Security Analysis on Password-based Authentication Scheme for Multi-Server Environments*

Youngsook Leet [1], Jeeyeon Kim[2], Dongho Wont[2]

Department of Cyber Investigation Police, Howon University, 727, Impi-Myeon, Gunsan-si, Jeonrabuk-do, 573-718, Korea
ysooklee@howon.ac.kr
[2]School of Information and Communication Engineering, Sungkyunkwan University, 300 Cheoncheon-dong, Jangan-gu, Suwon-si, Gyeonggi-do, 440-746, Korea
jeeyeonkim@paran.com, dhwon@security.re.kr

Abstract. Recently, Tan proposed a remote user authentication scheme suited for multi-server environments, in which users can be authenticated using a single password shared with the registration center. A fundamental requirement for password-based authentication is security against off-line password guessing attacks. However, Tan's scheme fails to meet the requirement. In this paper, we report this security problem with Tan's scheme.

Keywords: authentication scheme; smart card; password; off-line password guessing attack; multi-server environment.

1 Introduction

In 2011, Tan [8] proposed an efficient remote user authentication scheme suited for multi-server environments [1, 2, 3, 4, 9, 10, 11, 12, 13]. In its article, Tan claims that the user can be authenticated by all servers included in multi-server environments using a single password shared with the registration center and establishes the session key to be shared with between the server and the user.

In addition to making this claim, Tan claims to exhibit various merits with its scheme: (1) it allows the user to register only once with the registration center and then he/she is able to gain access to all servers included in multi-server environments without registering with every single server; (2) it does not require any server and the registration center to maintain a password table for verifying the legitimacy of login users; (3) it allows users to choose and change their passwords according to their liking and hence gives more user convenience; (4) it allows the user to change its password freely after assuring the legality of it; (5) it is extremely efficient in terms of

* This work was supported by Howon University in 2012 t The first author
Corresponding author.

the computational cost since the protocol participants perform only a few hash function operations; (6) it allows the user two factor security [8].

First of all, a fundamental requirement for password-based authentication is security against off-line dictionary attacks [14]. However, Tan's scheme fails to meet the requirement. In this paper, we report this security problem with Tan's scheme. What we do in this work is to report these security vulnerabilities of Tan's scheme.

2 Review of Tan's Password Authentication Scheme

This section reviews a remote user authentication scheme proposed by Tan [7]. The scheme participants include a registration center, a remote user, and multiple servers. For simplicity, we denote the registration center by *RC,* the remote user by *Uz,* and the servers by Si, S2, , *Sn.* The scheme assumes that the registration center *RC* is a trust party responsible for securely delivering the secret keys to be shared with between (// and *Si*.

Tan's scheme consists of four phases: initialization phase, registration phase, login phase, and authentication phase. The initialization phase is processed when the server who wants to join to the system registers with the registration center. The registration phase is performed only once per user when a new user registers itself with the registration center. The login and the authentication phases are carried out whenever a user wants to gain access to each server included in multi-server environments. Before the registration phase is performed for the first time, the registration center *RC* decides on the following system parameters: a one-way hash function *h* and two cryptographic keys x and *y.* The keys x and *y* are shared securely with the registration center. The notation in Table 1. is employed throughout this paper

Table 1. Notation

pw	Password of an entity U_i
ID,	Identity of an entity *U,*
SID,	Identity of an entity 5,
$_{t1, t2, t3}$	Timestamp
$E_K(X)$	Encryption of *X* using an asymmetric key *K*
$D_K(X)$	Decryption of *X* using an asymmetric key *K*
x, y	A cryptographic key
h()	One-way hash function
11	Concatenation operation
ED	XOR operation
m, n,	Random number

2.1 Initialization Phase

This phase is invoked whenever a server wants to join this group. During this phase, the registration center *RC* and the server perform the following running:

Step 1. A server *S,* who wants to registration with the system submits its identity *SID,* to the registration center *RC* via a secure channel.

Step 2. After receiving *S,* 's identity *SID, RC* computes p_i *as* $p_i = h(SIDv)$ and sends < p_i> *to RC* through a secure channel.

2.2 Registration Phase

This is the phase where a new registration of a user takes place. The registration proceeds as follows:

Step 1. A user *U,,* who wants to register with the registration center *RC,* submits a registration request, consisting of its identity *ID,,* to the registration center *RC* via a secure channel

Step 2. Upon receiving the request <*ID,*>, *RC* computes *K,* = x) and sends <K_1> to user U.

Step 3. Now the user *U,* chooses its password *PW,* at will and computes *B, = K, El) h(ID,IIPW,).* Then *U,* stores the values <*B,, ID,, ho*> on its smart card.

2.3 Authentication and Password Change Phase

If *U,* wants to change its password, *U,* inserts its smart card and its identity *ID,* and password *P.* The user *U,* issues a *Require* of replacing old password with a new password. The smart card executes the following steps.

Step 1. Given *IDE, Require,* and *PW,* the smart card generates a timestamp computes *T,= B, G) h(ID,IIPW,), F_1= E,(ID,IIRequirellt $_1$).*
Then *U,* sends the password request message <*ID, F_1*> to the registration center *RC.* **Step 2.** After receiving the message <*ID,, F $_1$*> , *RC* first acquires the current timestamp t_2 and computes *G,* as *G, = DT,(F).* Then *RC* verifies that: (1) *ID,* is valid, (2)
t_2 — At where *At* is the maximum allowed time interval for transmission delay. If both of these conditions hold, *RC* believes that the responding party is the genuine user and makes a tag which denotes Yes as the response for the request. Otherwise, *RC* makes a tag which denotes No. Now *RC* generates a new timestamp t_3, computes F_2 = EJ/D,Iitagl lt_3) and sends to the response message <F_2> to the user *U.*
Step 3. Having received <F_2> from *RC, U,* computes G_2 as $G_2 = D, (F_2)$. If tag represents No, *U,* stop the password change. Otherwise, the user *U,* chooses a new password *PW,,_,* computes *B,,,,, = B, El) h(ID,IIPW,) El) h(ID,IIPW,,,)* and replaces *B,* with

B. on the smart card.

3 Cryptanalysis of Tan's Scheme

In this section we point out that Tan's scheme suffers from an off-line password guessing attack [13].

3.1 Flaws in the scheme

Tan [7] claims that its authentication scheme prevents an attacker from learning some registered user's password via an off-line password guessing attack. But, unlike the claim, Tan's protocol is vulnerable to an off-line password guessing attack mounted by extracting the secret information from a smart card [8]. Now we assume that an attacker has stolen the U's smart card or gained access to it and extracted the secret value(B,) stored in it by monitoring its power consumption [5, 6]. More concretely, the problem with Tan's scheme is that whoever obtains the value *B,* stored in U,'s smart card, *RC's* response message F_2, and U·'s password change request message *F*, can find out the user U:s password *PW,*.

Acknowledgments

This work was supported by Howon University in 2012. The first author is Youngsook Lee (ysooklee@howon.ac.kr).

References

1. Chang C. and Kuo J. Y. An efficient multi-server password authenticated keys agreement scheme using smart cards with access control, IEEE Proceeding of the 19th International Conference on Advanced Information Networking and Applications 2 (2005) 257-260.
2. Ku W.-C., Chang S.-T., and Chiang M.-H. Weaknesses of a remote user authentication scheme using smart cards for multi-server architecture, IEICE Transactions on Communications E88-B(8) (2005) 3451-3454.
3. Li L.-H., Lin I.-C., and Hwang M.-S. A remote password authentication scheme for multi-server architecture using neural networks, IEEE Transaction on Neural Networks 12(6) (2001) 1498-1504.
4. Lin I.-C., Hwang M.-S., and Li L.-H. A new remote user authentication scheme for multi-server internet environments, Future Generation Computer System 19 (2003) 13-22.
5. P. Kocher, J. Jaffe, B. Jun, Differential power analysis, in Advances in Cryptology-CRYPTO'99 (1999) 388-397.
6. T.S. Messergers, E.A. Dabbish, R.H. Sloan, Examining smart card security under the threat of power analysis attacks, IEEE Trans. Comput. 51 (5) (2002) 541-552.

7. Z. Tan, Improvement on A Password Authentication Scheme for Multi-server Environments, Journal of Convergence Information Technology, 6 (1) 218-228, January, 2011.
8. Tian X., Zhu R.—W., and Wong D.S. Improved efficient remote user authentication schemes, International Journal of Network Security 4(2) (2007) 149-154.
9. Tsai J.-L. Efficient multi-server authentication scheme based on one-way hash function without verification table, Computers \&\ Security 27 (2008) 115-121.
10. Tsuar W.-J. An enhanced user authentication scheme for multi-server internet services, Applied Mathematics and Computation 170 (2005) 258-266.
11. Tsuar W.-J., Wu C.-C., and Lee W.-B. A flexible user authentication for multiserver internet services, Networking-JCN 2001 LNCS 2093 (2001) 174-183.
12. Tsuar W.-J., Wu C.-C., and Lee W.-B. A smart card-based remote scheme for password authentication in multi-server Internet services, Computer Standards \&\ Interfaces 27 (2004) 39-51
13. Y. L. and D. W. Security vulnerabilities of a Remote user authentication scheme using smart cards suited for a multi-server environment, Lecture Notes in Computer Science, 5593, (2009), 164-172.
14. Yang W.-H. and Shieh S.-P. Password authentication schemes with smart card, Computers \& Security 18(8) (1999) 727-733.