Further Enhanced Authentication Scheme for Telemedicine Systems

Hong Jiang, Baoyuan Kang, Lin Si, Mingming Xie

Abstract— **Telemedicine system allows patients at home can access the medical services. But the security and integrity of transmitting data should be guaranteed. Recently, to telemedicine system, Lu et al. proposed a biometric based authentication scheme combining password and smart card, and claimed that their scheme satisfies many security properties. But, in this paper, we show that Lu et al.'s scheme is vulnerable to anonymity attack, and based on anonymity attack the attacker then can conduct user and server impersonation attack. Furthermore, we proposed improved scheme. Security analyses show that our improved scheme not only overcomes the flaws of Lu et al.'s scheme but also keeps its merits and satisfies more security properties.**

Index Terms—**Authentication Scheme; Telemedicine System; Biometric; Security**

I. INTRODUCTION

With the developments of telecommunication and the mobile networks technology, telemedicine allows patients at home can access the medical services as at hospital. Telemedicine also allows doctors in multiple locations to share information and discuss cases. Telemedicine greatly reduces the cost of medical care and provides a lot of convenience to the patients. But the patients' sensitive data may be eavesdropped by an illegal entity due to the openness of communication environment. Therefore, the protection of patient's privacy is a key issue. Generally, communication entities can use authentication schemes [1, 2] to authenticate each other and guarantee sensitive data security. Many authentication schemes were proposed for various applications [3-14]. Secure authentication schemes, which guarantees confidential and authorized interaction between the patient and remote server, are essential to telemedicine system [15].

In the past, for telemedicine system, a lot of authentication schemes based on password were proposed [16-21]. But authentication schemes only based on password are vulnerable to password guessing attack. Recently, to telemedicine system, many biometric based authentication schemes combining password and smart card were proposed [22-26]. Compared to password, biometrics keys cannot be forged and cannot be guessed easily. In 2013, Awasthi et al. [22] proposed a biometric authentication scheme for telemedicine system with nonce. However, in 2014, Mishra et al. [23] and Tan et al.[24] pointed that Awasthi et al.'s scheme was vulnerable to password guessing attack and user anonymity attack. Tan et al. also proposed a three factor authentication scheme to remedy the weaknesses of Awasthi et al.'s scheme. But, Arshad et al. [25] showed that Tan et al.'s scheme did not withstand denial-of service and replay attacks. They also presented an improved scheme. However, in 2015, Lu et al. [26] showed that Arshad et al.'s scheme [25] fails to protect against off-line password guessing attack and showed that in case the adversary succeeded in getting identity and password of an arbitrary user, he can impersonate any user of the system. Furthermore, they proposed an enhanced Biometric-Based authentication Scheme for telemedicine information systems. But, in this paper, we show that Lu et al.'s scheme is vulnerable to anonymity attack, and based on anonymity attack the attacker then can conduct user and server impersonation attack. Furthermore, we proposed improved scheme. Our improved scheme not only overcomes the flaws of Lu et al.'s scheme but also keeps its merits and satisfies more security properties.

The rest of the paper is organized as follows. In Section 2, we review Lu et al.'s scheme and show its weaknesses. In Section 3, we propose an improved authentication scheme for telemedicine system. The security analyses of the proposed scheme are given In Section 4. Conclusion is given in Section 5.

II. LU ET AL.'S SCHEME AND ITS WEAKNESSES

In 2015, Lu et al. [26] proposed an enhanced biometric-based authentication scheme for telemedicine information systems. There are two participants, one patient and one server in their scheme. The patient and the server will complete mutual authentication and generate session key. In this section we review Lu et al.'s scheme and show its flaws

A Lu et al.'s scheme

Lu et al.'s scheme contains three phases: registration, authentication and password change.

Registration

(1) The patient U inputs his biometric B_i , identity ID_i and password PW_i . Then, U calculates

$$MP_i = PW_i \oplus H(B_i)$$

and submits $\{ID_i, MP_i\}$ to the server S.

(2) When receiving the message, S computes $AID_i = ID_i \oplus h_2(x)$, $V_i = h_1(ID_i \| MP_i)$ and issues a smart card SCi which contains the information $\{AID_i, V_i, h_1(), h_2()\}$ to U

Login and Authentication

(1) U inserts SCi into a card reader and keys his identity ID_i ,

Manuscript received June 20, 2018

Hong Jiang, School of Management, Tianjin polytechnic university, Tianjin, 300387, China,

Baoyuan Kang, School of Computer science and software, Tianjin polytechnic university, Tianjin, 300387, China

Lin Si, School of Computer science and software, Tianjin polytechnic university, Tianjin, 300387, China

Mingming Xie, School of Computer science and software, Tianjin polytechnic university, Tianjin, 300387, China

password PW_i and biometric B_i . SCi computes $h_1(ID_i \| PW_i \oplus H(B_i))$ and verifies whether it is equal to the value V_i . If true, *U* passes through the verification. Then, SCi selects a random number d_u and computes

$K = h_1(ID_i \| ID_i \| AID_i)$,

$M_1 = K \oplus d_u P$, $M_2 = h_1(ID_i \| T_1 \| d_u P)$

and transmits $\{M_1, M_2, AID_i, T_1\}$ to *S*.

(2) When receiving the login request, S first examines whether $|T_1 - T_C| < \Delta T$, where T_C is the current timestamp of the *S*. If holds, *S* uses his private key *x* to derive ID_i by computing $M_1 \oplus h_2(x)$, he then computes $d_u P = K \oplus M_1$ and checks

$h_1(ID_i \| T_1 \| d_u P) = ?M_2$.

If correct, *S* then generates a random number d_S and computes

$M_3 = K \oplus d_S P$,

SK = dsduP,

$M_4 = h_1(K \| T_2 \| SK \| d_u P)$,

where T_2 is the current timestamp. At last, *S* sends the message $\{M_3, M_4, T_2\}$ to U .

(3) Upon receiving the message, *U* first checks the freshness of T_2 . Then, *U* retrieves $d_S P$ by computing $M_3 \oplus K$ and computes

SK = dudsP, $M_4' = h_1(K \| T_2 \| SK \| d_u P)$

to verify whether M_4' is equal to the received M_4 . If holds, *U* computes $M_5 = h_1(K \| d_S P \| SK \| T_3)$ and then sends the message $\{M_5, T_3\}$ to *S*, where T_3 is the current timestamp.

(4) After receiving $\{M_5, T_3\}$, *S* verifies whether $|T_3 - T_C| < \Delta T$ and

$M_5' = h_1(K \| d_S P \| SK \| T_3) = M_5$.

If both conditions hold, *S* authenticates *U* and accepts *SK* as the session key for further operations.

Password change

If U doubts his password may be leaked, he can alter the old password to a new one as follows. *U* inserts his SCi into the device and submits his ID_i , PW_i and B_i . Then SCi verifies whether $h_1(ID_i \| PW_i \oplus H(B_i)) = ?V_i$. If valid, *U* inputs a new password PW^{new} , SCi calculates $V_i^{new} = h_1(ID_i \| PW^{new} \oplus H(B_i))$, then replaces V_i with V_i^{new}

B The weaknesses of Lu et al.'s scheme

This section shows that Lu et al.'s scheme [26] has some security drawbacks, which are discussed in the following subsections. The following attacks are based on the assumptions that a malicious attacker has completely monitor over the communication channel connecting *U* and *S* in login and authentication phase. So the attacker can eavesdrop, modify, insert, or delete any message transmitted via public channel.

The user anonymity attack

Once user U_j intercepts the message $\{M_1, M_2, AID_i, T_1\}$ sent to S by user U_i , the user U_j can obtain the real identity of the user U_i from intercepted AID_i and its AID_j , ID_j .

In fact, since

$AID_i = ID_i \oplus h_2(x)$, $AID_j = ID_j \oplus h_2(x)$.

So,

$AID_i \oplus AID_j = ID_i \oplus ID_j$.

Then,

$ID_i = ID_j \oplus AID_i \oplus AID_j$.

Therefore, using his identity information ID_j and AID_j , the user U_j can compute the real identity of the user U_i from the intercepted information AID_i .

The server impersonation attack

Based on the above described anonymity attack, the user U_j can further conduct the server impersonation attack with the intercepted information $\{M_1, M_2, AID_i, T_1\}$.

With the computed real identity of the user U_i from the he above described anonymity attack, the attacker U_j can compute

$K = h_1(ID_i \| ID_i \| AID_i)$, $d_u P = K \oplus M_1$.

Then U_j as the real server generates a random number d_S and computes

$M_3 = K \oplus d_S P$,

SK = dsduP,

$M_4 = h_1(K \| T_2 \| SK \| d_u P)$,

where T_2 is the current timestamp. At last, U_j sends the message $\{M_3, M_4, T_2\}$ to U_i , and U_i cannot find any impersonation. The user U_j successfully counterfeits the patient U_i .

The user impersonation attack

Based on the above described anonymity attack, the user U_j can also conduct the user impersonation attack with the intercepted information $\{M_1, M_2, AID_i, T_1\}$, since the attacker U_j can as the user U_i compute

$K^* = h_1(ID_i \| ID_i \| AID_i)$,

$M_1^* = K^* \oplus d_u^* P$, $M_2^* = h_1(ID_i \| T_1^* \| d_u^* P)$

in time T_1^* and U_j can finish the next steps as the patient U_i in authentication phase. So, the user U_j can successfully impersonate user U_i to cheat the server.

III. THE PROPOSED SCHEME

This section presents a slight modification scheme to overcome the weaknesses of Lu et al.'s scheme. In the proposed scheme, in order to resist the user anonymity attack, the server employs a random number in registration phase. The proposed scheme also contains three phases: registration, login and authentication and password updating.

A Registration

(1) $U_i \rightarrow S : \{ID_i, MP_i\}$

The patient U_i inputs his biometric B_i , identity ID_i and password PW_i . Then, U_i calculates

$MP_i = PW_i \oplus H(B_i)$

and submits $\{ID_i, MP_i\}$ to the server *S*.

(2) $S \rightarrow U_i : \{AID_i, V_i, N_i, h_1(), h_2()\}$

On receiving the message, *S* chooses a random number N_i and computes

$AID_i = ID_i \oplus h_2(x \| N_i)$, $V_i = h_1(ID_i \| MP_i)$

and issues a smart card SCi which contains the information $\{AID_i, V_i, N_i, h_1(), h_2()\}$ to U_i

B Login and Authentication

(1) $U_i \rightarrow S : \{M_1, M_2, AID_i, N_i, T_1\}$

U_i inserts SCi into a card reader and keys his identity ID_i , password PW_i and biometric B_i . SCi computes and verifies whether

$h_1(ID_i \| PW_i \oplus H(B_i)) = V_i$.

If true, SCi chooses a random number d_i and computes

$K = h_1(ID_i \| ID_i \oplus AID_i)$,

$M_1 = K \oplus d_i P$, $M_2 = h_1(ID_i \| T_1 \| d_i P)$

and transmits $\{M_1, M_2, AID_i, N_i, T_1\}$ to *S*.

(2) $S \rightarrow U_i : \{M_3, M_4, T_2\}$

Upon receiving the login request, *S* first examines whether $|T_1 - T_C| < \Delta T$, where T_C is the current timestamp of the *S*. If holds, *S* uses his private key *x* and received N_i to derive

$ID_i = AID_i \oplus h_2(x \| N_i)$,

then computes

$K = h_1(ID_i \| ID_i \oplus AID_i)$

and

$d_i P = K \oplus M_1$.

Then *S* checks

$h_1(ID_i \| T_1 \| d_i P) = ? M_2$.

If correct, *S* generates a random number d_S and computes

$M_3 = K \oplus d_S P$,

$SK = d_S(d_i P)$,

$M_4 = h_1(K \| T_2 \| SK \| d_i P)$,

where T_2 is the current timestamp. At last, *S* sends the message $\{M_3, M_4, T_2\}$ to U_i .

(3) $U_i \rightarrow S : \{M_5, T_3\}$

Upon receiving the message, U_i first checks the freshness of T_2 . Then, U_i retrieves $d_S P = M_3 \oplus K$ and computes $SK = d_i(d_S P)$ .Then U_i verify whether $M_4' = h_1(K \| T_2 \| SK \| d_i P) = ? M_4$.

If sure, U_i computes $M_5 = h_1(K \| d_S P \| SK \| T_3)$ and sends the message $\{M_5, T_3\}$ to *S*, where T_3 is the current timestamp.

(4) After receiving $\{M_5, T_3\}$, *S* verifies whether

$|T_3 - T_C| < \Delta T$

and

$M_5' = h_1(K \| d_S P \| SK \| T_3) = ? M_5$.

If both conditions hold, *S* authenticates U_i and accepts *SK* as the session key for further communication.

C Password change

On demand for update password, U_i inserts his SCi into the device and submits his ID_i , PW_i and B_i . Then SCi verifies whether $h_1(ID_i \| PW_i \oplus H(B_i)) = ? V_i$. If sure, U_i inputs a new password PW' , SCi calculates $V_i' = h_1(ID_i \| PW' \oplus H(B_i))$,then replaces V_i with V_i'

IV. SECURITY ANALYSIS OF THE PROPOSED SCHEME

This section analyses the security of the proposed scheme under the assumptions that a malicious attacker can eavesdrop, modify, insert, or delete any message transmitted via public channel [26].

Compared with Lu et al.'s scheme [26], since there is a slight modification in the improved scheme, many security properties of Lu et al.'s scheme are kept. To remedy the flaws of Lu et al.'s scheme, here we only analyses the ability of the proposed scheme to resist user anonymity attack and impersonation attack.

User anonymity

In the proposed scheme, the identity of the patient U_i is protected by AID_i , and

$AID_i = ID_i \oplus h_2(x \| N_i)$, $AID_j = ID_j \oplus h_2(x \| N_j)$.

So,

$AID_i \oplus AID_j = ID_i \oplus ID_j \oplus h_2(x \| N_i) \oplus h_2(x \| N_j)$

.

Then

$ID_i = AID_i \oplus AID_j \oplus ID_j \oplus h_2(x \| N_i) \oplus h_2(x \| N_j)$

Since the random number N_i is not equal to the random number N_j , $h_2(x \| N_i) \oplus h_2(x \| N_j)$ is not zero string. Even if the attacker know the two random number N_i and N_j , since the attacker does not know the private key x of the server, he cannot obtain the identity information of the

patient U_i by the attack method described above.

Impersonation attack

The attacker who does not know the identity information of user, then cannot compute

$K = h_1(ID_i \| ID_i \| AID_i)$.

So, the attack methods describedabove are infeasible to the proposed scheme, the proposed scheme is secure against the user and server impersonation attacks.

V. Conclusion

In this paper, we show that Lu et al.'s authentication scheme for telemedicine system is vulnerable to anonymity attack, and based on anonymity attack the attacker then can conduct user and server impersonation attack. Furthermore, we proposed improved scheme. Security analyses show that our improved scheme not only overcomes the flaws of Lu et al.'s scheme but also keeps its merits.

Acknowledgment

This work is supported by the Applied Basic and Advanced Technology Research Programs of Tianjin (No. 15JCYBJC15900).

References

[1] Abdalla, M., Fouque, PA., Pointcheval, D., "Password-based authenticated key exchange in the three party setting". In: International conference on theory and practice in public key cryptography, pp 65–84, 2005

[2] Kang, B., Han, J., "Cryptanalysis and improvement on three-party protocols for password authenticated key exchange", ICETC 2010 - 2010 2nd International Conference on Education Technology and Computer, v 5, p V5197-V5201, 2010, ICETC 2010 - 2010 2nd International Conference on Education Technology and Computer

[3] Amin, R., Islam, SH., Biswas, GP., Khan MK., Leng L., Kumar N., "Design of an anonymity-preserving three-factor authenticated key exchange protocol for wireless sensor networks". Comput Netw 101: 42–62, 2016

[4] Challa, S., Wazid, M., Das, AK., Kumar, N., Reddy, AG., Yoon, EJ., Yoo, KY., "Secure signature-based authenticated key establishment scheme for future iot applications". IEEE Access 5:3028–3043, 2017

[5] Das, AK., "A secure and robust temporal credential-based three-factor user authentication scheme for wireless sensor networks". Peer-to-Peer Networking and Applications 9(1):1–22 , 2016

[6] Ding, W., Ping, W., "Two birds with one stone: two-factor authentication with security beyond conventional bound". IEEE Trans Dependable Secure Comput PP(99):1–10, 2016

[7] Doshi, N., Kumari, S., Mishra, D., Li, X., Choo, K., Sangaiah, AK., "A password based authentication scheme for wireless multimedia systems". Multimedia Tools & Applications 1:1–26, 2017

[8] Jiang, Q., Khan, MK., Lu, X., Ma, J., He, D., "A privacy preserving three-factor authentication protocol for e-health clouds". J Supercomput 72(10):3826–3849, 2016

[9] Khan, MK., Kumari, S., Gupta, MK., "More efficient key-hash based fingerprint remote authentication scheme using mobile device". Computing 96(9):793–816, (2014)

[10] Kumari, S., Das, AK., Wazid, M., Li, X., Wu, F., Choo, KR., Khan, MK., "On the design of a secure user authentication and key agreement scheme for wireless sensor networks". Concurrency & Computation Practice & Experience 29(23):1–18, (2016)

[11] Nam, J., Choo, K., Han, S., Kim, M., Paik, J., Won, D. "Efficient and anonymous two-factor user authentication in wireless sensor networks: achieving user anonymity with lightweight sensor computation". PLoS ONE 10(4):e0116709, 2015

[12] Gao, T., Wang, Q., Wang, X., Gong, X., "An Anonymous Access Authentication Scheme Based on Proxy Ring Signature for CPS-WMNs", Mobile Information Systems ,Volume 2017 (2017), Article ID 4078521, 11 pages

[13] Lee, Y., Paik, J., "Security Analysis and Improvement of an Anonymous Authentication Scheme for Roaming Services", The Scientific World Journal ,Volume 2014 (2014), Article ID 687879, 8 pages

[14] Li, l., "Analysis and Enhancement of a Password Authentication and Update Scheme Based on Elliptic Curve Cryptography", Journal of Applied Mathematics ,Volume 2014 (2014), Article ID 247836, 11 pages

[15] Chiou, S., Lin, C., "An Efficient Three-Party Authentication Scheme for Data Exchange in Medical Environment, Security and Communication Networks " , Volume 2018 (2018), Article ID 9146297, 15 pages

[16] Khan, M., Kumari, S., Cryptanalysis and Improvement of "An Efficient and Secure Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems", Security and Communication Networks, v 7, n 2, p 399-408, 2014.

[17] Zhao, Y., Zhang, C., "Cryptanalysis and improvement of an authentication scheme for telecare medical information systems", International Journal of Electronic Security and Digital Forensics, v 6, n 3, p 157-168, 2014

[18] Siddiqui, Z., Abdullah, A., Khan, M., Alghamdi, A., "Cryptanalysis and improvement of a secure authentication scheme for telecare medical information system with nonce verification", Peer-to-Peer Networking and Applications, v 9, n 5, p 841-853, 2016

[19] Sun, Y., "An improved password authentication scheme for telecare medical information systems based on chaotic maps with privacy protection", Journal of Information Hiding and Multimedia Signal Processing, v 7, n 5, p 1006-1019, 2016

[20] Li, C.T., and Hwang, M.S., "An efficient biometrics-based remote user authentication scheme using smart cards". J. Netw. Comput. Appl. 33(1):1–5, 2010.

[21] Chang, C., Lee, J., Lo, Y., Liu, Y., "A secure authentication scheme for telecare medical information systems", Smart Innovation, Systems and Technologies, v 63, p 303-312, 2017, Advances in Intelligent Information Hiding and Multimedia Signal Processing - Proceeding of the 12th International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 2016

[22] Awasthi, A.K., and Srivastava, K., "A biometric authentication scheme for telecare medicine information systems with nonce". J. Med. Syst. 37(5):1–4, 2013.

[23] Mishra, D., Mukhopadhyay, S., Kumari, S., Khan, M.K., Chaturvedi, A., "Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce". J. Med. Syst. 38(5):1–11, 2014.

[24] Tan, Z., "A user anonymity preserving three-factor authentication scheme for telecare medicine information systems". J. Med. Syst. 38(3):1–9, 2014.

[25] Arshad, H., and Nikooghadam, M., "Three-factor anonymous authentication and key agreement scheme for telecare medicine information systems". J. Med. Syst. 38(12):1–12, 2014.

[26] Lu, Y., Li, L., Peng, H., Yang Y., "An Enhanced Biometric-Based Authentication Scheme for Telecare Medicine Information Systems Using Elliptic Curve Cryptosystem", J. Med. Syst. 39(3):1–8, 2015