Security Weaknesses of Li's Remote User Password Authentication Scheme Using Smart Card

Jie LING[a], Guang-Qiang ZHAO [b*], Yi LIU [c]

Faculty of Computer, Guangdong University of Technology, Guangzhou, 510006, China

[a]jling@gdut.edu.cn, [b]gqzh88@126.com, [c] yiliu@gdut.edu.cn

*Corresponding author: Guang-Qiang ZHAO

Keywords: Smart card, Impersonation attack, Anonymity, Clock synchronization.

Abstract. User authentication is an important technology to guarantee that only the legal users can access resources from the remote server. The advantages of smart cards are storage and computation abilities. Recently, Li et al. pointed out the security problems of Chen et al's password authentication scheme and they proposed an enhanced smart card based remote user password authentication scheme and claimed it is secure, However, We find that Li scheme is still vulnerable. It cannot resist user impersonation attack and insider attack. Besides, it also suffers from user anonymity violation and clock synchronization problem.

Introduction

In 2000, Hwang-Li introduced the concept of smart card in password based on user authentication systems. Since then a considerable amount of research [1-10] has been carried out in this field. In 2009, Hsiang and Shih [1] showed that Liao-Wang [2] scheme cannot resist insider attack, masquerade attack, and server spoofing attack, meanwhile, the scheme cannot achieve mutual authentication. And they proposed an enhanced scheme on Liao-Wang scheme, However, Sood et al.[3] pointed out that Hsiang et al.'s scheme is still insecure; it fails to resist replay attack, impersonation attack and stolen smart attack. And they proposed a secure dynamic identity based authentication scheme. Unfortunately, Xiong Li et al.[4] found that Sood et al's scheme still suffers from some attacks such as leak-of-verifier attack, stolen smart card attack and impersonation attack. Chen et al [5] proposed a robust smart-card based remote user password authentication scheme. Unfortunately, Saru et al [6] pointed out that Chen's scheme fails to resist impersonation attacks and insider attack and does not provide important features such as user anonymity, confidentiality to air messages. Later, Li et al [7] also showed that Chen et al.'s scheme cannot ensure forward secrecy and the password change phase of the scheme is unfriendly and inefficient when the users update their passwords, in order to eliminate these problems, they proposed a modified smart card based user authentication scheme and claim it is more secure. In 2012, He et al[8] proposed an efficient ID-based scheme for mobile client-server environment on ECC without the MapToPoint function. The scheme attempts to cope with many of the well know security and efficiency problems of previous schemes. Despite of its claim of provable security, unfortunately, in 2013, Ding Wang et al.[9] pointed out that He et al.'s scheme cannot resist a reflection attack and also a parallel attack; it suffers from clock synchronization problem and user anonymity violation. And they proposed an enhanced scheme.

In this paper, we showed that Xie's scheme is in fact still insecure in the face of an active attacker. We demonstrated it by presenting stolen smart card attack and impersonation attack that breach the essential goal of mutual authentication. Besides, we pointed out that it also suffers from user anonymity violation and clock synchronization problem and cannot detect the wrong password quickly.

Review of Li's Scheme

Before the review, we first notify the whole notations that will be used throughout the paper. The notations we used in this paper.

U_i: the ith user
SC: the smart card
S: the authentication server
ID_i: the user U_i*'s* identity
PWi: the user Ui*'s* password
x: the master secret key hold by server S
$\triangle T$: the maximum transmission delay
p,q: two large prime numbers that satisfy $p = 2q + 1$
Z_q: the ring of integers modulo q
Z^*_q: The multiplicative of Z_q

Li et al.'s scheme consists of Registration phase, Login phase, Authentication phase and Password change phase. The details scheme performs as follows, and it is also shown in Figure I.

Registration phase

Step1. U_i chooses his identity ID_i and password PW_i and submits them to S via a secure channel.

Step2. S computes security parameters A_i= h ($ID_i||PW_i$) ^{PWi} mod p, B_i = h (ID_i) $^{(x+PWi)}$ mod p.

Step3. S stores {A_i, B_i, h (), p, q} on a SC and issues the SC to U_i via a secure channel.

Login phase

Step1. U_i inserts SC into a card reader and inputs his identity ID_i and password PW_i.

Step2. SC computes A_i^* = h ($ID_i||PW_i$)^{PWi} mod p, and compares $A_i^*$with A_i, where A_i is stored in SC. If they are not equal, it means the user entered a wrong password and SC terminates the session. If A_i=A_i^*, SC performs the following steps.

Step3. SC chooses a random number α $\in_R Z_q^*$ and computes: $C_i = B_i$ / h (ID_i)^{PWi} mod p, D_i = h (ID_i) $^{\alpha}$mod p, M_i =h ($ID_i||C_i||D_i||T_i$), where T_i is the current time.

Step4. SC sends the login request message {ID_i, D_i, M_i, T_i} to S.

Authentication phase

Step1. S checks that the ID_i is valid and that T_i^* - $T_i \leqslant \triangle T$, where $T_i^*$is the time the login request was received. If either or both are invalid, the login request is rejected.

Step2. S computes: C_i^* = h (ID_i)$^{\mathrm{x}}$ mod p, M_i^*=h ($ID_i||C_i^*||D_\mathrm{i}||T_i$).

Step3. S compares M_i^* with received M_i. If equal, the login request is accepted and U_i is authenticated by server S; otherwise, the login request is rejected.

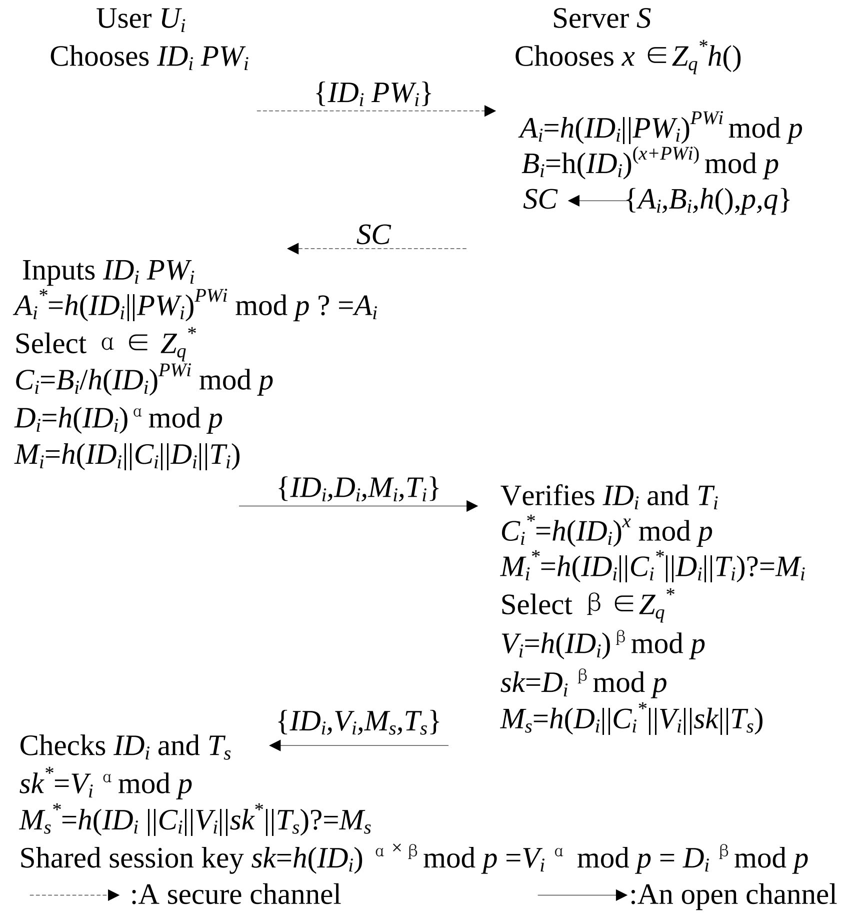
Step4. S generates a random number $\beta \in_R Z_q^*$ and computes: V_i =h (ID_i)$^{\beta}$ mod p, and the shared session key sk = D_i^{β} mod p.

Step5. S gets the current time stamp T_S, and computes M_S=h ($ID_i||C_i^*||V_i||sk||T_S$), and sends the mutual- authentication message {ID_i,V_i, M_S, T_S} to U_i.

Step6. Upon receiving the message, U_i checks ID_i and compares T_S with T_S^*, where T_S^* is the time the mutual authentication message was received. If ID_i is valid and T_S^* - $T_S \leqslant \triangle T$, U_i performs the following steps.

Step7.U_i computes: sk^*=V_i^{α} mod p, M_S^* =h ($ID_i||C_i||V_\mathrm{i}||sk^*||T_S$), And compares M_S^* with the received M_S. If they are not equal, the session is terminated. On the contrary, if M_S^* = M_S, the server S is authenticated by the user U_i.

At last, the user U_i and the server S share an agreed session key sk =h (ID_i) $^{\alpha\beta}$ mod p.



User U_i Server S

Chooses ID_i PW_i Chooses $x \in Z_q^* h()$

$\{ID_i\ PW_i\}$

$A_i=h(ID_i||PW_i)^{PWi}$ mod p

B_i=h$(ID_i)^{(x+PWi)}$ mod p

$SC \leftarrow \{A_i,B_i,h(),p,q\}$

SC

Inputs ID_i PW_i

$A_i^*=h(ID_i||PW_i)^{PWi}$ mod p ? $=A_i$

Select $\alpha \in Z_q^*$

$C_i=B_i/h(ID_i)^{PWi}$ mod p

$D_i=h(ID_i)^{\alpha}$ mod p

$M_i=h(ID_i||C_i||D_i||T_i)$

$\{ID_i,D_i,M_i,T_i\}$

Verifies ID_i and T_i

$C_i^*=h(ID_i)^x$ mod p

$M_i^*=h(ID_i||C_i^*||D_i||T_i)?=M_i$

Select $\beta \in Z_q^*$

$V_i=h(ID_i)^{\beta}$ mod p

$sk=D_i^{\ \beta}$ mod p

$M_s=h(D_i||C_i^*||V_i||sk||T_s)$

$\{ID_i,V_i,M_s,T_s\}$

Checks ID_i and T_s

$sk^*=V_i^{\ \alpha}$ mod p

$M_s^*=h(ID_i\ ||C_i||V_i||sk^*||T_s)?=M_s$

Shared session key $sk=h(ID_i)^{\ \alpha\times\beta}$ mod p $=V_i^{\ \alpha}$ mod p = $D_i^{\ \beta}$ mod p

:A secure channel :An open channel

Figure I Li et al's scheme

Password Change phase

This phase is invoked whenever U_i wants to change his password PW_i with a new password $\mathrm{PW}_{\mathrm{i}}^{\mathrm{new}}$, and it can be finished without communicating with the server S.

Step1. U_i inserts his/her smart card into a card reader and submits his/her identity ID_i, password PW_i, and requests to change the password.

Step2. SC computes A_i^* =h $(ID_i||PW_i)^{PWi}$ mod p, and compares $A_i^*$with A_i, where A_i is stored in SC. If they are not equal, SC rejects the password change request. On the contrary, if A_i^*=A_{i}, the user is asked to key a new password PWinew.

Step3. SC computes A_i^{new}=h $(ID_i||PW_i^{new})^{PWinew}$ mod p, B_i^{new} = B_i×h $(ID_i)^{PWinew}$/h$(ID_i)^{PWi}$

Step4. SC replaces A_i,B_i using A_i^{new}, B_i^{new}, respectively.

Cryptanalysis of Li's Scheme

User impersonation Attack

During login phase, U_i sends login message $\{ID_i, D_i, M_i, T_i\}$ to S, An attacker U_a can easily obtain the ID_i of U_i by intercepting any login request between U_i and S. Then in near future, U_a can impersonate U_i to cheat S as follows:

(1)U_a sends the registration request = $\{ID_i, PW_a\}$, where ID_i is the identity of U_{i} and PW_a is chosen by U_a as his password.

(2)S sends U_a the smart card contains $\{A_a,B_a,$h$(),p,q\}$,

where A_a = h$(ID_i||\ PW_a)^{\ PWa}$ mod p, B_a=h$(ID_i)^{(x+PWa)}$ mod p.

(3)U_a extracts values $\{A_a, B_a$, h (), p, $q\}$ from his/her smart card and computes C_i=B_a / h $(ID_i)^{PWa}$ mod p = h$(ID_{\mathrm{i}})^{\mathrm{X}}$ mod p.

(4) U_a chooses a random number $a^* \in_R Z_q^*$ and computes: D_a = h $(ID_i)^{\ a^*}$, M_a=h $(ID_i||C_i||D_a||T_a)$, where T_a is the current time of U_a.

(5) U_a sends the login request $\{ID_i, D_a, M_a, T_a\}$ to S

It is easy to see that, S will of course accept it as a legal user because of the reasons: i> It contains valid identity ID_i of U and the fresh timestamp T_a. ii > The equivalence $M_a^* = M_a$ holds since $M_a^* =$ h $(ID_i||C_i^*||D_a||T_a)$ where $C_i^* = C_i =$ h$(ID_i)^x$ mod p. S accept the adversary U_a and sends the response $\{ID_i, V_i, M_s, T_s\}$,upon the adversary U_a receiving the response message, just ignore it and computes the session key $sk = V_i^{a^*}$.

Not preserving user anonymity and intractability

User anonymity requires that only the server knows the identity of the user with whom he is interacting, while any third party is unable to do this. While, user intractability requires that any adversary should be prevented from linking one unknown user interacting with the server to another transcript, that is to say, the adversary is not capable of telling whether he has observed the same user twice. In Li's scheme, the user's identity *ID* is transmitted in plain-text, which may leak the identity of the logging user once the login messages were eavesdropped. That is to say, without employing any effort an adversary can distinguish and recognize the particular transactions performed by the specific user *U*. Moreover, the user's identity *ID* is static in all the login phases, which may facilitate the attacker to trace out the different login request messages belonging to the same user and to derive some information related to the user *U*. In summary, neither initiator anonymity nor initiator un-traceability can be preserved in their scheme.

The clock synchronization problem

It is well known that, remote user authentication schemes employing timestamp to provide message freshness may still suffer from replay attacks as the transmission delay is unpredictable in existing networks. Besides, clock synchronization is difficult and expensive in existing network environments, especially in wireless and mobile networks [10] and distributed networks [11]. Hence, these schemes employing the timestamp mechanism to resist replay attacks are not suitable for mobile applications [12-13]. In Li's scheme, obviously, this principle is violated.

Insider attack

Password authentication is the most important and convenient protocol for verifying users to get the system's resources. If the password of a user can be derived by the server in the registration protocol, it is called the insider attack; it is a common practice in the real world that many users use the same passwords to access different servers for their convenience without remembering different passwords for different servers. However, the security of Li's authentication scheme relies on the secrecy of his password. Moreover, disclosure of users' passwords to anyone is risky. Li et al. skip this important aspect while building the registration phase of their scheme. Users submit the registration request message $\{ID_i, PW_i\}$ consisting their plaintext passwords to S. Therefore, malicious privileged insiders at S have direct access to users' passwords PW and they can misuse them to impersonate the legal users or craft other harms.

Conclusion

In this paper we have reviewed Li's enhanced smart card based remote user password authentication scheme. The improved scheme is equipped with a claimed proof of provable security. We have shown that besides the problems of clock synchronization and user anonymity violation. It suffers from other weakness. We described how an attacker can break the security walls of the scheme by merely obtaining user's identity from intercepted login request. We have enlightened that the presence of user's plaintext identity in login request is the main reason behind various vulnerabilities such as impersonation attack; also the improved scheme cannot resist stolen smart attack. In future, we plan to come up with more viable approach for user authentication with user anonymity.

Acknowledgment

This research was financially supported by the Project of Guangzhou Science and Technology(No.2014J4100201), and the Project of Guangdong Province Science and Technology(No.2013B040401017,2014A010103029), and the Key Program of the Natural Science

Foundation of Guangdong Province(No.S2012020011071),and the Natural Science Foundation of Guangdong Province (No.2014A030313517).

References

[1] Hsiang H-C Shih W-Improvement of the secure dynamic ID based remote user authentication scheme for multi-server environment. Computer Standards &Interfaces.2009, 31(3), 1118-1123

[2] Liao Y-P, Wang S-S, A secure dynamic ID based remote user authentication scheme for mult-server environment. Computer Standards & Interfaces. 2009, 31(2).24-29

[3] Sood S-K Sarje A-K, Singh K.A secure dynamic identity based authentication protocol for multi-server architecture. Journal of Network and Computer Applications.2011, 31(2)609 -18

[4] Xiong Li Yongping Xiong Jian Ma et al. An efficient and security dynamic identity based authentication protocol for multi-server architecture using smart cards Journal of Net-work and Computer Applications.2012,35(8)763-769.

[5] B. L. Chen, W.C. Kuo. Lih-Chyau Wu. Robust smart-card based remote user password authentication scheme. International Journal of Communication Systems. Vol.27, No.2, pp.377-389, 2014.

[6] Saru Kumari, Muhammad Khurram Khan. Cryptanalysis and improvement of 'a robust smart-card-based remote user password authentication scheme'. International Journal of Communications Systems. http://onlinelibrary.wiley.com/doi/10.1002/dac.2590. In press.

[7] X. Li, J.W. Niu. Muhammad Khurram Khan,et al. An enhanced smart card based remote user password authentication scheme. Journal of Network and Computer Applications, Vol.36, No.5, pp.1365-1371, 2013.

[8] D.He.J.Chen, J.Hu, An id-based client authentication with key agreement protocol for mobile client-server environ-ment on ECC with provable security, Information Fushion .2012, 13(2) 223 -230.

[9] Ding Wang, Chun-guang Ma Cryptanalysis of a remote user authentication scheme for mobile client-server environment based on ECC. Information Fusion 2013,14(2) 498-503.

[10] A. Giridhar,P. Kumar, Distributed clock synchronization over wireless networks: algorithms and analysis, in: Pro-ceedings of the 45th IEEE conference on Decision and Control ,IEEE,2006, 4915-4920

[11] J.Han.D.Jeong, A practical implementation of IEEE 1588-2008 transparent clock for distributed measurement and control systems. IEEE Transactions on instrumentation and Measurement 2010, 59(8) 433-439.

[12] S. Islam, G,Biswas. A more efficient and secure id-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, Journal of Systems and Software .2011, 84(12)1892-1898

[13] C.Chang. C,Lee, A secure single sign-on mechanism for distributed computer networks IEEE Transactions on Industrial Electronics 2012,67(2)629-637.