2014 IEEE Workshop on Electronics, Computer and Applications

Weaknesses of the Yoon-Kim-Yoo Remote User Authentication Scheme Using Smart Cards

Te-Yu Chen
National Tainan Junior College of Nursing, Taiwan
e-mail: chendytw@gmail.com

Chung-Huei Ling
Department of Computer Science and Information Engineering, Asia University, Taiwan
e-mail: 101267004@live.asia.edu.tw

Min-Shiang Hwang
Department of Computer Science and Information Engineering, Asia University, Taiwan
Department of Health Services administration, China Medical University, Taiwan
e-mail: mshwang@asia.edu.tw
(Corresponding Author)

***Abstract*—A user authentication scheme is a mechanism employed by a server to authenticate the legality of a user before he/she is allowed to access the resource or service provided by the server. Due to the Internet's openness and lack of security concern, the user authentication scheme is one of the most important security primitives in the Internet activities. Many researchers have been devoted to the study of this issue. There are many authentication schemes have been proposed up to now. However, most of these schemes have both the advantages and disadvantages. Recently, Yoon, Kim and Yoo proposed a remote user authentication scheme which is an improvement of Liaw et al.'s scheme. Unfortunately, we find their scheme is not secure enough. In this paper, we present some flaws in Yoon-Kim-Yoo's scheme. This proposed cryptanalysis contributes important heuristics on the secure concern when researchers design remote user authentication schemes.**

Keywords-cryptography; user authentication; guessing attack; Smart card

I. INTRODUCTION

With the rapid growth in the networking and information technologies, more and more servers provide their services to a number of users who might distribute over different regions around the world through the Internet [14, 16, 17, 29]. Due to the Internet's openness and lack of security concern, how to provide service for admissible users becomes a critical topic. A user authentication scheme is a mechanism employed by a server to authenticate the legality of a user before he/she is allowed to access the resource or service provided by the server [12, 15]. Many attacking methods had been proposed on the user authentications [5, 7, 28, 43, 46]. Therefore, the user authentication scheme is one of the most important security primitives in the Internet activities. Some methods for solving user authentication problem are based on biometric approaches [33]. Many researchers have been devoted to the study of this issue. There are many authentication schemes have been introduced in the literatures [1, 2, 8, 21, 24, 34, 35, 38, 44, 47]. Some schemes are based on smart card [3, 37]. Some schemes were proposed to solve user authentication and key agreement problems [19, 20]. Some schemes are used to solve the user authentication problem for grid computing [11, 30].

Up to now, the password-based approach is the most popular one among various kinds of user authentication schemes. In 1981, Lamport [27] developed a password-based user authentication scheme in which a password table is used for completing user authentication. However, the presence of the password table results in paying additional maintenance cost and suffering from some attacks once it is revealed [13]. After that, various approaches [31, 39, 40, 41, 42] without employing password table are proposed for improving the security and/or efficiency.

Endowed with the properties of the portability, efficiency, and cryptographic capacity, smart cards have been widely employed in the design of user authentication schemes. In 2000, Hwang and Li [13] proposed a novel password-based remote user authentication scheme based on ElGamal public key cryptosystem [6] using smart cards. This scheme did not need any password or verification table in the authentication procedure. Later, Sun [36] proposed another scheme to improve the efficiency of Hwang and Li's scheme. However, Chien et al. showed that Sun's scheme did not provide mutual authentication and did not allow users to freely choose their passwords [4]. Chien et al. accordingly proposed an efficient and practical solution to remote user authentication in 2002. Therefore, Hwang et al. proposed a simple remote user authentication scheme [15] in the same year. This scheme does not require any password or verification table, and any legal user can arbitrarily choose and change their password at their will. In 2006, Liaw et al. [9] proposed an efficient and complete remote user authentication scheme using smart cards which is inspired by Hwang et al.'s scheme. Their scheme is nonce-based and free from synchronization problems. However, Yoon et al. [45] found that Liaw et al.'s scheme does not secure against some attacks and proposed an improved scheme. Yoon, Kim, and Yoo claimed their scheme could provide strong key

978-1-4799-4565-8/14/$31.00©2014 IEEE

agreement function with the property of perfect forward secrecy and reduce the computation loads for smart cards.

Unfortunately, we find Yoon et al.'s scheme is still insecure. In this paper, we will show that their scheme is vulnerable to password guessing attacks and suffers some defects.

II. WEAKNESS OF YOON-KIM-YOO' S SCHEME

In this section, we introduce Yoon et al.'s scheme [45] and then point out its weaknesses. The notations used throughout this article are summarized in Table 1.

Yoon-Kim-Yoo's scheme is composed of five phases: the registration phase, the login phase, the verification phase, the session phase, and the updated password change phase. The five phases are described as follows.

[The registration phase]

This phase is initiated by a user U whenever he/she registers to the server S.

R1. U selects a random number R and memorizes it for the moment, and computes $vpw=PW \oplus b$.

R2. $U \Rightarrow S$: $\{ID, vpw\}$.

R3. After receiving the registration request, the remote server adopts its secrete key x to perform the following computations:

$v = h(ID, x)$.

$e = v \oplus vpw$.

$vk = h(v, e)$.

R4. S loads $(e, vk, h())$ into a smart card and issues the smart card to U.

R5. After receiving the smart card, U enters R into his/her smart card, and U does not need to memorize R after this step.

Table 1: The notations used in this article

Notation	Description
U	The user
ID	The identity of U
PW	The password of U
S	The remote server
x	The secret key of S
$h()$	The cryptographic hash function
p	A public large prime number
α	A public primitive element mod p
	A secure channel
$\rightarrow$	A common channel

[The login phase]

This phase is invoked while a user U wants to login the server S.

L1. U inserts his/her smart card into the terminal and then enters his/her identity ID and password PW.

L2. U's smart performs the following computations:

$vpw' = PW \oplus R$,

$vk' = h(e \oplus vpw', e)$,

Verify whether vk' is equal to the stored vk?

$C = h(e \oplus vpw', N_i)$,where N_i is a random nonce.

L3. $U \rightarrow S$: $\{ID, C, N_i\}$.

[The verification phase]

While receiving the login request message $\{ID, C, N_i\}$ from the user U, the server S performs the following steps.

V1. S verifies the validity of the user identity ID. If it is incorrect, S rejects the login request. Otherwise, S computes $v' = h(ID, x)$, $C' = h(v', N_i)$, and compares the result value C' with the received C. If they are not equal, S rejects the login request. Otherwise, S generates a random nonce N_S and computes $h(v', N_i, N_S)$.

V2. $S \rightarrow U$: $\{N_S, h(v', N_i, N_S)\}$.

V3. As receiving the acknowledge message $\{N_S, h(v', N_i, N_S)\}$ from S, U computes $h(v, N_i, N_S)$ and compares the result value with the received $h(v', N_i, N_S)$. If they are equal, U computes $h(v, N_S, N_i)$.

V4. $U \rightarrow S$: $\{ h(v, N_S, N_i)\}$.

V5. After S receiving this message, S verifies whether $h(v', N_S, N_i)$ is equal to $h(v, N_S, N_i)$. If they are equal, S and U complete the mutual authentication.

[The session phase]

In order to agree a secure session key in this session, S and U perform the following operations.

S1. $U \rightarrow S$: $\{ W=\alpha^{Ni} \bmod p\}$.

S2. $S \rightarrow U$: $\{ S_i=\alpha^{Ns} \bmod p\}$.

S3. $U \rightarrow S$: $\{h(v, S_i, K_u)\}$, where $K_u = S_i^{Ni} \bmod p\}$.

S4. $S \rightarrow U$: $\{h(v', W, K_S)\}$, where $K_S = W^{Ns} \bmod p\}$.

S5. Both S and U check whether $h(v, S_i, K_u)$ is equal to $h(v', W, K_S)$. if yes, a session key, $K= \alpha^{NsNi}$, is created between S and U.

[The password change phase]

When the user U wants to update his/her password from PW to PW_{new}, the following steps are performed.

P1. U inserts his/her smart card into the terminal, enters his/her identity ID and old password PW, and requests to change his/her password.

P2. The smart card computes $vk^* = h(e \oplus PW \oplus R, e)$, and then compares vk^* with vk stored on the smart card. If they are not equivalent, the smart card terminates this session; otherwise, the smart card requests U to enter his/her new password PW_{new}.

P3. The smart card updates e with $e \oplus PW \oplus PW_{new}$.

Some researches had shown that it is possible to extract the secret information stored in a smart card [25, 26]. Consequently, in Yoon-Kim-Yoo's scheme, if a user's smart card is held by an attacker for some reasons, the attacker can carry out the password guessing attack by performing the following steps.

A1. Extract e, vk, and R stored in the smart card.

A2. Guess a candidate password PW'.

A3. Compute both $vpw' = PW' \oplus R$, $v' = vpw' \oplus e$, and $vk' = h(v', e)$.

A4. Compare vk' with vk.

A5. If they are equal, the correct password will be successfully guessed. Otherwise, try another candidate password and repeat Steps A2 and A5 till the correct password is found.

In Step A3, if the user's password has been correctly guessed, i.e. $PW = PW'$, then the value of $v' = vpw' \oplus e$ which yields $PW' \oplus R \oplus e$ would be equal to the user's secrete information $v=h(ID, x)$; and the computed value of vk' is equal to vk stored in the smart card. Therefore, the above password guessing procedure would indicate that the correct password has been successfully guessed in Step A5. Accordingly, the proposed password guessing attack is sound.

In general, passwords created by human beings are low-entropy forms. Hence it does not take much time to complete this attack. After obtaining the user's password, the attacker can masquerade as the user logins the server, or the attacker can change the password to interfere with the user's legitimate login.

The privacy is an important issue on the Internet nowadays. To maintain the transmission privacy after authentication, it is necessary to encrypt the messages transmitted between the user and the server. There is a session key established in Yoon-Kim-Yoo's scheme. However, their session key establish scheme is mainly from Diffie–Hellman key exchange protocol in which some modular exponential computations should be performed. With the limited computing capability, the heavy modular exponential computation is not suitable for smart card. Therefore Yoon-Kim-Yoo's scheme is inefficient due to the high computation cost on the smart card. Therefore, the session key establishment should be further considered in their scheme.

III. CONCLUSION

In this article, we presented some flaws in Yoon-Kim-Yoo's scheme. We have shown that the password guessing attack exits in their scheme. Moreover, the disadvantages of their session key establishment have been described carefully. These weaknesses of Yoon-Kim-Yoo's scheme proposed in this paper are deserved to be taken into consideration seriously while designing a remote user authentication scheme.

ACKNOWLEDGMENT

This study was supported by the National Science Council of Taiwan under grant NSC 102-2221-E-468-020 and NSC 101-2622-E-468-002-CC3.

REFERENCES

[1] A. Awasthi, "On the authentication of the user from the remote autonomous object", International Journal of Network Security, Vol. 1, No. 3, pp. 166-167, 2005.

[2] T. Y. Chang, M. S. Hwang, W. P. Yang, "A communication-efficient three-party password authenticated key exchange protocol", Information Sciences, vol. 181, pp. 217-226, 2011.

[3] C. C. Chang and C. Y. Lee, "A smart card-based authentication scheme using user identify cryptography", International Journal of Network Security, Vol. 15, No. 2, pp. 139-147, 2013.

[4] H. Y. Chien, J. K. Jan, and Y. M. Tseng, "An efficient and practical solution to remote authentication: Smart card," Computers and Security, vol. 21, no. 4, pp. 372-375, 2002.

[5] M. L. Das, "Comments on `Improved efficient remote user authentication schemes'", International Journal of Network Security, Vol. 6, No. 3, pp. 282-284, 2008.

[6] T. ElGamal, "A public-key cryptosystem and a signature scheme based on discrete logarithms," IEEE Transactions on Information Theory, vol. IT-31, no. 4, pp. 469-472, 1985.

[7] T. H. Feng, C. H. Ling, and M. S. Hwang, "Cryptanalysis of Tan's improvement on a password authentication scheme for multi-server environments", International Journal of Network Security, Vol. 16, No. 4, pp. 318-321, 2014.

[8] D. He, J. Chen, and J. Hu, "Weaknesses of a remote user password authentication scheme using smart card," International Journal of Network Security, vol. 13, no. 1, pp. 58-60, 2011.

[9] H. T. Liaw, J. F. Lin, and W. C. Wu, "An efficient and complete remote user authentication scheme using smart cards," Mathematical and Computer Modelling, vol. 44, no. 1-2, July 2006.

[10] C. L. Hsu, "Security of chien et al.'s remote user authentication scheme using smart cards," Computer Standards and Interfaces, vol. 26, no. 3, pp. 167-169, 2004.

[11] J. Hu, H. Xiong, and Z. Chen, "Further improvement of an authentication scheme with user anonymity for wireless communications", International Journal of Network Security, Vol. 14, No. 5, pp. 297-300, 2012.

[12] M. S. Hwang, S. K. Chong, and T. Y. Chen, "Dos-resistant id-based password authentication scheme using smart cards," Journal of Systems and Software, vol. 83, no. 1, pp. 163-172, 2010.

[13] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 46, no. 1, pp. 28-30, 2000.

[14] M. S. Hwang, J. W. Lo, S. C. Lin, "An efficient user identification scheme based on ID-based cryptosystem", Computer Standards & Interfaces, vol. 26, no. 6, pp.565-569, Oct. 2004.

[15] M. S. Hwang, C. C. Lee, Y. L. Tang, " A simple remote user authentication scheme", Mathematical and Computer Modelling, vol. 36, no. 1-2, pp.103-107, Jul. 2002.

[16] M. S. Hwang, Eric J.L. Lu, I. C. Lin, "Adding timestamps to the secure electronic auction protocol", Data & Knowledge Engineering, vol. 40, no. 2, pp. 155-162, Feb. 2002.

[17] M. S. Hwang and P. C. Sung, "A study of micro-payment based on one-way hash chain", International Journal of Network Security, vol. 2, no. 2, pp. 81-90, Mar. 2006.

[18] T. Hwang and W. C. Ku, "Reparable key distribution protocols for internet environments," IEEE Transactions on Communications, vol. 43, no. 5, pp. 1947-1950, May 1995.

[19] Q. Jiang, J. Ma, G. Li, and L. Yang, "Robust two-factor authentication and key agreement preserving user privacy", International Journal of Network Security, Vol. 16, No. 3, 2014, pp. 229-240.

[20] W. S. Juang and J. L. Wu, "Efficient user authentication and key agreement with user privacy protection", International Journal of Network Security, Vol. 7, No. 1, pp. 120-129, 2008.

[21] M. H. Kim and C. K. Koc, "Improving the Novikov and Kiselev user authentication scheme", International Journal of Network Security, Vol. 6, No. 3, pp. 241-245, 2008.

[22] W. C. Ku, C. M. Chen, and H. L. Lee, "Cryptanalysis of a variant of peyravian-zunic's password authentication scheme," IEICE

Transactions on Communication, vol. E86-B, no. 5, pp. 1682-1684, May 2003.

[23] W. C. Ku and S. M. Chen, "Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 50, no. 1, pp. 204-207, 2004.

[24] M. Kumar, "An enhanced remote user authentication scheme with smart card," International Journal of Network Security, vol. 10, no. 3, pp. 175-184, 2010.

[25] M. Kumar,, "A new secure remote user authentication scheme with smart cards," International Journal of Network Security, vol. 11, no. 2, pp. 88-93, 2010.

[26] M. Kumar, M. K. Gupta, and S. kumari, "An improved efficient remote password authentication scheme with smart card over insecure networks," International Journal of Network Security, vol. 13, no. 3, pp. 167-177, 2011.

[27] L. Lamport, "Password authentication with insecure communication," Communications of ACM, vol. 24, pp. 770-772, 1981.

[28] C. C. Lee, "Two attacks on the Wu-Hsu user identification scheme," International Journal of Network Security, Vol. 1, No. 3, pp. 147-148, 2005.

[29] C. T. Li, M. S. Hwang, C. Y. Liu, "An electronic voting protocol with deniable authentication for mobile ad hoc networks", Computer Communications, vol. 31, issue 10, pp. 2534-2540, June 2008.

[30] R. Lu, Z. Cao, Z. Chai, and X. Liang, "A Simple User Authentication Scheme for Grid Computing," International Journal of Network Security, Vol. 7, No. 2, pp. 202-206, 2008.

[31] K. V. Mangipudi and R. S. Katti, "A hash-based strong password authentication protocol with user anonymity," International Journal of Network Security, vol. 2, no. 3, pp. 205-209, 2006.

[32] C. Mitchell, "Limitations of challenge-response entity authentication," Electronics Letters, vol. 25, no. 17, pp. 1195-1196, 1989.

[33] A. Prakash, "A biometric approach for continuous user authentication by fusing hard and soft traits," International Journal of Network Security, Vol. 16, No. 1, pp. 65-70, 2014.

[34] R. Ramasamy and A. P. Muniyandi, "An efficient password authentication scheme for smart card," International Journal of Network Security, vol. 14, no. 3, pp. 180-186, 2012.

[35] S. K. Sood, "An improved and secure smart card based dynamic identity authentication protocol," International Journal of Network Security, vol. 14, no. 1, 2012.

[36] H. M. Sun, "An efficient remote user authentication scheme using smart cards," IEEE Transactions on Consumer Electronics, vol. 46, no. 4, pp. 958-961, 2000.

[37] H. Tang, X. Liu, L. Jiang, "A robust and efficient timestamp-based remote user authentication scheme with smart card lost attack resistance," International Journal of Network Security, Vol. 15, No. 6, pp. 446-454, 2013.

[38] X. Tian, R. W. Zhu, D. S. Wong, "Improved efficient remote user authentication schemes," International Journal of Network Security, Vol. 4, No. 2, pp. 149-154, 2007.

[39] C. S. Tsai, C. C. Lee, and M. S. Hwang, "Password authentication schemes: Current status and key issues," International Journal of Network Security, vol. 3, no. 2, pp. 101-115, 2006.

[40] B. Wang and Z.-Q. Li, "A forward-secure user authentication scheme with smart cards," International Journal of Network Security, vol. 3, no. 2, pp. 116-119, 2006.

[41] R. C. Wang and C. C. Yang, "Cryptanalysis of two improved password authentication schemes using smart cards," International Journal of Network Security, vol. 3, no. 3, pp. 283-285, 2006.

[42] S. Wang, Z. Cao, and H. Bao, "Efficient certificateless authentication and key agreement (CL-AK) for grid computing," International Journal of Network Security, vol. 7, no. 3, pp. 342-347, 2008.

[43] C. Y. Yang, C. C. Lee, and S. Y. Hsiao, "Man-in-the-Middle Attack on the Authentication of the User from the Remote Autonomous Object," International Journal of Network Security, Vol. 1, No. 2, pp. 81-83, 2005.

[44] L. Yang, J. F. Ma, and Q. Jiang, "Mutual authentication scheme with smart cards and password under trusted computing," International Journal of Network Security, vol. 14, no. 3, pp. 156-163, 2012.

[45] E. J. Yoon, S. H. Kim, and K. Y. Yoo, "A security enhanced remote user authentication scheme using smart cards," International Journal of Innovative Computing, Information and Control, vol. 8, no. 5(B), pp. 3661-3675, May 2012.

[46] E. J. Yoon and K. Y. Yoo, "A forgery attack on a low computation cost user authentication scheme," International Journal of Network Security, Vol. 3, No. 1, pp. 51-53, 2006.

[47] X. Zhuang, C. C. Chang, Z. H. Wang, Y. Zhu, "A simple password authentication scheme based on geometric hashing function," International Journal of Network Security, Vol. 16, No. 4, pp. 271-277, 2014