PRIVACY PRESERVING USER AUTHENTICATION SCHEME BASED ON SMART CARD

Beaton Kapito[1], Patrick Ali[1], Levis Eneya[1] and Hyunsung Kim[1,2]

[1]Mathematical Sciences Department, University of Malawi, Chancellor College, Zomba, Malawi

[2]Department of Cyber Security, Kyungil University, Kyungbuk, Korea

ABSTRACT

One of the most commonly used user authentication mechanisms is two factor authentication based on smart card and password. The core feature of the scheme is to enforce that the user must have the smart card and know the password in order to gain access to server. Recently, Liu et al. proposed a smart card based password authentication scheme and argued that it is secure against insider attack, replay attack and man in the middle attack and provides perfect forward secrecy. In this paper, we show security weaknesses in Liu et al.'s scheme focused on off-line password guessing attack and masquerading attack and it does not provide perfect forward secrecy and anonymity. Accordingly, we propose a privacy preserving user authentication scheme based on smart card, denoted as PUAS, to remedy these security weaknesses and to provide anonymity and perfect forward secrecy. PUAS is more secure with a bit of computational overhead to support several positive properties in security and privacy.

KEYWORDS

User Authentication, Password Authentication, Smart Card, Bilinear Pairing, Privacy

1. INTRODUCTION

The rapid progress of networks facilitates more and more computers connecting together to exchange great information and share system resources. Password authentication with smart card is one of the most convenient and effective authentication mechanisms for remote systems to assure one communicating party of the legitimacy of the corresponding party by acquisition of corroborative evidence. This technique has been widely deployed for various kinds of authentication applications, such as remote login, online banking, e-commerce and e-health [1-3]. Since Lamport proposed the first remote authentication scheme based on the passwords, a series of authentication schemes have been proposed to improve system security and computation efficiency [4-8]. Lamport's scheme is based on a password table maintained by a server, which suffers not only from password attacks but also suffers from the cost of protecting and maintaining the password table [5]. To enhance the security of the password based authentication scheme, Chang and Wu introduced password and smart card based two factor user authentication scheme [6]. The main drawback of Chang and Wu's scheme is using static identity that publicly transmitted identity will reveal user privacy. To conquer the issue, Das et al. proposed an authentication scheme using dynamic identity [7]. However, Liao et al. showed that Das et al.'s scheme cannot resist user impersonation attack and also proposed an improved scheme with mutual authentication [8].

DOI:10.5121/ijcis.2018.8302

In 2009, Xu et al. proposed a novel user authentication and claimed that their scheme is secure against various attacks [9]. However, Song and Sood et al. found that Xu et al.'s scheme has some weaknesses and proposed improved schemes [5, 10]. Subsequently, Chen et al. pointed out that there are vulnerabilities on Song and Sood et al.'s schemes [11]. Then, Chen et al. presented an enhanced version to solve the weaknesses. Recently, Li et al. claimed that Chen et al.'s scheme is still insecure and proposed a modified smart card based remote user password authentication scheme [12]. Unfortunately, Liu et al. showed that there are weaknesses in Li et al.'s scheme, such as from a man-in-the-middle attack and an insider attack and proposed a remedy scheme [13].

Hence, the purpose of this paper is to provide cryptanalysis on Liu et al.'s scheme and proposes a new privacy preserving user authentication scheme based on smart card, denoted PUAS. First of all, we will show Liu et al.'s scheme is weak against off-line password guessing attack and masquerading attack, and does not provide perfect forward secrecy and anonymity. To solve the weaknesses in Liu et al.'s scheme, PUAS adopts dynamic identity and bilinear pairing, which could provide privacy.

This paper is organized as follows. Section 2 reviews Liu et al.'s smart card based password authentication scheme. In Section 3, security weaknesses will be shown against Liu et al.'s authentication scheme. A new privacy preserving user authentication scheme is proposed in Section 4 with the security and performance analyses at Section 5. Section 6 concludes this paper.

2. REVIEW OF LIU ET AL.'S AUTHENTICATION SCHEME

Liu et al. proposed a smart card based password authentication scheme, which is consisted of four phases: registration phase, login phase, authentication phaseand password change phase [13]. Liu et al. argued that their scheme can achieve mutual authentication and users can freely choose and change their passwords. This section reviews Liu et al.'s scheme briefly. Table 1 shows definition of notations used in this paper.

Table 1. Notations.

Notation	Description
S	The server
U_i	The i^{th} user
SC	The smart card
x	The master secret key of S
ID_i	The identity of U_i
PW_i	The password of U_i
T_i	The timestamp i
sk	The shared session key
$h(.)$	A secure hash function
$E(.)$	A symmetric key encryption based on AES
$D(.)$	A symmetric key decryption based on AES
$\hat{e}(.)$	A bilinear map
$\oplus$	Exclusive-or operation
$\|\|$	Concatenation operation

2.1. Registration Phase

Before starting Liu et al.'s authentication scheme, the server S selects the master secret key x and a one-way hash function $h(\cdot)$. The registration phase is as follows:

Step 1. The user U_i selects his/her identity ID_i, password PW_i, and a random number r, and then computes $h(r||PW_i)$.U_i submits $\{ID_i,h(r||PW_i)\}$to S for registration over a secure channel.

Step 2. S computes $A_i=h(ID_i \oplus x)||h(x)$,$B_i=A_i \oplus h(r||PW_i)$ and $C_i=h(A_i||ID_i||h(r||PW_i))$.

Step 3. S stores the data $\{B_i, C_i, h(\cdot)\}$ on a new smart card (SC) and issues it to U_i over a securechannel.

Step 4. U_i stores the random number r into SC.

2.2. Login Phase

This phase is invoked whenever U_i wants to login to S. The steps of this phase are shown as follows:

Step 1. U_i inserts his/her SCinto a card reader and inputs ID_i and PW_i.

Step 2. SCfirst computes two parameters $A_i'=B_i \oplus h(r||PW_i)$ and $C_i'=h(A_i'||ID_i||h(r||PW_i))$.Then, SC examines whether C_i' is equal to C_i. If the equation holds, SCcontinues to perform Step 3; otherwise, SCterminates this session.

Step 3. SC randomly selects a number $\alpha$and computes $D_i=h(ID_i \oplus \alpha)$and $E_i=A_i' \oplus \alpha \oplus T_i$, where T_i is the current timestamp of U_i.

Step 4. SCsends the login request message $\{ID_i, D_i, E_i, T_i\}$ to S.

2.3. Authentication Phase

After completing this phase, U_i and S can mutually authenticate each other and establish a shared session key for the subsequent secret communication.

Step 1. S verifies whether ID_i is valid and $T_i' - T_i \leq \Delta T$,where T_i' is the time of receiving the login request message and ΔT is a valid time threshold. If both conditions are true, S continues to execute Step 2; otherwise, S rejects the login request.

Step 2. S computes $A_i=h(ID_i \oplus x)||h(x)$,$\alpha'=E_i \oplus A_i \oplus T_i$and $D_i'=h(ID_i \oplus \alpha')$.Then, S compares whether D_i'equals D_i. If theyare equal, S confirms that U_i is valid and the login request is accepted; otherwise, the login request is rejected.

Step 3. S randomly selects a number β and computes $F_i=h(ID_i \oplus \beta)$ and $G_i=A_i \oplus \beta \oplus T_s$.

Step 4. S sends the mutual authentication message $\{F_i, G_i, T_s\}$ to U_i.

Step 5. Upon receiving the message $\{F_i, G_i, T_s\}$, SC checks the validity of T_s. If $T_s' - T_s \leq \Delta T$, where T_s' is time of receiving the mutual authentication message, SCcontinues to perform Step 6; otherwise, SC terminates this connection.

Step 6. SCcomputes $\beta'=G_i \oplus A_i \oplus T_sandF_i'=h(ID_i \oplus \beta')$and then checks whether F_i' equals F_i. If they are equal, the validity of S is authenticated; otherwise, the session is terminated.

Step 7. U_i and S construct a shared session key $sk=h(\alpha||\beta'||h(A_i' \oplus ID_i))=h(\alpha'||\beta||h(A_i \oplus ID_i))$.

2.4. Password Change Phase

Liu et al.'s protocol allows users to freely update their passwords. The password change phase works as follows:

Step 1. U_i inserts his/her SCinto a card reader,enters his/her old identity ID_i and password PW_i, andrequests to change the password.

Step 2. SCcomputes $A_i^*=B_i \oplus h(r||PW_i)$ and $C_i^*=h(A_i^*||ID_i||h(r||PW_i))$, and then checks whether C_i^* equals C_i that is stored in SC. If the equation holds, U_i submits the new password PW_i^{new}.Otherwise, SCrejects thepassword change request.

Step 3.SCcomputes $B_i^{new}=A_i^* \oplus h(r||PWi^{new})$ and $C_i^{new}=h(A_i^*||ID_i||h(r||PW_i^{new}))$.Then, SCreplaces B_i and C_i with B_i^{new} and C_i^{new}, respectively.

3. SECURITY WEAKNESS OF LIU ET AL.'S AUTHENTICATION SCHEME

This section provides security weaknesses in Liu et al.'s authentication scheme, which are focused on off-line password guessing attack (OPGA), masquerading attack (MA) with smart card loss attack, no perfect forward secrecy (PFS) and no anonymity.

3.1 Off-line Password Guessing Attack

Kocher et al. explained that various information stored in SCs could be extracted by physically monitoring its power consumption [14]. So it is possible to say that if a user loses his/her SC, all information in SCmay be revealed to the attacker. In Liu et al.'s authentication scheme, SC stores important information for user login and authentication phases. Furthermore, for the proper attack, it is assumed that the attacker could listen and get the messages from the communication between U_i and S.

UsingSCinformation of U_i, which are $\{B_i, C_i, r, h(\cdot)\}$ andID_i from the communication messages $\{ID_i, D_i, E_i, T_i\}$ and $\{F_i, G_i, T_s\}$, attacker can perform OPGA to find PW_ias follows. (1) The attacker guesses a password candidate PW_i' and computes $A_i'=B_i \oplus h(r||PW_i')$ and $C_i'=h(A_i'||ID_i||h(r||PW_i'))$. (2) The attacker checks whether C_i' is equal to C_i. If they are the same, the password guessing is successful. Otherwise, the attacker repeats Steps (1) and (2) until the correct password is withdrawn.

3.2 Masquerading Attack

When an attacker gets or steals the user's SCin OPGA, he/she can login and authenticate to S, and compute the session key sk between U_i and S. So the attacker can impersonate the legitimate user U_i. It is critical problem that the attacker can be authenticated to S using user's SCinformation. The attacker can illegally extract the secret values in the user's SC and get some important information.

So, the attacker impersonate $U_i$after the success of OPGA as follows. (1) The attacker computesA_i, C_i, D_i and E_i using ID_i, PW_i, B_i, C_i and r, generates a random number $\alpha_{at}$and sends $\{ID_i, D_i, E_i, T_i\}$ to S. (2) S cannot figure out that the message is from the attacker. So, Sauthenticates the attacker's message,computes A_i, α_{at}, D_i', $F_i$and G_i, generates $\beta$and then sends $\{F_i, G_i, T_s\}$ to the attacker. Therefore, the attacker can login and be authenticated to S with forming the session key $sk=h(\alpha_{at}||\beta'||h(A_i' \oplus ID_i))$, which is the same to S's session keysk.

3.3 No Perfect Forward Secrecy

PFS is a feature of specific key agreement schemes that gives assurances the session key will not be compromised even if the private key of the server is compromised. But Liu et al.'s scheme does not achieve PFS.

In Liu et al.'s scheme, the attacker can compute the all session keys between U_i and S if the attacker knows one of long-term keys as follows. (1) The attacker gets$\{ID_i,D_i,E_i, T_i\}$ and $\{F_i, G_i, T_s\}$ in the previous communication between U_i and S. (2) The attacker knows one of long-term secret x of S and could derive $A_i'=h(ID_i \oplus x)||h(x)$. So the attacker can compute α' and β' as $\alpha'=E_i \oplus A_i' \oplus T_i$ and $\beta'=G_i \oplus A_i' \oplus T_s$. After that, the attacker could compute $sk'=h(\alpha'||\beta'||h(A_i' \oplus ID_i))$. Therefore, Liu et al.'s scheme does not provide PFS.

3.4 No Anonymity

Liu et al.'s authentication scheme does not provide the anonymity. In this scheme, U_i sends his/her own identifier $ID_i$to S over public communication without any protection. Therefore, an attacker can easily get ID_i from public communications. This results in the identity exposure problem. Therefore, the lack of anonymity in Liu et al.'s scheme raises privacy related problems that need to be addressed to Internet of things. To solve this problem, it is necessary to use anonymity mechanism in the communication.

4. PRIVACY PRESERVING USER AUTHENTICATION SCHEME

In this section, we propose a new privacy preserving user authentication scheme (PUAS) based on smartcard and bilinear pairing. PUAS could solve all the security problems and privacy issue depicted in Liu et al.'s authentication scheme. In PUAS, there are also two participants, U_i and S, which is consisted of four phases, registration phase, login phase, authentication phase and password changing phase.

4.1 Bilinear Pairings

Let G_1 be an additive cyclic group generated by P whose order is a prime q, and G_2 is a multiplicative cyclic group of the same order. A map $\hat{e}(.) : G_1 \times G_1 \rightarrow G_2$ is called a bilinear mapping if it satisfies the following properties:

-*Bilinear property*: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$, for all $P$and Q in G_1 and all a and b in Z_q^*.
-*Non-degenerate*: There exists P and Q in G_1 such that $\hat{e}(P, Q)=1$.
-*Computable*: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for all P and Q inG_1.

We note that G_1 is the group of points on an elliptic curve and G_2 is a multiplicative subgroup of a finite field. Typically, the mapping $\hat{e}$ will be derived from either the Weil or the Tate pairing on an elliptic curve over a finite field.

4.2 PUAS

This section proposes a new privacy preserving user authentication scheme to solve the security and privacy problems in Liu et al.'s scheme, which provides mutual authentication between the user and the server and does not require time synchronization. In order to prevent the problems of clock synchronization or a delay-time limitations, PUAS adopts the challenge-response mechanism. The security of PUAS is based on bilinear Diffie-Hellman problem (BDHP) and one-wayness of the hash function.

For the system setup, system administrator sets a Bilinear map $\hat{e}(.)$ and $h(\cdot):\{0,1\}^{*}\rightarrow G_1$, which is a cryptographic hash function with an output size of 512 bits. Furthermore, system administrator selects encryption and decryption function, $E(\cdot)$ and $D(\cdot)$, based on Advanced Encryption Standard (AES). Then, the system administrator publishes the system parameters $<G_1, G_2, \hat{e}(.), q, P, h(\cdot), E(\cdot), D(\cdot)>$. PUAS consists of four phases namely; registration, login, authentication and password change phases as shown in Figures 1 and 2.

[Registration Phase] This phase is executed by the following steps when a new user U_i wants to be registered to the server$S$.

RP1. When U_i wants to register with S, U_i selects his/her identity ID_i and password PW_i.U_i generates a random number $r$and computes $RPW_i=h(PW_i\|r)$.U_i submits ID_i and $RPW_i$to S.

RP2. On receiving the registration request, Sgenerates a random number w and computes $A_i=h(ID_i\oplus x)$,$B_i=h(A_i)\oplus RPW_i$, $C_i=E_x(ID_i\|w)$ and $D_i=(h(A_i)\|ID_i\|RPW_i)$.$S$ personalizes a $SC$with the parameters $\{B_i,C_i,D_i, \hat{e}(.),h(\cdot), P\}$ and sends it to U_i over a secure channel.

RP3. U_i computes $P_i=h(ID_i\|PW_i)\oplus r$ and writes P_i into his SC.

[Login Phase] If U_i wants to login, U_i inserts SC in a card reader and inputs ID_i' and PW_i'. Then, SC performs the following operations:

LP1. SC extracts $r'=P_i\oplus h(ID_i'\|PW_i')$ and computes $RPW_i'=h(PW_i'\|r')$, $h(A_i)'=B_i\oplus RPW_i'$ and $D_i'=(h(A_i)'\|ID_i'\|RPW_i')$. SC verifies D_i' with stored D_i. If it does not hold, SC rejects U_i's login request. Otherwise, SC generates a fresh random number α, computes $E_i=aP$ and $F_i=h(C_i\|h(A_i)'\|E_i)$ and sends a login request message $\{C_i, E_i, F_i\}$ to S.

[Authentication Phase] Upon receiving the message $\{C_i, E_i, F_i\}$, S and SC execute the following steps for mutual authentication and session key agreement as follows:

AP$_1$. S computes $ID_i\|w=D_x(C_i)$, $A_i'=h(ID_i\oplus x)$ and $F_i'=h(C_i\|h(A_i')\|E_i)$, and verifies F_i' with the received F_i. If it does not hold, S rejects the request. Otherwise, S generates a fresh random number β, computes $L_i=\beta P$, $SK=\beta E_i$, $C_i'=E_x(ID_i\|\beta)\oplus SK$ and $M_i=h(ID_i\|C_i'\|h(A_i')\|L_i\|SK)$ and sends back a message $\{L_i, C_i', M_i\}$ to U_i. SC computes $SK'=\alpha L_i$, $C_i''=C_i'\oplus SK'$ and $M_i'=h(ID_i'\|C_i'\|h(A_i)'\|L_i\|SK')$and verifies M_i' with the received M_i.If it does not hold, U_i rejects the request. Otherwise, SC updates $C_i$with C_i''.

After the mutual authentication and session key agreement between U_i and S, they could securely communicate with each other based on the established SK.

[Password Change Phase]This phase is invoked whenever U_i wants to change his/her password. By invoking this phase, U_i can easily change his/her password without taking any assistance from S. If U_i wants to change his/her password, U_i inserts SC in a card reader and inputs ID_i' and PW_i'. Then, SC performs the following operations:

PC1. SC extracts $r'=P_i\oplus h(ID_i'\|PW_i')$ and computes $RPW_i'=h(PW_i'\|r')$, $h(A_i)'=B_i\oplus RPW_i'$ and $D_i'=(h(A_i)'\|ID_i'\|RPW_i')$. SC verifies D_i' with stored D_i. If it does not hold, SC rejects U_i's request. Otherwise, SC asks U_i to input a new password PW_i^{new} and computes $RPW_i^{new}=h(PW_i^{new}\|r')$,$B_i''=h(A_i)'\oplus RPW_i^{new}$ and $D_i''=(h(A_i)'\|ID_i\|RPW_i^{new})$. SC replaces B_i'' and D_i'' by $B_i$and D_i, respectively.

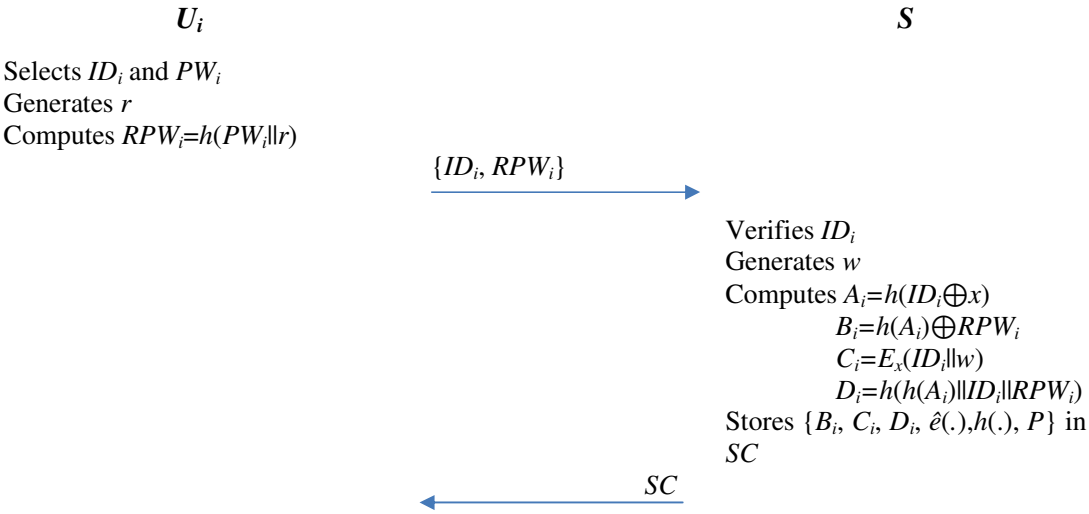

Figure 1. Registration phase of PUAS

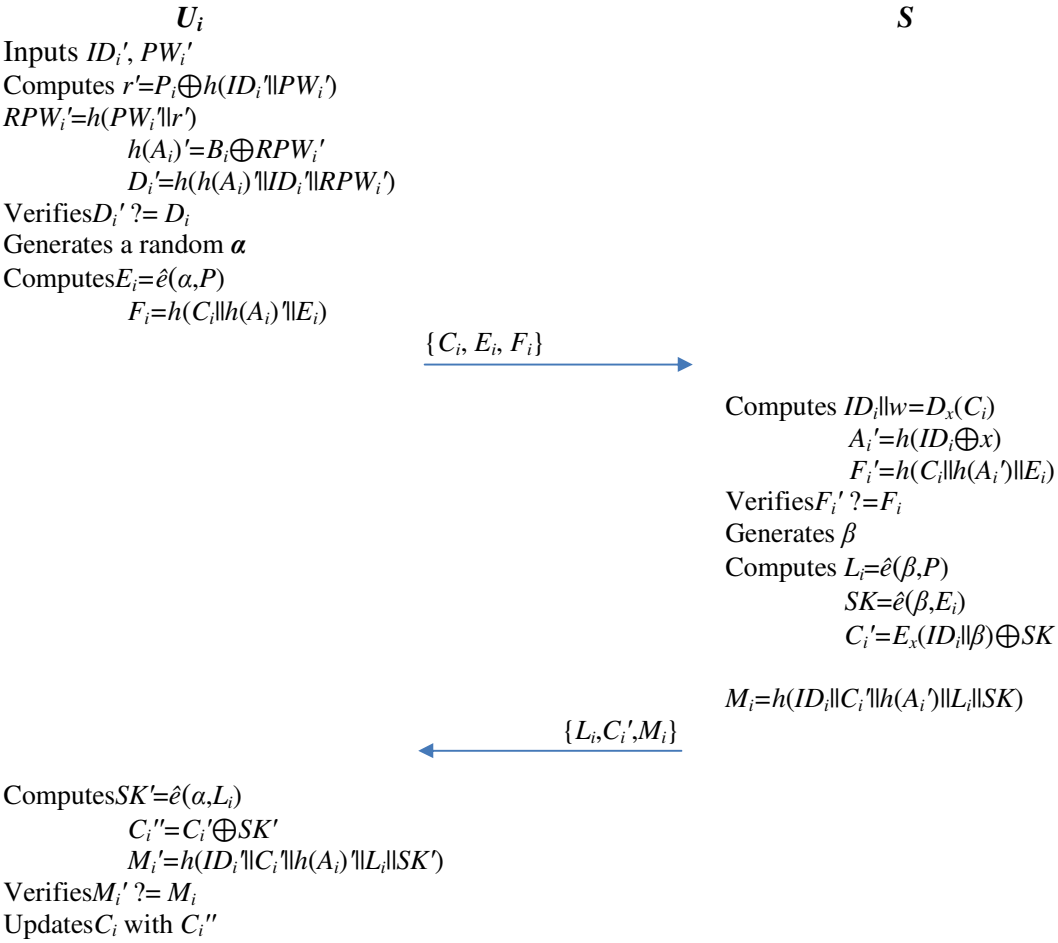

Figure 2. Login and authentication phases of PUAS

5. ANALYSIS

This section provides security and performance analyses of PUAS. For the security analysis, three security properties of PUAS are considered mainly to show security against OPGA and MA with smart card loss attack, and provide PFS. Furthermore, PUAS provides anonymity. After that, we provide performance analysis of PUAS and comparison with the related schemes in [12-13].

5.1 Security Analysis

For the proper security analysis, we follow the Dolev-Yao threat model [15] and consider the risk of side-channel attack [14]to construct the threat assumptions which are described as follows:
- An adversary can be either U_i or S. Any registered user can act as an adversary.

- An adversary can eaves drop every communication in public channels. He/she can capture any message exchanged between U_i and S.

- An adversary has the ability to alter, delete or reroute the captured message.
- Information can be extracted from the smart card by examining the power consumption of the card.

[Off-line Password Guessing Attack]Suppose an user loses his/her smart card and an adversary gets it, and extracts all of the information stored on the smart card $\{B_i, C_i, D_i, P_i, \hat{e}(.), h(.), P\}$ by power consumption analysis. However, he/she cannot obtain any password related information. There are three values B_i, D_i and P_i related to the password. Each value is related with two unknown values to the attacker. Therefore, PUAS is strong against OPGA because the attacker could not do any guessing attack due to two unknown values in each value.

[Masquerading Attack] Suppose an adversary intercepts all of the message $\{C_i, E_i, F_i\}$ and $\{L_i, C_i', M_i\}$ transmitted in public channel between U_i and S, and steals the smart card of U_i to get $\{B_i, C_i, D_i, P_i, \hat{e}(.), h(.), P\}$. There are two possible attacks to the attacker to masquerade U_i as or S. For U_iMA, the attacker need to form a legal login message $\{C_i, E_i, F_i\}$. However, the attacker could not form a legal value F_i due to the lack of knowledge on A_i, which is related with the password guessing attack. For SMA, the attacker need to form a message $\{L_i, C_i', M_i\}$. However, the attacker could not form a legal value M_i due to the lack of knowledge on A_i and C_i', which are related to the long term secret x of S. Therefore, PUAS is strong against MA.

[Perfect Forward Secrecy] The security of PUAS is based on the bilinear pairing. In PUAS, a session key is computed between U_i and Sas $SK=\hat{e}(\alpha, \beta P)=\hat{e}(\alpha P, \beta)$. Even if S's long term secret key x is compromised, the adversary cannot retrieve α nor β from E_i and $L_i$to generate the session key. The session key of PUAS is based on the difficulty of BDHP. Thereby, PUAS provides PFS.

[Anonymity] To address anonymity, PUAS uses C_i, which is an amplified encrypted identity and is regularly changed in each session. Only S could generate and check the identity of U_i by using the long term secret key x. Furthermore, the renewal of is not only depending on x but also depending on the session key SK. Thereby, only legal entity could know the amplified identity $E_x(ID_i||\beta)$. Thereby, PUAS provides anonymity.

Table 2. Security and privacy comparison of user authentication schemes.

Properties / Schemes	OPGA	MA	PFS	Anonymity
Li et al. [12]	No	No	Yes	No
Liu et al. [13]	No	No	No	No
PUAS	Yes	Yes	Yes	Yes

5.2 Performance Analysis

This subsection evaluates the performance of PUAS in terms of computational cost. Table 3 shows a comparison of PUAS and the related schemes [12-13]. From Table 3, we can see that PUAS has a bit overhead than the other schemes to provide security and privacy. The security and privacy are top most important in any cryptographic schemes. For the efficient comparison, we only considered login and authentication phases' operational requirements with the notations M, E, B, S and H for multiplication/division operation, modulus exponential operation, bilinear pairing operation, symmetric encryption/decryption operation and hash operation, respectively.

Table 3. Performance comparison of user authentication schemes.

Entities / Schemes	U_i	S	Total
Li et al. [12]	$1M+3E+4H$	$3E+3H$	$1M+6E+7H$
Liu et al. [13]	$6H$	$6H$	$12H$
PUAS	$2B+5H$	$2B+2S+4H$	$4B+2S+9H$

6. CONCLUSION

In this paper, we provided analyses on Liu et al.'s smart card based password authentication scheme. Our research showed that Liu et al.'s scheme is vulnerable to the password guessing attack and impersonation attack and furthermore does not provide perfect forward secrecy not anonymity. As a remedy scheme of Liu et al.'s scheme, we proposed a privacy preserving user authentication scheme (PUAS) based on smart card. We demonstrated that PUAS has much better security features and performance when compared to Liu et al.'s scheme and the related other schemes.

ACKNOWLEDGEMENTS

Corresponding author is Hyunsung Kim. This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (NRF-2017R1D1A1B04032598).

REFERENCES

[1] Kim, H. S., Lee, S. W., & Yoo, K. Y., (2003) "ID-based Password Authentication Scheme using Smart Cards and Fingerprints," ACM Operating Systems Review, pp. 32-41.

[2] Tzong-Chen, W., & Hung-Sung, S., (1996) "Authenticating passwords over an insecure channel," Computers & Security, Vol. 15, No. 5, pp. 431-439.

[3] Nyirongo, R., Kuonga, S., Ali, P., Eneya, L., & Kim, H., (2017) "Cryptanalysis and Enhancement of Password Authentication Scheme for Smart Card," International Journal on Cryptography and Information Security, Vol. 7, No. 3, pp. 1-13.

[4] Lamport, L., (1981) "Password authentication with insecure communication," Communications of the ACM, Vol. 24, No. 11, pp. 770-772.

[5] Song, R., (2010) "Advanced smart card based password authentication protocol," Computer Standards & Interfaces, Vol. 32, pp. 321-325.

[6] Chang, C. C., & Wu, T. C., (1991) "Remote password authentication with smart cards," IEE Proceedings Part E Computers and Digital Techniques, Vol. 138, No. 3, pp. 165-168.

[7] Das, M. L., Saxena, A., & Gulati, V. P., (2004) "A dynamic ID-based remote user authentication scheme," IEEE Transactions on Consumer Electronics, Vol. 50, No. 2, pp. 629-631.

[8] Liao, I. E., Lee, C. C., & Hwang, M. S., (2005) "Security enhancement for a dynamic ID-based remote user authentication scheme," in Proceedings of the International Conference on Next Generation Web Services Practices 2005, pp. 437-440, Korea, August 2005.

[9] Xu, J., Zhu, W. T., & Feng, D. G., (2009) "An improved smart card based password authentication scheme with provable security," Computer Standards & Interfaces, Vol. 31, No. 4, pp. 723-728.

[10] Sood, S. K., Sarje, A. K., & Singh, K., (2010) "An improvement of xu et al.'s authentication scheme using smart cards," in Proceedings of the Third Annual ACM Bangalore Conference 2010, pp. 17–22, Bangalore, Karnataka, India, 2010.

[11] Chen, B. L., Kuo, W. C., & Wuu, L. C., (2012) "Robust smart-card-based remote user password authentication scheme," International Journal of Communication Systems, Vol. 27, No. 2, pp. 377-389.

[12] Li, X., Niu, J., Khan, M. K., & Liao, J., (2013) "An enhanced smart card based remote user password authentication scheme," Journal of Network and Computer Applications, Vol. 36, No. 5, pp. 1365-1371.

[13] Liu, Y., Chang, C. C., & Chang, S. C., (2017) "An Efficient and Secure Smart Card Based Password Authentication Scheme," International Journal of Network Security, Vol. 19, No. 1, pp. 1-10.

[14] Kocher,P., Jaffe,J., Jun, B., & Rohatgi,P., (2011) "Introduction to differential power analysis,"Journal of Cryptographic Engineering, Vol. 1, No. 1, pp. 5-27.

[15] Dolev, D., & Yao,A., (1983) "On the security of public key protocols,"IEEE Transactions on Information Theory, Vol. 29, No. 2, pp. 198-208.

AUTHORS

Beaton Kapito received the B.E. degree in Mathematics from Chancellor College of University of Malawi and is currently a Masters Degree student with the Department of Mathematics, Chancellor College, University of Malawi. He is also working as a part time lecturer at Chancellor College, University of Malawi from 2017. He is also an adjunct lecturer at Malawi Adventist University,an affiliate of The University of Eastern Africa, Baraton. He has been a Mathematics teacher at Chikwawa Secondary School, Soche Adventist Secondary Schooland Chileka Mission Secondary School. His research interest is in Cryptography: His Masters thesis proposal is "Privacy Preserving Authenticated Key Agreement for Internet of Things."

Patrick Ali received the M.Sc. and the Ph.D. degree from Department of Mathematics, Chancellor College, University of Malawi in 2006 and from the Department of Mathematics, University of KwaZulu-Natal, South Africa in 2011, respectively. He is a senior lecturer at the Department of Mathematical Sciences, Chancellor College, University of Malawi from 2006 and is the current Head of Department. He has been an active researcher in graph theory and combinatorial matrix theory. He achieved the research grant from IMU-Simons African Fellowship Grant at 2016. He also achieved two conference awards of the second best PhD student talk at the 52nd SAMS Annual Congress at 2009 and the best PhD student talk at the Faculty of Science and Agriculture Postgraduate Research Day at 2010.

Levis Eneya received the Ph.D. degree from the Humboldt University of Berlin, Germany in 2010. He is the current Dean of Science and is a Senior Lecturer in the Department of Mathematics, University of Malawi, Malawi. Before becoming dean of faculty in January 2015. He has been an active researcher in optimization, mathematical modelling, and strengthening mathematics teaching and learning through problem solving. He has worked on developing efficient optimization methods for minimizing energy functionals; infectious diseases modelling; and he is currently working on transport optimization and logistics in value chain analysis, and optimization of transport networks in cities. He is also in a team of five, on a collaborative project "Improving Quality and Capacity of Mathematics Teacher Education in Malawi" between the University of Malawi and University of Stavanger in Norway, funded by the NORAD (2014 - 2018). He also served as president of the Southern Africa Mathematical Sciences Association (SAMSA) from 2012 - 2014.

Hyunsung Kim received the M.Sc. and Ph.D degrees in computer engineering from Kyungpook National University, Korea, in 1998 and 2002. He is a Professor with the Department of Cyber Security, Kyungil University, Korea from 2012. Furthermore, he is currently a visiting professor at the Department of Mathematical Sciences, Chancellor College, University of Malawi, Malawi from 2015. He also was a visiting researcher at Dublin City University for 2009. From 2000 to 2002, he worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2012 with the Department of Computer Engineering, Kyungil University. His research interests include cryptography, VLSI, authentication technologies, network security, ubiquitous computing security and security protocol.