Improvement of Manik et al.'s remote user authentication scheme

Jue-Sam Chou, [a] ,Yalin Chen [b] Jyun-Yu Lin [c]

[a] Department of Information Management, Nanhua University Chiayi, 622, Taiwan
jschou@mail.nhu.edu.tw
Tel: 886+(0)5-2721001ext.56226

[b] Institute of information systems and applications, National Tsing Hua University
d949702@oz.nthu.edu.tw
Tel: 886+(0)3-5738997

[c] Department of Information Management, Nanhua University Chiayi, 622, Taiwan
asurejoker@gmail.com
Tel: 886+(0)5-2721001 ext.2017

Abstract

In 2005, Manik et al. propose a novel remote user authentication scheme using bilinear pairings which allows a valid user to login to the remote system but prohibits too many users to login with the same login-ID. It also provides a flexible password change function. In this paper, we will show that this remote user authentication scheme is not secure, an adversary can always pass the authentication.

Keywords: bilinear pairings, security, Key-Compromise Impersonation, authentication, smart card

1. Introduction

In 1976, Diffie and Hellman first propose a public key cryptosystem based on the complex discrete logarithm problem [3] and opened the modern cryptography era. After that, several developed cryptosystems such as RSA [4], Digital signature [5] based on the Public-Key Infrastructure are proposed. Because these systems have a superior security level, many researches work in this area attempting to improve and extend some existed applications. Under this scenario, the idea of ID-Based public-key cryptosystem was first introduced in 1984 by Shamir which [6] allows a user to use his ID as his public key.

Recently, in 2001, bilinear pairings such as Weil pairing and Tate pairing defined on elliptic curves were proved and can be applied to cryptography. The bilinear pairings are an effective method to reduce the complexity of the discrete log problem in a finite field [1] [2]. Pairing provides a good setting for the bilinear Diffie–Hellman problem and has been used to design several cryptosystems. The benefit of a bilinear pairing cryptosystem is that it remains the same security level but reduces the computation cost. Many protocols are designed based on the Weil pairing. For example, one-round tripartite key agreement[7], the ID-based public-key encryption scheme based on bilinear Diffie–Hellman problem[8], ID-based authentication key agreement protocol based on pairing[9] and ID-based signature schemes[10], etc.

In 2005, Manik et al. propose a novel remote user authentication scheme using bilinear pairings [12] to prevent an adversary from launching a forgery attack in a login session. In this paper, we propose an impersonation attack on their remote user authentication scheme by showing that any malicious users can impersonate an entity to deceive the remote server. So, their scheme cannot provide the security as claimed.

The organization of this article is as follows: in Section 2, we present the preliminaries of bilinear pairings and the four secure attributes [11] in a key agreement protocols. In Section 3, we review the Manik et al.'s remote user authentication scheme. In section 4, we describe how their scheme is easy to suffer from the impersonation attack. Finally, a conclusion is given in Section 5.

2. Bilinear pairings

In this section, we will first introduce the concepts of bilinear pairings map under the assumption that G_1 is an additive cyclic group generated by P, whose order is a prime q, and G_2 is a multiplicative cyclic group of the same order. After that, the four secure attributes [11] in a sound authenticated key agreement protocol are described.

2.1 Bilinear pairings map

A map e: $G_1 \times G_1 \rightarrow G_2$ is called a bilinear map if it satisfies the following properties:

1. Bilinear: e(aP, bQ) =e(P ,Q)^{ab} for all P, Q$\in$ G_1 and a, b$\in Z_q^*$.
2. Non-degenerate: there exist P, Q$\in$ G_1 such that e(P,Q)$\neq$1.
3. Computable: there is an efficient algorithm to compute e(P; Q) for all P, Q$\in$ G_1.

2.2 Security attributes

In order to reach a higher security level, Wilson and Menezes [11] defined several security attributes. We show these attributes in the following. Here, we assume A and B are two honest entities.

1. Known-Key Security
   In each round of key agreement protocol, A and B should generate a unique session key. Each session key generated in one protocol round is independent and should not be exposed if other session keys are compromised.
2. Forward Secrecy
   The forward secrecy property is that if A and B's current session key are compromised, the session keys used in the past should not be recovered.
3. Key-Compromise Impersonation (KCI) attack
   A protocol which is secure against the KCI attack means that if A's long-term secret key is compromised, the adversary who knows the value can not impersonate others to A.
4. Unknown Key-Share attack
   After the protocol, A believes he shares a key with B, but B mistakenly believes that the key is instead shared with an adversary. Therefore, a sound authenticated key agreement protocol should prevent the unknown key-share situation.

3. Review of Manik et al.'s remote user authentication scheme

Manik et al.'s scheme has three mainly phases, the setup phase, the registration phase, and the authentication phase.

3.1 Setup phase

Let G_1 be an additive cyclic group of a prime order q, G_2 be a multiplicative cyclic group of the same order, and P be a generator of G1. Define e :($G_1 \times G_1 \in G_2$) to be a bilinear mapping and H: $\{0,1\}^* \rightarrow G_1$ be a cryptographic hash function. Suppose the remote system (RS) selects a secret key s and computes his public key as Pub_{RS}=sP. Then, the RS publishes the system parameters (G_1, G_2, e, q, P, Pub_{RS}, H) and keeps s secret.

3.2 Registration phase

This phase is executed by the following steps when a new user U_i wants to register with the RS.

Step1. U_i submits his identity ID_i and password PW_i to the RS.

Step2. On receiving the registration request, the RS computes
Reg_{ID_i} = sH(ID_i) + H(PW_i).

Step3. The RS personalizes a smart card with the parameters ID_i, Reg_{ID_i}, H( ) and sends the smart card to U_i over a secure channel.

3.3 Authentication phase

This phase will be executed whenever a user wants to log into the RS. We describe it as follows and also delineate it in figure 1.

a. login

Suppose the ID_i of user U_i is stored in the smartcard and U_i wants to login to the remote system, then the smart card will process the login operation after U_i has inserted the smart card and inputted the ID_i and PW_i to the terminal. For example, the smart card will compute $DID_i = T * Reg_{ID_i}$ and $V_i = T * H(PW_i)$, where T is the user system's timestamp. After that, terminal will send the login request <ID_i, DID_i, V_i, T> to the RS over the public channel.

b. verification

After receiving the login message <ID_i, DID_i, V_i, T>, RS will perform the following operations to verify it.

Step1. Verify the validity of the time interval between T^* and T. If $(T^* - T) \le \Delta T$, then RS goes to step2 else rejects. Here ΔT denotes the time delay which is in the tolerable range by both the user and RS.

Step2. Checks to see whether $e(DID_i - V_i, P) = e(H(ID_i), Pub_{RS})^T$ holds, if it holds, RS accepts the login request; otherwise, it rejects. The deduction process is as follows:

$$
\begin{aligned}
e\,(DID_i - V_i, P) &= e(T * Reg_{ID_i} - V_i, P) \\
&= e((T(s * H(ID_i) + H(PW_i) - T * H\,(PW_i), P) \\
&= e(s * H(ID_i), P)^T = e(H(ID_i), Pub_{RS})^T
\end{aligned}
$$

The protocol is also shown below in Figure1:

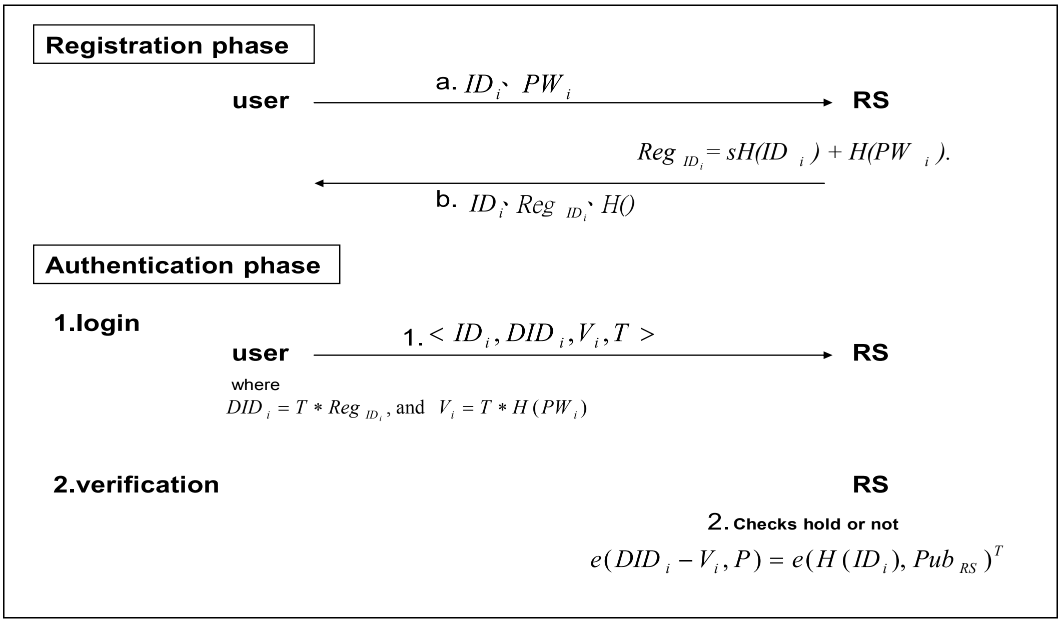

Registration phase
user
a. ID_i、PW_i
RS
$Reg_{ID_i} = sH(ID_i) + H(PW_i)$.
b. ID_i、Reg_{ID_i}、$H()$
Authentication phase
1.login
user
1. $< ID_i, DID_i, V_i, T >$
RS
where
$DID_i = T * Reg_{ID_i}$, and $V_i = T * H(PW_i)$
2.verification
RS
2. Checks hold or not
$e(DID_i - V_i, P) = e(H(ID_i), Pub_{RS})^T$

Figure1. Both of the registration and authentication phase in Manik et al.'s scheme

3.4 Password change phase

This phase allows U_i to change his password freely. He can easily change his password without taking any assistance from the RS. This phase can be described as follows:

Step1. U_i first inputs his correct ID_i and PW_i, and then he submit a newly selected password PW_i^* to the smart card.

Step2. The smart card then does the computation as follows:

$$Reg^*_{ID_i} = Reg_{ID_i} - H(PW_i) + H(PW_i^*) = sH(ID_i) + H(PW_i^*).$$

Thus, the password can be changed to PW_i^* and the smart card will replace the previously stored Reg_{ID_i} by $\mathrm{Reg}^*_{ID_i}$.

4. Our attack

In this section we will analyze the protocol proposed by Manik et al. under the assumption that an adversary X wants to impersonate a legal registered user U_i to RS. After analyzing, we find that the protocol is not secure as they claimed. We describe our cryptanalysis as follows.

Step1. X can record any login message < ID_i, DID_i, V_i, T >, sent by U_i who had ever logged into RS. And then computes as follows:

$$\begin{aligned} DID_i\text{-}V_i &= T*\mathrm{Reg}_{ID_i} - T*H(PW_i). \\ &= T*[s*H(ID_i)+H(PW_i)] - T*H(PW_i) \\ &= T*s*H(ID_i) \end{aligned}$$

Step2. X can pick a random timestamp T' and computes T' * H(PW_j), where PW_j is X's randomly selected password not confirmed by RS.

Step3. X computes his DID_j and V_j as follows.

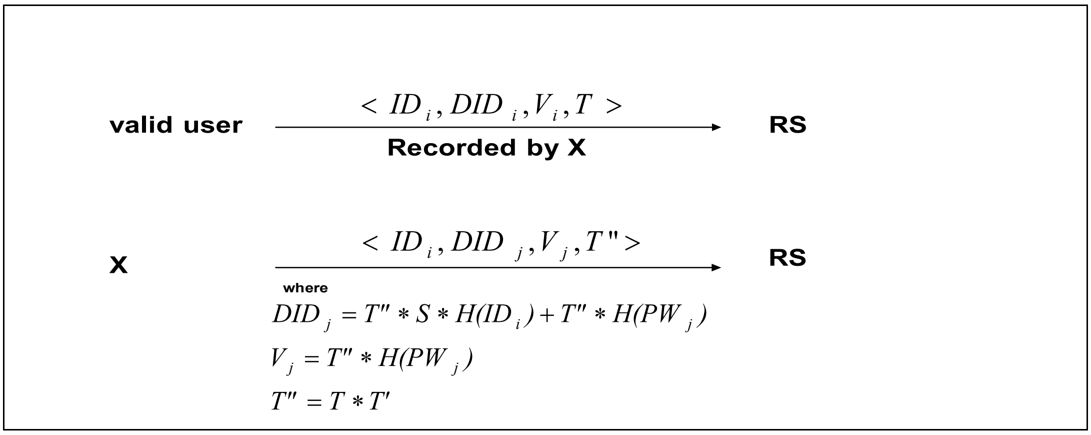
$$\begin{aligned} DID_j &= T'*(DID_i\text{-}V_i) + T'*T*H(PW_j) \\ &= T'*T*s*H(ID_i) + T'*T*H(PW_j), \text{ and} \\ V_j &= T'*T*H(PW_j), \text{ respectively.} \end{aligned}$$

Then X computes:(Let T * T' = T".)

$$\begin{aligned} DID_j\text{-}V_j &= T''*\mathrm{Reg}_{ID_i} - T''*H(PW_i) \\ &= \{T''*[s*H(ID_i) + H(PW_i)]\} - T''*H(PW_i) \\ &= T''*s*H(ID_i). \end{aligned}$$

Step4. At a later time T", when X wants to launch an attack, he can use this forged message <ID_i, DID_j, V_j, T"> to masquerade as U_i to RS.

Because RS doesn't store the ID and PW of a specific user. And it's verification depends only on checking whether $e(DID_j\text{-}V_j, P) = e(H(ID_i), Pub_{RS})^{T''}$ holds. If this equation holds, RS will accept the forged login message. Clearly, it can be seem that this verification equation holds. Since we already deduce (DID_j-V_j) to be T" * s * H(ID_i) in Step3. As a result, X can easily impersonate any valid user, for example ID_i, he wants by our method. We show our attack in figuare2.


valid user
$< ID_i, DID_i, V_i, T >$
Recorded by X
RS
X
$< ID_i, DID_j, V_j, T'' >$
RS
where
$DID_j = T'' * S * H(ID_i) + T'' * H(PW_j)$
$V_j = T'' * H(PW_j)$
$T'' = T * T'$

Figuare2. Our attack

5. Our improvement

The main problem in their scheme can be easily seen. It is that the value of V_i can be cancelled out from DID_i and $\mathrm{T} * \mathrm{s} * \mathrm{H}(\mathrm{ID}_i)$ remains after this cancellation. Thus, we must prevent this situation to occur. To remedy this problem, the verification equation should be modified to $\mathrm{e}(\mathrm{DID}_i, \mathrm{P}) = \mathrm{e}(\mathrm{T} * \mathrm{s} * \mathrm{H}(\mathrm{ID}_i) + \mathrm{V}_i, \mathrm{P})$.

6. Conclusions

In this paper, we have shown that Manik et al.'s scheme is vulnerable to the impersonate attack. We have also proposed the resolvable solution in Section 5.

References

[1]G.Frey, H. Ruck, A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves, Mathematics of Computation 62 (1994) 865–874.

[2] A.Menezes, T.Okamoto , S.Vanston, Reducing elliptic curve logarithms to logarithms in a finite field, IEEE Transaction on Information Theory 39 (1993) 1639–1646.

[3] Diffie, W., Hellman, M., 1976. New directions in cryptography. IEEE Transactions on Information Theory 22 (6), 644–654.

[4] R.L. Rivest, A. Shamir, L. Adelman, A method for obtaining digital signature and public key cryptosystem, Comm. ACM 21 (2) (1978) 120–126

[5] A. Fiat, A. Shamir, How to prove yourself: practical solutions to identification and signature problems, in: A.M. Odlyzko (Ed.), Advances in Cryptology, Proceedings of CRYPTO_86, 1986, Santa Barbara, CA, USA, Lecture Notes in Computer Science, vol. 263, Springer, New York, 1987.

[6] Shamir, Identity based cryptosystems & signature schemes, Advances in Cryptology, CRYPTO'84, Lecture Notes-Computer Science, 1984, pp. 47– 53.

[7] A. Joux, A one round protocol for tripartite Diffie–Hellman, in: Proceedings of Algorithmic Number Theory Symposium Lecture Notes in Computer Science, vol. 1838, Springer-Verlag, Berlin, 2000, pp. 385–394.

[8] D. Boneh, M. Franklin, Identity-based encryption from the Weil pairing, in: Advances in Cryptology—Crypto_01, LNCS 2139, Springer-Verlag, 2001, pp. 213–229.

[9] N.P. Smart, An identity based authentication key agreement protocol based on pairing, Electron. Lett. 38 (2002) 630–632.

[10] K.G. Paterson, ID-based signature from pairings on elliptic curves, Electron. Lett. 38 (18)(2002), 1025–1026.

[11] S. B. Wilson, and A. Menezes, ”Authenticated Diffie-Hellman key agreement protocols”, Proceedings of the 5th Annual Workshop on Selected Areas in Cryptography (SAC ’98), Lecture Notes in Computer Science, pp. 339-361, 1999.

[12] M. L. Das , and A. Saxena , “A novel remote user authentication scheme using bilinear pairings” Computers & Security, 2005