Available online at http://scik.org
J. Math. Comput. Sci. 3 (2013), No. 3, 799-807
ISSN: 1927-5307

SECURITY FLAWS IN AN IMPROVED TIMESTAMP-BASED REMOTE USER AUTHENTICATION SCHEME

JUAN QU

School of Mathematics and Statistics, Chongqing Three Gorges University, Wanzhou, Chongqing, 404000, China

Abstract. Recently, Awasthi et al. proposed a timestamp-based remote user authentication scheme. We point out that their scheme is vulnerable to smart card loss attack, offline password guessing attack and does not preserve anonymity of user. To overcome these flaws, we propose a new remote user authentication scheme. We also show that the proposed scheme not only solves the weaknesses which exist in Awasthi et al.'s scheme, but also can provide session key for the further communication.

Keywords: Authentication; Cryptanalysis; User anonymity; Stolen smart card attack; Offline password guessing attack.

2000 AMS Subject Classification: 97R50.

1. Introduction

With the repaid development of the Internet, the demand of Internet services is increasing. Remote user authentication is a mechanism which allows the user and the server to mutually authenticate the legitimacy of each other over public network. Since Lamport[1] proposed a password authentication protocol, ample of smart card based authentication protocols have been proposed[2]-[5]. In 1999, Yang and Shieh[6] proposed two password

Received April 28, 2013

authentication schemes with smart cards. Later, Fan[7] proposed an enhancement scheme to improve the security of Yang and Shieh's password authentication scheme. In 2003, Wang et al.[8] showed that an intruder was able to construct a forged login request from the intercepted legitimate login requests. In the same year, Shen et al.[9] proposed a modified scheme of the Yang-Shieh's scheme to withstand the forged login attack and provide mutual authentication. But, Awasthi et al.[10] pointed out that Shen et al.'s scheme is still vulnerable to the forged login attack, and Awasthi et al. proposed an improvement scheme. However, we will show that Awasthi et al.'s scheme is vulnerable to smart card loss attack , offline password guessing attack and does not preserve anonymity of user.
The remainder of this paper is organized as follows. In Section 2, we review a Preliminaries. In section 3, Awasthi et al.'s scheme is shown. The security analysis is discussed in Section 4. In section 5, an enhanced authentication scheme using smart card and ECC is proposed. Finally, the conclusions are given in Section 6.

2. Preliminaries

In this section, we introduce the basic concepts of ECC. In all elliptic curve cryptosystem, the elliptic curve equation is defined as the form of $E_p(a,b)$: $y^2 = x^3 + ax + b(\underline{m}odp)$. Given an integer $s \in F_p^*$ and a point $P \in E_p(a,b)$, the point-multiplication sP over $E_p(a,b)$ can be defined as $sP = P + P + P + \cdots + P(s$ times$)$. Generally, the security of ECC relies on the difficulties of the following problems.
Definition 1 Given two points P and Q over $E_p(a,b)$, the elliptic curve discrete logarithm problem (ECDLP) is to find an integer $s \in F_p^*$ such that $Q = sP$.
Definition 2 Given three points P, sP, and tP over $E_p(a,b)$ for s, $t\in F_p^*$, the computational Diffie-Hellman problem(CDLP) is to find the point $(st)P$ over $E_p(a,b)$.
Definition 3 Given two points P and $Q = sP + tP$ over F_p^* for s, $t\in F_p^*$, the elliptic curve factorization problem(ECFP) is to find two points sP and tP over $E_p(a,b)$.

3. Reviews of Awasthi et al.'s scheme

In 2011, Awasthi et al. analyzed the weaknesses of the Shen et al.'s scheme, and presented an improved remote authentication scheme. The modified scheme is composed for four phase: Initialization phase, Registration phase, Login phase and Authentication phase.

3.1.Initialization phase

Key information Center (KIC) is a trusted authority which generates global parameters. KIC also computes user's secret information and provides smart cards to users. KIC performs the following steps:

(1) Generates two large primes p and q and computes $n = pq$.

(2) Choose a prime number e and an integer d, such that $e \cdot d \bmod (p-1)(q-1) = 1$, where e is the system's public key, and d is the corresponding private key, which should be provided to the server in a safe way.

(3) Find an integer g, which is a primitive element in both $GF(p)$ and $GF(q)$ and the public information of the system.

3.2.Registration phase

A new user U_i securely submits his identifier ID_i and password PW_i to the KIC. The KIC then performs the following steps:

(1)Genarate the smart card's identifier CID_i for the user U_i and h_i as $CID_i = f(ID_i \oplus d)$, $h_i = g^{PW_i \cdot d} \bmod n$, where $f(x)$ is a one way function.

(2) Calculate the user's secret information $S_i = CID_i^d \bmod n$.

(3) Write n, e, g, ID_i, S_i and h_i into smart card of U_i and issue the smart card to the user through a secure channel.

3.3.Login phase

User U_i performs the following steps:

(1) Choose a random number r_i and compute X_i and Y_i as follows:

$X_i = g^{r_i \cdot PW_i} \bmod n$, $Y_i = S_i \cdot h_i^{r_i \cdot f(ID_i, T_c)} \bmod n$, where T_c is the timestamp at the login device and $f(x, y)$ is a one way function.

(2) User U_i sends $M = (ID_i, X_i, Y_i, n, e, g, T_c)$ to the remote server S, where M is a login

request message of the user U_i.

3.4.Authentication phase

After receiving the login request message M from U_i, the remote server will perform the following steps to verify the correctness of M.

(1) Verify that ID_i is a valid user identifier. If it is not then reject the login request.

(2) Check the validity of T_c. If $T_s - T_c > \triangle T$, then the server rejects the login request, where T_s is the current timestamp at the remote server, $\triangle T$ is expected legitimate time interval for transmission delay.

(3) Compute $CID_i = f(ID_i \oplus d)$.

(4) Check the equation $Y_i^e = CID_i \cdot X_i^{f(ID_i,T_c)} \bmod n$. If it holds, accept the login request, otherwise reject.

(5) $S \to M'$: $M' = (R, T_s')$, where $R = (f(ID_i, T_s'))^d \bmod n$ and T_s' is the current timestamp on the remote server. Upon receiving the message M' from the server, the user U_i verifies the server as follows.

(6) Check the time interval between T_s' and T_c', where T_c' is the timestamp when the user U_i receives the message M'. If $T_c' - T_s' > \triangle T$, then U_i rejects the remote server, where $\triangle T$ denotes the predetermined legitimate time interval of transmission delay.

(7) Compute $R' = R^e \bmod n$. If $R' \stackrel{?}{=} f(ID_i, T_s')$, accept the server otherwise reject server and disconnect it.

4. Flaws of Awasthi et al.'s scheme

In this section, we demonstrate that Awasthi et al.'s scheme is vulnerable to smart card loss attack , offline password guessing attack and does not preserve anonymity of user. The details of these flaws are described as follows.

4.1.Smart card loss attack

Smart card loss attack is that when the smart card is lost or stolen, unauthorized users can impersonate the user to login to the system or guess the password of the user using password guessing attack. If the user U_i's smart card is lost or stolen, the attacker A can extract the stored secret information $(n, e, g, ID_i, S_i, h_i)$ stored in the smart card.

Then, the attacker A can compute $h_i^e = g^{PW_i \cdot d \cdot e} \bmod n = g^{PW_i} \bmod n$. Then, the attacker A chooses a random number r_i' and computes $X_i' = (h_i^e)^{r_i'} \bmod n = g^{PW_i \cdot r_i'} \bmod n$, $Y_i' = S_i \cdot h_i^{r_i' \cdot f(ID_i, T_c')} \bmod n$, where T_c' is the attacker A at the login device. In the following, the attacker A sends the login request message $M' = (ID_i, X_i', Y_i', n, e, g, T_c')$ to the remote server S. After receiving M', the remote server S verifies that the ID_i is a valid user identifier and check the validity of $T_s' - T_c' \leq \triangle\, T$. Then, the remote server S computes $CID_i = f(ID_i \oplus d)$, check the equation $Y_i'^e \stackrel{?}{=} CID_i \cdot X_i'^{f(ID_i, T_c')} \bmod n$. It is obvious that

$$
\begin{aligned}
Y_i'^e &= S_i^e \cdot h_i^{r_i' \cdot f(ID_i, T_c') \cdot e} \bmod n \\
&= CID_i \cdot g^{PW_i \cdot d \cdot r_i' \cdot f(ID_i, T_c') \cdot e} \bmod n \\
&= CID_i \cdot g^{PW_i \cdot r_i' \cdot f(ID_i, T_c')} \bmod n \\
&= CID_i \cdot X_i'^{f(ID_i, T_c')} \bmod n.
\end{aligned}
$$

Therefore, S accept the login request. According to the above analysis, when the user U_i's smart card is stolen by the attacker A, then she/he can computes h_i^e. And with h_i^e, the attacker A can successful forge a valid login request message of the user U_i. Hence, Awasthi et al.'s scheme cannot resist the stolen smart card attack.

4.2.Offline password guessing attack

After the attacker A computes $h_i^e = g^{PW_i} \bmod n$ in the section 5.1. The attacker A can successfully guess the password of U_i as follows:

(1) The attacker A randomly chooses PW_i^*;

(2) Computes $g^{PW_i^*} \bmod n$;

(3) Verifies $g^{PW_i} \bmod n \stackrel{?}{=} g^{PW_i^*} \bmod n$.

4.3.User anonymity

User anonymity is an important feature that a practical authentication scheme should achieve. To prevent unauthorized entities from tracking the mobile user's movements. It is very important to ensure user anonymity such that user's real identity can only be recognized by server. In the login phase of Awasthi et al.'s scheme, user U_i sends the plaintext message $M = (ID_i, X_i, Y_i, n, e, g, T_c)$ to the remote server S. The attacker can easily get user's identity ID_i from the public channel. So, Awasthi et al.'s scheme fails in providing the privacy and anonymity of U_i during the login phase.

5. Proposed scheme

In this section, We propose our improved scheme that can protect against all the attacks mentioned in section 4. Suppose x is the secret key of KIC, and KIC computes $Q = x \cdot P$. Keeps secret x and publishes the public parameters P, n, Q, $h(\cdot) : (0,1)^* \longrightarrow Z_n^*$. Our scheme has four phases, registration, login, verification and password change phase. The details procedures are describes as follows.

5.1.Registration phase

1. user U_i chooses ID_i, pw_i and computes $pw_i \cdot P$.

2. U_i submits his ID_i and $pw_i \cdot P$ to KIC via a secret channel.

3. KIC computes $h_i = x \cdot pw_i \cdot P$, $S_i = h(x \| ID_i) \cdot P$, $T_i = h(ID_i \| pw_i \cdot P)$.

4. KIC issues smart card to U_i which contains values of S_i , h_i, T_i, and P via a secret channel.

5.2.Login phase

If U_i wants to access the server, he/she inserts smart card into the terminal, keys ID_i with pw_i, then the smart card verifies the equation $h(ID_i \| pw_i \cdot P) = T_i$ holds or not. If it holds, User U_i performs the following steps:

1. Chooses a random number $r_i \in Z_n^*$ and computes $R_i = r_i \cdot P$, $X_i = r_i \cdot pw_i \cdot P$, $Y_i = r_i \cdot h_i + h(S_i \| r_i \cdot Q)$.

2. User U_i sends $M = (R_i, X_i, Y_i, P)$ to the remote server S, where M is a login request message of the user U_i.

5.3.Authentication phase

After receiving the login request message M from U_i, the remote server will perform the following steps to verify the correctness of M.

1. Computes $S_i' = h(x \| ID_i) \cdot P$, $Y_i' = x \cdot X_i + h(S_i' \| x \cdot R_i)$, U_i checks whether $Y_i' \stackrel{?}{=} Y_i$. If this holds, S authenticates U_i otherwise login request is rejected.

2. For mutual authentication, S selects a random number $r_j \in Z_n^*$ and computes

$R_j = r_j \cdot P$, $Z_i = h(r_j \cdot R_i \| h(ID_i \| R_i))$, and then sends the mutual authentication message (R_j, Z_i) to U_i.

3. Upon receiving the mutual authentication message, U_i verifies $Z_i' = h(r_i \cdot R_j \| h(ID_i \| R_i)) \stackrel{?}{=} Z_i$. If this holds, U_i authenticates S otherwise login request is give up by U_i.

4. Now, U_i and S share the symmetric session key $S_k = h(r_i \cdot r_j \cdot P \| S_i)$ for performing further operations during a session.

5.4.Password-change phase

In the password-change phase, when a user wants to change his password pw_i with a new password pw_i^{new}, he inserts his smart card into smart card reader and enters his ID_i and password pw_i. The smart card performs the following operations without interacting with KIC:

1. Computes $T_i^* = h(ID_i \| pw_i \cdot P)$. If $T_i^* = T_i$, then U_i is allowed to change the password, otherwise password-change phase is terminated.

2. Computes $h_i^{new} = pw_i^{new} \cdot Q$ and replaces the old value of h_i with the new value. Now, the new password is successfully changed and this phase is terminated.

6. Cryptanalysis of the proposed scheme

In this section, we first describe the enhanced security features of our proposed scheme which is a modified form of Awasthi et al.'s scheme. Finally, the we summarize the functionality comparisons between our scheme and other remote user authentication schemes in Table 1. It is clear that our proposed scheme is more secure and reliable.

6.1.Resistance to smart card loss attack

Smart card attack cannot work on the improved scheme. When user U_i's smart card is lost or stolen, though the attacker can extract the stored secret information (S_i, h_i, T_i, P) stored in the smart card, the attacker has no way to compute X_i, Y_i to forge the login request message.

6.2.Resistance to offline-password guessing attack

The attacker has no way to carry out offline-guessing attack, because the password pw_i in h_i, T_i,and X_i is protected by hash function and ECDLP problem.

6.3.user anonymity

In the proposed scheme, a user's real real identity is concealed in the Y_i, and each login request message is different. So, our proposed scheme preserve user anonymity.

6.4.Session key agreement

The user and the server establish a secure session key $S_k = h(r_i \cdot r_j \cdot P \| S_i)$ in each session. With this session key, the user and the remote server can exchange confidential data securely.

6.5.Performance comparison

Table 1. *Comparison of security properties*

	Shen et al.'s scheme	***Awasthi et al.'s scheme***	***Proposed scheme***
User anonymity	No	No	Yes
forged attack	Yes	Yes	No
Smart card loss attack	Yes	Yes	No
Mutual authentication	No	Yes	Yes
Key agreement	No	No	Yes

Yes: Supported No: Not Supported

7. Summary

In this paper, we reviewed Awasthi et al.'s timestamp-based remote user authentication scheme. We found that Awasthi et al.'s scheme cannot defend against smart card loss attack , offline password guessing attack and does not preserve anonymity of a user. These flaws can cause the scheme to become unsecured. Finally, we propose an improvement scheme to overcome the identified problems and our scheme is more efficient and secure.

References

[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] Improving the security of 'a flexible biometrics remote user authentication scheme'. Computer Standards & Interfaces, 29(1) 2007:82-85.

[4] Tianjie Cao, Yingying Kan. Cryptanalysis of Two ID-Based Deniable Authentication Protocol from Pairings, Journal of Information and Computational Science, 6(4) 2009:1831-1837.

[5] W.Ku , S.T.Chang. Impersonation attacks on a dynamic id-based remote user authentication scheme using smart cards. IEICE Transactions, E88-B(5),2005:2165-2167.

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

[7] L. Fan, J.H. Li, H.W.Zhu. An enhancement of timestamp-based password authentication scheme. Computer & Security. 21(7),2002:665-667.

[8] B Wang,J.H Li,Z.P Tong. Cryptanalysis of an enhanced timestamp-based password authentication scheme. Computers & Security. 22(7),2003:643-645.

[9] J.J Shen, C.W.Lin, M.S.Hwang. Security enhancement for the timestamp-based password authentication scheme using smart cards. Computers & Security. 22(7),2003:591-595.

[10] Amit K.Awasthi, Keerti Srivastava, R.C.Mittal. An improved timestamp-based remote user authentication scheme. Computers and Electrical Engineering. 37(6),2011:869-874.