Security Analysis of A Dynamic ID-based Remote User Authentication Scheme

Amit K. Awasthi and Sunder Lal

Abstract — *Since 1981, when Lamport introduced the remote user authentication scheme using table, a plenty of schemes had been proposed with table and without table using. Recently Das, Saxena and Gulati have proposed A dynamic ID-based remote user authentication scheme. They claimed that their scheme is secure against ID-theft, and can resist the reply attacks, forgery attacks, and insider attacks and so on.*

In this paper we show that Das et al.'s scheme is completely insecure and using of this scheme is equivalent to an open server access without any password. [1]

Index Terms — Authentication, cryptography, security, cryptanalysis, smart cards, proxy user.

I. Introduction

REMOTE user authentication schemes allow a valid user to login to the remote server and to access the services provided. This authentication process runs over the insecure channels. Lamport's table based authentication scheme was enhanced in 2000, by Hwang and Li [7], to remote user authentication scheme using smart cards. Afterwards many schemes have been proposed to make secure the authentication over insecure channels. [1]-[3]-[4]-[5]-[7]-[8]-[10].

Recently Das et al. proposed a dynamic ID-based authentication scheme in [4]. In this scheme they introduce the concept of dynamic ID to overcome the problem of partial information leakage in static ID based schemes. This also avoids the risk of ID-theft.

In this paper, we shall point out that the Das et al. scheme is completely insecure. We shall show that in 'Login Phase' of this scheme the send login request is password independent. User may type any random password instead of a real one. Scheme does not prevent him from login. Secondly the user having the smartcard issued from the server may repudiate the server to create a new user, because smartcard has a common secret '*y*', which is used to make login for any user.

In my opinion al least a single information for a user must be static. In Das et al.'s scheme both the identity and password are dynamic, which is major drawback of the scheme. We also discuss some results regarding the authentication requirement. These may be beginning stone for the further research in the direction of dynamic identity.

In section II we review the Das et al's scheme. Section III consists of the comments on the scheme. In section IV we propose some rules for an authentication scheme. Finally in section V a brief conclusion is given.

II. Review of the Das et al. Scheme

In this section, we briefly review Das et al. scheme [4]. This scheme is composed of the registration phase, Login phase, authentication phase and the password change phase. The notations used throughout this paper are as follows:

U	the user
PW	the password of user U
S	the remote server
$h(.)$	a one way hash function
$\oplus$	bitwise XOR operation
$A \Rightarrow B$: M	A sends M to B over secure channel
$A \rightarrow B$: M	A sends M to B over insecure channel

Different phases work as follows:

A. Registration Phase

A user U_i wants to register to the remote system S.

1. U_i submits PW_i to S
2. S computes $N_i = h(PW_i) \oplus h(x)$, where x is secret of the remote system.
3. S Personalizes the smartcard with the parameters [$h(.)$, N_i, y], where y is a remote server's secret number stored in each registered user's smartcard.
4. $S \Rightarrow U_i$: PW_i and smartcard.

B. Login Phase

The user wants to login, inserts its smartcard to the terminal and keys his password PW_i. The smartcard perform the following steps:

1. Computes $CID_i = h(PW_i) \oplus h(N_i \oplus y \oplus T)$, where T is the current date and time.
2. Computes $B_i = h(CID_i \oplus h(PW_i))$
3. Computes $C_i = h(T \oplus N_i \oplus B_i \oplus y)$
4. $U_i \rightarrow S$: CID, N_i , C_i , T

C. Authentication Phase

Upon receiving the login request (CID, N_i , C_i , T) at time T^* , S verifies as :

1. Verify the validity of the time interval $T - T^*$
2. Computes $h(PW_i) = CID_i \oplus h(N_i \oplus y \oplus T)$
3. Computes $B_i = h(CID_i \oplus h(PW_i))$

[1] This work was supported in part by the University Grant Commission – INDIA under Grant No. 8-9(98)-(SR-I)

A. K. Awasthi is with the Department of Applied Science, Hindustan College of Science and Technology, Farah, Mathura, UP, INDIA. (E-mail: awasthi_hcst@ yahoo.com)

S. Lal is with the Department of Mathematics, Institute of Basic Science, Dr. B. R. A. University, Agra, UP, INDIA.

.

4. Checks that $C_i = h(T \oplus N_i \oplus B_i \oplus y)$ holds to accept the login request.

D. Password Change Phase

When user wants to change the password he inserts smartcard in to the device, keys thw password PW_i and request to change the password to new one PW_{New}. Smartcard computes $N_i^* = N_i \oplus h(PW_i) \oplus h(PW_{New})$ and replaces the N_i with new N_i^*. Password gets changed.

III. Comment on Das et al. scheme

Weakness of Registration Phase:

Step 1. U_i submits PW_i to S

Step 4. $S \Rightarrow U_i$: PW_i and smartcard

Author are not specific about the channel of communication in step-1. If channel is public, the scheme is vulnerable to the hacking of the password at the very first step of registration.

In step-4 sending of the password PW_i to U_i is redundant. In other way step-1 may be modified as- U_i send request to register. On receiving it server may choose random password and computes the step 2, 3, 4 as it is. On getting random password the user may change this password using password change protocol.

Author used y which seems to be common to the all user. If it is not common table will be required at the server side to maintain it. And if it is common then there is a security threat discussed in next lines.

Login phase (step-4) shows that the information N_i may be publicly accessed. It is not difficult to catch by the user sending the login request. User having a smartcard with parameters $[h(.), N_i, y]$, password PW_i and the information N_i may repudiate the remote server to make a valid registration of some new user. For it he computes $h(x) = N_i \oplus h(PW_i)$.

$h(x)$ is secret information of the remote server to compute the parameter Ni, now the user U_i has all the power to register new user as the remote server. To do so he may simply run a parallel protocol of registration phase. Since y used in this scheme is not authenticated anywhere. This shows that the user U_i may be choose y randomly.

One more possible attack may be as – User simply changes its password by running the change password protocol. Now he makes a duplicate of the smartcard. And again he changes its password. Now the second password with the duplicate smartcard may be given to third party to access the server although the third party is not a valid registered user. Now the new user may authenticate itself to the server. Server has no information about the identity of the user. Hence server is not able to detect who user, either original or fraud, has logged.

The above discussion shows that the registration phase is insecure and having a lot of threats.

Weakness of Authentication Phase (Login & Verification):

This phase is again completely insecure, because whole process of authentication is independent of the password. Attack may work as –

Login Phase

The user wants to login, inserts its smartcard to the terminal and keys a random password P instead of his real password PW_i. The smartcard perform the following steps:

1. Computes $CID_i = h(P) \oplus h(N_i \oplus y \oplus T)$, where T is the current date and time.
2. Computes $B_i = h(CID_i \oplus h(P))$
3. Computes $C_i = h(T \oplus N_i \oplus B_i \oplus y)$
4. $\mathrm{U_i} \rightarrow \mathrm{S}$: CID, N_i, C_i, T

A. Authentication Phase

Upon receiving the login request (CID, N_i, C_i, T) at time T^*, S verifies as :

1. Verify the validity of the time interval $T - T^*$
2. Computes $h(P) = CID_i \oplus h(N_i \oplus y \oplus T)$
3. Computes $B_i = h(CID_i \oplus h(P))$
4. Checks that $C_i = h(T \oplus N_i \oplus B_i \oplus y)$ holds to accept the login request.

Look at the step 3 in login phase, the computation of $C_i = h(T \oplus N_i \oplus B_i \oplus y)$ is password independent, because $B_i = h(CID_i \oplus h(P))$ is equivalent to $h(h(N_i \oplus y \oplus T))$, which is common for any password has been taken. Same discussion for step 4 in authentication phase may be given.

The above discussion shows, C_i will hold true, this shows that this scheme is equivalent to no password scheme, because with any random password user may access the server.

Suppose an intruder theft the smartcard for a short duration and makes a duplicate of it. Now he has no need to crack the password because he may insert any random password. Server will authenticate the intruder as a valid user.

IV. Some Results

Law 1: *To identify an entity in nature at least single unique information must be required.*

It is trivial, if we have to call a person among a crowed. We simply call a name, which represents a person. The person, whose name was asked, listen the request. And then we may identify the person.

Again, if there are more than one person named “Lalit” in that crowed. Than it becomes difficult to identify that of to whom we are intended. Thus the requirement is – the given information must be unique.

For example – We ask a child “Bring a rose”. Child simply goes to the garden and brings a specific type of flower. The unique information, the name “Rose”, represents that flower.

Law 2: *To authenticate an entity al least single information representing the entity must bet static.*

To authenticate an entity, we require more than single information representing an identity. As in above example, we have told a person that the name of person is Lalit, height is 5’ 6’’, thin, handicapped by left hand and so on. Now it becomes very easy to authenticate physically to the person named “Lalit”. Here all information is static.

Now we try to verify this result for just two information, without any loss of generality. Say, first information is

"*Identity*" and other information is "*Password*". We choose these to word according to their meaning too. If both information are static, authentication is trivial.

If one information, say Identity, is static and other "Password " is dynamic. Then for authentication, Server (who wants to authenticate) will compute a challenge by using the static information of the user (who wants to be authenticated). And give this information to solve the user. User may solve this challenge only if he has the other information, password. If challenge is solved user responses the server. And in this way server authenticates the user. Similar proof may be given for static 'Password' and dynamic 'Identity'.

In case both Identity and Password are dynamic. How server will determine the challenge. To make authentication sure both (Identity and Password) should be dependent on each other. Suppose a user sends an updated identity to the server. Server simply computes as challenge. If a user has password, he may solve challenge to response the server. Server authenticates the Identity – Password pair, but not the entity holds it. Because, the identity and password both these are dynamic. There may be a chance the same Identity – Password pair may be taken by some other entity. Then, how server will differentiate them? Obviously, some static information will be required to differentiate them. Hence the result.

V. Conclusion

In this paper we show that the Das et al.'s scheme is completely insecure and works like an open channel. No password is required to authenticate the user. We also introduce two laws which should be hold for each authentication scheme.

We also announce an open problem – Is it possible to create any authentication scheme with only single static information? No dynamic or static password like information is needed. Biometric authentication successfully holds for this problem. So need to device a non-biometric authentication scheme.

.

References

[1] A. K. Awasthi and S. Lal, "An enhanced remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.,* vol. 50, No. 2, pp. 583-586, May 2004.

[2] C. K. Chan and L. M. Cheng, "Cryptanalysis of a remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.,* vol. 46, pp. 992-993, 2000.

[3] C. C. Chang and T. C. Wu, "Remote password authentication with smart cards," *IEE Proceedings-E,* vol. 138, no. 3, pp. 165-168, 1993.

[4] M. L. Das, A. Saxena and V. P. Gulati, "A dynamic ID-based remote user authentication scheme", ," *IEEE Trans. Consumer Electron.,* vol. 50, No. 2, pp. 629 -631, May 2004.

[5] C. C. Chang and S. J. Hwang, "Using smart cards to authenticate remote passwords," *Computers and Mathematics with applications,* vol. 26, No. 7, pp. 19-27, 1993.

[6] C. C. Chang and K. F. Hwang, "Some forgery attack on a remote user authentication scheme using smart cards," *Informatics,* vol. 14, no. 3, pp. 189 - 294, 2003.

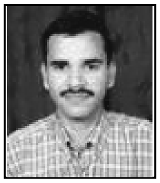
[7] M. S. Hwang and L. H. Li, "A new remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.,* vol. 46, No. 1, pp. 28-30, 2000.

[8] M. Kumar "New remote user authentication scheme using smart cards," *IEEE Trans. Consumer Electron.,* vol. 50, No. 2, pp. 597-600, May 2004.

[9] K. C. Leung, L. M. Cheng, A. S. Fong, and C. K. Chan, "Cryptanalysis of a modified remote user authentication scheme using smart cards", *IEEE Trans. Consumer Electron.,* vol. 49, No. 4, pp. 1243-1245, Nov 2003

[10] J. J. Shen, C. W. Lin and M. S. Hwang, "A modified remote user authentication scheme using smart cards", *IEEE Trans. Consumer Electron.,* vol. 49, No. 2, pp. 414-416, May 2003.

[11] S. J. Wang, "Yet another login authentication using N-dimensional construction based on circle property", *IEEE Trans. Consumer Electron.,* vol. 49, No. 2, pp. 337-341, May 2003.



Amit K Awasthi received his M. Sc. Degree in 1999 from Bareilly College, (M. J. P. Rohilkhand University,) Bareilly. He is currently a lecturer in Department of Applied Science, Hindustan College of Science and Technology, Farah, Mathura, INDIA. He is member of Indian Mathematical Society, Group for Cryptographic Research, Cryptography Research Society of India and Computer Society of India. His current research interests include data security and cryptography.

Sunder Lal is currently a professor and Head of Department of Mathematics, IBS Khandari, Dr. B. R. A. University, Agra, INDIA. He is member of Indian Mathematical Society, Group for Cryptographic Research, and Cryptography Research Society of India. His current research interests include cryptography, number theory and applied algebra.