Appl. Math. Inf. Sci. 6 No. 2S pp. 355S-361S (2012)

Applied Mathematics & Information Sciences
An International Journal

A New Dynamic ID-based User Authentication Scheme to Resist Smart-Card-Theft Attack

Yung-Cheng Lee
Department of Security Technology and Management, WuFeng University, Chiayi 62153, Taiwan
Corresponding author: Email: yclee@wfu.edu.tw

Received June 15, 2011; Revised September 12, 2011; Accepted December 10, 2011
Published online: May 1, 2012

Abstract: Password-based remote authentication schemes provide users with convenient and secure mechanisms to access resources through networks. Such schemes can be further divided into static ID and dynamic ID schemes. The main drawback of the static ID scheme is that an adversary can intercept the fixed login ID and masquerade as a legal user to log into the system. On the other hand, dynamic ID schemes can eliminate the risk of ID-theft and protect user's privacy. In 2004, Das et al. proposed a dynamic ID-based remote user authentication scheme. Their scheme allows users to select and update their passwords freely, and the server does not need to maintain a verifier table. In this paper, we first demonstrate that their scheme is not secure. We then propose an improved scheme for security enhancement. This improved scheme has a dynamic advantage such that an adversary cannot trace the users. Because the smart card generates a different random number for each authentication session, the forward messages are always different for each login. This causes the guessing attacks to fail, because the adversary has not enough information to verify his/her guess. Further, the adversary cannot successfully guess the correct password even if he/she obtains the smart card. Therefore, the proposed scheme can withstand smart-card-theft attack.

Keywords: Password Authentication, Dynamic ID, Smart-Card-Theft Attack

1 Introduction

Remote authentication schemes provide users with convenient and secure mechanisms to access resources through networks. Password authentication is the most widely used mechanism for remote authentication schemes. However, due to the open nature of the Internet, many remote authentication schemes are vulnerable to various attacks such as guessing attack, modification attacks, replay attack, and impersonation attack.

In 1981, Lamport [10] proposed a remote authentication scheme with a one-way hash function. Subsequently, many methods have been proposed to improve the efficiency and security of authentication schemes [3,5,8,12,13,19,22]. The security mechanisms of a few remote authentication schemes are based on smart cards. Because smart cards are portable and tamper-resistant, they are widely used in secure remote authentication schemes [5,7,20,22].

Password-based authentication schemes can be further divided into static ID and dynamic ID schemes. The main drawback of the static ID scheme is that an adversary can intercept the fixed login ID and masquerade as a legal user to log into the system. On the other hand, dynamic ID schemes can eliminate the risk of ID theft [18].

In 2004, Das et al. proposed a dynamic ID-based remote user authentication scheme using smart cards (hereafter referred to as the DSG scheme) [6]. The dynamic ID feature prevents the leakage of identity information during login, thus preventing ID-theft attack. This scheme allows users to select and update their passwords freely. The security of the scheme is based on the secure

one-way hash function. Moreover, this scheme does not need to maintain a verifier table, thereby strengthening the scheme against stolen-verifier attacks. Das et al. stated that their scheme can resist replay attack, forgery attack, guessing attack, and insider attack. However, several papers pointed out a few drawbacks in their protocol [2,9,14,16,23]. Awasthieven and Lal showed that their protocol is password independent and is thus completely insecure [3]. Zhang et al. indicated that any adversary can masquerade as a legal user to log into the server even without the user's password [23]. In addition, Misbahuddin et al. reported several weaknesses in the DSG scheme [16]. Liao et al. [14] showed that the above protocol cannot protect against guessing attack and they proposed an enhanced scheme that achieves mutual authentication. However, Misbahuddin et al. [17] demonstrated that the scheme proposed by Liao et al. cannot withstand impersonation attack and reflection attack. Moreover, it is completely insecure, because a user can successfully log into the remote system with a random password.

In 2009, Wang et al. [21] proposed a scheme to fix security flaws of the DSG scheme. However, Ahmed et al. [1] and Lee et al. [11] showed that their scheme is also vulnerable to various security attacks such as password guessing attack, masquerading attack, denial of service attack and message alteration attack.

In general, a remote authentication scheme is designed for a single-server environment. In a multi-server environment, a user must register with each server individually and memorize different passwords to log into each server. This approach is both inconvenient and impractical. To mitigate this problem, a few user authentication schemes for multi-server environments have been proposed. In these schemes, a user only needs to register with one server once, and then he/she will be allowed to log into any server in the system. In 2009, Liao et al. [15] proposed a dynamic ID-based remote user authentication scheme for multi-server environments. However, Chen et al. [4] revealed that the scheme proposed by Liao et al. is vulnerable to insider attack.

In this paper, we first demonstrate that the DSG scheme is vulnerable to guessing attack and impersonation attack. An adversary can successfully guess the password and masquerade as a legal user to log into the system. We propose an improved scheme to enhance the security. The dynamic ID feature of the improved scheme offers an advantage in that it can resist guessing attack and smart-card-theft attack.

The rest of the paper is organized as follows. In Section 2, we briefly describe the DSG scheme and discuss its drawbacks. In Section 3, we propose a new improved scheme to enhance the security. The security analysis and discussions are presented in the next section. Finally, we make conclusions.

2 The DSG Scheme and Its Drawbacks

2.1 The DSG Scheme

The DSG scheme [6] includes the following related phases: (1) the registration phase and (2) the authentication phase. The registration phase is performed only at the first time that the user intends to join the system, and the authentication phase is executed every time the user logs into the system. The notations used throughout this paper are as follows:

U_i: a qualified user.
PW_i: U_i's password.
S: the server that users intend to log into.
$h(.)$: a secure one-way hash function.
$\oplus$: bitwise XOR operation.
DID_i: user's dynamic identity.
x: the secret key of the server.
T: a timestamp.
$A \Rightarrow B : M$: A sends M to B through a secure channel.
$A \rightarrow B : M$: A sends M to B through a public channel.

2.1.1 Registration Phase

In the registration phase, user U_i sends password PW_i to server S. The server performs the following steps:

R-1 Compute a nonce $N_i = h(PW_i) \oplus h(x)$ □, where x is the secret key of the server.
R-2 Install a smart card with $h(.)$, N_i, and y, where y is the server's secret information.
R-3 $S \Rightarrow U_i$: smart card.
The server forwards the smart card to the user.

2.1.2 Authentication Phase

This phase is performed whenever a user wants to log into the remote system. The authentication phase is further divided into the login phase and the verification phase as follows.

(A) Login Phase

User U_i inserts the smart card into the card-reader, and then inputs password PW_i. The smart card performs the following steps:

L-1 Compute the user's dynamic identity DID_i using PW_i, N_i, y, and timestamp T as follows: $DID_i = h(PW_i) \oplus h(N_i \oplus y \oplus T)$.

L-2 Compute $B_i = h(DID_i \oplus h(PW_i))$.

L-3 Compute $C_i = h(N_i \oplus B_i \oplus y \oplus T)$.

L-4 $U_i \rightarrow S$: DID_i, N_i, C_i, T.

The user sends the message $\{DID_i, N_i, C_i, T\}$ to the server after the completion of steps L-1 to L-3.

(B) Verification Phase

Upon receiving the login message $\{DID_i, N_i, C_i, T\}$, the server authenticates user U_i by performing the following steps:

V-1 Check whether timestamp T is in the expected time interval. The server accepts the login request and proceeds with the authentication process only if the received message is nearly online.

V-2 Compute $h(PW_i) = DID_i \oplus h(N_i \oplus y \oplus T)$ □.

V-3 Compute $B_i = h(DID_i \oplus h(PW_i))$ □.

V-4 Compute $C_i' = h(N_i \oplus B_i \oplus y \oplus T)$, and check whether the received message C_i is equal to C_i'. If it holds, then the server accepts the login request; otherwise, the server rejects the login request and terminates the operation.

2.1.3 Password Update Phase

The DSG scheme allows users to update their passwords freely. If user U_i wants to update his/her password, the procedure is as follows:

U-1 U_i inserts the smart card into the card-reader and inputs his/her password PW_i.

U-2 U_i chooses a new password PW_{i_new}.

U-3 The smart card computes $N_{i\_new} = N_i \oplus h(PW_i) \oplus h(PW_{i\_new})$. Note that $N_{i-new} = h(PW_{i\_new}) \oplus h(x)$.

U-4 The smart card replaces N_i with N_{i_new}. Henceforth, the user can log into the system by using the new password PW_{i_new}.

2.2 Drawbacks of the DSG Scheme

The security of the DSG scheme is based on a one-way hash function. This scheme allows users to select and update their passwords freely, and it can also resist ID-theft attack, replay attack, and stolen-verifier attack. However, in this section, we demonstrate that the DSG scheme is vulnerable to guessing attack and impersonation attack. The guessing attack is initiated by an insider of the system, whereas the impersonation attack can be initiated by any adversary. The attacks are described in detail as follows.

2.2.1 Guessing Attack

Let us suppose that user U_i intends to masquerade as the legal user U_j to log into the system; the procedure is as follows:

G-1 First, user U_i intercepts message N_j in step L-4 after U_j's login request.

G-2 Next, U_i computes $N_i \oplus N_j$. Note that:

$$\begin{aligned} & N_i \oplus N_j \\ &= h(PW_i) \oplus h(x) \oplus h(PW_j) \oplus h(x) \\ &= h(PW_i) \oplus h(PW_j). \end{aligned}$$

G-3 Using $N_i \oplus N_j$, U_i obtains U_j's hashed password $h(PW_j)$ by $(N_i \oplus N_j) \oplus h(PW_i)$. In general, for easy memorization, the bit-length of the password is always fairly short. Thus, PW_j can be easily guessed with the help of $h(PW_j)$.

From the above discussions, insider U_i can obtain U_j's password PW_j. Therefore, the DSG scheme cannot resist the insider's guessing attack.

2.2.2 Impersonation Attack

The DSG scheme is also vulnerable to impersonation attack. Let us suppose that an adversary A intends to masquerade as a legal user U_i to access the system. The adversary performs the following:

I-1 Intercepts the message (DID_i, N_i, C_i, T) after U_i forwards a login request.

I-2 Computes N_i' by $N_i' = N_i \oplus T \oplus T'$, where T' is the current timestamp.

I-3 $A \rightarrow S$: DID_i, N_i', C_i, T'.

The adversary sends the message $\{DID_i, N_i', C_i, T'\}$ to the server. The server will

accept the login request according to the following theorem:

Theorem 1. *An adversary can successfully masquerade as a legal user to log into the server, if he/she replaces message* N_i *and timestamp T with* $N_i \oplus T \oplus T'$ *and T', respectively.*

Proof: We prove the theorem according to the verification steps. In the verification phase, upon receiving the login message (DID_i, N_i', C_i, T'), the server performs the following steps:

V-1' Verify the validity of the time. *T'* is valid if the transmission delay is within a reasonable time interval.

V-2' Compute $DID_i \oplus h(N_i' \oplus y \oplus T')$.

Because

$$DID_i \oplus h(N_i' \oplus y \oplus T')$$
$$= DID_i \oplus h((N_i \oplus T \oplus T') \oplus y \oplus T')$$
$$= DID_i \oplus h(N_i \oplus y \oplus T)$$
$$= h(PW_i),$$

the server can obtain $h(PW_i)$ by computing $DID_i \oplus h(N_i' \oplus y \oplus T')$.

V-3' Compute $B_i = h(DID_i \oplus h(PW_i))$ □ Note that:

$B_i = h(DID_i \oplus h(PW_i)) = h(N_i' \oplus y \oplus T')$.

V-4' Check whether C_i is equal to $h(N_i' \oplus B_i \oplus y \oplus T')$. If this condition is true, the server accepts the login request. Note that because $N_i' = N_i \oplus T \oplus T'$, thus:

$$h(N_i' \oplus B_i \oplus y \oplus T')$$
$$= h(N_i \oplus T \oplus T' \oplus B_i \oplus y \oplus T')$$
$$= h(N_i \oplus B_i \oplus y \oplus T)$$
$$= C_i.$$

Therefore, the server will accept the login request. That is, if the adversary sends the message $\{DID_i, N_i', C_i, T'\}$, where $N_i' = N_i \oplus T \oplus T'$, to the server, the server will accept the login request. Therefore, the DSG scheme cannot withstand impersonation attack.

3. The Improved Scheme

In this section, we present an improved scheme to fix the flaws of the DSG scheme. This improved scheme includes registration phase, authentication phase, and password update phase.

3.1. Registration Phase

The registration phase of the improved scheme is similar to that of the DSG scheme as follows:

LR-1 $U_i \Rightarrow S: PW_i$.

User U_i sends password PW_i to remote server *S*.

LR-2 $S \Rightarrow U_i$: smart card.

On receiving PW_i, the server computes $N_i = h(PW_i) \oplus h(x)$ and installs $\{h(.), N_i, h(x)\}$ in the smart card. Next, the server sends the smart card to the user. Note that the only built-in parameters in the smart card are $h(.)$, N_i, and $h(x)$. An adversary cannot obtain $\{h(.), N_i, h(x)\}$ by any means, because smart cards are tamperproof.

3.2 Authentication Phase

The authentication phase is also further divided into login phase and verification phase. In the authentication phase, user U_i sends a login request to server *S*. After successful verification of the login request, the server allows the user to access the system. The login phase and the verification phase proceed as follows.

3.2.1 Login Phase

If a user U_i intends to log into the system, he/she inserts a smart card into the card-reader and inputs his/her password PW_i. The smart card performs the following procedure after PW_i is proved:

LL-1 Generate a random number *R* and compute the dynamic identity DID_i by:

$DID_i = h(PW_i) \oplus h(N_i \oplus h(x) \oplus R)$.

LL-2 Compute $B_i = h(N_i \oplus h(N_i \oplus h(x) \oplus R))$.

LL-3 Compute $C_i = h(B_i \oplus h(x) \oplus T)$, where *T* is the timestamp.

LL-4 $U_i \rightarrow S: DID_i, C_i, T$.

The user sends the message $\{DID_i, C_i, T\}$ to the server. Note that the random number *R* is updated for every authentication session, thereby B_i also will be renewed for each login.

3.2.2 Verification Phase

Upon receiving the login message $\{DID_i, C_i, T\}$, the server authenticates user U_i by performing the following steps:

LV-1 Verifies the validity of timestamp T. If T is within an expected time interval, the server accepts the login request; otherwise, the request is rejected.

LV-2 Computes $B_i = h(DID_i \oplus h(x))$ □. Note that:

$$B_i = h(DID_i \oplus h(x))$$
$$= h(h(PW_i) \oplus h(N_i \oplus h(x) \oplus R) \oplus h(x))$$
$$= h(N_i \oplus h(N_i \oplus h(x) \oplus R)).$$

LV-3 Compute $C_i' = h(B_i \oplus h(x) \oplus T)$ and check whether the received message C_i is equal to C_i'. If this condition is true, the server accepts the login request; otherwise, it rejects the login request and terminates the operation.

3.3 Password Update Phase

Our scheme also allows users to update their passwords freely. If a user wants to update his/her password, the update procedure is identical to that of the DSG scheme.

4. Security Analysis and Discussions

The dynamic ID feature is an advantage of remote authentication schemes. The dynamic ID property protects authentication schemes from ID-theft attack. An adversary cannot trace the user if the forward message is really dynamic. Thus far, many improved schemes have been proposed in order to enhance the security of authentication schemes. However, most improved schemes cannot ensure really dynamic, because a few transmitted parameters are fixed. Any adversary can trace the user by using the fixed message. For example, in Misbahuddin's scheme [16], the user sends the message $\{ DID_i, N_i, ID_i, T \}$ to the server. An adversary can determine that the message is sent by the same user, if he/she intercepts the same N_i and ID_i on two authentication sessions. Therefore, the advantage of the dynamic ID is lost in these schemes.

The proposed scheme achieves a really dynamic ID feature, because each element in the message $\{ DID_i, C_i, T \}$ is updated for every login session. The request message is refreshed such that the adversary cannot replay the intercepted ID to log into the system, and he/she cannot trace the user with the intercepted message. Therefore, the proposed scheme is indeed a dynamic identity scheme.

The improved scheme has its merits, as reported by Das et al. [6]. Moreover, it can resist impersonation attack, guessing attack, and smart-card-theft attack. A smart-card-theft attack indicates that an adversary obtains a smart card and uses that card to gain access to the system. The proposed improved scheme has the following security features.

(1) It can resist impersonation attack. In the verification phase, the server checks whether $C_i = h(B_i \oplus h(x) \oplus T)$. It is impossible for an adversary to obtain B_i and to successfully masquerade as a legal user to log into the system, without knowing the secret information $h(x)$. Thus, this improved scheme can withstand impersonation attack.

(2) It can resist guessing attack. In the improved scheme, the smart card generates a different random number for each login session. A random number R is adopted in the scheme so that the forward message $\{ DID_i, C_i, T \}$ always varies for each login attempt. The adversary's guessing attack fails, because there is no enough information to verify the guess. As a result, even if an adversary obtains the smart card and inputs the candidate password to login, his/her attempt fails because he/she cannot know whether his/her guess is correct.

(3) It can resist smart-card-theft attack. Smart cards are important devices because they are simple and convenient to use. However, if cardholders lose their smart cards, they are prone to security risk. With the smart card, an adversary can guess the password to log into the system. A legal user may incur a greater loss if the smart card is used for financial transactions or other important applications. In general, when an adversary obtains the smart card, he/she can perform the following steps to guess the password before attempting to log into the system.

S-1 Intercept the login message as described in step L-4 in section 2.

S-2 Obtain the smart card by any means. For example, if an adversary is aware of the fact that a VIP has a large sum of money deposited in his/her bank account, the adversary will intentionally steal the smart card of the VIP to gain access to his/her financial resources.

S-3 Input the same timestamp and attempt to guess the password. The adversary can verify his/her guess by comparing the output message with the previous intercepted message. If the output

message of the smart card is the same as the previous intercepted message, the guess is successful; otherwise, the process continues until the correct password is obtained.

In our improved scheme, because of different random number generated for each login session, the output of the smart card always varies even if the adversary inputs the same parameters to the card. This causes the guessing attack to fail, because the comparison method is rendered unworkable. Thus, an adversary cannot successfully guess the exact password despite gaining possession of the smart card. Therefore, the smart-card-theft attack is avoided.

5. Conclusions

Password authentication schemes are simple mechanisms for remote authentication. In 2004, Das et al. proposed a dynamic ID-based remote user authentication scheme using smart cards. Their scheme allows users to select and update their passwords freely, and the server does not need to maintain a verifier table. In this paper, we show that their scheme is as not secure as they declared. Their scheme is vulnerable to guessing attack and an adversary can masquerade as a legal user to log into the system. Finally, we propose an improved scheme to enhance the security. The scheme has the following merits:

(1) It has dynamic identity feature such that adversaries cannot trace the users.
(2) It can resist impersonation attack and guessing attack. In the proposed scheme, the smart card generates a different random number for each session; consequently, the forward messages are always different for each login session. This causes guessing attacks to fail, since the adversary does not have enough information to verify his/her guess.
(3) In addition, it can resist smart-card-theft attack. In the improved authentication scheme, because of the generation of a different random number for each login session, the output messages of the smart card always vary even if the same parameters are input to this card. This causes the guessing attacks to fail, because the comparison method is rendered unworkable. Thus, an adversary cannot successfully guess the correct password even if he/she obtains the smart card, thereby the improved scheme can resist smart-card-theft attack.

Acknowledgments

The author gratefully acknowledges the helpful comments and suggestions of Prof. Y.C. Hsieh and the reviewers, which have improved the presentation.

References

[1] M.A. Ahmed, D.R. Lakshmi and S.A. Sattar, Cryptanalysis of A More Efficient and Secure Dynamic ID-Based Remote User Authentication Scheme. International Journal of Network Security & Its Applications, Vol.1, No.3, (2009), 32-37.

[2] A.K Awasthi, Comment on A Dynamic ID-based Remote User Authentication Scheme. Transaction on Cryptology, Vol.1, No.2, (2004), 15-16.

[3] A.K. Awasthi and S. Lal, A Remote User Authentication Scheme Using Smart Cards with Forward Secrecy. IEEE Transactions on Consumer Electronics, Vol.49, No.4, (2003), 1246-1248.

[4] T.Y. Chen, M.S. Hwang, C.C. Lee and J.K. Jan, Cryptanalysis of A Secure Dynamic ID Based Remote User Authentication Scheme for Multi-Server Environment. Proceedings of the Fourth International Conference on Innovative Computing, Information and Control, (2009).

[5] H.Y. Chien, J.K. Jan and Y.M. Tseng, An Efficient Solution to Remote Authentication: Smart Card. Computers & Security, Vol.21, No.4, (2002), 372-375.

[6] 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), 629-631.

[7] M.S. Hwang, C.C. Lee and Y.L. Tang, A Simple Remote User Authentication Scheme. Mathematical and Computer Modeling, Vol.36, (2002), 103-107.

[8] T. Kwon and J. Song. Efficient and Secure Password-Based Authentication Protocols against Guessing Attack. Computer Communications, Vol.21, (1998), 853-861.

[9] W.C. Ku and S.T. Chang, Impersonation Attack on a Dynamic ID-Based Remote User Authentication Scheme Using Smart Cards. IEICE Transactions on Communications, Vol.E88-B, No.5, (2005), 2165-2167.

[10] L. Lamport, Password Authentication with Insecure Communication. Communications of ACM, Vol.24, (1981), 770-772.

[11] H. Lee, D. Choi, Y. Lee, D. Won and S. Kim, Security Weaknesses of Dynamic ID-based Remote User Authentication Protocol. Proceedings of the World Academy of Science Engineering and Technology, Is.59, (2009), 190-193.

[12] C.C. Lee, M.S. Hwang and W.P. Yang, A Flexible

Remote User Authentication Scheme Using Smart Cards. ACM Operating Systems Review, Vol.36, No.3, (2002), 46-52.

[13] C.C. Lee, L.H. Li and M.S. Hwang, A Remote User Authentication Scheme Using Hash Functions. ACM Operating Systems Review, Vol.36, No.4, (2002), 23-29.

[14] I.E. Liao, C.C. Lee and M.S. Hwang, Security Enhancement for A Dynamic ID-Based Remote User Authentication Scheme. Proceedings of the International Conference on the Next Generation Web Services Practices, (2005), 22-26.

[15] Y.P. Liao and S.S. Wang, A Secure Dynamic ID-Based Remote User Authentication Scheme for Multi-Server Environments. Computer Standards & Interfaces, Vol.31, No.1, (2009), 24-29.

[16] M. Misbahuddin, M.A. Ahmed, A.A. Rao, C.S. Bindu and M.A.M. Khan, A Novel Dynamic ID-Based Remote User Authentication Scheme. Proceedings of the 2006 Annual India Conference, (2006), 1-5.

[17] M. Misbahuddin and C.S. Bindu, Cryptanalysis of Liao-Lee-Hwang's Dynamic ID Scheme. International Journal of Network Security, Vol.6, No.2, (2008), 211-213.

[18] A. Saxena, M.L. Das, V.P. Gulati and D.B. Phatak, Dynamic Remote User Authentication. Proceedings of the International Conference on Advanced Computing and Communications, (2004), 313-315.

[19] J.J. Shen, C.W. Lin and M.S. Hwang, A Modified Remote User Authentication Scheme Using Smart Cards. IEEE Transactions on Consumer Electronics, Vol.49, No.2, (2003), 414-416.

[20] H.M. Sun, An Efficient Remote User Authentication Scheme Using Smart Cards. IEEE Transactions on Consumer Electronics, Vol.46, No.4, (2000), 958-961.

[21] Y.Y. Wang, J.Y. Liu, F.X. Xia and J. Dan, A More Efficient and Secure Dynamic ID-Based Remote User Authentication Scheme. Computer Communications, (2009), 586-585.

[22] W.H. Yang and S.P. Shieh, Password Authentication Schemes with Smart Card. Computer & Security, Vol.18, No.8, (1999), 727-733.

[23] X. Zhang, Q. Feng and M. Li, A Modified Dynamic ID-based Remote User Authentication Scheme. Proceedings of the 2006 International Conference on Communications, Circuits and Systems, Vol.3, (2006), 1602-1604.

Yung-Cheng Lee received the Ph.D. degree in Electrical Engineering from National Cheng Kung University, Taiwan, in 1999. He was the Chairman of the Department of Electrical Engineering and Department of Computer Science and Information Engineering, National Formosa University; and also was the Dean of Security and Engineering School. Currently, he is the Dean of Academic Affair, WuFeng University, Taiwan. His research interests include network security, artificial intelligence and cryptography.