Comment on four two-party authentication protocols

Yalin Chen[1], Jue-Sam Chou[2,*], Chun-Hui Huang[3]

[1] Institute of information systems and applications, National Tsing Hua University
d949702@oz.nthu.edu.tw
[2] Department of Information Management, Nanhua University, Taiwan, R.O.C
*: corresponding author
jschou@mail.nhu.edu.tw
Tel: 886+ (0)5+272-1001 ext.56536
[3] Department of Information Management, Nanhua University, Taiwan, R.O.C
g6451519@mail1.nhu.edu.tw

Abstract

In this paper, we analyze the protocols of Bindu et al., Goriparthi et al., Wang et al. and Hölbl et al.. After analyses, we found that Bindu et al.'s protocol suffers from the insider attack if the smart card is lost, both Goriparthi et al.'s and Wang et al.'s protocols can't withstand the DoS attack on the password change phase which makes the password invalid after the protocol run, and Hölbl et al.'s protocol is vulnerable to the insider attack since a malevolent legal user can deduce KGC's secret key x_s.

Keywords: *password authentication protocol, insider attack, denial-of-service attack, smart card lost problem, mutual authentication, man-in-the-middle attack*

1. Introduction

Authentication protocols provide two entities to ensure that the other party is the intended one whom he attempts to communicate with and can be examined by using three factors: type, efficiency and security. Generally speaking, authentication protocols can be divided into two types. One is password-based that can make a user be authentic to a remote entity by using his human-rememberable password. And the other is public key cryptography-based that makes a user can be authenticated by using his private key instead of password. In a password-based protocol, a user registers at the remote server to become a legal user for accessing the server's resource and the server maintains a password table for authenticating valid users. However, for avoiding the stolen-verifier attack, the server usually issues a smart card to the registered user to get rid of storing a password table. Thereafter, the user can take use of his password and the smart card to logon the server. In a public key-based system, users have to register at KGC (Key Generation Center) for obtaining their public keys and corresponding private keys. Then, they can be authenticated by the intended entity using their private keys. For improving the efficiency of key management in an authentication protocol, an identity-based cryptosystem is usually used in which KGC issues a private key to a registering user and uses the user's identity as his public key. As to other efficiency considerations, such as computational and communicational overhead, researchers generally reduce the computational load of a protocol by using simple techniques, such as secure one-way hash functions and symmetric key encryptions, as much as possible. Of course, asymmetric key encryptions which are less efficient in computations (i.e., RSA, ECC, ElGamal, and bilinear pairings) are used as well. As for giving thought to the communicational overhead, researchers usually do their best to reduce the number of passes (for instance, to only two), since it is the dominant factor in considering the efficiency in a protocol. The most important feature of an authentication protocol is its security since it provides two entities to authenticate each other through an insecure network. Attackers may eavesdrop, modify or intercept the messages to and from in a communication channel to collect and deduce some meaningful information to defraud the other party. Hence, the transmitted messages must be dealt with some techniques to prevent from various attacks, such as password guessing attack, impersonate attack, insider attack, man-in-the-middle attack, and so on.

Recently from 2002 to 2010, many studies [1-41] were proposed to secure authentication protocols. In 2008, Bindu et al. proposed an improved protocol [14] on Chien et al.'s scheme [3]. Their protocol is a smart card based password authentication protocol and operates with symmetric key encryption algorithm. They claimed that their protocol is secure, can achieve user anonymity, and prevent various attacks, such as replay attack, stolen-verifier attack, password guessing attack, insider attack, and man-in-the-middle attack. In 2009, Goriparthi et al. proposed a scheme [27] which is improved from Das et al.'s protocol [2] and can avoid the weakness existing in Chou et al.'s [5] (also modified from Das et al.'s). Goriparthi et al.'s protocol is also a smart card based password authentication protocol and bases on bilinear pairings. They claimed that their protocol is secure and can withstand replay attack and insider attack. In the same year, Wang et al. [31] proposed an improvement on Das et al.'s protocol [2]. Their scheme is a smart card based password authentication protocol as well and operates with secure one-way hash function. They claimed that their protocol is secure and can achieve mutual authentication. Also in 2009, Hölbl et al. [40] improved two identity-based authentication protocols, Hsieh et al. [1] and Tseng et al. [8]. Their protocols are neither password-based nor smart card based protocols. They are identity-based public key cryptosystem and operate with ElGamal signature scheme. Hölbl et al. claimed the protocols are not only efficient but also secure. Although all of the above schemes mentioned claimed that they are secure; however, in this paper, we found some threats existing in them, correspondingly. We will show them in turn.

The remainder of this paper is organized as follows: In Section 2, we review and attack on the protocol of Bindu et al. [14]. Then, we review and attack on the protocols of Goriparthi et al. [27], Wang et al. [31], and Hölbl et al. [40] in Section 3 through 5, respectively. Finally, a conclusion is given in Section 6.

2. Review and attack on the improvement of Bindu et al.

In this section, we first review Bindu et al.'s scheme [14] in Section 2.1 then show the insider attack launched by an insider who is supposed to have obtained another legal user's smart card in Section 2.2.

2.1 Review of Bindu et al.'s scheme

There are three phases in Bindu et al.'s scheme: the registration phase, the login phase and the authentication phase.

In the registration phase, the server S issues to legal user i a smart card which contains m_i and I_i, where m_i=H($ID_i \oplus s$)$\oplus$H(s)$\oplus$H(PW_i), I_i=H($ID_i \oplus s$)$\oplus s$, and s is S's secret key.

When i wants to login to S, he starts the login phase by computing $r_i=g^x$ (x is a random number chosen by i), $M=m_i \oplus$H(PW_i), $U=M \oplus r_i$, $R=I_i \oplus r_i$= H($ID_i \oplus s$)$\oplus s \oplus r_i$, and $E_R[r_i, ID_i, T]$ (T is a timestamp, and $E_R[r_i, ID_i, T]$ is a ciphertext encrypted by the secret R). He then sends {U, T, $E_R[r_i, ID_i, T]$} to S.

In the authentication phase, after receiving {U, T, $E_R[r_i, ID_i, T]$} at timestamp T_s, S computes $R= U \oplus$H(s)$\oplus s$ $=M \oplus r_i \oplus$H(s)$\oplus s$ $=m_i \oplus$H(PW_i)$\oplus r_i \oplus$H(s)$\oplus s$ = H($ID_i \oplus s$) $\oplus$H(s)$\oplus$H(PW_i)$\oplus$H(PW_i)$\oplus r_i \oplus$H(s)$\oplus s$ = H($ID_i \oplus s$)$\oplus r_i \oplus s$, decrypts $E_R[r_i, ID_i, T]$, checks to see if $T_s - T$ is less than $\triangle$T, and compares R with H($ID_i \oplus s$)$\oplus s \oplus r_i$ to see if they are equal. If they are, he sends { T_s, $E_R[r_s, r_i+1, T_s]$} to i, where $r_s=g^y$ and y is a random number chosen by S. After that, i verifies the validity of the time interval, decrypts $E_R[r_s, r_i+1, T_s]$, and checks to see if r_i+1 is correct or not. If it is, S is authentic. Then, i sends {$E_{Kus}[r_s+1]$} to S, where $Kus=r_s^x=g^{xy}$. S decrypts the message and checks to see if the value of r_s+1 is correct or not. If it is, i is authentic.

2.2 Attack on Bindu et al.'s scheme

If C lost his smart card and the card is got by an insider E, E can impersonate C to log into S. We show the attack in the following.

For that C's smart card stores m_c=H($ID_c \oplus s$)$\oplus$H(s)$\oplus$H(PW_c) and I_c=H($ID_c \oplus s$)$\oplus s$, and E's smart card stores m_e=H($ID_e \oplus s$)$\oplus$H(s)$\oplus$H(PW_e) and I_e=H($ID_e \oplus s$)$\oplus s$, suppose E gets C's smart card but doesn't have the knowledge of PW_c, E can choose a random number x and computes $r_c=g^x$, $V= m_e \oplus I_e \oplus \mathrm{H}(PW_e)=\mathrm{H}(s)\oplus s$, $M=I_c\oplus V= \mathrm{H}(ID_c\oplus s)\oplus s\oplus \mathrm{H}(s)\oplus s = \mathrm{H}(ID_c\oplus s)\oplus \mathrm{H}(s)$ which equals $m_c\oplus \mathrm{H}(PW_c)$, $U=M\oplus r_c$, and $R= I_c\oplus r_c$. Then, E masquerades as C by sending $\{U, T, \mathrm{E}_R[r_c, ID_c, T]\}$ to S. After receiving the message, S computes $R=U\oplus \mathrm{H}(s)\oplus s$ and compares R with $\mathrm{H}(ID_c\oplus s)\oplus s \oplus r_c$. If they are equal, S sends C the message $\{ T_s, \mathrm{E}_R[r_s, r_c+1, T_s]\}$. E intercepts the message, decrypts $\mathrm{E}_R[r_s, r_c+1, T_s]$, and uses r_s to compute $Kus=r_s^x=g^{xy}$. E then can send a correct message $\{\mathrm{E}_{Kus}[r_s+1]\}$ to S, to let S authenticate him as C. In other words, insider E can successfully launch an insider attack if the user's smart card is lost.

More clarity, we demonstrate why $R=U\oplus \mathrm{H}(s)\oplus s$ is equal to $\mathrm{H}(ID_c\oplus s)\oplus s\oplus r_c$ by the following equations.

$$
\begin{aligned}
R &= U\oplus \mathrm{H}(s)\oplus s \\
&= M\oplus r_c\oplus \mathrm{H}(s)\oplus s \quad \cdots\cdots \because\ U=M\oplus r_c \\
&= I_c\oplus V\oplus r_c\oplus \mathrm{H}(s)\oplus s \quad \cdots\cdots \because\ M=I_c\oplus V \\
&= \mathrm{H}(ID_c\oplus s)\oplus s\oplus V\oplus r_c\oplus \mathrm{H}(s)\oplus s \quad \cdots\cdots \because\ I_c=\mathrm{H}(ID_c\oplus s)\oplus s \\
&= \mathrm{H}(ID_c\oplus s)\oplus s\oplus \mathrm{H}(s)\oplus s\oplus r_c\oplus \mathrm{H}(s)\oplus s \quad \cdots\cdots \because\ V=\mathrm{H}(s)\oplus s \\
&= \mathrm{H}(ID_c\oplus s)\oplus s\oplus r_c
\end{aligned}
$$

3. Review and attack on the protocol of Goriparthi et al.

In this section, we first review Goriparthi et al.'s scheme [27] in Section 3.1 then we demonstrate that it is vulnerable to the DoS attack on the password change phase which can make the password invalid after their protocol run in Section 3.2.

3.1 Review of Goriparthi et al.'s scheme

In the password change phase of Goriparthi et al.'s protocol, when client C wants to change his password *PW*, he keys his *ID* and *PW* to his smart card. The smart card verifies *ID* (without verifying his password *PW*) to see if it is correct. If it is, the smart card will subsequently receive a new password *PW** submitted by C and compute $Reg^*_{ID}= Reg_{ID} - \mathrm{h}(PW)+\mathrm{h}(PW^*)= s\cdot \mathrm{h}(ID)+\mathrm{h}(PW^*)$, where $Reg_{ID}= s\cdot \mathrm{h}(ID) + \mathrm{h}(PW)$ is stored in C's smart card, $\mathrm{h}(\cdot)$ is a map-to-point hash function $\mathrm{h}:\{0,1\}^*\rightarrow G_1$, and G_1 is a group on an elliptical curve. Finally, the smart card will replace Reg_{ID} with Reg^*_{ID}.

3.2 Attack on Goriparthi et al.'s scheme

In the protocol, assume that there is an attacker temporarily gets access to C's smart card. He randomly selects two passwords PW' and PW'' as the old and the new ones, respectively. The smart card will then compute $Reg'_{ID} =Reg_{ID} - \mathrm{h}(PW') +\mathrm{h}(PW'')= s\cdot \mathrm{h}(ID)+\mathrm{h}(PW)-\mathrm{h}(PW') +\mathrm{h}(PW'')$ and replace Reg_{ID} with Reg'_{ID}. This would make C's password *PW* invalid.

4. Review and attack on the protocol of Wang et al.

In this section, we first review Wang et al.'s scheme [31] in Section 4.1, then demonstrate that it is vulnerable to the DoS attack on the password change phase which can make the password invalid after the protocol run in Section 4.2.

4.1 Review of Wang et al.'s protocol

In Wang et al.'s protocol , C inserts his smart card, keys *PW*, and requests to change the password *PW* to a new one *PW**. Then, the smart card computes $N_i^* = N_i \oplus \mathrm{H}(PW) \oplus \mathrm{H}(PW^*)$ and replaces N_i with N_i^*, where $N_i = \mathrm{H}(PW_i) \oplus \mathrm{H}(x)$ is stored in C's smart card, PW_i is chosen by the user when he registers at the remote server S, and x is S's secret key.

4.2 Attack on Wang et al.'s protocol

Obviously, this protocol also exits the same security loophole as does in [27]. Since if an attacker temporarily gets access to C's smart card and reads the value of N_i, he can use two random values PW' and PW'' to compute $N_i' = N_i \oplus \mathrm{H}(PW') \oplus \mathrm{H}(PW'')$ and replace N_i with N_i'. From then on, client C can never pass the authentication and the attack succeeds.

5. Review and attack on the protocol of Hölbl et al.

Hölbl et al. [40] proposed two improvements of two-party key agreement protocols. In the following, we first briefly review then present our attack on both of their protocols, respectively.

5.1 Review of Hölbl et al.'s first protocol

Hölbl et al.'s first protocol consists of three phases: the system setup phase, the private key extraction phase, and the key agreement phase.

In the system setup phase, KGC chooses a random number x_s and keeps it secret. He computes $y_s = g^{x_s}$ and publishes it.

In the private key extraction phase, with each user having his identity *ID*, KGC selects a random number k_i, and calculates i's private key $v_i = I_i k_i + x_s u_i$ (mod p-1) and public key $u_i = g^{k_i}$ (mod p), where $I_i = \mathrm{H}(ID_i)$.

In the key agreement phase, user A chooses a random number r_a, computes $t_a = g^{r_a}$, and then sends { u_a, t_a, ID_a } to user B. After receiving { u_a, t_a, ID_a }, B chooses a random number r_b , calculates $t_b = g^{r_b}$, and then sends { u_b, t_b, ID_b } back to A. Finally, A and B can compute their common session key, $K=(u_b^{I_b}\cdot y_s^{u_b}\cdot t_b)^{(v_a+r_a)}= g^{(v_b+r_b)\cdot(v_a+r_a)}$ and $K=(u_a^{I_a}\cdot y_s^{u_a}\cdot t_a)^{(v_b+r_b)}=g^{(v_a+r_a)\cdot(v_b+r_b)}$, respectively, where I_a=H(ID_a) and I_b=H(ID_b).

5.2 Attack on Hölbl et al.'s first protocol

Assume that an insider C calculates I_c=H(ID_c) and q=gcd(I_c, u_c), and computes $w=I_c/q$, $z=u_c/q$, and $j=v_c/q$, where v_c is C's private key. Hence, gcd(w, z)=1. Then, he can use the extended Euclid's algorithm to find α and β both satisfying that $\alpha\cdot w+\beta\cdot z=1$. As a result, he can obtain both x_s and k_c, since $v_c=1\cdot j_c\cdot q_c=(\alpha\cdot w+\beta\cdot z)\cdot j_c\cdot q_c =(\alpha\cdot I_c/q+\beta\cdot u_c/q)\cdot j\cdot q=(\alpha\cdot I_c+\beta\cdot u_c)\cdot j=I_c\cdot(\alpha\cdot j)+(\beta\cdot j)\cdot u_c$ and $v_c=I_c\cdot k_c+x_s\cdot u_c$, where x_s is KGC's secret key and k_c is a random number selected by KGC satisfying $u_c=g^{k_c}$. More clearly, the value x_s he obtains is equal to $\beta\cdot j$.

After obtaining x_s, C can deduce any user's private key in the same manner. As an example, in the following, we demonstrate how C can deduces i's private key, k_i. C calculates I_i=H(ID_i) and q_i=gcd(I_i, u_i), computes $w_i=I_i/q_i$ and $z_i=u_i/q_i$, and then uses the extended Euclid's algorithm to compute γ and ε satisfying that $\gamma\cdot w_i+\varepsilon\cdot z_i=1$. Finally, since $v_i=1\cdot j_i\cdot q_i =(\gamma\cdot w_i+\varepsilon\cdot z_i)\cdot j_i\cdot q_i =(\gamma\cdot I_i/q_i+\varepsilon\cdot u_i/q_i)\cdot j_i\cdot q_i =(\gamma\cdot I_i+\varepsilon\cdot u_i)\cdot j_i =I_i\cdot(\gamma\cdot j_i)+(\varepsilon\cdot j_i)\cdot u_i$ and $v_i =I_i\cdot k_i+x_s\cdot u_i$, he can calculate $j_i=x_s/\varepsilon$ and thus obtains i's private key by computing $v_i=\cdot j_i\cdot q_i$. With the knowledge of i's private key, insider C can impersonate user i to communicate with any other legal user. That is, to a minimum, an insider attack exists.

5.3 Review of Hölbl et al.'s second protocol

Hölbl et al.'s second protocol consists of three phases: the system setup phase, the private key extraction phase, and the key agreement phase.

The system setup phase of this protocol is the same as the one in the first protocol.

In the private key extraction phase, with each user having his identity ID, KGC selects a random number k_i, and calculates i's private key $v_i=k_i+x_s\cdot$H(ID_i, u_i) and public key $u_i=g^{k_i}$.

In the key agreement phase, user A chooses a random number r_a, computes $t_a= g^{r_a}$, and then sends { u_a, t_a, ID_a } to user B. After receiving { u_a, t_a, ID_a }, B chooses a random number r_b , calculates $t_b= g^{r_b}$, and then sends { u_b, t_b, ID_b } to A. Finally, A and B can compute their common session key, $K= (u_b\cdot y_s^{\mathrm{H}(ID_b,u_b)}\cdot t_b)^{(v_a+r_a)} = g^{(v_b+r_b)\cdot(v_a+r_a)}$ and $K= (u_a\cdot y_s^{\mathrm{H}(ID_a,u_a)}\cdot t_a)^{(v_b+r_b)} = g^{(v_a+r_a)\cdot(v_b+r_b)}$, respectively.

5.4 Attack on Hölbl et al.'s second protocol

Likewise, we can launch the same attack, as do in the first one, on this scheme. Since gcd(1, H(ID_c, u_c))=1, an insider C can use the extended Euclid's algorithm to find α and β both satisfying that $\alpha \cdot 1+\beta \cdot$H($ID_c$, u_c) =1. And since $v_c=k_c+x_s \cdot$H(ID_c, u_c) and 1=(k_c/v_c)$\cdot$1+(x_s/v_c)$\cdot$H(ID_c, u_c), he can obtain both x_s and k_c by letting $x_s=\beta \cdot v_c$ and $k_c=\alpha \cdot v_c$, where v_c is C's private key, x_s is KGC's secret key and k_c is a random number selected by KGC satisfying $u_c=g^{k_c}$. Consequently, similar to the result as shown in the attack of the first protocol, insider C can impersonate user i to communicate with any other legal user. That is, to the minimum, there exists an insider attack in their second scheme. Therefore, the protocol fails.

6. Conclusion

We have analyzed the protocols of Bindu et al. [14], Goriparthi et al. [27], Wang et al. [31], and Hölbl et al. [40]. After analyses, we found that Bindu et al.'s suffers from the insider attack if the smart card is lost, Goriparthi et al.'s and Wang et al.'s can't withstand the DoS attack on the password change phase which can make the password invalid after the protocol run, and Hölbl et al.'s are vulnerable to the insider attack since a malevolent legal user can deduce KGC's secret key x_s.

References

[1] B. T. Hsieh, H. M. Sun, T. Hwang, C. T. Lin, "*An Improvement of Saeednia's Identity-based Key Exchange Protocol*", Information Security Conference 2002, pp. 41-43, 2002.

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

[3] H. Y. Chien, C. H. Chen, "A Remote Password Authentication Preserving User Anonymity," *Proceedings of the 19th International Conference on Advanced Information Networking and Applications* (AINA '05), Vol.2, pp. 245-248, March 2005.

[4] J. S. Chou, M. D. Yang, G. C. Lee, "Cryptanalysis and improvement of Yang-Wang password authentication schemes", http://eprint.iacr.org/2005/466, December 2005.

[5] J.S. Chou, Y. Chen, J. Y. Lin, "Improvement of Das et al.'s remote userauthentication scheme", http://eprint.iacr.org/2005/450.pdf, December 2005.

[6] M. Peyravian, C. Jeffries, "Secure remote user access over insecure networks", *Computer Communications*, Vol. 29, No. 5, pp. 660-667, March 2006.

[7] I. E. Liao, C. C. Lee, M. S. Hwang, "A password authentication scheme over

insecure networks”, *Journal of Computer and System Sciences*, Vol. 72, No. 4, pp. 727-740, June 2006.

[8] Y. M. Tseng, “An Efficient Two-Party Identity-Based Key Exchange Protocol”, *Informatica*, Vol. 18, No. 1, pp. 125-136, January 2007.

[9] J. Nam, Y. Lee, S. Kim, D. Won, “Security weakness in a three-party pairing-based protocol for password authenticated key exchange”, *Information Sciences*, Vol. 177, No. 6, pp. 1364-1375, March 2007.

[10] H. R. Chung, W. C. Ku, “Three weaknesses in a simple three-party key exchange protocol”, *Information Sciences*, Vol. 178, No. 1-2, pp. 220-229, January 2008.

[11] T. H. Chen, W. B. Lee, “A new method for using hash functions to solve remote user authentication”, Computers *& Electrical Engineering*, Vol. 34, No. 1, pp. 53-62, January 2008.

[12] H. B. Chen, T. H. Chen, W. B. Lee, C. C. Chang, “Security enhancement for a three-party encrypted key exchange protocol against undetectable on-line password guessing attacks”, *Computer Standards & Interfaces*, Vol. 30, No. 1-2, pp. 95-99, January 2008.

[13] H. Guo, Z. Li, Y. Mu, X. Zhang, “Cryptanalysis of simple three-party key exchange protocol”, *Computers & Security*, Vol. 27, No. 1-2, pp. 16-21, March 2008.

[14] C. S. Bindu, P. C. S. Reddy, B. Satyanarayana, “Improved remote user authentication scheme preserving user anonymity”, *International Journal of Computer Science and Network Security*, Vol. 8, No. 3, pp. 62-65, March 2008.

[15] Y. Lee, J. Nam, D. Won, “Vulnerabilities in a remote agent authentication scheme using smart cards”, *LNCS: AMSTA*, Vol. 4953, pp. 850-857, April 2008.

[16] W. S. Juang, S. T. Chen, H. T. Liaw, “Robust and efficient password-authenticated key agreement using smart cards”, *IEEE Transactions on Industrial Electronics*, Vol. 55, No. 6, pp. 2551-2556, June2008.

[17] W. S. Juang, W. K. Nien, “Efficient password authenticated key agreement using bilinear pairings”, *Mathematical and Computer Modelling*, Vol. 47, No. 11-12, pp. 1238-1245, June 2008.

[18] J. Y. Liu, A. M. Zhou, M. X. Gao, “A new mutual authentication scheme based on nonce and smart cards”, *Computer Communications*, Vol. 31, No. 10, pp. 2205-2209, June 2008.

[19] M. Hölbl, T. Welzer, B. Brumen, “Improvement of the Peyravian-Jeffries’s user authentication protocol and password change protocol”, *Computer Communications*, Vol. 31, No. 10, pp. 1945-1951, June 2008.

[20] J. L. Tsai, “Impersonation attacks on Rhee et al.’s authentication scheme”, *http://dtim.mis.hfu.edu.tw/2008/paper/C044.pdf*, June 2008.

[21] J. L. Tsai, "Efficient multi-server authentication scheme based on one-way hash function without verification table", *Computers & Security,* Vol. 27, No. 3-4, pp. 115-121, May-June 2008.

[22] E. J. Yoon, K. Y. Yoo, "Improving the novel three-party encrypted key exchange protocol", *Computer Standards & Interfaces*, Vol. 30, No. 5, pp. 309-314, July 2008.

[23] R. C. Phan, W. C. Yau, B. M. Goi, "Cryptanalysis of simple three-party key exchange protocol (S-3PAKE)", *Information Sciences,* Vol. 178, No. 13, pp. 2849-2856, July 2008.

[24] C. C. Chang, J. S. Lee, T. F. Cheng, "Security design for three-party encrypted key exchange protocol using smart cards", ACM Proceedings of the 2nd international conference on Ubiquitous information management and communication, pp. 329-333, 2008.

[25] T. Xiang, K. Wong, X. Liao, "Cryptanalysis of a password authentication scheme over insecure networks", *Computer and System Sciences*, Vol. 74, No. 5, pp. 657-661, August 2008.

[26] G. Yang, D. S. Wong, H. Wang, X. Deng, "Two-factor mutual authentication based on smart cards and passwords", *Journal of Computer and System Sciences*, Vol. 74, No. 7, pp.1160-1172, November 2008.

[27] T. Goriparthi, M. L. Das, A. Saxena, "An improved bilinear pairing based remote user authentication scheme", *Computer Standards & Interfaces*, Vol. 31, No. 1, pp. 181-185, January 2009.

[28] H. S. Rhee, J. O. Kwon, D. H. Lee, "A remote user authentication scheme without using smart cards", *Computer Standards & Interfaces*, Vol. 31, No. 1, pp. 6-13, January 2009.

[29] Y. Liao, S. S. Wang, "A secure dynamic ID based remote user authentication scheme for multi-server environment", *Computer Standards & Interfaces,* Vol. 31, No. 1, pp. 24-29, January 2009.

[30] J. Munilla, A. Peinado, "Security flaw of Hölbl et al.'s protocol", *Computer Communications*, Vol. 32, No. 4, pp.736-739, March 2009.

[31] Y. Y. Wang, J. Y. Liu, F. X. Xiao, J. Dan, "A more efficient and secure dynamic ID-based remote user authentication scheme", *Computer Communications*, Vol. 32, No. 4, pp. 583-585, March 2009.

[32] H. C. Hsiang, W. K. Shih, "Weaknesses and improvements of the Yoon–Ryu–Yoo remote user authentication scheme using smart cards", *Computer Communications*, Vol. 32, No. 4, pp. 649-652, March 2009.

[33] D. Z. Sun, J. P. Huai, J. Z. Sun, J. X. Li, "Cryptanalysis of a mutual authentication scheme based on nonce and smart cards", *Computer*

Communications, Vol. 32, No. 6, pp. 1015-1017, April 2009.

[34] S. K. Kim , M. G. Chung, “More secure remote user authentication scheme”, *Computer Communications*, Vol. 32, No. 6, pp. 1018-1021, April 2009.

[35] H. R. Chung, W. C. Ku, M. J. Tsaur, “Weaknesses and improvement of Wang et al.'s remote user password authentication scheme for resource-limited environments”, *Computer Standards & Interfaces*, Vol. 31, No. 4, pp. 863-868, June 2009.

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

[37] J. H. Yang, C. C. Chang, “An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem”, *Computers & Security*, Vol. 28, No. 3-4, pp. 138-143, May-June 2009.

[38] M. S. Hwang, S. K. Chong, T. Y. Chen, “DoS-resistant ID-based password authentication scheme using smart cards”, *Journal of Systems and Software*, In Press, Available online 12 August 2009.

[39] H.C. Hsiang, W.K. Shih, “Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment”, *Computer Standards & Interfaces*, Vol. 31, No. 6, pp. 1118-1123, November 2009.

[40] M. Hölbl, T. Welzer, “Two improved two-party identity-based authenticated key agreement protocols”, *Computer Standards & Interfaces*, Vol. 31, No. 6, pp. 1056-1060, November 2009.

[41] C. T. Li, M. S. Hwang, “An efficient biometrics-based remote user authentication scheme using smart cards”, *Journal of Network and Computer Applications*, Vol. 33, No. 1, pp. 1-5, January 2010.