mina Sartipi
University of Tennessee at Chattanooga
615 McCallie Avenue
Chattanooga, TN 37403
1 423 425 5336
Mina-Sartipi@utc.edu

Matt McNeely
University of Tennessee at Chattanooga
615 McCallie Avenue
Chattanooga, TN 37403
mjz584@mocs.utc.edu

ABSTRACT

Recently, smart health applications in remotely monitoring and automatically evaluating the wellbeing of patients have attracted interest of many researchers. These applications pose opportunities to violate security and privacy. The Heath Insurance Portability and Accountability Act (HIPPA) by the U.S. government regulate protection of security and privacy in medical data. The medical data in wireless health applications is gathered by wireless mobile sensors/devices and sent to clinical servers for analysis. An approach is required to protect patient privacy and mitigate possible risks during both data acquisition and transmission. To achieve such security and privacy of health data, we design a fuzzy authentication framework based on a fuzzy vault scheme, fingerprint biometric technique, and zero-knowledge authentication. Our protection has low overhead and is transparent and usable to patients who may not be technology-savvy.

Categories and Subject Descriptors

C.2.2 **[Computer-Communication Networks]:** Network Protocols; K.4.4 **[Computers and Society]:** Electronic Commerce - *Electronic data interchange (EDI), Security;* K.6.5 **[Management of Computing and Information Systems]:** Security and Protection - *Authentication*; E.3 **[Data]:** Data - *Public Key Cryptosystems.*

General Terms

Algorithms, Performance, Design, Reliability, Security, Theory, Legal Aspects, Verification

Keywords

Usable protection, fuzzy vault, zero-knowledge authentication, HIPPA.

1. INTRODUCTION

The wireless and mobile sensing technology is helping researcher to improve healthcare and wellness of patients in an innovative way. The autism research group at Georgia Technology Institute uses Smart Toys for automatic capture and annotation of developmental data [21]. The analysis and retrospective review of children's play behaviors help early identification of autism spectrum disorder and other developmental delays. The behavior data captured by automated devices are useful for monitoring the effectiveness of the interventions for behavioral and learning disabilities in children. Additionally, the wearable wireless sensors [22] help to accurately assess motor abilities of stroke survivors, which is important in selecting the best therapies for them. Wearable systems have the ability to measure motor behavior at home and for longer periods than could be observed in a clinical setting. Above systems usually have wearable wireless sensors to sense behavior data, assess them using standardized clinical rating scales, and then transit the analyzed data to clinical servers.

In this paper, we present a solution to protect the medical data against security and privacy violation while gathering, processing, and transmitting the data. The Heath Insurance Portability and Accountability Act (HIPPA) by the U.S. government regulate protection of security and privacy in medical data [1]. This protection needs to be transparent to patients, since they are not trained with knowledge of information security such as encryption and biometrics. Therefore, challenges in developing usable protection to health data are two folds. 1) Our system need to be robust against following threats and risks: i) wearable sensors may be lost or stolen; ii) wearable sensors may be used by unauthorized users; iii) wireless communication channel may be recorded, sniffed, or injected, iv) replay attack may occur during authentication. 2) Our protection method needs to be transparent and usable to patients with low overhead. To achieve such a protection method, we design a novel authentication framework based on a fuzzy vault scheme [7], fingerprint biometric technique, and zero-knowledge authentication [5]. Communication and access of health data are protected by authentication and encryption. We use fingerprint biometrics to authenticate patients to the mobile wireless sensors/devices because fingerprint biometrics is accurate and easy to collect. We integrate the fingerprint biometrics with a fuzzy vault scheme [2] zero-knowledge protocol [3] to provide adjustable authentication. The secret locked in wireless devices is used to encrypt health related data to protect privacy of patients. Our framework complies with HIPPA [1], and aim to transparently protect users and health data transmission under above four kinds of threats.

2. RELATED WORK

The fuzzy vault is an example of recent work that focuses on combining cryptography and biometrics to take advantage of both fields [14, 4]. The traditional cryptography does not provide adjustable levels of security or authentication but biometrics provide both non-repudiation and convenience. The fuzzy vault scheme has been recently applied to the field of body area sensor network [8, 5, 6, 7, 9]. However, Scheirer et al. [12] suggests a number of attacks targeting on the fuzzy vault scheme such as record multiplicity and blended substitution attacks. The attacks via record multiplicity assume that an attacker intercepts multiple encodings which are created using the same biometric data (e.g. two fuzzy vaults created using templates of the same fingerprint, but different chaff points). The blended substitution attack considers the scenario where a malicious attacker injects his own data into someone's template. The work by Kholmatov [13] realized correlation attack against the fuzzy vault scheme. Our approach counters the substitution and correlation attacks by integrating fuzzy vault scheme with zero-knowledge authentication, from which the encodings of biometric data are not sent through communication channels.

3. BACKGROUND

3.1 Fuzzy Vault Scheme

Utilizing fingerprint minutiae templates as encryption keys introduces a layer of inconsistency into the decryption process. This lack of exact key reproduction greatly increases the amount of errors encountered by the user wishing to unlock the secret. An error tolerant cryptographic algorithm is required to allow for this variance found within the biometric lock as each presented minutiae template could differ simply by altering the pressure placed on the fingerprint reader. Such error tolerant algorithms rely on meeting a threshold of key features of the key [2, 8].

The fuzzy vault scheme utilizes the polynomial reconstruction problem to secure a secret. Each fingerprint minutiae template generated produces some level of variation, and this variation inherently leads to each template examined as an unordered set. The set of unordered minutiae points *P* are utilized to generate polynomial projections, and randomly generated, unassociated chaff points are layered on top of the generated projects to lock the secret within the vault [2, 8].

Presenting a template to unlock the vault undergoes the same polynomial projection process. No chaff points are used when unlocking the vault. Instead, the fuzzy vault scheme relies on a given threshold of points on both the unlocking template *Q* and the locking polynomial. This threshold provides a level of tolerance for biometric inconsistencies given the biometric data is properly aligned with little noise. A user might need to present multiple minutiae templates before unlocking the secret *S* from the polynomial if either the threshold is set too high to produce ample overlap of the polynomial points. The security of the fuzzy vault scheme relies on the number of chaff points inserted into the polynomial projections. It is common for the number of chaff points to exist as some order of magnitude larger than the number of points within the minutiae template [2, 8].

3.2 Zero-Knowledge Authentication

Acknowledgement of a secret's authentication without exposing any information about the secret is crucial in sensitive environments. Zero-knowledge authentication presents a verifier with a randomized statement of proof to demonstrate the secret is known. Often, multiple, randomized statements are issued to filter malicious attempts. Once the verifier is convinced of the provider's knowledge authentication is granted. Zero-knowledge based authentication provides a layer of security to implemented encryption mechanisms as the decryption process can occur within an environment more likely to be free of potential eavesdroppers. Sending only a verification statement of successful decryption prevents unwanted access to the data being secured. The security of zero-knowledge authentication increases with the number of issued challenges by the verifier and the complexity of the statement randomization.

The protocol behind zero-knowledge authentication is the Feige-Fiat-Shamir protocol [11]. This protocol implements the proofs of zero-knowledge through the two entities *Prover* and *Verifier*. The Prover selects two large integers p and q to generate the product $n = pq$. The Prover then generates a private and public vector such that the remainder upon division with n yields the same remainder. This vector is sent to the Verifier.

Upon reception, the Verifier awaits a randomly generated integer from the Prover to unlock the vector. Once unlocked, the Verifier computes a value and sends it to the Prover as the first step of verification. The Prover uses this value to affirm the Verifier's request and returns a value representing this condition. If the Verifier can validate this response the Prover is authenticated.

4. OUR SYSTEM

Our designed protection complies with the Health Insurance Portability and Accountability Act (HIPAA) [1] requirements to be a trustworthy platform and toolkit. The HIPPA requires a unique identifier for tracking user identity, technical security measures to guard against unauthorized access to the health information while it is being transmitted over a network, data integrity, and an access control scheme be applied to the system to control access to the electronic information [1]. Moreover, our protection is provides usable security which means it is transparent to users and plug-n-play. Fingerprint biometrics is chosen to authenticate patients because of its security, accuracy and convenience as it does not require patients to remember password or carry authentication tokens or keys. The fuzzy vault scheme [7] is based on binding the biometric template with a secret key and scrambling it with a large amount of redundant data, such that it is computationally infeasible to extract eh secret key without possession of the biometric trait.

To mitigate attacks to fuzzy vault scheme and preserve usability from fingerprint biometric, we integrate the fuzzy scheme with zero-knowledge authentication. The advantage of zero-knowledge authentication is that the claimant proves to the verifier that she knows a secret, without revealing it. The interactions between claimant (Smart phone) and verifier (Clinic Server) are so designed that they cannot lead to revealing or guessing the secret. Zero-knowledge protocol (we use Feige-Fiat-Shamir Protocol [11]) is secure because it does not send out secret of claimant. Our protocol contains five steps: 1) locking secret data in secure vault with fingerprint template; 2) claimant sends witness to verifier to initiate authentication; 3) verifier sends challenges (0 or 1) to claimant; 4) the claimant unlock vaults and calculate the response; and 5) claimant sends responses to verifier as shown in Figure 1. From above five steps, the patient is authenticated by presenting fingerprint biometric data to decode secret S in vault and the device is authenticated by proving possession of secret S. This protects our application against smart phone tampering or loss.

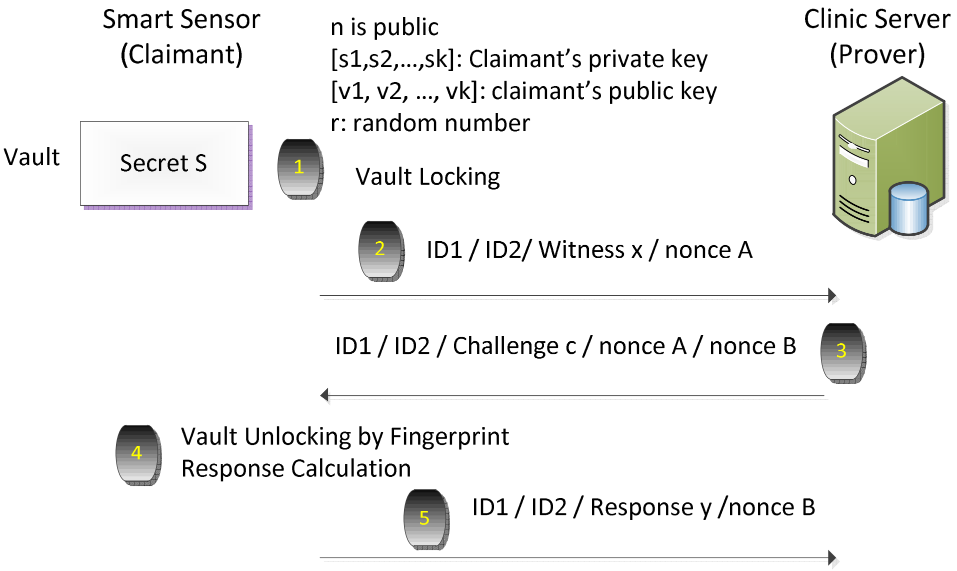
Smart Sensor
(Claimant)
n is public
[s1,s2,…,sk]: Claimant's private key
[v1, v2, …, vk]: claimant's public key
r: random number
Clinic Server
(Prover)
Vault
Secret S
1
Vault Locking
2
ID1 / ID2/ Witness x / nonce A
ID1 / ID2 / Challenge c / nonce A / nonce B
3
4
Vault Unlocking by Fingerprint
Response Calculation
5
ID1 / ID2 / Response y /nonce B

Figure 1. Authentication based on a fuzzy vault scheme and zero-knowledge protocol

The first step in our protocol is to lock secret *S* in a secure vault using fingerprint of patients. The second step sends the identity of smart sensor, clinic server, witness and nonce A to initiate the authentication with $x = s^2 \bmod n$ where *s* is the secret data, *n* is public, *r* is a random number less than *n*. The secret *S* contains $s_1, s_{2,} ..., s_k$ is claimant's private key, and $v = [v_1, v_2, ..., v_k]$ is the public key of claimant. The verifier challenges the claimant in the third step with a challenge $c = [c_1, c_2, ..., c_k]$ with the value of c's 0 or 1. The claimant unlock secret S using fingerprint template of patients and calculate response $y = (rs_1^{c_1} s_2^{c_2}, ..., s_k^{c_k}) \bmod n$ in the fourth step, and reply to verifier in in the fifth step during authentication. The nonce *A* and nonce *B* are only used once to counter replay attacks during authentication. The fuzzy vault is a construct used to lock the secret (*S*) using a set of values *P* [2], which are fingerprint templates in our application. Once the vault has been locked, it can be unlocked only with another set of values *Q* which has a significant number of values in common with set *P*. We use fingerprint template of the same patient as set of values *Q*. The construction and locking of vault is accomplished by: 1) generating a *vth* order polynomial p over the variable *x* that encodes the secret *S*, 2) computing the value of the polynomial at different values of x from set *P* and creating a set $R = \{a_i, p(a_i)\}$, where $1 \leq i \leq |A|$, and 3) adding randomly generated set of points called chaff to *R* which do not lie on the polynomial. Once the vault is constructed, unlocking it based on the set *Q* is done by constructing a set $P' = \{(u,v) | (u,v) \in R, u \in Q\}$. The unlock process is possible only if *Q* has significant number of legitimate points while are on the polynomial [2]. Our protocol preserves privacy of patient biometric data because no biometric template or fuzzy vault concealed by biometric template is transmitted through network, which protect us against correlation attack [13]. Our protocol is secure because the secret data is concealed and protected by biometric data. The claimant authenticates itself by proving the possession of biometric data and secret data to verifier without sending it. Moreover, our protocol is also robust against replay attack by adding nonce in communication between claimant and verifier. The nonce can be used only once so that it cannot be replayed by attackers.

The secret key unlocked by patient fingerprint is used to generate stream key in RC4 [10] cipher, which is used to encrypt data of patients. RC4 is an efficient stream cipher to encrypt real-time data. This enables efficient encryption for data collected by sensors attached to limbs of patients because only exclusive-or operation is perform during byte-based encryption. This conforms to transmission security in HIPPA [1]. We further reduce overhead of encryption by pre-process key generation before real-time encryption.

5. SYSTEM ANALYSIS

Our system is secure when wearable sensors are lost or stolen because unauthorized users cannot authenticate themselves and unlock stored secret by their fingerprint. The privacy of patients are protected because fingerprint template of patients will not be sent over wireless network, but only used to unlock the secret stored in the wearable sensors or mobile devices. The protection is robust under sniffing and injection attacks because neither the biometrics template nor the secret is sent to server for authentication. The protection is against replay attacker when we use nonce in step 2 and step 3 shown in Figure 1. The nonce is used once and discarded by the remote server; therefore, replayed nonce will not be accepted.

6. CONCLUSION

We have presented a usable protection to systems that continuously monitor patient behavior data using wearable wireless sensors to comply with HIPPA. Our novel protection is based on fuzzy vault scheme and zero-knowledge authentication. The fingerprint biometrics is used to increase usability and flexibility of the system. Our approach is robust to security threats such as unauthorized access, network sniffing, and replay attack.

7. ACKNOLEDGEMENT

This work is partially supported by NSF DUE-0942581, DUE-1129444, and Tennessee Higher Education Commission's Center of Excellence in Applied Computational Science and Engineering.

8. REFERENCES

[1] HIPPA. http://www.hhs.gov/ocr/privacy/.

[2] A. Juels and M. Sudan. A fuzzy vault scheme. In IEEE International Symposium on Information Theory, 2002.

[3] S. Goldwasser, S. Micali, and C. Racko. The knowledge complexity of interactive proof systems. SIAM Journal on Computing, 18(1):186-208, 1989.

[4] U. Uludag, S. Pankanti, and A. K. Jain. Fuzzy vault for fingerprints. *In Proceedings of Audio- and Video-Based Biometric Person Authentication (AVBPA)*, Lecture Notes in Computer Science 3546, pages 310-319. Springer, 2005.

[5] F. M. Bui and D. Hatzinakos. Biometric methods for secure communications in body sensor networks: resource-efficient key management and signal-level data scrambling. EURASIP J. Adv. Signal Process, 2008:109:1-109:16, January 2008.

[6] S. Cherukuri, K. K. Venkatasubramanian, S. K. Gupta, and E. K. Gupta. Biosec: A biometric based approach for securing communication in wireless networks of biosensors implanted in the human body. In Workshop on Wireless Security and Privacy (WiSPr), 2003.

[7] E. S. Reddy and I. R. Babu. Authentication using fuzzy vault based on iris textures. In the Second Asia International Conference on Modeling Simulation (AICMS), pages 361 - 368, May 2008.

[8] K. K. Venkatasubramanian, A. Banerjee, S. K. S. Gupta, and K. S. Sandeep. PSKA: usable and secure key agreement scheme for body area networks. Transaction on Information Technology Biomedicine, 14:60-68, January 2010.

[9] K. K. Venkatasubramanian, A. Banerjee, and S.K.S. Gupta. EKG-based key agreement in body sensor networks. In IEEE INFOCOM Workshops, pages 1 -6, April 2008.

[10] RC4. http://www.rsa.com/rsalabs/node.asp?id=2250.

[11] U. Feige, A. Fiat, and A. Shamir. Zero-knowledge proofs of identity.Journal of Cryptology, pages 77-94, 1988.

[12] W.J. Scheirer and T.E. Boult. Cracking fuzzy vaults and biometric encryption. In Biometrics Symposium, pages 1 {6, September 2007.

[13] A. Kholmatov and B. Yanikoglu. Realization of correlation attack against fuzzy vault scheme. In Society of Photo-Optical Instrumentation Engineers (SPIE) Conference Series, volume 6819, March 2008.

[14] C.C.Y. Poon, Y. T. Zhang, and S. D. Bao. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. IEEE Communications Magazine, 44(4):73-81, April 2006.

[15] In Proceedings of Audio- and Video-Based Biometric Person Authentication (AVBPA), Lecture Notes in Computer Science 3546, pages 310-319. Springer, 2005.

[16] T. L. Westeyn, G. D. Abowd, T. E. Starner, J. M. Johnson, P. W. Presti and K. A. Weaver, Monitoring children's developmental progress using augmented toys and activity recognition, *Proceedings of International Meeting for Autism Research (IMFAR)*. Chicago, IL, May 7-9, 2009.

[17] A. Parnandi, E. Wade, M. Matarić, Motor function assessment using wearable inertial sensors, *Engineering in Medicine and Biology Society (EMBC), 2010 Annual International Conference of the IEEE* , vol., no., pp.86-89, Aug. 31 2010-Sept. 4 2010.