J Med Syst (2013) 37:9929
DOI 10.1007/s10916-013-9929-4

ORIGINAL PAPER

On the Security of A Dynamic ID-based Authentication Scheme for Telecare Medical Information Systems

Han-Yu Lin

Received: 30 November 2012 / Accepted: 14 January 2013 / Published online: 24 January 2013

Abstract Telecare medical information systems (TMISs) are increasingly popular technologies for healthcare applications. Using TMISs, physicians and caregivers can monitor the vital signs of patients remotely. Since the database of TMISs stores patients' electronic medical records (EMRs), only authorized users should be granted the access to this information for the privacy concern. To keep the user anonymity, recently, Chen et al. proposed a dynamic ID-based authentication scheme for telecare medical information system. They claimed that their scheme is more secure and robust for use in a TMIS. However, we will demonstrate that their scheme fails to satisfy the user anonymity due to the dictionary attacks. It is also possible to derive a user password in case of smart card loss attacks. Additionally, an improved scheme eliminating these weaknesses is also presented.

Keywords Telecare · Dynamic · Authentication · ID-based · Anonymity

Introduction

Healthcare has been paid more and more attention in countries with aging populations. Home healthcare are especially popular for recent years due to the development of telecommunication technology and the coming of low-cost mobile devices. A telecare medical information system (TMIS) is a kind of home healthcare techniques taking the advantages of Internet to remotely monitor patients' vital signs and allows physicians and caregivers to access and update medical information at any time. The medical information of patients is called electronic medical records (EMRs) which are as important as paper records and should be carefully protected for ensuring patients' privacy. Only authenticated users should be given the appropriate authorizations to access the resources of TMISs. To enforce strict access control policy, we have to adopt a secure remote user authentication scheme first.

Generally speaking, password based authentication schemes [6, 10, 12, 15, 16] are commonly utilized approaches in which each user first registers to the remote medical server with his identity (ID) and a chosen password. The medical server also keeps a password table for subsequent verifications. In 1981, Lamport [10] used one-way hash functions to propose a simple password authentication scheme in which the remote server stores hashed passwords to increase the security. However, his scheme could not withstand either the replay or impersonation attacks. Since user identity is also sensitive information when a patient with chronic diseases attempts to login the remote medical server, many researchers [1, 2, 4, 5, 7–9, 11, 13, 17–21, 23, 25–27] begin studying dynamic ID authentication schemes. Instead of using static ID, such schemes generate a different virtual ID with respect to each login session even for the same user, so as to fulfill user anonymity.

In 2004, Das et al. [4] proposed a dynamic ID-based remote user authentication scheme. A major characteristic of their scheme is that the server is unnecessary to store a password table, which releases the server-side burdens. Still, some researchers [1, 9, 11] pointed out their scheme is insecure under the server spoofing, impersonation and dictionary attacks. Later, several improved mechanisms [11, 21, 26] eliminating the drawbacks of Das et al.'s scheme are proposed.

In 2010, Tsai et al. [19] proposed a new dynamic ID authentication scheme using smart cards. Their scheme employed the concept of two-factor authentication, i.e.,

H.-Y. Lin (✉)
Department of Computer Science and Engineering,
National Taiwan Ocean University, 2, Beining Road,
Keelung, 202 Taiwan Republic of China
e-mail: lin.hanyu@msa.hinet.net

something you know (like passwords) and something you have (like smart cards). They also showed that previous works [21, 26] are vulnerable to the impersonation attack and could not satisfy the anonymous requirement of dynamic ID authentication schemes. Yet, the security of Tsai et al.'s scheme is based on the assumption of trusted servers, i.e., they did not consider the possibility of privileged insider attack in which a malicious remote server can easily derive legitimate users' passwords.

In 2012, Wu et al. [24] introduced an authentication scheme for TMISs. Their scheme is suitable for the mobile devices. By reviewing Wu et al.' scheme, He et al. [5] found out that their scheme is vulnerable to the impersonation and insider attacks and further addressed an enhanced variant. Yet, Wei et al. [22] pointed out a weakness of both their works [5, 24] and proposed a new scheme with two-factor authentication for TMISs. Later, Zhu [28] improved Wei *et al*'s scheme to withstand the off-line password guessing attacks. More recently, Chen et al. [3] came up with a dynamic ID-based authentication scheme for TMISs. Nevertheless, in this paper, we first demonstrate that the user identity of Chen et al.'s scheme will be compromised under the dictionary attack. A user password can be further derived with the smart card loss attacks. Then we give an enhanced variant to eliminate these weaknesses.

Chen et al.'s scheme and security weaknesses

In this section, we first briefly review Chen et al.'s scheme [3] and then shows their security vulnerabilities.

Review of *Chen* et al.'s scheme

Without loss of generality, Chen et al.'s scheme can be divided into registration, login, authentication and password change phases. Let x be the master secret of remote server and $h(\cdot)$ a collision-resistant one-way hash function. We describe each phase as follows:

Registration phase

A patient U_i associated with the identity ID_i first chooses his password pw_i and a random integer r_i to compute $RPW_i = h(r_i, pw_i)$. The information (ID_i, RPW_i) is then sent to the medical server S via a secure channel. Upon receiving it, the medical server S checks the validity of ID_i and then sets $N = 0$ in the registration records if ID_i is a new user. Note that when U_i re-registers to the remote server S due to smart card loss, the value N is increased by 1. Then S computes $J = h(x, ID_i, N)$, $L = J \oplus RPW_i$ and $y = h(RPW_i, ID_i)$, and delivers a smart card containing (L, y) to U_i via a secure channel. After receiving it, U_i stores r_i into the smart card.

Login phase

To login the remote TMIS, U_i first enters his (ID_i, pw_i) and the smart card computes $RPW_i = h(r_i, pw_i)$, $J = L \oplus RPW_i$, $C_1 = h(T_i, J)$ and $AID_i = ID_i \oplus h(y, T_i)$, where T_i is the current timestamp. Finally, the login request $\{AID_i, T_i, RPW_i, C_1\}$ is sent to the remote server S.

Authentication phase

Upon receiving the login request, S first verifies if $(T_i' - T_i) \leq \Delta T$ where T_i' is the timestamp of receiving time and ΔT is the valid time transmission interval. Otherwise, S rejects it. Then S searches the account database to find an ID_i' satisfying that $h(h(RPW_i, ID_i'), T_i) = AID_i \oplus ID_i'$. If it does not exist, S terminates the request. S further computes $J = h(x, ID_i', N)$ and verifies whether $C_1 = h(T_i, J)$. If it holds, ID_i' is authenticated.

Then S sends $\{C_2 = h(C_1, J, T_s), T_s\}$ where T_s is the current timestamp to U_i. After receiving it, U_i first checks if T_s is within the valid time transmission interval and then computes a session key $sk = h(C_2 \oplus J)$ for subsequent communication.

Password change phase

To change the password, the user U_i first enters his old and new passwords (pw_i, pw_i^*). Then the smart card computes $RPW_i' = h(r_i, pw_i)$, $y' = h(RPW_i', ID_i)$ and compares if $y' = y$. If it holds, the smart card proceeds to compute $L^* = L \oplus RPW_i' \oplus h(r_i, pw_i^*)$ and updates L as L^*.

Security weaknesses of Chen et al.'s scheme

We demonstrate that a malicious adversary can (i) reveal the user identity of Chen et al.'s scheme by plotting the dictionary attack and (ii) derive both the user identity and password in case of smart card loss attacks as follows:

(i) Dictionary attacks: An adversary first intercepts a login request $\{AID_i, T_i, RPW_i, C_1\}$ and chooses a candidate ID_j from the dictionary to check if

$$AID_i = ID_j \oplus h\left(h\left(RPW_i, ID_j\right), T_i\right).$$

If it does not hold, the adversary repeats the process until finding the correct one. As each user's identity is easily rememberable words, we claim that the dictionary attack is feasible.

(ii) Smart card loss attacks: Since every smart card stores $\{L, y, r\}$, an adversary picking up a lost smart card first retrieves the stored (y, r) and then chooses a pair of candidate (ID_j, pw_j) to perform the off-line password guessing by verifying whether

$$y = h\left(h\left(r, pw_j\right), ID_j\right).$$

If it holds, the adversary has found out the correct identity along with user's password.

Proposed scheme

In this section, we introduce an enhanced variant motivated by Zhu's scheme [28] and based on the famous RSA problem [14]. We define used notations as Table 1. The proposed scheme also consists of four phases as those defined in Chen et al.'s scheme. Initially, the medical server S selects two large primes (p, q), computes $N = pq$, chooses an integer e relatively prime to $(p-1)(q-1)$ and derives d satisfying $ed \equiv 1 \pmod{(p-1)(q-1)}$. The parameter d is the master secret of medical server S. Details of each phase are described as follows:

Registration phase

A patient U_i associated with the identity ID_i performs the following interactive steps with the remote server S:

Step 1 U_i chooses a password PW_i and an integer $t \in_R Z_N$ to compute

$$W_i = h(PW_i \oplus t), \tag{1}$$

and then sends (ID_i, W_i) to the server S via a secure channel.

Table 1 The used notations

p, q	two large primes
N	the product of p and q
S	medical server
e	the public key of medical server
d	the master secret of medical server
U_i	patient
ID_i	the identity of U_i
$t \in_R Z_N$	element t is a random integer in set Z_N
PW_i	password
$a \parallel b$	concatenation of a and b
$\oplus$	logical operation XOR
ΔT	valid transmission time interval

Step 2 Upon receiving it, the server S computes

$$n_i = W_i \oplus h(d \oplus ID_i), \tag{2}$$

and issues a smart card containing (N, n_i, e) to U_i via the secure channel.

Step 3 After receiving the smart card, U_i stores t into the smart card.

Login phase

To login the remote medical server S, U_i first enters his (ID_i, PW_i) and then the smart card chooses $k_i \in_R Z_N$ to compute:

$$W_i = h(PW_i \oplus t), \tag{3}$$

$$H_i = n_i \oplus W_i = h(d \oplus ID_i), \tag{4}$$

$$CID_i = h(H_i \oplus k_i), \tag{5}$$

$$R_i = h(CID_i, k_i, ID_i, T_1), \text{ where } T_1 \text{ is the current timestamp}, \tag{6}$$

$$X_i = (CID_i \| k_i \| ID_i)^e \bmod N, \tag{7}$$

The login request (X_i, R_i, T_1) is then sent to S.

Verification phase

S performs the following steps to authenticate requested user and generate a session key between them:

Step 1 Check if $(T_2 - T_1) \leq \Delta T$ where T_2 is the timestamp of receiving time and ΔT is the valid transmission time interval.

Step 2 If it holds, S computes

$$(CID_i \| k_i \| ID_i) = X_i^d \bmod N, \tag{8}$$

$$H_i' = h(d \oplus ID_i), \tag{9}$$

$$R_i' = h(h(H_i' \oplus k_i), k_i, ID_i, T_1), \tag{10}$$

and then checks if $CID_i = h(H_i' \oplus k_i)$ and $R_i' = R_i$; else, the session is terminated.

Step 3 S further computes

$$\lambda = h\left(H_i', CID_i, R_i', T_1, T_2\right), \tag{11}$$

$$V_s = h\left(\lambda, H_i', T_1, T_2\right), \tag{12}$$

and returns (V_s, T_2) to U_i.

Step 4 Upon receiving it, U_i checks if $(T_3 - T_2) \leq \Delta T$ where T_3 is the timestamp of receiving time. If it holds, U_i computes

$$\lambda' = h(H_i, CID_i, R_i, T_1, T_2), \quad (13)$$

$$V_s' = h\left(\lambda', H_i, T_1, T_2\right), \quad (14)$$

and then compares whether $V_s' = V_s$. If it holds, U_i and the medical server S have authenticated each other. The parameter λ is then used as a session key for subsequent communication.

Password-change phase

To change the password, U_i enters his old and new passwords (PW_i, PW_i'). Then the smart card computes

$$n_i' = n_i \oplus h(PW_i \oplus t) \oplus h\left(PW_i' \oplus t\right), \quad (15)$$

and updates n_i as n_i'.

Security Analyses

We give some discussions in relation to the security of the proposed scheme. We show that our scheme is secure against following existential attacks:

i. ***Can the proposed scheme withstand ID-theft attacks?***

In the login phase, a dynamic ID CID_i is not sent to the remote server S directly. It is embedded in the parameters (X_i, R_i) which are protected by the one-way hash function (OHF) and the intractable RSA problem. Even if an adversary successfully obtains CID_i, he cannot derive the real identity without the random number k_i and the master secret *d of the server S.*

ii. ***Can the proposed scheme withstand privileged insider attacks?***

When a user registers to a remote server, the server receives the user identity along with an encapsulated password $W_i = h(PW_i \oplus t)$. To derive the real password of user, a malicious server has to invert the OHF and know the random number t chosen by the user. Consequently, it is impossible for any malicious server to derive the real password of registered user.

iii. ***Can the proposed scheme withstand password guessing attacks?***

When an adversary attempts to plot the password guessing attack for intercepted messages (X_i, R_i, T_1), he will face the difficulty of inverting OHF and solving the RSA problem. Even if an insider attacker can obtain W_i from the secure channel, he also has to find out the random number t first.

iv. ***Can the proposed scheme withstand impersonation attacks?***

To impersonate a legitimate user, an adversary has to generate valid login request (X_i, R_i, T_1) for passing the server's authentication. However, without the real password of user, any adversary could not successfully pass the verification of remote server.

v. ***Can the proposed scheme withstand server spoofing attacks?***

To masquerade as a remote server in the verification phase, an adversary must return a valid response $V_s = h(\lambda, H_i', T_1, T_2)$. However, without the master secret d, the adversary cannot compute the correct V_s and will be detected by the user.

vi. ***Can the proposed scheme withstand stolen-verifier attacks?***

Since in the proposed scheme, the remote server is unnecessary to maintain a verification table, our scheme will not suffer from the stolen-verifier attack.

vii. ***Can the proposed scheme achieve forward secrecy?***

In the proposed scheme, a session key λ changes with different communication sessions. Therefore, even if the session key of previous session is accidentally compromised, the confidentiality of current communicated messages is still fulfilled.

viii. ***Can the proposed scheme withstand smart card loss attacks?***

A smart card stores the information of (N, n_i, e, t). An adversary obtaining a lost smart card still cannot derive user's password without the master secret d of remote server or generate a valid login request to pass the authentication.

Conclusions

Secure remote user authentication for TMISs is a vital application for home healthcare technologies. In this paper, we pointed out some weaknesses of recently proposed work, i.e., Chen et al.'s scheme. To eliminate these security drawbacks, we also proposed an enhanced variant and analyzed its security. The proposed scheme is more secure and thus appealing to the practical environments.

Acknowledgment We would like to thank anonymous referees for their valuable suggestions. This work was supported in part by the

National Science Council of Republic of China under the contract number NSC 101-2218-E-019-005.

References

1. Awasthi, A. K., Comment on a dynamic ID-based remote user authentication scheme. *Trans. Cryptol.* 1(2):15–16, 2004.
2. Chen, C., He, D., Chan, S., Bu, S. J., Gao, Y., and Fan, R., Lightweight and provably secure user authentication with anonymity for the global mobility network. *Int. J. Commun. Syst.* 24 (3):347–362, 2011.
3. Chen, H. M., Lo, J. W., and Yeh, C. K., An efficient and secure dynamic ID-based authentication scheme for telecare medical information systems. *J. Med. Syst.* 36(6):3907–3915, 2012.
4. Das, M. L., Saxana, A., and Gulati, V. P., A dynamic ID-based remote user authentication scheme. *IEEE Trans. Consum. Electron.* 50(2):629–631, 2004.
5. He, D., Chen, J., and Zhang, R., A more secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36 (3):1989–1995, 2011.
6. Hwang, M. S., and Li, L. H., A new remote user authentication scheme using smart cards. *IEEE Trans. Consum. Electron* 46 (1):28–30, 2000.
7. Juang, W. S., and Wu, J. L., Two efficient two-factor authenticated key exchange protocols in public wireless lans. *Comput. Electr. Eng.* 1(35):33–40, 2009.
8. Khan, M. K., Kim, S. K., and Alghathbar, K., Cryptanalysis and security enhancement of a more efficient and secure dynamic ID-based remote user authentication scheme. *Comput. Commun.* 34 (3):305–309, 2011.
9. Ku, W. C., and Chang, S. T., Impersonation attacks on a dynamic ID-based remote user authentication scheme using smart cards. *IEICE Trans. Commun.* E88-B(5):2165–2167, 2005.
10. Lamport, L., Password authentication with insecure communication. *Commun. ACM* 24(11):770–772, 1981.
11. Liao, I., Lee, C. C. and Hwang, M. S., "Security enhancement for a dynamic ID-based remote user authentication scheme, *Proceedings of 2005 International Conference on Next Generation Web Services Practices*, Seoul, Korea, 2005, pp. 437–440.
12. Lin, C. L., Sun, H. M., and Hwang, T., Attacks and solutions on strong-password authentication. *IEICE Trans. Commun.* E84-B (9):2622–2627, 2001.
13. Misbahuddin, M., and Bindu, C. S., Cryptanalysis of Liao-Lee-Hwang's dynamic ID scheme. *Int. J. Netw. Secur.* 2(6):211–213, 2008.
14. Rivest, R., Shamir, A., and Adleman, L., A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM* 21(2):120–126, 1978.
15. Shimizu, A., A dynamic password authentication method by one way function. *Syst. Comput. Jpn.* 22(7):32–40, 1991.
16. Shimizu, A., Horioka, T., and Inagaki, H., A password authentication method for contents communication on the Internet. *IEICE Trans. Commun.* E81-B(8):1666–1673, 1998.
17. Su, R., and Cao, Z. F., An efficient anonymous authentication mechanism for delay tolerant networks. *Comput. Electr. Eng.* 3 (36):435–441, 2010.
18. Tang, H. B. and Liu, X. S., "Cryptanalysis of a dynamic ID-based remote user authentication with key agreement scheme," *Int. J. Commun. Syst.*, to appear, 2012.
19. Tsai, J. L., Wu, T. C., and Tsai, K. Y., New dynamic ID authentication scheme using smart cards. *Int. J. Commun. Syst.* 23(12):1449–1462, 2010.
20. Wang, R. C., Juang, W. S., and Lei, C. L., Robust authentication and key agreement scheme preserving the privacy of secret key. *Comput. Commun.* 34(3):274–280, 2011.
21. Wang, Y. Y., Liu, J. Y., Xiao, F. X., and Dan, J., A more efficient and secure dynamic ID-based remote user authentication scheme. *Comput. Commun.* 32(4):583–585, 2009.
22. Wei, J., Hu, X., and Liu, W., An improved authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36 (6):3597–3604, 2012.
23. Wen, F., and Li, X., An improved dynamic ID-based remote user authentication with key agreement scheme. *Comput. Electr. Eng.* 38(2):381–387, 2011.
24. Wu, Z. Y., Lee, Y. C., Lai, F., Lee, H. C., and Chung, Y., A secure authentication scheme for telecare medicine information systems. *J. Med. Syst.* 36(3):1529–1535, 2012.
25. Wu, S., Zhu, T., and Pu, Q., Robust smart-cards-based user authentication scheme with user anonymity. *Secur. Commun. Netw.* 5 (2):236–248, 2011.
26. Yoon, E. J., and Yoo, K. Y., *"Improving the dynamic ID-based remote mutual authentication scheme", Proceedings of 2006 OTM Workshops, Lecture Notes in Computer Science*, vol. 4277. Springer, Berlin, pp. 499–507, 2006.
27. Yoon, E. J., Yoo, K. Y., and Ha, K. S., A user friendly authentication scheme with anonymity for wireless communications. *Comput. Electr. Eng.* 3(37):356–364, 2011.
28. Zhu, Z., An efficient authentication scheme for telcare medical information system. *J. Med. Syst.* 36(6):3833–3838, 2012.