A New Secure Mutual Authentication Scheme with Smart Cards Using Bilinear Pairings

Hae-Jung Kim
College of Liberal Education, Keimyung University
Daegu 704-701, Republic of Korea

Eun-Jun Yoon
Department of Cyber Security, Kyungil University
Kyungsangpuk-Do 712-701, Republic of Korea

Ki-Dong Bu
Department of Computer Engineering, Kyungil University
Kyungsangpuk-Do 712-701, Republic of Korea

Copyright © 2014 Hae-Jung Kim, Eun-Jun Yoon and Ki-Dong Bu. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Abstract

Mutual authentication is an important security property for providing secure remote communication in client-server environment. Up to now, various remote user authentication schemes with smart card using bilinear pairings were proposed by different researchers. Unfortunately, most previously proposed authentication schemes do not provide mutual authentication and session key agreement. This paper proposes a new secure mutual authentication scheme with smart cards using bilinear pairings. It can not only achieve strong security, resist the strong variant of security attacks but also retain most previously proposed practical merits.

1Corresponding author
Keywords: Mutual authentication; Smart card; Bilinear pairings; Cryptanalysis, Password

1 Introduction

Mutual authentication is important for providing secure remote communication in client-server environment. Smart card and password based remote authentication scheme is one of the most significant two-factor mechanisms to achieve the strong security requirements.

In 2005, Das et al. [1] proposed a remote user authentication scheme with smart card using bilinear pairings that provides the users to choose and change their passwords by their own choices. In 2006, Fang et al. [2] proposed an improvement over Das et al.’s scheme to remedy security weaknesses. However, Giri et al. [3] proposed another improvement over Fang et al.’s scheme to provide strong security. In 2012, Awasthi [4] showed some attacks on Giri et al.’s scheme and then proposed an improved protocol that provides the better security as compared to the schemes previously discussed.

Unfortunately, most previously proposed authentication schemes do not provide mutual authentication and session key agreement. This paper proposes a new secure mutual authentication scheme with smart cards using bilinear pairings. It can not only achieve strong security, resist the strong variant of security attacks but also retain most previously proposed practical merits.

This paper is organized as follows: Section 2 demonstrates our proposed scheme. The correctness proof and security analyses are in Section 3. Finally, the conclusion is given in Section 4.

2 Proposed Mutual Authentication Scheme

This section proposes a secure mutual authentication scheme with smart cards using bilinear pairings. The proposed scheme consists of four phases: setup, registration, mutual authentication, and password change phases.

2.1 Setup phase

The setup phase proceeds as follows by the remote server $RS$.

1. $RS$ selects two groups: $G_1$ as an additive cyclic group of order prime $q$ and $G_2$ as a multiplicative cyclic group of the same order.

2. $RS$ defines a function $e : G_1^2 \rightarrow G_2$ is a bilinear mapping and $H(\cdot) : \{0,1\}^* \rightarrow G_1$ is a cryptographic hash function.
3. RS defines a secure one-way hash function $h(\cdot) : \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$.

4. RS chooses randomly a secret key (private key) $s$ and computes the public-key as $Pub_{RS} = sP$, where $P$ is a generator of the group $G_1$.

5. RS publishes the system parameters $(G_1, G_2, q, Pub_{RS}, e, H(\cdot))$ and keeps the parameter $s$ as secret.

### 2.2 Registration phase

A user $U_i$ submits his/her identifier $ID_i$ and password $PW_i$ to the RS. These private data must be sent over a secure channel. RS performs the following steps to issue the smart card to the user $U_i$.

1. Compute a secret parameter $SP_i = PW_i Pub_{RS}$.

2. Compute registration identifier of the user $U_i$ as $Reg_{ID_i} = sH(ID_i) + SP_i$.

3. Load $Pub_{RS}, ID_i, Reg_{ID_i}, h(SP_i)$, and $H(\cdot)$ in the memory of the smart card and issues the card to $U_i$.

### 2.3 Mutual authentication phase

Authentication phase is divided in two sub-phases: (1) the login phase and (2) the verification phase.

#### 2.3.1 Login phase

If the user $U_i$ wants to log into the RS, he/she must insert his/her smart card into a card reader and keys in his/her identifier $ID_i$ and password $PW_i$. Then the smart card performs the following steps:

1. Compute $A = PW_i Pub_{RS}$.

2. Compute $B = Reg_{ID_i} - A$.

3. Randomly select a number $r$ and compute $C = rP + B$.

4. Compute $D = TB + r Pub_{RS}$, where $T$ is the user system’s current timestamp.

5. sends the login request message $M = < ID_i, C, D, T >$ to the RS over a public channel.
Insert the smart card
Input $ID_i$ and $PW_i$
Compute $A = PW_i Pub_{RS}$
Compute $B = Reg_{ID_i} - A$
Select random number $r$
Compute $C = rP + B$
Generate current timestamp $T$
Compute $D = TB + rPub_{RS}$
\[
\{ID_i, C, D, T\} \rightarrow \text{Check } (T' - T) \geq \Delta T
\]
\[
\text{Check } e(D - sX, P) = e(H(ID_i), Pub_{RS})^T
\]
Select random number $t$
Compute $Y = tP$
Compute $sk = tX$
Compute $Z = h(sH(ID_i), sk, T)$
\[
\{Y, Z\} \leftarrow \text{Compute } sk = rY
\]
Check $Z = h(B, sk, T)$

Common session key $sk = rtP$

---

2.3.2 Verification phase

Assume that the $RS$ receives the login request message $M = < ID_i, C, D, T >$ at time $T'$, the $RS$ and the smart card perform the following steps for mutual authentication between the user $U_i$ and the $RS$.

1. $RS$ verifies the validity of the time interval between $T'$ and $T$. If $(T' - T) \geq \Delta T$, then the $RS$ rejects the login request, where $\Delta T$ denotes the expected valid time interval for transmission delay. Otherwise, it goes for the next step.

2. $RS$ computes $X = C - sH(ID_i)$. 

Figure 1: Mutual authentication phase
3. RS checks whether $e(D - sX, P) \overset{?}{=} e(H(ID_i), Pub_{RS})^T$. If it holds, the RS accepts the login request; otherwise, rejects it.

4. RS randomly selects a number $t$ and computes $Y = tP$.

5. RS computes the common session key $sk = tX$ and $Z = h(sH(ID_i), sk, T)$

6. RS forwards the message $< Y, Z >$ to $U_i$.

7. After receiving the message $< Y, Z >$, the user $U_i$ computes the common session key $sk = rY$.

8. $U_i$ checks $Z = h(B, sk, T)$. If it holds, the user believes the trustworthy of RS.

After finishing the mutual authentication, both the user $U_i$ and the remote server RS uses the common session key $sk = rtP$ for their subsequent communication.

2.4 Password change phase

If the user $U_i$ wants to change his/her password from $PW_i$ to $PW_i^{new}$, he/she should insert his/her smart card into a card reader and keys in his/her identifier $ID_i$, old password $PW_i$, new password $PW_i^{new}$. Then the smart card performs the following steps:

1. Compute $SP_i' = PW_i Pub_{RS}$.

2. Check the validity $h(SP_i) \overset{?}{=} h(SP_i')$. If valid, it computes $Reg_{ID_i^{new}} = sH(ID_i) + SP_i^{new}$, where $SP_i^{new} = PW_i^{new} Pub_{RS}$

3. Load $Pub_{RS}, ID_i, Reg_{ID_i^{new}}$ and $H(\cdot)$ in the memory of the smart card and issue the card to $U_i$.

3 Correctness Proof and Security Analysis

This section provides a security and performance analysis of the proposed mutual authentication scheme.
3.1 Correctness proof

The above Step 3 in the verification phase is verified by the following:

\[ e(D-sX, P) = e(TB + rPub_RS - sX, P) \]
\[ = e(TB + rPub_RS - s(C - sH(ID_i)), P) \]
\[ = e(TB + rPub_RS - s(rP + B - sH(ID_i)), P) \]
\[ = e(TB + rPub_RS - s(rP + RegID_i - A - sH(ID_i)), P) \]
\[ = e(TB + rPub_RS - s(rP + sH(ID_i) + SP_i - SP_i - sH(ID_i)), P) \]
\[ = e(TB + rPub_RS - s(rP), P) \]
\[ = e(TB + rPub_RS - rsP, P) \]
\[ = e(TB + rPub_RS - rPub_RS, P) \]
\[ = e(TB, P) \]
\[ = e(T(RegID_i - A), P) \]
\[ = e(T(sH(ID_i) + SP_i - SP_i), P) \]
\[ = e(TsH(ID_i), P) \]
\[ = e(TH(ID_i), sP) \]
\[ = e(H(ID_i), Pub_RS)^T \]

(1)

3.2 Security analysis

In replay attack, an attacker can attempt to record an exchanged message. However, the replay of the old request message \( M = \langle ID_i, C, D, T \rangle \) sent by user fails because the validity of these messages can be checked through the timestamp. Let us assume that an attacker traps a valid message \( M = \langle ID_i, C, D, T \rangle \) sent by the user \( U_i \). If the attacker tries to forge the request message \( M \), attacker must compute \( s \). But, it is computationally infeasible to compute \( s \) from given \( P \) and \( Pub_RS \) due to Discrete Logarithm Problem (DLP). The proposed scheme achieves mutual authentication between the user and the remote server by computing the common session key \( sk = rtP \). The proposed scheme uses the Elliptic Curve Diffie-Hellman key exchange to provide mutual authentication for the user and the remote server.

4 Conclusions

In client-server communication environments, secure mutual authentication is an important security property for providing secure remote communication between the user and the remote server. This paper proposed a new secure
mutual authentication scheme with smart cards using bilinear pairings. The proposed scheme can not only achieve strong security including mutual authentication, resist the strong variant of security attacks but also retain most previously proposed practical merits.

Acknowledgements

This work was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education, Science and Technology(No. 2010-0010106).

References


Received: September 6, 2014