Security Analysis of an Efficient Smart Card-Based Remote User Authentication Scheme Using Hash Function

Ashok Kumar Das[1], Vanga Odelu[2], and Adrijit Goswami[3]

[1] Center for Security, Theory and Algorithmic Research
International Institute of Information Technology, Hyderabad 500 032, India
iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in
[2] Department of Mathematics
Rajiv Gandhi University of Knowledge Technologies, Hyderabad 500 032, India
odelu.vanga@gmail.com
[3] Department of Mathematics
Indian Institute of Technology, Kharagpur 721 302, India
goswami@maths.iitkgp.ernet.in

Abstract. In a remote user authentication scheme, a remote server verifies whether a login user is genuine and trustworthy. Several remote user authentication schemes using the password, the biometrics and the smart card have been proposed in the literature. In 2012, Sonwanshi et al. proposed a password-based remote user authentication scheme using smart card, which uses the hash function and bitwise XOR operation. Their scheme is very efficient because of the usage of efficient one-way hash function and bitwise XOR operations. They claimed that their scheme is secure against several known attacks. Unfortunately, in this paper we find that their scheme has several vulnerabilities including the offline password guessing attack and stolen smart card attack. In addition, we show that their scheme fails to protect strong replay attack.

Keywords: Cryptanalysis, Password, Remote user authentication, Smart card, Security, Hash function.

1 Introduction

Remote user authentication plays an important role in order to identify whether communicating parties are genuine and trustworthy where the users are authenticated by a remote server before allowing access to services. Several password-based schemes (for example [4], [7], [9]) or biometric-based schemes (for example [2], [3], [6]) have been proposed for remote user authentication. As pointed out in [7], an idle password-based remote user authentication scheme using smart cards needs to satisfy the following requirements: (1) without maintaining verification tables; (2) a user can freely choose and update password; (3) resistance to password disclosure to the server; (4) prevention of masquerade attacks; (5) resistance to replay, modification, parallel session and stolen-verifier attacks;

Sabu M. Thampi et al. (Eds.): SSCC 2013, CCIS 377, pp. 236–242, 2013.

(6) a easy-to-remember password; (7) low communication cost and computation complexity; (8) achieve mutual authentication between login users and remote servers; (9) resistance to guessing attacks even if the smart card is lost or stolen by attackers; (10) session key agreement; (11) resistance to insider attacks; and (12) prevention of smart card security breach attacks.

In 2012, Sonwanshi et al. proposed a remote user authentication scheme based on passwords using the smart card [9]. Their scheme is based on the one-way hash function and bitwise XOR operation. Due to efficiency of the hash function as well as bitwise XOR operation, their scheme is very efficient in computation. They claimed that their scheme is secure against various known attacks such as (i) resilient to Denial-of-Service (DoS) attack; (ii) resilient to offline password guessing attack; (iii) resilient to impersonation attack; (iv) resilient to parallel session attack; and (v) resilient to stolen smart card attack. However, in this paper we show that their scheme is insecure. We show that their scheme is vulnerable to the offline password guessing attack and stolen smart card attack. In addition, we show that their scheme fails to protect strong replay attack.

The rest of this paper is organized as follows. In Section 2, we review Sonwanshi et al.'s remote user authentication scheme using smart card. In Section 3, we show that Sonwanshi et al.'s scheme is vulnerable to offline password guessing attack and stolen smart card attack. In this section, we also show that their scheme fails to protect strong replay attack. Finally, we conclude the paper in Section 4.

2 Review of Sonwanshi et al.'s Smart Card Based Remote User Authentication Scheme

In this section, we briefly review the recently proposed Sonwanshi et al.'s scheme [9]. Their scheme consists of four phases: registration phase, login phase, authentication phase and password change phase. For describing this scheme, we use the notations given in Table 1.

Table 1. Notations used in this paper

Symbol	Description
U_i	User
S_j	Remote server
ID_i	Identity of user U_i
PW_i	Password of user U_i
X	Permanent secret key only known to the remote server S_j
$h(\cdot)$	Secure one-way hash function (e.g., SHA-1 [1])
$A\|\|B$	Data A concatenates with data B
$A \oplus B$	XOR operation of A and B

The different phases of Sonwanshi et al.'s scheme are described in the following subsections.

2.1 Registration Phase

In this phase, the user U_i needs to register with the remote server S_j providing his/her own identity ID_i and hashed password $h(PW_i)$ via a secure channel. This phase has the following steps:

Step R1. U_i first selects ID_i and PW_i. U_i then sends the registration request message $\langle ID_i, h(PW_i)\rangle$ to S_j via a secure channel.

Step R2. After receiving the message in Step R1, S_j computes $A_i = h(X||ID_i)$ and $B_i = A_i \oplus h(ID_i||h(PW_i))$, and issues a smart card containing the information $(A_i, B_i, h(\cdot))$ and sends the smart card to U_i via a secure channel.

2.2 Login Phase

If the user U_i wants to access services from the remote server S_j, U_i needs to perform the following steps:

Step L1. U_i inserts his/her smart card into a card reader of the specific terminal and inputs his/her identity ID_i^* and password PW_i^*.

Step L2. The smart card then computes $B_i^* = A_i \oplus h(ID_i^*||h(PW_i^*))$ using the stored value of A_i in its memory, and then verifies the condition $B_i^* = B_i$. If they do not match, it means that U_i enters his/her ID_i and PW_i incorrectly and this phase terminates immediately. Otherwise, the smart card executes Step L3.

Step L3. The smart card uses the current system timestamp T_u to compute $CID = h(PW_i^*) \oplus h(A_i||T_u)$ and $E_i = h(B_i||CID||T_u)$, and sends the login request message $\langle ID_i, CID, E_i, T_u\rangle$ to S_j via a public channel.

2.3 Authentication Phase

In this phase, S_j authenticates U_i. For this purpose, after receiving the login request message $\langle ID_i, CID, E_i, T_u\rangle$ from U_i, S_j executes the following steps:

Step A1. S_j verifies the format of the message and ID_i. S_j then checks the validity of the timestamp by $|T_u - T_u'| < \triangle T$, where T_u' is the current system timestamp of S_j and $\triangle T$ is the expected transmission delay. If these conditions are valid, S_j computes $A_i^* = h(X||ID_i)$ using its secret key X, $h(PW_i^*) = CID \oplus h(A_i^*||T_u)$, and $B_i^* = A_i^* \oplus h(ID_i||h(PW_i^*))$. S_j then computes $E_i^* = h(B_i^*||CID||T_u)$ and checks whether $E_i^* = E_i$. If it does not hold, S_j rejects the user U_i as an illegal user and the phase terminates immediately. Otherwise, S_j goes to execute Step A2.

Step A2. S_j computes $F_i = h(A_i^*||B_i^*||T_s)$, where T_s is the current system timestamp of the remote server S_j. S_j sends the acknowledgment message $\langle F_i, T_s\rangle$ to the user U_i via a public channel.

Step A3. After receiving the acknowledgment message in Step A2, U_i checks the validity of the timestamp by $|T_s - T_s'| < \triangle T$, where T_s' is the current system timestamp of U_i and $\triangle T$ is the expected transmission delay. If this is valid, U_i further computes $F_i^* = h(A_i||B_i||T_s)$ and checks whether $F_i^* = F_i$. If it holds, U_i computes a secret session key shared with S_j as $SK_{U_i,S_j} = h(A_i||T_u||T_s||B_i)$. Similarly, S_j also computes the same secret session key shared with U_i as $SK_{U_i,S_j} = h(A_i^*||T_u||T_s||B_i^*)$ for their future secure communications.

The registration, login and authentication phases of Sonwanshi et al.'s scheme are summarized in Table 2.

Table 2. Summary of message exchanges during the registration phase, the login phase and the authentication phase of Sonwanshi et al.'s scheme [9]

User (U_i)	Remote server (S_j)
Registration phase	
$\langle ID_i, h(PW_i) \rangle \xrightarrow{\quad}$	
	$\xleftarrow{\quad} \langle Smart\,Card(A_i, B_i, h(\cdot)) \rangle$
Login phase	
$\langle ID_i, CID, E_i, T_u \rangle \xrightarrow{\quad}$	
Authentication phase	
	$\xleftarrow{\quad} \langle F_i, T_s \rangle$

2.4 Password Change Phase

For security reasons, it is expected that the user U_i needs to change his/her password at any time locally without contacting the remote server S_j. This phase consists of the following steps:

Step P1. U_i inserts his/her smart card into a card reader of the specific terminal and inputs identity ID_i and old password PW_i^{old}. The smart card then computes $B_i^* = A_i \oplus h(ID_i||h(PW_i^{old}))$, and verifies the condition $B_i^* = B_i$. If the condition does not hold, this phase terminates immediately.

Step P2. The user U_i is asked to input his/her chosen new changed password PW_i^{new}. The smart card then computes $B_i^{**} = A_i \oplus h(ID_i||h(PW_i^{new}))$. Finally, the smart card updates B_i with B_i^{**} in its memory.

3 Cryptanalysis on Sonwanshi et al.'s Scheme

In this section, we show that Sonwanshi et al.'s scheme is insecure against different attacks, which are given in the following subsections.

3.1 Offline Password Guessing Attack

As in [9], we also assume that if an adversary (attacker) gets the user U_i's smart card, the attacker can retrieve all sensitive information stored in the smart card's memory by monitoring the power consumption of the smart card [5], [8]. Thus, the attacker knows the values A_i and B_i. By eavesdropping the login request message $\langle ID_i, CID, E_i, T_u \rangle$ during the login phase, the attacker also knows ID_i containing in the message, since the message is sent via a public channel.

Note that $A_i = h(X||ID_i)$ and $B_i = A_i \oplus h(ID_i||h(PW_i))$. X is a secret number kept to the server S_j only and it is usually a 1024-bit number. So, deriving X from A_i is a computationally infeasible problem for the attacker due to the one-way collision resistant property of the hash function $h(\cdot)$. However, knowing A_i, B_i, and ID_i, the adversary executes an offline password guessing attack and then derives the user U_i's password PW_i iterating on all possible choices of PW_i. Our attack has the following steps:

Step 1. The adversary computes $h(ID_i||h(PW_i)) = A_i \oplus B_i$.
Step 2. The adversary selects a guessed password PW_i'.
Step 3. Knowing ID_i from the login request message $\langle ID_i, CID, E_i, T_u \rangle$, the adversary computes the hash value $h(ID_i||h(PW_i'))$.
Step 4. The adversary compares the computed hash value $h(ID_i||h(PW_i'))$ with the derived hash value $h(ID_i||h(PW_i)) = A_i \oplus B_i$.
Step 5. If there is a match in Step 4, it indicates that the correct guess of the user U_i's password PW_i. Otherwise, the adversary repeats from Step 2.

As a result, the adversary can succeed to guess the low-entropy password PW_i of the user U_i. The detailed steps of the offline password guessing attack of Sonwanshi et al.'s scheme are illustrated in Table 3.

3.2 Stolen Smart Card Attack

Suppose the user U_i's smart card is lost/stolen by an attacker. The attacker can then extract the information $(A_i, B_i, h(\cdot))$ from the memory of the smart card using the power analysis attacks [5], [8], where $A_i = h(X||ID_i)$ and $B_i = A_i \oplus h(ID_i||h(PW_i))$. Again the attacker knows the identity ID_i of the user U_i from the login request message eavesdropped by that attacker. The attacker can derive the hash value $h(ID_i||h(PW_i)) = A_i \oplus B_i$ using the extracted A_i and B_i. Using the offline password guessing attack as stated in Section 3.1, the attacker can retrieve the password PW_i of the user U_i. As a result, once the attacker knows ID_i and PW_i of the user U_i, the attacker can use this smart card in order to successfully login to the remote server S_j. Hence, Sonwanshi et al.'s scheme fails to protect stolen smart card attack.

3.3 Fails to Protect Strong Replay Attack

Suppose an adversary intercepts the login request message $\langle ID_i, CID, E_i, T_u \rangle$ during the login phase, and replays the same message to the remote server S_j

Table 3. Summary of offline password guessing attack on Sonwanshi et al.'s scheme [9]

User (U_i)	Attacker	Remote server (S_j)
	1. Obtain U_i's smart card and gets the information (A_i, B_i).	
2. $\langle ID_i, CID, E_i, T_u \rangle \longrightarrow$		
	3. Eavesdrops the login request message in Step 2 and stores ID_i of U_i.	
	4. Knowing A_i and B_i, computes $h(ID_i \| h(PW_i)) = A_i \oplus B_i$.	
	5. Guesses a password PW_i'.	
	6. Computes $h(ID_i \| h(PW_i'))$ using ID_i from Step 3.	
	7. Compares $h(ID_i \| h(PW_i'))$ with $h(ID_i \| h(PW_i))$. If there is a match, PW_i is derived. Otherwise, the attacker executes from Step 5 to guess another password.	

within a valid time interval. Then S_j treats this message as a valid message, because the condition $|T_u - T_u'| < \triangle T$ will be satisfied, where T_u' is the current system timestamp of S_j and $\triangle T$ is the expected transmission delay.

Similarly, the attacker can intercept the message $\langle F_i, T_s \rangle$ during the authentication phase and replay the same message within a valid time interval. In this case, S_j also treats this message as valid as the condition $|T_s - T_s'| < \triangle T$ will be satisfied, where T_s' is the current system timestamp of U_i and $\triangle T$ is the expected transmission delay. Of course, this attack depends on the expected time interval $\triangle T$. If this interval is very short, then the attacker could not succeed. Thus, this attack is weak.

To overcome such weakness, one can adopt the similar strategy as suggested in [2], where instead of using timestamp one can use random nonce for this purpose.

4 Conclusion and Future Works

Recently Sonwanshi et al. proposed an efficient smart card based remote user authentication using the one-way hash function and bitwise XOR operation. Though their scheme is efficient in computation, in this paper we have shown that their scheme is still vulnerable to offline password guessing attack and stolen smart card attack. Further, their scheme fails to protect strong replay attack. In future work, we aim to propose an improved scheme which needs to be secure and efficient. We also encourage the readers to come up with their proposed improvements in order to remedy these weaknesses found in Sonwanshi et al.'s scheme.

Acknowledgements. The authors would like to acknowledge the anonymous reviewers for their helpful comments and suggestions.

References

1. Secure Hash Standard, FIPS PUB 180-1, National Institute of Standards and Technology (NIST), U.S. Department of Commerce (April 1995)
2. Das, A.K.: Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards. IET Information Security 5(3), 145–151 (2011)
3. Das, A.K.: Cryptanalysis and further improvement of a biometric-based remote user authentication scheme using smart cards. International Journal of Network Security & Its Applications 3(2), 13–28 (2011)
4. Hwang, M.S., Li, L.H.: A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics 46(1), 28–30 (2000)
5. Kocher, P.C., Jaffe, J., Jun, B.: Differential power analysis. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 388–397. Springer, Heidelberg (1999)
6. Li, C.T., Hwang, M.S.: An efficient biometric-based remote authentication scheme using smart cards. Journal of Network and Computer Applications 33, 1–5 (2010)
7. Li, C.-T., Lee, C.-C., Liu, C.-J., Lee, C.-W.: A Robust Remote User Authentication Scheme against Smart Card Security Breach. In: Li, Y. (ed.) DBSec. LNCS, vol. 6818, pp. 231–238. Springer, Heidelberg (2011)
8. Messerges, T.S., Dabbish, E.A., Sloan, R.H.: Examining smart-card security under the threat of power analysis attacks. IEEE Transactions on Computers 51(5), 541–552 (2002)
9. Sonwanshi, S.S., Ahirwal, R.R., Jain, Y.K.: An Efficient Smart Card based Remote User Authentication Scheme using hash function. In: Proceedings of IEEE SCEECS 2012, pp. 1–4 (March 2012)