Advanced Science and Technology Letters
Vol.111 (NGCIT 2015), pp.70-73
http://dx.doi.org/10.14257/astl.2015.111.14

# 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,

ISSN: 2287-1233 ASTL

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.

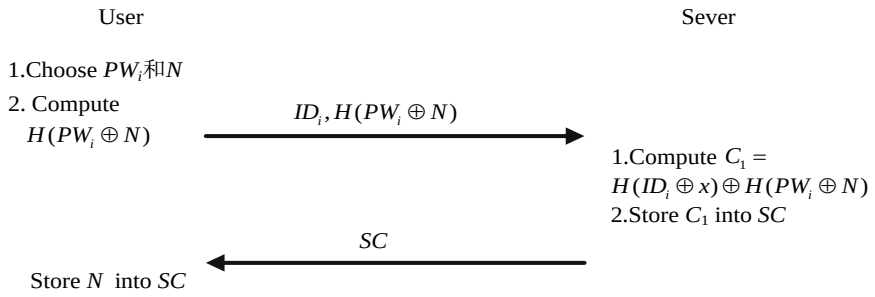


**Fig. 1.** Processes in the registration phase

Authentication phase is as figure 2.

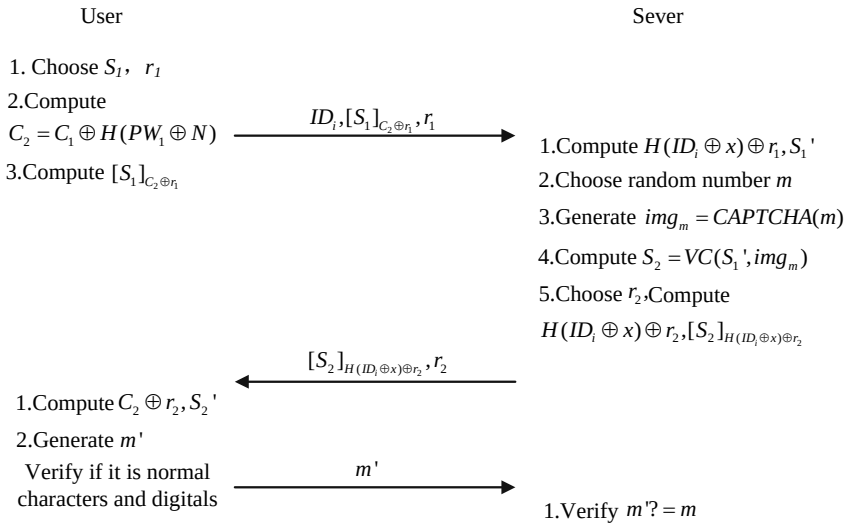


**Fig. 2.** Processes in the authentication phase

## 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

1. Hwang, M.S., Lee, L.H., A new remote user authentication scheme using smart card. IEEE Transactions on Consumer Electronics 46 (1):28–30 , 2000.
2. Sun, H.M. An efficient remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics 46:958–961., 2000
3. Chien, H.Y., Jan, J.K., Tseng, Y.M., An efficient and practical solution to remote authentication: smart card. Computers and Security 21 (4):372–375, 2002
4. Hsu, C.L., Security of Chien et al.'s remote user authentication scheme using smart cards. Computer Standards and Interfaces 26 (3):167–169, 2004
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
6. Debiao He, Hao Hu: Cryptanalysis of a Dynamic ID-Based Remote User Authentication Scheme with Access Control for Multi-Server Environments. IEICE Transactions 96-D(1): 138-140, 2013
7. Chen, T.H., Huang, J.C., A novel user-participating authentication scheme. The Journal of System and Software 83:861-867, 2010

 