Improvement of recently proposed Remote User Authentication Schemes

Guanfei Fang and Genxun Huang
Science Institute of Information Engineering University,
Zhengzhou, 450002, P.R.China
feifgf@163.com

Abstract

Recently **Manik et al.** [13] proposed a novel remote user authentication scheme using bilinear pairings. **Chou et al.** [14] identified a weakness in Manik et al.'s scheme and made an improvement. **Thulasi et al.** [15] show that both Manik et al.'s and Chou et al.'s schemes are insecure against forgery attack and replay attack. But Thulasi et al. do not propose a improvement. In this paper, we propose an improvement to over come the flaws.

Key Words：Authentication、Bilinear pairings、Smart Card、Password、Timestamp.

1. Introduction

Remote User Authentication scheme allows the authenticated user to login to the remote system to access the services offered. In 1981, Lamport [1] introduced the first well-known hash-based password authentication scheme. Recently, Manik et al. [13] proposed a remote user authentication scheme using bilinear pairings. In the scheme, they use Timestamps to avoid replay attacks while sending the authentication request over a public channel. But this is completely insecure as an adversary can use this information for illegal login later.

Chou et al. [14] identified that the verification of Manik et al.'s scheme involves subtraction of two components, which are passed over the public channel leading to replay attack. One can do replay by adding same information to those two components, as it results in valid verification. To overcome replay attack, they suggested a modification in verification part of Manik et al.'s scheme, however Thulasi et al. [15] observed that the modified scheme also suffers from the replay attack. And they further point to more attacks on [13]. But they do not propose a improvement to over come the flaws, which lead to the insecurity of the schemes.

In this paper, we cryptanalyze Manik et al.'s and Chou et al.'s schemes. And in the end, we propose an improvement to over come the flaws which Thulasi et al. found.

The organization of the paper is as follows. In Section-2, we present the preliminaries of bilinear pairings. In Section-3 Manik et al.'s scheme is briefly reviewed. Chou et al.'s attack on Manik et al.'s scheme is reviewed in Section-4. In Section-5 Thulasi et al. attack on Chou et al.'s scheme and Manik et al.'s scheme is given. We improve Manik et al.'s scheme in Section-6. We concluded in Section-7.

2. Bilinear Pairings

Let G_1 be an additive cyclic group of prime order q and G_2 be the multiplicative cyclic group of the same order. Practically we can think of G_1 as a group of points on an elliptical curve over Z_q , and G_2 as a subgroup of the multiplicative group of a finite field $Z^*_{q^k}$ for some k$\in Z^*_q$. Let P be a generator of G_1 . A bilinear pairing is a map e: $G_1 \times G_1 \rightarrow G_2$ having the following three properties:

Bilinear: $e(aP, bQ)= e(P,Q)^{ab}$, for all $P,Q\in G_1$ and ,ab$\in Z^*_q$.

Non-degenerate: $\forall P$ where P is not a generator, there exists $Q\in G_1$ such that $e(P,Q)1$.

Computable: $e(P,Q)$ is computable in polynomial time.

Discrete Logarithm Problem (DLP): Given two elements $P,Q\in G_1$ find an integer $a\in Z^*_q$, such that $Q = aP$ whenever such an integer exists.

Computational Diffie-Hellman Problem (CDHP): Given *(P, aP, bP) for any*, $ab\in Z^*_q$, compute abP.

Decisional Diffie-Hellman Problem (DDHP): Given *(P, aP, bP, cP) for any* $a,b,c\in Z^*_q$,decide whether $c = ab$ mod q.

Gap Diffie-Hellman (GDH) group: G_1 is a *GDH group* if there exists an efficient polynomial time algorithm which solves the *DDHP* in G_1 and there is no probabilistic polynomial time algorithm which solves the *CDHP* in $G_1$with non negligible probability of success.

Bilinear Diffie-Hellman Problem (BDH): Given *(P, aP, bP, cP)* for any $a, b, c\in Z^*_q$, compute $e(P,P)^{abc}$.

3. Review of Manik et al.' scheme

In this section, we briefly review Manik et al.'s scheme. This scheme consists of four phases. Registration phase; Login phase; Authentication phase; and Password change phase. The notations used through out the paper are as follows.

U: User
ID: Identity of the user
PW: Password of user U
RS: Remote Server
H: $\{0, 1\}^* \rightarrow G_1$ is a hash function.
P is generator of G_1
s is a secret key of RS
$Pub_{RS} = sP$ is public key of RS

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 (G1, G2, e, q, P, Pub_{RS}, H) and keeps s secret.

Different phases work as follows

Registration Phase

U submits his identity *ID* and password *PW* to the *RS*

RS computes $\text{Re g}_{ID} = s.H(ID)+H(PW)$

RS personalizes smart card with *ID,* Re g_{ID}, $H(.)$and sends the smart card to U over a secure channel.

Login Phase

User U inserts smart card in a terminal and submits ID and PW .

Smart card computes $DID = T.\mathrm{Re}\ g_{ID}$

$$V = T.H(PW)$$

Sends login request <ID, DID ,V ,T > to the RS over a public channel where T is the user system's time stamp.

Verification phase

RS receives <ID, DID, V, T > at time T^* and verifies the validity of the time interval between T^* and T checking if $(T^* - T) \leq \Delta T$. It accepts the request and checks whether $e(DID - V, P) = e(H(ID), Pub_{RS})^T$

Password change phase

User U inserts smart card into a terminal and submits his identity ID and password PW .Smart card verifies if this ID is same as the ID stored in the smart card.

U submits a new password PW^* .Smart card computes

$$\mathrm{Re}\ g_{ID}^{\ *} = \mathrm{Re}\ g_{ID} - H(PW) + H(PW^*) = s.\ H(ID) + H\ (PW^*)$$

Smart card replaces the previously stored $\mathrm{Re}\ g_{ID}$ value by $\mathrm{Re}\ g_{ID}^{\ *}$

4. Chou et al.'s attack on Manik et al.'s scheme

Chou et al. [14] pointed that the verification in [13] $e(DID - V, P) = e(H(ID), Pub_{RS})^T$ holds valid even when $DID' = DID + a$ and $V' = V + a$ where $a \in G_1$, as shown below.

$$\begin{aligned} e(DID - V, P) &= e(DID + a - V - a, P) \\ &= e(DID - V, P) \\ &= e(H(ID), Pub_{RS})^T \end{aligned}$$

To avoid this, Chou et al [14] proposed different verification technique as $e(DID,P) = e(TsH(ID) + V,P)$ to avoid the subtraction effect of [13].

5. Thulasi et al.'s **attacks**

5.1. On Chou et al.'s scheme

The verification in [13] is modified by Chou et al. [14] as

$e(DID,P) = e(TsH(ID) + V,P)$.

We note that this verification also holds valid for $DID' = DID + a'$ and $V' = V + a'$ where $a' \in G_1$, as shown below.

$$\begin{aligned} e(DID' ,P) &= e(DID + a' ,P) \\ &= e(DID,P)\ e(a' ,P) \\ &= e(TsH(ID) + V,P)\ e(a' ,P) \\ &= e(TsH(ID) + V + a', P) \\ &= e(TsH(ID) + V',P) \end{aligned}$$

Thus the approach of Chou et al., by adding V on the right side instead of left side, cannot solve the problem as shown above.

5.2. Further attacks on Manik et al.'s scheme

Thulasi et al. further point to more attacks on [13].

Forgery attack

Given P and $P_{pub} = sP$, finding s is Discrete Logarithm Problem (DLP) but given x and xQ , it is feasible to compute Q.

In login phase, the tuple $<ID, DID, V, T>$ is being sent to RS over a public channel. Any adversary tapping this message can compute a valid $<ID, DID', V', T'>$.

As $DID = T.\text{Re g}_{ID}$, where $T \in Z^*_q$

$V = T.H(PW)$,

Attacker can compute T^{-1}, Re g_{ID} and $H(PW)$ as below.

$$\text{Re g}_{ID} = T^{-1}DID = T^{-1}T.\text{Re g}_{ID}$$

$$H(PW) = T^{-1}V = T^{-1}T.H(PW)$$

Now, attacker can form the valid tuple $<ID, DID', V', T'>$ for time stamp T' computing:

$$DID' = T'.\text{Re g}_{ID} , \; V' = T'.H(PW).$$

Weakness in Password Change Phase

In the Password Change Phase, User submits ID, old password PW and new password PW^* but there is no verification is done to validate the old password. So anyone knowing the ID and having the smart card can change the secret information Re g_{ID} in the smart card.

6. Our improvement

We propose an improvement for the flaws in the Manik et al.’s scheme. The authentication scheme that we improve on is as follow:

Registration Phase

U submits his identity ID and password PW to the RS

RS computes $\text{Re g}_{ID} = s.H(ID)$.

$H_{PW} = H(PW)$.

RS personalizes smart card with ID, Re g_{ID}, H_{PW}, $H(.)$ and sends the smart card to U over a secure channel.

Login Phase

User U inserts smart card in a terminal and submits ID and PW .

Smart card checks whether $H_{PW} = H(PW)$.if expression is right then Smart card computes:

$DID = T.\text{Re g}_{ID}$

$ET = \text{E}_{PubRS}\,[T]$. where E_{PubRS} is Public key encryption

Sends login request $< ID, DID, ET >$ to the RS over a public channel where T is the user system’s time stamp.

Verification phase

RS receives $<ID, DID, ET>$ at time T^* , first computes $T = \text{E}_s\,[ET]$and verifies the validity of the time interval between T^* and T checking if$(T^* - T) \le \Delta T$. It accepts the request and checks whether $e(DID, P) = e(H(ID), Pub_{RS})^T$ is hold.

Password change phase

User U inserts smart card into a terminal and submits his identity ID and password PW .Smart card verifies if this ID and $H(PW)$ are same as the ID and H_{PW} stored in the smart card.

U submits a new password PW^* .Smart card computes:

$$H_{PW}^* = H(PW^*)$$

Smart card replaces the previously stored H_{PW} value by H_{PW}^*

We prove the improved scheme is secure for the replay attack and forgery attack as following:

Adversary can obtain the $<ID, DID, ET>$ in login phase, but because the s is secrete, so the attacker want to get T from ET is same as figure out Discrete Logarithm Problem (DLP). Also the attacker want to get T from DID is same as figure out Discrete Logarithm Problem (DLP).Therefore the improvement is secure for forgery attack.

7. Conclusion

In this paper, we analyzed both Manik et al.'s scheme and Chou et al.'s scheme. We propose an improvement for the flaws that Thulasi et al. found. And we prove the improved scheme is secure for the replay attack and forgery attack in the end. At the same time, we overcome the weakness in Password Change Phase.

References

[1] L. Lamport, "*Password Authentication with Insecure Communication*", Communications of the ACM, vol. 24, no. 11, pp 770-772, 1981.

[2] C. C. Chang and W. Y. Liao. *"A remote password authentication scheme based upon ElGamal's signature scheme"*, Computers & Security, vol. 13, no. 2, pp.137-144, 1994.

[3] D. P. Jablon. *"Strong password-only authenticated key exchange"*, ACM Computer Communications Review, vol.26, no. 5, pp.5-20, 1996.

[4] A. Shimizu, T. Horioka and H. Inagaki. *"A Password Authentication Method for Contents Communications on the Internet"*, IEICE Trans. On Commun., vol.E81-B, no. 8, pp.1666-1673, 1998.

[5] M. S. Hwang and L. H. Li. *"A New Remote User Authentication Scheme Using Smart Cards"*, IEEE Trans. On Consumer Electron., vol. 46, no.1, pp.28-30,2000.

[6] C. C. Lee, M. S. Hwang and W. P. Yang *"A flexible remote user authentication scheme using smart cards"*, ACM Operating Systems Review, vol. 36, no. 3, pp.46-52, 2002.

[7] T. C. Yeh, H. Y. Shen and J. J. Hwang. *"A Secure One-Time Password Authentication Scheme Using Smart Cards"*, IEICE Trans. on Commun.vol.E85-B, no. 11, pp. 2515-2518, 2002.

[8] C. C. Lee, L. H. Li, M. S. Hwang. *"A Remote User Authentication Scheme Using Hash Functions"*, ACM Operating Systems Review, vol. 36, no. 4, pp. 23-29, 2002.

[9] J. J. Shen, C. W. Lin, M. S. Hwang. *"A Modified Remote User Authentication Scheme Using Smart Cards"*, IEEE Trans. On Consumer Electron,vol. 49, no. 2,pp.414-416, 2003.
[10] A. K. Awasthi, S. Lal. *"A Remote User Authentication Scheme Using Smart Cards with Forward Secrecy"*, IEEE Trans. On Consumer Electron., vol.49,no. 4,pp.1246-1248, 2003.
[11] Manik. L. Das, Ashutosh Saxena and V. P. Gulati. *"A Dynamic ID-based Remote User Authentication Scheme"*, IEEE Trans. On Consumer Electron., vol. 50, no.2,pp.629-631, 2004.
[12] W. C. Ku. *"A Hash-Based Strong-Password Authentication Scheme without Using Smart Cards"*, ACM Operating Systems Review, vol. 38, no. 1, pp. 29-34,2004.
[13] Manik. L. Das, Ashutosh Saxena, V. P. Gulati, D. B. Phatak *"A novel remote user authentication scheme using bilinear pairings"*, Computers & Security (In Press),2005.
[14] J. S. Chou, Y. Chen, J. Y. Lin "*Improvement of Manik et al.'s remote user authentication scheme"*, http://eprint.iacr.org/2005/450.pdf
[15] **G. Thulasi**, **Manik Lal Das**, **Ashutosh Saxena** "Cryptanalysis of recently proposed Remote User Authentication Schemes", http://eprint.iacr.org/2006/028.pdf