Volume 3, No. 6, June 2012

Journal of Global Research in Computer Science

ISSN-2229-371X

RESEARCH PAPER

Available Online at www.jgrcs.info

ADVANCED SECURE REMOTE USER AUTHENTICATION SCHEME PRESERVING USER ANONYMITY

Chandra Sekhar Vorugunti*[1], Mrudula Sarvabhatla[2]
*[1]Department of Information and Communication Technology, DA-IICT, Gandhinagar,Gujarat,India
vorugunti_chandra_sekhar@daiict.ac.in[1]
[2]Department of Computer Science and Engineering, Sri Venkateswara University,Tirupathi,Andhra Pradesh,India
mrudula.s911@gmail.com[2]

Abstract: To ensure secure transmission of data and to authenticate remote user while accessing server resources, smart card based remote user authentication schemes have been widely adopted. In 2004, Das et al proposed first of its kind of protocol for remote user authentication with smart cards using Dynamic Id to protect user anonymity. In 2005, Chien et al pointed out that Das et al scheme failed to preserve user anonymity and the scheme is equivalent to open access without any password and proposed a new scheme to remedy of Das et al. In 2008 Bindu et al pointed out that Chien et al scheme is insecure against Insider attack and Man in the Middle attack and proposed a new scheme to remedy of Chien et al. In this paper we will show that Bindu et al scheme cannot preserve user anonymity under their assumption. In addition their scheme is vulnerable to user-impersonation attack, server-masquerading attack, Man in the Middle attack, stolen smart card attack, password guessing attack, replay attack, fails to achieve mutual authentication and perfect forward secrecy (PFS). We then present our improved scheme to overcome the vulnerabilities stated in Bindu et al’s scheme while preserving all the merits of their scheme.

Key Words: Smart card, Authentication , Authentication protocols, Remote Server Access

INTRODUCTION

Remote user authentication is a mechanism in which a remote user is validated to access remote server resources or services over an insecure communication channel. Smart card based password authentication scheme is one of the most widely used technique for various kinds of authentication applications such as online banking, online shopping etc. password authentication with smart cards is an efficient two-factor authentication mechanism. Due to their various advantages like flexibility, low computational cost, smart cards are widely deployed in various E-Commerce applications to validate the legitimacy of a user. Due to their wide spread usage various researchers proposed user authentication schemes using smart cards.

Most of the proposed schemes many of them [1,6,9,16,20] assume that the smart card is tamper resistant i.e. (not possible to extract the protected software and data from smartcard processors). Some schemes [2,5,17,18] shown that the secret data stored in the smart card can be extracted by some means such as Micro probing, Software attacks, Eaves dropping, Fault generation and monitoring the power consumption etc. The above mentioned attacks clears that the adversary can tamper and extract the data from the tamper-resistant smart cards and can perform various vulnerability attacks such as user-impersonation attack, server masquerading attack Man in the Middle attack etc.

In addition most of the schemes proposed [6, 7, 8, 12, 14, 20] do not preserve user anonymity i.e., preserving user identity, which is critical source of information. An adversary can perform various attacks like [3, 19] traffic analysis attack, java script attack, cookie stealing attack etc. to intercept user id. Along with other intermediate transmitted messages an adversary can create a legal forged login messages. Once an adversary intercepts user identity, he can track user login history and current location [15].

In 2004, Das et al [9] proposed a Dynamic Id based remote user authentication scheme based on smart cards to protect user anonymity. The Dynamic Id scheme allows user to choose and change their passwords freely and do not maintain verifier table to validate the legitimacy of a user. However various researchers [4, 10, 11] have shown that Das et al scheme is insecure against various attacks like impersonation attack, insider attack etc. The researchers also showed that Das et al scheme fails to protect user anonymity and it is password independent.

In 2005 Chien and Chen [7], pointed out that Das et al’s scheme fails to protect user anonymity and then proposed a new scheme to overcome the weakness in Das et al scheme. The Chien et al claim that their scheme preserves the merits of Das et al scheme and provides user anonymity.

In 2008 Bindu et al [13] showed that Chien et al scheme is vulnerable to Insider attack and Man in the Middle attack, if the smart card is no longer tamper resistant i.e. the secret information stored in the smart card can be extracted. Therefore Bindu et al proposed an improved scheme and claimed that improved scheme eliminates the security flaws in Chien et al. In this paper, we will show that the Bindu et al scheme is still vulnerable to the Impersonation attack, server masquerade attack, stolen smart card attack, password guessing attack. We then propose an improvement scheme over Bindu et al‘s scheme to remedy their drawbacks, while preserving all the merits of their schemes.

In summary, our scheme has the following advantages: 1) the server does not need password or verification tables for user validity checking. 2) users can freely choose and change their passwords 3) User anonymity is maintained.4) Mutual

Authentication is achieved 5) Session key exchange with perfect forward secrecy is provided 6) The scheme can resist various kinds of attacks such as smart card stolen verifier attack, password guessing attack, replay attacks and server impersonation attacks, all these are achieved even if the smart card is non-tamper resistant.

The rest of the paper is organized as follows. In section II a brief review of Bindu et al's scheme is given. Section III describes the security weakness of Bindu et al scheme. In section IV our improved scheme is proposed and its security analyses are discussed in section V. The comparison of the both the protocols are given in section VI and section VII provides the conclusion of the paper.

REVIEW OF BINDU ET AL.'S SCHEME

In this section, we examine the improved remote user authentication scheme proposed by Bindu et al in 2008.The scheme is composed of three phases: the registration, login, and authentication phase .The notations used in Bindu et al.'s scheme are listed below:
U: the user
ID: the identity of U.
PW: the password of U.
S: the remote server.
x: the secret key of S
h(.) : a secure one-way and collision resistant hash function.
$E_R[M]$: a symmetric encryption of message M using secret key R.
p, g : the parameters of Diffie–Hellman key exchange protocol
$\oplus$: the exclusive – OR (XOR) operation.

Registration Phase:

This phase is invoked whenever a user U registers with the remote system for the first time.

(R1) U selects his user identity ID, password PW, and then computes h(PW). User submits the ID and h(PW) to the system for registration.
(R2) U to S: {ID, h(PW)}
(R3) S Computes $m=h(ID \oplus x) \oplus h(x) \oplus h(PW)$ and
$I = h(ID \oplus x) \oplus x$.
(R4) S issues a smart card containing m, I, h(.), g, p

Login Phase:

Whenever the user wants to login to remote server S, the following procedure is performed.

(L1) U inserts his smart card into the card reader of a terminal
and inputs his ID and PW.
(L2) The smart card generate a random number $r_u = g^u \bmod p$
Compute $M = m \oplus h(PW)$
Compute $C = M \oplus r_u$
Compute $R = I\oplus r_u = h(ID \oplus x) \oplus x \oplus r_u$
(L3) Smart card sends $\{C, T, E_R [r_u, ID, T]\}$ to the server where T is the timestamp and the $E_R [r_u, ID, T]$ is the cipher text encrypted with 'R'.

Authentication Phase:

After receiving U's login request message, the server S performs the following steps:

(A1) S computes $R= C \oplus h(x) \oplus x$ then decrypts the message $E_R [r_u, ID, T]$ using R to obtain the plain text $[r_u, ID, T]$.

(A2) Test the validity of time interval between T and T' where
T' is a time stamp when server received the message.

(A3) The server S computes $R = h(ID \oplus x) \oplus x \oplus r_u$. If they are equal, S accepts the login request else rejects request.

(A4) S to U: $\{T1, E_R\{r_s,r_u+1,T1\}\}$,where $r_s = g^s \bmod p$ and T1 is the server current time stamp.

(A5) On receiving the reply message $\{T1, E_R\{r_s,r_u+1,T1\}\}$ user tests the validity of the time intervals and checks whether the decrypted data contains the value r_u+1. If so user can generate the session key $K_{us} = (r_s)^u \bmod p = g^{us} \bmod p$ and the server is authenticated to the user.
(A6) Then the user delivers the message E: $_{Kus}$ $[r_s+1]$ to the server.

(A7) Server decrypts the received message and checks whether it is equal to r_s+1, if yes, the user is authenticated and the server can be assured of a session key established between server and the user.

WEAKNESS OF BINDU ET AL. 'S SCHEME

In Bindu et al scheme, they concluded that their scheme counters the weakness in chien et al scheme[7] i.e. insider attack and man in the middle attack and they claimed that their scheme could also prevent 1) replay attack, 2) guessing attack.

In this section, we will show that Bindu et al.'s scheme is still vulnerable to revealing of secret key of server to legal user, user-impersonation attack, server-masquerading attack, Man in the Middle attack, stolen smart card attack, password guessing attack, replay attack, fails to achieve mutual authentication and perfect forward secrecy (PFS).

Revealing of Secret Key of Server to Legal User:

Assume that an adversary 'E' is a legal user. He can extract the secret data stored in his smart card by some means [12,13] then he can derive the secret key 'x' of server as follows .

$$m = h(ID \oplus x) \oplus h(x) \oplus h(PW). \quad (1)$$

$$I = h(ID \oplus x) \oplus x. \quad (2)$$

A legal user already knows his ID and extracted 'I' stored in his smart card can perform guessing attack for 'x'. Guess a secret value x^* and check $h(ID \oplus x^*) \oplus x^* = I$. If they are equal then the secret value of server S is x^*. Otherwise he can repeat the process to get correct value x^*. Once he knows the 'x', then can find out h(x) as h(.) is available on this smart card by substituting the values in (1) .

A legal user without performing the above attacks can simply find out x $\oplus$ h(x) value as follows. (x $\oplus$ h(x) value is used by Server in A1 to authenticate user).

$$m \oplus I = x \oplus h(x) \oplus h\,(PW) \qquad (3)$$

$$m \oplus I \oplus h\,(PW) = x \oplus h(x) \qquad (4)$$

a legal user knows m, I, h(.) and PW, he will substitute in (4) and gets the value for x $\oplus$ h(x) .

User Impersonation Attack:

User/Server Impersonation means that if an adversary 'E' who is a legal user of the system has obtained the secret information stored in a legal user smart card or some intermediate computational results which a smart card sends to server, then he can crash the mutual authentication scheme by masquerading as user/server.

An adversary E who is a legal user can impersonate another legal user U of Server S as follows.

a. Intercept the U's login request message {C, T, $E_R[r_u$,ID,T]}.
b. Compute R = C $\oplus$ x $\oplus$ h(x). x $\oplus$ h(x) can be calculated as specified in A of section III, Equation (4) without doing any complex calculations by an adversary.
c. Decrypt $E_R[r_u$,ID,T] using R, Then the adversary E comes to know the ID. (Hence in Bindu et al.'s scheme user anonymity is not preserved.), r_u, T.
d. Whenever E wants to impersonate U he can send a fake login request message {C, T^*, $E_R[r_u$, ID, T^*]} to S with proper T^*. It will pass the authentication process (A1) of S. C, R, ID, r_u can be replayed and they are fixed values (doesn't changes with time). only value adversary needs to take care is T^*. E can find out the valid T^* by eaves dropping the communication between U and S.

Server Masquerade Attack:

An adversary E can impersonate Server S as follows.

a. Intercept U's login request message {C, T, $E_R[r_u$,ID,T]}.
b. Compute R = C$\oplus$ x$\oplus$h(x) .x$\oplus$h(x) can be calculated as specified in equation (4) of A of section III without doing any attacks by an adversary. Now E came to know the secret key R through which the User and Server encrypts and decrypts the message. Hence now any message to U from S can be easily intercepted and decrypted by E.
c. Now, whenever U sends a new login request message {C*, T*, $E_{R^*}[r_u{}^*$, ID, T*]}. E intercepts the login request message from U. Computes C* $\oplus$ x $\oplus$ h(x) to obtain R*. Then decrypts the message to get $r_u{}^*$, ID, T*.
d. E can impersonate S by sending {T_1, $E_{R^*}[r_s$, $r_u{}^*$+1, T_1]} where $r_{s\,=}$ g^s mod p.
e. As mentioned In B of section III, E can get correct T_1 by eaves dropping the messages from U to S.
f. U will decrypt the message and checks whether the decrypted message contains $r_u{}^*$+1. If so U proceeds to create session key with the E assuming it S.

Stolen SmartCard Attack:

In case a legal user U's smart card is stolen by an adversary E who is also a legal user of S, then as mentioned in A of section III, E can extract the secret data stored in the smart card by any means [12,13]. Once E gets m, I stored in U's smart card then E can get ID and PW of U as follows

$$m = h(ID \oplus x) \oplus\ h(x) \oplus h(PW). \qquad (1)$$

$$I = h(ID \oplus x) \oplus x. \qquad (2)$$

As E is legal user he knows 'x' the secret key of S as discussed in A of section III. He performs guessing attack using equation (2). He guess an ID of U as ID* and checks whether h(ID* $\oplus$ x) $\oplus$ x is equal to I . If they are equal then ID* is the ID of U else he select another ID* and repeats the above guessing attack until the match is found. Once he gets the correct ID of U, He performs similar attack on equation (1) to get PW of U. This is one of severe vulnerability in Bindu et al.'s scheme. Once a valid user smart card is lost then the legitimate adversary can use the card as his own.

Man in the Middle Attack:

A Man-in-the-Middle attack is an attack in which the adversary gets in the middle of a valid user U and S while running of the scheme. He imitates as user while talking to server and vice versa.

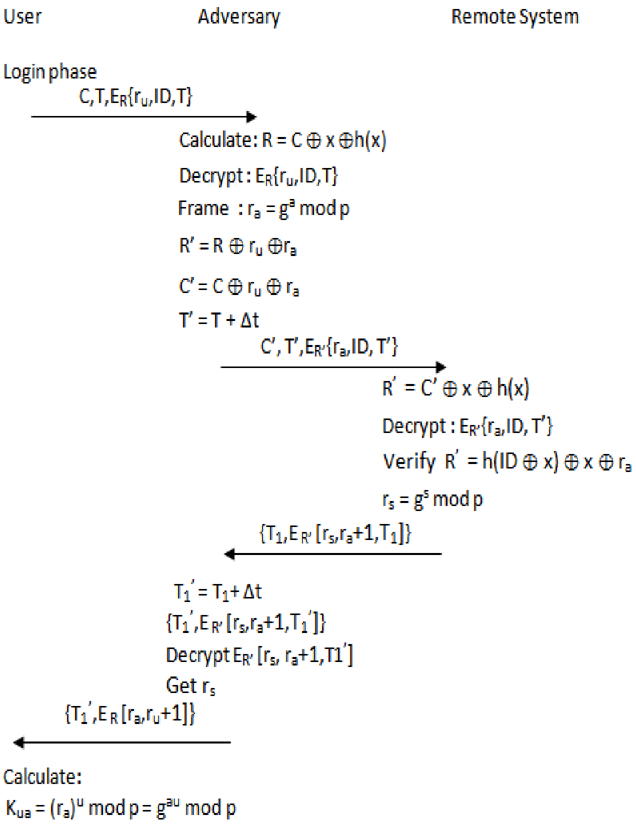
User
Adversary
Remote System
Login phase
C,T,$E_R\{r_u$,ID,T}
Calculate: R = C $\oplus$ x $\oplus$h(x)
Decrypt : $E_R\{r_u$,ID,T}
Frame : $r_a = g^a$ mod p
R' = R $\oplus$ r_u $\oplus r_a$
C' = C $\oplus$ r_u $\oplus$ r_a
T' = T + Δt
C', T', $E_{R'}\{r_a$,ID, T'}
R' = C' $\oplus$ x $\oplus$ h(x)
Decrypt : $E_{R'}\{r_a$,ID, T'}
Verify R' = h(ID $\oplus$ x) $\oplus$ x $\oplus$ r_a
$r_s = g^s$ mod p
{T_1,$E_{R'}$ [r_s,r_a+1,T_1]}
$T_1{}'$ = T_1+ Δt
{$T_1{}'$,$E_{R'}$ [r_s,r_a+1,$T_1{}'$]}
Decrypt $E_{R'}$ [r_s, r_a+1,T1']
Get r_s
{$T_1{}'$,E_R [r_a,r_u+1]}
Calculate:
$K_{ua} = (r_a)^u$ mod p = g^{au} mod p

Figure 1. Graphical View of Man in the middle attack in Bindu et.al's scheme.

Failure to Achieve Mutual Authentication:

As shown in B, C, and E of section III Bindu et al's scheme suffer from user impersonation attack, server masquerade attack, man in the middle attack. Hence their scheme has failed to achieve mutual authentication among user U and remote server S [21].

Failure to Achieve Secure Session Key Agreement with Perfect Forward Secrecy(PFS):

The purpose of PFS is that even if an adversary records all the cipher text messages sent by the user U to S, and later he come to know the secret session key used for encrypting the cipher text, It must not possible for him to decrypt the recorded cipher texts. In E of section III, we showed that Bindu et al's scheme suffers from man in the middle attack. In this attack an adversary creates a session key with both user (K_{au}) and system (K_{us}). Hence the adversary can able to decrypt all the messages encrypted by user with secret session key (K_{au}) and the messages encrypted by server S with secret session key (K_{us}). Hence Bindu et al's scheme has failed to achieve perfect forward secrecy [21].

OUR IMPROVED SCHEME

In this section, we present an improved scheme over Bindu et al.'s scheme to remedy their security flaws (i.e vulnerabilities to Revealing of secret key of server to legal user, User impersonation attack, Server masquerading attack, Stolen smart card attack, Man in the middle attack, preserving user anonymity etc) while preserving their merits. The proposed scheme is divided in to four phases: the registration, login, authentication, and password change phases.

Registration Phase:

This phase is invoked whenever a user U wants to register first time with the remote server S. The following steps are performed.

(R1) The user U first chooses his Identity ID and password PW, and a random number b.
(R2) U to S: {ID, h(b || PW)}
(R3) S computes:
$W = h(ID \| x) \oplus h(b\|PW)$
where 'x' is the secret of S.
(R4) S to U, a smart card containing W and the public parameters {h(.), p, g}

Login Phase:

Whenever user wants to login into the remote server S, he inserts his smart card into the terminal and inputs his ID, PW and b. Then the smart card performs the following tasks.

(L1) Compute $I = W \oplus h(b \| PW) = h(ID \| x)$
(L2) : Generate random numbers a , u $\neq 0$.
(L3) : Compute :
$r_u = g^u \bmod p$
$C = g^{a.I} \bmod p$,
$R = g^{a.I.h(x)} \bmod p = C^{h(x)} \bmod p$.
(L4) : U to S : {C,T,$E_R[r_u$,ID,T]} where T is the User time stamp and $E_R[r_u$,ID,T] is the cipher text encrypted using R.

Authentication Phase:

On receiving the login request message from U, S performs the following tasks

(A1) Compute R from C, which is in login request message sent by U and server secret key x. $R = C^{h(x)} \bmod p$.
(A2) Test the validity of time interval between T and T* where T* is the Server time on which the login message is received.
(A3) Verify whether the following equation holds $R = g^{a.h(ID\|x).h(x)} \bmod p$. If the equation doesn't hold reject the login request.
(A4) Generate a random number s .
Compute:
$r_s = g^s \bmod p$
$K_{us} = (r_u)^s \bmod p = g^{us} \bmod p$
S to U: {T_1,$E_R[r_s$,h(ID||r_u||T||T1||K_{us})]} where T_1 is the current time of the remote server S.
(A5) On receiving the login reply message from the server, U performs following tasks:
check the validity of the time intervals.
decrypt the message from Server $E_R[r_s$,h(ID||r_u||T||T1|| K_{us})]
Extract r_s from the reply message and
calculate $K_{us} = (r_s)^u \bmod p$ and calculates the hash value h(ID||r_u||T||T1|| K_{us}). If hash values are equal then server is authenticated to the user.
(A6) U to S: M = h(r_s || K_{us})
(A7) Server S verifies h(r_s|| K_{us}) = M is so user is authenticated to S.

SECURITY ANALYSIS OF IMPROVED SCHEME

In this section we discuss and demonstrate how our proposed scheme fixes the vulnerabilities found in Bindu et al.'s scheme while preserving the merits of their scheme.

User Anonymity:

To preserve user anonymity in our scheme we are sending ID of a user in an encrypted form using the one-time secret key R. To know the user who sent the login request, the remote server S must decrypt the message $E_R[r_u$,ID,T] using R, To calculate R, S stores data in Smart card of the user such that it can calculate R on swipe of the smart card by the user. In Bindu et al.'s scheme once the legitimate adversary E gets the secret data stored in the smart card by some means [2,5,17,18], As discussed in A of section III, the adversary E can find out the secret key x of the server and once he obtain the intermediate computation result, he can derive secret key R, $R = C \oplus x \oplus h(x)$, E gets x, h(x) from data stored in smart card as discussed in A of section III and C from intermediate computational result.

To resolve this problem the secret key x, R must not be derived from either the secret data stored in the smart card or the intermediate computational result. In our scheme we stored only $W= h(ID\|x) \oplus h(b \| PW)$ on the smart card. It is computationally infeasible for an adversary E who is a legal user, even he knows ID, PW, b to calculate x, which is secret key of remote system S this is due to one-way and collision resistant properties of hash function. It is also computationally infeasible to calculate I = h(ID ||x) for a legal user even he knows ID, as it's not possible for him to get x as discussed above. Similarly, if E obtains the intermediate computational result C, It is computationally in feasible to get h(x) from the formula $C^{h(x)} \bmod p$, owing to discrete logarithm properties.

As discussed above in our scheme it's not possible even for an adversary who is a legal user to know the secret key of server x from the data stored in the smart card (which is not the case with Bindu et al.'s scheme as discussed in A of section III) and it's not possible to calculate the secret key R from the intermediate computational result. Same is the case when a legal user intercepts other user login messages. Hence in our system based on hash function and discrete logarithm property we protected the user anonymity.

Resistance to User Impersonation Attack:

To impersonate a user U, an adversary E who is also a legal user must fake a login message C,T,$E_R[r_u$,ID,T] and a reply message M = h(r_s || K_{us}) (A6) to the remote server S. To impersonate U, E must know the ID of U to create a fake message, As shown in A of section V it's not possible for E to get R, so he cannot decrypt the login message sent by U and get U's Identity i.e ID. Another way, E can replay a valid login message from U but still he needs to forge a valid reply message to S i.e M = h(r_s || K_{us}) (A6). To send a forged reply M = h(r_s || K_{us}), E must know r_s sent by S to U. S sent r_s to U in A4. The adversary to get r_s, must decrypt $E_R[r_s$,h(ID||r_u||T||T1||K_{us})] but as discussed in A of section V its not computationally feasible to derive R even for a legal adversary E. Hence in our scheme it is impossible for anyone to impersonate a legal user U in our scheme.

Resistance to Server Masquerade attack:

To masquerade as remote server S, An adversary E has to send U, a forged reply message {T_1,$E_R[r_s$,h(ID||r_u||T||T1||K_{us})]} as in A4 once E received the login message from U. As shown in A of section V it is computationally infeasible for E to derive R to decrypt the login message {C,T,$E_R[r_u$,ID,T]} to obtain r_u, ID.In A4 remote server S sends {T_1,$E_R[r_s$,h(ID||r_u||T||T1||K_{us})]} to U. To get r_s, K_{us}, E must derive R, which we shown in A of V as computationally infeasible. Hence E cannot obtain r_s, K_{us} to forge the reply message from remote server S. Hence in our scheme it is impossible for anyone to masquerade as server.

Resistance to Offline Password Guessing Attack and Stolen smartCard Attack:

In our scheme we stored only W = h(ID || x) ⊕ h(b||PW) in the smart card. As demonstrated in A of section V an adversary E who is a legal user of the remote server S, doesn't obtains ID and x. As b is a random number chosen by the user U, E doesn't knows it. Without knowing ID,x,b it is computationally infeasible to calculate PW after obtaining W from the U's smart card, owing to hash function properties. It's not the case with Bindu et al.'s scheme in which an adversary who is a legal user from the stolen smart card can able to obtain both the ID and PW as discussed in C of section III. Hence our scheme provides resistant to offline password guessing attacks and stolen smart card attack.

Mutual Authentication:

In our proposed scheme, To authenticate U, the server S will validate U by comparing R in A1 equals to A3 and the message sent by U in A6 i.e h(r_s|| K_{us}) = M. In A of V we shown that in our scheme it's not possible to obtain ID, R,x,h(x) by an adversary even he is a legal user. In B of section V we have shown that our scheme provides resistant to user impersonation attack. It's not possible for E to forge login messages sent by U. To send a fake login message to S by E, E needs to compute C, I. To calculate I, E needs U's PW and ID. As shown in A of section V our scheme preserves user anonymity hence it's not possible for E to get ID of U. In D of section V we shown that our scheme resists offline password attacks, hence E cannot obtain PW of U without ID and PW, E cannot create a forge login message.
On the other hand, U authenticates S by checking the cipher text $E_R[r_s$,h(ID||r_u||T||T1||K_{us})]. In C of section V we shown that it's not possible for E to forge $E_R[r_s$,h(ID||r_u||T||T1|| K_{us})] to masquerade as S. Only the legal server S who knows the x,h(x) can derive R from $C^{h(x)}$ mod p to decrypt the login message sent by U. Then S can extract r_u,ID and computer r_s and K_{us} can able to frame a valid $E_R[r_s$,h(ID||r_u||T||T1||K_{us})] message .

Secure Session Key Agreement with Perfect Forward Secrecy:

In Bindu et al scheme as discussed in E of section III, MiM attack causes the revealing of secret shared session key between U and S to adversary. In our proposed scheme, User and Server send r_u and r_s in an encrypted format using 'R'. In A of section V we shown that it's computationally infeasible to calculate R by an adversary, hence it's not possible for an adversary, even he is legal user to perform man in the middle attack and decrypt the cipher text containing r_u and r_s. Hence our proposed scheme provides secure session key agreement with perfect forward secrecy (PFS).

COMPARISON OF SECURITY FEATURES

Table I. Comparision of Security Features

Security feature	Bindu et al.'s scheme	Anil K Sarje et al [22]	Anil K Sarje et al [23]	Proposed scheme
Withstanding user impersonation attack	No	No	No	Yes
Withstanding Server masquerade attack	No	No	No	Yes
With standing man in the middle attack	No	No	No	Yes
Achieving mutual authentication	No	No	No	Yes
Preserving User Anonymity	No	No	No	Yes
Preserving Secrecy of remote server secret key	No	No	No	Yes
Withstanding Stolen smart card attack	No	No	No	Yes
Providing Perfect forward secrecy	No	No	No	Yes
Session key exchange	Yes	Yes	Yes	Yes

CONCLUSION

In 2008 Bindu et al.'s proposed an improved remote user authentication scheme preserving user anonymity which is an improved version of the scheme proposed by chien et al in 2004. However in this paper we shown that Bindu et al.'s scheme doesn't preserve user anonymity as they claim to be. In addition we have shown that Bindu et al.'s scheme is vulnerable to numerous attacks like user impersonation attack, server masquerade attack, man in the middle attack, stolen smart card attack and fails to provide with perfect forward secrecy. In addition we proposed our scheme which is an improved version over Bindu et al.'s scheme while preserving all their merits. Our proposed scheme doesn't compromise on any attack even the secret information stored in the smart cards are revealed. We also provided the comparison of various authentication protocols with our proposed one. The comparison table suggests that our protocol is more secure compared to other similar protocols.

REFERENCES

[1] Sandeep Kumar Sood, "An Improved and Secure Smart Card Based Dynamic Identity Authentication Protocol," International Journal of Network Security, Vol.14, No.1, PP.39-46, Jan. 2012

[2] Oliver Kömmerling, Markus G. Kuhn: Design Principles for Tamper-Resistant Smartcard Processors, Proceedings of the USENIX Workshop on Smartcard Technolo^{gy} (Smartcard '99), Chicago, Illinois, USA, May 10-11, 1999, USENIX Association, pp. 9-20,

ISBN 1-880446-34-0.

[3] Richard Clayton, George Danezis, Markus G. Kuhn: Real World Patterns of Failure in Anonymity Systems, in Ira S. Moskowitz (ed.): Information Hiding, 4th International workshop, IHW 2001, Pittsburgh, USA, April 25-17, 2001, Proceedings, LNCS 2137, Springer-Verlag, pp. 230-245, ISBN 3-540-42733-3.

[4] A.K. Awasthi, Comment on 'a dynamic ID-based remote user authentication scheme', Transaction on Cryptology, Vol. 1, No. 2, 2004, pp. 15-17.

[5] E. Brier, C. Clavier, and F. Oliver, Correlation power analysis with a leakage model, Lecture Notes in Computer Science, Vol. 3156, 2004, pp. 135-152.

[6] Y.C. Chen, and L.Y. Yeh, An efficient nonce-based authentication scheme with key agreement, Applied Mathematics and Com- putation, Vol. 169, No. 2, 2005, pp. 982-994.

[7] H.Y. Chien and C.H. Chen, A remote authentication scheme preserving user anonymity, IEEE International Conference on Advanced Information Networking and Appli- cations, Vol. 2, 2005, pp. 245-248

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

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

[10] I-En Liao, C. C. Lee and M. S. Hwang, (2005), "Security enhancement for a dynamic ID-based remote user authentication scheme", in IEEE CS Press, NWeSP'05, pp. 437-440, Seoul, Korea.

[11] A. K. Awasthi, S. Lal, (2004), "Security analysis of a dynamic ID based remote user authentication scheme",\ http://eprint. iacr.org/2004/238.pdf.

[12] M.L. Das, A. Saxena, V. Gulati, and D. Phatak, A novel remote user authentication scheme using bilinear pairings, Computers & Security, Vol. 25, No. 3, 2006, pp. 184-189.

[13] C.S.Bindu, P.C.S.Reddy and B.Satyanarayana, "Improved Remote User Authentication Scheme Preserving User Anonymity," International Journal of Computer Science and Network Security, Vol. 8, No. 3, pp. 62-66(2008).

[14] M.L. Das, V.L. Narasimhan, A simple and secure authentication and key establishment protocol, First International Conference on Emerging Trends in Engineering and Technol- ogy, 2008, pp. 844-849.

[15] Y. Wei, H. Qiu and Y. Hu, Security analysis of

authentication schemes with anonymity for wireless, IEEE International Conference on Communication Technology, 2006, pp. 1-4.

[16] M.S. Hwang, C.C. Lee, and Y.L. Tang, A simple remote user authentication scheme, Mathematical and Computer Modelling, Vol. 36, No. 1, 2002, pp. 103-107.

[17] T.S.Messerges, E.A.Dabbish and R.H.Sloan, "Examing smartcard security under the threat of power analysis attacks," IEEE Transactions on Computers, vol. 5, no. 3, pp. 514-522, 2002.

[18] W.C. Ku, C.M. Chen and H.L.Lee, "Cryptanalysis of a variant of peyravian-Zunic's password authentication scheme," IEEE Transactions on Communications,, vol. E86-B, no. 5, pp. 1682-1684, May 2003.

[19] Wen-Bing Horng, Cheng-Ping Lee, Jian-Wen Peng, "A Secure Remote Authentication Scheme Preserving User Anonymity with Non-Tamper Resistant SmartCards", Web Transactions on Information Science and Applications, Issue 5, Volume 7, pp. 619-628, May 2010.

[20] C. Yang, W. Ma, B. Huang, and X. Wang, Password-based access control scheme with remote user authentication using smart cards, Advanced Information Networking and Applications Workshops, 2007, pp. 448-452.

[21] Mark Stamp "Information Security:Principles and Practise" second edition, Wiley.

[22] Vorugunti chandra Sekhar, Mrudula S, "An Improvement of Anil K Sarje et al.'s Authentication Scheme Using Smart Cards" to apper in IEEEexplore.

[23] Vorugunti chandra Sekhar, Mrudula S, "Cryptanalysis and Improvement of "An Improvement of Liou et al.'s Authentication Scheme using Smart Cards" by Anil K Sarje et al." to apper in IEEEexplore.