Available online at www.sciencedirect.com
ScienceDirect
Computer Standards & Interfaces 31 (2009) 181 – 185
COMPUTER STANDARDS & INTERFACES
www.elsevier.com/locate/csi

An improved bilinear pairing based remote user authentication scheme

Thulasi Goriparthi [a,1], Manik Lal Das [b,1], Ashutosh Saxena [c,*,1]

[a] University of Hyderabad, Gachibowli, Hyderabad 500046, India
[b] Dhirubhai Ambani Institute of Information and Communication Technology, Gandhinagar, Ahmedabad 382007, India
[c] SETLabs, Infosys Technologies Limited, Hyderabad DC, Survey No.210, Lingampally, Hyderabad 500019, India

Received 18 April 2006; received in revised form 31 October 2007; accepted 18 November 2007
Available online 5 December 2007

Abstract

Recently Das et al. proposed a novel remote user authentication scheme using bilinear pairings. Chou et al. identified a weakness in Das et al.'s scheme and made an improvement. In this paper, we show that both Das et al.'s and Chou et al.'s schemes are insecure against forgery and replay attacks. We proposed an improved scheme that overcomes the security flaws without affecting the merits of the original scheme.

Keywords: Authentication; Bilinear pairings; Smart Card; Password; Timestamp

1. Introduction

Remote User Authentication scheme allows the authenticated user to access the services offered by the remote system. Lamport [1] introduced the first well-known hash-based password authentication scheme, but the scheme suffers from high hash computation overhead and password resetting problems. Thereafter, many authentication schemes have been proposed based on hashed password [2–7] and on public key cryptography [4,5,8–12]. It is observed that, many times, a paper typically breaks a previous scheme and proposes a new one [4,5,7,13,16], which someone breaks later and, in turn, proposes a new one, and so on. Most of such work, though quite important and useful, essentially provides an incremental advance to the same basic theme [14].

Recently, Das et al. [6] proposed a remote user authentication scheme using bilinear pairings. In their scheme, timestamps are used to avoid replay attacks while sending the login request over a public channel. Chou et al. [15] identified that the verification of Das et al.'s scheme involves subtraction of two components, which are passed over a public channel and can lead to replay attack. The replay attack can be performed by adding the same information to the two components while still retaining a valid verification. To overcome replay attack, Chou et al. suggested a modification in the verification part of Das et al.'s scheme. However, we observed that the modified scheme by Chou et al. still suffer from the replay attack. This paper cryptanalyzes Das et al.'s and Chou et al.'s schemes and then proposes an improved scheme, which is resilient to the forgery and replay attacks.

The organization of the paper is as follows. In Section 2, we present the preliminaries of bilinear pairings, complexity assumptions and notations used in the paper. In Section 3, Das et al.'s scheme is briefly reviewed. Chou et al.'s attack on Das et al.'s scheme is reviewed in Section 4. In Section 5, we cryptanalyze the Chou et al.'s and Das et al.'s schemes. Section 6 presents our scheme. Section 7 analyses the security of the proposed scheme. We conclude the paper in Section 8.

2. Preliminaries

2.1. Relevance to the computer standards

User authentication is a common practice to verify users before allowing access to enterprise/server resource. Password-based authentication system plays an important role for

* Corresponding author.
E-mail addresses: thulasi@dcis.uohyd.ernet.in (T. Goriparthi), maniklal.das@ieee.org (M. Lal Das), ashutosh_saxena01@infosys.com (A. Saxena).
[1] Part of this work was done when all authors were affiliated to Secure Technology Lab., Institute for Development and Research in Banking Technology, Hyderabad 500057, India, and acknowledge it.

0920-5489/$ - see front matter © 2007 Elsevier B.V. All rights reserved.
doi:10.1016/j.csi.2007.11.016

user authentication, but due to dictionary attack of memorized password, now-a-days, password and a token combination acts as a secure authentication mechanism, which is termed as "two-factor authentication" [19], adopted by several industry, academia and Government agencies. In contrast, public key-based authentication technique [17] has already been applied in various applications, such as Secure Socket Layers [20], Pretty Good Privacy [18], etc. As a consequence, user authentication is a de-facto standard and requirement in computer and information systems, ranging from boarder security to consumer electronics.

2.2. 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 $a,b, \in Z_q^*$.
Non-degenerate: For all P, where P is not a generator, there exists $Q \in G_1$ such that $e(P,Q) \neq 1$.
Computable: $e(P,Q)$ is computable in polynomial time.

2.3. Complexity assumptions

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 $a,b \in Z_q^*$, *compute abP.*

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

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 $e(P,P)^{abc}$.

2.4. Notations

The notations used through out the paper are as follows.

U	User
ID	Identity of U
PW	Password of U
RS	Remote Server
$H: \{0,1\}^* \rightarrow G_1$	A map-to-point hash function.
P	Generator of G_1
S	Secret key of RS
P_{pub}	Public key of RS, where $P_{pub}=sP$
$h; \{0,1\}^* \rightarrow Z_q^*$	One way hash function
$\|\|$	Concatenation operation

3. Review of Das et al.'s scheme

In this section, we briefly review Das et al.'s scheme. The scheme consists of four different phases and they work as follows

3.1. Registration phase

R1. U submits his identity ID and password PW to the RS
R2. RS computes $Re\ g_{ID}=sH(ID) + H(PW)$
R3. RS personalizes smart card with ID, $Re\ g_{ID}$, $H(.)$ and sends the smart card to U in a secure manner.

3.2. Login phase

L1. U inserts smart card in a terminal and submits ID and PW.
L2. Smart card computes $DID=T\ Re\ g_{ID}$ and $V=TH(PW)$
L3. Sends login request $<ID,DID,V,T>$ to RS over a public channel where T is the user system's timestamp.

3.3. Verification phase

V1. RS receives $<ID,DID,V,T>$ at time T^* and verifies the validity of the time interval between T^* and T, by checking if $(T^* - T) \leq \Delta T$. If it holds, checks whether $e(DID\text{-}V,P)=e(H(ID),P_{pub})^T$. If both checks hold, RS accepts the login request, rejects otherwise.

3.4. Password change phase

P1. U inserts smart card in a terminal and submits ID and password PW. Smart card verifies the entered ID with the stored one in the smart card. If ID is matched, it prompts U for a new password. U submits a new password PW^*.
P2. Smart card computes $Re\ g_{ID}^* = Re\ g_{ID}\text{-}H(PW) + H(PW^*) = sH(ID) + H(PW^*)$
P3. Smart card replaces the previously stored $Re\ g_{ID}$ by $Re\ g_{ID}^*$

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

Chou et al. pointed out that the verification in Das et al.'s scheme $e(DID\text{-}V,P) = e(H(ID),P_{pub})^T$ holds valid even with $DID' = DID + a$ and $V' = V + a$ where $a \in G_1$, as shown below.

$$e\Big(DID' - V', P\Big) = e(DID - V, P) = e(H(\mathrm{ID}), P_{\mathrm{pub}})^T$$

To avoid this, Chou et al. proposed a modified verification technique as $e(DID,P) = e(TsH(ID) + V,P)$ to overcome the defect in verification of Das et al.'s scheme.

5. Cryptanalysis of Chou et al.'s and Das et al.'s schemes

Chou et al. identified that the verification of Das et al.'s scheme involves subtraction of two components, which are passed over the public channel leading to replay attack. The