Contents lists available at ScienceDirect

Computer Communications

journal homepage: www.elsevier.com/locate/comcom

Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'

Muhammad Khurram Khan [a,*], Soo-Kyun Kim [b], Khaled Alghathbar [a,c]

[a] Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia
[b] Department of Game Engineering, PaiChai University, Republic of Korea
[c] Information Systems Department, College of Computer and Information Sciences, King Saud University, Saudi Arabia

ARTICLE INFO

Article history:
Available online xxxx

Keywords:
Authentication
Security
Smart card
Cryptanalysis
Password

ABSTRACT

Remote user authentication is a method, in which remote server verifies the legitimacy of a user over an insecure communication channel. Currently, smart card-based remote user authentication schemes have been widely adopted due to their low computational cost and convenient portability for the authentication purpose. Recently, Wang et al. proposed a dynamic ID-based remote user authentication scheme using smart cards. They claimed that their scheme preserves anonymity of user, has the features of strong password chosen by the server, and protected from several attacks. However, in this paper, we point out that Wang et al.'s scheme has practical pitfalls and is not feasible for real-life implementation. We identify that their scheme: does not provide anonymity of a user during authentication, user has no choice in choosing his password, vulnerable to insider attack, no provision for revocation of lost or stolen smart card, and does provide session key agreement. To remedy these security flaws, we propose an enhanced authentication scheme, which covers all the identified weaknesses of Wang et al.'s scheme and is more secure and efficient for practical application environment.

1. Introduction

With the large-scale proliferation of internet and network technologies, smart card-based authentication schemes have been widely deployed to verify the legitimacy of remote user's login request. In remote authentication process, a remote server authenticates a registered user based on his secret credentials. In traditional authentication schemes, the server or system has to store a password table to save passwords of all the registered users of the system. In 1981, Lamport presented a remote user authentication scheme using password tables [1]. Lamport claimed that his scheme is secure even if an adversary eavesdrops on the communication between a user and remote system. In 2000, Hwang and Li [2] identified that Lamport's scheme is susceptible to the risks of hacking and modifying the password table. Thus, Hwang and Li proposed a remote user authentication scheme without using the password table, which was based on El Gamal public key encryption method [3]. Until now, there have been ample of remote user authentication schemes published in the literatures and each published scheme has its own merits and demerits [4–28].

A common feature among most of the published schemes is that the user's identity is static in all the transaction sessions, which may leak some information about that user and can create risk of ID-theft during the message transmission over an insecure channel. To overcome this risk, Das et al. [16] proposed a dynamic ID-based remote user authentication scheme. Their scheme is novel, because dynamic identity for each transaction session can avoid the risk of id-theft or impersonation. Their scheme was based on one way hash functions and user can freely choose and change passwords without any hassle. Das et al. claimed that their scheme is secured against replay, forgery, guessing, insider, and stolen verifier attacks. Unfortunately, later on, some researchers revealed that their scheme is not as much secured as they claimed and has some drawbacks.

First, Awashti [17] identified that Das et al.'s scheme is completely insecure and works like an open channel. Awashti also concluded that Das et al's scheme does not full fill the basic needs of authentication schemes. Later on, Chien and Chen [23] pointed out that Das et al.'s scheme failed to protect the anonymity of a user and then proposed an improved remote authentication scheme, which preserves user anonymity. Furthermore, Ku and Chang also revealed some more weaknesses of Das et al.'s scheme [18]. Ku and Chang demonstrated that Das et al.'s scheme is susceptible to the impersonation attack, in which an intruder can

[*] Corresponding author.
E-mail address: mkhurram@ksu.edu.sa (M.K. Khan).

0140-3664/$ - see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.comcom.2010.02.011

easily get login into the remote system. Furthermore, Ku and Chang pointed out that Das et al.'s scheme has risk of insider attack and cannot be easily repaired [18].

Liao et al. [25] also analyzed the security of Das et al.'s scheme and showed that their scheme is vulnerable to guessing attack and does not provide mutual authentication. To overcome the security pitfalls of Das et al.'s scheme, Liao et al. proposed an enhancement to cope with the aforementioned security flaws. However, later on, Misbahuddin and Bindu [26] identified that the security patch of Liao et al. is still not secure and their scheme cannot withstand impersonation attack, reflection attack and is completely insecure as a user can successfully log on to a remote system with a random password.

Afterward, Liao and Wang [27] presented a dynamic ID-based remote user authentication scheme for multi-server environment. Their scheme attempts to preserve user's anonymity and uses simple hash functions. Liao and Wang claimed that their scheme achieves mutual authentication and provides session key agreement. Later on, Hsiang and Shih [28] identified that Liao and Wang's scheme is vulnerable to insider's attack, masquerade attack, server spoofing attack, registration center spoofing attack and is not reparable.

More recently, Wang et al. [19] showed that Das et al.'s scheme is completely insecure for its independence of using passwords, does not provide mutual authentication, and cannot resist fake-server attack. Wang et al. proved that Das et al.'s scheme performs only unilateral authentication (only client authentication) and remote user has no information about the authenticity of the remote authentication system, thus Das el al.'s scheme is susceptible to the server spoofing attack. Wang et al. then proposed a dynamic ID-based remote user authentication scheme and claimed that their scheme is more efficient and secure than Das et al.'s scheme.

However, in this paper, firstly, we show that Wang et al.'s scheme suffers from attacks and have some practical security pitfalls. Moreover, we discuss that their scheme has weaknesses and is insecure, inefficient, and infeasible for implementation in the real environment. To overcome the security flaws of Wang et al.'s scheme, we propose an improved dynamic ID-based remote user authentication scheme which provides the missing security provisions that are necessary for a practical and real-life smart card-based authentication scheme.

Rest of the paper is organized as follows: Section 2 briefly reviews Wang et al.'s scheme, Section 3 elaborates on the weaknesses and security pitfalls of their scheme, Section 4 presents our proposed improved scheme, Section 5 discusses the security analysis of our scheme, Section 6 provides security features of the presented scheme, and at the end, Section 7 concludes this paper.

2. Review of Wang et al.'s scheme

In this section, we briefly review Wang et al.'s scheme which consists of four phases namely; registration phase, login phase, verification phase, and password-change phase.

A. Registration phase

When a user U_i wants to perform his registration, he requests remote sever with his chosen ID_i. The remote server performs the following steps:

(i) Computes $N_i = h(pw_i) \oplus h(x) \oplus ID_i$, where x is the secret key of remote server S, is the password for U_i chosen by S.

(ii) S personalizes the smart card with parameters $\{h(.), N_i, y\}$ where y is the secret code of remote server stored in smart card of each registered user.

(iii) S returns smart card and pw_i to the registered user.

B. Login phase

When U_i wants to login into S, he inserts his smart card in the terminal and keys in his identity ID_i and pw_i password, then the smart card performs the following steps:

(i) Computes $CID_i = h(pw_i) \oplus h(N_i \oplus y \oplus T) \oplus ID_i$, where T is the current time stamp of the user's U_i machine.

(ii) Now, U_i sends login message $m = \{ID_i, CID_i, N_i, T\}$ to the remote authentication server S for performing the authentication process.

C. Verification phase

Upon receiving the login message m, the authentication server S performs the following steps:

(i) Checks the validity of time stamp with the current date and time T'. If $(T' - T) \leqslant \Delta T$ holds, S accepts the login request of U_i, otherwise the login request is rejected.

(ii) Computes $h'(pw_i) = CID_i \oplus h(N_i \oplus y \oplus T) \oplus ID_i$.

(iii) Computes $ID_i = h'(pw_i) \oplus h(x) \oplus N_i$ and verifies whether it is equal to ID_i or not. If it holds, the remote server S accepts the login request, otherwise login request is rejected.

(iv) Computes $a' = h(h'(pw_i) \oplus y \oplus T')$ and sends message $\{a', T'\}$ to U_i.

(v) After receiving the response message from S at time T^*, U_i checks the validity of time stamp whether $(T^* - T) \geqslant \Delta t$, if not, U_i computes and $a = h(h(pw_i) \oplus y \oplus T')$ compares a with the received a'. If it is valid, U_i confirms the authenticity of remote server S, otherwise terminates the operation.

D. Password-change phase

When U_i wants to change his password, he inserts smart card into the terminal device, keys in the password pw_i, and requests to change the password to new one, i.e. pw_{new}. Then, the smart card computes $N_i^* = N_i \oplus h(pw_i) \oplus h(pw_{new})$ and replaces N_i the with the new N_i^* in the smart card.

3. Comments on security pitfalls of Wang et al.'s scheme

(i) In wang et al.'s scheme, the password is chosen by the remote server S without the consent of U_i and he has no choice of choosing his own password, which is not a case in real-life applications, e.g. email subscription and online banking, etc. Secondly, pw_i the chosen by server could be long and random (for example, 1024 or 2048 bits), which might be difficult for a registered user U_i to remember easily and it is most likely that U_i may forget this long and random password if he is not frequently using the system. Secondly, Wang et al.'s scheme has pitfall of insider's attack of S by privileged user who has come to know the password of U_i and can misuse the system in future [22].

(ii) Wang et al.'s scheme does not preserve the anonymity of U_i. In the verification phase, ID_i and CID_i are transmitted to the authentication server S over insecure channel in the login message $m = \{ID_i, CID_i, N_i, T\}$. In some authentication scenarios, e.g. electronic voting or secret online-order placement, it is very important to preserve the privacy of a user because an adversary sniffing the communication channel can eavesdrop the communication parties involve in the authentication process and can easily analyze the transaction being performed by U_i [27]. Thus, Wang et al.'s scheme fails in providing the privacy and anonymity of U_i during the authentication phase.

(iii) Wang et al.'s scheme does not have provision to provide the session key and its agreement between the U_i and S. It is pertinent that after the successful authentication process, both parties will communicate some secret messages, which should be encrypted to provide the confidentiality and secrecy of transmitted data, e.g. online money transfer or secure-order placement. For providing this confidentiality a shared-session key is required, but in Wang et al.'s scheme, U_i and S will need to perform some other means of generating and sharing the session key, which will undoubtedly create computational, and communication overhead and delay in the process.

(iv) It is one of the requirements of smart card-based authentication schemes that in case of lost of cards, there should be provision in the system for invalidating the further use of lost smart card, otherwise an adversary can impersonate valid registered user [24]. Through keeping record of valid card identifier of each registered user, the authentication system can distinguish the valid card from the invalid one. Unfortunately, Wang et al.'s scheme overlooked this feature and there is no prerequisite to revoke the lost smart card. This flaw would become more catastrophic if an adversary has got lost smart card and has revealed password of a valid user by any means to login into the system for performing secure transaction, e.g. online banking and e-commerce, etc. Thus, their scheme becomes fail in providing the important feature of smart card-based authentication for revoking the lost smart cards without changing the user's identities [24].

4. Proposed authentication scheme

In this section, we propose an efficient and secure dynamic ID-based authentication scheme to overcome the weaknesses of Wang et al.'s scheme. Due to its simplicity, computational efficiency and proven security, we use simple Hash functions to propose our scheme. Our presented scheme consists of five different phases namely; registration phase, login phase, authentication phase, password-change phase, and revocation of lost or stolen smart card phase. These phases work as follows:

A. Registration phase

This phase is invoked whenever user U_i initially registers or re-registers to the authentication server S. Suppose x and y are two secret keys of S, and y is used to provide user anonymity during the authentication phase. Let N denotes the number of times a user U_i registers by authentication server S. This value of N is used to revoke a smart card in case of theft or stolen and its value is stored in user's U_i account database on the authentication server S. The secret keys are securely stored in the authentication server S. We recommend system implementers to use high security measures, e.g. strong administration policies and procedures, firewalls, intrusion detection softwares to protect the sensitive data on server. We assume that stringent security measures are implemented at the remote server S to make authentication system secure against different kind of attacks and adversary cannot hack the secret information such as ID_i and secret keys x and y stored in the server. The following steps are performed to complete the registration phase:

(i) U_i chooses his ID_i and pw_i and generates a random number r and computes $RPW = h(r\|pw_i)$.
(ii) U_i submits his ID_i and RPW to the S over a secure channel.
(iii) S checks the registration credentials of U_i and checks whether his chosen ID_i is already in the database or not. If ID_i already exists in the database, S intimates U_i to choose another ID_i. In addition, S checks the registration record of U_i and if U_i is a new user then S sets value of $N = 0$, otherwise if U_i is re-registering in the system then S sets N=*1* and stores values ID_i and N in the database.
(iv) S computes $J = h(x\|IDU)$ where $IDU = (ID_i\|N)$.
(v) S computes $L = J \oplus RPW$.
(vi) Now, S issues smart card to U_i which contains values of L and y over a secure channel.
(vii) U_i securely stores random number r in the smart card and does not need to remember its value. This step completes the registration process.

B. Login phase

When U_i wants to login into S, he inserts his smart card in the terminal and inputs his ID_i and pw_i. Smart card performs the following steps:

(i) Computes $RPW = h(r\|pw_i)$ and $J = L \oplus RPW$, where random number r is securely pre-stored in the smart card.
(ii) Acquires the current timestamp T_i and computes $C_1 = h(T_i\|J)$
(iii) Generates a random number d and computes an anonymous ID of U_i by $AID_i = ID_i \oplus h(y\|T_i\|d)$.
(iv) At the end of login phase, U_i sends login message $m = \{AID_i, T_i, d, C_1\}$ to S for the authentication process.

C. Authentication phase

Upon receiving the login request message $m = \{AID_i, T_i, d, C_1\}$, the authentication server S verifies its authenticity by the following steps:

(i) Verifies the validity of time interval between T_i and T'. If $(T' - T_i) \geqslant \Delta T$, then S rejects the login request and intimates U_i about the timestamp expiry and refuse the further operations. Here ΔT denotes the expected valid time interval for transmission delay and T' denotes receiving timestamp of login message m.
(ii) Computes $ID_i = AID_i \oplus h(y\|T_i\|d)$ and validates if ID_i is a valid user's ID then performs further operations, otherwise terminates the operation and informs U_i about it.
(iii) Checks the value of N in the database and computes $IDU = (ID_i\|N)$
(iv) Computes $J = h(x\|IDU)$ and checks whether $h(T_i\|J) \overset{?}{=} C_1$. If they are equal, it means U_i is an authentic user and S accepts the login request, otherwise the login request is rejected and user is informed about the decision.
(v) For mutual authentication, S acquires current timestamp T_s and computes $C_2 = h(C_1 \oplus J \oplus T_s)$ and then sends the mutual authentication message $\{C_2, T_s\}$ to U_i.
(vi) Upon receiving the mutual authentication message, U_i verifies the time interval between T_s and T'', where T'' is the time stamp when mutual authentication message was received. If $(T'' - T_s) \geqslant \Delta T$, then U_i rejects this message and terminates the operation, otherwise step (vii) is performed.
(vii) U_i checks whether $h(C_1 \oplus J \oplus T_s) \overset{?}{=} C_2$. if this holds, U_i authenticates S otherwise login request is given up by U_i.
(viii) Now, U_i and S share the symmetric session key $S_k = h(C_2 \oplus J)$ for performing further operations during a session.

D. Password-change phase

In the password-change phase, when a user wants to change his password pw_i with a new password pw_i', he inserts his smart card into the smart card reader and enters his ID and password. The smart card performs the following operations without interacting with remote server S:

(i) Computes $RPW^* = h(r \| pw_i)$ and $J^* = L \oplus RPW^*$. If $J \overset{?}{=} J^*$ hold, then U_i is allowed to change the password, otherwise password-change phase is terminated.
(ii) Computes $L = J \oplus RPW \oplus RPW^* \oplus h(r \| pw'_i)$ and replaces the old value of L with the new value. Now, the new password is successfully changed and this phase is terminated.

E. Lost smart card revocation phase

In case of lost or stolen of smart card, U_i requests S for its revocation. S first validates the U_i by his secret credentials, e.g. mother's maiden name, date of birth, national ID card number, or some other values known to U_i. After validating the revocation request, S changes the value of N to revoke the smart card. In every case of stolen or lost of smart card, the value of N is incremented by one. Later on, U_i can re-register to S without changing his ID_i. Here, U_i is strongly recommended not to use any previous values for his new registration, e.g. password and random number, otherwise anybody can impersonate U_i by using the same credentials previously saved in the lost or stolen smart card.

5. Security analysis and discussion

In this section, we provide an in-depth security analysis and discussion of the proposed scheme against its contemporaries. We prove that the presented scheme can withstand various possible attacks found in the current literature.

5.1. User anonymity

In our scheme, user's U_i anonymity is preserved at each login request. We compute an anonymous identity $AID_i = ID_i \oplus h(y \| T_i \| d)$ for U_i and this ID will be different at each login attempt because it is calculated with the time stamp T_i and random number d. The authentication server S can retrieve the value of ID_i because y, a secret shared key, is used to hide the user's U_i identity during the transmission of login message and only S can recover ID_i of the user U_i. Hence, in the presented scheme, an intruder or adversary cannot identify the person trying to login into the server. On the other hand, this feature is not present in [19].

5.2. Session key agreement

The proposed scheme provides session key agreement during the authentication phase. A session key $S_k = h(C_2 \oplus J)$ is shared between U_i and S. The value of C_2 is generated by C_1, time stamp T_i and T_s, and secret value of J. Thus, S_k will be different for each login session and cannot be replayed or reused after the expiration of login session. Hence, U_i and S can use S_k to securely perform encryption and decryption of subsequence messages. This property also full fills the requirements of forward secrecy of session key [27].

5.3. Secret key forward secrecy

In our scheme, even if the server's secret keys x and y happens to be compromised, an adversary cannot impersonate legitimate users by using the revealed keys, because he cannot compute AID_i and C_1, in the login message without knowledge of the user's ID_i, pw_i, r and IDU. Thus, the presented scheme preserves the forward secrecy of secret keys x and y.

5.4. Resistance to stolen verifier and insider attack

In real environment, it is a common practice that many users use same passwords to access different applications or servers for their convenience of remembering long passwords and use them easily. However, if the system manager or a privileged insider of S has known the passwords of U_i, he may try to impersonate U_i by accessing other servers where U_i could be a registered user. In our scheme, U_i registers to S by presenting $RPW = h(r \| pw_i)$ instead of pw_i and $h(pw_i)$. The value of r is not revealed to S so the insider of S cannot obtain pw_i by performing offline guessing attack on $h(r \| pw_i)$. Furthermore, the improved scheme does not maintain the verifier table and can resist the insider attack [22] and stolen verifier attack [2].

5.5. Securely chosen and update password

In the presented scheme, the legitimate smart card holder can freely choose and change his password without any hassle of contacting the remote server S. Any other person, even having stolen or lost smart card cannot change or update the password without knowing the corresponding valid ID_i and pw_i of the smart card holder.

5.6. Revocation of smart card

In our scheme, if a registered user's smart card is stolen or lost, he can request the remote server S to revoke his smart card for future use. The S can easily revoke the smart card by incrementing the value of N by one in its secure database. The value of N is protected in L, which is securely stored in the smart card. If an adversary who stole or theft smart card of U_i wants to login into S, he cannot pass the authentication phase as the value of N has already been incremented by one in the database of S and old smart card becomes useless for future use.

5.7. Mutual authentication

In the presented protocol, mutual authentication of U_i and S is performed to keep trust of both communication parties. According to the requirements of authentication, U_i should also authenticate remote server, otherwise server spoofing attack may occur which may cause catastrophic affect on both parties in case of financial transactions communication. In our scheme, S sends mutual authentication message $\{C_2, T_s\}$ to U_i to validate its authenticity. The value of C_2 is calculated by J which is only known to U_i and S and this message is infeasible to forge by a fake server to impersonate the S.

5.8. Resistance to denial of service attack

In our scheme, the value of $h(x \| IDU)$ is not stored directly in the smart card but it is combined with other values, e.g. random password $RPW = h(r \| pw_i)$ where r is a random number securely stored in smart card. It is obvious that the value of $h(x \| IDU)$ cannot be derived without having r and pw_i of the U_i. Furthermore, the passwords are not stored at the verification server, so the proposed scheme is robust against the DoS attack resulting from the verification table or the stolen smart card.

5.9. Replay and parallel session attack

Our scheme can withstand replay attack because the authenticity of two messages $m = \{AID_i, T_i, d, C_1\}$ and $\{C_2, T_s\}$ is verified by checking the freshness of time stamps T_i and T_s, respectively. On the other hand, the presented scheme resists parallel session attack, in which an adversary U_a may replay the authentication server's response message $\{C_2, T_s\}$ and user's login request message $m = \{AID_i, T_i, d, C_1\}$ within the threshold time ΔT. However,

Table 1
Security and performance comparison of proposed scheme with Wang et al.'s scheme.

Security features and performance	Proposed scheme	Wang et al. [19]
User's anonymity	Yes	No
Securely chosen password	Yes	No
Session key agreement	Yes	No
Revocation of smart card	Yes	No
Insider's attack	No	Yes
Computational operations in registration phase	2H	2H
Computational operations in login phase	3H	2H
Computational operations in authentication phase	5H	4H
Computational operations in password-change phase	2H	2H
Communication cost in login phase	$2\|h\|$	$\|h\|$
Communication cost in authentication phase	$\|h\|$	$\|h\|$

H, the computational cost of one hash operation; $|h|$, the bit-length of cryptographic hash value.

this attack will not work because of the different message computation structure of C_1 and C_2.

6. Security features and performance analysis of proposed scheme

In this section, we summarize the security features of our proposed scheme and compare its security and robustness with Wang et al.'s scheme [19]. Table 1 demonstrates that our scheme is more secure and robust than Wang et al.'s scheme and achieves more security features, which were not considered in their scheme and are essentially required in implementing a practical and universal remote user authentication scheme using smart cards.

Besides, it can be seen from Table 1 that our scheme needs only three more hashing operations than Wang et al.'s scheme. This is because our scheme provides user anonymity and session key computation, which require more hashing operations to enhance the security of authentication system. Hence, the computational overhead and communication cost of the proposed scheme are almost same as Wang et al.'s scheme with several enhanced security features, which are indispensable for implementing a reliable and trustworthy remote user authentication system.

7. Conclusion

In this paper, we have presented cryptanalysis and weaknesses of Wang et al.'s dynamic ID-based remote user authentication scheme. Firstly, we showed that Wang et al.'s scheme is vulnerable to insider attack, does not preserve anonymity of a user, long and random password for a user to remember, no provision for revocation of lost or stolen smart card and no support for session key agreement during authentication process. To overcome the identified problems, we have proposed an enhanced smart card-based authentication scheme, which improves all the identified weaknesses of Wang et al.'s scheme and is more secure and robust for real-life use.

References

[1] L. Lamport, Password authentication with insecure communication, Communications of the ACM 24 (11) (1981) 770–772.
[2] M.S. Hwang, L.H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (1) (2000) 28–30.
[3] T. El Gamal, A public-key cryptosystem and a signature scheme based on discrete logarithms, IEEE Transactions on Information Theory 31 (4) (1985) 469–472.
[4] S.J. Wang, J.F. Chang, Smart card-based secure password authentication scheme, Computers & Security 15 (3) (1996) 231–237.
[5] W.H. Yang, S.P. Shieh, password authentication schemes with smart cards, Computers & Security 18 (8) (1999) 727–733.
[6] H.M. Sun, An efficient remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (4) (2000) 958–961.
[7] C.C. Lee, M.S. Hwang, 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, M.S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 49 (2) (2003) 414–416.
[9] C.C. Chang, K.F. Hwang, Some forgery attacks on a remote user authentication scheme using smart cards, Informatics 14 (3) (2003) 289–294.
[10] K.C. Leung, L.M. Cheng, A.S. Fong, C.K. Chan, Cryptanalysis of a modified remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 49 (4) (2003) 1243–1245.
[11] C.L. Hsu, Security of Chien et al.'s remote user authentication scheme using smart cards, Computer Standards & Interfaces 26 (3) (2004) 167–169.
[12] M. Kumar, New remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 50 (2) (2004) 597–600.
[13] M.K. Khan, J. Zhang, Improving the security of 'a flexible biometrics remote user authentication scheme', Computer Standards & Interfaces 29 (2007) 82–85.
[14] W.C. Ku, S.T. Chang, M.H. Chiang, Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards, IEE Electronics Letters 41 (5) (2005).
[15] M.K. Khan, Fingerprint biometric-based self-authentication and deniable authentication schemes for the electronic world, IETE Technical Review 3 (2009) 191–195.
[16] M.L. Das, A. Saxena, V.P. Gulati, A dynamic ID-based remote user authentication scheme, IEEE Transactions on Consumer Electronics 50 (2) (2004) 629–631.
[17] A.K. Awashti, Comment on a dynamic ID-based remote user authentication scheme, Transactions on Cryptology l (2) (2004) 15–16.
[18] W.C. Ku, S.T. Chang, Impersonation attack on a dynamic ID-based remote user authentication scheme using smart cards, IEICE Transactions on Communication E88-B (5) (2005) 2165–2167.
[19] Y.Y. Wang, J.Y. Kiu, F.X. Xiao, J. Dan, A more efficient and secure dynamic ID-based remote user authentication scheme, Computer Communications 32 (2009) 583–585.
[20] S.K. Kim, M.G. Chung, More secure remote user authentication scheme, Computer Communications 32 (2009) 1018–1021.
[21] 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 28 (2009) 138–143.
[22] W.C. Ku, S.M. Chen, Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 50 (2004) 204–207.
[23] H.Y. Chien, C.H. Chen, A remote authentication scheme preserving user anonymity, in: International Conference on AINA'05, vol. 2, 2005, p. 2005.
[24] C.I. Fan, Y.C. Chan, Z.K. Zhang, Robust remote authentication scheme with smart cards, Computers & Security 24 (2005) 619–628.
[25] I. Liao, C.C. Lee, M.S. Hwang, Security enhancement for a dynamic ID-based remote user authentication scheme, in: Proceedings of the National Conference on Next Generation Web Services Practices, 2005, p. 4.
[26] M. Misbahuddin, C.S. Bindu, Cryptanalysis of Liao–Lee–Hwang's dynamic ID scheme, International Journal of Network Security 6 (2008) 211–213.
[27] Y.P. Liao, S.S. Wang, A secure dynamic ID-based remote user authentication scheme for multi-server environment, Computer Standards & Interfaces 31 (2009) 24–29.
[28] H.C. Hsiang, W.K. Shih, Improvement of the secure dynamic ID-based remote user authentication scheme for multi-server environment, Computer Standards & Interfaces 31 (2009) 1118–1123.

Please cite this article in press as: M.K. Khan et al., Cryptanalysis and security enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme', Comput. Commun. (2010), doi:10.1016/j.comcom.2010.02.011