Security Analysis of Improved User Authentication Schemes Using Smart Cards

Xiao Hong YIN1, Chun Ming TANG2, Zuo Wen TAN1,2,3*

1 Nanchang Institute of Science & Technology, Nanchang 330108, China
2 Key Laboratory of Information Security, School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China
3 School of Information Technology, Jiangxi University of Finance and Economics, Nanchang 330032, China
hub_t@tom.com, ctang@gzhu.edu.cn, tanzyw@163.com
* Corresponding author: Zuowen Tan, email: tanzyw@163.com

Abstract. Smart card based remote user authentication is a broadly adopted method of authentication within insecure communication channels. Recently, Wen and Li proposed a dynamic ID-based remote user authentication protocol with key agreement. Unfortunately, Kim, Nam and Won pointed out that Wen and Li’s authentication protocol suffers from leakage of some key information to an adversary and a man-in-the-middle attack. Kim et al. proposed an improved ID-based remote user authentication scheme. In this work, we revisit Kim et al.’s protocol. Our results indicate that their scheme is vulnerable to smart card loss attack, stolen verifier attack and privileged insider attack. Furthermore, the authentication protocol cannot provide perfect forward secrecy and user anonymity. These weaknesses also exist in Wen and Li’s authentication scheme.

1. Introduction
Over a public channel, a remote server always needs to authenticate users. In 1981, Lamport first proposed a password based authentication scheme [1]. When the smart card based password authentication schemes execute, the smart card takes one password and the user identity as input, computes the login message and sends the login request message to the server. Then the server checks its validity. Smart card based password authentication is one of the most convenient two-factor authentication mechanisms. Yang and Shieh [2] introduced the first smartcard-based password authentication scheme without a sensitive verification table stored on the server [3]. It has one advantage over common only password based schemes, since the latter have to maintain a sensitive password (or salted password) table on the server. Since the seminal work of Yang and Shieh, there have been a great number of two-factor schemes [4-6]. Due to their low computational cost and convenient portability, these authentication schemes have been widely adopted for various kinds of applications, such as e-banking, e-government and e-health.

In most of the previous two-factor schemes, user’s identity is transmitted in plain-text over public channel. Therefore, they cannot provide user privacy. Since the user’s identity is static in all the
transaction sessions, an attacker may link different login sessions together to trace user activities which leads to leakage of the partial information about the user. To address such issues, Das et al. [7] proposed a dynamic ID-based remote user authentication scheme. Dynamic identity based authentication technique can provide the user anonymity. Unfortunately, Chien and Chen [8] showed that Das et al.’s scheme fails to protect the anonymity of a user. Later on, a few attacks on Das et al.’s scheme, such as the impersonation attack, insider attack [9] and guessing attack [10] are found. Moreover, Das et al.’s scheme does not provide mutual authentication [10,11]. Liao and Wang [12] proposed a dynamic ID-based remote user authentication scheme. However, Hsiang and Shih [13] demonstrated that Liao and Wang’s improved scheme is vulnerable to insider attack and masquerade attack. Wang et al. also presented an improvement on Das et al.’s scheme [11]. But Khan et al. [14] showed that Wang et al.’s scheme [11] is vulnerable to insider attack. It can neither protect the anonymity of a user nor support the session key agreement [14]. Khan et al. also proposed a dynamic ID based remote user authentication scheme and claimed that their scheme was secure than Wang et al.’s scheme [14]. However, Madhusudhan and Mittal [15] demonstrated that Khan et al.’s scheme is vulnerable to insider attack.

Madhusudhan and Mittal [15] point out that a remote user smart card based anonymous authentication scheme should satisfy the following nine security requirements and ten desirable attributes. Recently, Wen and Li [16] showed that Wang et al.’s scheme [11] is not secure against impersonation attacks launched by any adversary at anytime and could leak some key information to legal users, who can launch an off-line guessing attack. Wen and Li proposed a new dynamic ID-based authentication scheme with key agreement using symmetric cryptology [16]. It is claimed that their new scheme overcomes the weaknesses of Wang et al.’s scheme [11]. Unfortunately, Kim et al. showed that Wen and Li’s improved scheme leaks partial information and the session keys [17]. Kim et al. also proposed an improvement [18]. In this work, however, we will demonstrate that Kim et al.’s scheme is vulnerable to smart card loss attack, stolen-verifier attack, and privileged insider attack. Moreover, it cannot provide perfect forward secrecy and user anonymity. Wen and Li’s scheme also suffers from the same these security pitfalls.

The rest of this paper is organized as follows. Section 2 reviews Kim et al.’s scheme. The cryptanalysis of Kim et al.’s scheme is presented in Section 3. Finally, conclusion is given in Section 4.

2. Review of Kim et al’s scheme
In this section, we will briefly describe the two-factor scheme proposed by Kim et al. [18]. Kim et al.’s scheme consists of five phases, namely, registration phase, login phase, authentication and key exchange phase, mutual authentication and key confirmation phase and off-line password change phase. The notations and abbreviations used in the Kim et al.’s scheme are listed in Table 1.

| Notations | Descriptions | Notations | Descriptions |
|-----------|--------------|-----------|--------------|
| $S$       | The server   | $h(.)$    | A one-way hash function |
| $U_i$     | The $i$th user | $||$       | String concatenation |
| $pwi$     | The $U_i$’s password | $\rightarrow$ | Message transmission |
| $ID_i$    | The $U_i$’s identity | $T$       | A timestamp |
| $x$       | The secret key of the server | $SK$      | The session key |
| $\oplus$ | The exclusive- or operation | $KC$      | The key confirmation |

2.1. Registration phase
When a user $U_i$ wants to register with the server $S$, $U_i$ performs the following operations:

Step 1. $U_i$→$S$: $\{ID_i, pwi\}$. The user $U_i$ selects an identity $ID_i$ and password $pwi$, then $U_i$ submits $\{ID_i, pwi\}$ to the server $S$ via a secure channel.

Step 2. $S$→$U_i$: Smart card. Upon receiving the message $\{ID_i, pwi\}$, the server $S$ calculates $ni=h(ID_i||pwi)$, $mi=ni \oplus x$, $Ni=h(ID_i) \oplus h(pwi) \oplus h(x) \oplus h(mi)$. 


The parameter $n_i$ is kept secret by the server $S$. $S$ stores $\{h(\cdot), N_i, n_i\}$ in a smart card and sends the smart card to $U_i$ via a secure channel.

### 2.2. Login phase

When the user $U_i$ wants to access the server $S$, $U_i$ inserts his smart card into a card reader and inputs his identity $I_D_i$, password $p_w_i$. The following operations will be performed.

1. The smart card computes a dynamic identity $C_I_D_i, A_i=h(I_D_i) \oplus h(p_w_i), B_i=N_i \oplus h(I_D_i) \oplus h(p_w_i), C_I_D_i=h(A_i) \oplus h(n_i) \oplus B_i \oplus h(N_i) \oplus T$.

2. $U_i \rightarrow S$: $\{C_I_D_i, T, N_i, n_i\}$. The user $U_i$ sends the login request $\{C_I_D_i, T, N_i, n_i\}$ to the server $S$ over a public channel, where $T$ is the time stamp.

### 2.3. Authentication and key exchange phase

1. When the server $S$ receives the message $\{C_I_D_i, T, N_i, n_i\}$ at time $T'$, $S$ checks the validity of the timestamp $T$. If $|T' - T| \leq \Delta T$, $S$ searches the registered list for $n_i$.

2. If $n_i$ is in the registered list, the server $S$ calculates $m_i = n_i \oplus x, B_i = h(x) \oplus h(m_i), A_i = B_i \oplus N_i$. Then $S$ verifies whether the equation holds: $C_I_D_i \oplus h(A_i) = h(h(n_i) \oplus B_i \oplus h(N_i) \oplus T)$. If the equation holds, $S$ continues the following steps. Otherwise, $S$ terminates the session.

3. $S \rightarrow U_i$: $\{K_{C'}^C, T'\}$. $S$ computes the session key $SK=h(A_i || T || B_i || T')$ and the key confirmation message $K_{C'}^C = h(B_i || SK || T')$. Then $S$ sends the response message $\{K_{C'}^C, T'\}$ to $U_i$.

### 2.4. Mutual authentication and key confirmation phase

1. On receiving the response message $\{K_{C'}^C, T'\}$ at time $T''$, the user first checks whether the time delay $T'' - T' \leq \Delta T$ holds. If it is valid, $U_i$ computes the session key $SK=h(A_i || T || B_i || T')$ and the key confirmation message $K_{C'}^C = h(B_i || SK || T'')$. Next, the user $U_i$ checks whether the received $K_{C'}^C$ equals $K_{C'}$. If they do not equal, $U_i$ rejects. Otherwise, $U_i$ proceeds.

2. $U_i \rightarrow S$: $\{K_{C'}^C, T''\}$. The user computes the key confirmation message $K_{C''}^C = h(A_i || SK || T'')$ and sends it to the server $S$.

3. The server $S$ computes $K_{C''}^C = h(A_i || SK || T'')$. Then $S$ checks whether the received $K_{C''}^C$ equals $K_{C''}$. If it does not hold, $U_i$ is rejected. Otherwise, $S$ accepts $U_i$'s request.

### 3. Cryptanalysis of Kim et al.’s scheme

Compared with other related schemes, the Kim et al.‘s scheme has attractive properties, such as high computation efficiency and low communication cost. Assume that the identity can be represented with 32 bits, the output size of secure one-way hash functions is 160 bits and the size of a timestamp is 32 bits. In the login phase of the scheme, the user $U_i$ needs to send the message $\{C_I_D_i, T, N_i, n_i\}$ to the server. It contains $160 \times 3 + 32 = 512$ bits. In the authentication and key exchange phase, the server sends $\{K_{C'}^C, T''\}$ back to $U_i$. It is $160 + 32 = 192$ bits long. Finally, in the mutual authentication and key confirmation phase, $U_i$ sends the key confirmation message to the server. It is 192 bits long. Therefore, the communication cost is low. Moreover, the login phase in the Kim et al.‘s scheme needs only six hashing operations and six Exclusive-OR operations in the smart card side. In the authentication and key exchange phase, the server requires eight hashing operations and six Exclusive-OR operations. While in the mutual authentication and key confirmation phase, the scheme requires three hashing operations in the smart card side. The scheme preserves the low-computation property for the smart card.

It is claimed that Kim et al.‘s scheme [18] both maintains the merits of the original scheme and eliminates the security flaws of Wen and Li’s scheme [16]. However, it is still far from an “ideal” anonymous two-factor protocol to be applicable for practical applications. In this section, we will demonstrate that some security flaws still exist in the Kim et al.‘s scheme. It actually fails to resist
smart card loss attack (i.e., SR6), stolen verifier attack (i.e., SR7) and privileged insider attack (i.e., SR9). Moreover, it cannot provide perfect forward secrecy (i.e., DA7) and strong anonymity (i.e., DA8). In addition, the timestamp will incur inconvenience for the smart card based application environments. The same cryptanalyses also apply to Wen and Li’s scheme.

3.1. Smart card loss attack
Kim et al.’s scheme supports user password free update. During the password changing phase, the user changes his password and sets any new password only with smart cards and does not need to communicate with the server. Therefore, Kim et al.’s scheme achieves user friendliness. However, since there is no verification of the authenticity of the old password before the update of new password, it is a kind of inherent security threat.

In the real two-factor applications, users do tend to leave their smart card unattended. For example, users have forgotten their smart cards in the card reader for a period of a few minutes or several days. If an attacker manages to gain temporary access to the smart card of legitimate user Ui, she can easily change the password of user Ui’ as follows.

Step 1. The adversary first inserts the smart card in a terminal device, and selects two different passwords \( p_{w}' \) and \( p_{w}'' \) as the old and the new password, respectively. Then the adversary keys IDi with \( p_{w} \) and \( p_{w}^* \) and issues a request of changing password to the smart card.

Step 2. The smart card will compute \( N_{i}'' = N_{i} \oplus h(p_{w}') \oplus h(p_{w}'') \), then it replaces \( N_{i} \) with \( N_{i}'' \). When the user Ui uses the smart card to access the server in the subsequent authentication, the login request can never pass the verification of the server S. Thus, the legitimate user Ui cannot login successfully even after getting her smart card back. We describe the attack as follows.

Step 1. Since Ui is unaware of the change of message stored in the card, Ui still keys IDi with \( p_{w} \).

Step 2. The smart card computes \( A_{i}=h(IDi) \oplus h(p_{w}) \), \( B_{i}^{*}=h(IDi) \oplus h(p_{w}^*) \), \( C_{i}^{*}=h(A_{i}) \oplus h(mi) \oplus h(N_{i}^*) \oplus T \). Upon receiving the login request \( \{C_{i}^{*}, T, N_{i}^*, n_{i}\} \), S computes \( m_{i}=n_{i} \oplus x \), \( B_{i}=h(x) \oplus h(m_{i}) \). Since \( B_{i}^{*}=h(IDi) \oplus h(p_{w}) \), \( C_{i}^{*}=h(IDi) \oplus h(p_{w}^*) \), the verification equation \( C_{i}^{*}=h(A_{i}) \oplus h(mi) \oplus B_{i}^{*} \oplus h(N_{i}^*) \oplus T \) will not hold. S will refuse the login request.

The above description confirms that Dos attacks can be launched easily once the smart card is lost.

3.2. Stolen verifier attack
If verification tables are stored in the server, the authentication scheme will suffer from the leakage of the verification information, which may lead to serious security flaws. In the Kim et al.’s scheme, \( n_{i} \) is kept secret by the server S. The server maintains the verifier table of all the unique message \( n_{i} \), which makes the protocol susceptible to the stolen-verifier-attacks.

3.3. Privileged insider attack
If the password of a user can be derived by the server in the registration phase, such a scheme suffers from the inside attack [9,10]. During the registration phase of Kim et al.’s scheme, the user sends the password \( p_{w} \) in form of plaintext to the server. S directly obtains the user’s password \( p_{w} \). In the real application environment, a user may use the same password to login different servers. A malicious privileged insider would use the password of the user to login to other servers. Thus, Kim et al.’s scheme cannot withstand the insider attacks.
3.4. Lack of perfect forward secrecy

The perfect forward secrecy [20,21,22] means that even though the master secret key $x$ of the server or password and identity of the user is disclosed, any session keys generated from the previous execution of the protocol will not be compromised. Kim et al.’s scheme cannot provide perfect forward secrecy.

Assume the adversary has intercepted a certain login message $\{\text{CID}_i, T, N_i, n_i\}$. With the compromised secret key $x$, she computes $m_i = n_i \oplus x$, $B_i = h(x) \oplus h(m_i)$, $A_i = N_i \oplus B_i$. Thus, by using two timestamps $\{T, T'\}$ from the login request and the login response, the adversary calculates session key $SK = h(A_i || T || B_i || T')$.

Assume that an adversary has obtained $U_i$'s long-term secret $A_i = h(ID_i) \oplus h(pwi)$. Note that neither the password nor identity is compromised. We discuss what will happen next in two cases.

(1) The session key will be compromised.

Further assume that the adversary has recorded the message transmitted between the server and the user. The adversary needs to record the whole login message $\{\text{CID}_i, T, N_i, n_i\}$ and the whole response message $\{KC', T'\}$ only for the first time. For other sessions, the adversary only needs to record two timestamps $\{T, T'\}$. With knowledge of the long-term secret $A_i$ and the intercepted message of previous sessions, the adversary calculates the session keys as follows. First, she computes $B_i = A_i \oplus N_i$. Then she retrieves the session key $SK = h(A_i || T || B_i || T')$ by using the intercepted two timestamps $\{T, T'\}$.

(2) It will lead to impersonation attacks.

With the secret $A_i$, an adversary can impersonate $U_i$ to access $S$ as follows.

Step 1. The adversary computes $B_i = A_i \oplus N_i$. $\text{CID}_i = h(A_i) \oplus h(n_i) \oplus B_i \oplus h(N_i) \oplus T$.

Step 2. The adversary sends the login request message $\{\text{CID}_i, T, N_i, n_i\}$ to the server $S$. Since $B_i = A_i \oplus N_i = h(x) \oplus h(n_i)$, the server $S$ believes that the message is sent by the legal user. Similarly, with the long-term secret $A_i$, an adversary also can impersonate $S$ to fool $U_i$.

Step 1. The adversary computes $B_i = A_i \oplus N_i$. Upon receiving the user $U_i$'s login request message $\{\text{CID}_i, T, N_i, n_i\}$, the adversary computes a session key $SK = h(A_i || T || B_i || T')$ and $KC' = h(B_i || SK || T')$.

Step 2. The adversary sends the response message $\{KC', T'\}$ to the user $U_i$. Obviously, the user $U_i$ will believe that the response message is sent by the intended server $S$.

3.5. Lack of user anonymity

In open network environments, an adversary always intercepts the public communication channel. Suppose that the user $U_i$ sends the login request message $\{\text{CID}_i, T, N_i, n_i\}$ to the server $S$. The message $\{N_i, n_i\}$ is for the user $U_i$’s exclusive use and is unchanged for any access to the server $S$ if the password has not been updated. Moreover, even after the password is changed, $n_i$ is the same for a user and a server. That is, $n_i$ binds a registered user with a server. Thus any adversary could easily trace the user by checking whether $\{N_i, n_i\}$ or $\{n_i\}$ of different execution of protocols is the same. Thus, the user anonymity is not well protected even though the user’s identity is not revealed.

4. Conclusion

In this work, we revisit the schemes [16,18]. Detailed security analysis demonstrates that two schemes [16,18] are susceptible to smart card loss attack, stolen verifier attack and privileged insider attack. Moreover, they cannot provide perfect forward secrecy and strong anonymity. To design an “ideal” anonymous two-factor authentication protocol which can fulfill nine security requirement and ten desirable attributes mentioned in [15] is challenging.
Acknowledgment
This work was supported in part by the National Natural Science Foundation of China under Grant (61462033), Natural Science Foundation of Jiangxi Province (20161BAB202059), the Open Project Program of Key Laboratory of Guangdong Provincial Key Laboratory of Information Security under Grant(No. GDXXAQ2016-10), Foundation of Jiangxi Educational Committee under Grant (GJJ151239), and Nanchang Key Laboratory and Characteristic Specialty.

References
[1] L. Lamport. Password Authentication with Insecure Communication[J]. Communication of ACM,1981, 24:28-30.
[2] W.-H. Yang, S.-P. Shieh. Password Authentication Schemes with Smart Cards[J]. Comput. Security,1999, 18(8): 727–733,1999.
[3] R. Amin, S. H. Islam, G. Biswas, M. K. Khan, L. Leng, and N. Kumar. Design of an Anonymity-Preserving Three-Factor Authenticated Key Exchange Protocol for Wireless Sensor Networks[J]. Computer Networks, 2016, 101:42-62.
[4] Ding Wang, Debiao He, Ping Wang, Chao-Hsien Chu. Anonymous Two-Factor Authentication in Distributed Systems: Certain Goals Are Beyond Attainment[J]. IEEE Transactions on Dependable and Secure Computing, 2015, 12(4): 428-442.
[5] D. Mishra, A. K. Das, and S. Mukhopadhyay. A Secure and Efficient ECC-based User Anonymity-Preserving Session Initiation Authentication Protocol Using Smart Card[J]. Peer-to-peer Networking and Applications, 2016, 9(1):171-192.
[6] Li X, Niu JW, Kumari S, Liao JG, Liang W. An Enhancement of a Smart Card Authentication Scheme for Multi-Server Architecture. Wirel. Pers. Commun.,2015, 80(1): 175–192.
[7] M.L. Das, A. Saxena, and V.P. Gulati. A Dynamic ID-based Remote User Authentication Scheme[J]. IEEE Trans. Consumer Electronics, 2004, 50(2): 629–631.
[8] H.Y. Chien and C.H. Chen. A Remote Authentication Scheme Preserving User Anonymity[C]. Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA'05), 2005, 245-248.
[9] W.C. Ku and S.T. Chang. Impersonation Attack on a Dynamic ID-based Remote User Authentication Scheme Using Smart Cards[J]. IEICE Transactions on Communication E88-B,2005, 5: 2165-2167.
[10] I. Liao, C.C. Lee, and M.S. Hwang. Security Enhancement for a Dynamic ID-based Remote User Authentication Scheme[C]. Proceedings of the National Conference on Next Generation Web Services Practices, 2005, 437-440.
[11] Y.Y. Wang, J.Y. Kiu, F.X. Xiao, and J. Dan. A More Efficient and Secure Dynamic ID-based Remote User Authentication Scheme[J]. Computer Communications, 2009, 32:583–585.
[12] Y.P. Liao and S.S. Wang. A Secure Dynamic ID-based Remote User Authentication Scheme for Multi-Server Environment[J]. Computer Standards & Interfaces,2009, 31:24–29.
[13] H.C. Hsiang and W.K. Shih. Improvement of the Secure Dynamic ID-based Remote User Authentication Scheme or Multi-Server Environment[J]. Computer Standards & Interfaces,2009, 31:1118–1123.
[14] M.K. Khan, S.K. Kim, and K. Alghathbar. Cryptanalysis and Security Enhancement of a ‘More Efficient & Secure Dynamic ID-based Remote User Authentication Scheme’[J]. Computer Communications,2011, 34:305–309.
[15] R. Madhusudhan, R.C. Mittal. Dynamic ID-based Remote User Password Authentication Schemes Using Smart Cards: A review[J]. Journal of Network and Computer Applications, 2012, 35:1235–1248.
[16] F. Wen and X. Li. An Improved Dynamic ID Based Remote User Authentication Scheme with Key Agreement Scheme[J]. Computers & Electrical Engineering, 2012, 38(2):381–387.
[17] M. Kim, N. Park, and D. Won. Security Weakness of a Dynamic ID-based User Authentication...
Scheme with Key Agreement[C]. CSA-12, LNEE, 2012, 203:687–692.

[18] M. Kim, J. Nam, and Dongho Won. An Improved Secure Dynamic ID-based Remote User Authentication Scheme with Key Agreement Using Symmetric Cryptology[J]. International Journal of Security and Its Applications, 2013, 7(3):143-152.

[19] A. Chaturvedi, A. K. Das, D. Mishra, and S. Mukhopadhyay. Design of a Secure Smart Card-based Multi-Server Authentication Scheme[J]. Journal of Information Security and Applications, 2016, 30:64-80.

[20] M. Wazid, A. K. Das, S. Kumari, X. Li, and F. Wu. Design of an Efficient and Provably Secure Anonymity Preserving Three-factor User Authentication and Key Agreement Scheme for TMIS[J]. Security and Communication Networks, 2016, 9 (13) :1983-2001.

[21] A.K. Awasthi, S. Lal. A Remote User Authentication Scheme Using Smart Cards with Forward Secrecy[J]. IEEE Trans. Consumer Electronics, 2003, 49(4): 1246–1248.

[22] Qi Xie, Duncan S. Wong, Guilin Wang, Xiao Tan, Kefei Chen, Liming Fang, Provably Secure Dynamic ID-Based Anonymous Two-Factor Authenticated Key Exchange Protocol with Extended Security Model [J]. IEEE Transactions on Information Forensics and Security, 2017, 12(6): 1382-1392.