JKSCI

한국컴퓨터정보학회논문지
Journal of The Korea Society of Computer and Information
Vol. 25 No. 2, pp. 93-103, February 2020
https://doi.org/10.9708/jksci.2020.25.02.093

Cryptanalysis and Improvement of RSA-based Authentication Scheme for Telecare Medical Information Systems

Keewon Kim*

*Professor, Dept. of Applied Computer Engineering, Dankook University, Yongin, Korea

[Abstract]

The telecare medical information system (TMIS) supports convenient and rapid health-care services. A secure and efficient authentication and key agreement scheme for TMIS provides safeguarding electronic patient records (EPRs) and helps health care workers and medical personnel to rapidly making correct clinical decisions. Giri et al. proposed an RSA-based remote user authentication scheme using smart cards for TMIS and claimed that their scheme could resist various malicious attacks. In this paper, we point out that their scheme is still vulnerable to lost smart card attacks and replay attacks and propose an improved scheme to prevent the shortcomings. As compared with the previous authentication schemes for TMIS, the proposed scheme is more secure and practical.

▸ **Key words**: Telecare Medical Information System, Password Based Authentication, Smart Card, Security, Biometric

[요 약]

원격 의료 정보 시스템(TMIS; Telecare Medical Information System)은 편리하고 빠른 헬스 케어(health-care) 서비스를 제공한다. 원격 의료 정보 시스템을 위한 안전하고 효율적인 인증 및 키 합의 기법은 전자 환자 기록(EPR; Electronic Patient Record)을 안전하게 보호하고, 헬스케어 종사자와 의료진이 신속하고 정확하게 임상 의사결정(clinical decision)을 할 수 있도록 도와준다. Giri 등은 원격 의료 정보 시스템을 위한 스마트 카드(smart card)를 이용한 RSA기반 원격 사용자 인증 기법을 제안하였으며, 제안한 기법이 다양한 악의적인 공격에 강인하다고 주장하였다. 본 논문에서는 그들의 기법이 여전히 스마트 카드 분실 공격(lost smart card attack)과 재전송 공격(replay attack)에 취약함을 보이고, 그러한 단점을 개선한 기법을 제안한다. 기존의 원격 의료 정보 시스템을 위한 인증 기법들과 안전성을 비교한 결과를 보면, 제안한 기법이 더욱 안전하고 실용적이다.

▸ **주제어**: 원격 의료 정보 시스템, 패스워드 기반 인증, 스마트 카드, 보안, 생체정보

• First Author: Keewon Kim, Corresponding Author: Keewon Kim
*Keewon Kim (nirkim@dankook.ac.kr), Dept. of Applied Computer Engineering, Dankook University
• Received: 2019. 11. 07, Revised: 2019. 01. 22, Accepted: 2020. 01. 27.

http://www.ksci.re.kr pISSN:1598-849X | eISSN:2383-9945

I. Introduction

The telecare medical information system (TMIS) enables or supports health-care delivery services. The recent availability of low-cost telecommunication systems and custom-made physiological monitoring devices have made it possible to bring the advantages of telemedicine directly into the patients' home, i.e. a connection between patients at home and doctors at a clinical center or a home health-care (HHC) agency [1].

The authentication and key agreement are essential to ensure data integrity, confidentiality, and availability for TMIS. The password authentication scheme using smart cards is one of the commonly used mechanisms. In 1981, the first remote password-based authentication scheme is proposed by Lamport [2]. However, Lamport's scheme needs to maintain a password list and suffers from interpolation attacks so many enhanced schemes using smart cards have been proposed to remedy drawbacks of Lamport's scheme [3-4]. Also, many researchers have proposed password-based user authentication schemes using smart cards for TMIS.

In 2012, Wu et al. [5] proposed a discrete logarithm problem (DLP) based authentication scheme with a pre-computation approach for TMIS. Later, He et al. [6] pointed out that Wu et al.'s scheme was insecure against impersonation attacks and insider attacks, and then proposed an improved scheme to enhance the security. They also introduced an improved scheme and claimed that their proposed scheme eliminates the flaws of Wu et al.'s scheme. Their scheme is also more appropriate for low power mobile devices in TMIS. However, Wei et al. [7] demonstrated that both Wu et al.'s and He et al.'s schemes are vulnerable to off-line password guessing attacks once the patient's smart card was compromised and inefficient to meet the two-factor authentication. They also presented an improved authentication scheme for TMIS and claimed that the improved scheme is efficient and achieved two-factor authentication. Later, Zhu [8] found that Wei et al.'s scheme cannot withstand off-line password guessing attacks. Zhu also designed a new authentication scheme using the RSA algorithm [9]. Zhu et al. demonstrated that their scheme was secure against various attacks. However, Khan and Kumari [10] found that Zhu's scheme cannot achieve some important characteristics necessary for secure user authentication. Recently, Giri et al. [11] demonstrated that Khan and Kumari's scheme was still insecure against off-line password guessing attack and presented that Khan and Kumari's scheme did not provide any security if the password of a patient was compromised. To enhance the security, Giri et al. proposed an RSA-based remote user authentication scheme for TMIS.

In this paper, we demonstrate that Giri et al.'s scheme is not secure for applications in TMIS, i.e. their scheme is vulnerable to the replay attack and the lost smart card attack. Then we propose an improved authentication scheme to solve these problems. The security analysis and performance analysis show the proposed scheme is more suitable for applications in TMIS.

II. Review and Security Weaknesses of Giri et al.'s scheme

This section presents the brief description of Giri et al.'s authentication scheme [11].

1. Giri et al.'s authentication scheme

The notations used throughout this paper are summarized in Table 1. Giri et al.'s scheme consists of following four phases: initial phase, registration phase, authentication and session key agreement phase, and password change phase.

1.1 Initial phase

The telecare server S selects two large primes p, q and computes $n = p \times q$. The server S keeps p, q

as secret parameters and publishes n as public parameter. Then, the server S chooses a prime e $(1 < e < (p-1)(q-1))$ and computes d such that $e \times d \equiv 1 \bmod (p-1)(q-1)$. The server S also chooses a one-way hash function $h(\cdot): \{0,1\}^* \rightarrow Z_q^*$. The server S publishes e as public and keeps d as secret.

1.2 Registration phase

A patient U_i can register to the telecare server S by computing following steps:

1. The patient U_i chooses an identity ID_i, a password pw_i and a random number b_i. Then, U_i computes $pwb_i = h(pw_i \| b_i)$ and sends the registration message $\{ID_i, pwb_i\}$ to the telecare server S through a secure channel.
2. After receiving the registration message $\{ID_i, pwb_i\}$, S computes $R_i = h(ID_i \| d)$, $A_i = R_i \oplus pwb_i$, $B_i = (pwb_i \| R_i)^e \bmod n$ and $L_i = h(R_i \| pwb_i)$. Then, S stores $\{ID_i, A_i, B_i, L_i, h(\cdot)\}$ into the memory of the smart card and issues it for the patient U_i.
3. After receiving the smart card, U_i stores b_i into the memory of his/her smart card.

1.3 Login phase

In this phase, U_i inserts his/her smart card to the terminal or the smart card reader and provides his/her password pw_i. Then, the smart card performs the following operations:

1. The smart card computes $pwb'_i = h(pw_i \| b_i)$, $R'_i = A_i \oplus pwb'_i$ and $L'_i = h(R'_i \| pwb'_i)$. Then, the smart card checks whether computed L'_i is equal with the stored L_i or not. If it does not hold, the smart card rejects the session otherwise proceeds to the next step.
2. The smart card generates a random number N_1, computes $C_i = h(pwb_i \| N_1 \| R'_i)$ and $D_i = pwb_i \oplus N_1$, and sends the login message $\{ID_i, B_i, C_i, D_i RIGHT$ to the telecare server S.

Table 1. Notations

Notations	Meanings
U_i	A user
S	A remote telecare server
ID_i	The identity of U_i
pw_i	The password of U_i
F_i	The biometrics of U_i
SK	A shared session key between U_i and S
$h()$	The secure one-way hash function
$Z^{*}{}_{q}$	The multiplicative group of the ring Z_q of integers modulo q
e	The public key of S
d	The private key of S
g	The generator of Z_q
$\|$	The concatenation operator
$\oplus$	The bitwise XOR operator
N_1, N_2	Random numbers
T_1, T_2, T_3, T_4	Timestamps
ΔT	The expected valid time interval for the transmission delay

1.4 Authentication and session key agreement phase

After receiving the login message $\{ID_i, B_i, C_i, D_i RIGHT$ from the smart card, the server S will check whether the login message is valid or not. If valid then it is implied that the U_i is a valid patient. The procedure of authentication and session key agreement phase is as follows:

1. The server S first checks the validity of the patient's identity ID_i. If it is valid, the server S computes $R_i = h(ID_i \| d)$ and $(pwb_i^* \| R_i^*) = (B_i)^d \bmod n$. Then, the server S checks R_i and R_i^* are equal or not. If they are equal, go to the next step; otherwise reject the login message.
2. The server S derives $N_1^* = pwb_i^* \oplus D_i$ and computes $C_i^* = h(pwb_i^* \| N_i^* \| R_i)$. Then, the server S checks whether the computed C_i^* is equal to the received C_i. If it holds, S authenticate U_i and proceeds to the next step.
3. The server S generates a random number N_2 and computes $N_3 = N_1^* \oplus N_2$, $K_i = h(R_i \| N_2)$. Then, it sends the message $\{N_3, K_i\}$ to the patient U_i for the mutual authentication.
4. After receiving the message $\{N_3, K_i\}$, the smart card derives $N'_2 = N_3 \oplus N_1$ and computes

$K'_i = h(R'_i \| N'_2)$. Then, the smart card compares the computed K'_i with the received K_i. If they are equal, the medical healthcare server S is authenticated to the patient U_i and the mutual authentication holds good. Then, both the user U_i and the server S agree upon a common secret session key $SK_{U_i} = h(ID_i \| pwb'_i \| N_1 \| N'_2)$ or $SK_S = h(ID_i \| pwb_i^* \| N_1^* \| N_2)$ for the secure communication in the future at the same session. It is easily shown that SK_{U_i} and SK_S are same.

1.5 Password change phase

If the patient U_i wants to change his/her password, U_i inserts the smart card to the card reader and submits the password pw_i. The procedure of password change phase performs following steps:

1. The smart card computes $pwb'_i = h(pw_i \| b_i)$, $R'_i = A_i \oplus pwb'_i$, and $L'_i = h(R'_i \| pwb'_i)$. Then the smart card checks whether the computed L'_i is equal to the stored L_i. If they are not equal, the smart card rejects the patient U_i. Otherwise, the smart card asks U_i to enter a new password.
2. U_i submits a new password pw_i^{new} to the smart card. Then, the smart card computes $pwb_i^{new} = h(pw_i^{new} \| b_i)$, $A_i^{new} = R'_i \oplus pwb_i^{new}$, $B_i^{new} = (pwb_i^{new} \| R'_i)^e \bmod n$ and $L_i^{new} = h(R'_i \| pwb_i^{new})$.
3. The smart card stores new computed parameters A_i^{new}, B_i^{new}, L_i^{new} into the memory by replacing A_i, B_i, L_i, respectively.

2. Security weaknesses of Giri et al.'s scheme

In this subsection, we show that Giri et al.'s scheme [11] is vulnerable to lost smart card attacks and replay attacks, which is based on the following assumptions:

- An adversary is able to extract the information from the smart card [12-15].
- An adversary is able to eavesdrop all the messages, which are transmitted between the user and the server via public channel. Moreover, the adversary can modify, delete and resend all the messages, and can also replay any message to any other entity [16].
- An adversary may be a legitimate user or an outsider [16,17]

Due to above mentioned assumptions, an adversary can obtain the parameters from the smart card $\{ID_i, A_i, B_i, L_i, b_i, h(\cdot)\}$, and can intercept and record the messages $\{ID_i, B_i, C_i, D_i\}$ and $\{N_3, K_i\}$ transmitted via public channel. With the help of these assumptions, the adversary can perform the following attacks successfully.

2.1 Security against lost smart card attacks

In Giri et al.'s scheme, they claimed that their scheme can resist lost smart card attacks. However, we found it is not true due to the following analysis. We suppose that an adversary E has stolen U_i's smart card and extracted the stored values $\{ID_i, A_i, B_i, L_i, b_i, h(\cdot)\}$ through someway [12-15]. From the registration phase of Giri et al.'s scheme, we know $A_i = h(ID_i \| d) \oplus h(pw_i \| b_i)$ and $h(ID_i \| d) = A_i \oplus h(pw_i \| b_i)$. Therefore, $L_i = h(h(ID_i \| d) \| h(pw_i \| b_i)) = h(A_i \oplus h(pw_i \| b_i) \| h(pw_i \| b_i))$. Then E can successfully find out U_i's password pw_i by performing the following procedure.

1. The adversary E selects a password candidate pw_i^* from a dictionary.
2. E computes $L_i^* = h(A_i \oplus h(pw_i^* \| b_i) \| h(pw_i^* \| b_i))$ and compares it with L_i. If they are equal, E gets the correct the password pw_i of U_i. Otherwise, E selects another password candidate from the dictionary and tries it again until E finds the correct answer.

Let n be the number of passwords in the password dictionary of attacker. Then, the time complexity of this dictionary attack is

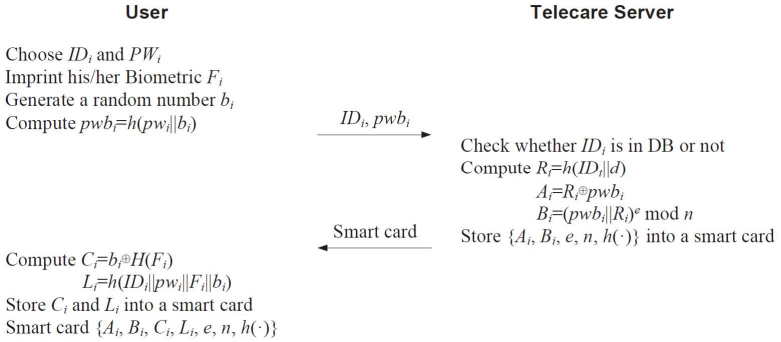

Fig. 1. Registration phase of the proposed scheme

$O(|n| \cdot (3T_H + T_R))$, where T_H and T_R are the running time of the hash function and the XOR operation, respectively. We can see that the time to find a user's password is a linear function of the number of candidate passwords in the dictionary.

2.2 Security against replay attacks

Suppose an adversary E has eavesdropped a past login message $\{ID_i, B_i, C_i, D_i\}$ of U_i. E is able to launch a replay attack and logins to the telecare server by resending the eavesdropped message $\{ID_i, B_i, C_i, D_i\}$ to the telecare server. In other words, E without running the "Login phase", sends the eavesdropped message $\{ID_i, B_i, C_i, D_i\}$ to the telecare server. In the "Authentication and session key agreement phase", upon receiving the message $\{ID_i, B_i, C_i, D_i\}$, the telecare server after the validity check of ID_i computes $R_i = h(ID_i||d)$ and $(pwb_i^*||R_i^*) = (B_i)^d \bmod n$, and checks whether R_i is equal to the decrypted R_i^* or not. Since R_i and R_i^* are equal, the telecare server derives $N_1^* = pwb_i^* \oplus D_i$, computes $C_i^* = h(pwb_i^*||N_i^*||R_i)$, and checks whether C_i^* is equal to the received C_i. Since C_i^* and C_i are equal, the telecare server will authenticate the adversary E as U_i, and E will be able to login to the telecare server. Thus, the adversary can easily login to the telecare server by resending an old login message. Since the telecare server does not check the freshness of the received login message $\{ID_i, B_i, C_i, D_i\}$, and authenticates the user in the "Authentication and key agreement phase", the telecare server will not be able to discover replay attacks.

III. The Proposed Scheme and Security Analysis

In this section, we propose an improved authentication scheme for TMIS which can resist lost smart card attacks and replay attacks. Our scheme consists of four phases.

1. The proposed scheme

1.1 Initial phase

The telecare server S selects two large primes p, q and computes $n = p \times q$. The server S keeps p, q as secret parameters and publishes n as public parameter. Then, the server S chooses a prime e $(1 < e < (p-1)(q-1))$ and computes d such that $e \times d \equiv 1 \bmod (p-1)(q-1)$. The server S also chooses a one-way hash function $h(\cdot): \{0,1\}^* \rightarrow Z_q^*$. The server S publishes e as public and keeps d as secret.

1.2 Registration phase

Before a user (e.g. patient, doctor, nurse, etc.) can use the telecare server's services, the user has to register with the telecare server. At the end of the registration phase, the user obtains a smart card that contains the required information for accessing the provided services. As illustrated in Fig. 1 the registration phase of the proposed scheme proceeds as follows.

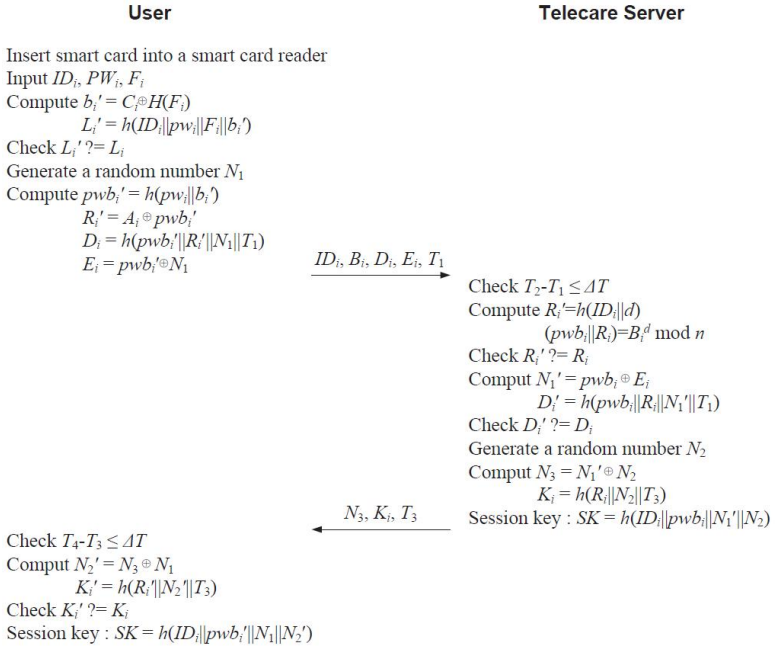

Fig. 2. Login and authentication phase of the proposed scheme

Step R1: The user U_i chooses an identity ID_i and a password pw_i, and imprints his/her biometrics F_i at a sensor. After that, U_i generates a random number b_i and computes $pwb_i = h(pw_i||b_i)$. Finally, U_i sends ID_i and pwb_i to the telecare server S through a secure channel.

Step R2: Upon receiving ID_i and pwb_i, the telecare server S checks whether ID_i is already in database or not. If ID_i does not exist, S computes $R_i = h(ID_i||d)$, $A_i = R_i \oplus pwb_i$, and $B_i = (pwb_i||R_i)^e \bmod n$. Then, S stores $\{A_i, B_i, e, n, h(\cdot)\}$ into a smart card. Finally, S sends the smart card to U_i through the secure channel.

Step R3: When U_i receives the smart card, U_i computes $C_i = b_i \oplus H(F_i)$ and $L_i = h(ID_i||pw_i||F_i||b_i)$, and stores them in the memory of it.

1.3 Login and authentication phase

The registered user can access the telecare server's information and services by successfully performing the login phase. In this phase, first the smart card checks the legitimacy of the user by verifying the inputted identity ID_i, password pw_i, and biometrics F_i. Then, the smart card computes a login request message and sends it to the telecare server. The user and the telecare server mutually authenticate each other and agree a shared session key that will be used to encrypt/decrypt and authenticate subsequent communications. After the mutual authentication, the user can login to the telecare server and obtain desired services. As illustrated in Fig. 2, this phase includes the following steps.

Step A1: The user U_i inserts his/her smart card into a smart card reader, enters his/her ID_i, and pw_i, and imprints his/her biometrics F_i at the sensor. Then, the smart card computes $b'_i = C_i \oplus H(F_i)$ and $L'_i = h(ID_i||pw_i||F_i||b'_i)$, and checks whether the computed L'_i is equal with the stored L_i or not. If it does not hold, it halts the process. Otherwise, it proceeds to the next step. The smart card generates a random number N_1, computes $pwb'_i = h(pw_i||b'_i)$, $R'_i = A_i \oplus pwb'_i, D_i = h(pwb'_i||R'_i||N_1||T_1)$, and $E_i = pwb'_i \oplus N_1$, and sends a login message $\{ID_i, B_i, D_i, E_i, T_1\}$ to the telecare server S, where T_1 is the current timestamp.

Step A2: Upon receiving the login request message $\{ID_i, B_i, D_i, E_i, T_1\}$ at the time T_2, the telecare

server checks the validity of the timestamp T_1 by checking the condition $T_2 - T_1 \leq \Delta T$, where ΔT is the expected valid time interval for the transmission delay. If it is invalid, the phase terminates immediately. Otherwise, the telecare server computes $R'_i = h(ID_i \| d)$ and $(pwb_i \| R_i) = (B_i)^d \bmod n$, and checks whether the computed R'_i is equal with the decrypted R_i or not. If they are not equal, the telecare server terminates the session. Otherwise, the telecare server computes $N'_1 = pwb_i \oplus E_i$ and $D'_i = h(pwb_i \| R_i \| N'_1 \| T_1)$, and checks whether the computed D'_i is equal with the received D_i or not. If they are not equal, the telecare server terminates the session. Otherwise, the telecare server authenticates the user, generates a random number N_2, and computes $N_3 = N'_1 \oplus N_2$ and $K_i = h(R_i \| N_2 \| T_3)$. Finally, the telecare server computes the session key $SK = h(ID_i \| pwb_i \| N'_1 \| N_2)$ and sends a message $\{N_3, K_i, T_3\}$ to the user, where T_3 is the current timestamp.

Step A3: Upon receiving the login request message $\{N_3, K_i, T_3\}$ at the time T_4, the telecare server checks the validity of the timestamp T_3 by checking the condition $T_4 - T_3 \leq \Delta T$. If it is invalid, the phase terminates immediately. Otherwise, the telecare server computes $N'_2 = N_3 \oplus N_1$ and $K'_i = h(R'_i \| N'_2 \| T_3)$, and checks whether the computed K'_i is equal with the received K_i or not. If they are not equal, the telecare server terminates the session. Otherwise, the user authenticates the telecare server and computes the shared session key SK as $SK = h(ID_i \| pwb'_i \| N_1 \| N'_2)$.

1.4 Password and biometrics update phase

When a user suspects that his/her password is used or misused by a third party, the user changes the password immediately. In this phase, the user can update his/her old password pw_i to a new password pw_i^{new} and his/her old biometrics F_i to a new biometrics F_i^{new}. This phase includes the following steps.

Step P1: The user inserts his/her smart card into a smart card reader, enters his/her ID_i and pw_i, and imprints his/her biometrics F_i at the sensor.

Step P2: The smart card computes $b'_i = C_i \oplus H(F_i)$ and $L'_i = h(ID_i \| pw_i \| b'_i)$, and checks whether the equation $L'_i = L_i$ holds or not. If the equation does not hold, the smart card halts the process. Otherwise, the smart card asks U_i to enter new password and imprint new personal biometrics.

Step P3: The user enters a new password pw_i^{new} and imprints a new personal biometrics F_i^{new}.

Step P4: The smart card computes

$$pwb_i = h(pw_i \| b'_i),$$
$$R_i = A_i \oplus pwb_i$$
$$A_i^{new} = R_i \oplus pwb_i^{new}$$
$$B_i^{new} = (pwb_i^{new} \| R_i)^e \bmod n$$
$$L_i^{new} = h(ID_i \| pw_i^{new} \| F_i^{new} \| b'_i)$$

Finally, the smart card replaces A_i, B_i, and L_i with A_i^{new}, B_i^{new}, and L_i^{new}, respectively.

2. Security analysis of the proposed scheme

In this subsection, the resistance of the proposed scheme against various security attacks such as privileged insider attacks, replay attacks, lost smart card attacks, password guessing attacks, impersonation attacks, and stolen verifier attacks is examined. Furthermore, the functionality of our proposed scheme provides some security requirements, such as known-key security and session-key security.

2.1 Privileged insider attacks

In real environments, a user U_i may use the same identity ID_i and password pw_i to register various remote servers for his/her convenience. If a privileged insider E can know U_i's password pw_i, E may try to use pw_i to impersonate U_i to

login other remote servers.

A malicious insider in the telecare server's system may try to achieve user's password. Note that during the registration phase of our scheme, the user U_i sends the registration request message $\{ID_i, pwb_i\}$ to S via a secure channel, where $pwb_i = h(pw_i||b_i)$ and b_i is a random number. Since b_i is unknown to the server S, to derive the password pw_i of the user U_i from pwb_i, the server S needs to guess correctly both pw_i and b_i. A malicious insider cannot know the user's password pw_i as hash function $h(\cdot)$ cannot be reverted. Moreover, the insider cannot perform password guessing attacks as user does not submit b_i to S. Therefore, the server S has no feasible way to derive pw_i of the user U_i. As a result, an insider cannot derive pw_i and b_i, and hence, our scheme is secure against privileged insider attacks.

2.2 Replay attacks

As discussed in subsection 2.2 of Section 2, Giri et al.'s scheme [11] is vulnerable to replay attacks because the telecare server does not check the freshness of the received login message $\{ID_i, C_i, B_i, D_i\}$. In order to withstand replay attacks, we use timestamps and two fresh random numbers N_1 and N_2 to ensure the freshness of the login and authentication messages.

Assume that an adversary E eavesdrops all the transmitted messages $\{ID_i, B_i, D_i, E_i, T_1\}$ and $\{N_3, K_i, T_3\}$ during the login and authentication phase. Suppose the adversary sends the eavesdropped login request message $\{ID_i, B_i, D_i, E_i, T_1\}$ to the telecare server. In Step A2 of the proposed scheme, the telecare server can detect a replay attack by checking the condition $T_2 - T_1 \leq \Delta T$, where T_2 and ΔT denote the telecare server's current time and the maximum transmission delay, respectively. In the login and authentication phase of the proposed scheme, if the adversary replaces the timestamp T_1 and D_i with a current timestamp T'_1 and $D'_i = h(pwb_i||R_i||N_1||T'_1)$, then the telecare server can detect this modification by checking D_i. Therefore, our proposed scheme is secure against replay attacks.

2.3 Lost smart card attacks

Suppose the user's smart card is lost, stolen or copied, and an adversary extracts all the stored information $\{A_i, B_i, C_i, L_i, e, n, h(\cdot)\}$ from the memory of the smart card through someway [12,13], where $A_i = R_i \oplus pwb_i = h(ID_i||d) \oplus h(pw_i||b_i)$, $B_i = (pwb_i||R_i)^e \bmod n = (h(pw_i||b_i)||h(ID_i||d))^e \bmod n$, $C_i = b_i \oplus H(F_i)$, and $L_i = h(ID_i||pw_i||F_i||b_i)$. Let an adversary E try to derive the password pw_i in off-line from A_i, B_i, and L_i, and guess the password pw_i^*. To verify the guessed password pw_i^* with A_i is equivalent to obtain $h(ID_i||d)$ and b_i. To guess the password pw_i from B_i, E faces to decrypt $(pwb_i||h(ID_i||d))^e \bmod n$. Also, E has to obtain b_i and F_i to verify the guessed password pw_i^* with L_i. However, it is computationally infeasible for E to obtain b_i, F_i, and d. Therefore, without knowing b_i, F_i, and d simultaneously, the adversary E cannot explore any useful information to threat the security of our scheme.

2.4 On-line password guessing attacks

On-line password guessing attacks occur when an adversary continuously guesses every possible password and tries to log into the server till he is successful. The attack is detectable in our proposed scheme. If an adversary E tries to guess a user's password, E would use the guessed password to compute a login message, and then send it to the server for doing the verification. However, the probability of guessing the correct password is very low. If the guess is wrong, the server can easily detect that there is an adversary attempting to login illegally. Therefore, on-line password guessing attacks cannot succeed.

2.5 Off-line password guessing attacks

Suppose that an adversary E obtains the values of $\{A_i, B_i, C_i, L_i, e, n, h(\cdot)\}$ stored in the smart card and the transmitted message $\{ID_i, B_i, D_i, E_i, T_1\}$ and $\{N_3, K_i, T_3\}$, and wants to get the password pw_i. As illustrated in subsection 2.3 in this section, E cannot check the guessed password pw_i^* from the stored value $\{A_i, B_i, C_i, L_i, e, n, h(\cdot)\}$ in the smart card without the help of F_i, b_i, and d, where $A_i = h(ID_i||d) \oplus h(pw_i||b_i)$, $B_i = (h(pw_i||b_i)||h(ID_i||d))^e \bmod n$, $C_i = b_i \oplus H(F_i)$, and $L_i = h(ID_i||pw_i||F_i||b_i)$. Also, we can see that E cannot get the password pw_i by the equations $B_i = (h(pw_i||b_i)||h(ID_i||d))^e \bmod n$, $D_i = h(h(pw_i||b_i)||h(ID_i||d)||N_1||T_1)$, $E_i = h(pw_i||b_i) \oplus N_1$, and $K_i = h(h(ID_i||d)||N_2||T_3)$, because E doesn't know b_i and d. Therefore, our scheme is secure against off-line password guessing attacks.

2.6 Impersonation attacks

An impersonation attack is an attempt by an adversary E to generate a legal message of the user or the server. We assume E can eavesdrop all transmitted messages $\{ID_i, B_i, D_i, E_i, T_1\}$ and $\{N_3, K_i, T_3\}$ from the previous session between U_i and S. First, suppose E wants to impersonate a valid user U_i to the server S. To impersonate U_i to S, E has to generate a valid login request message $\{ID_i, B_i, D_i, E_i, T_1\}$ to prove its legitimacy, where $B_i = (h(pw_i||b_i)||h(ID_i||d))^e \bmod n$, $D_i = h(h(pw_i||b_i)||h(ID_i||d)||N_1||T_1)$, and $E_i = h(pw_i||b_i) \oplus N_1$. However, E cannot generate a valid login message without the value pw_i, b_i, F_i, and d. Therefore, the adversary cannot impersonate a legal user. Secondly, suppose E wants to impersonate a legal server and spoof the user U_i. E has to produce a valid response $\{N_3, K_i, T_3\}$, where $K_i = h(h(ID_i||d)||N_2||T_3)$. However, since E does not know S's private key d, E cannot compute K_i. Therefore, the adversary is not able to produce a response message and impersonate a legal server. Hence, the proposed scheme is secure against user impersonation attacks and authentication is provided in our scheme.

2.7 Stolen verifier attacks

The stolen verifier attack means that a malicious user steals or modifies the verification data (e.g., plaintext passwords, hashed passwords) stored in the server.

In the proposed scheme, the telecare server does not maintain any passwords, biometrics or verification information of users in its database. The only secret information that needs to be maintained by the server is the private key d. Therefore, the proposed scheme is secure against stolen verifier attacks.

2.8 Known-key security

In the proposed scheme, the shared session key $SK = h(ID_i||pwb_i||N_1||N_2)$ changes in each session run. Even if an adversary somehow obtains a shared session key, he/she still is not able to compute other session keys. Because, values of N_1 and N_2 differ in each session run, and without knowing N_1 or N_2, it is difficult to compute the session key. Therefore, known-key security is provided in our proposed scheme.

2.9 Session key security

The proposed scheme provides session key security. The session key $SK = h(ID_i||pwb_i||N_1||N_2)$ is not known by anyone but only U_i and S since the random values N_1 and N_2 are protected by the secure one-way hash function. Nothing about this session key $SK = h(ID_i||pwb_i||N_1||N_2)$ is known to anybody but U_i and S. Therefore, the proposed scheme provides the session key security.

3. Security and performance comparison

In this section, we compare the security and

Table 2. Security attributes comparison of the proposed scheme with related schemes

Schemes	P1	P2	P3	P4	P5	P6	P7	P8	P9
Wu et al.[5]	X	√	X	√	√	X	√	√	√
He et al.[6]	√	√	X	√	√	√	√	√	√
Wei et al.[7]	√	√	X	X	√	√	√	√	√
Zhu[8]	√	X	√	X	√	√	√	√	√
Khan-Kumari[10]	√	√	X	√	√	√	√	√	√
Giri et al.[11]	√	X	X	√	√	√	√	√	√
Th proposed	√	√	√	√	√	√	√	√	√

P1: Privileged insider attacks
P2: Replay attacks or Parallel session attacks
P3: Lost smart card attacks
P4: On-line password guessing attacks
P5: Off-line password guessing attacks
P6: Impersonation attacks
P7: Stolen verifier attacks
P8: Known-key security
P9: Session key security
√: The scheme can resist such attack or provide such security property.
X : The scheme cannot resist such attack or provide such security property.

performance of the proposed scheme with the recently published password-based authentication schemes for TMIS [5-8,10]. It can be easily seen from Table 2 that most of the authentication schemes for TMIS does not satisfy desirable security attributes, although the proposed scheme ensures overcome the weaknesses of existing schemes.

A user needs to perform the login and authentication phases repeatedly to establish authorized session, although the registration phase and the password and biometrics update phase are almost one time, therefore, we are only discussing the computation overhead of the login and authentication phase. Table 3 shows the computation overhead of these scheme in the login and authentication phase, where T_e, T_h, T_{inv}, T_m, and T_{div} denote the time of executing a modular exponentiation, a one-way hash function operation, a inversion, a multiplication, and a division, respectively. The cost of our scheme is slightly higher than that of Giri et al.'s scheme in the user side. However, Giri et al.'s scheme is vulnerable to lost smart card attacks and replay attacks. As a result, our scheme is superior to Giri et al.'s scheme in terms of security.

Table 3. Computation cost comparison of the proposed scheme with related schemes

Schemes	User side	Server side
Wu et al.[5]	$4T_h+T_e$	$4T_h+T_e$
He et al.[6]	$5T_h+T_e+T_{inv}$	$5T_h+T_e+T_{inv}$
Wei et al.[7]	$5T_h+T_e+T_m$	$5T_h+T_e+T_{div}$
Zhu[8]	$4T_h+T_e$	$4T_h+T_e$
Khan-Kumari[10]	$6T_h+2T_e$	$4T_h+3T_e$
Giri et al.[11]	$5T_h$	$4T_h+T_e$
Th proposed	$6T_h$	$4T_h+T_e$

IV. Conclusions

In this paper, we have discovered two security weaknesses in Giri et al.'s RSA-based authentication scheme for TMIS. We have shown that Giri et al.'s scheme is vulnerable to replay attacks and lost smart card attacks. In order to improve the security, we have proposed a robust RSA-based authentication and key agreement scheme for TMIS. According to the security and performance analysis, the proposed scheme withstands various attacks. Therefore, our scheme is suitable to be applied in TMIS.

We only provide a heuristic security analysis to the proposed protocol. In the future, we will research a more efficient and secure authentication protocol for TMIS and demonstrate it is theoretically secure with security proof using formal proof model.

REFERENCES

[1] C. Lambrinoudakis, and S. Gritzalis, "Managing Medical and Insurance Information Through a Smart-card-based Information System," J. Med. Syst., Vol. 24, No. 4, pp. 213-234, Aug. 2000. DOI: 10.1023/A:1005549330655

[2] L. Lamport, "Password Authentication with Insecure Communication," Comm. ACM, Vol. 24, No. 11, pp. 770-772, Nov. 1981. DOI: 10.1145/358790.358797

[3] M.S. Hwang, and L.H. Li, "A New Remote User Authentication Scheme Using Smart Cards," IEEE Trans. Consum. Electron., Vol. 46, No. 1, pp. 28-30, Feb. 2000. DOI: 10.1109/30.826377

[4] Y.F. Chang, C.C. Chang, and J.Y. Kuo, "A Secure One-time

Password Authentication Scheme Using Smart Cards without Limiting Login Times," ACM SIGOPS Operating Systems Review, Vol. 38, No. 4, pp. 80-90, Oct. 2004. DOI: 10.1145/1031154.1031164

[5] Z.Y. Wu, Y.C. Lee, F. Lai, H.C. Lee, Y. Chung, "A Secure Authentication Scheme for Telecare Medicine Information Systems," J. Med. Syst., Vol. 36, No. 3, pp. 1529-1535, Jun. 2012. DOI: 10.1007/s10916-010-9614-9

[6] D. He, J. Chen, R. Zhang, "A More Secure Authentication Scheme for Telecare Medicine Information Systems," J. Med. Syst., Vol. 36, No. 3, pp. 1989-1995, Jun. 2012. DOI: 10.1007/s10916-011-9658-5

[7] J. Wei, X. Hu, W. Liu, "An Improved Authentication Scheme for Telecare Medicine Information Systems," J. Med. Syst., Vol. 36, No. 6, pp. 3597-3604, Dec. 2012. DOI: 10.1007/s10916-012-9835-1

[8] Z. Zhu, "An Efficient Authentication Scheme for Telecare Medicine Information Systems," J. Med. Syst., Vol. 36, No. 6, pp. 3833-3838, Dec. 2012. DOI: 10.1007/s10916-012-9856-9

[9] R.L. Rivest, A. Shamir, L. Adleman, "A Method for Obtaining Digital Signatures and Public-key Cryptosystems," Commun. ACM, Vol. 21, No. 2, pp. 120-126, Feb. 1978. DOI: 10.1145/359340.359342

[10] M.K. Khan, and S. Kumari, "An Authentication Scheme for Secure Access to Healthcare Services," J. Med. Syst., Vol. 37, No. 4, pp. 9954, Aug. 2013. DOI: 10.1007/s10916-013-9954-3

[11] D. Giri, T. Maitra, R. Amin, and P.D. Srivastava, "An Efficient and Robust RSA-Based Remote User Authentication for Telecare Medical Information Systems," J. Med. Syst. Vol. 39, No. 1, pp.145, Jan. 2015. DOI: 10.1007/s10916-014-0145-7

[12] P. Kocher, J. Jae, B. Jun, "Differential Power Analysis," CRYPTO 99, LNCS 1666, pp. 388-397, 1999. DOI: 10.1007/3-540-48405-1_25

[13] T. Messerges, E. Dabbish, R. Sloan, R., "Examining Smart-card Security under the Threat of Power Analysis Attacks," IEEE Trans. Comput. Vol. 51, No. 5, pp. 541-552, May 2002. DOI: 10.1109/TC.2002.1004593

[14] E. Brier, C. Clavier, and F. Olivier, "Correlation Power Analysis with a Leakage Model," CHES 2004, LNCS 3156, pp. 16-29, 2004. DOI: 10.1007/978-3-540-28632-5_2

[15] T. Eisenbarth, T. Kasper, A. Moradi, C. Paar, M. Salmasizadeh, and M.T.M. Shalmani, "On the Power of Power Analysis in the Real World: A Complete Break of the Keeloq Code Hopping Scheme," CRYPTO 08, LNCS 5157, pp. 203-220, 2008. DOI: 10.1007/978-3-540-85174-5_12

[16] C. Boyd, and A. Mathuria, "Protocols for Authentication and Key Establishment" Springer, 2003.

[17] C.C. Yang, H.W. Yang, and R.C. Wang, "Cryptanalysis of Security Enhancement for the Timestamp-based Password Authentication Scheme Using Smart Cards," IEEE Trans. Consum. Electron., Vol. 50, No. 2, pp. 578-579, May 2004. DOI: 10.1109/TCE.2004.1309428

Authors

Keewon Kim received the M.S. and Ph.D. degrees in Computer Engineering from Kyungpook National University, Korea, in 2001 and 2006, respectively. He is currently an assistant professor in the department of Applied Computer Engineering, Dankook University. He is interested in information security, security protocol, VLSI, and big data analysis.