International Journal of Security and Its Applications
Vol. 9, No. 6 (2015), pp. 115-124
http://dx.doi.org/10.14257/ijsia.2015.9.6.12

An Improved User-Participating Authentication Scheme

Huang Shi*, Tianjie Cao and Gao Caiyun

School of Computer Science and Technology, China University of Mining and Technology, Xuzhou, 221116, P.R.China

Abstract

Authentication between user and server has become more and more important in the insecure network. Chen et al's proposed a user-participating authentication scheme. The CAPTCHA techniques and visual secret sharing is used in their scheme. The scheme can complete mutual authentication and resist certain known attacks. But for password guessing attack and denial-of-service attack, it can not resist. Therefore, an improved scheme to eliminate these weaknesses is proposed in this paper.

Keywords: *Authentication, Security, Smartcard, Visual secret sharing*

1. Introduction

With the rapid development of computer network technology, more and more people use the services of the remote servers. Therefore, mutual authentication between users and servers has become a troublesome problem. One method can resolve the problem is through the password-based authentication.

Hwang and Lee proposed a new remote user authentication scheme using smart card [1]. The server in this scheme needs to compute user's passwords and does not need to store verification tables. Sun proposed an efficient remote user authentication scheme using smart cards [2]. A one-way hash function is used in this scheme, but the passwords used in this scheme are hard to be remembered. Chien et al. proposed an efficient and practical scheme [3]. It is allowed to choose and change passwords by users and the mutual authentication between user and server is provided in this scheme. But the scheme can not resist parallel session attacks [4]. To improve security, many password schemes have been proposed. However, most of them are still vulnerable to various attacks [5-6].

Recently, Chen proposed a novel user-participating authentication scheme [7]. The CAPTCHA and visual secret sharing technology are used in this scheme. The advantages in Yang's scheme also exist in this scheme and it can complete the mutual authentication between user and server. But the scheme can not resist the password guessing and denial of service attack. Therefore, an improved scheme is proposed in this paper. The propose scheme can eliminate the weakness in the Chen's scheme.

2. Review of Chen et al.'s Scheme

Some notations used in the scheme are as follows:

U_i, S, SC: a user, the remote authentication server, smart card.

ID_i, PW_i: the user U_i's identity, the user U_i's password.

x: the long-term secret key of S.

N, m, r : three random numbers.

$\oplus$: the bitwise XOR operation.

img_m: CAPTCHA image. There are distorted numbers and characters m on the image. These numbers and characters can be the human eyes identification.

$VC(.,.)$: (2,2) visual cryptography scheme function. A secret image and a predefined share image are entered and another share image is outputted.

$CAPTCHA(\cdot)$: CAPTCHA image generator function. A series of numbers or characters are entered and the corresponding CAPTCHA image is generated.

$H(\cdot)$: a secure one-way hash function.

$[\cdot]_k$: a symmetric encryption function with the key k.

The scheme consists of three phases: registration phase, authentication phase and the password update phase.

Registration phase. In this phase, user U_i completes the registration to the server S. S chooses key x as its long-term key and keeps x secret.

(1) User U_i selects his password PW_i and a random number N. User U_i computes $H(PW_i \oplus N)$ and sends his identity ID_i and $H(PW_i \oplus N)$ to the server S.

(2) After receiving the message form user U_i, S computes $C_1 = H(ID_i \oplus x) \oplus H(PW_i \oplus N)$ and stores C_1 into SC. S sends the smart card to user. User U_i stores the random number N into smartcard.

Authentication Phase. In this phase, it will complete the mutual authentication between the user and server. User U_i inserts the smartcard into login equipment and input his identity ID_i and password PW_i. SC will perform the following operations:

(1) SC generates the previously VCS share image S_1 and chooses the random number r_1. Then, SC computes $H(PW_i \oplus N), C_2 = C_1 \oplus H(PW_i \oplus N), H(S_1, r_1.C_2), [S_1]_{C_2 \oplus r_1}$. SC sends the message $\{ID_i, [S_1]_{C_2 \oplus r_1}, r_1, H(S_1, r_1, C_2)\}$ to server S.

(2) After receiving message form SC, S computes $H(ID_i \oplus x) \oplus r_1$ ($H(ID_i \oplus x) \oplus r_1 = C_2 \oplus r_1 = C_1 \oplus H(PW_i \oplus N) \oplus r_1$) and decrypts $[S_1]_{C_2 \oplus r_1}$ into S_1'. S verifies whether $H(S_1', r_1, C_2)$ is equal to $H(S_1, r_1, C_2)$. If they are equal, the following operations will be performed, else the login request will be refused.

(3) S randomly chooses message m which is made up by digitals and characters and generates the CAPTCHA image $img_m = CAPTCHA(m)$. S chooses random number r_2, then computes another share image $S_2 = VC(S_1', img_m)$, symmetric key $H(ID_i \oplus x) \oplus r_2$ and $[S_2]_{H(ID_i \oplus x) \oplus r_2}$. S sends message $[S_2]_{H(ID_i \oplus x) \oplus r_2}, r_2, H(S_2, r_2, C_2)$ to SC.

(4) After receiving the message form S, SC computers symmetric key $C_2 \oplus r_2 = H(ID_i \oplus x) \oplus r_2$ and decrypts $[S_2]_{H(ID_i \oplus x) \oplus r_2}$ to S_2'. SC verifies whether $H(S_2', r_2, C_2)$ is equal to $H(S_2, r_2, C_2)$. If they are equal, the server S will be verified

and the following operation will be performed, else SC will stop the connection with server.

(5) SC overlay share image S_1 and S_2' which will obtain message m'. SC sends the message m' to server S. S verifier whether m' is equal to m. If they are equal, user U_i is verified by server S.

3. Password Update Phase

In this phase, it will complete the password update operation. Given that user U_i wants to update the password PW_i to PW_i'. Without the help of server S, user U_i can perform the following operation to complete it. User U_i enters his identity ID_i, the old password PW_i and the new password PW_i' to smartcard SC, then SC computes $H(PW_i \oplus N), H(PW_i' \oplus N)$ and $C_1' = C_1 \oplus H(PW_i \oplus N) \oplus H(PW_i' \oplus N)$. SC replaces C_1 with C_1'.

There are security vulnerabilities in Chen et al.'s scheme. Given that attacker can obtain user's password or the secret information in the smartcard, but attacker can not know the user's password and secret information in the same time. If he has both in the same time, there is no method to prevent the attacker to imitate the users. Attacker can break the smartcard quickly and easily. They can obtain the secret information in the smartcard by the consumption of performance testing or analysis of the disclosure of information.

Chen *et al.*'s scheme can not resist the password guessing attack and denial of service attack.

3.1 Password Guessing Attack

Users prone choose passwords which is easy to remember as their passwords. Therefore, attackers can guess user's password. In Chen *et al.*'s scheme, there are two issue need to be attended. One is that the user's passwords can not be spread between the client and server in the authentication process. The other is that it is need to preserve the sensitive information in the smartcard. If the smartcard is lost and the date in the smartcard is obtained, the information about passwords can not be disclosed.

Chen *et al.*'s scheme can not resist the password guessing attack. The following is the example about it.

If the smartcard is lost and attacker obtains the smartcard, the attacker can obtain the information N and C_1 in the smartcard. The attack process is as follow:

(1) Attacker guesses a new password PW' and computes $C_2' = C_1 \oplus H(PW' \oplus N)$;

(2) Attacker can obtained $H(S_1, r_1, C_2)$ and random number r_1 in the transmission channel. If $W = [S_1]_{C_2 \oplus r_1}$, the attacker can obtain the S_1' by decrypting the W ($S_1' = D_{C_2' \oplus r_1}[W]$).

(3) Attacker computes $H(S_1', r_1, C_2')$. If $H(S_1', r_1, C_2')$ is equal to $H(S_1, r_1, C_2)$, the guessing password PW' is the correct password. If not, the guessing password PW' is error.

In the second step, attacker can obtain the share image information S_1'. Images have a certain format. If the information of S_1' satisfies the format of a kind of format, the guessing is correct. If not, the guessing is error.

3.2. Denial of Service Attack

In Chen *et al.*'s scheme, the password update is completed in the smartcard which is not need the help of server. Chen et al.'s scheme can not resist denial of service attack.

Given that attacker obtains user U_i's smartcard temporarily. Attacker inserts the smartcard to login device and performs the following operations: Attacker randomly chooses two different passwords PW' and PW'' as the old password and the new password. Attacker requests password update to smartcard. The SC computes $H(PW'\oplus N), H(PW''\oplus N),$ and $C_1' = C_1 \oplus H(PW'\oplus N) \oplus H(PW''\oplus N)$. Then, SC replaces C_1 with C_1' to complete the password update. From now on, user U_i will not pass the authentication process without the new password PW''.

4. The Improved User-Participating Authentication Scheme

First, the format of share images is defined. Share images are all bitmap. The fixed format is as followed:

Typedef struct tagbitmap{

Long bmtype;// Bitmap type which must be 0

Long bmWidth;// Bitmap width which is 256

Long bmHeight;// Bitmap height which is 200

Long bmWidthBytes;// The number of byte in each line which is 256

Word bmPlanes;// The number of color planes which is 3

Word bmBitsPixel;// The number of pixel bytes which is 32

Lpvoid bmBits;// Bitmap memory pointer }bitmap;

The format of share image is defined by both the user and server, so the attackers do not know. The attackers can not verify their guess by the format of share images.

There are also three phases in the improved scheme. They are also registration phase, authentication phase and password update phase.

4.1 Registration Phase

(a) $U_i \to S$ ： $ID_i, H(PW_i \oplus N)$

User U_i selects his password PW_i and a random number N. User U_i computes $H(PW_i \oplus N)$ and sends his identity ID_i and $H(PW_i \oplus N)$ to the server S.

(b) $S \to SC$ ： $C_1, H(\cdot)$

After receiving the message form user U_i, S computes $C_1 = H(ID_i \oplus x) \oplus H(PW_i \oplus N)$ and stores C_1 into SC. S sends the smart card to user. User U_i stores the random number N into smartcard.

Registration phase is as Figure 1.

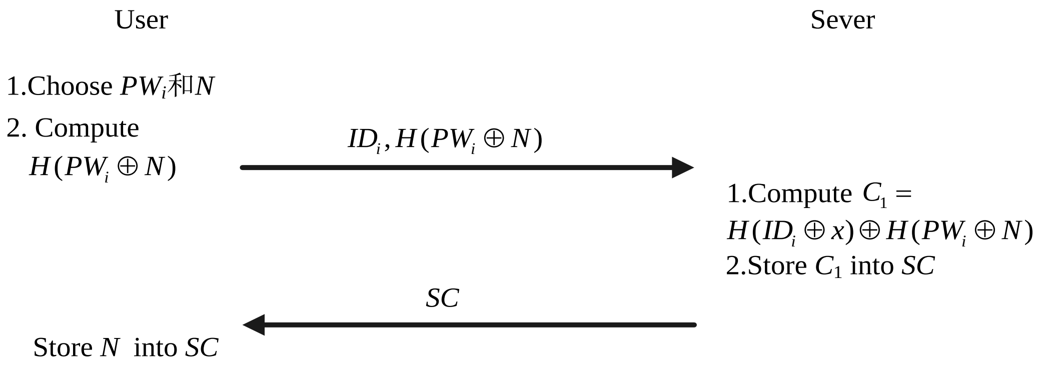

Figure 1. Processes in the Registration Phase

4.2. Authentication Phase

(a) $SC \to S$： $ID_i, [S_1]_{C_2 \oplus r_1}, r_1$

User U_i inserts the smartcard into login equipment and input his identity ID_i and password PW_i. SC will perform the following operations:

(a.1) SC generates the previously VCS share image S_1 and chooses the random number r_1. (a.2) SC computes $H(PW_i \oplus N), C_2 = C_1 \oplus H(PW_i \oplus N), [S_1]_{C_2 \oplus r_1}$. SC sends the message $\{ID_i, [S_1]_{C_2 \oplus r_1}, r_1\}$ to server S;

(b) $S \to SC$： $[S_2]_{H(ID_i \oplus x) \oplus r_2}, r_2$

After receiving message form SC, S performs the following operations:

(b.1)S computes symmetric key $H(ID_i \oplus x) \oplus r_1 = C_2 \oplus r_1 = C_1 \oplus H(PW_i \oplus N) \oplus r_1$) and decrypts $[S_1]_{C_2 \oplus r_1}$ into S_1'.

(b.2)S randomly chooses message m which is made up by digitals and characters and generates the CAPTCHA image $img_m = CAPTCHA(m)$.

(b.3)S chooses random number r_2, then computes another share image $S_2 = VC(S_1', img_m)$, symmetric key $H(ID_i \oplus x) \oplus r_2$ and $[S_2]_{H(ID_i \oplus x) \oplus r_2}$. S sends message $[S_2]_{H(ID_i \oplus x) \oplus r_2}, r_2$ to SC;

(c) $SC \to S$： m'

After receiving the message form S, SC does the following operations:

(c.1)SC computers symmetric key $C_2 \oplus r_2 = H(ID_i \oplus x) \oplus r_2$ and decrypts $[S_2]_{H(ID_i \oplus x) \oplus r_2}$ to S_2'.

(c.2)SC overlay share image S_1 and S_2' which will obtain message m'. If message m' is the normal characters or digitals, server S is verified by user U_i. SC sends the message m' to server S.

Finally, S verifies whether m' is equal to m. If they are equal, user U_i is verified by server S.

Authentication phase is as Figure 2.

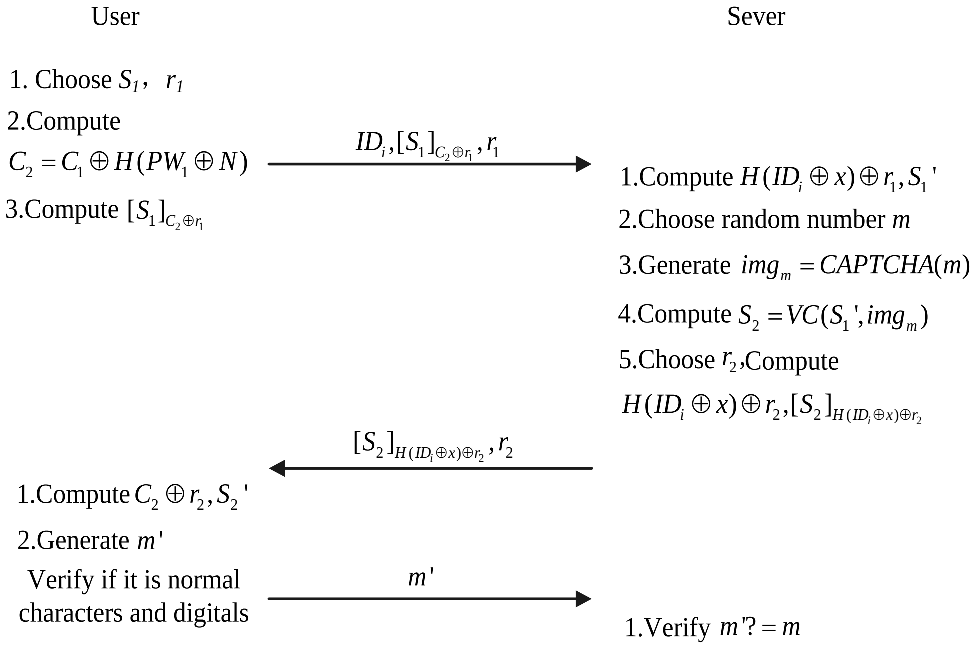
User
Sever
1. Choose S_1， r_1
2.Compute
$C_2 = C_1 \oplus H(PW_1 \oplus N)$
3.Compute $[S_1]_{C_2 \oplus r_1}$
$ID_i, [S_1]_{C_2 \oplus r_1}, r_1$
1.Compute $H(ID_i \oplus x) \oplus r_1, S_1'$
2.Choose random number m
3.Generate $img_m = CAPTCHA(m)$
4.Compute $S_2 = VC(S_1', img_m)$
5.Choose r_2,Compute
$H(ID_i \oplus x) \oplus r_2, [S_2]_{H(ID_i \oplus x) \oplus r_2}$
$[S_2]_{H(ID_i \oplus x) \oplus r_2}, r_2$
1.Compute $C_2 \oplus r_2, S_2'$
2.Generate m'
Verify if it is normal
characters and digitals
m'
1.Verify $m'? = m$

Figure 2. Processes in the Authentication Phase

4.3. Password Update Phase

Schemes are suffered from the DOS. Therefore, given that if attackers temporarily obtain user's smartcard, they can not get any information in the smartcard.

Given that user U_i wants to update the password PW_i to PW_i'. The process of password update is as followed:

(a) $SC \to S$： $ID_i, [S_1]_{C_2 \oplus r_1}, r_1$

User U_i inserts the smartcard into login equipment and input his identity ID_i and password PW_i. SC will perform the following operations:

(a.1) SC generates the previously VCS share image S_1 and chooses the random number r_1. (a.2) SC computes $H(PW_i \oplus N), C_2 = C_1 \oplus H(PW_i \oplus N), [S_1]_{C_2 \oplus r_1}$. SC sends the message $\{ID_i, [S_1]_{C_2 \oplus r_1}, r_1\}$ to server S;

(b) $S \to SC$： $[S_2]_{H(ID_i \oplus x) \oplus r_2}, r_2, H(S_2, m, r_2)$

After receiving message form SC, S performs the following operations:

(b.1)S computes symmetric key $H(ID_i \oplus x) \oplus r_1 = C_2 \oplus r_1 = C_1 \oplus H(PW_i \oplus N) \oplus r_1)$ and decrypts $[S_1]_{C_2 \oplus r_1}$ into S_1'.

(b.2)S randomly chooses message m which is made up by digitals and characters and generates the CAPTCHA image $img_m = CAPTCHA(m)$.

(b.3)S chooses random number r_2, then computes another share image $S_2 = VC(S_1', img_m)$, symmetric key $H(ID_i \oplus x) \oplus r_2, [S_2]_{H(ID_i \oplus x) \oplus r_2}$ and $H(S_2, m, r_2)$. S sends message $[S_2]_{H(ID_i \oplus x) \oplus r_2}, r_2, H(S_2, m, r_2)$ to SC;

(c) After receiving the message form S, SC does the following operations:

(c.1)SC computers symmetric key $C_2 \oplus r_2 = H(ID_i \oplus x) \oplus r_2$ and decrypts $[S_2]_{H(ID_i \oplus x) \oplus r_2}$ to S_2'.

(c.2)SC overlay share image S_1 and S_2' which will obtain message m'. SC verifies that whether $H(S_2', m', r_2)$ is equal to $H(S_2, m, r_2)$.If they are not equal, password update operation can not be performed. If they are equal, the following operations are performed: First, user U_i enters his identity ID_i, the old password PW_i and the new password PW_i' to smartcard SC, then SC computes $H(PW_i \oplus N), H(PW_i' \oplus N)$ and $C_1' = C_1 \oplus H(PW_i \oplus N) \oplus H(PW_i' \oplus N)$. SC replaces C_1 with C_1'.
Password update phase is as Figure 3.

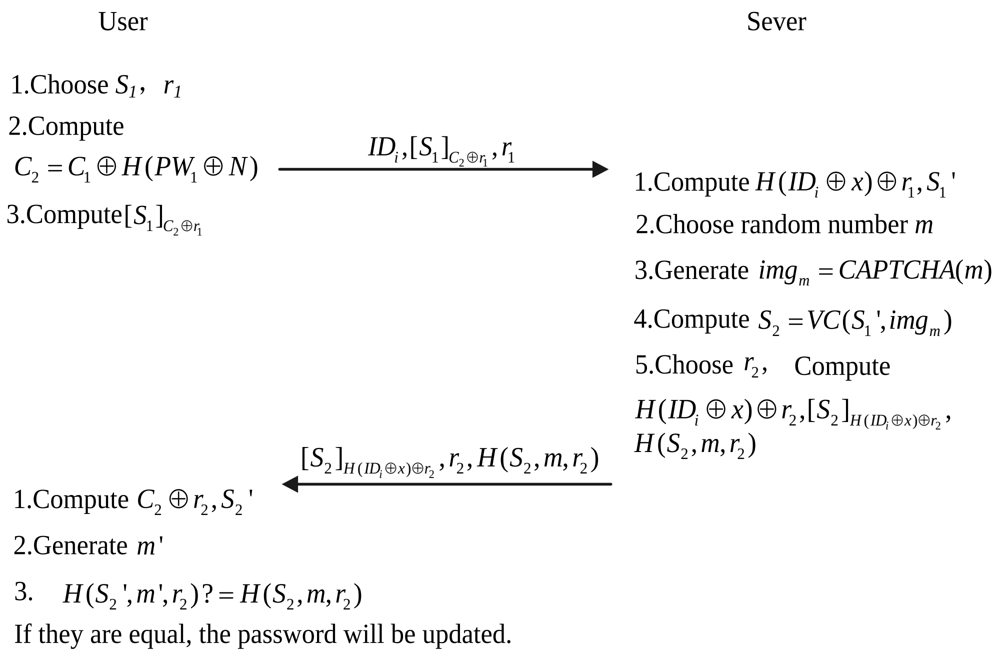
User
Sever
1.Choose S_1, r_1
2.Compute
$C_2 = C_1 \oplus H(PW_1 \oplus N)$
3.Compute$[S_1]_{C_2 \oplus r_1}$
$ID_i, [S_1]_{C_2 \oplus r_1}, r_1$
1.Compute $H(ID_i \oplus x) \oplus r_1, S_1'$
2.Choose random number m
3.Generate $img_m = CAPTCHA(m)$
4.Compute $S_2 = VC(S_1', img_m)$
5.Choose r_2, Compute
$H(ID_i \oplus x) \oplus r_2, [S_2]_{H(ID_i \oplus x) \oplus r_2}$,
$H(S_2, m, r_2)$
$[S_2]_{H(ID_i \oplus x) \oplus r_2}, r_2, H(S_2, m, r_2)$
1.Compute $C_2 \oplus r_2, S_2'$
2.Generate m'
3. $H(S_2', m', r_2) ? = H(S_2, m, r_2)$
If they are equal, the password will be updated.

Figure 3. Authentication Processes in the Password Updating Phase

5. Security Analysis of the Improved Scheme

The proposed scheme can resist the password guessing attack and denial of service attack. First, it is need to give two assumptions:

Assumption 1: Secure one-way function whose enter is variable-length string and the output is fixed-length string. The definition of secure one-way function $H(\cdot)$ is as followed:

It is easy to compute $H(m)$ with the input message m;

It is Computationally infeasible to get message m form hash value $H(m)$;

It is Computationally infeasible to find two different message m_1 and m_2 that hash value $H(m_1) = H(m_2)$.

Assumption 2: Secure CAPTCHA which can secure and effective resist identification form proxy or software. CAPTCHA is a difficult artificial intelligence problem for computers, but it is easy for human to distinguish.

The proposed scheme can resist a variety of malicious attacks. They are shown as followed:

(1) Replay attack

For each login request, scheme generates a new different message m. If attacker intercepts the information $ID_i, [S_1]_{C_2 \oplus r_1}, r_1$ in step (a) and replay these information to server, attacker must have fresh message m' to satisfy the authentication in step (c). In order to obtain the message m', attacker must know the share S_1 and S_2, but S_1 and S_2 is preserved by secure one-way function and symmetric cryptosystem. The attacker can not obtain share S_1 and S_2. So he can not get message m'.

(2) Password guessing attack

If the smartcard is lost, the attacker can get the information C_1 and N in the smartcard. The attack attempts to guess the password. But he can not verify his guess through the intercepted information. The scheme can resist the password guessing attack.

(3) On-line guessing attack

In the scheme, users need to identify the message m form the overplayed share images to verify they are legit users. Within a short period of time, the attacker can repeatedly login the system. So the scheme can resist on-line guessing attack.

(4) Man-in-the-middle attack

Man-in-the-middle attack means that an active attacker intercepts the communication information between the legal user and the server and uses some means to successfully masquerade as both the server to the user and the user to the server. Then, the user will believe that he is talking to the intended server and vice versa.

If an attacker attempts to imitate the legal user, the attacker must have the correct message m to pass authentication. In order to obtain the message m', attacker must know the share S_1 and S_2, but S_1 and S_2 is preserved by secure one-way function and symmetric cryptosystem. The attacker can not obtain share S_1 and S_2. So he can not imitate legal user.

If an attacker attempts to imitate legal server, he must to forge the message $[S_2]_{H(ID_i \oplus x) \oplus r_2}, r_2$. But the attacker does not know the long-term key x. He can not forge the message, So he can not imitate legal user.

(5) Denial of service attack

Scheme sets up that the attacker can not get any information from smartcard if attacker temporarily obtains the smartcard. The attacker can not modify the password. So the scheme is secure against denial of service attack.

6. Conclusion

Modern life sees ever more authentication protocols required when making use of Internet network services like E-learning, on-line polls, on-line ticket-order system, roll call systems, on-line games, etc. Chen proposed scheme can not effective against the password guessing attack and denial-of-service attack. An improved scheme to eliminate the security vulnerability is proposed in this paper.

Acknowledgement

This work was supported in part by The Social Technology Project of China University of Mining and Technology (Grant No. 2014KJZX07).

References

[1] M. S. Hwang and L. H. Lee, "A new remote user authentication scheme using smart card", IEEE Transactions on Consumer Electronics, vol. 46, no. 1, **(2000)**, pp. 28-30.

[2] H. M. Sun, "An efficient remote user authentication scheme using smart cards", IEEE Transactions on Consumer Electronics, vol. 46, **(2000)**, pp. 958-961.

[3] H. Y. Chien, J. K. Jan and Y. M. Tseng, "An efficient and practical solution to remote authentication: smart card", Computers and Security, vol. 21, no. 4, **(2002)**, pp. 372-375.

[4] C. L. Hsu, "Security of Chien et al.'s remote user authentication scheme using smart cards", Computer Standards and Interfaces, vol. 26, no. 3, **(2004)**, pp. 167-169.

[5] C.-T. Li, "A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card", IET Information Security, vol. 7, no. 1, **(2013)**, pp. 3-10.

[6] D. He and H. Hu, "Cryptanalysis of a Dynamic ID-Based Remote User Authentication Scheme with Access Control for Multi-Server Environments", IEICE Transactions 96-D(1), **(2013)**, pp. 138-140.

[7] T. H. Chen and J. C. Huang, "A novel user-participating authentication scheme", The Journal of System and Software, vol. 83, **(2010)**, pp. 861-867.

Authors

Huang Shi, born in October, 1979, Anhui, The People′s Republic of China 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 Computer Software and Theory from the China University of Mining and Technology. His research interests include security protocols and network security. Email: huangshi@cumt.edu.cn

Tianjie Cao 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 aprofessor 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

Gao Caiyun, received her bachelor's degree and master's degree from the China University of Mining and Technology.