PLOS ONE

RESEARCH ARTICLE

An enhanced password authentication scheme for session initiation protocol with perfect forward secrecy

Shuming Qiu[1,2☯]*, **Guoai Xu**[1☯]*, **Haseeb Ahmad**[3☯], **Yanhui Guo**[1☯]

1 School of CyberSpace Security, Beijing University of Posts and Telecommunications, Beijing, 100876, China, **2** Elementary Educational College, Jiangxi Normal University, Nanchang, 330022, China, **3** Department of Computer Science, National Textile University, Faisalabad, 37610, Pakistan

☯ These authors contributed equally to this work.
* qiushuming2008@163.com (SQ); xga@bupt.edu.cn (GX)

Citation: Qiu S, Xu G, Ahmad H, Guo Y (2018) An enhanced password authentication scheme for session initiation protocol with perfect forward secrecy. PLoS ONE 13(3): e0194072. https://doi.org/10.1371/journal.pone.0194072

Editor: Muhammad Khurram Khan, King Saud University, SAUDI ARABIA

Received: December 31, 2017

Accepted: February 25, 2018

Published: March 16, 2018

Data Availability Statement: All relevant data are within the paper and its Supporting Information files.

Funding: This research is supported by the National Key Research and Development Plan (Grant No. 2017YFB0801901) to GX and National Key Research and Development Program of China (Grant no. 2017YFB0801900) to GX. The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Abstract

The Session Initiation Protocol (SIP) is an extensive and esteemed communication protocol employed to regulate signaling as well as for controlling multimedia communication sessions. Recently, Kumari et al. proposed an improved smart card based authentication scheme for SIP based on Farash's scheme. Farash claimed that his protocol is resistant against various known attacks. But, we observe some accountable flaws in Farash's protocol. We point out that Farash's protocol is prone to key-compromise impersonation attack and is unable to provide pre-verification in the smart card, efficient password change and perfect forward secrecy. To overcome these limitations, in this paper we present an enhanced authentication mechanism based on Kumari et al.'s scheme. We prove that the proposed protocol not only overcomes the issues in Farash's scheme, but it can also resist against all known attacks. We also provide the security analysis of the proposed scheme with the help of widespread AVISPA (Automated Validation of Internet Security Protocols and Applications) software. At last, comparing with the earlier proposals in terms of security and efficiency, we conclude that the proposed protocol is efficient and more secure.

1 Introduction

The Session Initiation Protocol (SIP) is an important and popular communications protocol for signaling and controlling multimedia communication sessions in applications including Internet telephony for voice and video calls, private IP telephone systems, as well as instant messaging over Internet Protocol (IP) networks [1, 2]. Up to now, SIP has gained the attention of extensive scholastic community.

The first authentication scheme for SIP based on hyper text transfer protocol (HTTP) digest authentication can be traced back to 1999 proposed by Franks et al. [3]. In 2005, Yang et al. [4] pointed out that the scheme of Franks et al. [3] cannot resist the off-line password guessing attack and the server impersonation attack. Subsequently, Yang et al. [4] presented an new scheme to cope with the aforementioned issue in [3]. However, Huang et al. [5] proved that

Competing interests: The authors have declared that no competing interests exist.

Yang et al.'s [4] scheme cannot resist the stolen-verifier, the off-line password guessing and the Denning-Sacco attacks [6], and is not suitable for power constraint devices because of the high computational cost. In 2005, in order to improve Yang et al.'s [4] scheme, Durlanik and Sogukpinar [7] proposed an efficient and secure authentication scheme for SIP using the Elliptic Curve Cryptography (ECC). It is known that ECC could provide the same security with a smaller key size comparing with the other traditional Public Key Cryptography. Subsequently, numerous one-factor, two-factor and three factor authentication schemes have been proposed for SIP using ECC, RSA, Hash function or Chaotic theory, etc [7–25].

1.1 Related works

Recently, Zhang et al. [26] pointed out that the existing protocols for SIP require the SIP server maintaining a password or verification table, which makes these protocols vulnerable to stolen-verifier attack, server spoofing attack, insider attack, and password-guessing attack. To address these issues, Zhang et al. proposed a new two-factor authentication protocol for SIP by using smart cards to avoid maintenance of password tables at the SIP server.

Later, Zhang et al. [27] showed that their scheme [26] is prone to impersonation attack problem. To remedy this problem, the authors proposed a much improved protocol based on Zhang et al.'s protocol [26] by using smart card. However, Farash [28] pointed out that Zhang et al. protocol [27] is still insecure against the impersonation attack. Thereupon, Farash proposed an improved protocol by making a slight change in Zhang et al. protocol [27]. However, Lu et al. [29] analyzed the security of Farash's [28] scheme and pointed out that the enhanced scheme presented by Farash et al. [28] has still some security vulnerabilities, including key-compromise impersonation attack, off-line guessing attack and lack of anonymity, pre-verification. Afterwards, Lu et al. designed a preserving anonymous authentication protocol to remedy the security limitations of Farash's scheme. The authors showed that their scheme is resistance to all known attacks besides those attacks existed in Farash's scheme. But subsequently, Kumari [30] showed that an adversary is able to calculate the user's identity and password once the adversary obtains the datum of user's smart card in Lu et al. [29]'s scheme. Thus, Kumari [30] claimed that Lu et al.'s scheme does not adhere to two-factor security criterion. Besides, the author also pointed out that the key agreement procedure of Lu et al. [29]'s scheme cannot culminate to achieve the intended aim of authenticated key agreement. On the other hand, in order to eliminate the drawbacks of Zhang et al. [26]'s scheme, Irshad et al. [31] also developed an enhancement SIP authentication scheme only using a single round-trip in 2005. But, Arshad et al. [32] found that the improvement of Irshad et al. [31] was also susceptible to the user impersonation attack and further proposed their improved scheme regarding performance and security analyses. However, the modified scheme of Arshad et al. [32] was demonstrated to be lacking user anonymity and mutual authentication and susceptible to the key-compromise impersonation attack by Lu et al. [33]. In 2014, Jiang et al. [34] also observed that Zhang et al.'s scheme [26] was prone to the user impersonation attack and made a few modifications to enable more secure than the original design. Azrour et al. [35] showed that Jiang et al.'s protocol suffers from server impersonation attack.

In 2014, Tu et al. [36] also proved that Zhang et al. [26]'s scheme is vulnerable to user impersonation attack. Furthermore, Tu et al. [36] proposed an enhanced protocol to improve the security. However, Farash [37] pointed out that Tu et al.'s scheme is still vulnerable to server impersonation attack and proposed an improvement in Tu et al.'s scheme. In 2015, Chaudhry et al. [38] also showed that Tu et al.'s scheme [36] is vulnerable to server impersonation, replay and denial of services attacks as well as lacking user anonymity. Moreover, Chaudhry et al. [38] also analyzed that Farash's improvement [37] on Tu et al.'s scheme [36] is lacking

user anonymity and is also vulnerable to replay attack. Thereupon, Chaudhry et al. [38] proposed an anonymous authenticated key agreement scheme while claiming that it is more secure and suitable for all lightweight environments. Recently, Kumari et al. [39] also analyzed Farash's protocol [37] and showed that it is vulnerable to user impersonation attack, password guessing attack, session-specific temporary information leakage attack and lacks to provide user anonymity. Furthermore, Kumari et al. [39] proposed an improved protocol, and showed that their protocol is not only robust against all known attacks, but is also lightweight as compared to Farash's protocol [37]. From the above analysis, one can observes that most of these protocols have still some security loopholes and not really reach the security of the authentication protocol. Accordingly, it is still a challenging academic topic to design a more secure and efficient authentication and key agreement protocol for SIP.

1.2 Contribution of this paper

The positional relation of the proposed scheme and related researches are depicted in Fig 1. The contributions of this paper are listed as follows:

- We concentrate on analyzing the security of Kumari et al. [39]'s authentication scheme for SIP, and point out that Kumari et al. [39]'s scheme fails to provide pre-verification, local password change in smart card and perfect forward secrecy, is also susceptible to key-compromise impersonation attack.
- To overcome aforementioned limitations, we propose an improved scheme while maintaining the benefits of the original schemes at the cost of slight increase in the computation consumptions by employing "Fuzzy-Verifier" [40]. Besides, we prove that our scheme provides various security features including perfect forward secrecy and resistance against key-compromise impersonation attack, etc.
- We use AVISPA tool to prove that proposed scheme satisfies the mutual authentication and session key secrecy.
- We provide security and performance comparisons with various relevant schemes. It illustrates that the proposed scheme is efficient and more secure than the prevalent schemes.

1.3 Organization of this paper

The remainder of this paper is organized as follows: Section "Preliminaries" introduces some notations, associated difficult problems based on ECC and adversary model used in this paper. The review and cryptanalysis of Kumari et al. [39]'s scheme is detailed in

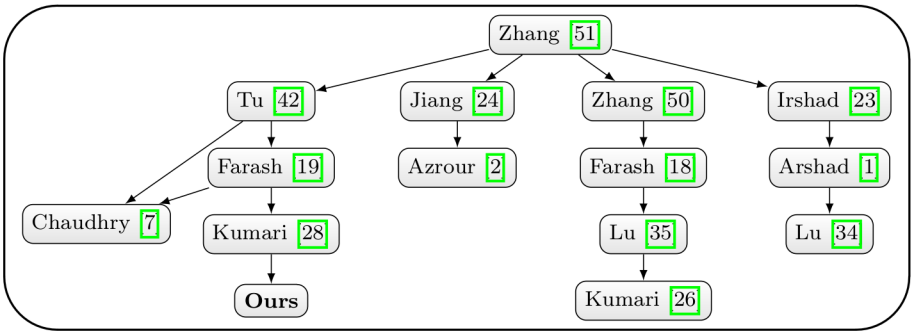

Fig 1. Positional relation of the proposed scheme.

https://doi.org/10.1371/journal.pone.0194072.g001

Section "Review of Kumari et al.'s scheme" and Section "Cryptanalysis of Kumari et al.'s scheme", respectively. Section "The enhanced scheme for SIP" provides our proposed scheme. Section "Security analysis of the enhanced scheme" and Section "Formal security validation using AVISPA tool" highlight an informal and formal security analysis of our scheme, respectively. The performance and functionality comparison is presented in Section "Comparative analysis of performance". At last, we provide concluding remarks in Section "Conclusion".

2 Preliminaries

In this section, we describe some notations and the definitions of one-way hash function and hard problems related with the Elliptic Curve Cryptography(ECC) and the capacities of the adversary in this paper. Some notations used in this paper are listed in Table 1.

2.1 Intractable problems

Definition 1 (Collision-resistant one-way hash function) A secure one-way hash function $h(\cdot)$: $\{0, 1\}^* \rightarrow \{0, 1\}^n$ takes an arbitrary length binary string $x \in \{0, 1\}^*$ as an input, and outputs a binary string $y = h(x) \in \{0, 1\}^n$. A cryptographic hash function $h(\cdot)$ satisfies the following properties.

1. It is hard to find the the input $x \in \{0, 1\}^*$ in polynomial time for given $y \in \{0, 1\}^n$;
2. It is hard to find $x' \in \{0, 1\}^*$ such that $x' \neq x$ and $h(x) = h(x')$;
3. It is hard to find a pair $(x, x') \in \{0, 1\}^*$ such that $h(x) = h(x')$, where $x' \neq x$.

In ECC, the elliptic curve equation is defined as the form of $E_p(a, b)$: $y^2 = x^3 + ax + b(\mathrm{mod}\, p)$ over a finite field F_p, where $a, b \in F_p$ and $4a^3 + 27b \neq 0(\mathrm{mod}\, p)$.

Definition 2 (ECDLP) For given generator P and $Q = mP$ in $E_p(a, b)$, where m is randomly selected from F_p and p is sufficiently large prime, it is computationally hard by a probabilistic polynomial time (PPT) adversary $\mathcal{A}$ to calculate the secret value $m \in F_p$ such that $Q = mP$.

Definition 3 (ECCDHP) For given points $mP, nP \in E_p(a, b)$, computing mnP is computationally infeasible by a probabilistic polynomial time (PPT) adversary $\mathcal{A}$.

Table 1. Notations and abbreviations.

Symbol	Description
S	Server
U	Patient/User
ID	Identity of U
PW	Password of U
c_u, a_u	Random numbers of U
k_s	Secret key of S
b, c_s	Random numbers of S
$\|\|$	The string concatenation operation
$\oplus$	The bitwise XOR operation
$\mathcal{A}$	Malicious adversary
$h(\cdot)$	Collision free one-way hash function
$\rightarrow$	An insecure channel
$\Rightarrow$	A secure channel
sk	Session key between U and S

https://doi.org/10.1371/journal.pone.0194072.t001

2.2 Adversary model

Throughout this paper, according to [40–43], the capacities of the adversary $\mathcal{A}$ are summarized as follows:

1. The adversary $\mathcal{A}$ has the capability to extract all parameters stored in smart card utilizing the power analysis method [41, 42].
2. The adversary $\mathcal{A}$ is able to control the open communication channel completely, i.e. he can intercept, modify, delete, block, and resend the messages over the open channel.
3. The adversary $\mathcal{A}$ can list all pairs of (ID_i, PW_i) from $(\mathcal{D}_{PW}, \mathcal{D}_{ID})$ in a polynomial time, where $\mathcal{D}_{PW}$ and $\mathcal{D}_{ID}$ denote the space of passwords and the space of identities, respectively.
4. The adversary $\mathcal{A}$ can either intercept the password of the user via malicious device or extract the parameters from smart card, but not both.
5. While evaluating forward secrecy, the adversary $\mathcal{A}$ can obtain server's private key or comprise of the user's password.
6. When it comes to key-compromise impersonation attack, we assume that $\mathcal{A}$ knows the long-term private key of server.

3 Review of Kumari et al.'s scheme

3.1 System setup phase

The server S chooses an elliptic curve E over the finite field F_q and an additive group G of order p with P as generator, a one-way hash function $h(\cdot)$, a secret key $k_s \in Z_p^*$ computes its public key $Q = kP$. At last, S publishes its public parameters $\{E(F_q), P, p, Q, h(\cdot)\}$, and keeps k_s as its long-term private key.

3.2 Registration phase

In this phase, the user U is registered as a legal user by executing the following steps over the secure channel:

Step 1: User U selects his identity ID, password PW and a random number $a_u \in Z_p^*$. Then, he computes $VPW = h(ID||PW||a_u)$ and sends the registration request message $\{ID, VPW\}$ to server S

Step 2: After receiving the request message $\{ID, VPW\}$, S calculates $r_u = (VPW + h(ID||k_s))P$, and stores r_u in a new smart card SC. Also, S issues $SC = \{r_u, Q = k_sP, h(\cdot)\}$ to U

Step 3: Upon receiving the new smart card SC, U inserts a_u in SC. Finally, $SC = \{r_u, Q = k_sP, a_u, h(\cdot)\}$ and U is thus registered as a legal user.

3.3 Login and mutual authentication phase

In this phase, user U establishes the session key with server S as follows:

Step 1: U inserts his smart card SC to a card reader and inputs his identity ID and password PW.

Step 2: U selects a random number $b \in Z_p^*$, and computes bP, $V = bQ$, $W_u = b(r_u - VPW \cdot P)$. U further calculates $f_u = ID \oplus V_x$, $z_u = h(ID||bP||V_y||W_u)$, where V_x, V_y are x^{th}, y^{th} components of V, respectively. At last, U sends the login request message $\{f_u, bP, z_u\}$ to S.

Step 3: After receiving the request message $\{f_u, bP, z_u\}$, S computes $V = k_sQ$. Subsequently, S computes $ID = f_u \oplus V_x$ and further calculates $W_u^* = h(ID||k_s)bP, z_u^* = h(ID||bP||V_y||W_u^*)$. S then checks whether $z_u^* \stackrel{?}{=} z_u$. If it holds, S chooses a random number $c \in Z_p^*$ and calculates $sk = h(W_u^*||bP||V||c||ID)$, $Auth_s = h(c||sk)$. Afterwards, S sends the challenge request message $\{c, Auth_s\}$ to u.

Step 4: After receiving the challenge message $\{c, Auth_s\}$, U calculates $sk = h(W_u||bP||Q||V||c||ID)$, $Auth_s^* = h(c||sk)$. U then checks whether $Auth_s^* \stackrel{?}{=} Auth_s$. If it holds, U calculates $Auth_u = h(ID||c + 1||sk)$ and sends the response message $\{Auth_u\}$ to S.

Step 5: Once receiving the response message $\{Auth_u\}$, S computes $Auth_u^* = h(ID||c + 1||sk)$. U then verifies whether $Auth_u^* \stackrel{?}{=} Auth_u$. If $Auth_u^* = Auth_u$, S believes that it has successfully established the session key sk with U.

3.4 Password changing phase

In this phase, U can change his password by interacting with the server S. After U establishes the session key sk with S, U changes his password by performing the following steps:

Step 1: User U selects his new password PW^{new} and two random numbers $a_u^{new}, e \in Z_p^*$. Subsequently, he computes $VPW^{new} = h(ID||PW^{new}||a^{new})$ and then calculates $m_u = Enc_{sk}(ID||e||VPW^{new}||h(ID||e||VPW^{new}))$. At last, U send the request message $\{m_u, e\}$ to server S.

Step 2: After receiving the request message $\{m_u, e\}$, S computes $Dec_{sk}(m_u) = ID||e||VPW^{new}||h(ID||e||VPW^{new})$. Subsequently, S verifies the validity of $h(ID||e||VPW^{new})$. If it passes the validity test, afterwards S calculates $r_u^{new} = (VPW^{new} + h(ID||k_s))P, m_s = Enc_{sk}(r_u^{new}||h(ID||e + 1||r_u^{new}))$. S then sends response message $\{m_s\}$ to U.

Step 3: Upon getting the message $\{m_s\}$, U decrypts m_s and obtains $r_u^{new}, h(ID||e + 1||r_u^{new})$. Subsequently, U verifies the validity of $h(ID||e + 1||r_u^{new})$. If it passes the validity test, U replaces r_u^{new}, a_u^{new} with r_u, a_u, respectively.

4 Cryptanalysis of Kumari et al.'s scheme

Kumari et al. [39] claimed that their scheme can resist many known attacks. However, we explain minutely that the scheme of Kumari et al. not only fails to provide pre-verification in smart card, perfect forward secrecy and efficient password changing, but also fails to resist key-compromise impersonation attack in the following subsections. Actually, the above functions are fundamental and crucial to authentication scheme for session initiation protocol. Accordingly, these imply that their scheme is still unsuitable for the practical session initiation protocol.

4.1 Pre-verification in smart card

When a user inputs her/his password and identity, if the smart card verifies their correctness, implies that respective protocol can provide pre-verification in smart card. But, Kumari et al.'s scheme is not providing such mechanism.

In the login phase of Kumari et al.'s scheme, the smart card is unable to provide any verification for the password and identity information of user because there is no verified information in smart card. If the user inputs the wrong password and identity or an adversary $\mathcal{A}$ performs this step, the smart card fails to check this problem. Until the server finds the

incorrectness of the login, the session will not be terminated. In this case, it increases computational cost of server. Consequently, Kumari et al.'s scheme is unable to provide the pre-verification in smart card.

4.2 Key-compromise impersonation attack

Let us consider a scenario that when the long-term private key of server S is compromised, an adversary $\mathcal{A}$ can certainly impersonate the legal server of being legitimate user, but if $\mathcal{A}$ is not impersonated as the legal user by the corresponding server, we say that this protocol can resist key-compromise impersonation attack. It is a pity that Kumari et al.'s scheme is unable to withstand this attack. Now, let's execute the following steps to attack their scheme.

Step 1: Firstly, the adversary $\mathcal{A}$ gets some useful information $\{r_u, kP, a_u\}$ stored in smart card utilizing the side-channel attack [41]. $\mathcal{A}$ then captures the login request message $\{f_u, bP, z_u\}$ of user. If the long-term private key k of S is revealed to $\mathcal{A}$, $\mathcal{A}$ computes $V = k(bP)$, and further calculates the real identity $ID = f_u \oplus v_x$. As an illegal user, $\mathcal{A}$ randomly selects $b' \in Z_p^*$ and computes $V' = b'(kP)$, $w'_u = b'(r_u - h(ID||PW||a_u))P = b'h(ID||k)P, f'_u = ID \oplus V'_x$, $z'_u = h(ID||b'P||V_y||w'_u)$. Subsequently, the adversary $\mathcal{A}$ sends the forged request message $\{f'_u, b'P, z'_u\}$ to S.

Step 2: On receiving the request message, S then computes $V' = k(b'P)$, $ID = f'_u \oplus V'_x$, $w^*_u = h(ID||k)b'P$, $z^*_u = h(ID||b'P||V'_y||w*_u)$ and checks the correctness of z'_u. Obviously, $z^*_u = z'_u$. This infers that the illegal user $\mathcal{A}$ is successfully authenticated by server S. S further chooses a random number $c \in Z_p^*$ and calculates $sk = h(w^*_u||b'P||kP||V'||c||ID)$, $Auth_s = h(c||sk)$. Finally, the server S returns the message $\{c, Auth_s\}$ to $\mathcal{A}$.

Step 3: On receiving the challenge message from the server, $\mathcal{A}$ computes $sk' = h(w'_u||b'P||kP||V'||c||ID), Auth^*_s = h(c||sk')$ and verifies whether $Auth_s \stackrel{?}{=} Auth^*_s$. If it holds, then $\mathcal{A}$ calculates $Auth'_u = h(ID||c+1||sk')$ and sends the response message $\{Auth'_u\}$ to S.

Step 4: Upon getting the response message, S computes $Auth^*_u = h(ID||c+1||sk)$ and checks whether $Auth^*_u = Auth'_u$. We know that it is obvious. Therefore, the server S undoubtedly believes that it has successfully established the session key sk with the legal user. Actually, the server suffers from the key-compromise impersonation attack.

Accordingly, we infer that Kumari et al.'s scheme fails to resist key-compromise impersonation attack.

4.3 Perfect forward secrecy

In case, when the long-term private key k is compromised to the adversary $\mathcal{A}$, $\mathcal{A}$ will execute the following steps to attack Kumari et al.'s scheme.

Step 1: $\mathcal{A}$ intercepts the login request message $\{f_u, bP, z_u\}$ of user S. Afterwards, $\mathcal{A}$ computes $V = k(bP)$ and obtains $\{V_x, V_y\}$.

Step 2: $\mathcal{A}$ gets $ID = f_u \oplus V_x$ and further computes $w^*_u = h(ID||k)bP$.

Step 3: $\mathcal{A}$ captures the challenge request message $\{c, Auth_s\}$ of server S and calculates

$$sk = h(w^*_u||bP||V||c||ID).$$

Afterwards, the adversary $\mathcal{A}$ obtains the current session key sk when the long-term private key k is revealed to $\mathcal{A}$, and thus the whole session is completely exposed to $\mathcal{A}$.

Therefore, Kumari et al.'s scheme fails to provide the perfect forward secrecy.

4.4 Efficient password changing

In the password changing phase of Kumari et al.'s scheme, if the user U wants to change her/his password, she/he must firstly establish the session key with the server. In this way the communication and computational overhead is increased to a large extent.

5 The enhanced scheme for SIP

In this section, we present an improved scheme based on the Kumari et al.'s scheme. Meanwhile, our proposed scheme not only overcomes the limitations of Kumari et al.'s scheme but also achieves mutual authentication and resists against various known attacks. Specifically, we employ public-key primitive to intrinsically protect the identity of the user and provide perfect forward secrecy. In registration phase, the server S generates a random nonce b to prevent the long-term private key of S from being compromised. In the password changing phase, the smart card SC can provide the function of the local password change. The proposed scheme is comprised of four phases, i.e., system initialization, registration, login-authentication and password change. The registration and login-authentication phases are depicted in Fig 2.

5.1 System initialization phase

In this phase, the server S selects an elliptic curve E over the finite field F_p, a random number $k \in Z_p^*$ and a one-way hash function $h(\cdot)$. S then computes $G = kP$ as the public key of S. Finally, the server S publishes the parameters $\{E, P, G, h(\cdot)\}$, while maintains k_s as the long-term private key of S.

5.2 Registration phase

Step 1. The user U chooses an identity ID.

Step 2. $U \Rightarrow S$: $\{ID\}$.

Step 3. After receiving the registration message from U, S chooses two random numbers a_u, $b \in Z_p^*$ and calculates $N = h(k||ID||b)$, $VPW = h(PW_0||a_u||ID)$, where PW_0 is the initial password. S further computes $r_u = N \oplus VPW$ and $A_u = h((h(ID) \oplus VPW) \bmod n_0)$, where n_0 is an integer and $2^4 \leq n_0 \leq 2^8$. Subsequently, S stores $\{ID, b\}$ in its database.

Step 4. $S \Rightarrow U$: $\{SC, PW_0\}$, where the smart card SC contains $\{r_u, P, a_u, A_u, p, G = kP, n_0, h(\cdot)\}$.

Step 5. On receiving the smart card SC from S, the user U should immediately change the initial password during password update phase.

5.3 Login and mutual authentication phase

Once the patient U registers to the server successfully, he can send the login request to the server S when he wants to enjoy the service as follows:

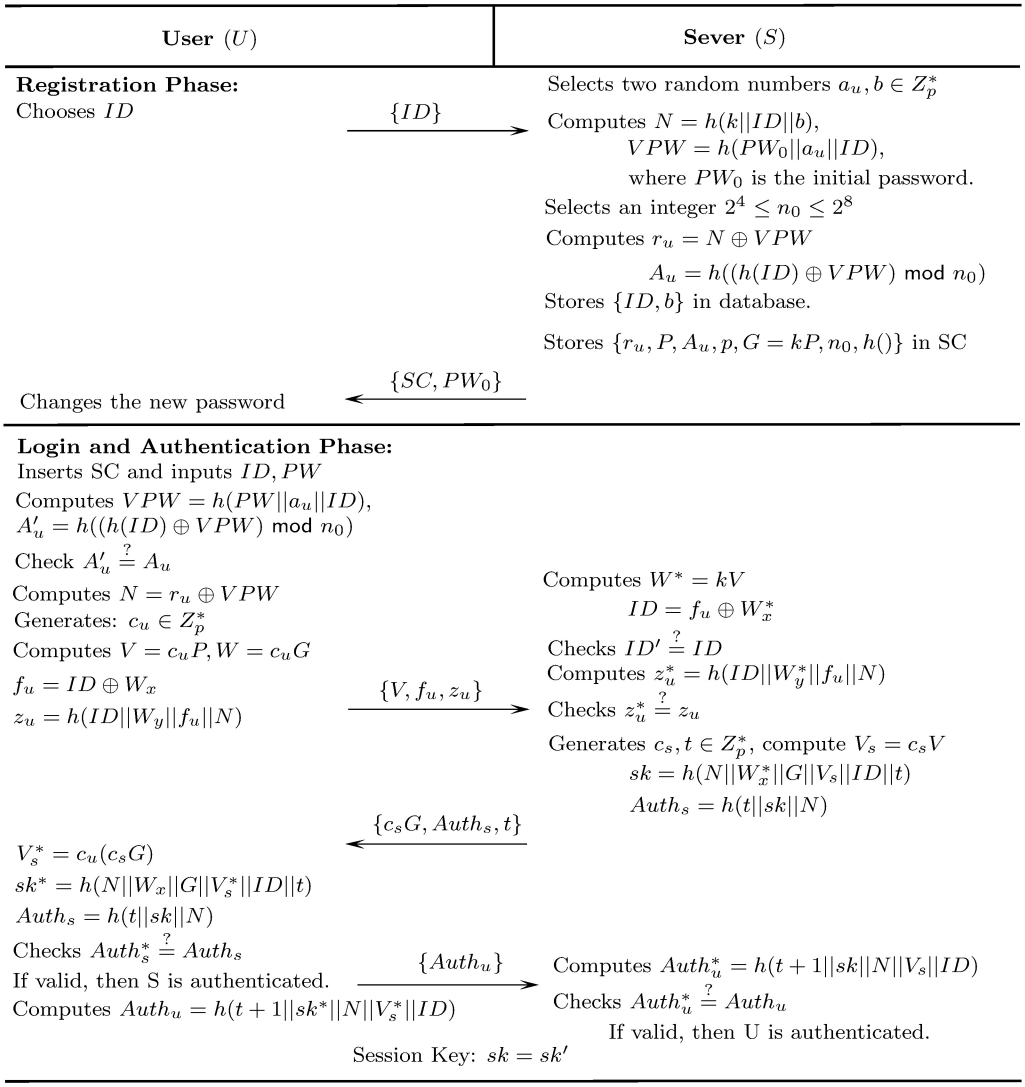

Fig 2. Registration and authentication phase of our scheme.

https://doi.org/10.1371/journal.pone.0194072.g002

Step 1. *U* inserts the smart card *SC* into a card reader and inputs *ID*, *PW*.

Step 2. *SC* calculates $VPW = h(PW||a_u||ID)$, and then computes $A'_u = h((h(ID) \oplus VPW) \bmod n_0)$. Then *SC* checks the correctness of A'_u by comparing the value of A_u sorted in *SC*. If $A'_u = A_u$, it shows that *ID*, *PW* are valid. Otherwise, the session is terminated.

Step 3. *SC* continues computing $N = r_u \oplus VPW$ and chooses a random number $c_u \in Z_p^*$, and then computes $V = c_u P$, $W = c_u G$, $f_u = ID \oplus W_x$, $z_u = h(ID||W_y||f_u||N)$, where W_x, W_y are x^{th}, y^{th} components of *W*, respectively.

Step 4. $U \rightarrow S$: $\{V, f_u, z_u\}$.

Step 5. After obtaining $\{V, f_u, z_u\}$, *S* calculates $W^* = kV$, $ID = f_u \oplus W_x^*$ and checks $ID'_i \stackrel{?}{=} ID_i$ by searching database list. If these are not equal, *S* judges that the input password is wrong. As

the wrong attempts exceed the threshold (such as 8), S forms a judgement that the smart card is usurped by some attacker. What's more, S locks the smart card until U re-registers. Otherwise, S computes $z_u^* = h(ID||W_y^*||f_u||N)$ and verifies $z_u^* \stackrel{?}{=} z_u$. If it is not found valid, S exits the session and counts a number $T = 1$. Alongwith, S suspends the card until U re-registers when T exceeds some threshold value. Otherwise, S generates a random number c_s, $t \in Z_p^*$ and computes $V_s = c_s V$, $sk = h(N||W_x^*||G||V_s||ID||t)$, $Auth_s = h(t||sk||N)$.

Step 6. $S \rightarrow U$: $\{c_sG, Auth_s, t\}$.

Step 7. On receiving the message $\{C_sG, Auth_s, t\}$, U computes $V_s^* = c_u(c_sG)$,

$$sk^* = h(N||W_x||G||V_s^*||ID||t),$$

$$Auth_s^* = h(t||sk^*||N),$$

and checks whether $Auth_s^* \stackrel{?}{=} Auth_s$ If these are not equal, the session is terminated. Otherwise, S is authenticated by U and U accepts the session key sk^*. Afterwards, U computes $Auth_u = h(t+1||sk^*||N||V_s^*||ID)$, and sends $\{Auth_u\}$ to S.

Step 8. $U \rightarrow S$: $\{Auth_u\}$.

Step 9. After receiving the challenge message $\{Auth_u\}$, S computes $Auth_u^* = h(t+1||sk||N||V_s||ID)$ and checks whether $Auth_u^* \stackrel{?}{=} Auth_u$. If it is found valid, then U is authenticated.

Step 10. Finally, both the patient U and the server S agree on a common session key $sk = sk^*$.

5.4 Password update phase

This phase is incorporated to facilitate the user to change her/his password at will for which U and SC can execute the following steps:

Step 1. Firstly, U inserts the smart card into the card reader. U then inputs ID', PW' and a new password PW^{new}.

Step 2. The smart card SC calculates $VPW' = h(PW||a_u||ID)$, and then computes $A_u' = h((h(ID_i) \oplus VPW) \bmod n_0)$. Subsequently, SC verifies whether $A_u' = A_u$. If these are not equal, SC rejects U to change the password.

Step 3. Otherwise, SC generates a random number a_u^{new} and calculates $VPW^{new} = h(PW^{new}||a_u^{new}||ID), r_u^{new} = VPW \oplus VPW^{new} \oplus r_u, A_u^{new} = h((h(ID) \oplus VPW^{new} \bmod n_0)$.

Finally, SC stores a_u^{new}, r_u^{new}, A_u^{new} in place of a_u, r_u, A_u in smart card, respectively.

6 Security analysis of the enhanced scheme

In this part, we prove that the proposed scheme is secure against the attacks found overlooked by Kumari et al. Besides, we show that the proposed scheme also takes care common security features. To facilitate the discussion, we also adopt the attack model proposed by Kumari et al. and the adversary model, that is, an adversary $\mathcal{A}$ can completely monitor the open communication channel, therefore, is able to insert, delete or modify any messages among correspondents. Moreover, $\mathcal{A}$ has the ability to obtain all useful information of the smart card by the side-channel attack [41]. When it comes to key-compromise impersonation attack and perfect forward secrecy, the long-term private key k_s is revealed to $\mathcal{A}$.

6.1 User anonymity and user un-traceability

In this enhanced scheme, on one hand, there is no identity notations transmitted in the open channel or stored in smart card. On the other hand, suppose that the adversary $\mathcal{A}$ captures the messages $\{V, f_u, z_u\}$, $\{c_s G, Auth_s, t\}$ and $\{Auth_u\}$ from the public channel. But in order to obtain the user U's identity ID, $\mathcal{A}$ needs to know W_x, which is not available since W_x is computed using the random number c_u. Moreover, $\mathcal{A}$ cannot guess the correct identity, since, $\{N, VPW\}$ are also not available. Further, even if $\mathcal{A}$ obtains the smart card of U and extracts the information in SC, $\mathcal{A}$ cannot recover the identity of U since ID is protected by one-way hash function and modulo operator. In process of login and authentication, $\mathcal{A}$ has no ability to trace the user's identity, since, every transmitted message is different and does not reveal any location information about user. Therefore, the user anonymity and user un-traceability are ensured by the proposed scheme.

6.2 Privileged insider attack

In the registration phase, user U only submits ID to the server S. S subsequently sets an initial password PW_0 for U. After receiving the smart card and PW_0, U immediately changes the password that U knows only. Therefore, no privileged insider can access and compute user's password, that is, the proposed scheme resists privileged insider attack.

6.3 Pre-verification in the smart card

In the login phase of Kumari et al.'s scheme, the smart card is inability to provide any verification for the identity and password of any user increases the burden on the server. While in our login phase, the smart card checks whether $A'_u \stackrel{?}{=} A_u$ after inputting ID, PW. If it is found valid, SC sends the request message to S. Otherwise, it defers the session until the correct password and identity are entered. This implies that our method saves the computational and communication costs when there exists incorrect input or an illegal user. Consequently, the pre-verification is successfully provided by the proposed scheme.

6.4 Key-compromise impersonation attack

In our scheme, although the secret key k of the server S is compromised by the adversary $\mathcal{A}$, $\mathcal{A}$ cannot impersonate the legal user U to cheat S. Because, the adversary $\mathcal{A}$ cannot know the random number b of S or the correct $\{ID, PW\}$, therefore, he is unable to compute the correct value of N though the information in smart card is extracted. Thus, $\mathcal{A}$ cannot calculate the correct request message $\{V, f_u, z_u\}$ and cannot be authenticated by S. Consequently, our scheme is able to resist the key-compromise impersonation attack.

6.5 Server impersonation attack

Because, k is a long-term private key and b is also a random secret value of server S, therefore, the adversary $\mathcal{A}$ cannot recover $W^* = kV$, $ID = f_u \oplus W^*$, $N = h(k||ID||b)$ and is not able to forge $sk = h(N||W_x^*||G||V_s||ID||t)$, $Auth_s = h(t||sk||N)$. Thus, $\mathcal{A}$ is unable to impersonate the server S to the user U.

6.6 Off/On-line password guessing attack

In the proposed scheme, the adversary $\mathcal{A}$ cannot guess the correct identity and password of U even if it extracts the information $\{r_u, A_u, G, n_o\}$ in SC. If $\mathcal{A}$ guesses a pair of ID and PW, it shows that the equation $A'_u \stackrel{?}{=} A_u$ must be satisfied. But according to "fuzzy-verifier" [40], $\mathcal{A}$

still cannot be sure if the ID' and PW' are the correct ID and PW, respectively. $\mathcal{A}$ only guesses the correct value by launching the on-line guessing to server S. But the number space of the ID' and PW' is large enough to be immune to the on-line guessing attack, therefore, the smart card SC remains suspended until U re-registers once the wrong login times exceeds the the fixed threshold. Therefore, the proposed scheme can withstand the off/on-line password guessing attack.

6.7 Replay attack

Suppose that $\mathcal{A}$ has captured all the communication messages $\{\{V, f_u, z_u\}, \{c_sG, Auth_s, t\}, \{M_i\}\}$ through open channel and tried to replay them to U or S. However, the proposed scheme takes advantage of some random numbers $\{c_u, c_s, t\}$ that remain different in every session to prevent replay attack. In the process of communication, after receiving the request/challenge message, both the user and the server can immediately verify the validity of the random number every-time if $\mathcal{A}$ replays the communication message. Therefore, the replay attack is prevented by the proposed scheme.

6.8 Session-specific temporary information attack

In the proposed scheme, if the random numbers c_u, c_s, t are compromised, then the adversary $\mathcal{A}$ can calculate $W = c_uG$ and further computes W_x. $\mathcal{A}$ captures the transmitted messages $\{V, f_u, z_u, c_sG, t\}$. Afterwards, $\mathcal{A}$ computes $ID = f_u \oplus W_x$, $V_s = c_sV$. But in order to obtain the session key $sk = h(N||W_x||G||V_s||ID||t)$, $\mathcal{A}$ must have ability to know the value of N that is not available, since, N is protected by the private k and the random number b of server S. Implies, $\mathcal{A}$ still can not calculate the session key sk, although, the random numbers $\{c_u, c_s, t\}$ are compromised. Therefore, the proposed protocol is secured against the session-specific temporary information attack.

6.9 Man-in-the-middle attack

Suppose that an adversary $\mathcal{A}$ intercepts the login request message $\{V, f_u, z_u\}$ and the information stored in smart card. In order to launch the man-in-middle attack, $\mathcal{A}$ needs to compute $\{V^*, f_u^*, z_u^*\}$ for sending to server S. Although, $\mathcal{A}$ chooses a random c_u^*, still $\mathcal{A}$ cannot know the value of N and the real identity ID, therefore, he can not compute f_u^* and z_u^*. On the other hand, even if he intercepts the challenge message $\{c_sG, Auth_s, t\}$, $\mathcal{A}$ still can not compute the forged message $\{c_s^*G, Auth_s^*, t^*\}$ as he does not know the values of $\{N, ID\}$. Without knowing the server's private key k and random number b, computation of N is computationally infeasible for the adversary $\mathcal{A}$. Thus, the attacker $\mathcal{A}$ does not have any ability to modify the login request message or the challenge message. As a result, our scheme also resists the man-in-the-middle attack.

6.10 Mutual authentication

In the proposed scheme, S firstly checks the validity of ID. Afterwards, S authenticates U by verifying whether $z_u^* = z_u$ and checking whether $Auth_u^* = Auth_u$, respectively. On the other hand, U authenticates S by testing whether $Auth_s^* = Auth_s$. Consequently, our proposed scheme provides mutual authentication.

6.11 Perfect forward secrecy

When it comes to the forward secrecy, we assume that the private key k of S is compromised and that the adversary $\mathcal{A}$ obtains the sensitive datum $\{r_u, A_u, G\}$ stored in smart card and the

transmitted message $\{V, f_u, z_u\}$. $\mathcal{A}$ can compute $W = kV$ and calculates $ID = f_u \oplus W_x$. But in order to calculate the previous session key $sk = h(N||W_x||G||V_s||ID||t)$, $\mathcal{A}$ must know c_u or c_s. However, it is impossible for $\mathcal{A}$ to obtain c_u from V or c_s from c_sG and calculate c_uc_sG due to the intractability of *ECDLP* and *ECCDHP*. Thus, even by obtaining the private key k of server S and the smart card, the adversary $\mathcal{A}$ is still unable to calculate the session key sk. As a result, the proposed scheme provides perfect forward secrecy.

6.12 Efficient password changing

In the proposed protocol, if the user U wants change her/his password, U only needs to interact with the smart card SC to perform some operators. In this phase, the server S is not involved in the process of password changing. Therefore, our proposed protocol is efficient in password changing phase.

7 Formal security validation using AVISPA tool

AVISPA (Automated Validation of Internet Security Protocols and Applications) is a push-button software tool for the automated validation of Internet security-sensitive protocols and applications [44]. The AVISPA supports High Level Protocol Specification Language called as HLPSL and is usually used to provide the formal security verification of the simulated protocol. The simulation results in AVISPA can point out that whether proposed protocol is secure against the active and passive attacks. The architecture of the AVISPA tool is depicted in Fig 3 and its detailed introduction can be found in [44].

Accordingly, in order to test the security of the proposed protocol, we also use the AVISPA software tool to simulate it. Firstly, we translate the proposed protocol in HLPSL. The specifications for the roles for the user U_i, the server S, the session, goal and environment in HLPSL are depicted in Figs 4, 5 and 6, respectively. Since only OFMC and CL-AtSe backends support the Diffie-Hellman and the bitwise exclusive-OR (XOR) operation, after execution through the OFMC and CL-AtSe backends, the simulation results ensure that our proposed protocol is

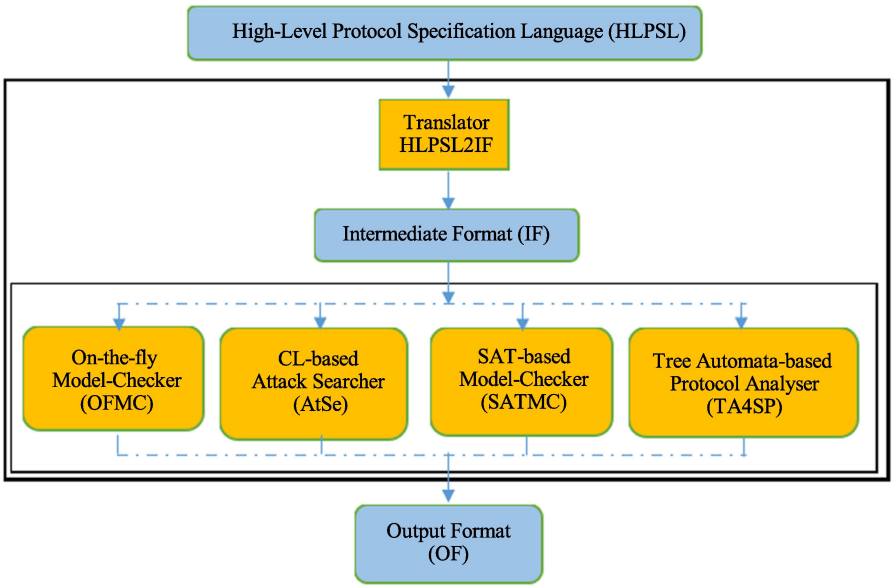

Fig 3. Architecture of the AVISPA tool.

https://doi.org/10.1371/journal.pone.0194072.g003

```
role alice(Ui,S:agent,SKas:symmetric_key,H,Mul:hash_func,
Snd,Rcv:channel(dy))
played_by Ui
def=
local State:nat,
ID,Pw,G,VPw,W,Cu,Cs,B,N,P,T,Vs:text,
Ru,A,Au,V,Fu,Zu,Su,Auths:message,
Inc:hash_func
const alice_server,subs1,subs2,subs3,subs4,subs5,subs6,
subs7:protocol_id
init State:=0
transition
1.State=0/\Rcv(start)=|>
State':=1
/\ID':=new()
/\Snd({ID'}_SKas)
/\secret({ID},subs1,{Ui,S})
2.State=1/\Rcv({Ru'.P'.Au'.G'.A'}_SKas)=|>
State':=2
/\Cu':=new()
/\VPw':=H(Pw.A.ID)
/\N':=xor(Ru,VPw')
/\V':=Mul(Cu'.P)
/\W':=Mul(Cu'.G)
/\Fu':=xor(ID,W')
/\Zu':=H(ID.W'.Fu'.N)
/\Snd(V'.Fu'.Zu')
/\secret({Pw},subs2,{Ui})
/\secret({Cu},subs3,{Ui})
/\witness(Ui,S,alice_server_cu,Cu')
3.State=2/\Rcv(Su'.Auths'.T')=|>
State':=3/\request(Ui,S,server_alice_cs,Cs)
end role
```

Fig 4. Role specification of U_i in HLPSL.

https://doi.org/10.1371/journal.pone.0194072.g004

SAFE against the active and passive attacks under the Dolev-Yao model [45]. The simulation results of the proposed scheme are provided in Figs 7 and 8.

8 Comparative analysis of performance

This section analyzes the performance of our proposed scheme by comparing it with Zhang et al.'s [27], Jiang et al.'s [34], Irshad et al.'s [31], Chaudhry et al.'s [38], Tu et al.'s [36],

```
role server(S,Ui:agent,SKas:symmetric_key,H,Mul:hash_func,
Snd,Rcv:channel(dy))
played_by S
def=
local State:nat,
ID,Pw,G,VPw,B,N,P,K,Cs,T,Cu,Vs,W:text,
Ru,A,Au,V,Fu,Zu,Su,SK,Auths:message,
Inc:hash_func
const alice_server,server_alice,subs1,subs2,
subs3,subs4,subs5,subs6,subs7:protocol_id
init State:=0
transition
1.State=0/\Rcv(ID')=|>
State':=1
/\A':=new()
/\N':=H(K.ID.B)
/\VPw':=H(Pw.A'.ID)
/\Au':=H(xor(H(ID),VPw))
/\Ru':=xor(N,VPw')
/\secret({B},subs4,{S})
/\secret({K},subs5,{S})
/\Snd({A'.Au'.Ru'}_SKas)
2.State=1/\Rcv(V'.Fu'.Zu')=|>
State':=2
/\Cs':=new()
/\T':=new()
/\Vs':=Mul(Cs'.V')
/\Su':=Mul(Cs'.G)
/\SK':=H(N.W.Fu'.Vs'.ID.T')
/\Auths':=H(T'.SK'.N)
/\witness(S,Ui,server_alice_cs,Cs')
/\secret({Cs'},subs6,{Ui,S})
/\secret({SK'},subs7,{Ui,S})
/\Snd(Su'.Auths'.T')
end role
```

Fig 5. Role specification of *S* in HLPSL.

https://doi.org/10.1371/journal.pone.0194072.g005

Zhang et al.'s [26], Farash's [37] and Kumari et al.'s [39] schemes. Generally, in order to compare the computational complexity, we neglect the lightweight operations like exclusive-OR operation and string concatenation. We list some operations's descriptions used in our paper as below:

```
role session(S,Ui:agent,SKas:symmetric_key,H,Mul:hash_func)
def=
local SI,SJ,RI,RJ:channel(dy)
composition
alice(Ui,S,SKas,H,Mul,SI,RI)
/\server(Ui,S,SKas,H,Mul,SJ,RJ)
end role

role environment()
def=
const ui,s:agent,
skas:symmetric_key,
h,mul:hash_func,
id,pw,g,vpw,b,n,ru,p,au,auths,t,a,v,fu,zu,su:text,
alice_server_cu,server_alice_cs,subs1,subs2,
subs3,subs4,subs5,subs6,subs7:protocol_id
intruder_knowledge={ui,s,h,mul,ru,au,a,p,g,v,fu,zu,su,auths,t}

composition

session(ui,s,skas,h,mul)
/\session(s,ui,skas,h,mul)
end role
goal
secrecy_of subs1
secrecy_of subs2
secrecy_of subs3
secrecy_of subs4
secrecy_of subs5
secrecy_of subs6
secrecy_of subs7
authentication_on alice_server_cu
authentication_on server_alice_cs
end goal
environment()
```

Fig 6. Role specification of the session, goal and environment in HLPSL.

https://doi.org/10.1371/journal.pone.0194072.g006

```
% OFMC
% Version of 2006/02/13
SUMMARY
    SAFE
DETAILS
    BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
    /home/span/span/testsuite/results/plos_scheme.if
GOAL
    as_specified
BACKEND
    OFMC
COMMENTS
STATISTICS
    parseTime: 0.00s
    searchTime: 0.04s
    visitedNodes: 16 nodes
    depth: 4 plies
```

Fig 7. The simulation result using the OFMC backend.

https://doi.org/10.1371/journal.pone.0194072.g007

- T_{pa}: the time for performing an elliptic curve point addition operation.
- T_{pm}: the time for performing a point multiplication operation.
- T_{me}: the time for performing a modular exponentiation operation.
- T_{sed}: the time for performing symmetric cryptography.
- T_h: the time for performing a hash operation.

According to the experimental results performed as [46], T_h, T_{pm}, T_{pa} and T_{sed} take approximately 0.0023ms, 2.226ms, 0.0288ms and 0.0046ms, respectively. The above timings are obtained on a personal computer which has a Intel Pentium Dual CPU E2200 2.20GHz processor, 2048 MB of RAM and the Ubuntu 12.04.1 LTS 32bit operating system [46].

In this section, the comparative analysis is twofold as follows:

- Comparison of computational complexity (Table 2)
- Comparison of security features (Table 3)

According to Table 2, the total computational costs of our proposed scheme in login and authentication phase is $13T_h + 6T_{pm} \approx 13.3859ms$. The results provide that the proposed scheme outperforms [26, 27, 31, 34, 36–38]. In comparison to Kumari et al. [39], our scheme

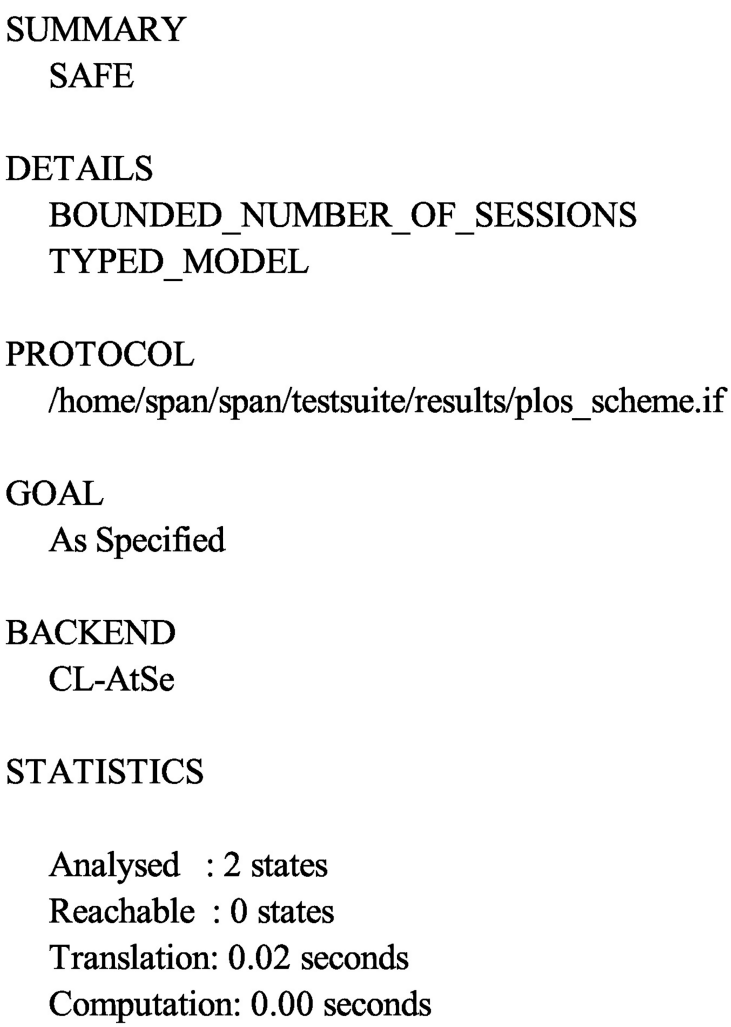

Fig 8. The simulation result using the CL-AtSe backend.

https://doi.org/10.1371/journal.pone.0194072.g008

has slightly more computational costs. However, it is an acceptable range under the trade-off of security and usability.

From Table 3, we observe that these proposals [26, 27, 31, 34, 36–39] lack some security ingredients and have more security problems than the proposed scheme. In Kumari et al.'s

Table 2. Comparison of computational complexity in login-authentication phase.

Scheme	User computations	Server computations	Total of computation overhead
Zhang et al. [27]	$4T_h + 3T_{pm}$	$4T_h + 4T_{pm}$	$8T_h + 7T_{pm} \approx 15.6004ms$
Jiang et al. [34]	$5T_h + 4T_{pm} + 1T_{pa}$	$4T_h + 4T_{pm} + 1T_{pa}$	$9T_h + 8T_{pm} + 2T_{pa} \approx 17.8863ms$
Irshad et al. [31]	$6T_h + 4T_{pm}$	$6T_h + 3T_{pm}$	$12T_h + 7T_{pm} \approx 15.6096ms$
Chaudhry et al. [38]	$5T_h + 3T_{pm} + 1T_{pa}$	$5T_h + 3T_{pm} + 2T_{sed}$	$10T_h + 6T_{pm} + 1T_{pa} + 2T_{sed} \approx 13.417ms$
Tu et al. [36]	$4T_h + 3T_{pm} + 1T_{pa}$	$4T_h + 3T_{pm}$	$8T_h + 6T_{pm} + 1T_{pa} \approx 13.4032ms$
Zhang et al. [26]	$6T_h + 1T_{pa} + 5T_{pm}$	$4T_h + 2T_{pa} + 4T_{pm}$	$10T_h + 3T_{pa} + 9T_{pm} \approx 20.1434ms$
Farash [37]	$5T_h + 3T_{pm} + 1T_{pa}$	$4T_h + 3T_{pm}$	$9T_h + 6T_{pm} + 1T_{pa} \approx 13.4055ms$
Kumari et al. [39]	$5T_h + 1T_{pa} + 3T_{pm}$	$5T_h + 2T_{me}$	$10T_h + 1T_{pa} + 5T_{pm} \approx 11.1818ms$
Ours	$7T_h + 3T_{pm}$	$5T_h + 3T_{pm}$	$13T_h + 6T_{pm} \approx 13.3859ms$

https://doi.org/10.1371/journal.pone.0194072.t002

Table 3. Comparison of security features.

Security features	Zhang et al. [27]	Jiang et al. [34]	Irshad et al. [31]	Chaudhry et al. [38]	Tu et al. [36]	Zhang et al. [26]	Farash [37]	Kumari et al. [39]	Ours
F_1	No	No	Yes	No	No	No	No	Yes	Yes
F_2	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
F_3	No	No	No	No	No	No	No	No	Yes
F_4	□	□	□	□	□	□	□	No	Yes
F_5	Yes	Yes	No	Yes	No	□	Yes	Yes	Yes
F_6	No	No	Yes	Yes	No	Yes	No	Yes	Yes
F_7	Yes	No	No	Yes	No	Yes	No	Yes	Yes
F_8	Yes	Yes	No	□	No	Yes	No	Yes	Yes
F_9	Yes	Yes	Yes	Yes	No	Yes	Yes	Yes	Yes
F_{10}	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
F_{11}	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
F_{12}	No	No	No	No	No	No	No	No	Yes

F_1: Provides user anonymity and user un-traceability; F_2: Resists privileged insider attack; F_3: Provides pre-verification in the smart card; F_4: Resists key-compromise impersonation attack; F_5: Resists server impersonation attack; F_6: Resists off/On-line password guessing attack; F_7: Resists replay attack; F_8: Resists session-specific temporary information attack; F_9: Resists man-in-the-middle attack; F_{10}: Provides mutual authentication; F_{11}: Provides perfect forward secrecy; F_{12}: Provides efficient password changing. "Yes" means the property is satisfied; "No" means the property is not satisfied and "□" means the property is not discussed.

https://doi.org/10.1371/journal.pone.0194072.t003

scheme [39], the authors declared that their protocol is secured against user impersonation attack, password guessing attack and session-specific temporary information attack applicable on Farash's scheme [37]. On one hand, it is well known that perfect forward secrecy is a key security feature of key agreement scheme. Perfect forward secrecy ensures the security of the session key. On the other hand, key-compromise impersonation attack is also a fatal attack on SIP. If we have measures to resist this attack, why not to design such scheme? However, according to our observation, we find that Kumari et al.'s scheme [39] cannot provide the perfect forward secrecy and is vulnerable to key-compromise impersonation attack. Meanwhile, key-compromise impersonation attack is not considered by all schemes of Table 3, expect our scheme. Fortunately, we have taken effective measures to tackle key-compromise impersonation attack in our scheme, that is, the server stores random secret values b in its database. Besides, the proposed protocol utilizes the technique of "fuzzy-verifiers" [40] to resist off-line identity guessing attack and provides more security features, including pre-verification in the smart card and efficient password changing. Therefore, the proposed scheme not only address the security problems of Kumari et al.'s scheme [39] but also retains all their merits as depicted in Table 3. Although, our scheme employs a slightly complex elliptic curve point multiplication operation, but, as a trade-off, it can resist all known-attacks that are very important ingredients of the security of mutual authentication.

9 Conclusion

In this paper, we have provided a security analysis of Kumari et al.'s scheme [39] to prove that their scheme [39] is vulnerable to key-compromise impersonation attack and does not provide perfect forward secrecy, pre-verification in the smart card and efficient password changing. In order to remedy these limitations in Kumari et al.'s [39] scheme, we propose an enhanced authentication scheme with refined security. The proposed scheme inherits the merits of the Kumari et al.'s [39] scheme, resists the aforementioned attacks and provides more comprehensive security features with a slightly high computational cost than [39]. Additionally, the

simulating results of the proposed protocol using AVISPA software infer that this proposed protocol is secure against active and passive attacks. Finally, in comparison with the previously proposed schemes, we conclude that the proposed protocol is more secure and effective to be implemented in real-life scenarios. Actually, many of the existing protocols can not be unconditional security. In order to enhance the security of the authentication protocol, a number of three-factor authentication protocols have been designed. Therefore, in our future work, we will design a more secure three-factor mutual authentication protocol based on smart cards to be implemented in many practical scenarios, such as: Internet of Things, Wireless Sensor Networks, Medical Care Systems, Vehicular Ad Hoc Networks, etc.

Supporting information

S1 Fig. Registration and authentication phase of our scheme.
(EPS)

S2 Fig. Architecture of the AVISPA tool.
(EPS)

S3 Fig. Role specification of U_i in HLPSL.
(EPS)

S4 Fig. Role specification of S in HLPSL.
(EPS)

S5 Fig. Role specification of the session, goal and environment in HLPSL.
(EPS)

S6 Fig. The simulation result using the OFMC backend.
(EPS)

S7 Fig. The simulation result using the CL-AtSe backend.
(EPS)

Acknowledgments

The authors thank the anonymous reviewers and the Editor for the constructive comments and generous feedback. The authors are also grateful to Dr. Shehzad Ashraf Chaudhry for the valuable suggestions on this paper. This work was supported by the National Key Research and Development Program of China (No. 2017YFB0801900 and No. 2017YFB0801901).

Author Contributions

Writing – original draft: Shuming Qiu, Guoai Xu, Haseeb Ahmad, Yanhui Guo.

References

1. Shen C, Nahum E, Schulzrinne H, Wright CP. The impact of TLS on SIP server performance: measurement and modeling. IEEE/ACM Transactions on Networking, 20(4):1217–1230 (2012). https://doi.org/10.1109/TNET.2011.2180922
2. Session Initiation Protocol. https://en.wikipedia.org/wiki/Session_Initiation_Protocol (accessed on December 2017).
3. Franks J, Hallam-Baker P, Hostetler J, Lawrence S, Leach P, Luotonen A. HTTP Authentication: Basic and digest access authentication. IETF RFC.,1999; 2617.
4. Yang C, Wang R, Liu W. Secure authentication scheme for session initiation protocol. Comput Secur. 2005; 24:381–386. https://doi.org/10.1016/j.cose.2004.10.007

5. Huang HF, Wei WC, Brown GE. A new efficient authentication scheme for session initiation protocol. In: 9th Joint Conference on Information Sciences., 2006.
6. Denning D, Sacco G. Timestamps in key distribution systems. Commun ACM. 1981; 24(8): 533–536. https://doi.org/10.1145/358722.358740
7. Durlanik A, Sogukpinar I. SIP authentication scheme using ECDH. World Enformatika Soc Trans Eng Comput Technol. 2005; 8:350–353.
8. Arkko J, Torvinen V, Camarillo G, Niemi A, Haukka T. Security mechanism agreement for SIP sessions. IETF Internet Draft.;2002 Jun.
9. Arshad R, Ikram N. Elliptic curve cryptography based mutual authentication scheme for session initiation protocol. Multimed Tools Appl. 2013; 66(2):165–178. https://doi.org/10.1007/s11042-011-0787-0
10. Challa S, Das AK, Kumari S, Odelu V, Wu F, Li X. Provably secure three-factor authentication and key agreement scheme for session initiation protocol. Security and Communication Networks. 2016; 9(18): 5412–5431. https://doi.org/10.1002/sec.1707
11. Chaudhry SA, Khan I, Irshad A, Ashraf MU, Khan MK, Ahmad HF. A provably secure anonymous authentication scheme for session initiation protocol. Secur Commun Netw.; 2016. https://doi.org/10.1002/sec.1672.
12. Chaudhry SA, Naqvi H, Shon T, Sher M, Farash MS. Cryptanalysis and Improvement of an Improved Two Factor Authentication Protocol for Telecare Medical Information Systems. J. Medical Systems. 2015; 39(6): 1–11. https://doi.org/10.1007/s10916-015-0244-0
13. Chen TH, Yeh HL, Liu PC, Hsiang HC, Shih WK. A secured authentication protocol for SIP using elliptic curves cryptography. FGIT-FGCN. 2010; 119(1): 46–55. https://doi.org/10.1007/978-3-642-17587-9_6
14. Farash MS, Attari MA. An Enhanced authenticated key agreement for session initiation protocol. Inf Technol Control. 2013; 42(4):333–342. http://dx.doi.org/10.5755/j01.itc.42.4.2496
15. Farash MS, Chaudhry SA, Heydari M, Sadough SMS, Kumari S, Khan MK. A lightweight anonymous authentication scheme for consumer roaming in ubiquitous networks with provable security. Int. J. Communication Systems. 2017; 30(4). https://doi.org/10.1002/dac.3019
16. He DB, Chen J, Chen Y. A secure mutual authentication scheme for session initiation protocol using elliptic curve cryptography. Secur Commun Netw. 2012; 5(12):1423–1429. https://doi.org/10.1002/sec.506
17. Khan MK. Fingerprint Biometric-based Self-Authentication and Deniable Authentication Schemes for the Electronic World. Iete Technical Review. 2009; 26(3): 191–195.
18. Kumari S, Karuppiah M, Das AK, Li X, Wu F, Gupta V. Design of a secure anonymity-preserving authentication scheme for session initiation protocol using elliptic curve cryptography. J Ambient Intell Human Comput. 2017. https://doi.org/10.1007/s12652-017-0460-1
19. Kumari S, Khan MK. More secure smart card-based remote user password authentication scheme with user anonymity. Security and Communication Networks. 2014; 7(11): 2039–2053. https://doi.org/10.1002/sec.916
20. Liu FW, Koenig H. Cryptanalysis of a SIP authentication scheme. In: 12th IFIP TC6/TC11 International Conference, CMS, Lecture Notes in Computer Science. 2011; 7025: 134–143. https://doi.org/10.1007/978-3-642-24712-5_11
21. Qiu SM, Xu GA, Ahmad H, Wang LC. A Robust Mutual Authentication Scheme Based on Elliptic Curve Cryptography for Telecare Medical Information Systems. IEEE Access. 2017. https://doi.org/10.1109/ACCESS.2017.2780124
22. Sutrala AK, Das AK, Odelu V, Wazid M, Kumari S. Secure anonymity-preserving password-based user authentication and session key agreement protocol for telecare medicine information systems. Computer Methods and Programs in Biomedicine. 2016; 135: 167–185. https://doi.org/10.1016/j.cmpb.2016.07.028 PMID: 27586489
23. Tang H, Liu X. Cryptanalysis of Arshad et al'.s ECC-based mutual authentication scheme for session initiation protocol. Multimed Tools Appl. 2013; 65(3): 321–333. https://doi.org/10.1007/s11042-012-1001-8
24. Tsai JL. Efficient nonce-based authentication scheme for session initiation protocol. Int J Netw Secur. 2009; 8(3):312–316.
25. Wang XM, Guo W, Zhang WF, Khan MK, Alghathbar K. Cryptanalysis and improvement on a parallel keyed hash function based on chaotic neural network. Telecommunication Systems. 2013; 52(2): 515–524. http://dx.doi.org/10.1007/s11235-011-9457-9
26. Zhang L, Tang S, Cai Z. Efficient and flexible password authenticated key agreement for voice over internet protocol session initiation protocol using smart card. International Journal of Communication Systems. 2014; 27(11):2691–2702. http://dx.doi.org/10.1002/dac.2499

27. Zhang L, Tang S, Cai Z. Cryptanalysis and improvement of password-authenticated key agreement for session initiation protocol using smart cards. Security and Communication Networks. 2014; 7 (12):2405–2411. https://doi.org/10.1002/sec.951

28. Farash MS. An improved password-based authentication scheme for session initiation protocol using smart cards without verification table. Int J Commun Syst. 2014. https://doi.org/10.1002/dac.2879

29. Lu YR, Li LX, Peng HP, Yang YX. An anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography. Multimed Tools Appl. 2015; 76: 1801. https://doi.org/10.1007/s11042-015-3166-4

30. Kumari S. Design flaws of "an anonymous two-factor authenticated key agreement scheme for session initiation protocol using elliptic curve cryptography". Multimed Tools Appl. 2017; 76: 13581. https://doi.org/10.1007/s11042-016-3771-x

31. Irshad A, Sher M, Rehman E, Ch SA, Hassan MU, Ghani A. A single round-trip sip authentication scheme for voice over internet protocol using smart card. Multimedia Tools and Applications. 2015; 74 (11):1–18. https://doi.org/10.1007/s11042-013-1807-z

32. Arshad H, Nikooghadam M. An efficient and secure authentication and key agreement scheme for session initiation protocol using ECC. Multimedia Tools Appl. 2016; 75(1): 181–197. https://doi.org/10.1007/s11042-014-2282-x

33. Lu YR, Li LX, Yang YX. Robust and efficient authentication scheme for session initiation protocol. Math Probl Eng.; 2015. https://doi.org/10.1155/2015/894549. Article ID 894549, 9.

34. Jiang Q, Ma J, Tian Y. Cryptanalysis of smart-card-based password authenticated key agreement protocol for session initiation protocol of zhang et al. International Journal of Communication Systems. 2014; 28(7). https://doi.org/10.1002/dac.2767

35. Azrour M, Farhaoui Y, Ouanan M. A New Secure Authentication and Key Exchange Protocol for Session Initiation Protocol Using Smart Card. International Journal of Network Security. 2017; 19(6): 870–879. https://doi.org/10.6633/IJNS.201711.19(6).02

36. Tu H, Kumar N, Chilamkurti N, Rho S. An improved authentication protocol for session initiation protocol using smart card. Peer-to-Peer Network Applied. 2015; 8(5): 903–910. https://doi.org/10.1007/s12083-014-0248-4

37. Farash MS. Security analysis and enhancements of an improved authentication for session initiation protocol with provable security. Peer-to-Peer Networking and Applications. 2014; 1–10. https://doi.org/10.1007/s12083-014-0315-x.

38. Chaudhry SA, Naqvi H, Sher M, Farash MS, Hassan MU. An improved and provably secure privacy preserving authentication protocol for sip. Peer-to-Peer Networking and Applications. 2017; 10(1): 1–15. https://doi.org/10.1007/s12083-015-0400-9

39. Kumari S, Chaudhry SA, Wu F, Li X, Farash MS, Khan MK. An improved smart card based authentication scheme for session initiation protocol. Peer-to-Peer Networking and Applications., 2015. https://doi.org/10.1007/s12083-015-0409-0.

40. Wang D, Wang P. Two birds with one stone: two-factor authentication with security beyond conventional bound. IEEE Trans Depend Secur Comput. 2016. https://doi.org/10.1109/TDSC.2016.2605087

41. Kocher P, Jaffe J, Jun B. Differential power analysis. Advances in Cryptology. 1999; 1666:388–397. https://doi.org/10.1007/3-540-48405-1_25

42. Messerges TS, Dabbish EA, Sloan RH. Examining smart-card security under the threat of power analysis attacks. IEEE Trans Comput. 2002; 51(5): 541–552. https://doi.org/10.1109/TC.2002.1004593

43. Wang D, He DB, Wang P, Chu C. Anonymous two-factor authentication in distributed systems: certain goals are beyond attainment. IEEE Trans Depend Secur Comput. 2015; 12(4):428–442. https://doi.org/10.1109/TDSC.2014.2355850

44. AVISPA. Automated validation of internet security protocols and applications. http://www.avispa-project.org/ (accessed on December 2017).

45. Dolev D, Yao A. On the security of public key protocols. IEEE Trans Inf Theory. 1083; 29(2):198–208. https://doi.org/10.1109/TIT.1983.1056650

46. Kilinc H, Yanik T. A survey of SIP authentication and key agreement schemes. IEEE Communications Surveys and Tutorials. 2014; 16(2): 1005–1023. https://doi.org/10.1109/SURV.2013.091513.00050