An Efficient and Robust Remote User Authentication Method

Mohammed Khan

Abstract

Wu-Chieu proposed an enhanced remote user authentication scheme to improve the security of a user-friendly remote user authentication scheme with smart cards. However, we demonstrate that their scheme is vulnerable and susceptible to the attacks and can easily be cryptanalyzed. Their scheme performs only unilateral authentication (only client authentication) and there is no mutual authentication between user and remote system, so their scheme suffers from the server spoofing attack. Furthermore, their scheme is slower in detecting the wrong input-password, and users cannot change their passwords. This paper proposes an efficient and secure remote authentication scheme to solve the problems found in Wu-Chieu's scheme. In addition, the computational costs and efficiency of the proposed scheme is better than other related published schemes.

Keywords: authentication, security, smart card, cryptography, password

I. Introduction

In remote authentication methods, legitimacy of the remote users is authenticated over an insecure communication channel. In 1981, Lamport [1] proposed a remote user authentication scheme using password tables. In 2000, Hwang and Li [2] identified that Lamport's scheme has the risks of attacking and modifying the password table. So, Hwang and Li presented a novel remote user authentication method without using the password table on the basis of El-Gamal public key encryption method [3]. To improve the previous research work, many remote user authentication schemes have been proposed [4-29] and each scheme has its pros and cons.

In some of the published schemes, password is computed by the remote system and

assigned to the users, but length of the password is usually long and random and there is no user's consent in selecting the passwords, which make these schemes infeasible. So in 2003, Shyi-Bin [10] proposed an authentication scheme in which users are free to choose and change their passwords. Later in 2004, Yang-Wang [14] identified that the scheme of Shyi-Bin's suffers from the forgery attack and the password guessing attack. More recently, Wu-Chieu [15] also pointed out impersonation attack on Shyi-Bin's scheme and described that an adversary can easily impersonate a valid user and gets login into the system. Consequently, they proposed a modified remote user authentication scheme. Wu-Chieu claimed that their scheme is better and secure than the scheme of Shyi-Bin [10].

However, in this paper, we demonstrate that the Wu-Chieu's scheme also suffers from the attacks and can be easily cryptanalyzed. We describe that their scheme only performs unilateral authentication (only client authentication) and user has no information about the authenticity of the remote system. Thus, their scheme is susceptible to the server spoofing attack. We also point out that their scheme is slower in detecting the wrong input-password, and users cannot change their passwords. For the remedy of the problems in Wu-Chieu's scheme, we propose an improved and efficient remote user authentication, in which users can update their passwords freely and securely without help of the remote system, and wrong input-password is detected at the user end instead of server side. Furthermore, user and remote system performs mutual authentication to verify each other. Moreover, computational costs and efficiency of the improved scheme is better than other related schemes of [10] and [15].

Rest of the paper is organized as follows; Section II briefly reviews the Wu-Chieu's scheme, Section III demonstrates the cryptanalysis and weaknesses of their scheme, Section IV proposes an improved and efficient scheme, Section V performs the security analysis of the proposed scheme, Section VI elaborates the efficiency of the presented scheme, and Section VII concludes this paper.

II. Review of Wu and Chieu's Scheme

Wu and Chieu's scheme is divided into three phases, namely; registration, login, and authentication. In the following subsections, their scheme is briefly reviewed.

A. Registration Phase

In the registration phase, user U_i chooses his ID_i and password Pw_i , and submits to the registration server. Upon receiving the registration request, remote system performs the following operations:

1. Computes A_i by $A_i = h(ID_i, x)$ where x is the private key of the server, $h(.)$ is the collision-free one-way hash function.
2. Computes B_i by $B_i = g^{A_i \cdot h(pw_i)} \pmod{p}$, where p is a large prime number and g is a public primitive element in $GF(P)$.
3. Remote server personalizes the smart card, which contains the information $\{ID_i, A_i, B_i, h(.), p, g\}$ and issues smart card to the U_i .

B. Login Phase

In the login phase, user inserts his smart card into the reader machine or terminal and enters his ID_i and pw_i^* . Smart card performs the followings operations:

1. Computes $D_i^* = g^{h(pw_i^*)} \pmod{p}$, and $C_1 = h(T \oplus B_i)$
2. User sends login message $m = \{ID_i, C_1, D_i^*, T\}$ to the remote server over an insecure network.

C. Authentication Phase

Remote system receives the message from the user and performs the following operations at time T' :

1. Checks the format of ID_i . If the format is not correct, remote system rejects the login request.
2. Verify the validity of time interval between T and T' . If $(T' - T) \geq \Delta T$, where ΔT denotes the expected valid time interval for transmission delay, then remote system rejects the login request.
3. Computes $A_i = h(ID_i \oplus x)$, $B_i^* = (D_i^*)^{A_i} \pmod{p}$ and $C_1^* = h(T \oplus B_i^*)$

4. Compares whether $C_1^* = C_1$ or not. If they are equal, it means user is authentic and remote system accepts the login request otherwise, the login request is rejected.

III. Cryptanalysis and Weaknesses of Wu-Chieu's Scheme

Wu-Chieu's scheme is vulnerable to the attacks and can easily be cryptanalyzed. In the following subsections, we demonstrate the cryptanalysis and weaknesses of their scheme.

1. Wu-Chieu's scheme performs only unilateral authentication i.e. only client authentication and there is no authenticity of the remote system. So, their scheme has risk of manipulating the user's data by setting up fake server by an adversary [16, 21]. Here, we assume that an adversary Bob is an eavesdropper over the insecure channel between remote system and application user. The user U_i sends login information i.e. $m = \{ID_i, C_1, D_i^*, T\}$ over the insecure channel, so Bob also gets it. Here, Bob can spoof the U_i by impersonating the server. Bob plays the role of fake-server and sends a fake mutual authentication message to U_i by performing the following operations:
 - a. Computes $C_2 = h(C_1 \oplus T')$, where T' is the timestamp of Bob. Now, Bob sends $\{C_2, T'\}$ to U_i for the mutual authentication.
 - b. Upon receiving the message $\{C_2, T'\}$, user validates T' . If it is invalid, user terminates the operation.
 - c. User U_i computes C_2 and confirms either $C_2 = h(C_1 \oplus T')$ or not. If it holds true, the U_i believes that Bob is an authentic server, while Bob is an adversary and becomes successful in deceiving the U_i . Hence, Wu-Chieu's scheme can not withstand the server spoofing attack and an eavesdropper can easily play the role of authentication server.
2. If user U_i inserts wrong password by mistake, this wrong password will be detected by remote server in the authentication phase. Hence, Wu-Chieu's scheme is very slow in detecting the wrong passwords, which could be keyed-in by mistake.
3. In Wu-Chieu's scheme, there is no way to change the passwords. As an example, if

the password of U_i is compromised or he wants to change the password for any reasons, then there is no any method to change the password in their scheme. So, this drawback also not fulfills the user's requirement of authentication protocols [16] [18].

IV. Proposed Remote User Authentication Scheme

In this section, we propose an efficient and secure remote user authentication scheme with smart cards, which can withstand the security pitfalls found in Wu-Chieu's scheme.

A. Registration Phase

In the registration phase, user U_i chooses his ID_i and password Pw_i , and submits to the registration server. Upon receiving the registration request, remote system performs the following operations:

1. Computes $A_i = h(ID_i \oplus x)$ and $V_i = A_i \oplus pw_i$, where x is the private key of the remote system and $h(.)$ is collision free one-way hash function.
2. Remote system personalizes the smart card with the secure information $\{ID_i, A_i, V_i, h(.)\}$ and issues the card to the U_i .

B. Login Phase

If U_i wants to login into the system, he inserts his smart card into the terminal and enters his ID_i and pw_i^* . Smart card performs the following operations:

1. Computes $B_i = V_i \oplus pw_i^*$, and verifies whether B_i equals to the stored A_i or not. If they are equal, smart card performs further operations, otherwise terminates the operation.
2. Computes $C_1 = h(B_i \oplus T)$, where T is the current timestamp of the input device is.
3. At the end of login phase, U_i sends login message $m = \{ID_i, C_1, T\}$ to the remote server over an insecure network channel.

C. Authentication Phase

In the authentication phase, remote system receives the message from the user and performs the following operations:

1. Checks the format of ID_i . If the format is not correct, remote system rejects the login request.
2. Verify the validity of time interval between T and T' . If $(T' - T) \geq \Delta T$, where ΔT denotes the expected valid time interval for transmission delay, then remote system rejects the login request.
3. Computes $B_i^* = h(ID_i \oplus x)$ and $C_1^* = h(B_i^* \oplus T)$
4. Compares whether $C_1^* = C_1$ or not. If they are equal, it means user is authentic and remote system accepts the login request, and performs step 5 otherwise, the login request is rejected.
5. For the mutual authentication, remote system acquires current timestamp T'' and computes $C_2 = h(B_i^* \oplus T'')$ and then sends mutual authentication message $\{C_2, T''\}$ to the U_i .
6. Upon receiving the message $\{C_2, T''\}$, user verifies the validity of time interval between T'' and T''' . If the timestamp is valid, U_i performs step 7, otherwise rejects the further operations.
7. U_i computes $C_2^* = h(B_i^* \oplus T'')$ and compares $C_2^* = C_2$. If they are equal, user believes that the remote party is authentic system and the mutual authentication between U_i and remote server is completed, otherwise U_i terminates the operation.

D. Password Change Phase

Whenever U_i wants to change his old password pw_i to the new password pw'_i , he performs the following operations without any help from the remote system:

1. Computes $B_i = V_i \oplus pw_i = h(ID_i \oplus x)$
2. Compares B_i and stored value of A_i on smart card. If they are equal, U_i is allowed to change the password; otherwise password change request is rejected.
3. Computes $V'_i = B_i \oplus pw'_i$
4. Stores V'_i on the smart card and replaces the old value of V_i . Now, new password is successfully updated and this phase is terminated.

V. Security Analysis of the Proposed Scheme

In this section, we perform security analysis of the presented scheme.

1. It is very difficult for anyone to derive the server's secret key x from the hash value of $A_i = h(ID_i \oplus x)$, because of the security property of one-way hash functions [6].
2. To withstand replay attacks, neither the replay of an old login message $\{ID_i, C_1, T\}$ in the login phase nor the replay of the remote system's response $\{C_2, T''\}$ in step 5 of the authentication phase will work. It would be failed in steps 2 and 6 of the authentication phase, because of the time interval $(T' - T) \geq \Delta T$ and $(T''' - T'') \geq \Delta T$, respectively.
3. From the login message $\{ID_i, C_1, T\}$, it is infeasible to compute B_i by using equation $C_1 = h(B_i \oplus T)$, because it is computed by the secure one-way hash function.
4. Proposed scheme protects from the impersonation attack found in [10]. An attacker can attempt to modify login message $\{ID_i, C_1, T\}$ into $\{ID_i, C_A, T_A\}$. However, this impersonation attempt will be failed in the step 3 of the authentication phase, because an attacker has no way of obtaining the value of $B_i^* = h(ID_i \oplus x)$ to compute the valid value of C_1 .
5. Server spoofing attack is completely solved by providing the mutual authentication between user and remote system. Remote system sends mutual authentication message $\{C_2, T''\}$ to the user. If an attacker intercepts it and resends the forge message i.e. $\{C_A, T_A\}$ to the user, it will be verified in steps 6 and 7 of the authentication phase because the value of C_2 is computed by $C_2 = h(B_i^* \oplus T'')$. In addition, replay of this message can be exposed because of the time stamp.
6. In the password change phase, value of B_i is compared with the value of A_i . If these two values are not same, user is not allowed to change the password. Furthermore, when the smart card is stolen or theft, unauthorized users can not change new password. Hence, proposed scheme also protects from the denial of service attack using stolen smart card.

VI. Efficiency of the Proposed Scheme

The performance and efficiency of the proposed scheme are summarized in table 1.

Our scheme is completely based on one-way collision free hash functions, which are computationally faster than modular exponentiations [6]. In the registration, login, and authentication phases, without mutual authentication, scheme in [10] requires 2 times exponential and 5 times hash operations, while scheme in [15] requires 3 times exponential and 6 hash operations. While on the other hand, proposed scheme requires only 6 hash computations with the mutual authentication so, the computational complexity of our scheme is less than [10] and [15]. Furthermore, schemes of [10] and [15] detect wrong input-password at the server end, while our scheme checks the input-password at the client end and prompts the user on the spot without any transmission delay of network. Besides, proposed scheme enables users to update their passwords freely and securely without the help of remote system. In contrast, scheme in [10] allows users to change their passwords but users have to submit their smart cards to the remote system for changing passwords, which is an inefficient solution while in scheme [15]; there is no any method to change the passwords. In addition, compared with [10] and [15], only our scheme supports mutual authentication to protect the system from the server spoofing attack [16, 21]. Moreover, our scheme consumes less memory space on the smart card to store user's public information. Hence, it is obvious that proposed scheme is more efficient and secure in terms of computations, performance, and security.

Table 1. Comparisons of efficiency

	[10]	[15]	Proposed scheme
Computation in registration phase	1 T_{Exp} , 2 T_H	1 T_{Exp} , 2 T_H	1 T_H
Computation in login phase	1 T_{Exp} , 2 T_H	1 T_{Exp} , 2 T_H	1 T_H
Computation in authentication phase	1 T_H	1 T_{Exp} , 2 T_H	4 T_H (with mutual authentication)
Mutual authentication	Not supported	Not supported	Supported
Password change phase	Supported	Not supported	Supported
Wrong password detection speed	Slow	Slow	Fast
Public information on smart card	$h(\cdot)$, p , g	$h(\cdot)$, p , g	$h(\cdot)$

T_{Exp} : the computation time for modular exponentiation.

T_H : the computation time for a one-way hash function.

VII. Conclusion

In this paper, we presented an enhancement of Wu-Chieu's scheme. We showed that their scheme does not provide mutual authentication between user and remote server,

so user can not trust on the authenticity of the remote server. We also discussed that their scheme is slow in detecting the wrong passwords and does not allow users to change their passwords. To solve these problems, we proposed an efficient and secure remote user authentication scheme, in which legal users can change their passwords freely and securely, and wrong input password is detected very fast at the time of input. In addition, server spoofing attacks is completely solved by providing mutual authentication between user and remote system. Moreover, computational costs and efficiency of the proposed scheme is better than those of the related published schemes.

References

- [1] L. Lamport, Password Authentication with Insecure Communication, Communications of the ACM 24 (11) (Nov. 1981) 770-772.
- [2] Hwang, M.S., and Li, L.H. A New Remote User Authentication Scheme using Smart Cards, IEEE Transactions on Consumer Electronics 46 (1) (2000) 28-30.
- [3] El Gamal, T. A Public-key Cryptosystem and A Signature Scheme Based on Discrete Logarithms, IEEE Transactions on Information Theory 31 (4) (July 1985) 469-472.
- [4] M.K Khan, K. Alghathbar, "Cryptanalysis and Security Improvements of 'Two-Factor User Authentication in Wireless Sensor Networks'", Sensors, vol. 10, Issue 3, pp. 2450-2459, 2010.
- [5] W.H. Yang and S.P. Shieh, Password Authentication Schemes with Smart Cards, Computers and Security 18 (8) (1999) 727-733.
- [6] V. Odelu, A.K. Das, Y. S Rao, S. Kumari, M.K Khan, K.K.R Choo, "Pairing-based CPABE with Constant-size Ciphertexts and Secret Keys for Cloud Environment", Computer Standards & Interfaces, Elsevier, vo. 54, pp. 3-9, 2017
- [7] C. C. Lee, M. S. Hwang, and W. P. Yang, A Flexible Remote User Authentication

- Scheme Using Smart Cards, ACM Operating Systems Review 36 (3) (2002) 46-52.
- [8] J. J. Shen, C. W. Lin, and M. S. Hwang, A Modified Remote User Authentication Scheme Using Smart Cards, IEEE Transactions on Consumer Electronics 49 (2) (May 2003) 414-416.
- [9] C. C. Chang and K. F. Hwang, Some Forgery Attacks On a Remote User Authentication Scheme Using Smart Cards, Informatics, 14 (3) (2003) 289 -294.
- [10] Shyi-Tsong Wu and Bin-Chang Chieu, A User Friendly Remote Authentication Scheme with Smart cards, Computers & Security 22 (6) (2003) 547-550.
- [11] K. C. Leung, L. M. Cheng, A. S. Fong, and C. K. Chan, Cryptanalysis of a Modified Remote User Authentication Scheme Using Smart Cards, IEEE Transactions on Consumer Electronics 49 (4) (Nov. 2003) 1243-1245.
- [12] C.L. Hsu, Security of Chien et al.'s Remote User Authentication Scheme Using Smart Cards, Computer Standards and Interfaces 26 (3) (2004) 167– 169.
- [13] M. Kumar, New Remote User Authentication Scheme Using Smart Cards, IEEE Transactions on Consumer Electronics 50 (2) (May 2004) 597-600.
- [14] C. C. Yang and R. C. Wang, Cryptanalysis of a User Friendly Remote Authentication Scheme with Smart cards, Computers & Security 23 (5) (2004) 425-427.
- [15] S.T Wu and B.C Chieu, A Note on a User Friendly Remote User Authentication Scheme with Smart Cards, IEICE Transactions Fundamentals 87-A (8) (August 2004) 2180-2181.
- [16] E. J Yoon, E. K Ryu, K.Y Yoo, Efficient Remote User Authentication Scheme based on Generalized ElGamal Signature Scheme, IEEE Trans. Consumer Electronics 50 (2)

(2004) 568-570.

[17] Lin, C.H., and Lai, Y.Y, A Flexible Biometrics Remote User Authentication Scheme, *Computer Standard and interfaces* 27 (1) (2004) 19–23.

[18] W.C. Ku, S.T. Chang and M.H. Chiang, Further Cryptanalysis of Fingerprint-based Remote User Authentication Scheme Using Smartcards, *IEE Electronics Letters* 41 (5) 2005

[19] E. J Yoon, E. K Ryu, K.Y Yoo, An Improvement of Hwang-Lee-Tang's Simple Remote User Authentication Scheme, *Computers and Security* 24 (2005) 50-56.

[20] R. Lu and Z. Cao, "Efficient Remote User Authentication Scheme Using Smart Card", *Computer Networks* (article in press), Online April 2005.

[21] Asokan N, Debar H, Steiner M, Waidner M, Authenticating Public Terminals, *Computer Networks* 31 (8) (April 1999) 861-870.

[22] Horng, S.J. Tzeng, S.F. Pan, Y. Fan, P. Wang, X. Li, T. Khan, M.K, "b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET", *IEEE Transactions on Information Forensics Security*, 2013, 8, 1860–1875.

[23] Z. Liu, X. Huang, Z. Hu, M.K. Khan, H. Seo, L. Zhou, "On emerging family of elliptic curves to secure internet of things: ECC comes of age", *IEEE Transactions on Dependable and Secure Computing*, pp. 99, 2017, pp. 237-248

[24] S.F Tzeng, S.J Horng, T. Li, X. Wang, P.H. Huang, M.K Khan, "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET", *IEEE Transactions on Vehicular Technology*, vol 66, no. 4, pp. 3235-3248, 2017

[25] A.K Das, M. Wazid, N. Kumar, M.K Khan, K.W.R Choo, Y.H Park, "Design of

Secure and Lightweight Authentication Protocol for Wearable Devices Environment”,
IEEE Journal of Biomedical and Health Informatics, vol. 22, issue 4, pp. 1310-1322,
2017

[26] F. Wu, L. Xu, S. Kumari, X. Li, A.K. Das, M.K Khan, M. Karuppiah, R. Baliyani, “A
Novel and Provable Authentication and Key Agreement Scheme with User Anonymity for
Global Mobility Networks”, Security and Communication Networks, 2016

[27] I. Uddin, M. Guizani, B.S Kim, S. Hassan, M.K Khan, “Trust Management
Techniques for the Internet of Things: A Survey”, vol. 7, pp. 29763-29787, IEEE Access,
2018

[28] A.S Tolba, M.K Khan, Khaled A, “Systems and Methods for Three Factors
Authentication”, US Patent No. 8862888, 2014

[29] D. He, N. Kumar, Muhammad Khurram Khan, L. Wang, J. Shen, “Efficient
Privacy-Aware Authentication Scheme for Mobile Cloud Computing Services”, IEEE
Systems Journal, Volume 12, Issue: 2, June 2018

[30] M.K Khan, “Fingerprint Biometric-based Self-Authentication and Deniable
Authentication Schemes for the Electronic World”, IETE Technical Review, vol. 26, issue
3, pp. 191-195, 2009

[31] S. Kumari, M.K Khan, R. Kumar, "Cryptanalysis and improvement of 'a privacy
enhanced scheme for telecare medical information systems'", Journal of Medical Systems,
vol 37, issue, 4, 2013