On security of a remote user authentication scheme without using smart cards

He Debiao*, Chen Jianhua, Hu Jin

School of Mathematics and Statistics, Wuhan University, Wuhan, Hubei 430072, China

Abstract: The security of a password authentication scheme using smart cards proposed by Rhee et al. is analyzed. A kind of impersonation attack is presented. The analyses show that the scheme is insecure for practical application. In order to eliminate the security vulnerability, an efficient countermeasure is proposed.

Key words: Authentication; Security; Cryptanalysis; Smart card; Attacks.

1. Introduction

User authentication is the essential security mechanism for remote login systems in which a password-based authentication scheme is the most commonly used technique to provide authentication between the legal users and the remote server.

In 1981, Lamport [1] proposed a password-based authentication scheme using password tables to authenticate remote users over insecure network. In Lamport's scheme, password table is used to verify the legitimacy of users. In 2000, Hwang et al. pointed out that once the password table was stolen or modified in this scheme, the whole authentication system will be affected [2]. Therefore, they proposed a remote user authentication scheme using smartcard without maintaining a password table. Afterwards, many schemes have been proposed to enhance the security and practicability [3-11].

In the real world, despite the recognition of their functionalities and security, smart cards have not yet prevailed. The high cost of the cards and readers remains a burden to issuers or users. In addition, there are more subtle problems in deploying the necessary infrastructure for smart cards, including the method of uploading different secure access modules (SAMs) into card readers. These obstacles have restricted the application of smart cards to the small fields such as financial transactions. Meanwhile, the common use of universal serial bus (USB) sticks these days has motivated our study. Many devices, such as PCs, USB sticks, mobile phones, and PDAs et al., are not designed to provide tamper-resistance. So we may not be able to directly use the existing authentication schemes using smart cards.

Recently, Rhee et al. [12] proposed a remote user authentication scheme without using smart cards. They claimed their scheme can withstand various attacks. But we find that their scheme is vulnerable to the impersonation attack. So it is insecure for practical application. Thus in order to eliminate the security vulnerability, we propose an efficient countermeasure in this paper.

The rest of the paper is organized as follows: Section 2 briefly reviews Rhee et al.'s scheme, Section 3 elaborates on the attack of their scheme, Section 4 provides some countermeasures to eliminate the security vulnerability of their scheme, Section 5 concludes this paper.

*Corresponding author.

E-mail: hedebiao@163.com, *Tel*:+008601530718492 7, *Fax*: +008602787817667

2. Review of Rhee et al. et al.'s scheme

The notations used throughout this paper are described as in the following.

- U_i: a user.
- $ID_i, PW_i : U_i$'s identifier, password respectively.
- S: a remote server.
- p: a large prime number.
- $x : S$'s secret keys.
- $T_i, T_S : U_i$'s current timestamp, and S's current timestamp, respectively.
- $h_1(\cdot), h_2(\cdot)$: two secure hash functions.
- $\oplus$: bitwise XOR operation.
- ||: concatenation operation

Rhee et al.'s scheme involves three phases: the registration phase, the login phase, the authentication phase.

Registration phase. In this phase, the user U_i initially registers with the server S.

1) U_i chooses his ID_i and PW_i and sends them to the server S over a secure channel.

2) Upon receiving $\{ID_i, RPW_i\}$, S checks the validity of ID_i. If ID_i is not valid, S rejects the registration. Otherwise, S generates a random r_i number and computes $Y_i = \{Y_{i,1}, Y_{i,2}\}$, where $Y_{i,1} = ID_i^{r_i \cdot x} \cdot h_1(PW_i) \bmod p$ and $Y_{i,2} = ID_i^{r_i} \bmod p$. At last, S sends $\{h_1, h_2, p, Y_i\}$ to U_i's device over a secure channel.

3) Upon receiving $\{h_1, h_2, p, Y_i\}$, U_i's device stores it.

Login phase. In this phase, the user U_i sends a login request message to the server S whenever U_i wants to access some resources upon S.

1) U_i's device generates two random numbers a, b and computes $Y_i' = \frac{Y_{i,1}}{h_1(PW_i)} \bmod p$, $M = h_1(Y_i' \oplus T_i \oplus ID_i)$, $C_1 = (Y_{i,2})^a \bmod p$, $C_2 = (Y_i')^a \cdot M \bmod p$ and $C_3 = (Y_{i,2})^b \bmod p$, where T_i is the current time stamp.

2) U_i's device sends the message $M_1 = \{ID_i, Y_{i,2}, C_1, C_2, C_3, T_i\}$ to the server S.

Verification phase. In this phase, the server *S* verifies the authenticity of the login message requested by the user U_i.

1) Upon receiving the message M_1, S checks the validity of ID_i. If ID_i is not valid, S stops the session.
2) S checks the freshness of T_i. The freshness of T_i is checked by performing $T' - T_i \le \Delta T$, where T' is the time when S receives the above message and ΔT is a valid time interval. If T_i is not fresh, S aborts the current session.
3) S computes $t_1 = C_2 \cdot (C_1^x)^{-1} \bmod p$, $t_2 = h_1((Y_{i,2})^x \oplus T_i \oplus ID_i) \bmod p$ and checks if t_1 equals t_2. If t_1 equals t_2, S accepts the login request. Otherwise, the login request is rejected.
4) S computes $C_4 = h_2(C_3^x \oplus T_S) \bmod p$ and sends the message $M_2 = \{C_4, T_S\}$ to U's device.
5) Upon receiving the message M_2, U_i's device checks the freshness of T_S. The freshness of T_S is checked by performing $T'' - T_S \le \Delta T$, where T'' is the time when U_i's device receives the above message and ΔT is a valid time interval.
6) U_i's device computes $C_4^* = h_2((Y_i')^b \oplus T_S) \bmod p$ and checks if C_4^* equals C_4. If C_4^* equals C_4, U_i's device thinks S is authenticated. Otherwise, U_i's device stops the session.

3. Impersonation attack on Rhee et al. et al.'s scheme

The security of their scheme is mainly based on the security of a one-way function and the difficulty of computing the discrete logarithm. In the following, we will show that an attacker can pretend to be a legal user and login the remote server successfully by registering and intercepting valid login request sent by the legal user

Suppose an attacker U_f attempts to impersonate a legal user U_i with identity ID_i. He can login the remote server successfully by performing the following steps:

1) U_f intercepts a login request message of the user $U_i: M_1 = \{ID_i, Y_{i,2}, C_1, C_2, C_3, T_i\}$.

2) U_f computes $ID_f = ID_i^{-1} \bmod p$. Then chooses ID_f as the identity, the random number PW_f as the password. The attacker U_f can get the message $\{h_1, h_2, p, Y_f\}$ through the registration phase, where $Y_f = \{Y_{f,1}, Y_{f,2}\}$, where $Y_{f,1} = ID_f^{r_f \cdot x} \cdot h_1(PW_f) \bmod p$, $Y_{f,2} = ID_f^{r_f} \bmod p$ and r_f is a random number generated by S.

3) U_f generates two random number a, b computes $\overline{Y_f} = \frac{Y_{f,1}}{h_1(PW_f)} \bmod p$, $Y_f' = (\overline{Y_f})^{-1} \bmod p, Y_{f,2}' = Y_{f,2}^{-1} \bmod p$, $M = h_1(Y_f' \oplus T_i \oplus ID_i)$, $C_1 = (Y_{f,2}')^a \bmod p$, $C_2 = (Y_f')^a \cdot M \bmod p$ and $C_3 = (Y_{f,2}')^b \bmod p$, where T_i is the current time stamp. U_f sends the message $\{ID_i, Y_{f,2}', C_1, C_2, C_3, T_i\}$ to the server.

It is easy to verify that $\{ID_i, Y_{i,2}, C_1, C_2, C_3, T_i\}$ is a valid login request. Since

$$Y_f' = (\overline{Y_f})^{-1} \bmod p = (\frac{Y_{f,1}}{h_1(PW_f)})^{-1} \bmod p = (\frac{ID_f^{r_f \cdot x} \cdot h_1(PW_f)}{h_1(PW_f)})^{-1} \bmod p = ID_f^{-r_f \cdot x} \bmod p$$

$, Y_{f,2}' = Y_{f,2}^{-1} \bmod p = ID_f^{-r_f} \bmod p$, then

$$\begin{aligned} t_1 &= C_2 \cdot (C_1^x)^{-1} \bmod p = \frac{(Y_f')^a \cdot M}{((Y_{f,2}')^a)^x} \bmod p \\ &= \frac{(ID_f^{-r_f \cdot x})^a \cdot M}{((ID_f^{-r_f})^a)^x} \bmod p = M \bmod p \\ &= h_1(Y_f' \oplus T_i \oplus ID_i) \bmod p = h_1(ID_f^{-r_f \cdot x} \oplus T_i \oplus ID_i) \bmod p \\ &= h_1((ID_f^{-r_f})^x \oplus T_i \oplus ID_i) \bmod p = h_1((Y_{i,2})^x \oplus T_i \oplus ID_i) \bmod p \\ &= t_2 \end{aligned}$$

Therefore, Rhee et al.'s scheme suffers from the impersonation attack. Rhee et al.'s scheme is insecure

4. Countermeasure

The vulnerability to the undetectable on-line dictionary attack described above actually stems

from the adversary can deduce user's secret information through the secret information owned by himself. There is a simple countermeasure to overcome the security vulnerability. If we let the user's ID is generated by the server instead of being chosen by the user in the registration phase, then we can avoid the users to choose a specialized ID, such as $ID_f = ID_i^{-1} \bmod p$, for computing other users's secret information $Y_i = \{Y_{i,1}, Y_{i,2}\}$ and the attack described above is not valid. But if the ID is generated by the server, the user may forget the ID easily. We can through another hash operation to destroy the relation among the user's secret information. We recommend the following changes to Rhee et al.'s scheme:

- $Y_{i,1} = h_1(ID_i)^{r_i \cdot x} \cdot h_1(PW_i) \bmod p$;
- $Y_{i,2} = h_1(ID_i)^{r_i} \bmod p$;

With this modification applied, the secret information of the adversary is no longer useful in verifying password guesses. Then the countermeasure can withstand the attack.

5. Conclusion

In [12], Rhee et al. proposed a password authentication scheme without using smart cards and demonstrated its immunity against various attacks. However, by reviewing of their scheme and analyzing its security, we find their scheme is vulnerable to the impersonation attack. The analyses show that the scheme is insecure for practical application. In order to eliminate the security vulnerability, we proposed an efficient countermeasure. After our modification, Rhee et al.'s scheme is secure under our attack.

Reference

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

[2]. 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.

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

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

[5]. C.C. Lee, M.S. Hwang, W.P. Yang, A flexible remote user authentication scheme using smart cards, ACM Operating Systems Review 36 (3) (2002) 46 – 52.

[6]. J.J. Shen, C.W. Lin, M.S. Hwang, A modified remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 49 (2) (2003) 414 – 416.

[7]. M. Kumar, New remote user authentication scheme using smart cards, IEEE Transactions on Consumer Electronics 50 (2) (2004) 597 – 600.

[8]. W.C. Ku, S.T. Chang, M.H. Chiang, Further cryptanalysis of fingerprint-based remote user

authentication scheme using smartcards, IEE Electronics Letters 41 (5) (2005).
[9]. M.K. Khan, J. Zhang, Improving the security of ‘a flexible biometrics remote user authentication scheme’, Computer Standards & Interfaces 29 (2007) 82–85.
[10]. S.K. Kim, M.G. Chung, More secure remote user authentication scheme, Computer Communications 32 (2009) 1018–1021.
[11]. J.H. Yang, C.C. Chang, An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem, Computers & Security 28 (2009) 138–143.
[12]. H. S. Rhee, J. O. Kwon, D. H. Lee, A remote user authentication scheme without using smart cards, Computer Standards & Interfaces 31 (2009) 6–13.