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
E-mail address: huangshi@cumt.edu.cn

Abstract. Authentication between user and server has become more and more important in the insecure network. The scheme can complete mutual authentication and resist certain known attacks. But for password guessing attack and denial-of-service attack, it cannot 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 cannot 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].

2 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 \( C_1' = C_1 + H(PW_i \oplus N) \oplus H(PW_i' \oplus N) \). \( SC \) 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. 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 \( C_1' = C_1 + H(PW' \oplus N) \oplus H(PW'' \oplus N) \). Then, \( SC \) replaces \( C_i \) with \( C_i' \) to complete the password update. From now on, user \( U_i \) will not pass the authentication process without the new password \( PW'' \).

3 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.

Chen et al.’s scheme can not resist the password guessing attack and denial of service attack.
After receiving the message from user $U_i$, $S$ computes $C_i = H(ID \oplus x) \oplus H(PW_i \oplus N)$ and stores $C_i$ 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.

**Fig. 1. Processes in the registration phase**

Authentication phase is as figure 2.

**Fig. 2. Processes in the authentication phase**

4 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.

5 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 cannot effective against the password guessing attack and denial-of-service attack. An improved scheme to eliminate the security vulnerability is proposed in this paper.

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

References

5. C.-T. Li, A new password authentication and user anonymity scheme based on elliptic curve cryptography and smart card, IET Information Security, 7(1), 3-10, 2013