Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

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

Narendra Panwar[1]

[1] Uttarakhand Technical University

Received: 10 December 2015 Accepted: 3 January 2016 Published: 15 January 2016

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 networkbased 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 cryptanalyze 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.

Index terms— security, authentication, remote user, smart card.

1 Introduction

n 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.

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. [ID i ,CID i ,A i ,T] of User U i H(PW i)=A i ?H(x)?ID i CID i *=H(PW i)?H(A i ?y?T*)?ID i Send M i =[ID i ,CID i ,A i ,T*] to S

2 Verification Phase

Verify T*-T? ?T, if time interval is incorrect then reject login request otherwise accept M i and perform:H(PW i)*=CID i ?H(A i ?y?T*)?ID i Compute ID i *=H(PW i)*?H(x)?A i

Here ID i * and ID i are equals so login request accepted by the server and S performs: CID i =H(PW i)?H(A i ?y?T)?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)?A a ?ID a Compute H(PW i)=A i ?H(x)?ID i

3 Proposed Scheme

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

4 a) Registration phase

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

Step 1: chooses his/her identity and password and computes

. Then sends the registration request

Step 2: Upon receiving from , S veri_es the validity of and computes

Step 3: computes then captures current date and time in T and create a record in its database.

Step 4: stores into the smart card of and sends the smart card through a secure channel to the user

Step 5: Upon receiving the smart card from stores into smart card and does not need to remember after _nishing registration phase. Finally, smart card contains 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: inserts his/her smart card into the card reader and inputs the identity and password The smart card computes where is retrieved from its memory space.

Step 2: The Step 1: reveals M 1 by using the Chinese Remainder Theorem (CRT) with p and q to obtain and . Then veri_es the revealed with the stored corresponding to ID . If _T, S replaces with new time variable T in its database. Otherwise, rejects login request.

Step 2: If Step 1 holds, S computes and checks if computed equals received . If it holds, would successfully authenticate and computes the session key shared with .

Step 3: computes and send it to .

Step 4: Ui computes M *=H(VIDikRx) and check if computed M * equals received . If it does not hold,i U i U i U i U i U i U i U i U 's, S S S S S S S S S i U i U i U ID i PW i H(IDi PW i R where

x Rx number generated by random PW i R x)] to S. i ID H(ID [PW i R x i ID H(ID [ ] VID i =H(K?ID i) i =VID i ?H(ID i PW i R x N T ,] R x [H(.),N i T] S , i U [H(.),N i T] R x , i ID i ID PW i VID i VID i *=N i ?H(ID i PW i R x), Rx T=T+1 and M 1 =(ID i VID i * R x T) 2 Rx T i Ti Ti T T VID i i U 's, VID i * =H(K?ID i VID i), k =H(VID i R x S T) . i U 2 =H(VID R x M 1 M2 2 2 M Cryptanalysis andID PW i PW i * k =H(VID i R x T) S S . i U R x * R x

5 Global Journal of Computer Science and Technology

Volume XVI Issue IV Version I ( ) number generated by Then, the smart card V.

6 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 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 authentication messages. Then, the adversary cannot retrieve any static parameter from these messages, due to the . Hence, the proposed scheme can preserve user anonymity.

7 b) Resistance to offine password guessing attack

Suppose that a malicious legitimate attacker user has got smart card, and the secret information and 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 and 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.

8 c) Resistance to stolen verifier attack

In the proposed scheme no sensitive verifiers corresponding to the users are maintained by . Therefore, the proposed scheme is free from the stolen verifier attack. Based on the dificulty of the one-way hash algorithm, any previously generated session keys cannot be revealed without knowledge of the and . As a result our scheme provides the property of forward secrecy.

9 VI.

10 Computational Cost Analysis

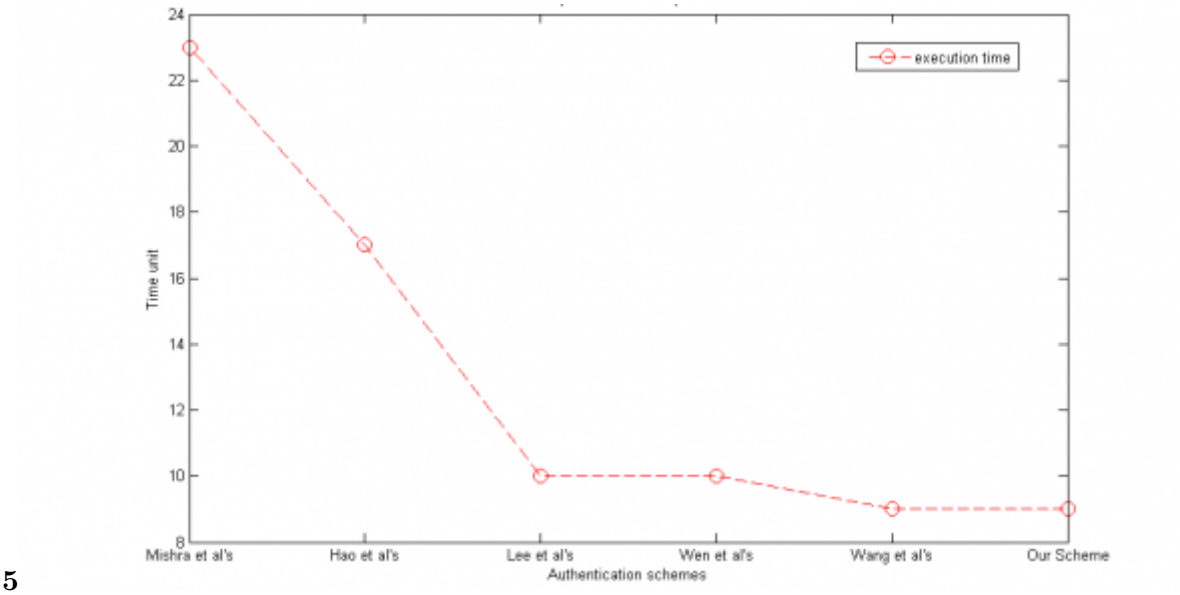
In this scheme we have taken 1.0 unit average run time for a single one-way secure hash function operation. The proposed scheme requires lower computation overhead with comparison to other schemes, which is shown in the Table **??** and the Figure **??**. Wang et al.s scheme was proposed for resolving 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 enhanced scheme, which overcome the vulnerabilities of [15] i ID i ID VID i VID i i U 's, i U 's, i U 's, . i U . i U M 1 . i U CRT. CRT. R x R x R x PW i . i U , PW i N i N i [H(.),N i T Ua S T . i U H(ID i PW i R x). 1 =(ID i VID i R x T) 2 M 2 *=H(VID i R x M 2 M . i U S k =H(VID i R x T © 2016

11 B*=H(ID

i PW i * R x B=H(ID i PW i R x), *) A i =A i ?B?B*. i A R x i U 's, x * PW i * PW i . i U PW i [1]

Figure 1:

[1] © 2016 Global Journals Inc. (US) 1



5

Figure 2: Table 5 :

1NotationII

Figure 3: Table 1 : Notation Table II .

2

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

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 The bit-wise XOR operation
H(.)	A collision free one-way hash function such as SHA-256
x,y	Secret Keys of S

Year 2016 26

User U i	Server S
Registration Phase	
Select ID i Send ID i to Server S	Choose PW Sends PW i and Smart Card to U i through secure channel

[Note: i Compute A i =H(PW i)?H(x)?ID i Store [A i ,y,H(.)] into Smart Card]

Figure 4: Table 2 :

2

Figure 5: Table 2 :

2

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)?H(A i ?y?T)?ID i Send M i =[ID i , CID i , A i ,T] to S.	Verification Phase Verify T*-T ? ? T, if time interval is incorrect then reject login request otherwise accept M i and perform: H(PW i)*=CID i ?H(A i ?y?T)?ID i Compute ID i *=H(PW i)*?H(x)?A i If ID i *and ID i are not equals, then reject login request otherwise S performs: Computes B= H(H(PW i)*?y?T 2) Sends [B, T 2] to U i
Server Verification Phase Verify T 2 -T? ?T, if the time interval is incorrect then U i terminate phase, otherwise perform: Computes B*=H(H(PW i) y T 2) If B*=B holds U i confirms the identity of S.	
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 ?H(PW i)?H(NPW i) Store A i * into smart card with replacing A i .	

Figure 6: Table 2 :

3

Legitimate User (Attacker) U a Using smart card	Server S

[Note: Compute H(x)=H(PW a)?A a ?ID a Intercept previous message]

Figure 7: Table 3 :

3

i ID * * Ui	ID * i	
	i * A H(x)	y
H(x)		

[Note: © 2016 Global Journals Inc. (US) 1]

Figure 8: Table 3 :

4

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:	

Figure 9: Table 4 :

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)?H(A l ?y?T)?ID l	Intercept message M 1 of User U l M1=[ID l ,CID l ,A l ,T] Compute H(x)=H(PW a)?A a ?ID a Change password Compute H(PW l)=A l ?H(x)?ID smart card computes mod n and sends a login request to c) Authentication phase Upon receiving the login request M1 from , performs the following steps:

*[Note: lAttacker user U a computes:A a *=A l ?H(PW l)?H(NPW l)Store A l * into smart card replacing with A l .]*

Figure 10:

Year 2016
30
Ui stops the session. Otherwise, Ui now successfully
authenticate S and use shared
session key with for securing future communications.
d) Password change phase
In this phase, the user inserts the smart card
into device and inputs , original password i ,
new
password and*, is a new random
where

Figure 11:

Figure 12:

[Lee] , Y.-C Lee . *Narn-Yih*

[Das et al. ()] 'A dynamic id-based remote user authentication scheme'. M Das , V Gulati , A Saxena . 10.1109/TCE.2004.1309441. *IEEE Transactions on Consumer Electronics* 2004. 50 (2) p. .

[Wang et al. ()] 'A more eficient and secure dynamic ID-based remote user authentication scheme'. J D Y Y Wang , J Y Liu , F X Xiao . *Computer Communications* 2009. 32 p. .

[Wu et al. ()] 'A Password-Based User Authentication Scheme for the Integrated EPR Information System'. Z.-Y Wu , Y Chung , F Lai , T.-S Chen . 10.1007/s10916-010-9527-7. http://link.springer.com/10.1007/s10916-010-9527-7 *Journal of Medical Systems* 2012. 36 (2) p. .

[Liao and Wang ()] 'A secure dynamic ID based remote user authentication scheme for multi-server environment'. Y.-P Liao , S.-S Wang . 10.1016/j.csi.2007.10.007. http://dx.doi.org/10.1016/j.csi.2007.10.007http://linkinghub.elsevier.com/retrieve/pii/S092054890700103 *Computer Standards & Interfaces* 2009. 31 (1) p. .

[Sun ()] *An eficient remote use authentication scheme using smart cards*, H.-M Sun . 10.1109/30.920446. 2000.

[Lee et al. ()] *Attacking and Improving on Lee and Chiu ' s Authentication Scheme Using Smart Cards*, Y Lee , H Yang , D Won . 2010. Berlin Heidelberg; Berlin, Heidelberg: Springer. p. .

[Van Leeuwen ()] 'Authentication : A Concise Survey'. PG M J , J Van Leeuwen . *Computers & Security* 1986. 5 p. .

[Chang and Hwang ()] 'Cryptographic authentication of passwords, in: Security Technology'. C C Chang , S J Hwang . 10.1109/CCST.1991.202203. *Proceedings. 25th Annual 1991 IEEE International Carnahan Conference on*, (25th Annual 1991 IEEE International Carnahan Conference on) 1991. 1991. p. .

[Chiu ()] 'Improved remote authentication scheme with smart card'. Chiu . *Computer Standards and Interfaces* 2005. 27 (2) p. .

[Lee et al. ()] 'Improvement of Chien et al.'s remote user authentication scheme using smart cards'. S.-W Lee , H.-S Kim , K.-Y Yoo . 10.1016/j.csi.2004.02.002.URL. http://dx.doi.org/10.1016/j.csi.2004.02.002.URLhttp://www.sciencedirect.com/science/article/pii/S0920548904000170 *Computer Standards &* 2005. 27 (2) .

[Kumar ()] 'New remote user authentication scheme using smart cards'. M Kumar . 10.1109/TCE.2004.1309433. *IEEE Transactions on Consumer Electronics* 2004. 50 p. .

[Tsai et al. ()] 'Password authentication schemes: Current status and key issues'. C S Tsai , C C Lee , M S Hwang . doi:10.1109/ ICM2CS. 2009.5397977. http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=5397977 *International Journal of Network Security* 2006. IEEE. 3 p. .

[Lamport ()] 'Password authentication with insecure communication'. L Lamport . 10.1145/358790.358797. URLhttp://portal.acm.org/citation.cfm?doid=358790.358797 *Communications of the ACM* 1981. 24 (11) p. .

[Yen ()] 'Security of a one-time signature'. S.-M Yen . 10.1049/el:19970460. *Electronics Letters* 1997. 33 (8) p. .