Dynamic ID-Based Password Authentication Protocol with Strong Security against Smart Card Lost Attacks

Qi Xie

School of Information Science and Engineering,
Hangzhou Normal University Hangzhou 310036, China
qixie68@yahoo.com.cn

Abstract. Seeing that the existing dynamic ID-based password authentication protocols are vulnerable to various attacks, a novel dynamic ID-based password authentication protocol using smart card is proposed. Compared to the existing protocols, the proposed protocol can protect the user's anonymity, can resist the password guessing attacks and smart card lost attacks. On the other hand, our protocol has many advantages, such as perfect forward security, no verification tables, no server's public key and timestamp. To the best of my knowledge, this is the first secure dynamic ID-based password authentication protocol.

Keywords: password authentication protocol, dynamic ID, smart card, anonymity.

1 Introduction

In order to access any resource of the remote server, the user and the server should pass through the mutual authentication in public networks. Password authentication is one of the simplest and the most widely used strategies, because the user only needs to use the short password. However, one of the major challenges of designing password authentication protocols is how to resist the password guessing attacks, as password is supposed to be easy-to-remember, and the password space is small.

In 1981, Lamport [1] proposed the first password authentication protocol with verification table, but this protocol is insecure if the verification table was modified or stolen. Therefore, how to design smart card based password authentication protocols without verification table is an important research topic. In 1993, Chang-Wu [2] introduced password authentication scheme with smart cards using public-key cryptography, but it requires high computation cost for implementation and public key directory for maintain and protection. Thus, many researchers dedicated to design password authentication schemes with smart cards without server's public key, and proposed many schemes [3-8]. However, most of them have been broken shortly after they were proposed [5-8]. Especially, most of the existing schemes are vulnerable to the off-line password guessing attacks if all the secret numbers stored in the smart card are disclosure.

In most of the proposed user authentication protocols the user's identity was static. Thus, it will leak partial information about the user to the adversary over an insecure channel, and cannot protect the user's privacy. Therefore, Das et al.[9] proposed a

P. Sénac, M. Ott, and A. Seneviratne (Eds.): ICWCA 2011, LNICST 72, pp. 412–418, 2012.

dynamic ID-based remote user authentication scheme using smart cards in 2004. Though their scheme has many advantages, Awashti [10] showed that their scheme is insecure, because no password is required to authenticate the user. Chien-Chen [11], Ku-Chang [12] and Liao et al.[13] also pointed out that Das et al.'s scheme cannot protect the user's anonymity, suffers from impersonation attack and guessing attacks, respectively. Moreover, Liao et al. proposed an improved scheme, but Misbahuddin et al. [14] showed that their scheme cannot resist impersonation attack and reflection attack. Recently, Wang et al. [15] proposed another improved dynamic ID-based remote user authentication scheme and claimed that their scheme is more efficient and secure than Das et al.'s scheme. However, Khan et al. [16] showed that their scheme has four weaknesses and proposed an improved scheme. In 2010, He et al. [17] pointed out that Khan et al.'s scheme still suffers from three weaknesses. Thus, Das et al. and all the improved schemes are insecure.

In this paper, we proposed a novel dynamic ID-based password authentication protocol using smart card. Compared to the existing protocols, the proposed protocol can protect the user's anonymity, can resist the password guessing attacks and smart card lost attacks. On the other hand, our protocol has many advantages, such as perfect forward security, no verification tables, no server's public key and timestamp.

2 The Proposed Protocol

In this section, we propose a novel dynamic ID-based user authentication protocol, which consists of three phases: user registration, authentication and session key generation, password change.

The following notations are used throughout this paper:

- p, q : two large prime numbers, such as $q \mid p-1$.
- g : a primitive element for $GF(p)$ with order q .
- U_i : the user.
- S : the server.
- ID_i : U_i 's identity.
- SC : smart card.
- PW_i : U_i 's password.
- x : S 's secret number.
- SK : a session key between U_i and S .
- $h()$: a secure one-way hash function.

2.1 User Registration

U_i and S carry out the following steps during the user registration phase

Step 1: U_i chooses his password PW_i and identity ID_i , and sends ID_i to S .

Step 2: After receiving ID_i from U_i , S computes

$$N_0 = h(ID_i)^x \bmod p\,, \tag{1}$$

where x is the secret number of S. S stores ID_i, one-way hash function $h()$ and N_0 into a smart card (SC for short) and issues this smart card to U_i via secure communication channel.

Step 3: When SC is available, U_i inserts SC into a terminal device, keys his password PW_i, then SC computes

$$N_i = N_0 \oplus h(PW_i) = h(ID_i)^x \oplus h(PW_i) \bmod p\,, \tag{2}$$

and replaces N_0 with N_i.

2.2 Authentication and Session Key Generation

When U_i is about to logon to the server S, U_i and S carry out the following protocol. Figure 1 illustrates this phase.

Step 1: U_i inserts smart card into a terminal device, keys his password PW_i, SC generates random nonce b and k, computes

$$N_s = g^k \bmod p\,, \tag{3}$$

$$CID = h(ID_i)^b \bmod p\,, \tag{4}$$

$$C_0 = (N_i \oplus h(PW_i))^b = h(ID_i)^{xb} \bmod p\,, \tag{5}$$

$$C_1 = C_0 \oplus N_s = h(ID_i)^{xb} \oplus N_s \bmod p\,, \tag{6}$$

Then U_i sends (C_1, CID) to S.

Step 2: After receiving (C_1, CID), S generates a random nonce d, computes

$$N_u = g^d \bmod p\,, \tag{7}$$

$$N_s = C_1 \oplus CID^x \bmod p\,, \tag{8}$$

$$h(N_s{}^d)\,, \tag{9}$$

and sends $(h(N_s{}^d), N_u)$ to U_i.

Step 3: When $h(N_s{}^d)$ and N_u are available, U_i computes $h(N_u{}^k)$, and checks if

$$h(N_s{}^d) = h(N_u{}^k)\,. \tag{10}$$

If so, then S is authenticated, U_i computes and sends $h(N_u{}^k + 1)$ to S. Otherwise, abort.

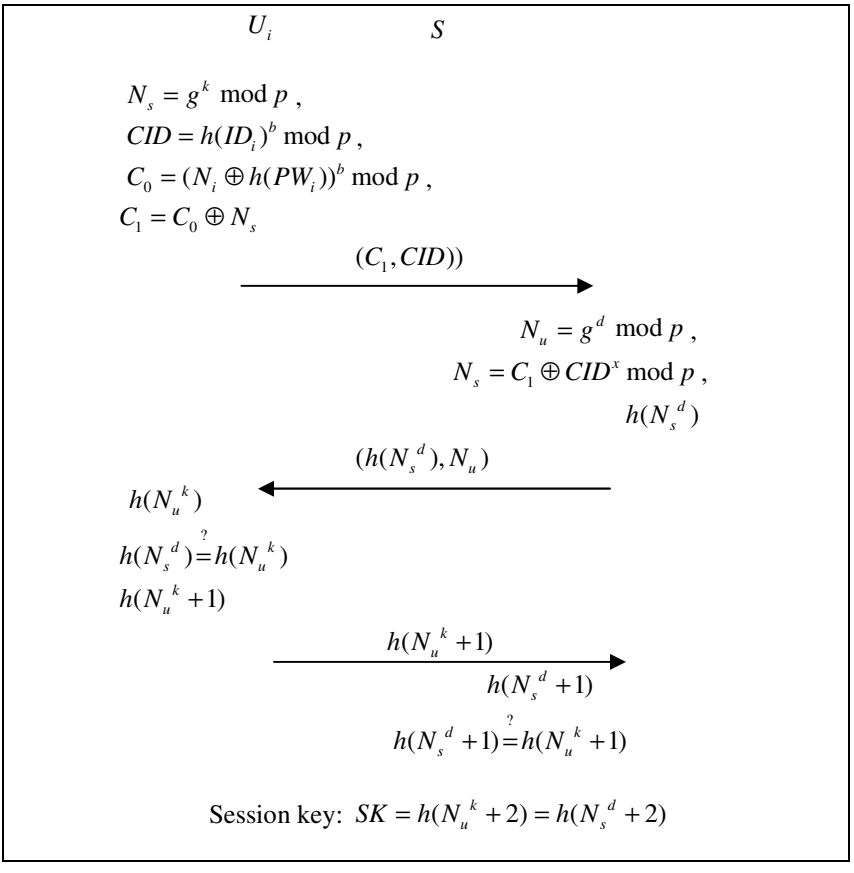

Fig. 1. Authentication and session key generation phase

Step 4: After receiving $h(N_u{}^k + 1)$, S computes $h(N_s{}^d + 1)$ and checks if

$$h(N_s{}^d + 1) = h(N_u{}^k + 1) \tag{11}$$

If so, then U_i is authenticated.

The session key shared between U_i and S is

$$SK = h(N_u{}^k + 2) = h(N_s{}^d + 2). \tag{12}$$

2.3 Password Change

When U_i wants to change his password, he inserts smart card into a terminal device, keys his old password PW_i and the new password PW_{new}, the SC computes

$$N_{new} = h(PW_i) \oplus N_i \oplus h(PW_{new}), \tag{13}$$

and replaces N_i with N_{new}.

3 Security Analysis

In this section, we show that the proposed scheme can resist all sorts of the existing attacks. To the best of my knowledge, this is the first secure dynamic ID-based password authentication protocol.

3.1 Password Guessing Attack and Smart Card Lost Attack

If an attacker obtains $N_i = h(ID_i)^x \oplus h(PW_i) \bmod p$ stored in the user U_i's smart card, and wants to guess the password PW_i by the following two cases.

Case 1: Attacker does off-line password guessing attack by eavesdropping the interactive messages between U_i and S. Obviously, the attacker can get all interactive messages $(C_1, CID))$, $(h(N_s{}^d), N_u)$ and $h(N_u{}^k + 1)$, where $N_s = g^k \bmod p$ and $N_u = g^d \bmod p$, $N_u{}^k$ and $N_s{}^d$ are the Diffie-Hellman values of N_u and N_s, which include the random nonce k and d. However, the attacker cannot find the relationship between $h(ID_i)^x$ and interactive messages $(C_1, CID))$ without knowing x and b. Therefore, an attacker cannot verify whether his guessed password is right or not.

Case 2: If an attacker does on-line password guessing attack, it is still impossible. Since the attacker can guess the password $PW_i^{'}$ and compute

$$C_0^{'} = (N_i \oplus PW_i^{'})^e, \tag{14}$$

$$C_1^{'} = C_0^{'} \oplus g^f, \tag{15}$$

$$CID^{'} = h(ID_i)^e \tag{16}$$

for randomly chosen e and f, and sends $(C_1^{'}, CID^{'}))$ to S, but he cannot generate the right $h(N_u{}^e + 1)$ for S. Therefore, S can detect the attacker.

3.2 Replay Attack

If an attacker replay user U_i 's login message $CID = h(ID_i)^b \bmod p$ and $C_1 = C_0 \oplus N_s = h(ID_i)^{xb} \oplus N_s \bmod p$, S can retrieve N_s but the attacker cannot. S can return the authentication message $h(N_s{}^d)$ and N_u, which include the random nonce d and Diffie-Hellman value $N_s{}^d$, but the attacker cannot verify whether the authentication message $h(N_s{}^d)$ is right or not. On the other hand, the attacker cannot generate the authentication message $h(N_u{}^k + 1)$ and pass through the authentication of S. Therefore, the proposed protocol can resist the replay attack.

3.3 Impersonation Attack and Forgery Attack

If a legal user U_v wants to impersonate U_i to pass through the authentication of S, but it is impossible. The reason is that U_v cannot generate the correct authentication message $h(N_u^{\,k}+1)$ and pass through the authentication of S without knowing the U_i's password.

3.4 Perfect Forward Security

In proposed protocol, the session key is forward security. Since an attacker cannot obtain all the random nonce k and d, even if he knows the user's password PW_i, S's secret number x, N_i, N_u and N_s. So he cannot get the Diffie-Hellman values $N_u^{\,k}$ or $N_s^{\,d}$ between the server and the user. Therefore, an attacker cannot compute

$$SK = h(N_u^{\,k}+2) = h(N_s^{\,d}+2)\,. \tag{17}$$

3.5 Known Key Security

In proposed protocol, because the session key $SK = h(N_u^{\,k}+2) = h(N_s^{\,d}+2)$ is dependent to the random nonce k and d, which are different to other sessions. Therefore, an attacker cannot know the previous or the future session keys when he gets one session key.

3.6 The User's Anonymity and Untraceability

In proposed protocol, the user U_i's ID_i is hidden in the authentication messages $CID = h(ID_i)^b \bmod p$ and $C_1 = C_0 \oplus N_s = h(ID_i)^{xb} \oplus N_s \bmod p$, which include the one-time-used random nonce b. Therefore, our protocol keeps user's anonymity and untraceability.

4 Conclusions

In this paper, we proposed the first secure dynamic ID-based password authentication protocol. Compared to the existing protocols, the proposed protocol has many advantages, for example, it can protect the user's anonymity; can resist the password guessing attacks and smart card lost attacks.

Acknowledgments. This research was supported by National Natural Science Foundation of China (No.61070153).

References

1. Lamport, L.: Password Authentication with Insecure Communication. Communications of the ACM 24, 770–772 (1981)
2. Chang, C.C., Wu, T.C.: Remote Password Authentication with Smart Cards. IEE Proceedings-E Computers and Digital Techniques 138, 165–168 (1993)
3. Hsiang, H.C., Shih, W.K.: Weaknesses and Improvements of the Yoon–Ryu–Yoo Remote User Authentication Scheme using Smart Cards. Computer Communications 32, 649–652 (2009)
4. Kim, S.K., Chung, M.G.: More Secure Remote User Authentication Scheme. Computer Communications 32, 1018–1021 (2009)
5. Munilla, J., Peinado, A.: Off-line Password-guessing Attack to Peyravian-Jeffries's Remote User Authentication Protocol. Computer Communications 30, 52–54 (2006)
6. Shim, K.A.: Security Flaws of Remote User Access over Insecure Networks. Computer Communications 30, 117–121 (2006)
7. Hölbl, M., Welzer, T., Brumen, B.: Improvement of the Peyravian-Jeffries's User Authentication Protocol and Password Change Protocol. Computer Communications 31, 1945–1951 (2008)
8. Munilla, J., Peinado, A.: Security Flaw of Hölblet et al.'s Protocol. Computer Communications 32, 736–739 (2009)
9. Das, M.L., Saxena, A., Gulati, V.P.: A dynamic ID-based Remote User Authentication Scheme. IEEE Transactions on Consumer Electronics 50, 629–631 (2004)
10. Awashti, A.K.: Comment on a Dynamic ID-based Remote User Authentication Scheme. Transactions on Cryptology 1, 15–16 (2004)
11. Chien, H.Y., Chen, C.H.: A Remote Authentication Scheme Preserving User Anonymity. In: International Conference on AINA 2005, vol. 2, pp. 245–248 (2005)
12. Ku, W.C., Chang, S.T.: Impersonation Attack on a Dynamic ID-based Remote User Authentication Scheme using Smart Cards. IEICE Transactions on Communications, E88-B, 2165–2167 (2005)
13. Liao, I.E., Lee, C.C., Hwang, M.S.: Security Enhancement for a Dynamic ID-based Remote User Authentication Scheme. In: International Conference on Next Generation Web Services Practices (2005)
14. Misbahuddin, M., Bindu, C.S.: Cryptanalysis of Liao–Lee–Hwang's Dynamic ID Scheme. International Journal of Network Security 6, 211–213 (2008)
15. Wang, Y.Y., Kiu, J.Y., Xiao, F.X., Dan, J.: A More Efficient and Secure Dynamic ID-based Remote User Authentication Scheme. Computer Communications 32, 583–585 (2009)
16. Khan, M.K., Kim, S.K., Alghathbar, K.: Cryptanalysis and Security Enhancement of a 'more efficient & secure dynamic ID-based remote user authentication scheme'. Computer Communications 34, 305–309 (2011)
17. He, D.B., Chen, J.H., Hu, J.: Weaknesses of a Dynamic ID-based Remote User Authentication Scheme, `http://eprint.iacr.org/2010/240`