Cyber Security and Applications 1 (2023) 100008

Contents lists available at ScienceDirect

Cyber Security and Applications

journal homepage: http://www.keaipublishing.com/en/journals/cyber-security-and-applications/

Cryptanalysis on "a secure three-factor user authentication and key agreement protocol for TMIS with user anonymity "

Anjali Singh, Marimuthu Karuppiah*, Rajendra Prasad Mahapatra

Department of Computer Science and Engineering, SRM Institute of Science and Technology, NCR Campus, Ghaziabad, Uttar Pradesh 201204, India

ARTICLE INFO

Keywords:
Authentication
Smart cards
Telecare medicine information system
User anonymity

ABSTRACT

The health-care delivery services were made possible by telecare medicine information systems (TMIS). These systems are paving the way for a world where computerised telecare facilities and automated patient medical records are the norm. Authentication schemes are common mechanisms for preventing unauthorised access to medical records via insecure networks. Amin and Biswas recently proposed an authentication scheme for TMIS, asserting that their scheme can withstand various attacks. Despite this, their scheme still has significant security weaknesses. In this paper, we present a cryptanalysis of Amin and Biswas' scheme and show that it is subject to a variety of attacks.

1. Introduction

The increased proliferation of distributed networks has resulted in more resource and service exchange among user devices. As a result, during this cyber-connected period, there has been an increase in transaction volume.

Due to the open nature of network that is dispersed, for application systems, system security and robust privacy protection techniques have become an inevitable requirement. As a result, authentication of the user may be a critical security element that must be included in such systems in order to distinguish legitimate users from potential threats.

One of the applications of distributed networks is the Telecare medical information system (TMIS). TMIS creates an effective and practical connection through an insecure internet between the patient and the doctor. Therefore, in order to access critical medical data over unsecure communication, data security, privacy, and user authentication are of utmost importance. There have been numerous user authentication mechanisms for TMIS proposed recently [1–22], but it has been shown that the majority of these protocols fall short of meeting all security requirements.

Recently, Mishra et al. [23] suggested a user authentication technique with anonymity for the users. Unfortunately, according to Amin and Biswas [24], user anonymity is not guaranteed by the technique and mutual authentication in Mishra et al's strategy. Furthermore, Amin and Biswas concluded that Mishra et al's is susceptible to a variety of attacks. Then, to address the shortcomings in Mishra et al's scheme, Amin and Biswas provided an updated authentication scheme. First, we show that Amin and Biswas's strategy [24] is not able to satisfy the user anonymity property and doesn't give complete forward secrecy and mutual authentication. It's also susceptible to forging and password guessing attacks when used offline.

The remainder of the paper is divided into the following sections. The scheme devised by Amin and Biswas is examined in Section 2. Section 3 discusses the problems in Amin and Biswas' strategy. In Section 4, you'll find the conclusions.

2. Review of the scheme [24]

Registration, login, authentication, and password update are the four sections of the authentication process. The explanations are as follows:

2.1. Notations

The notations used in this paper are defined in the table.

Notation	Description
U_j	User
r	Random variable
A	Adversary
ID_j	Identity of the user
PWD_j	Password of the user
T_j	fingerprint
H()	Bio-hash function
$h(\cdot)$	One-way hash function
SC	Smart card
SK	Session key
||	Concatenation operation
$\cdot$	ECC based scalar point multiplication
$\oplus$	Bit-wise exclusive OR operation

* Corresponding author.
E-mail address: marimuthume@gmail.com (M. Karuppiah).

https://doi.org/10.1016/j.csa.2022.100008
Received 3 May 2022; Received in revised form 4 July 2022; Accepted 10 September 2022
Available online 23 September 2022

2.2. User registration phase

The medical server accepts registrations from anyone during this phase to gain access to medical services.

1. User selects ID_j, password PWD_j, and biometric template such as fingerprint T_j. Then, U_j submits ID_j, A_j, and F_j through secure link or in person to the medical server after computing $A_j = h(ID_j||PWD_j)$ and $F_j = H(T_j)$.
2. Then, Medical server S computes $A_j = h(ID_j||PWD_j)$, $K = h(ID_s||z||ID_j)$, $B_j = h(ID_j||A_j) \oplus K$, $CID_j = E_z(ID_j||r)$ and issues a SC for the U_j after storing F_j, A_j, B_j, CID_j, $h(\cdot)$, $H(\cdot)$ into the memory of the SC using protected channel. We assume that a user selects low entropy ID_j, PWD_j that are individually guessable in time that is polynomial.

2.3. Login phase

The U_j can use a medical server with a card reader or terminal device to access the medical server at any time and from any location after successfully completing the registration procedure. The following is a list of all the steps in this phase:

1. The U_j first embeds his or her SC into the card reader device, then embeds the biometric template T_j into the sensor device. $F_j^* = H(T_j)$ is computed by the card reader and compared to the stored F_j. Biometric verification is successful if it matches, and the U_j is asked to input ID_j, PWD_j; otherwise, the connection is terminated.
2. $A_j^* = h(ID_j||PWD_j)$ is computed by the card reader and compared to the stored A_j. The matching result determines whether or not the U_j provided valid ID_j, PWD_j. Proceed to the next stage if it matches; Else, the connection will be canceled.
3. The terminal generates a nonce at random r_j and calculates $D_1 = r_j \cdot N$, $K = B_j \oplus h(ID_j||A_j^*)$, $D_2 = r_j \oplus K$, $D_4 = h(ID_j||r_j||K)$ and sends D_2, D_4 and CID_j over the public/open channel as a login message to the medical server.

2.4. Authentication and key agreement phase

The U_j and the medical server must establish mutual authentication and a shared session key agreement at this phase. All of the steps in this phase are listed below:

1. The medical server decrypts CID_j using the server's secret key z and gets $(ID_j^*||r) = DE_z(CID_j)$, $K = h(ID_s||z||ID_j^*)$, $r_j^* = D_2 \oplus K$, $D_1^* = r_j^* \cdot N$, $D_4^* = h(ID_j||r_j^*||K)$ and matches D_4^* with the received D_4. The medical server trusts it if it matches the U_j's legitimacy.
2. The medical server generates a nonce at random r_k and calculates $D_1 = r_k \cdot N$, $SK = r_k \cdot D_1^* = r_k \cdot r_j^* \cdot N$, $J_1 = H_1 + D_1^*$, $L_j = h(ID_j^*||h(H_1)||K)$, $CID_j^{'} = E_z(ID_j^*||r^{'})$ and transmits a reply message L_j, J_1 and $CID_j^{'}$ to the U_j through the public channel, where $r^{'}$ is the medical server generates a random number.
3. The U_j computes $H_1^* = J_1 - D_1^*$, $L_j^* = h(ID_j||h(H_1^*)||K)$, $SK = r_j \cdot H_1^* = r_j \cdot r_k \cdot N$, and matches L_j^* with the received L_j depending on the reply message received. If they match, the U_j trusts the medical server's legitimacy, then the protocol performs mutual authentication by sharing SK. After mutual authentication, the U_j replaces the previous CID_j in the SC's memory with the new $CID_j^{'}$. Finally, the U_j computes $Z_j = h(ID_r||SK)$ and sends it via the public channel to the medical server.
4. Following receipt, the server calculates $Z_j^* = h(ID_j^*||SK)$ and compares it to the received Z_j. If they're compatible, both sides begin secure communication.

2.5. Password change phase

It's a useful attribute for adding a password change phase to any password-based user authentication mechanism, allowing users to change their passwords without the need for a medical server.

1. The U_j first puts the SC into the card reader and performs steps 1 and 2 of the login phase to verify the $U_j^{'}$s authenticity. After that, the card reader performs the procedures below to successfully change the password.
2. After user authentication, the card reader prompts the user to enter a new password, PWD_j^{new}, into the U_j, and after doing so, the card reader computes the values $A_j^{new} = h(ID_j||PWD_j^{new})$ and $B_j^{new} = h(ID_j||A_j^{new}) \oplus K$, where K is the old parameter, and then the card reader replaces A_j, B_j with the new values A_j^{new}, B_j^{new} and the password change phase is successfully completed.

3. Cryptanalysis of Amin and Biswa's scheme

This section describes the security limitations of the scheme in Amin and Biswas [24].

3.1. Adversary model

Adversary modeling is a crucial component of creating an authenticated protocol. A strategy for strengthening security by categorizing vulnerabilities and goals, and hence establishing protective measures against threats to the system, is known as adversary modeling. In this context, a threat could be a harmful attack carried out by an enemy, such as an adversary who could harm the resources. The adversary model is based on the assumptions below. These assumptions regarding an adversary's prowess are legitimate, and they've been made in contemporary works as well:

1. The message that was communicated across the insecure communication channels has little influence on the adversary. Intercepting, altering, and deleting any conveyed message are all examples of this [25–27]
2. Using a power analysis technique, the adversary can retrieve the security parameters encoded in the smart card [28–31].
3. The password dictionary can be enumerated offline by adversary [32,33].

3.2. Fails to offer user anonymity

Assume Adversary acquires the value A_j, B_j under assumption 2 from the stolen smart card, and the adversary intercepts the U_j's login request message $(D_2, CID_j, D_4, T_j, T_u)$. Now, Adversary has values $(A_j, B_j, D_2, CID_j, D_4, T_j, T_u)$. Adversary can find the user U_j's ID_j by doing the following:

1. Adversary assumes the identify of the user as ID_a.
2. Compute $K_a = B_j \oplus h(ID_a||A_j) = h(ID_j||A_j) \oplus h(ID_s||z||ID_j) \oplus h(ID_a||A_j)$.
3. Compute $r_j^* = D_2 \oplus K_a = r_j \oplus K \oplus K_a$.
4. Compute $D_4^* = h(ID_a||r_j^*||K_a)$.
5. Compare $D_4^* \stackrel{?}{=} D_4$. If this is the case, the adversary's guessed identity is right.
6. If false, the adversary must repeat steps (1–4) until the current identity is obtained.

Hence, the attacker can learn the user's identify. The foregoing steps have a time complexity of $O(\mid D_{ID} \mid \times(4T_{xor} + 6T_h))$, where $\mid D_{ID} \mid$ denotes the identity space size, T_{xor} denotes the XOR operation execution time, and T_h denotes the hash operation execution time. As a result, Amin and Biswas's scheme fails to offer user anonymity.

3.3. Prone to offline passsword guessing attack

Assume Adversary obtain the values $\{A_j, B_j, J_i, h(\cdot)\}$ under assumption 2, the login request message is intercepted by Adversary from the stolen/lost SC of $(ID_j, D_2, CID_j, D_4, T_j, T_u)$ under assumption 1. As previously stated, Adversary can uncover a user's original identification ID_j. Adversary can perform an offline password guessing attack using these values as follows:

1. Adversary assumes password of the user U_j as PWD_a.
2. Compute $z_j^* = J_i \oplus h(A_j \oplus PWD_j) = z_j \oplus h(A_j \oplus PWD_j) \oplus h(A_j \oplus PWD_j) = z_j$.
3. Compute $A_j^* = h(ID_j||PWD_a)$.
4. Compare $A_j \stackrel{?}{=} A_j^*$. If this is the case, adversary's guessed PWD_a is correct.
5. If false, the adversary must repeat steps (1–4) till you get your hands on the current password.

Hence, the attacker can learn the user's password.

The foregoing steps take $O(\mid D_{PWD} \mid \times(6T_{xor} + 4T_h))$, where $\mid D_{PWD} \mid$ denotes the identity space size, T_{xor} presents the XOR operation execution time, and T_h presents the hash operation execution time. In reality, the password space is usually somewhat limited, such as $\mid D_{PWD} \mid <= 10^6$. As a result, Amin and Biswas's strategy is susceptible to an offline password guessing attack.

3.4. Fails to offer perfect forward secrecy

Assume that under assumption 2, Adversary intercepted and documented the messages that had previously been conveyed $(ID_j, D_2, CID_j, D_4, T_j, T_u)$ and (T_s, M_j) and obtained the value $(A_j, B_j, J_i, h(\cdot))$ from the SC. If the attacker has the user password PWD_j as previously discussed, the previously traded session key can be calculated as follows:

1. Adversary computes $A_j = h(ID_j||PWD_j)$ and $z_j = J_i \oplus h(A_j||PWD_j)$.
2. Then Adversary computes the $SK = h(ID_j \oplus A_j \oplus z_j \oplus T_u \oplus T_s)$.

As a result, since revealing the user's password affects the secrecy of previous session keys, Amin and Biswa's scheme doesn't provide perfect forward secrecy.

3.5. Prone to forgery attack

Under assumption 2, Adversary acquires the values $\{ A_j, B_j, J_i, h(\cdot) \}$ from the smart card. As previously stated, Adversary can obtain U_j's identification ID_j and password PWD_j. Using this information, the adversary can complete the login phase steps and submit the login request message $\{ID_j, D_2, CID_j, D_4, T_j, T_a\}$ to the server, where T_a represents the Adversary's current time stamp. Server can check the newness of the timestamp T_a when it receives the message $\{ID_j, D_2, CID_j, D_4, T_j, T_a\}$ from attacker. Because Adversary utilises the correct timestamp, the verification is valid. The server then performs the processes of the authentication phase to verify that the adversary is a valid user. It's obvious that the server won't notice anything or any deformity because the login request $\{ID_j, D_2, CID_j, D_4, T_j, T_a\}$ is genuinely made by adversary using the valid U_j's identity Id_j and password PWD_j. The message (T_s, M_j) is then sent to user U_j by Server S. As a result, S will accept Adversary's login request from U_j. Adversary intercepts the (T_s, M_j) communication and finds $SK = h(ID_j \oplus A_j \oplus z_j \oplus T_u \oplus T_s)$. Finally, both the Server and the Adversary will have the same SK. As a result, since the adversary can impersonate a valid user by successfully signing in using the credentials of server S, Amin and Biswa's scheme is vulnerable to forgery attack.

3.6. Fails to offer mutual authentication

Mutual authentication is accomplished using an effective password authentication approach, which means that the server not only verifies the authenticity of the user, but the user can also verify the server's legitimacy. Furthermore, no unauthorised users or cloud servers have the ability to impersonate a legitimate user or server. An attacker can mimic a valid user, as previously stated. As a result, the mutual authentication setup is broken. As a result, mutual authentication is not achievable.

4. Conclusion

We investigated Amin and Biswas's authentication technique and found that it is not able to deliver user anonymity, mutual authentication and perfect forward secrecy. Offline password guessing and forging attacks are also possible. As a result, Amin and Biswas's technique for wireless network communication is unsafe. Future efforts will be focused on bolstering Amin and Biswas's scheme, which will be capable of meeting all security criteria and objectives.

Funding statement

This research received no specific grant from any funding agency in the public, commercial, or not for profit sectors.

Data availability statement

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

Declaration of Competing Interest

Authors declare that they have no conflict of interest.

References

[1] S. Qiu, G. Xu, H. Ahmad, L. Wang, A robust mutual authentication scheme based on elliptic curve cryptography for telecare medical information systems, IEEE Access 6 (2017) 7452–7463.
[2] C.-M. Chen, B. Xiang, E.W. Ke, T.-Y. Wu, J.C.-W. Lin, Improvement of an anonymous and lightweight authentication scheme for TMIS, J. Appl. Math. Phys. 6 (1) (2018) 18–28.
[3] N. Radhakrishnan, M. Karuppiah, An efficient and secure remote user mutual authentication scheme using smart cards for telecare medical information systems, Inform. Med. Unlocked 16 (2019) 100092.
[4] P. Chandrakar, A.S. Chauhan, R. Ali, Cryptanalysis and improvement of a secure mutual authentication scheme for remote users, in: 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), IEEE, 2019, pp. 1–9.
[5] T.-T. Truong, M.-T. Tran, A.-D. Duong, Improved chebyshev polynomials-based authentication scheme in client-server environment, Secur. Commun. Netw. 2019 (2019) 11 4250743.
[6] Y. Park, K. Park, Y. Park, Secure user authentication scheme with novel server mutual verification for multiserver environments, Int. J. Commun. Syst. 32 (7) (2019) e3929.
[7] M. Hasson, A.A. Yassin, A.J. Yassin, A.M. Rashid, A.A. Yaseen, H. Alasadi, Password authentication scheme based on smart card and QR code, Indones. J. Electr. Eng. Comput. Sci. 23 (1) (2021) 140–149.
[8] L. Chen, K. Zhang, Privacy-aware smart card based biometric authentication scheme for e-health, Peer-to-Peer Netw. Appl. 14 (3) (2021) 1353–1365.
[9] M. Adeli, N. Bagheri, H.R. Meimani, On the designing a secure biometric-based remote patient authentication scheme for mobile healthcare environments, J. Ambient Intell. Humaniz. Comput. 12 (2) (2021) 3075–3089.
[10] Y. Zhou, Y. Luo, M.S. Obaidat, P. Vijayakumar, X. Wang, PAMI-anonymous password authentication protocol for medical internet of things, in: 2021 IEEE Global Communications Conference (GLOBECOM), IEEE, 2021, pp. 1–6.
[11] M.A. Khan, A. Ghani, M.S. Obaidat, P. Vijayakumar, K. Mansoor, S.A. Chaudhry, A robust anonymous authentication scheme using biometrics for digital rights management system, in: 2021 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), IEEE, 2021, pp. 1–5.
[12] S. Jegadeesan, M.S. Obaidat, P. Vijayakumar, M. Azees, M. Karuppiah, Efficient privacy-preserving anonymous authentication scheme for human predictive online education system, Cluster Comput. 25 (4) (2021) 2557–2571.
[13] M. Karuppiah, R. Saravanan, Cryptanalysis and an improvement of new remote mutual authentication scheme using smart cards, J. Discrete Math. Sci. Cryptogr. 18 (5) (2015) 623–649.
[14] P. Vijayakumar, M. Azees, S.A. Kozlov, J.J. Rodrigues, An anonymous batch authentication and key exchange protocols for 6G enabled VANETs, IEEE Trans. Intell. Transp. Syst. 23 (2) (2021) 1630–1638.
[15] X. Xia, S. Ji, P. Vijayakumar, J. Shen, J.J. Rodrigues, An efficient anonymous authentication and key agreement scheme with privacy-preserving for smart cities, Int. J. Distrib. Sens. Netw. 17 (6) (2021) 1–13. 15501477211026804

[16] L. Xiao, S. Xie, D. Han, W. Liang, J. Guo, W.-K. Chou, A lightweight authentication scheme for telecare medical information system, Connect. Sci. 33 (3) (2021) 769–785.
[17] K. Chatterjee, A secure three factor-based authentication scheme for telecare medicine information systems with privacy preservation, Int. J. Inf. Secur. Privacy (IJISP) 16 (1) (2022) 1–24.
[18] V.P. Gaikwad, J.V. Tembhurne, C. Meshram, C.-C. Lee, Provably secure lightweight client authentication scheme with anonymity for TMIS using chaotic hash function, J. Supercomput. 77 (8) (2021) 8281–8304.
[19] Y. Chen, J. Chen, An efficient and privacy-preserving mutual authentication with key agreement scheme for telecare medicine information system, Peer-to-Peer Netw. Appl. 15 (1) (2022) 516–528.
[20] H. Amintoosi, M. Nikooghadam, M. Shojafar, S. Kumari, M. Alazab, Slight: a lightweight authentication scheme for smart healthcare services, Comput. Electr. Eng. 99 (2022) 107803.
[21] M. Tanveer, A. Alkhayyat, S.A. Chaudhry, Y.B. Zikria, S.W. Kim, et al., REAS-TMIS: resource-efficient authentication scheme for telecare medical information system, IEEE Access 10 (2022) 23008–23021.
[22] M. Soni, D.K. Singh, Privacy-preserving authentication and key-management protocol for health information systems, in: Data Protection and Privacy in Healthcare, CRC Press, 2021, pp. 37–50.
[23] D. Mishra, S. Mukhopadhyay, A. Chaturvedi, S. Kumari, M.K. Khan, et al., Cryptanalysis and improvement of Yan et al.'s biometric-based authentication scheme for telecare medicine information systems, J. Med. Syst. 38 (6) (2014) 1–12.
[24] R. Amin, G.P. Biswas, A secure three-factor user authentication and key agreement protocol for TMIS with user anonymity, J. Med. Syst. 39 (8) (2015) 1–19.
[25] D. Dolev, A. Yao, On the security of public key protocols, IEEE Trans. Inf. Theory 29 (2) (1983) 198–208.
[26] M. Karuppiah, R. Saravanan, A secure remote user mutual authentication scheme using smart cards, J. Inf. Secur. Appl. 19 (4–5) (2014) 282–294.
[27] A. Pradhan, M. Karuppiah, R. Niranchana, M.A. Jerlin, S. Rajkumar, Design and analysis of smart card-based authentication scheme for secure transactions, Int. J. Internet Technol. Secur. Trans. 8 (4) (2018) 494–515.
[28] P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in: Annual International Cryptology Conference, Springer, 1999, pp. 388–397.
[29] T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE Trans. Comput. 51 (5) (2002) 541–552.
[30] M. Karuppiah, A.K. Das, X. Li, S. Kumari, F. Wu, S.A. Chaudhry, R. Niranchana, Secure remote user mutual authentication scheme with key agreement for cloud environment, Mob. Netw. Appl. 24 (3) (2019) 1046–1062.
[31] A. Maria, V. Pandi, J.D. Lazarus, M. Karuppiah, M.S. Christo, BBAAS: blockchain-based anonymous authentication scheme for providing secure communication in VANETs, Secur. Commun. Netw. 2021 (2021) 1–11 6679882.
[32] C.-G. Ma, D. Wang, S.-D. Zhao, Security flaws in two improved remote user authentication schemes using smart cards, Int. J. Commun. Syst. 27 (10) (2014) 2215–2227.
[33] M. Azees, P. Vijayakumar, M. Karuppiah, A. Nayyar, An efficient anonymous authentication and confidentiality preservation schemes for secure communications in wireless body area networks, Wirel. Netw. 27 (3) (2021) 2119–2130.