Improved Remote User Authentication Scheme Preserving User Anonymity

Mrs. C. Shoba Bindu[†], Dr P. Chandra Sekhar Reddy[††] and Dr B.Satyanarayana[†††]

JNTU College of Engineering, Anantapur, A.P, INDIA.
JNTU College of Engineering, Kukatpally, Hydearab, A.P, INDIA.
S.K. University, Anantapur A.P, INDIA.

Summary
In 2004, Das et. al proposed a Dynamic ID based remote authentication scheme to authenticate the users while preserving the user's anonymity .Chein et. al. pointed out that Das et. al scheme fails to protect the user's anonymity and proposed a new scheme to conquer the weakness in 2005. In this paper, we show that Chein et al scheme is insecure against Insider attack and Man-in-middle attack. An improved scheme is proposed that overcomes the security risk.

Key words:
Authentication, Password, Insider attack, Man-in-Middle attack.

1. Introduction

Password authentication with smartcards is one of the convenient and effective two-factor authentication mechanisms. This technology has been widely deployed for various kinds of authentication applications which include remote host login, online banking, access control of restricted vaults, activation of security devices and many more. Several schemes and improvements for remote user authentication schemes using smartcards [1-7, 9, 10] have been proposed.

In 2004, Das et. al. [9] proposed a dynamic ID-based remote user authentication scheme using smartcards which does not maintain any verifier table, allows users to change their password freely and they claimed that their scheme achieves user anonymity. But, in 2005 Chien et. al. [6] pointed out that Das et. al. scheme fails to protect the user's anonymity, and proposed an improved remote user authentication scheme with user anonymity.

In this paper we show that chien et al scheme is vulnerable to insider attack and man–in– middle attack. The remainder of the paper organized as follows: Section 2 reviews the Chein et. al. scheme, Section 3 points out the weakness of the Chein et. al.'s scheme. In section 4 we propose an improved scheme. In section 5, we analyze the security of our scheme. In section 6 we evaluate the efficiency of the proposed scheme. Finally, section 7 gives a brief conclusion.

Manuscript received March 5, 2008
Manuscript revised March 20, 2008

2. Review of Chein et. al. Scheme

In this section, we review the Chein et al. scheme. This scheme is composed of 3 phases namely the registration phase, the login phase and authentication phase. These phases are described as follows: The notations used throughout this paper are as follows:

U_i : The user.
PW_i : The password of user U_i.
ID_i : The identity of user U_i.
S : The remote server.
h (.) : A one way hash function.
$\oplus$: Bitwise XOR operation.
$E_k[x]$: Encryption of x using key k.
$D_k[x]$: Decryption of x using key k.

Registration Phase:

This phase is invoked whenever a user Ui registers with the remote system.
1. Ui selects a password PWi and submits his identity IDi and PWi to the remote system
2. S computes m = h (IDi $\oplus$ x)$\oplus$ h(x) $\oplus$ PWi and I = h((IDi $\oplus$ x) where x is secret key of the remote system.
3. S issues the smartcard to the user with the parameters m, I and the public parameters (h (.), p).

Login Phase:

The user Ui wants to login to the remote system, he inserts his smart card into the terminal, and inputs his IDi and PWi.
1. Generate a random number $r_u = g^x \bmod p$.
2. Compute M= m $\oplus$ PWi.
3. Compute C = M $\oplus$ r_u.
4. Computes R = I$\oplus$ r_u = (h (IDi $\oplus$ x) $\oplus$ r_u.

Ui sends {C,T ,E_R, [r_u, IDi, T] } to Server, where T is timestamp and the E_R [r_u, IDi, T] is cipher text of encrypted using secret key R.

Authentication Phase:

Upon receiving the message, Server authenticates the user Ui as follows:

1. Computes R with server's secret key x ,
   R = C ⊕h (x) then decrypt the message $E_R [r_u, IDi, T]$.
2. Test the validity of time interval between T and T', where T' is a timestamp when server receives the message.
3. Verify whether following equation holds:
   $R= h (IDi⊕x) ⊕ r_u$.
   If the equation does not hold, reject the service request.
4. Deliver the message $E_R [r_s, r_u +1]$ to the user, where $r_s = g^y \bmod p$.
5. Upon receiving the message $E_R [r_s, r_u +1]$ and the user checks whether decrypted data contains the value $r_u +1$. if so, the user can generate the session key $K_{us} = r_S^x = g^{xy}$ and delivers the secret information with server.

3. Weaknesses of Chein et. al. Scheme

In this section, we will show that Chein et. al.'s scheme is vulnerable to an insider attack and man-in –middle attack.

1. Insider Attack:

In the registration phase, user's password will be revealed to the remote system as the user submits his ID and Password PW. If the user uses password to access several servers for his convenience, the insider of the remote system can impersonate U to access other servers [13].

B. Man- in- Middle Attack: An adversary can imitate user while talking to the server and can imitate server while talking to the user.

The basis of the following attacks is based on the risk of smart card stored information. A legitimate user could extract the values stored in smartcard by some means [12, 13] then he/she could perform the Man-in-Middle attack.

In the registration phase, $m = h (IDi ⊕ x)⊕ h(x) ⊕ PWi$ and $I = h(IDi ⊕ x)$ is stored in the Ui 's smartcard. Once Ui extracts m and I from smart card by some means [6, 9] then he/she can easily derive h(x) by computing $h(x)= m⊕ I ⊕ PWi$.An adversary with a valid smart card can now perform the attack as follows:

Adversary intercepts the login message of user Ui: $\{C,T ,E_R [r_u , IDi, T] \}$to the server ,then adversary computes $R=C⊕ h(x)$ and decrypts $E_R [r_u, IDi, T]$. Generates $r_a = g^{x'} \bmod p$ & computes $R'=R⊕ r_u ⊕ r_a$ and $C'=C⊕ r_u ⊕ r_a$ and sends $\{C',T, E_{R'} [r_a, IDi, T]\}$to the server. The server authenticates the adversary as user Ui since $R' = h(IDi⊕ x) ⊕ r_a$ .Then the server delivers the message $E_{R'}[r_s,r_a+1]$ where $r_s = g^y \bmod p$. Now, the adversary intercepts the message and decrypts it using R' and calculates $K_{as} = r_S^{x'} = g^{x'y}$, then the adversary generates the message $E_R [r_{s'}, r_u+1]$ where $r_{s'} = g^{y'} \bmod p$ and sends it to Ui.

Then, Ui decrypts the received message and checks whether decrypted message contains the value r_u+1. if so, the user generates the session key $K_{us'} = r_{S'}^x = g^{xy'}$.

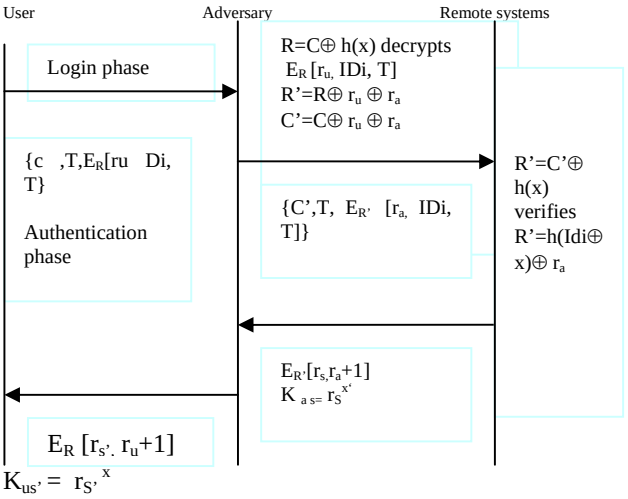

Fig. 1 Man-in-the-middle attack

Thus, the adversary can perform a man in the middle attack and could establish a key with the server and a key with user Ui.

4. The Improved Scheme

In this section, we propose an improved efficient remote user authentication scheme that protects the user's anonymity using the smart cards and overcomes the above mentioned attacks. The scheme is divided into three phases: the registration phase, the authentication and the password change phase. The notations used in this scheme are same as in Chien et. al. scheme. These phases are described as follows:

Registration Phase

First, the user gives the IDi and h(PWi) to remote system for registration. Next the remote system performs the fallowing steps:

1. Computes $m = h (IDi ⊕ x) ⊕h (x) ⊕ h (PWi)$ and $I= h(IDi ⊕ x)⊕ x$. where x is a secret key of server
2. Server issues the smart card to the user, where the smart card contains m, I and public parameters {h( ), P}.

Login Phase

Whenever the user wants to login to remote server S, he inserts his smart card into the terminal, and inputs his IDi and PWi.

1. Generate a random number
   $r_u = g^x \bmod p$.
2. Compute $M=m \oplus h(PWi)$
3. Compute $C=M \oplus r_u$
4. Compute $R= I \oplus r_u = h(IDi \oplus x) \oplus x \oplus ru$.

sends the message $\{C,T,E_R [r_u, IDi, T]\}$ to the server, where T is timestamp and the $E_R [r_u, IDi, T]$ is cipher text of encrypted using the secret key R.

Authentication Phase

After receiving the message, the server computes as follows:

1. Compute R with the server's secret key x, $R= C \oplus h(x) \oplus x$, then decrypts the message $E_R [r_u, IDi, T]$.
2. Test the validity of time interval between T and T' where T' is a time stamp when server receive message.
3. Verify whether the fallowing equation holds $R = h(IDi \oplus x) \oplus x \oplus r_u$. If the equation does not hold, reject the service request.
4. Deliver the message $\{T_1, E_R [r_s, r_u +1, T_1]\}$ to the user, where $r_s = g^y \bmod p$ and T_1 is the current timestamp.
5. Upon receiving the message $\{T_1, E_R [r_s, r_u +1, T_1]\}$, user tests the validity of the time interval and checks whether the decrypted data contains $r_u +1$. If so, the user can generate the session key $K_{us} = r_S^x = g^{xy}$ and that the server is authenticated to the user.
6. Then the user delivers the message $E_{Kus} [r_s +1]$ to the server.
7. Server decrypts the received message and checks whether it is equal to $r_s +1$ or not. If yes, the user is authenticated and that the server can be assured of a session key established between the server and the user.

5. Security analysis of the Improved Scheme

In this section, we are going to demonstrate that our scheme is secure:

1. *Replay attack*: The replay attacks cannot work in our scheme. That is, replaying neither the login message $M = \{C,T,E_R [r_u, IDi, T]\}$ of login phase nor the response message $M' = \{T_1, E_R [r_s, r_u +1, T_1]\}$ of authentication phase will succeed since the validity of M and M^1 can be checked with the time stamps T and T_1, respectively.
2. *Stolen-verifier attack:* Since the scheme had no verification table, nobody could obtain any verifiable information from the server to threaten the protocol. So, the scheme can prevent stolen-verifier attack.
3. *Guessing attack*: Our scheme, don't send the passwords through communication channel. It is only used by the user to trigger the secret value computation in smart card. So, the adversary can't verify his guessing from the eavesdropped data.
4. *Forward Secrecy:* The forward secrecy means that even though the shared secret is disclosed at some point, it will not cause the compromise of any earlier session. Suppose the secret key x is compromised the adversary can intercept the message C and computes $R= C \oplus h(x) \oplus x$, even then he can't know the session key kus, because the session key is computed by $k_{us} = g^{xy}$ based on Diffie-Hellman key exchange protocol. So, our scheme can achieve forward secrecy.
5. *Known-key secrecy:* The known-key security means the compromise of a past session key can't derive any further session key. If the session key K_{us} is known by the adversary, he can't compromise other session key K_{us}, because the session key is generated from random numbers $r_u = g^x$ and $r_s = g^y$ based on Diffie-Hellman protocol
6. *Insider attack:* In the registration phase, user submits h(PW) to the remote system. So, even an insider cannot know the password of a user. Hence, our scheme defends insider attack.
7. *Man-in-the-middle attack:* A registered user with a smart card can not perform this attack as h(x) or x cannot be computed from the values stored in the user's smart card.

6. Efficiency analysis

In this section, we show the comparisons of the efficiency between Chien et. al's scheme and our scheme to demonstrate that our scheme is not only secure but also efficient than Chien et. al's scheme. Table 1 gives the comparisons of efficiency between our scheme and Chien et. al's.

It can be viewed that our scheme can defend insider attack and man-in-the-middle attack with one extra XOR operation in registration phase, one extra hash function in Login phase and with two additional XOR operations in authentication phase, these operations do not cost much. In addition session key verification by the server can be achieved with one encryption done by the user and a decryption done by the system.

Table 1: Comparisons of Efficiency between our scheme and Chein et. al.'s

	Chien et al's scheme		Our Scheme	
	Smart card	System	Smart card	System
Computations of RP	0	3h, 3⊕	0	3h, 4⊕
Computations of LP	3⊕, 1E, 1e	0	1E,3⊕,1h, 1e	0
Computations of AP for authenticating users	0	2h, 1E , 5⊕	0	2h, 1E , 3⊕
Computations of AP for authenticating server & session key generation	1e, 1E	1e, 1E	1e, 1E	1e, 1E
Verification of session key by server	----	----	1E	1E
Information kept in the smart card	M,I , h( ), P	0	M,I , h( ), P	0

h : Computation operation of the hash function e: exponential computation operation
E: Encryption/Decryption operations ⊕: XOR
RP: Registration Phase LP: Login Phase AP: Authentication Phase

7. Conclusion

The threat of smart card security [8, 11, 12] is a crucial concern, where some secret information is stored is the memory of smart cards. It is important to judge the financial cost and time to extract the secret data from the smart card. If the cost as well as time is tolerable or higher than the cost of the secret inside the smart card, then one can take that risk while using smart card to store some secret data. If extracting a secret from the card leads to collapse the whole system (eg: chein et.al's scheme) then definitely some additional counter measure should be taken while designing the scheme.

We have shown that chain e al's scheme is insecure against insider attack and man-in-the-middle attack and have proposed a scheme which defends both the attacks, while still maintaining all the benefits of chein et al's scheme.

References

[1] Amit.K.Awasthi and Sunder Lal, "A Remote User Authentication with Forward Secrecy," *IEEE Transactions on Consumer Electronics*, vol. 49, no. 4, pp. 1246-1248, 2003.

[2] C.Chang, and T.Wu, "Remote Password Authentication with Smart Cards," *IEEE Proceedings – Computers and Digital Techniques*, vol. 138, No. 3, pp. 165-168, 1991.

[3] C.Chang, and S.Hwang, "Using Smart Cards to Authenticate Remote Passwords," *Computers and Mathematics with Application*, vol. 26, No. 7, pp. 19-27, 1993.

[4] E. J. Yoon, E. K. Ryu and K. Y. Yoo, "Further Improvement of an Efficient Password Based Remote User Authentication Scheme Using Smart Cards", IEEE Transactions on Consumer Electronics.

[5] H. Chien, J. Jan, and Y. Tseng, "An Efficient and Practical Solution to Remote Authentication: Smart Card," *Computers and Security*, Vol. 21, no. 4, pp. 372-375, 2002.

[6] Hung-Yu Chien, and Che-Hao Chen, "A Remote Password Authentication Preserving User Anonymity," *Proceedings of the 19th International Conference on Advanced Information Networking and Applications*, (AINA '05), 2005.

[7] I-En Liao, Cheng-Chi Lee and Min-Shiang Hwang " Security Enhancement for a Dynamic ID-based remote user Authentication Scheme" Proceedings of the international conference on Next Generation Web Services Practices(NWeSP'05) 2005.

[8] M.Joye and F. Oliver, "Side channel analysis," *Encyclopedia of cryptography and security*, Kluwer Academic publishers, pp. 571-576, 2005.

[9] M.L.Das, A.Saxena and V.P.Gulathi, " A Dynamic ID-based Remote User Authentication Scheme," *IEEE Transactions on Consumer Electronics*, vol. 50, no. 2, pp. 629-631, 2004.

[10] M.S.Hwang and L.H.Li, " A New Remote User Authentication Scheme Using Smart Cards," *IEEE Transactions on Consumer Electronics*, vol. 46, no. 1, pp. 28-30, Feb 2000.

[11] P.Kocher, J.Jaffe and B.Jun "Differential Power Analysis," Proceedings of Advances in cryptology (Crypto '99), LCNS 1666, pp. 388-397, 1999.

[12] 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.

[13] 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.

C. Shoba Bindu received her B.Tech Degree in Electronics & Comm. Engineering from Jawahar Lal Nehru Technological University, Anantapur, India, in 1997; M.Tech in Computer Science & Engineering from Jawaharlal Nehru Technological University, Anantapur, India, in 2002. She is currently pursuing her Ph.D in Computer Science at Jawahar Lal Nehru Technological University, Anantapur, A.P., India. Her Current Research Interest includes Network Security and Wireless Communication Systems.

Dr. P.Chandra Sekhar Reddy received his B.Tech Degree in Electronics & Communications Engineering from Jawaharlal Nehru Technological University, Anantapur, India. M.Tech in Applied Electronics from Baratiar University. He did his Ph.D. from JNTU, Anantapur in the year 2001 on "Routing in Adhoc Networks". He worked as trainee at ISRO for 10 months. He has a total of 15 years of experience. He has published 10 papers in journals, 20 in conferences and he has also authored a book. Currently he is the Professor coordinator in JNT University, Hyderabad.

Dr. B. Satya Narayana received his B.Sc. Degree in Mathematics, Economics and Statistics from Madras University, India, in 1985; Master of Computer Applications from Madurai Kamraj University in 1988. He did his Ph.D in Computer Networks from S.K. University, Anantapur, A.P., India. He has over 18 years of Teaching and Research experience. His Current Research Interest includes Computer Networks, Network Security and Intrusion Detection.