Enhanced Advanced Smart Card based Password Authentication Scheme

Ravi Singh Pippal
Vedica Institute of Technology, RKDF University, Bhopal
ravesingh@gmail.com

Abstract
In 2010, Ronggong Song proposed a smart card based authentication scheme. Its security depends on the one-way hash function as well as symmetric key cryptosystem. Author claimed that the scheme is secure against replay attack, impersonation attack, modification attack and parallel session attack. Further, it provides mutual authentication between user and server and generates session key. In this paper, we point out that Song's scheme is vulnerable to Denial-of-Service attack. In addition, server interaction is needed even during password change which is also susceptible to Denial-of-Service attack. Besides, modified scheme is proposed to overcome these security pitfalls.

Keywords: Authentication, Denial-of-Service attack, Encryption, Smart card.

1. Introduction

Since last few years, electronic transactions carried out over the Internet are gaining popularity and are widely accepted in the world. To keep data secure during its transmission over insecure network, sufficient security measures are needed. One of the key factors in security is authentication which is required for every transaction. It is the basic necessity prior to the user accesses the server. A lot of work has been done to secure the information from invalid users [1, 2]. One among various authentication schemes is password based authentication scheme. In conventional password based authentication schemes, server keeps verification table securely to verify the legitimacy of a user. Every user has its own credentials, identifier (ID) and password (PW). Whenever a user desires to access resources from a server, he/she has to present ID and PW to pass the authentication phase. The server verifies the PW corresponding to the ID from verification table and authenticates the user if the submitted password matches with the stored password.

However, this method is insecure since an attacker may access the contents of the verification table to break down the entire system. Storing the password in hashed format is one of the solutions [3]. The major drawback in this approach is size of the verification table which is directly proportional to the number of users, as a result security risk on the server is also increase. To resist possible attacks on the verification tables, smart card based password authentication scheme has been proposed. In smart card based password authentication scheme, server maintains only long term secret key/s without any

verification table. Since last decade number of smart card authentication schemes have been proposed [4-18]. In 2010, Ronggong Song proposed a smart card authentication scheme [18]. Its security depends on one-way hash function and symmetric key cryptosystem. Author claimed that the scheme provides mutual authentication between user and server and generates a session key. In addition, it is secure against replay attack, impersonation attack, modification attack and parallel session attack. However, this paper demonstrates the weakness of Song's scheme such as Denial-of-Service attack and insider attack. Every password change phase involves server interaction which is also vulnerable to Denial-of-Service attack. To resist these weaknesses, this paper proposes an enhancement of Ronggong Song's scheme.

The rest of the paper is organized as follows. A review of Ronggong Song's scheme is described in section 2. Security flaws of Song's scheme are illustrated in Section 3. Section 4 shows modified scheme and its security analysis explained in section 5. Finally, section 6 concludes the paper.

2. Review of Ronggong Song's Scheme

The scheme has five phases: Initial phase, Registration phase, Login phase, Authentication phase and Password change phase (as shown in fig. 1). The notations used in this article are defined as follows.

$h(\bullet)$	:	Secure one way hash function
x	:	Server secret key
ID_A	:	User identity
PW_A	:	Password of the user
$\oplus$	:	Exclusive OR operation
T_A	:	Date and Time at which user login request is created (User Time stamp)
T_S	:	Date and Time at which server reply message is created (Server Time stamp)
R_A	:	Random number
$E_{(x)}$	:	Encryption using symmetric key x
$D_{(x)}$	:	Decryption using symmetric key x
p, q	:	Prime numbers
$\|$	:	Concatenation
----→	:	Secure channel
⟶	:	Insecure channel

2.1 Initial Phase

Server selects two prime large prime numbers p and q such that $p = 2q + 1$, and chooses its secret key x in Z_q, a one-way hash function $h(\bullet)$ and a symmetric key cryptography algorithm with encryption $E(\bullet)$ and decryption $D(\bullet)$ operations. The server keeps both p and x secret.

2.2 Registration Phase

User U_A submits identity ID_A and password PW_A to the server. Upon receiving the registration request, server computes $B_A = h(ID_A^x \bmod p) \oplus h(PW_A)$ and issues a smart card to user U_A by storing (ID_A, B_A, $h(\bullet)$, $E(\bullet)$) into smart card memory.

2.3 Login Phase

User U_A inserts the smart card to the card reader and keys in ID_A and PW_A. The card reader generates a random number R_A, gets the current timestamp T_A of the system and computes $K_A = B_A \oplus h(PW_A)$, $W_A = E_{KA}(R_A \oplus T_A)$ and $C_A = h(T_A \| R_A \| W_A \| ID_A)$, where E_{KA} is the symmetric key encryption operation with the key K_A. Smart card sends the login request (ID_A, C_A, W_A, T_A) to the server.

2.4 Authentication Phase

Upon receiving the login request, server first checks the validity of ID_A and T_A to accept/reject the login request. If it is incorrect, the request is rejected else it consider for next step of check. The server computes $K_A = h(ID_A^x \bmod p)$, $R'_A = D_{KA}(W_A) \oplus T_A$ and checks whether C_A equals to $h(T_A \| R'_A \| W_A \| ID_A)$, where D_{KA} is the symmetric key decryption operation with the key K_A. If it is true then the user is authenticated and the server sends the message (ID_A, C_S, T_S) to the user, where $C_S = h(ID_A \| R'_A \| T_S)$ computed by the server and T_S is the server's current system time. Upon receiving the message, the smart card validates ID_A, T_S and checks whether C_S equals to $h(ID_A \| R_A \| T_S)$. If they are equal, server is authenticated. Both the user and server compute a common shared secret session key $sk = h(ID_A \| T_S \| T_A \| R_A) = h(ID_A \| T_S \| T_A \| R'_A)$.

2.5 Password Change Phase

Whenever a user wants to update his/her password, he/she has to present the credentials along with smart card infront of card reader and go through the above authentication procedure. First, the server authenticates the user with the old password PW_A. After getting the successful authentication affirmation from the server, the smart card asks the user to input the new password PW_A' and replaces the old B_A with the new $B_A' = B_A \oplus PW_A \oplus PW_A'$.

3. Security Flaws in Ronggong Song's Scheme

This section demonstrates that Ronggong Song's scheme is vulnerable to Denial-of Service attack and insider attack. Besides, it involves server during every password change phase which is susceptible to Denial-of-Service attack. Detailed description of these weaknesses is as follows:

User U_A		Server S
	Initial Phase	
		Select p, q, x Keep p, x secretly
	Registration Phase	
Select ID_A and PW_A	(ID_A, PW_A) Smart Card	$B_A = h(ID_A^x \bmod p) \oplus h(PW_A)$ Store $(ID_A, B_A, h(\cdot), E(\cdot))$ into smart card
	Login and Authentication Phase	
Input ID_A and PW_A Select R_A $K_A = B_A \oplus h(PW_A)$ $W_A = E_{KA}(R_A \oplus T_A)$ $C_A = h(T_A \Vert R_A \Vert W_A \Vert ID_A)$	(ID_A, C_A, W_A, T_A) →	Verify ID_A and T_A $K_A = h(ID_A^x \bmod p)$ $R'_A = D_{KA}(W_A) \oplus T_A$ $C'_A = h(T_A \Vert R'_A \Vert W_A \Vert ID_A)$ Verify $C'_A = C_A$ $C_S = h(ID_A \Vert R'_A \Vert T_S)$
Verify ID_A and T_S $C'_S = h(ID_A \Vert R_A \Vert T_S)$ Verify $C'_S = C_S$	← (ID_A, C_S, T_S)	
	Compute Common Secret Key	
$sk = h(ID_A \Vert T_S \Vert T_A \Vert R_A)$		$sk = h(ID_A \Vert T_S \Vert T_A \Vert R'_A)$

Fig. 1. Ronggong Song's scheme

3.1 Denial-of-Service Attack

To check whether the requested user is a legitimate bearer of smart card or not, entered password and identifier must be verified at the smart card level prior to login request creation [9]. In Ronggong Song's scheme, genuine user is able to create invalid login request by entering wrong password which will be detected only at the server side not at the user side. The same process can be repeated continuously to overload the server which restrains the server accessibility for the valid users. Nonexistence of early wrong password and wrong identifier detection leads to Denial-of-Service attack. Thus, Song's scheme shows inadequacy to resist Denial-of-Service attack. This attack can withstand at the smart card level itself by verifying the entered ID and PW prior to compute the login request.

3.2 Insider Attack

Any insider of system can obtain user's password during the registration phase and then purposely leaks the secret information or impersonate the legitimate user to access other servers [11]. In this scheme, PW_A is sent to server during the registration phase. So, any insider of server can easily get U_A's password and use it for some personal benefit.

3.3 Inappropriate Password Change Phase

In this scheme, server verifies the user authenticity before update the new password with the current password. Each time when user wants to change the password, entire process, same as login and authentication phases, is repeated which is inappropriate. Further, nonexistence of early wrong password detection leads to Denial-of-Service attack during password change phase [9]. Remedy to resist these weaknesses is that user can change the password securely by proving authenticity at the smart card level itself without taking any assistance from the server. To eliminate these drawbacks, modified smart card authentication scheme is proposed.

4. Proposed Modified Smart Card Authentication Scheme

In this section, we propose an enhancement to Ronggong Song's scheme (as shown in fig. 2). Enhanced scheme is the modified form of Ronggong Song's Scheme. It withstands all the security flaws described in the previous section. It consists of five phases out of which Initial phase and Authentication phase are same as Song's scheme. The rest of three modified phases are as follows.

4.1 Registration Phase

User U_A selects a random number 'b', computes $h(b \oplus PW_A)$ and submits $(ID_A, h(b \oplus PW_A))$ to the server. Upon receiving the registration request, server computes $B_A = h(ID_A^x \bmod p) \oplus h(b \oplus PW_A)$, $Z_A = h(h(ID_A^x \bmod p))$ and issues a smart card to user U_A by storing $(ID_A, B_A, Z_A, h(\bullet), E(\bullet))$ into smart card memory.

4.2 Login Phase

User U_A inserts the smart card to the card reader and keys in ID_A and PW_A'. The card reader computes $Z_A' = h(B_A \oplus h(b \oplus PW_A')) = h(h(ID_A^x \bmod p))$ and checks whether the computed Z_A' equals the stored Z_A or not. If true, the requested user is the correct bearer of the smart card otherwise rejects the login request. The reader generates a random number R_A, gets the current timestamp T_A of the system and computes $K_A = B_A \oplus h(PW_A)$, $W_A = E_{KA}(R_A \oplus T_A)$ and $C_A = h(T_A \| R_A \| W_A \| ID_A)$, where E_{KA} is the symmetric key encryption operation with the key K_A. Smart card sends the login request (ID_A, C_A, W_A, T_A) to the server.

4.3 Password Change Phase

This phase is invoked whenever user wants to change the present password PW_A with a new password PW_A^{new}. User U_A inserts the smart card to the card reader and then inputs ID_A and PW_A'. The smart card computes $Z_A' = h(B_A \oplus h(b \oplus PW_A')) = h(h(ID_A^x \bmod p))$ and checks whether the computed Z_A' equals the stored Z_A or not. If they are equal, the requested user is the legitimate holder of the smart

card and then asks the user to input the new password PW_A^{new} to replace the old B_A with the new $B_A^{new} = B_A \oplus h(b \oplus PW_A) \oplus h(b \oplus PW_A^{new})$. Smart card rejects the password change request if Z_A' and Z_A are not equal. To resist online password guessing attack, the reader locks the card if U_A enters wrong password more than limited number of times.

User U_A		**Server S**
	Initial Phase	
		Select p, q, x Keep p, x secretly
	Registration Phase	
Select ID_A, PW_A and b Compute $h(b \oplus PW_A)$	$(ID_A, h(b \oplus PW_A))$ ⇢	$B_A = h(ID_A^x \bmod p) \oplus h(b \oplus PW_A)$ $Z_A = h(h(ID_A^x \bmod p))$
	⇠ Smart Card	Store $(ID_A, B_A, Z_A, h(\bullet), E(\bullet))$ into smart card
	Login and Authentication Phase	
Input ID_A and PW_A' Compute $Z_A' = h(B_A \oplus h(b \oplus PW_A')) = h(h(ID_A^x \bmod p))$ Check whether $Z_A' = Z_A$ or not Select R_A $K_A = B_A \oplus h(PW_A)$ $W_A = E_{KA}(R_A \oplus T_A)$ $C_A = h(T_A \| R_A \| W_A \| ID_A)$	(ID_A, C_A, W_A, T_A) →	Verify ID_A and T_A $K_A = h(ID_A^x \bmod p)$ $R'_A = D_{KA}(W_A) \oplus T_A$ $C'_A = h(T_A \| R'_A \| W_A \| ID_A)$ Verify $C'_A = C_A$ $C_S = h(ID_A \| R'_A \| T_S)$
Verify ID_A and T_S $C'_S = h(ID_A \| R_A \| T_S)$ Verify $C'_S = C_S$	⇠ (ID_A, C_S, T_S)	
	Compute Common Secret Key	
$sk = h(ID_A \| T_S \| T_A \| R_A)$		$sk = h(ID_A \| T_S \| T_A \| R'_A)$

Fig. 2. Proposed modified scheme

5. Security Analysis

Enhanced scheme is a modified version of Ronggong Song's scheme. It inherits all the merits of Ronggong Song's scheme. Hence, this section discusses only the enhanced security features of the proposed scheme.

5.1 Insider Attack

In real world, many users use same passwords to access different servers for their handiness of remembering long passwords and use them easily. However, a privileged insider of server can get this

password and then try to impersonate a legal user by accessing other servers. In our scheme, $h(b \oplus PW_A)$ is sent to server instead of PW_A to resist insider attack. So, there is no chance to obtain U_A's password. Hence, our scheme is free from insider attack.

5.2 Early Wrong Password Detection

Card holder verification at the user side during login phase is very imperative to resist to Denial-of-Service attack. This scheme verifies the entered password and identifier at the user side prior to login request creation by comparing Z_A' with the stored Z_A. If the smart card finds either entered password or identifier wrong, immediately it will ask the user to enter correct password as well as correct identifier. It creates a login request only when smart card finds correct entered password as well as identifier. Further, it is not possible to guess identity and password correctly at the same time even after getting the smart card of a user. As a result, Denial-of-Service attack is completely eliminated.

5.3 Efficient Password Change Phase

In the proposed scheme, user can change the password at the card level itself without taking any assistance from the server. The smart card compares the computed Z_A' with the stored Z_A to verify the legitimacy of the user before update the new password. If it finds Z_A' and Z_A equal, then smart card asks the user to enter new password PW_A^{new} to replace present current PW_A with new password PW_A^{new}. It eliminates the role of server during password change phase as a result no Denial-of-Service attack and reduction of unnecessary burden on the server.

5.4 Performance

Proposed scheme is compared with Ronggong Song's scheme in order to measure the security in terms of possible attacks. From Table 1, we can see that our scheme is more secure and efficient as compare to Song's scheme. It includes early wrong password and wrong identifier detection which resists Denial-of-Service attack either during login phase or password change phase.

6. Conclusion

In this paper, we have shown that Ronggong Song's scheme is vulnerable to Denial-of-Service attack and insider attack. Further, server is involved during password change phase which is also susceptible to Denial-of-Service attack. To overcome these security flaws, this paper proposed an enhanced scheme over Ronggong Song's scheme. Our scheme resists Denial-of-Service attack as well as insider attack. In addition, user can change the password securely by proving the authenticity at the smart card level itself without involvement of server.

Table 1. Comparison between proposed scheme and Ronggong Song's scheme

Security Properties	Proposed Scheme	Ronggong Song's Scheme
User is allowed to choose and change the password	Yes	Yes
Provides mutual authentication	Yes	Yes
Provides secure session key generation	Yes	Yes
Resists replay attack	Yes	Yes
Resists impersonation attack	Yes	Yes
Resists guessing attack	Yes	Yes
Resists parallel session attack	Yes	Yes
Resists reflection attack	Yes	Yes
Free from verification table	Yes	Yes
Resists insider attack	Yes	No
Resists Denial-of-Service attack	Yes	No
Free from server involvement during password change	Yes	No
Provides early wrong password detection	Yes	No
Provides early wrong identifier detection	Yes	No

Acknowledgment

The author would like to thank Vedica Institute of Technology, RKDF University, Bhopal, India for providing the academic support.

References

[1] R. M. Needham, M. D. Schroeder, Using encryption for authentication in large networks of computers, Communications of the ACM 21 (12) (1978) 993-999.

[2] K. S. Booth, Authentication of signatures using public key encryption, Communications of the ACM 24 (11) (1981) 772-774.

[3] L. Lamport, Password authentication with insecure communication, Communications of the ACM 24 (11) (1981) 770-772.

[4] W. H. Yang, S. P. Shieh, Password authentication schemes with smart cards, Computers & Security 18 (8) (1999) 727-733.

[5] T. C. Wu, Remote login authentication scheme based on a geometric approach, Computer Communications 18 (12) (1995) 959-963.

[6] M. S. Hwang, L. H. Li, A new remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (1) (2000) 28-30.

[7] H. M. Sun, An efficient remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 46 (4) (2000) 958-961.

[8] M. S. Hwang, C. C. Lee, Y. L. Tang, A simple remote user authentication scheme, Mathematical and Computer Modelling 36 (1-2) (2002) 103-107.

[9] E. J. Yoon, E. K. Ryu, K. Y. Yoo, An improvement of Hwang-Lee-Tang's simple remote user authentication scheme, Computers & Security 24 (1) 50-56.

[10] H. Y. Chien, J. K. Jan, Y. M. Tseng, An efficient and practical solution to remote authentication: smart card, Computers & Security 21 (4) (2002) 372-375.

[11] W. C. Ku, S. M. Chen, Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 50 (1) (2004) 204-207.

[12] E. J. Yoon, E. K. Ryu, K. Y. Yoo, Further improvement of an efficient password based remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 50 (2) (2004) 612-614.

[13] X. M. Wang, W. F. Zhang, J. S. Zhang, M. K. Khan, Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards, Computer Standards and Interfaces 29 (5) (2007) 507-512.

[14] M. L. Das, A. Saxena, V. P. Gulati, A Dynamic ID-based remote user authentication scheme, IEEE Transactions on Consumer Electronics 50 (2) (2004) 629-631.

[15] I. E. Liao, C. C. Lee, M. S. Hwang, Security enhancement for a dynamic ID-based remote user authentication scheme, International Conference on Next Generation Web Services Practices (2005).

[16] Y. Y. Wang, J. Y. Liu, F. X. Xiao, J. Dan, A more efficient and secure dynamic ID-based remote user authentication scheme, Computer Communications 32 (4) (2009) 583-585.

[17] Z. Hao, N. Yu, A security enhanced remote password authentication scheme using smart card, 2nd International Symposium on Data, Privacy, and E-Commerce (ISDPE-2010) (2010) 56-60.

[18] R. Song, Advanced smart card based password authentication protocol, Computer Standards & Interfaces 32 (5-6) (2010) 321-325.