International Journal of Security and Its Applications
Vol.9, No.1 (2015), pp.387-396
http://dx.doi.org/10.14257/ijsia.2015.9.1.37

Security on Dynamic ID-based Authentication Schemes

Jingxuan Zhai[1,2], Tianjie Cao[1,*], Xiuqing Chen[1] and Shi Huang[1]

[1]*School of Computer, China University of Mining and Technology, Xuzhou, China*
[2]*Information Center, China University of Mining and Technology National University Science Park, Xuzhou, China*
**{tjcao@cumt.edu.cn}*

Abstract

Dynamic ID-based authentication schemes based on password and smart card are widely used to provide two-factor authentication and user anonymity. However, these schemes have one or the other possible security weaknesses. In this paper, we analyze the schemes of Li et al. and Wang et al. published in recent years. After the analysis, we demonstrates that Li et al.'s schemes are vulnerable to off-line password guessing attack if the user's identity is compromised, Li et al.'s scheme cannot withstand the impersonation attack and linkability attack, Wang et al.'s schemes cannot resist off-line password guessing attack if the attacker steals a smart card, Wang et al.'s schemes fail to provide forward security. Our result shows that none of the existing dynamic ID based authentication schemes can achieve all the desirable security goals.

Keywords: *Cryptography, Authentication, Key agreement, Anonymity, Forward security, Cloud computing*

1. Introduction

Cloud computing has drawn much attention from research and industry in recent years. Remote user authentication is a critical component of accessing remote services in cloud computing applications. Two-factor authenticated key agreement scheme based on password and smart card is the most convenient and popular way to protect the communication between the user and the remote server. To provide user anonymity, dynamic ID-based authentication schemes are proposed. Over the years, numerous of such schemes have been presented. Unfortunately, many of them have been pointed out to be flawed.

In 1981, Lamport [1] first considered password authentication scheme in the public network. This scheme is insecure if the verification table stored in the server is modified by an intruder. In 1990, Chang and Wu designed a remote authentication scheme without verification tables. This scheme reduces the server's burden of maintaining and protecting the verification tables. In 1991, Chang and Wu [2] proposed the first password authentication scheme using smart cards. Since then, many smart card based password authentication scheme were proposed to enhance security. These schemes assume the smart cards are tamper resistance. In 1999-2002, Kocher *et al.* [3] and Messerges *et al.*[4] pointed out that the secret data stored in the smart card could be extracted by physical intrusion or monitoring the power consumption. Therefore, these schemes become insure when we consider the smart card loss problem [5], especially off-line password guessing attacks and user impersonation attack.

In 2006, Liao *et al.* [6] considered ten desirable properties to evaluate the smart card based password authentication scheme. Later, Madhusudhan *et al.* [7] and Wang *et al.* [8] expanded the set of desirable security properties.

* Corresponding Author

ISSN: 1738-9976 IJSIA

To lay particular stress on practice, we put forward the more comprehensive desirable security requirements based earlier studies.

- No verification table: The server should not store any sensitive information corresponding to a particular user. Therefore, the server need not maintain and protect the verification table. If the server stores the user's authentication information, the server will be the attack target. There are many concrete cases that the hacker breaks the server and steals the verification table.
- No timestamps: Using timestamps will cause a lot of problems such as synchronization and delay problem.
- Public identity: It is prefer for the user to select his email address as the identity. It is not reasonable for the user to keep his identity secret. If the scheme to authenticate a user requests the user provide his identity, password and the smart card, this scheme will not be two-factor scheme and turn to a three-factor scheme.
- Resilience of privileged administrator attack: The password should only known by the user. Anyone, including the privileged administrator should not obtain the information about password. This assumption is reasonable. In some previous scheme, the user registers the system by sending his ID and password directly. Since many people use the same password in different applications, once the privileged administrator obtains a user's password, then, he can enter the user's other application using the compromised password.
- Freely chosen password: The user can selects his password and updates his password complying with his will.
- Mutual authentication: The attacker cannot impersonate the user even if he steals the user's smart card or password, but not both. The attacker cannot impersonate the server.
- Resilience of off-line password guessing attack: The scheme should resist off-line password guessing attack even if the attacker steals the user's smart card and extract the sensitive information stored in card.
- Resilience of undetected on-line password guessing attack: The scheme should resist undetected on-line password guessing attack even if the attacker steals the user's smart card and extract the sensitive information stored in card. An incorrect password guessing will be recorded by the server.
- No key control: The user and the server can agree on a session key. This session key should not be preselect by one of the participants.
- Key secrecy: The session key agreed by the user and the server should not be learned by the others.
- User anonymity: The user's identity should not revealed by the attacker.
- Unlinkability: The different sessions for the same user should not be linked by the attacker.
- Known-key security: If the attacker compromises a pervious session key, he could not impersonate the user or the server, compute the session key or derive the user's identity in another session. If the attacker compromises a pervious session key, he could not link the pervious session to the other one.
- Perfect forward security: Even if all secrets kept by the user and the server are compromised now, the scheme should provide key secrecy, user anonymity and session unlinkability for pervious sessions.
- Auditability: The scheme should support auditability by the server. If the scheme lacks the auditability, the user may abuse his privilege and free from responsibility. Further more, the cardholder can clone his smart card and sell to other people
- Availability: The scheme should prevent from denial-of-service attack (DoS attack). If the attacker obtains the smart card temporarily, the attacker should not change the password without the user's authorization.

Comparing the set of security requirement given by Madhusudhan *et al*. [7] and Wang *et al*. [8], we point out that it is necessary for a dynamic ID scheme to provide public user identity, unlinkability, forward anonymity and forward unlinkability, *etc*.

In 2012-2013, Madhusudhan *et al*. [7] and Xie [9] claimed that none of the existing schemes can achieve all the desirable security properties. Recently, to remove the security weaknesses of Lee *et al.'s* scheme [10], Li *et al.'s* scheme [11], Tsai *et al.'s* scheme [12], Sood *et al.'s* scheme, Li *et al.* [13], Wang *et al.* [8, 14] proposed some novel dynamic ID based authentication schemes. However, in this paper we find these schemes cannot satisfy the desirable security requirements. Our result shows that it is still difficult to design dynamic ID based authentication schemes which meet all the desirable security goals using password and smart card.

2. Li *et al.'s* Dynamic ID based Remote User Authentication Scheme for Multi-server Environment

The Li *et al.'s* scheme contains four phases. We show the main phases in Figure 1. In Li *et al.'s* scheme, the registration center *RC* chooses the secret key *x* and *y*. *RC* computes $h(x||y)$ and $h(SID||h(y))$ where *SID* is the identity of the server *S*, and then sends them to *S* via a secure channel.

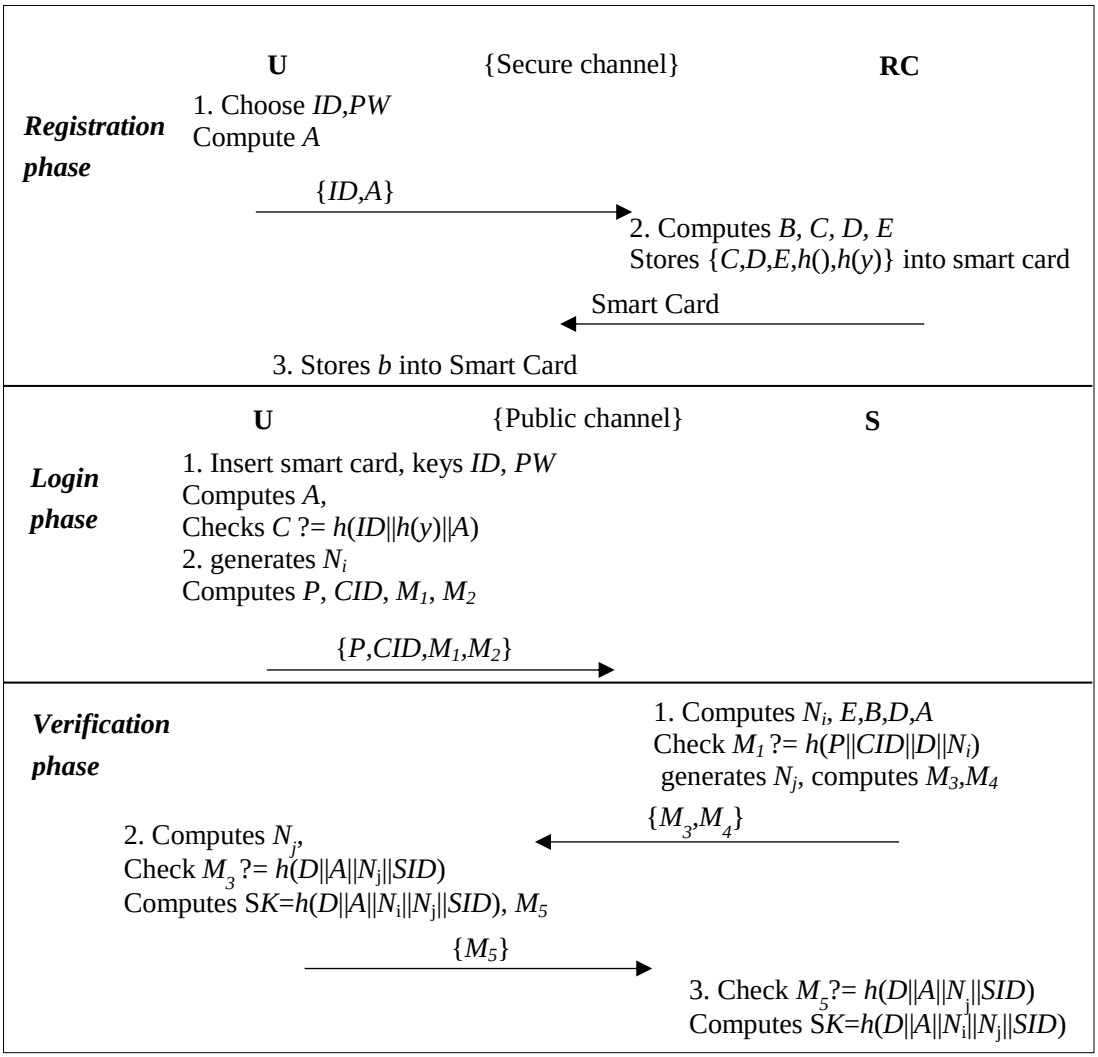


Figure 1. Li *et al.'s* Scheme

2.1. Registration Phase

Assume that the user U and the registration center RC have established a secure channel. U and RC perform the following steps in registration phase.

Step 1: U chooses identity ID, password PW and a random value b. U computes $A=h(b \oplus PW)$ and sends $\{ID,A\}$ to RC.

Step 2: RC computes $B=h(ID||x)$, $C=h(ID||h(y)||A)$, $D=h(B||(x||y))$ and $E=B \oplus h(x||y)$. RC stores $\{C,D,E,h(),h(y)\}$ on a smart card and sends it to U.

Step 3: U stores b into the smart card.

2.2. Login Phase

Whenever U intends to access the resources of S, U and S perform the following steps.

Step 1: U inserts the smart card and keys ID and PW. Then the smart card computes $A=h(b \oplus PW)$ and checks whether C is equal to $h(ID||h(y)||A)$. If they are not equal,the smart card terminates the session.

Step 2: The smart card generates a nonce N_i and computes $P=E \oplus h(h(SID||h(y))||N_i)$, $CID=A \oplus h(D||SID||N_i)$, $M_1=h(P||CID||D||N_i)$ and $M_2=h(SID||h(y)) \oplus N_i$. U sends login request message $\{P,CID,M_1,M_2\}$ to S.

2.3. Verification Phase

Step 1: Upon receiving the login message $\{P,CID,M_1,M_2\}$, S computes $N_i=h(SID||h(y)) \oplus M_2$, $E=P \oplus h(h(SID||h(y))||N_i)$, $B=E \oplus h(x||y)$, $D=h(B||h(x||y))$ and $A=CID \oplus h(D||SID||N_i)$. S checks whether $h(P||CID||D||N_i)$ is equal to M_1. If they are not equal, S terminates the session. Then S generates a random number N_j and computes $M_3=h(D||A||N_j||SID)$, $M_4=A \oplus N_i \oplus N_j$. Finally, S sends $\{M_3,M_4\}$ to U.

Step 2: Upon receiving $\{M_3,M_4\}$, U computes $N_j = A \oplus N_i \oplus M_4$ and checks $h(D||A||N_j||SID)$ with M_3. If they are not equal, U terminates the session. Then, the U computes $SK=h(D||A||N_i||N_j||SID)$ as the session key and sends $M_5=h(D||A||N_i||SID)$ to S.

Step 3: Upon receiving M_5, S computes $h(D||A||N_i||SID)$ and checks it with M_5. If they are equal, S successfully authenticates U and computes $SK=h(D||A||N_i||N_j||SID)$ as the session key.

2.4. Password Change Phase

Step 1: U inserts the smart card and keys ID and PW. The smart card computes $A=h(b \oplus PW)$ and checks whether $h(ID||h(y)||A)$ is equal to C. If they are not equal, the smart card terminates the session. Otherwise, U chooses a new password PW_{new} and a new random number b_{new}.

Step 2: The smart card computes $A_{new}=h(b_{new} \oplus PW_{new})$ and $C_{new}=h(ID||h(y)||A_{new})$ and replaces $\{b,C\}$ with $\{b_{new}, C_{new}\}$.

2.5. Cryptanalysis of Li *et al.'s* Scheme

Smart Card Loss Problem. Li *et al.'s* dynamic ID scheme cannot achieve two-factor authentication. The authors claimed that even the attacker extracts the information stored in the smart card he cannot login into the system. We assume that the attacker obtains a user's smart card. Without the user's password, the attacker can impersonate the cardholder to cheat the server.

Step 1: The attacker first extracts the information $\{C,D,E,h(),h(y),b\}$ stored in the smart card and intends to cheat the server S.

Step 2: The attacker generates a nonce N_i and a random value *CID*. Then he computes $P=E \oplus h(h(SID||h(y))||N_i)$, $M_1=h(P||CID||D||N_i)$ and $M_2=h(SID||h(y)) \oplus N_i$. The attacker sends login request message $\{P,CID,M_1,M_2\}$ to *S*.

Step 3: Upon receiving the login message $\{P,CID,M_1,M_2\}$, *S* computes $N^*=h(SID||h(y)) \oplus M_2$, $E^*=P \oplus h(h(SID||h(y))||N^*)$, $B^*=E^* \oplus h(x||y)$, $D^*=h(B^*||h(x||y))$ and $A^*=CID \oplus h(D^*||SID||N^*)$. *S* checks whether $h(P||CID||D^*||N^*)$ is equal to M_1. Obviously, we have $N^*=N_i$, $E^*=E$, $B^*=B$ and $D^*=D$. Therefor, the value of $h(P||CID||D^*||N^*)$ is equal to M_1. *S* accepts the login request. Then *S* generates a random number N_j and computes $M_3=h(D^*||A^*||N^*||SID)$, $M_4=A^* \oplus N^* \oplus N_j$. Finally, *S* sends $\{M_3,M_4\}$ to *U*.

Step 4: The attacker intercepts the message $\{M_3,M_4\}$ and computes $\hat{A}=CID \oplus h(D||SID||N_i)$

. Since $D^*=D$ and $N^*=N_i$, we have $\hat{A}=A^*$. The attacker computes $N_j^* = \hat{A} \oplus N_i \oplus M_4$. Here we show N_j^* is equal to N_j.

$$\begin{aligned} N_j^* &= \hat{A} \oplus N_i \oplus M_4 \\ &= A^* \oplus N^* \oplus M_4 \\ &= A^* \oplus N^* \oplus A^* \oplus N^* \oplus N_j = N_j \end{aligned}$$

Then, the attacker computes $SK_i=h(D||\hat{A}||N_i||N_j^*||SID)$ as the session key and sends $M_5=h(D||\hat{A}||N_i||SID)$ to *S*.

Step 5: Upon receiving M_5, *S* computes $h(D^*||A^*||N^*||SID)$ and checks it with M_5. Since $D^*=D$, $N^*=N_i$ and $\hat{A}=A^*$, $h(D^*||A^*||N^*||SID)$ and M_5 are equal. After *S* successfully authenticates *U*, *S* computes $SK_j=h(D^*||A^*||N^*||N_j||SID)$ as the session key. Obviously, there is $SK_i=SK_j$.

Linkability Attack. If the attacker is another legal user who registers at the same *RC* with *U*, he can mount linkability attack on Li et al.'s dynamic ID scheme.

Step 1: The attacker first extracts $h(y)$ stored in his smart card. We notice that $h(y)$ is the same as the value stored in other smart card.

Step 2: If the user *U* wants login *S*, *U* inserts the smart card and keys *ID* and *PW*. The smart card generates a nonce N_i and computes $P=E \oplus h(h(SID||h(y))||N_i)$, $CID=A \oplus h(D||SID||N_i)$, $M_1=h(P||CID||D||N_i)$ and $M_2=h(SID||h(y)) \oplus N_i$. *U* sends login message $\{P,CID,M_1,M_2\}$ to *S*.

Step 3: The attacker comes near the server *S* and intercepts the transmitted message $\{P,CID,M_1,M_2\}$. Then he computes $N^*=h(SID||h(y)) \oplus M_2$, $E^*=P \oplus h(h(SID||h(y))||N^*)$. Obviously, there is $E^*=E$ where $E=h(ID||x) \oplus h(x||y)$. *x* and *y* are constants in the system. For different identity *ID*, the corresponding value of *E* is different. After the attacker derive the unique value of *E*, the attacker can trace the user by observing this value. Thus. the inside attacker can link the different sessions to the same user.

Compromise of Identity Problem. In Li *et al.'s* dynamic ID scheme, the authors suppose that the identity and the password should be kept secret simultaneously. It is not reasonable in practice. In many applications, a user registers the system using Email address, phone number or student number as his identity. These identity information are known to all. Even the identity is a secret key of the user, the scheme could not satisfy key independence. If the attacker compromises a user's identity *ID*, he can launch off-line password guessing attack on a stolen smart card.

Step 1: The attacker first extracts the information $\{C,h(y),b\}$ stored in the smart card. We have an identical equation $C=h(ID||h(y)||h(b \oplus PW))$.

Step 2: The attacker guesses a password PW^* and checks whether *C* is equal to $h(ID||h(y)||h(b \oplus PW^*))$. If they are equal, the attacker obtains the correct password, otherwise, the attacker tries another password.

The weakness of Li's scheme is due to the fact that the user's identity is related to the password by the value of $C=h(ID||h(y)||h(b \oplus PW))$ stored in the smart card.

3. Wang *et al.'s* Dynamic ID based Remote User Authentication Scheme

The Wang *et al.'s* scheme also contains four phases: registration phase, login phase, verification phase and password change phase. We show these first three phases in Figure 2.

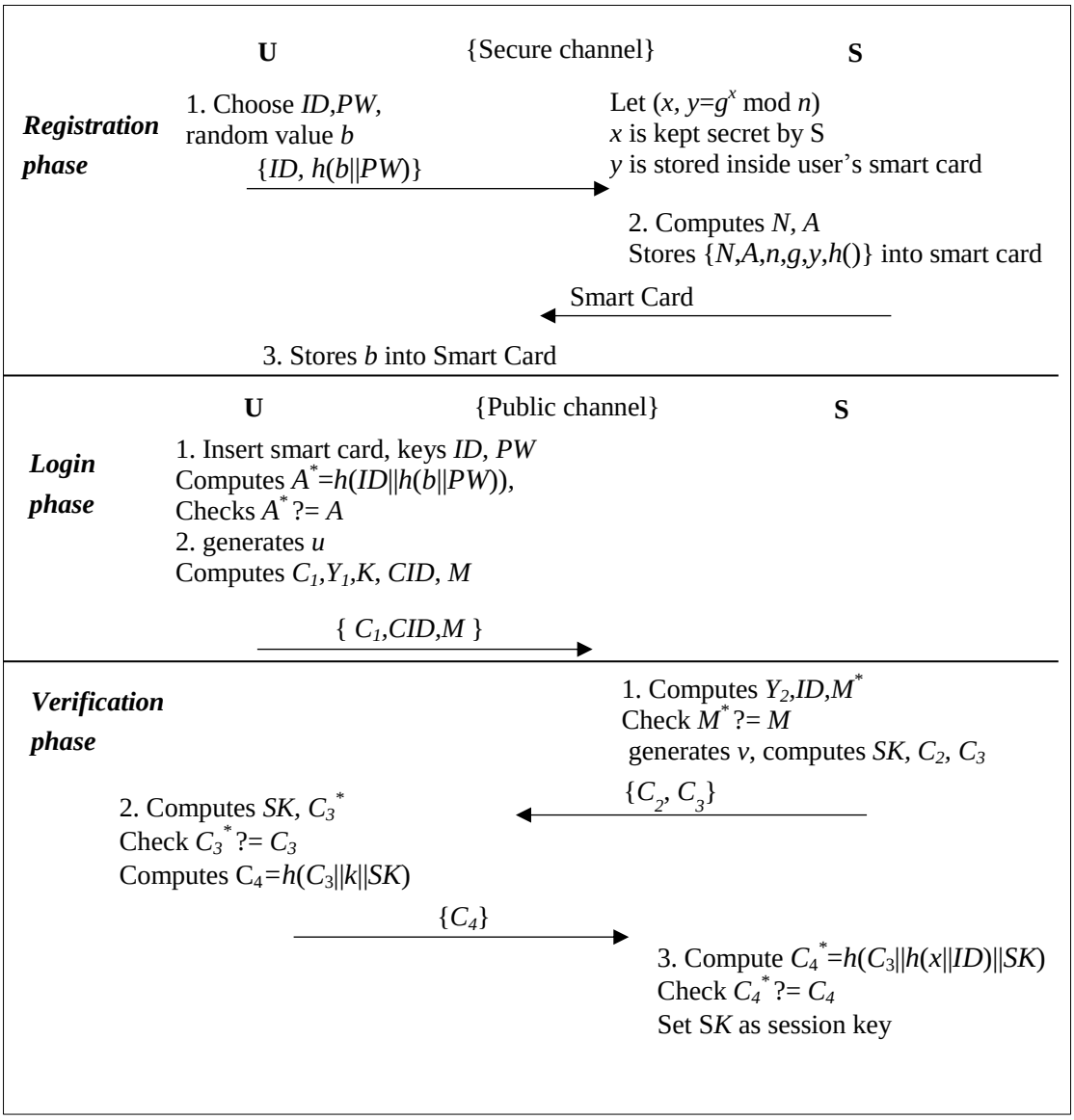


Figure 2. Wang *et al.'s* Scheme

3.1. Registration Phase

We assume that the user U and the server S have established a secure channel. Let $y=g^x \bmod n$ where n is a larger prime. (x,y) denote S's private key and its corresponding public key. U and S perform the following steps in registration phase.

Step 1: U chooses identity ID, password PW and a random value b. U sends $\{ID,h(b||PW)\}$ to S.

Step 2: S computes $N=h(b||PW) \oplus h(x||ID)$ and $A=h(ID||h(b||PW))$. S stores $\{N,A,n,g,y,h()\}$ on a smart card and sends it to U.

Step 3: U stores b into the smart card.

3.2. Login Phase

Step 1: U inserts the smart card and keys ID and PW. Then the smart card computes $A^*=h(ID||h(b||PW))$ and checks whether A^* is equal to the stored A. If they are not equal,the smart card terminates the session.

Step 2: The smart card generates a nonce u and computes $C_1=g^u \bmod n$, $Y_1=y^u \bmod n$, $k=N \oplus h(b||PW)$, $CID=ID \oplus h(C_1||Y_1)$ and $M=h(CID||C_1||k)$. U sends login request message $\{C_1,CID,M\}$ to S.

3.3. Verification Phase

Step 1: Upon receiving the login message $\{C_1,CID,M\}$, S computes $Y_2=(C_1)^x \bmod n$, $ID=CID \oplus h(C_1||Y_2)$ and $M^*=h(CID||C_1||h(x||ID))$ where x is its private key. S compares M^* with the received M. If they are not equal, the session is terminated. Otherwise, S generates a random number v and computes $SK=(C_1)^v \bmod n$, $C_2=g^v \bmod n$ and $C_3=h(SK||C_2||h(x||ID))$. Finally, S sends $\{C_2, C_3\}$ to U.

Step 2: Upon receiving $\{C_2, C_3\}$, U computes $SK=(C_2)^u \bmod n$, $C_3^*=h(SK||C_2||k)$, and checks C_3^* with C_3. If they are equal, U sets SK as the session key and sends $C_4=h(C_3||k||SK)$ to S.

Step 3: Upon receiving C_4, S computes $C_4^*=h(C_3||h(x||ID)||SK)$ and then checks whether C_4^* is equal to C_4. If the verification holds, S authenticates U and sets SK as the session key, otherwise, the session is terminated.

3.4. Password Change Phase

Step 1: U inserts the smart card and keys ID and PW. The smart card computes $A^*=h(ID||h(b||PW))$ and checks whether A^* is equal to A. If they are not equal, the smart card terminates the session. Otherwise, U picks a new password PW_{new}.

Step 2: The smart card computes $N_{new}=N \oplus h(b||PW) \oplus h(b||PW_{new})$, $A_{new}=h(ID||h(b||PW_{new}))$ and replaces N,A with N_{new} and A_{new}.

3.5. Cryptanalysis of Wang *et al.'s* Scheme

Off-line Password Guessing Attack.Wang *et al.* claimed that if the attacker steals a smart card and reveal the card's secret information he cannot launch off-line password guessing attack because he cannot guess ID and PW correctly at the same time. However, the attacker can launch password guessing attack without guessing the identity.

Step 1: The attacker first extracts the information $\{N,A,n,g,y,h(),b\}$ stored in the smart card.

Step 2: The attacker recorded login request message $\{C_1,CID,M\}$ in a previous session.

Step 3: The attacker guesses a password PW^* and computes $k^*=N \oplus h(b||PW^*)$. The attacker checks whether $h(CID||C_1||k^*)$ is equal to M. If they are equal, the attacker obtains the correct password, otherwise, the attacker tries another password.

Failure to Achieve Forward Anonymity.Although the session key is generated by Diffie-Hellman key agreement [15], Wang *et al.'s* dynamic ID scheme cannot provide forward anonymity. If the server's long-term key x is compromised, the attacker can derive the user's identity in a previous session.

Step 1: The attacker recorded login request message $\{C_1,CID,M\}$ in a previous session.

Step 2: The attacker computes $Y_1=(C_1)^x \bmod n$ using the compromised private key x and then obtains $ID=C ID \oplus h(C_1||Y_1)$. Thus, Wang et al.'s scheme cannot possesses anonymity once the server's long-term key x is compromised.

The same weakness also exists in Wang *et al.'s* another scheme [8].

4. Conclusion

In this paper, we have pointed out the security flaws of Li et al.'s, Wang et al.'s schemes. These weaknesses includes smart card loss problem, linkability attack, failure to achieve forward security, off-line password guessing attack, compromise of identity problem and smart card cloning problem. Up to now, none of the existing schemes can achieve all the desirable security goals. The identified security problems must be taken into account in designing dynamic ID based authentication scheme.

Acknowledgements

This work is supported by the 333 Project of Jiangsu Province (No. BRA2014047), and the Six Talent Peak Project of Jiangsu Province (No.2014-WLW-023).

References

[1] L. Lamport, "Password authentication with insecure communication", Communications of the ACM, vol. 24, no. 11, (**1981)**, pp. 770-772.
[2] C.-C. Chang and T.-C. Wu, "Remote password authentication with smart cards", Computers and Digital Techniques, IEE Proceedings E, vol. 138, no. 3, (**1991)**, pp. 165-168.
[3] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis", in Advances in Cryptology—CRYPTO'99, **(1999)**, pp. 388-397
[4] T. S. Messerges, E. A. Dabbish, and R. H. Sloan, "Examining smart-card security under the threat of power analysis attacks", Computers, IEEE Transactions on, vol. 51, no. 5, (**2002)**, pp. 541-552.
[5] J. Xu, W.-T. Zhu, and D.-G. Feng, "An improved smart card based password authentication scheme with provable security", Computer Standards & Interfaces, vol. 31, no. 4, (**2009)**, pp. 723-728.
[6] I.-E. Liao, C.-C. Lee, and M.-S. Hwang, "A password authentication scheme over insecure networks", Journal of Computer and System Sciences, vol. 72, no. 4, (**2006)**, pp. 727-740.
[7] R. Madhusudhan and R. Mittal, "Dynamic ID-based remote user password authentication schemes using smart cards: A review", Journal of Network and Computer Applications, vol. 35, no. 4, (**2012)**, pp. 1235-1248.
[8] D. Wang, C.-g. Ma, P. Wang, and Z. Chen, "Robust smart card based password authentication scheme against smart card security breach", Cryptology ePrint Archive, Report **(2012)**/4392012.
[9] Q. Xie, "Dynamic id-based password authentication protocol with strong security against smart card lost attacks", in Wireless Communications and Applications, ed: Springer, **(2012)**, pp. 412-418.
[10] C.-C. Lee, T.-H. Lin, and R.-X. Chang, "A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards", Expert Systems with Applications, vol. 38, no. 11, (**2011)**, pp. 13863-13870.
[11] C.-T. Li, C.-C. Lee, C.-J. Liu, and C.-W. Lee, "A robust remote user authentication scheme against smart card security breach", Data and Applications Security and Privacy XXV, (**2011)**, pp. 231-238.
[12] J. L. Tsai, T. C. Wu, and K. Y. Tsai, "New dynamic ID authentication scheme using smart cards", International Journal of Communication Systems, vol. 23, no. 12, (**2010)**, pp. 1449-1462.
[13] X. Li, J. Ma, W. Wang, Y. Xiong, and J. Zhang, "A novel smart card and dynamic ID based remote user authentication scheme for multi-server environments", Mathematical and Computer Modelling, vol. 58, no. 1–2, (**2013)**, pp. 85-95.
[14] D. Wang, C.-g. Ma, and P. Wu, "Secure password-based remote user authentication scheme with non-tamper resistant smart cards", in Data and Applications Security and Privacy XXVI, ed: Springer, **(2012)**, pp. 114-121.
[15] W. Diffie and M. E. Hellman, "New directions in cryptography", Information Theory, IEEE Transactions on, vol. 22, no. 6, (**1976)**, pp. 644-654.

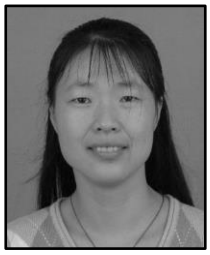
Authors

Jingxuan Zhai, he received his bachelor's degree and master's degree from the China University of Mining and Technology. he has been a Ph.D. degree candidate in applied computer Technology from the China University of Mining and Technology. His research interests include network security and security protocols.

Email: zhaijx@cumt.edu.cn

Tianjie Cao, he received the BS and MS degree in mathematics from Nankai University, Tianjin, China and the PhD degree in computer software and theory from State Key Laboratory of Information Security of Institute of Software, Chinese Academy of Sciences, Beijing, China. He is a professor of computer science in the School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, China. From 2007 to 2008, he has been a visiting scholar at the Department of Computer Sciences and CERIAS, Purdue University. His research interests are in security protocols and network security.

Email: tjcao@cumt.edu.cn



Xiuqing Chen, she received her bachelor's degree and master's degree from the China University of Mining and Technology. She has been a Ph.D. degree candidate in applied computer Technology from the China University of Mining and Technology. Her research interests include security protocols and network security.

Email: xiuqingchen@cumt.edu.cn