Security Vulnerabilities of User Authentication Scheme using Smart Card

Ravi Singh Pippal[1], Jaidhar C. D.[2], and Shashikala Tapaswi[1,⋆]

[1] ABV-Indian Institute of Information Technology and Management,
Gwalior-474015, INDIA,
[2] Defence Institute of Advance Technology, Girinagar,
Pune-411025, INDIA
{ravi,stapaswi}@iiitm.ac.in,jaidharcd@diat.ac.in

Abstract. With the exponential growth of Internet users, various business transactions take place over an insecure channel. To secure these transactions, authentication is the primary step that needs to be passed. To overcome the problems associated with traditional password based authentication methods, smart card authentication schemes have been widely used. However, most of these schemes are vulnerable to one or the other possible attack. Recently, Yang, Jiang and Yang proposed RSA based smart card authentication scheme. They claimed that their scheme provides security against replay attack, password guessing attack, insider attack and impersonation attack. This paper demonstrates that Yang et al.'s scheme is vulnerable to impersonation attack and fails to provide essential features to satisfy the needs of a user. Further, comparative study of existing schemes is also presented on the basis of various security features provided and vulnerabilities present in these schemes.

Keywords: Authentication; Cryptanalysis; Impersonation; Password; Smart card.

1 Introduction

Remote user authentication is used to verify the legitimacy of a remote user and it is mandatory for most of the applications like online banking, ID verification, medical services, access control and e-commerce. One among various authentication schemes is password based authentication scheme. In traditional password based authentication schemes, server keeps verification table securely to verify the legitimacy of a user. However, this method is insecure since an attacker may access the contents of the verification table to break down the entire system. Lamport [1] proposed password authentication scheme to authenticate remote users by storing the passwords in a hashed format. Nevertheless, this scheme has a security drawback as an intruder can go through the server and modify the contents of the verification table. To resist all possible attacks on the

[⋆] Corresponding author.

verification tables, smart card based password authentication scheme has been proposed. This scheme eliminates the use of verification table.

Today, authentication based on smart card is employed continuously in several applications like cloud computing, healthcare, key exchange in IPTV broadcasting, wireless networks, authentication in multi-server environment, wireless sensor networks and many more. Hence, it is necessary that the authentication scheme must be efficient as well as secure enough so that it can be utilized for practical applications.

1.1 Contribution of this Paper

Recently, Yang et al. [20] proposed an access control scheme using smart card. This paper demonstrates that Yang et al.'s scheme has following weaknesses: (i) unauthorized user can easily forge a valid login request. (ii) user is not able to choose and change the password freely. (iii) it does not provide mutual authentication, session key generation and early wrong password detection. (iv) it fails to solve time synchronization problem. Further, comparative study of existing schemes is also done on the basis of various security features provided and vulnerabilities present in these schemes.

The remainder of this paper is organized as follows. The existing literature related to smart card authentication schemes is explored in section 2. Section 3 describes a brief review of Yang et al.'s access control scheme using smart card. Security flaws of Yang et al.'s scheme along with comparison of existing schemes based on various security features and attacks are presented in section 4. Finally, section 5 concludes the paper.

2 Literature Review

Throughout the last two decades, various smart card authentication schemes have been proposed [2, 4, 6–9, 11–13, 15, 17, 20]. However, most of these schemes fail to fulfill the essential requirements of users. Hwang and Li [2] presented a remote user authentication scheme using ElGamal's cryptosystem and claimed that their scheme is free from maintaining verification table and able to resist replay attack. Chan and Cheng [3] found that Hwang-Li's scheme is vulnerable to impersonation attack. To improve efficiency, Sun [4] suggested a remote user authentication scheme using one way hash function. However, Hsu [5] proved that Sun's scheme is insecure against offline and online password guessing attacks. To handle these flaws, Chien et al. [6] proposed remote user authentication scheme using one-way hash function. Nevertheless, it exhibits parallel session attack [5]. To defend against insider attack and reflection attack over [6], Ku and Chen [7] presented an improved scheme which also provides the facility to change the password freely. But, it is found that the scheme is weak against parallel session attack and has insecure password change phase [8]. Further improvement has also been suggested by Yoon et al. [8]. However, the improved scheme remains vulnerable to guessing attack, Denial-of-Service attack and impersonation attack

[9]. To remedy these drawbacks, Wang et al. [9] proposed an enhanced scheme. Though, the scheme is weak against guessing attack, denning sacco attack and does not offer perfect forward secrecy [10].

Das et al. [11] offered a dynamic ID based remote user authentication scheme using one way hash function. They claimed that their scheme is secure against ID theft and able to withstand replay attack, forgery attack, guessing attack, insider attack and stolen verifier attack. Though, the scheme is weak against guessing attack [12] and insider attack [12, 13]. Additionally, the scheme is password independent [13] and does not provide mutual authentication [12, 13]. To beat these flaws, Wang et al. [13] suggested an improved scheme. However, Ahmed et al. [14] found that the scheme does not provide security against password guessing attack, masquerade attack and Denial-of-Service attack. An enhanced scheme has also been given to resist password guessing attack, user masquerade attack and server masquerade attack [15]. Nevertheless, the scheme is exposed to password guessing attack, server masquerade attack and lack of password backward security [16]. Song [17] proposed symmetric key cryptography based smart card authentication scheme and claimed that the scheme is able to resist the existing potential attacks. In addition, it provides mutual authentication and shared session key. However, Song's scheme fails to provide early wrong password detection [18] and perfect forward secrecy [18, 19]. Moreover, it does not resist offline password guessing attack and insider attack [19]. All the schemes discussed so far have their pros and cons. Recently, Yang, Jiang and Yang [20] proposed RSA based smart card authentication scheme. The authors claimed that their scheme has the ability to withstand existing attacks. Though, this paper proves that Yang et al.'s scheme is exposed to impersonation attack and does not provide essential features.

3 Review of Yang et al.'s scheme

This section briefly reviews Yang et al.'s access control scheme using smart card [20]. The notations used throughout this paper are summarized in Table 1. The scheme consists of four phases: Initialization phase, Registration phase, Login phase and Authentication phase. Three phases are shown in Fig. 1.

Table 1. Notations used in this paper

Symbols	Their meaning	Symbols	Their meaning
U_i	Remote user	T_A	Attacker time stamp
S	Authentication server	$\phi(N)$	Euler's totient function
U_A	Attacker	$H(\cdot)$	Collision-resistant hash function
ID_i	Identity of U_i	$\|$	Message concatination
PW_i	Password generated by S	$\dashrightarrow$	Secure channel
T_C	User time stamp	$\longrightarrow$	Insecure channel

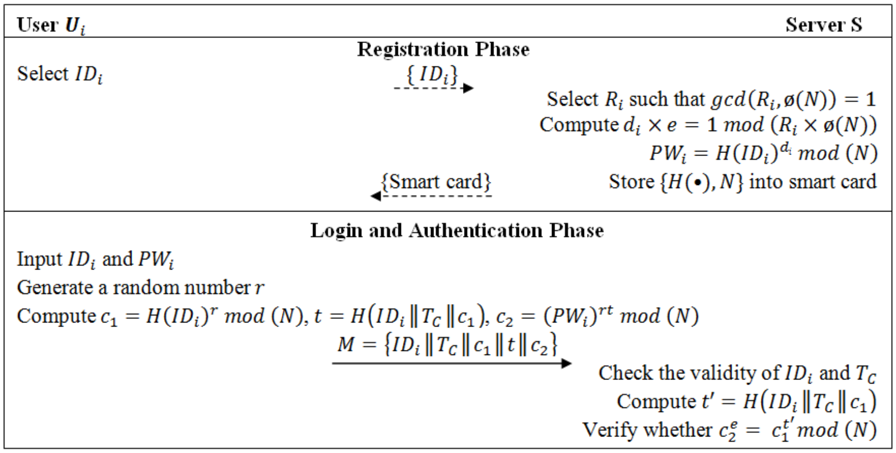
User U_i
Server S
Registration Phase
Select ID_i
$\{ID_i\}$
Select R_i such that $gcd(R_i, \phi(N)) = 1$
Compute $d_i \times e = 1\ mod\ (R_i \times \phi(N))$
$PW_i = H(ID_i)^{d_i}\ mod\ (N)$
{Smart card}
Store $\{H(\bullet), N\}$ into smart card
Login and Authentication Phase
Input ID_i and PW_i
Generate a random number r
Compute $c_1 = H(ID_i)^r\ mod\ (N)$, $t = H(ID_i \| T_C \| c_1)$, $c_2 = (PW_i)^{rt}\ mod\ (N)$
$M = \{ID_i \| T_C \| c_1 \| t \| c_2\}$
Check the validity of ID_i and T_C
Compute $t' = H(ID_i \| T_C \| c_1)$
Verify whether $c_2^e = c_1^{t'}\ mod\ (N)$

Fig. 1. Yang et al.'s scheme

3.1 Initialization Phase

In this phase, server S generates the following system parameters.

N : $N = p \times q$ such that $p = 2p_1 + 1$, $q = 2q_1 + 1$, where p, q, p_1, q_1 are all primes.

e : Secret key of the system satisfying $gcd(e, \phi(N)) = 1$.

3.2 Registration Phase

In this phase, U_i selects ID_i and submits it to S over a secure channel. Upon receiving the registration request from U_i, S selects R_i such that $gcd(R_i, \phi(N)) = 1$ and computes d_i such that $d_i \times e = 1\ mod(R_i \times \phi(N))$, U_i's password $PW_i = H(ID_i)^{d_i} mod(N)$ and delivers PW_i as well as smart card over secure channel to U_i by storing $\{H(\cdot), N\}$ into smart card memory.

3.3 Login Phase

U_i inserts the smart card to the card reader and keys in ID_i and PW_i. The card reader generates a random number r, computes $c_1 = H(ID_i)^r mod(N)$, $t = H(ID_i \parallel T_C \parallel c_1)$, $c_2 = (PW_i)^{rt} mod(N)$ and sends the login request $M = \{ID_i \parallel T_C \parallel c_1 \parallel t \parallel c_2\}$ to S.

3.4 Authentication Phase

Upon receiving the login request $M = \{ID_i \parallel T_C \parallel c_1 \parallel t \parallel c_2\}$; S first checks the validity of ID_i and T_C to accept/reject the login request. If true, S computes $t' = H(ID_i \parallel T_C \parallel c_1)$ and checks whether ${c_2}^e = {c_1}^{t'} mod(N)$ holds or not. If it holds, S accepts the login request M otherwise rejects it.

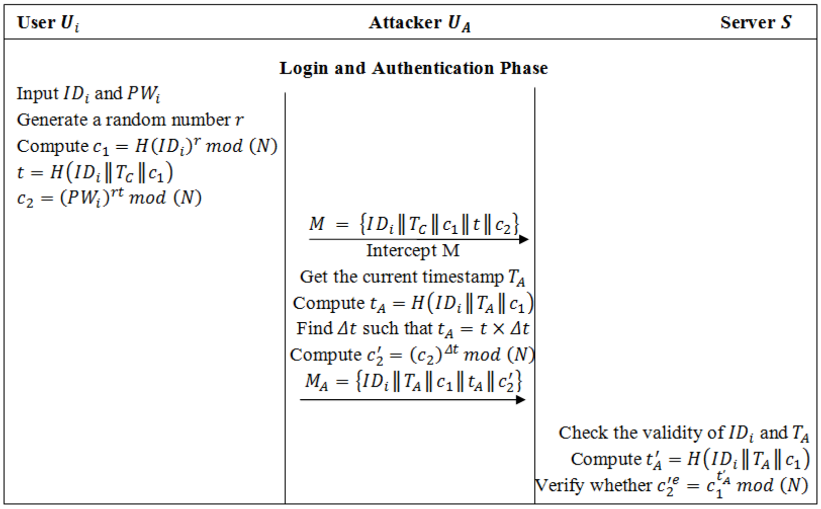
User U_i
Attacker U_A
Server S
Login and Authentication Phase
Input ID_i and PW_i
Generate a random number r
Compute $c_1 = H(ID_i)^r \ mod\ (N)$
$t = H(ID_i \| T_C \| c_1)$
$c_2 = (PW_i)^{rt} \ mod\ (N)$
$M = \{ID_i \| T_C \| c_1 \| t \| c_2\}$
Intercept M
Get the current timestamp T_A
Compute $t_A = H(ID_i \| T_A \| c_1)$
Find Δt such that $t_A = t \times \Delta t$
Compute $c_2' = (c_2)^{\Delta t} \ mod\ (N)$
$M_A = \{ID_i \| T_A \| c_1 \| t_A \| c_2'\}$
Check the validity of ID_i and T_A
Compute $t_A' = H(ID_i \| T_A \| c_1)$
Verify whether $c_2'^e = c_1^{t_A'} \ mod\ (N)$

Fig. 2. Impersonation attack on Yang et al.'s scheme

4 Weaknesses present in Yang et al.'s scheme

This section demonstrates the security flaws in Yang et al.'s scheme under the assumption that the attacker is able to intercept all the messages exchanged between U_i and S. It is found that this scheme has following weak spots: (i) vulnerable to impersonation attack, (ii) no early wrong password detection, (iii) no mutual authentication and (iv) no session key generation. In addition, this scheme fails to solve time synchronization problem and does not allow users to choose and change the password freely.

4.1 Vulnerable to impersonation attack

First, an attacker U_A intercepts the login request $\{ID_i \parallel T_C \parallel c_1 \parallel t \parallel c_2\}$ transmitted from user U_i to server S (as shown in Fig. 2). U_A gets the current timestamp T_A, computes $t_A = H(ID_i \parallel T_A \parallel c_1)$ and finds a value Δt such that $t_A = t \times \Delta t$. After getting Δt, U_A computes $c_2{}' = (c_2)^{\Delta t} mod(N) = (PW_i)^{r \times t_A} mod(N)$ and sends forged login request $M_A = \{ID_i \parallel T_A \parallel c_1 \parallel t_A \parallel c_2'\}$ to S. Once the request M_A is received, S computes $t_A' = H(ID_i \parallel T_A \parallel c_1) = t_A$ and verifies whether $c_2'^e = c_1^{t_A'} mod(N)$ or not which is obviously true. Hence, U_A is able to impersonate as legitimate user U_i.

4.2 No early wrong password detection

To prevent Denial-of-Service attack, password needs to be verified at the user side prior to login request creation. In this scheme, adversary can create invalid login request by entering wrong password which will be detected only at the server side not at the user side. Hence, it leads to Denial-of-Service attack.

4.3 No mutual authentication

It is necessary that not only server verifies the legal users, but users also need to verify the identity of the legal server to achieve two way secure communication. In this scheme, only the login request is verified at the server side to verify the legitimacy of the user. Hence, this scheme fails to provide mutual authentication. Further, session key is used to secure the entire communication between them and it must be changed from session to session. In this scheme, there is no session key generation.

In timestamp-based authentication schemes, the clock of the server and all registered user systems need to be synchronized. In addition, transmission delay of the login request needs to be limited. However, it is inefficient from the practical point of view specially for a large network where clock synchronization is hard to achieve. Yang et al.'s scheme fails to solve this problem. Moreover, users are not able to choose the password as per their convenience. They must remember the password issued by the server which causes inconvenience. Further, they are not able to change the password whenever they feel.

4.4 Performance comparison

This paper identifies the possible attacks for existing smart card authentication schemes. These include (i) impersonation attack (SA1), (ii) replay attack (SA2), (iii) password guessing attack (SA3), (iv) reflection attack (SA4), (v) parallel session attack (SA5), (vi) insider attack (SA6) and (vii) attack on password change phase (SA7). A comparison is presented in Table 2 based on the ideas given by different authors.

Further, essential security features that have to be offered by any authentication scheme is also spotted out. These features include (i) user chooses the password (SF1), (ii) user changes the password (SF2), (iii) early wrong password detection (SF3), (iv) mutual authentication (SF4), (v) session key generation (SF5) and (vi) free from time synchronization problem (SF6). A comparative

Table 2. Comparison based on various security attacks

Security Attacks	SA1	SA2	SA3	SA4	SA5	SA6	SA7
Hwang-Li [2]	Insecure[3]	Secure	Secure	NA	NA	NA	NA
H. M. Sun [4]	Secure	Secure	Insecure[5]	NA	NA	NA	NA
Chien et al. [6]	Secure	Secure	Insecure[7]	Insecure[7]	Insecure[5]	Insecure[7]	NA
Ku-Chen [7]	Insecure[9]	Secure	Insecure[9]	Secure	Insecure[8]	Secure	Insecure[8]
Yoon et al. [8]	Insecure[9]	Secure	Insecure[9]	Secure	Secure	Secure	Secure
Wang et al. [9]	Secure	Secure	Insecure[10]	Secure	Secure	Secure	Secure
Das et al. [11]	Secure	Secure	Insecure[12]	NA	NA	Insecure[12],[13]	Insecure[14]
Wang et al. [13]	Insecure[14]	Secure	Insecure[14]	Secure	Secure	NA	Insecure[14]
Hao-Yu [15]	Secure	Secure	Insecure[16]	Secure	Secure	NA	Secure
R. Song [17]	Secure	Secure	Insecure[19]	Secure	Secure	Insecure[19]	Secure
Yang et al. [20]	Insecure	Secure	Secure	NA	NA	NA	NA

[x] As per the reference [x]

Table 3. Comparison based on various security features provided

Security Features	**SF1**	**SF2**	**SF3**	**SF4**	**SF5**	**SF6**
Hwang-Li [2]	No	No	No	No	No	No
H. M. Sun [4]	No	No	No	No	No	No
Chien et al. [6]	Yes	No	No	Yes	No	No
Ku-Chen [7]	Yes	Yes	No	Yes	No	No
Yoon et al. [8]	Yes	Yes	No	Yes	No	No
Wang et al. [9]	Yes	Yes	Yes	Yes	Yes	No
Das et al. [11]	Yes	Yes	No	No	No	No
Wang et al. [13]	No	Yes	No	Yes	No	No
Hao-Yu [15]	No	Yes	No	Yes	No	No
R. Song [17]	Yes	Yes	No	Yes	Yes	No
Yang et al. [20]	No	No	No	No	No	No

study of existing schemes is given in Table 3 on the basis of these security features.

From both of these tables, it is clear that none of these schemes offer protection against identified attacks and fulfill the needs of a user.

5 Conclusion

Authentication is the imperative factor for any scheme that deals with the transmission of secret information over a public network. This paper pointed out that Yang et al.'s scheme has security flaws as an intruder can easily impersonate legal users to pass the authentication phase. Moreover, it does not allow users to choose and change the password freely which results inconvenience from the user's point of view. In addition, it does not provide mutual authentication, session key generation, early wrong password detection and fails to solve time synchronization problem. Hence, the scheme is computationally inefficient as well as insecure for practical applications.

Furthermore, performance comparison of existing smart card authentication schemes is also presented which shows that a lot of work has to be done in this field to provide secure and efficient authentication scheme. Before designing any authentication scheme, the identified security attacks must be taken into consideration along with the requirements desired by the end users.

Acknowledgments. The authors would like to thank ABV-Indian Institute of Information Technology and Management, Gwalior, India for providing the academic support.

References

1. Lamport, L.: Password authentication with insecure communication. Communications of the ACM. 24, 770-772 (1981).

2. Hwang, M.S., Li, L.H.: A new remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics. 46, 28-30 (2000).
3. Chan, C.K., Cheng, L.M.: Cryptanalysis of a remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics. 46, 992-993 (2000).
4. Sun, H.M.: An efficient remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics. 46, 958-961 (2000).
5. Hsu, C.L.: Security of two remote user authentication schemes using smart cards. IEEE Transactions on Consumer Electronics. 49, 1196-1198 (2003).
6. Chien, H.Y., Jan, J.K., Tseng, Y.M.: An efficient and practical solution to remote authentication: smart card. Computers and Security. 21, 372-375 (2002).
7. Ku, W.C., Chen, S.M.: Weaknesses and improvements of an efficient password based remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics. 50, 204-207 (2004).
8. Yoon, E.J., Ryu, E.K., Yoo, K.Y.: Further improvement of an efficient password based remote user authentication scheme using smart cards. IEEE Transactions on Consumer Electronics. 50, 612-614 (2004).
9. Wang, X.M., Zhang, W.F., Zhang, J.S., Khan, M.K.: Cryptanalysis and improvement on two efficient remote user authentication scheme using smart cards. Computer Standards and Interfaces. 29, 507-512 (2007).
10. Yoon, E.J., Lee, E.J., Yoo, K.Y.: Cryptanalysis of Wang et al.'s remote user authentication scheme using smart cards. In: 5th International Conference on Information Technology: New Generations, pp. 575-580, Las Vegas, USA (2008).
11. Das, M.L., Saxena, A., Gulati, V.P.: A dynamic ID-based remote user authentication scheme. IEEE Transactions on Consumer Electronics. 50, 629-631 (2004).
12. Liao, I.E., Lee, C.C., Hwang, M.S.: Security enhancement for a dynamic ID-based remote user authentication scheme. In: International Conference on Next Generation Web Services Practices, pp. 437-440, Seoul, Korea (2005).
13. Wang, Y.Y., Liu, J.Y., Xiao, F.X., Dan, J.: A more efficient and secure dynamic ID-based remote user authentication scheme. Computer Communications. 32, 583-585 (2009).
14. Ahmed, M.A., Lakshmi, D.R., Sattar, S.A.: Cryptanalysis of a more efficient and secure dynamic id-based remote user authentication scheme. International Journal of Network Security and its Applications. 1, 32-37 (2009).
15. Hao, Z., Yu, N.: A security enhanced remote password authentication scheme using smart card. In: 2nd International Symposium on Data, Privacy and E-Commerce, pp. 56-60, Buffalo, USA (2010).
16. Zhang, H., Li, M.: Security vulnerabilities of an remote password authentication scheme with smart card. In: 2011 International Conference on Consumer Electronics, Communications and Networks, pp. 698-701, XianNing, China (2011).
17. Song, R.: Advanced smart card based password authentication protocol. Computer Standards and Interfaces. 32, 321-325 (2010).
18. Pippal, R.S., Jaidhar, C.D., Tapaswi, S.: Comments on symmetric key encryption based smart card authentication scheme. In: 2nd International Conference on Computer Technology and Development, pp. 482-484, Cairo, Egypt (2010).
19. Horng, W.B., Lee, C.P., Peng, J.W.: Security weaknesses of Song's advanced smart card based password authentication protocol. In: 2010 IEEE International Conference on Progress in Informatics and Computing, pp. 477-480, Shanghai, China (2010).
20. Yang, C., Jiang, Z., Yang, J.: Novel access control scheme with user authentication using smart cards. In: 3rd International Joint Conference on Computational Science and Optimization, pp. 387-389, Huangshan, China (2010).