Computers & Security (2006) **25**, 184–189

ELSEVIER

Computers & Security

www.elsevier.com/locate/cose

A novel remote user authentication scheme using bilinear pairings

Manik Lal Das [a,b,*], **Ashutosh Saxena** [a], **Ved P. Gulati** [a], **Deepak B. Phatak** [b]

[a] *Institute for Development and Research in Banking Technology, Castle Hills, Road Number 1, Masab Tank, Hyderabad-500057, India*
[b] *K. R. School of Information Technology, Indian Institute of Technology, Mumbai-400076, India*

Received 20 January 2005; revised 16 August 2005; accepted 23 September 2005

KEYWORDS
Authentication;
Bilinear pairings;
Smart card;
Password;
Timestamp

Abstract The paper presents a remote user authentication scheme using the properties of bilinear pairings. In the scheme, the remote system receives user login request and allows login to the remote system if the login request is valid. The scheme prohibits the scenario of *many* logged in users with the *same* login-ID, and provides a flexible password change option to the registered users without any assistance from the remote system.

Introduction

Password authentication is an important technique to verify the legitimacy of a user. The technique is regarded as one of the most convenient methods for remote user authentication. Based on the computation complexity, password-based authentication schemes are classified into two broad categories, viz. hash-based (Menezes et al., 1996) authentication and public-key based authentication (IEEE P1363.2 Draft D12, 2003).

In 1981, Lamport introduced the first well-known hash-based password authentication scheme. Lamport's scheme suffers from high hash overhead and password resetting problems. Later, Shimizu et al. (1998) overcome the weakness of Lamport (1981) and proposed a modified scheme. Thereafter, many schemes and improvements (Lee et al., 2002; Peyravian and Zunic, 2000; Ku et al., 2003; Ku, 2004) on hash-based remote user authentication, have been proposed. These schemes take low computation cost and are computationally viable for implementation in a handheld device like smart card; however, the schemes primarily suffer from password guessing, stolen-verifier and

* Corresponding author. Institute for Development and Research in Banking Technology, Castle Hills, Road Number 1, Masab Tank, Hyderabad-500057, India. Tel.: +91 40 2353 4981; fax: +91 40 2353 5157.
E-mail addresses: mdas@it.iitb.ac.in, mldas@idrbt.ac.in (M. L. Das), asaxena@idrbt.ac.in (A. Saxena), vpgulati@idrbt.ac.in (V.P. Gulati), dbp@it.iitb.ac.in (D.B. Phatak).

0167-4048/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2005.09.002

denial-of-service attacks (Ku et al., 2003; Hsieh et al., 2003). In contrast, public-key based authentication schemes require high computation cost for implementation, but meet higher security requirements. So far, several research works on public-key based remote user authentication (Chang and Wu, 1993; Chang and Liao, 1994; Hwang and Yeh, 2002; Shen et al., 2003) have been done. Unfortunately, many times, a paper typically breaks a previous scheme and proposes a new one (Ku et al., 2003; Hsieh et al., 2003), 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 (Peyravian and Zunic, 2000).

Recently, the bilinear pairings (Boneh and Franklin, 2001), namely the Weil pairing and the Tate pairing of algebraic curves have been found as important applications (Boneh and Franklin, 2001; Hess, 2003) in cryptography and allowed us to construct identity (ID) based cryptographic schemes. In 1984, Shamir introduced the concept of ID-based cryptosystem; however, the practical ID-based schemes (Boneh and Franklin, 2001; Cocks, 2001) were found in 2001.

In this paper, we present a remote user authentication scheme using the properties of bilinear pairings. In our scheme, the user is assigned a smart card, which is being personalized by some parameters during the user registration process. The use of smart card not only makes the scheme secure but also prevents the users from distribution of their login-IDs, which effectively prevents the scenario of *many* logged in users with the *same* login-ID. The characteristics of our scheme are summarised as follows:

- The user's smart card generates a dynamic login request and sends it to the remote system for login to the system. The login request is computed by the smart card internally without any human intervention and the login request is composed by the user system's timestamp. Thus, an adversary cannot predict the next login request with the help of current login request.
- The users can choose and change their preferred passwords freely without any assistance from the remote system. During the user registration process, the remote system stores a secret component and other parameters in a smart card, and then sends it to the user securely. With the help of the smart card and its secret component the user can change his password without any assistance from remote system.
- The remote system does not maintain any password or verifier table for the verification of user login request. The login request verification requires user identity, remote system public-key corresponding to the remote system's secret key.
- The scheme prevents the scenario of *many* logged in users with the *same* login-ID. Typically, a registered user can share his password or secret component with others, thus all who know the password or secret component with respect to the user's login-ID, can login to the remote system. This generally happens in digital library, where a subscriber can share his login-ID and password with others, and many users (who knows login-ID and password) can download or view the digital document. In our scheme, the login request is generated by the smart card using its stored secret component without any human intervention. It is extremely difficult to extract the secret component from the smart card, and thus the user cannot share it with others. Even if the legitimate user's password is shared with others, the other person cannot login to the system without the smart card. Once a valid user logs into the remote system, his smart card will be inside the terminal until the user logs out. If the user pulls out the card from the terminal after login the remote system, the login session will be immediately expired. Thus, the scheme can successfully prevent the scenario of many logged in users with the same login-ID.
- The scheme can resist the replay, forgery and insider attacks.

The rest of the paper is organised as follows. In the next section, we give some preliminaries of bilinear pairings. In the section following that, we propose our scheme and analyse the scheme in Section Correctness, performance and security. Finally we conclude the paper in last section.

Preliminaries

Bilinear pairings

Suppose 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. A map $\hat{e}: G_1 \times G_1 \to G_2$ is called a bilinear mapping if it satisfies the following properties:

1. Bilinear: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in G_1$ and $a, b \in Z_q^*$.