Weaknesses of a dynamic ID-based remote user authentication scheme

He Debiao*, Chen Jianhua, Hu Jin

School of Mathematics and Statistics, Wuhan University, Wuhan, Hubei 430072, China

Abstract: The security of a password authentication scheme using smart cards proposed by Khan et al. is analyzed. Four kinds of attacks are presented in different scenarios. The analyses show that the scheme is insecure for practical application.

Key words: Authentication; Security; Cryptanalysis; Smart card; Attacks.

1. Introduction

User authentication is the essential security mechanism for remote login systems in which a password-based authentication scheme is the most commonly used technique to provide authentication between the legal users and the remote server.

In 1981, Lamport [1] proposed a password-based authentication scheme using password tables to authenticate remote users over insecure network. In Lamport's scheme, password table is used to verify the legitimacy of users. In 2000, Hwang et al. pointed out that once the password table was stolen or modified in this scheme, the whole authentication system will be affected [2]. Therefore, they proposed a remote user authentication scheme using smartcard without maintaining a password table. Afterwards, many schemes have been proposed to enhance the security and practicability [3-11].

A common feature among most of the published schemes is that the user’s identity is static in all the transaction sessions, which may leak some information about that user and can create risk of ID-theft during the message transmission over an insecure channel. To overcome this risk, Das et al. proposed a dynamic ID-based remote user authentication scheme [12]. Compared with other authentication schemes, this scheme has many advantages. In the scheme, the server does not maintain any verifier table, and moreover, the scheme is based on the one-way secure hash function, so its realization is simple and reliable. However, Das et al.’s scheme is completely insecure [13]. It failed to protect the anonymity of a user [14] and is susceptible to the impersonation attack [15], and the guessing attack [16].

To overcome the security pitfalls of Das et al.’s scheme, Liao et al. proposed an improved scheme. Misbahuddin et al. [17] demonstrated that Liao et al.’s scheme cannot withstand impersonation attack, reflection attack and is completely insecure as a user can successfully log on to a remote system with a random password.

In 2009, Wang et al. [18] proposed a 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. [19] identify that Wang et al.’s scheme has the following flaws: no provision of user’s anonymity during authentication, inability to offer user free choice in choosing his password,

*Corresponding author.

E-mail: hedebiao@163.com, *Tel*:+0086015307184927, *Fax*: +008602787817667

vulnerability to insider attack, no provision for revocation of lost or stolen smart card, and does provide session key agreement. To remedy these security flaws, they proposed an enhanced authentication scheme. They claimed their scheme covers all the identified weaknesses of Wang et al.’s scheme and is more secure and efficient for practical application environment.

However, in this paper, we show Khan et al.’s scheme suffers from three weaknesses: 1) inability to protect the user’s anonymity; 2) the session-key problem; 3) inefficiency of the double secret keys; and 4) other drawbacks. That is, it fails to fully meet the security requirements that this type of scheme should achieve.

The rest of the paper is organized as follows: Section 2 briefly reviews Khan et al.'s scheme, Section 3 elaborates on the weakness of their scheme, Section 4 concludes this paper.

2. Review of Khan et al.’s scheme

The notations used throughout this paper are described as in the following.

- U_i : a user.
- $ID_i, PW_i : U_i$ ’s identifier, password respectively.
- S : a remote server.
- $x, y : S$ ’s secret keys.
- $T_i, T_S : U_i$ ’s current timestamp, and S ’s current timestamp, respectively.
- $h(\cdot)$: a hash function.
- $\oplus$: bitwise XOR operation.
- ||: concatenation operation

Khan et al.'s scheme involves five phases, the registration phase, the login phase, the authentication phase, the password change phase, and the lost smart card revocation phase. We just give the first four phases here, since the last phase has nothing about our analysis.

Registration phase. In this phase, the user U_i initially registers with the server S .

1) U_i chooses his ID_i and PW_i, generates a random number r_i, and computes $RPW_i = h(r_i \,||\, PW_i)$. At last, U_i sends $\{ID_i, RPW_i\}$ to the server S .

2) Upon receiving $\{ID_i, RPW_i\}$, S checks the validity of ID_i. If ID_i is not valid, S rejects the registration. Otherwise, S computes $IDU_i = ID_i \,||\, N_i$, $J_i = h(x \,||\, IDU_i)$ and $L_i = J_i \oplus RPW_i$, where N equals 0 if U_i is a new user, otherwise N_i equals 1. At last, S delivers the smart card containing L_i and y to U_i .

3) Upon receiving the smart card, U_i stores r_i in the smart card and completes the registration.

Login phase. In this phase, the user U_i sends a login request message to the server S whenever U_i wants to access some resources upon S .

1) U_i inserts his smart card into a smart card reader and then inputs his ID_i and PW_i .

2) U_i 's smart card generates a random number d_i and computes $RPW_i = h(r_i \| PW_i)$, $J_i = L_i \oplus RPW_i$, $c_1 = h(T_i \| J_i)$, $AID_i = ID_i \oplus h(y \| T_i \| d_i)$ where T_i is the current time stamp.

3) U_i 's smart card sends the message $M_1 = \{AID_i, T_i, d_i, c_1\}$ to the server S .

Verification phase. In this phase, the server S verifies the authenticity of the login message requested by the user U_i .

1) Upon receiving the message M_1 , S checks the freshness of T_i . The freshness of T_i is checked by performing $T' - T_i \le \Delta T$, where T' is the time when S receives the above message and ΔT is a valid time interval. If T_i is not fresh, S aborts the current session.

2) S computes $ID_i = AID_i \oplus h(y \| T_i \| d_i)$ and checks the validity of ID_i . If ID_i is not valid, S stops the session.

3) S computes $IDU_i = ID_i \| N_i$, $J_i = h(x \| IDU_i)$ and $c_1' = h(T_i \| J_i)$. S checks if c_1 equals c_1' . If c_1 does not equal c_1' , S stops the session. Otherwise U is authenticated and S computes $c_2 = h(c_1 \oplus J_i \oplus T_S)$ and the session key $S_K = h(c_2 \oplus J_i)$. At last, S sends the message $M_2 = \{c_2, T_S\}$ to U 's smart card.

4) Upon receiving the message, U_i 's smart card checks the freshness of T_S . The freshness of T_S is checked by performing $T'' - T_S \le \Delta T$, where T'' is the time when U_i 's smart card receives the above message and ΔT is a valid time interval.

5) U_i 's smart card computes $c_2' = h(c_1 \oplus J \oplus T_S)$ and checks if c_1 equals c_1' . If c_1 does not equal c_1' , U_i 's smart card stops the session. Otherwise, S is authenticated and U_i 's

smart card computes the session key $S_K = h(c_2 \oplus J_i)$.

Password change phase. In this phase, the user U_i changes his/her password any time he/she wants.

1) U_i inserts his/her smart card into a smart card reader and then inputs his/her ID_i, PW_i and the new password PW_i'.

2) U_i's smart card computes $RPW_i^* = h(r_i \| PW_i)$, $J_i^* = L_i \oplus RPW_i$ and checks if J_i^* equals J_i. If J_i^* does not equal J_i, U's smart card reject the phase.

3) U_i's smart card computes $L_i^* = J_i \oplus RPW_i^* \oplus h(r \| PW_i')$ and replaces the value L_i.

3. Weaknesses of Khan et al.'s scheme

3.1. Inability to anonymity

Khan et al. claimed that their scheme can protect the anonymity of the user. However, we show that the identity of the target user U_i may be guessed by another user who is an insider with his or her own password and smart card. Our attack is based on the observation that AID_i is the XOR-ed value of ID_i and a digest of other secret components. The problem is that the secret components are commonly shared among all the users. To be more precise, the attack can be implemented as follows:

1) The attacker (say, user U_j) eavesdrops the victim's (say, user U_i's) authentication session from which AID_i, T_i and d_i can be extracted.

2) The attacker computes his own AID_j with ID_j, PW_j, d_i and T_i, where d_i and T_i are the captured session.

3) $AID_j = ID_j \oplus h(y \| T_i \| d_i)$ can be prepared because ID_j and PW_j are the attacker's ID and password, respectively.

4) Now the attacker can get ID_i by computing $AID_i \oplus AID_j \oplus ID_j$.

In the following, why this attack works is demonstrated. U_j can control his smart card completely, and certainly he can also control the value of T_j and the random number d_j, then he lets their value be T_i and d_i separately, and computes

$$AID_j = ID_j \oplus h(y \| T_i \| d_i)$$

and

$$\begin{aligned} & AID_i \oplus AID_j \oplus ID_j \\ & = (ID_i \oplus h(y \| T_i \| d_i)) \oplus (ID_j \oplus h(y \| T_i \| d_i)) \oplus ID_j \ . \\ & = ID_i \end{aligned}$$

3.2. The session-key problem

As noted by Blake-Wilson et al. [22], a number of security properties of key agreement have been proposed and the properties have been used to analyze the security of key agreement. The properties include known-key secrecy, unknown key-share resilience, no key control, key-compromise impersonation resilience and perfect forward secrecy. Forward secrecy requires that, if long-term private keys of one or more entities are compromised, the secrecy of previous session keys established by honest entities can be unaffected.

When analyzing the forward secrecy, Khan et al. claimed even if the server's secret keys x and y happens to be compromised, an adversary cannot impersonate legitimate users by using the revealed keys, and concluded their scheme can preserve the forward secrecy of secret keys x and y. They made a mistake in understanding the mean of forward secrecy. In fact, their scheme can't provide the forward secrecy. Once the adversary get the value x, y and some ciphertext translated c between the user and the server, he can compute the session key through the following method.

1) The attacker gets the value ID_i using the method described above and let N_i be zero.

2) The attacker computes $J_i = h(x \| IDU_i)$, where IDU_i equals $ID_i \| N_i$.

3) The attacker computes the session key $S_K = h(c_2 \oplus J_i)$.

4) The attacker gets the plaintext m by decrypting c using the session key S_K. If m is meaningful, the attacker get the correct session key. Otherwise, he lets N_i increment by one and repeats steps 2), 3) and 4) until get the correct session key.

From the above description, we can conclude the attacker can get the correct session by testing the possible value N_i. Then the search space is |**N**|, where **N** is the set of possible N_i and $|\cdot|$represents the cardinality of a set.

In fact, even though the attacker can't get the value ID_i, he can guess the value ID_i to carry out the attack, and the search space is | **ID** |×|**N**|, where **ID** is the set of possible ID's,. Note that generally|**N**| and |**ID**| are not very big, and unlike a space for cryptographic key.

3.3. Inefficiency of the double secret keys

We can see that the scheme of Khan et al. requires S to keep two keys secret, i.e., the secret key x and y. In common sense, it is possible to achieve the user authentication and key agreement service by using only one secret key. Therefore, two secret keys mean more overheads without the security enhancement for the whole authentication system.

3.4. Other drawbacks

In the step 2) of password change phase in Khan et al.'s scheme, the smart card checks if J_i^* equals J_i. But, in the registration phase, J_i is not stored in the smart card. We think Khan et al.'s may make a mistake when design the registration phase and the password change phase. We demonstrate the drawbacks as follows.

- **J_i is not stored in the smart card**

If J_i is not stored in the smart card, then the step 2) of password change phase in Khan et al.'s scheme must be canceled, then Khan et al.'s scheme is vulnerable to the Denial-of-service (DoS) attack.

In password authentication, DoS attack can cause permanent error on authentication by introducing unexpected data during the procedures of authentication. The most vulnerable procedure is the password changing phase since it usually refreshes the data in storage. If an attacker can modify the password, or tamper the message containing password with valid data format, the updated password or its related verification data will then be different from what the user expects. The user can never pass the subsequent authentication thereby. In Khan et al.'s scheme, the password changing phase is performed on the user terminal with smart cards, i.e., the user can change his password without communicating with the server [19]. This enhances the security of password changing as no sensitive message needs to be transmitted over the insecure network. Meanwhile, it relieves the overhead of the/a server. However, due to the drawbacks of design, it is still possible to load a DoS attack on password changing in their scheme.

Suppose an attacker temporarily gets access to the user U_i's smart card, he then inserts the card in a terminal device and performs the following operations. He randomly selects two different passwords PW' and PW'' as the old and the new password, respectively. Then he sends a changing password request to the smart card. Since J_i is not stored in the smart card, then the smart card will not check if J_i^* equals J_i, it just computes $RPW_i^* = h(r_i \| PW')$, $L_i^* = J_i \oplus RPW_i^* \oplus h(r \| PW'')$ and replaces the value L_i.

From then on, U_i can never pass the server's password authentication. This is because in the login phase, U_i cannot verify the legal server in the second step. Moreover, he cannot be verified by the server in the last step of authentication phase.

- **J_i is stored in the smart card**

If J_i is not stored in the smart card, then the step 2) of password change phase in Khan et al.'s scheme must be canceled, then Khan et al.'s scheme is vulnerable to the password guessing attack.

In Khan et al.'s scheme r_i, J_i, and L_i are stored in the smart card after registration. It's easy to say that there is the following relation between r_i, J_i, and L_i about PW_i.

$$J_i = L_i \oplus h(r_i \| PW_i)).$$

Then the adversary can carry out the off-line password guessing attack using the relation. The detailed description of the attack is as follows. The adversary can obtain the secret information r_i, J_i, and L_i stored in the stolen smart card by monitoring the power consumption [20] or by analyzing the leaked information [21]. Then he can carry out the password guess attack using r_i, J_i, and L_i.

1). The adversary selects a password $PW' s$ from a uniformly distributed dictionary.

2). The adversary computes $J_i' = L_i \oplus h(r_i \| PW_i'))$.

3). A then verifies the correctness of $PW' s$ by checking if J_i is equal to J_i'.

4). A repeats steps 1, 2, and 3 of this phase until the correct password is found.

4. Conclusion

Smart card-based user authentication technology has been widely deployed in various kinds of applications, such as remote host login, withdrawals from automated cash dispensers, and physical entry to restricted areas.

In [19], Khan et al. proposed a password authentication scheme using smart cards and demonstrated its immunity against various attacks. However, by reviewing of their scheme and analyzing its security, four kinds of weakness, i.e., 1) inability to protect the user's anonymity; 2) the session-key problem; 3) inefficiency of the double secret keys; and 4) other drawbacks are presented in different scenarios. The analyses show that the scheme is insecure for practical application.

Reference

[1]. L. Lamport, Password authentication with insecure communication, Communications of the ACM 24 (11) (1981) 770 – 772.

[2]. M.S. Hwang, L.H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (1) (2000) 28 – 30.

[3]. W.H. Yang, S.P. Shieh, password authentication schemes with smart cards, Computers & Security 18 (8) (1999) 727 – 733.

[4]. H.M. Sun, An efficient remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (4) (2000) 958 – 961.

[5]. C.C. Lee, M.S. Hwang, W.P. Yang, A flexible remote user authentication scheme using smart cards, ACM Operating Systems Review 36 (3) (2002) 46 – 52.

[6]. J.J. Shen, C.W. Lin, M.S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 49 (2) (2003) 414 – 416.

[7]. M. Kumar, New remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 50 (2) (2004) 597 – 600.

[8]. W.C. Ku, S.T. Chang, M.H. Chiang, Further cryptanalysis of fingerprint-based remote user authentication scheme using smartcards, IEE Electronics Letters 41 (5) (2005).

[9]. M.K. Khan, J. Zhang, Improving the security of ‘a flexible biometrics remote user authentication scheme’, Computer Standards & Interfaces 29 (2007) 82 – 85.

[10]. S.K. Kim, M.G. Chung, More secure remote user authentication scheme, Computer Communications 32 (2009) 1018 – 1021. 518

[11]. J.H. Yang, C.C. Chang, An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, Computers & Security 28 (2009) 138 – 143.

[12]. M.L. Das, A. Saxena, V.P. Gulati, A dynamic ID-based remote user authentication scheme, IEEE Transactions on Consumer Electronics 50 (2) (2004) 629 – 631. 508

[13]. A.K. Awashti, Comment on a dynamic ID-based remote user authentication scheme, Transactions on Cryptology l (2) (2004) 15 – 16.

[14]. H.Y. Chien, C.H. Chen, A remote authentication scheme preserving user anonymity, in: International Conference on AINA’05, vol. 2, 2005, p. 2005.

[15]. W.C. Ku, S.T. Chang, Impersonation attack on a dynamic ID-based remote user uthentication scheme using smart cards, IEICE Transactions on Communication E88-B (5) (2005) 2165 – 2167.

[16]. I. Liao, C.C. Lee, M.S. Hwang, Security enhancement for a dynamic ID-based remote user authentication scheme, in: Proceedings of the National Conference on Next Generation Web Services Practices, 2005, p. 4.

[17]. M. Misbahuddin, C.S. Bindu, Cryptanalysis of Liao – Lee – Hwang’s dynamic ID scheme, International Journal of Network Security 6 (2008) 211 – 213.

[18]. Y.Y. Wang, J.Y. Kiu, F.X. Xiao, J. Dan, A more efficient and secure dynamic ID-based remote user authentication scheme, Computer Communications 32 (2009) 583 – 585.

[19]. M.K. Khan et al., Cryptanalysis and security enhancement of a ‘more efficient & secure dynamic ID-based remote user authentication scheme’, Computer. Communications. (2010), doi:10.1016/j.comcom.2010.02.011

[20]. P. Kocher, J. Jaffe, B. Jun, Differential power analysis, Proc. Advances in Cryptology (CRYPTO'99), 1999, pp. 388 – 397.

[21]. T.S. Messerges, E.A. Dabbish, R.H. Sloan, Examining smart-card security under the threat of power analysis attacks, IEEE Transactions on Computers 51 (5) (2002) 541 – 552.

[22]. Blake-Wilson S, Johnson D, Menezes A. Key agreement protocols and their security analysis. In Proc. the Sixth IMA International Conference on Cryptography and Coding, Cirencester, UK, LNCS 1355, Springer-Verlag, 1997, pp.30-45.