Global Journal of Computer Science and Technology: E
Network, Web & Security
Volume 16 Issue 4 Version 1.0 Year 2016
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Cryptanalysis and Further Improvement of a Dynamic ID and Smart Card based Remote user Authentication Scheme

By Narendra Panwar
Uttarakhand Technical University

Abstract- Computer systems and their interconnections using networks have im-proved the dependence of both the organizations as well as the individuals on the stored information. This interconnection, in turn, has led to a heightened awareness of the need for data security and the protection of data and re- sources from electronic frauds, electronic eavesdropping, and network-based attacks. Consequently, cryptography and network security have evolved, leading to the development of smart cards to enforce network security. Re-cently, Rafael Martinez-Pelez and Rico-Novella Francisco [1] pointed out vul-nerabilities in Wang et al. [2] scheme. In this paper, we crypt-analyze Wanget al. scheme and demonstrated that our proposed scheme withstands thevulnerabilities pointed out by Francisco et al. and it completes all the re-cent security requirements of [3]. We implemented the proposed scheme in MATLAB and demonstrated that our proposed scheme is not vulnerable to the shortcomings pointed out by Francisco et al. in their scheme.

Keywords: security, authentication, remote user, smart card.

GJCST-E Classification : C.2.3 C.2.5

CRYPTANALYSISANDFURTHERIMPROVEMENTOFADYNAMICIDANDSMARTCARDBASEDREMOTEUSERAUTHENTICATIONSCHEME

Cryptanalysis and Further Improvement of a Dynamic ID and Smart Card based Remote user Authentication Scheme

Narendra Panwar

Abstract- Computer systems and their interconnections using networks have im-proved the dependence of both the organizations as well as the individuals on the stored information. This interconnection, in turn, has led to a heightened awareness of the need for data security and the protection of data and re- sources from electronic frauds, electronic eavesdropping, and network-based attacks. Consequently, cryptography and network security have evolved, leading to the development of smart cards to enforce network security. Re-cently, Rafael Martinez-Pelez and Rico-Novella Francisco [1] pointed out vul-nerabilities in Wang et al. [2] scheme. In this paper, we crypt-analyze Wanget al. scheme and demonstrated that our proposed scheme withstands thevulnerabilities pointed out by Francisco et al. and it completes all the re-cent security requirements of [3]. We implemented the proposed scheme in MATLAB and demonstrated that our proposed scheme is not vulnerable to the shortcomings pointed out by Francisco et al. in their scheme.

Keywords: security, authentication, remote user, smart card

I. Introduction

In 1981, a remote password authentication scheme was proposed by L. Lamport [4] over an insecure channel. Since then, several schemes [5], [6], [7], [8], [9], [10] have been proposed to address this problem for achieving more functionality and efficiency. In a traditional password scheme, each user has an identity and a secret password. If a person wants to log into a network system, they must submit their identity and the corresponding password.

Preprint submitted to Journal of Information Science and Applications May 31, 2016

To avoid storing a plain password table in a public network system, several scheme [4], [11], [12] have proposed a dictionary of verification tables to store each user ID and the corresponding one-way hash value of passwords in the remote system. In 2005, Chien et al.[9] pointed out that Das et al.[8] scheme cannot achieve user anonymity because an attacker can trace user with the static value. In 2010, Lee et al.[13] have analyzed the security of the smart card based user authentication scheme proposed by Lee and Chiu [14]. Their security analysis showed that scheme [9] does not achieve its main security goal of the two-factor security. To demonstrate this, they have shown that the scheme is vulnerable to an o_-line dictionary attack in which an attacker, who has obtained the secret values stored in the users smart card can easily find out its password. Besides reporting the security problem, they showed what really is causing the problem and how to fix it and they proposed a new and improved scheme than Lee and Chius scheme.

In 2012, Francisco et al. have shown security vulnerabilities like Denial of service, server spoong, impersonation in Wang et al. [2] scheme. We propose a scheme that can withstand the above mentioned attacks, we implemented and demonstrated the stated scheme using MATLAB. The paper is organized as follows.

In Section 2, we give a brief review on Wang et al.s scheme. We demon- strate the vulnerabilities of the scheme in Section 3. The proposed scheme and its security analysis are presented in section 4 and 5. Section 6 com- pares the performance of our proposed scheme with other related schemes. Finally, we conclude this paper in Section 7.

Author: e-mail: naren.rishikesh@gmail.com

Table 1: Notation Table

Symbol	Description
U_i	The User
S	The Remote Server
ID_i	Unique identity of U_i
PW_i	Unique password of U_i
S_k	The common session key
$\oplus$	The bitwise XOR operation
H(.)	A collision free one-way hash function such as SHA-256
x,y	Secret Keys of S

II. Review of Wang et al. Scheme

Wang et al. proposed a dynamic ID and smart card based remote user authentication scheme in which the remote server does not maintain a verification table and chooses the users password. Table 1 describes the notations used in this paper and Table 2 depicts review of Wang et al. scheme.

Table 2 : Wang et al scheme

User U_i	Server S
Registration Phase	
Select ID_i	Choose PW_i
Send ID_i to Server S	Compute A_i=H(PW_i)$\oplus$H(x)$\oplus ID_i$
	Store [A_i,y,H(.)] into Smart Card
	Sends PW_i and Smart Card to U_i through secure channel

Table 2 : Wang et al scheme

User U_i	Server S
Login Phase U_i keys in his/her ID_i and PW_i into smart card terminal and perform: $CID_i=H(PW_i)\oplus H(A_i\oplus y\oplus T)\oplus ID_i$ Send $M_i=[ID_i, CID_i, A_i, T]$ to S.	
	Verification Phase Verify $T^*-T \leq \Delta T$, if time interval is incorrect then reject login request otherwise accept M_i and perform: $H(PW_i)^*=CID_i\oplus H(A_i\oplus y\oplus T)\oplus ID_i$ Compute $ID_i^*=H(PW_i)^*\oplus H(x)\oplus A_i$ If $ID_i^*$and ID_i are not equals, then reject login request otherwise S performs: Computes $B= H(H(PW_i)^*\oplus y\oplus T_2)$ Sends $[B, T_2]$ to U_i
Server Verification Phase Verify $T_2-T\leq \Delta T$, if the time interval is incorrect then U_i terminate phase, otherwise perform: Computes $B^*=H(H(PW_i)\bigoplus y\bigoplus T_2)$ If $B^*=B$ holds U_i confirms the identity of S.	

Table 2 : Wang et al scheme

User U_i	Server S
Password Change Phase U_i insert smart card into card reader and keys in his/her PW_i, new password NPW_i and performs: $A_i^*=A_i\oplus H(PW_i)\oplus H(NPW_i)$ Store A_i^* into smart card with replacing A_i.	

III. Cryptanalysis of Wang et al. Scheme

In this section, we demonstrate that Wang et al. scheme is vulnerable to the followings attacks.

a) Denial-of-Service attack

There is no user id and password verification mechanism at client terminal. Therefore, if the user enters false identity $ID_i{}^*$ it will compute CID_i^* and U_i send it to the server S as login request without verifying users identity.S computes

$$H(PWD_i)^* = CID_i{}^* \oplus H(A_i \oplus y \oplus T) \oplus ID_i{}^*$$

and

$$ID_i{}^{**} = H(PW_i)^* \oplus H(x) \oplus A_i.$$

Computed $ID_i{}^{**}$ will never match to the ID_i^* received by the server from the user U_i. If such case happens unnecessary computing will be performed by the server, and it will lead to Denial-of-Service attack..

b) Impersonation attack

Wang et al.'s scheme cannot withstand impersonation attack. The attacker can create a valid login request message if he/she obtains $A_i{}^*H(x)$ and y. If a legitimate user with mal intent wishes to attack the server he/she can extract $H(x)$ from his/her card and can establish a valid session with the server and thus becoming an attacker using his/ her user privileges. Table 3 describes impersonation attack on Wang et al scheme.

Table 3 : Impersonation attack on Wang et al scheme

Legitimate User (Attacker) U_a	**Server S**
Using smart card Compute $H(x)=H(PW_a)\oplus A_a \oplus ID_a$ Intercept previous message $[ID_i, CID_i, A_i, T]$ of User U_i $H(PW_i)=A_i \oplus H(x) \oplus ID_i$ $CID_i{}^*=H(PW_i)\oplus H(A_i \oplus y \oplus T^*)\oplus ID_i$ Send $M_i=[ID_i, CID_i, A_i, T^*]$ to S	
	Verification Phase Verify $T^*-T \le \Delta T$, if time interval is incorrect then reject login request otherwise accept M_i and perform: $H(PW_i)^*=CID_i \oplus H(A_i \oplus y \oplus T^*)\oplus ID_i$ Compute $ID_i{}^*=H(PW_i)^* \oplus H(x) \oplus A_i$ Here $ID_i{}^*$ and ID_i are equals so login request accepted by the server and S performs: $B=H(H(PW_i)^* \oplus y \oplus T^{**})$ Sends $[B, T^{**}]$ to U_a

Table 3 : Impersonation attack on Wang et al scheme

Legitimate User (Attacker) U_a	**Server S**
Server Verification Verify $T^{**}-T^* \le \Delta T$, now time interval is correct and U_a perform: $B^*=H(H(PW_i)\oplus y \oplus T^{**})$ Now session will successfully start between the legitimate attacker U_a and server S.	CID

c) Server spoofing attack

Wang et al. scheme is vulnerable to server spoofing attack which is shown in Table 4. In this scheme, S needs to know y and $H(x)$ for verifying the legitimacy of each user. If the attacker is a legitimate user U_a he/she can impersonate as S to cheat U_i because he/she knows y and $H(x)$. After the user U_i receives the acknowledgement message $[B,T^{**}]$ he/she will compute $B^*=H(PW_i)\oplus y\oplus T^{**}$ and checks whether or not B^* is equal to B In this case, U_i will believe that the attacker is the legitimate S, and will establish a session key with S for further communication.

Table 4 : Server spoofing attack on Wang et al scheme

Legitimate User U_i	**Legitimate User (Attacker) U_a as S**
Login Phase U_i keys in his/her ID_i and PW_i into smart card terminal and perform: $CID_i=H(PW_i)\oplus H(A_i\oplus y\oplus T)\oplus ID_i$ Send $M_i=[ID_i,CID_i,A_i,T]$ to S.	**Intercept message M_i of User U_i** $M_i=[ID_i,CID_i,A_i,T]$ Compute $H(x)=H(PW_a)\oplus A_a\oplus ID_a$ Compute $H(PW_i)=A_i\oplus H(x)\oplus ID_i$ Computes $B=H(H(PW_i)\oplus y\oplus T^{**})$ Sends $[B,T^{**}]$ to U_i
Server Verification Verify $T^{**}-T^*\leq \Delta T$, if time interval is correct then U_i perform: $B^*= H(H(PW_i)\oplus y\oplus T^{**})$ Now the session will successfully start between legitimate user U_i and attacker user U_a.	

d) Password Change Phase Flaws

In the password change phase of Wang et al. scheme, we observe that an attacker user U_i can change password of any other legitimate user U_i's, which is shown in Table 5.

Global Journal of Computer Science and Technology (E) Volume XVI Issue IV Version I Year 2016

Table 5 : Password change flaws of Wang et al scheme

Legitimate User U_l	**Attacker User U_a**
Login Phase	
U_l keys his/her ID_l and PW_l into smart card terminal and perform:	
Computes	
$CID_l=H(PW_l)\oplus H(A_l\oplus y\oplus T)\oplus ID_l$	**Intercept message M_1 of User U_l**
Send $M1=[ID_l,CID_l,A_l,T]$ to S.	$M1=[ID_l,CID_l,A_l,T]$
	Compute $H(x)=H(PW_a)\oplus A_a\oplus ID_a$
	Change password
	Compute $H(PW_l)=A_l\oplus H(x)\oplus ID_l$
	Attacker user U_a computes:
	$A_a{*}=A_l\oplus H(PW_l)\oplus H(NPW_l)$
	Store $A_l{*}$ into smart card replacing with A_l.

IV. Proposed Scheme

This section proposes a strong, secure authentication scheme which will with- stand the security vulnerabilities which leads to the aforementioned attacks.

a) Registration phase

In this phase, the user U_i registers with the remote server S through a secure channel to be a authentic user.

Step 1: U_i chooses his/her identity ID_i and password PW_i and computes $H(ID_i \| PW_i \| R_x$ where R_x random number generated by U_i. Then U_i sends the registration request $H(ID \| PW_i \| R_x)]$ to S.

Step 2: Upon receiving $[ID_i\, H(ID \| PW_i \| R_x]$ from , S veri_es the validity of and computes $VID_i=H(K\oplus ID_i)$

Step 3: S computes $N_i=VID_i\oplus H(ID_i \| PW_i \| R_x$ then captures current date and time in T and create a record $[ID_i, T]$ in its database.

Step 4: S stores $[H(.), N_i T]$ into the smart card of U_i and sends the smart card through a secure channel to the user U_i

Step 5: Upon receiving the smart card from S, U_i stores into smart card and does not need to remember R_x after _nishing registration phase. Finally, U_i's, smart card contains $[H(.), N_i T, R_x]$

b) Login phase

In this phase, when an authentic user want to login to the remote server S, he/she must perform the following steps:

Step 1: U_i inserts his/her smart card into the card reader and inputs the identity ID_i and password PW_i The smart card computes $VID_i{*}=N_i\oplus H(ID_i \| PW_i \| R_x)$, where R_x is retrieved from its memory space.

Step 2: The smart card computes

$T=T+1$ and $M_1=(ID_i \| VID_i{*} \| R_x \| T)^2$ mod n

and sends a login request M_1 to S

c) Authentication phase

Upon receiving the login request M1 from U_i, S performs the following steps:

Step 1: S reveals M_1 by using the Chinese Remainder Theorem (CRT) with p and q to obtain ID_i VID_i R_x and T. Then S veri_es the revealed T with the stored T_i corresponding to ID_i. If T _ T, S replaces T_i with new time variable T in its database. Otherwise, S rejects U_i's, login request.

Step 2: If Step 1 holds, S computes $VID_i=H(K\oplus ID_i)$ and checks if computed VID_i equals received $VID_i{*}$. If it holds, S would successfully authenticate U_i and computes the session key $S_k=H(VID_i \| R_x \| T)$ shared with U_i.

Step 3: S computes $M_2=H(VID \| R_x$ and send it to U_i

Step 4: Ui computes M2*=H(VIDikRx) and check if computed $M_2{*}$ equals received M_2. If it does not hold, Ui stops the session. Otherwise, Ui now successfully authenticate S and use $S_k=H(VID_i \| R_x \| T)$ shared session key with S for securing future communications.

d) Password change phase

In this phase, the user U_i inserts the smart card into device and inputs ID_i, original password PW_i, new password $PW_i{*}$ and $R_x{*}$, where $R_x{*}$ is a new random number generated by U_i. Then, the smart card computes $B=H(ID_i\|PW_i\|R_x)$, $B^*=H(ID_i\|PW_i^*\|R_x^*)$ and $A_i=A_i\oplus B\oplus B^*$. Finally, the values A_i and R_x stored in U_i's, smart card are replaced with A and R_x^*, respectively. Here the password PW_i^* of user U_i has been changed to a new password PW_i^* with o_ine session.

V. Security Analysis

In this section, we analyzed the security of the proposed scheme and shown that our scheme is secure against the following well-known attacks. The security of our proposed authentication scheme is based on the secure hash function and the CRT. In the following steps, we analyzed the security of the proposed scheme to verify that the specified security requirements [3] are fulfilled.

a) Resistance to user anonymity attack

Suppose that the attacker intercepted U_i's, authentication messages. Then, the adversary cannot retrieve any static parameter from these messages, due to the CRT. Hence, the proposed scheme can preserve user anonymity.

b) Resistance to offine password guessing attack

Suppose that a malicious legitimate attacker user U_a has got U_i's, smart card, and the secret information $[H(.), N_i\ T$ and R_x can also be revealed under our assumption of the non-tamper resistant smart card. Even after gathering this information, the attacker has to at least guess both ID_i and PW_i, correctly at the same time, because it has been demonstrated that our scheme can provide identity protection. It is impossible to guess these two parameters correctly at the same time, and thus the proposed scheme can resist offine password guessing attack with smart card security breach.

c) Resistance to stolen verifier attack

In the proposed scheme no sensitive verifiers corresponding to the users are maintained by S. Therefore, the proposed scheme is free from the stolen verifier attack.

d) Resistance to user impersonation attack

As VID_i and N_i are protected by secure one-way hash function, any modification to these parameters of the legitimate user U_i's, will be detected by the server S. Because the attacker has no way of obtaining the values of ID_i PW_i and N_i cor-responding to user U_i he/she cannot fabricate the valid VID_i and Ni, Therefore, the proposed scheme is secure against user impersonation attack.

e) Resistance to server masquerading attack

In the proposed scheme, a malicious server S^* cannot compute the correct mes- sage $M_2=H(VID_i\|R_x$ without knowing U_i's, valid VID_i and R , S* has to break the secure one-way hash function to retrieve ID_i PW_i and R_x from $H(ID_i\|PW_i\|R_x)$. Therefore, the proposed scheme is free from server masquerading attack.

f) Resistance to replay attack

Our scheme can withstand replay attack because the authenticity of authentcation messages M_1 is verified by checking the time variable T.

g) Resistance to parallel session attack

If an adversary masquerade as legitimate user U_i by replaying a previously intercepted authentication message. The attacker cannot compute valid T because he does not know the values of $M_1=(ID_i\|VID_i\|R_x\|T)^2$ mod n corresponding to user U_i. Therefore, the resistance to parallel session attack can be guaranteed in our scheme.

h) Resistance to mutual authentication

In our scheme user U_i computes $M_2^*=H(VID_i\|R_x$ and veri_ed with received M_2. If it hold, U_i authenticate the server S veri_cation successfully and uses $S_k=H(VID_i\|R_x\|$ T shared session key with S for future communications.

i) Resistance to forward secrecy

Based on the dificulty of the one-way hash algorithm, any previously generated session keys cannot be revealed without knowledge of the VID_i R_x and T. As a result our scheme provides the property of forward secrecy.

VI. Computational Cost Analysis

In this scheme we have taken 1.0 unit average run time for a single one-way secure hash function operation. The proposed scheme requires lower computation overhead with comparison to other schemes, which is shown in the Table 6 and the Figure 1.

Table 6 : Computational cost analysis

Computational overhead/Scheme	A_1	A_2	A_3	A_4	A_5	Our Sch.
Computation overhead in the registration phase	5Th	5Th	3Th	3Th	2Th	2Th
Execution overhead in the registration phase	5.0	5.0	3.0	3.0	2.0	2.0
Computation overhead in the login phase	7Th	3Th	2Th	2Th	2Th	2Th
Execution overhead in the login phase	7.0	3.0	2.0	2.0	2.0	2.0
Computation overhead in the authentication phase	11Th	9Th	5Th	5Th	5Th	5Th
Execution overhead in the authentication phase	11.0	9.0	5.0	5.0	5.0	5.0
Total execution overhead	23.0	17.0	10.0	10.0	9.0	9.0

Schemes:A1: Mishra et al A2:Hao et al A3:Lee et al A4:Wen et al A5:Wang et al

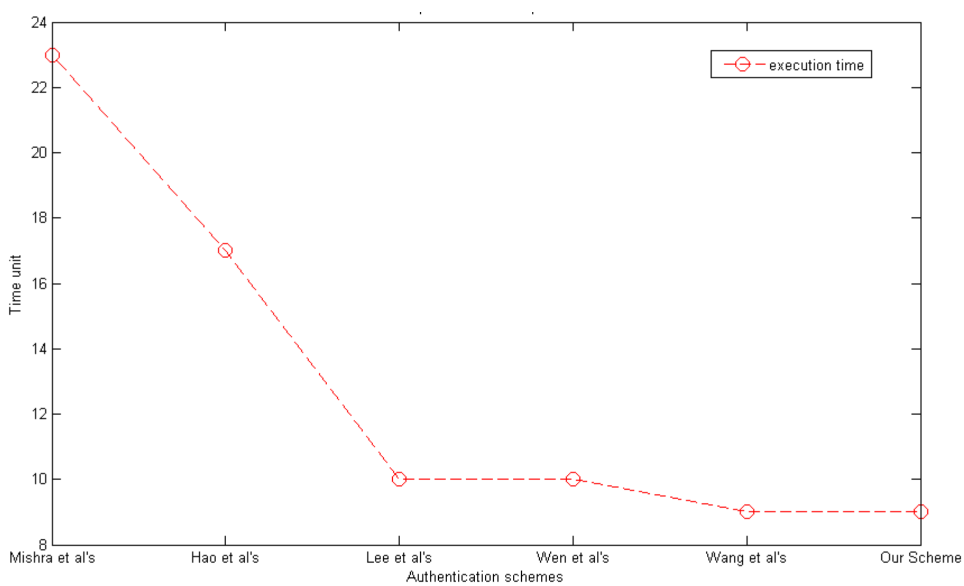

Figure 1 : Comparison of computational cost

VII. Conclusion

Wang et al.s scheme was proposed for resolving security issues presented in pre- vious work of [8]. However, we have discovered some security aws in their scheme making it vulnerable to various attacks such as impersonation, server spoofing and denial of service attack. Moreover, the scheme cannot withstand password change aws. As a remedy to the aforementioned weaknesses, we have presented an en- hanced scheme, which overcome the vulnerabilities of [15] and [1] scheme.

References Références Referencias

1. R. Mart'nez-Pel_aez, F. Rico-Novella, Weaknesses of an eficient and secure dynamic ID-based remote user authentication scheme, Procedia Technology 3 (2012) 351{353. doi:10.1016/j.protcy.2012.03.038. URLhttp://linkinghub.elsevier.com/retrieve/pii/ S2212017312002678
2. J. D. Y. Y. Wang, J.Y. Liu, F.X. Xiao, A more eficient and secure dynamic ID-based remote user authentication scheme, Computer Communications 32 (2009) 583{585.
3. C. S. Tsai, C. C. Lee, M. S. Hwang, Password authentication schemes: Current status and key issues, in: International Journal of Network Security, Vol. 3, IEEE, 2006, pp. 101{115. doi:10.1109/ ICM2CS. 2009.5397977.URL http://ieeexplore .ieee.org/lpdocs/epic03/wrapper.htm?arnumber=53 97977
4. L. Lamport, Password authentication with insecure communication, Communications of the ACM 24 (11) (1981) 770{772. doi:10.1145/358790.358797. URLhttp:// portal.acm.org/ citation.cfm? doid= 358790.358797

5. P. G.M.J, J. van Leeuwen, Authentication : A Concise Survey, Computers & Security 5 (1986) 243{250. doi:0167 4048/86.
6. H.-M. Sun, An eficient remote use authentication scheme using smart cards (2000). doi:10.1109/30.920446.
7. M. Kumar, New remote user authentication scheme using smart cards, in: IEEE Transactions on Consumer Electronics, Vol. 50, 2004, pp. 597{600. doi:10.1109/TCE.2004.1309433.
8. M. Das, V. Gulati, A. Saxena, A dynamic id-based remote user authentication scheme, IEEE Transactions on Consumer Electronics 50 (2) (2004) 629{631.arXiv:0410011,doi:10.1109/TCE.2004.1309441.
9. S.-W. Lee, H.-S. Kim, K.-Y. Yoo, Improvement of Chien et al.'s remote user authentication scheme using smart cards, Computer Standards & Interfaces27(2)(2005)doi:http://dx.doi.org/10.1016/j.csi.2004.02.002.URLhttp://www.sciencedirect.com/science/ article /pii/ S0920548904000170
10. Z.-Y. Wu, Y. Chung, F. Lai, T.-S. Chen, A Password-Based User Authentication Scheme for the Integrated EPR Information System, Journal of Medical Systems 36 (2) (2012) 631{638. doi:10.1007/s10916-010-9527-7.URL http://link .springer.com/ 10.1007/s10916-010-9527-7
11. C. C. Chang, S. J. Hwang, Cryptographic authentication of passwords, in: Security Technology, 1991. Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on, 1991, pp. 126{130. doi:10.1109/CCST.1991.202203.
12. S.-M. Yen, Security of a one-time signature, Electronics Letters 33 (8) (1997) 677{679. doi:10.1049/el:19970460.
13. Y. Lee, H. Yang, D. Won, Attacking and Improving on Lee and Chiu ' s Authentication Scheme Using Smart Cards, Springer Berlin Heidelberg, Berlin, Heidelberg, 2010, Ch. Attacking, pp. 377{385.
14. Y.-C. Lee, Narn-Yih; Chiu, Improved remote authentication scheme with smart card, Computer Standards and Interfaces 27 (2) (2005) 177{180.
15. Y.-P. Liao, S.-S. Wang, A secure dynamic ID based remote user authentication scheme for multi-server environment, Computer Standards & Interfaces 31 (1)(2009) 24{29. doi:10.1016/j.csi.2007.10.007. URL http://dx.doi.org/10.1016/j.csi.2007.10.007http://linkinghub.elsevier.com/retrieve/pii/S09205489070010 3

This page is intentionally left blank