Journal of Network and Computer Applications 34 (2011) 609–618

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

journal homepage: www.elsevier.com/locate/jnca

A secure dynamic identity based authentication protocol for multi-server architecture

Sandeep K. Sood *, Anil K. Sarje, Kuldip Singh

Department of Electronics & Computer Engineering, Indian Institute of Technology, Roorkee, India

ARTICLE INFO

Article history:
Received 13 June 2010
Received in revised form
22 October 2010
Accepted 18 November 2010
Available online 30 November 2010

Keywords:
Authentication protocol
Smart card
Dynamic identity
Password
Multi-server architecture

ABSTRACT

Most of the password based authentication protocols rely on single authentication server for the user's authentication. User's verification information stored on the single server is a main point of susceptibility and remains an attractive target for the attacker. In 2009, Hsiang and Shih improved Liao and Wang's dynamic identity based smart card authentication protocol for multi-server environment. However, we found that Hsiang and Shih's protocol is susceptible to replay attack, impersonation attack and stolen smart card attack. Moreover, the password change phase of Hsiang and Shih's protocol is incorrect. This paper presents a secure dynamic identity based authentication protocol for multi-server architecture using smart cards that resolves the aforementioned security flaws, while keeping the merits of Hsiang and Shih's protocol. It uses two-server paradigm in which different levels of trust are assigned to the servers and the user's verifier information is distributed between these two servers known as the service provider server and the control server. The service provider server is more exposed to the clients than the control server. The back-end control server is not directly accessible to the clients and thus it is less likely to be attacked. The user's smart card uses stored information in it and random nonce value to generate dynamic identity. The proposed protocol is practical and computationally efficient because only nonce, one-way hash functions and XOR operations are used in its implementation. It provides a secure method to change the user's password without the server's help. In e-commerce, the number of servers providing the services to the user is usually more than one and hence secure authentication protocols for multi-server environment are required.

1. Introduction

Smart cards have been widely used in many e-commerce applications and network security protocols due to their low cost, portability, efficiency and the cryptographic properties. Smart card stores some sensitive data corresponding to the user that assist in user authentication. The user (card holder) inserts his smart card into a card reader machine and submits his identity and password. Then smart card and card reader machine perform some cryptographic operations using submitted arguments and the data stored inside the memory of smart card to verify the authenticity of the user.

Most of the existing password authentication protocols are based on single-server model in which the server stores the user's password verifier information in its database. Password verifier information stored on the single server is mainly susceptible to stolen verifier attack. The concept of multi-server model removes this common point of susceptibility. The Protected Extensible Authentication Protocol jointly developed by Cisco Systems, Microsoft and RSA Security is the most widely used authentication protocol. It encapsulates the Extensible Authentication Protocol within an encrypted and authenticated Transport Layer Security (TLS) tunnel. This protocol is included with Microsoft Windows XP and Windows 7 operating systems. It is based on the single server authentication concept. On the other hand, Kerberos is the multi-server authentication protocol. The limitation of Kerberos protocol is that all the servers are equally exposed to the user. The proposed protocol uses multi-server model consisting of two servers that work together to authenticate the users. Yang et al. (2006) also suggested similar kind of two-server model for user's authentication. In the proposed protocol, different levels of trust are assigned to the servers and the service provider server is more exposed to the clients than that of the control server. The back-end control server is not directly accessible to the clients and thus it is less likely to be attacked. Two-server model provides the flexibility to distribute user passwords and the authentication functionality into two servers to eliminate the main point of vulnerability of the single-server model. Therefore, two-server model appears to be a reasonable choice for practical applications.

In a single server environment, the issue of remote login authentication with smart cards has already been solved by a variety of

* Corresponding author. Tel.: +91 1894276861.
E-mail addresses: san1198@gmail.com, ssooddec@iitr.ernet.in (S.K. Sood), sarjefec@iitr.ernet.in (A.K. Sarje), ksconfcn@iitr.ernet.in (K. Singh).

1084-8045/$ - see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.jnca.2010.11.011

schemes (Das et al., 2004; Chien and Chen, 2005; Liao et al., 2005; Yoon and Yoo, 2006; Liou et al., 2006). These conventional single-server password authentication protocols cannot be directly applied to multi-server environment because each user needs to remember different sets of identities and passwords. Different protocols have been suggested to access the resources of multi-server environment (Yang et al., 2006; Ford and Kaliski, 2000; Jablon, 2001; Lee and Chang, 2000; Li et al., 2001; Lin et al., 2003; Raimondo and Gennaro, 2003; Brainard et al., 2003; Juang, 2004; Chang and Lee, 2004; Hu et al., 2007; Tsaur et al., 2004; Yang et al., 2005; Mackenzie et al., 2006; Tsai, 2008; Liao and Wang, 2009; Hsiang and Shih (2009)). A secure and efficient remote user authentication protocol for multi-server environment should provide mutual authentication, key agreement, secure password update, low computation requirements and resistance to different feasible attacks.

Password is the most commonly used authentication technique in authentication protocols. Low entropy password makes system susceptible to dictionary attack. A number of static identity based remote user authentication protocols have been proposed to improve security, efficiency and cost. The user may change his password but cannot change his identity in password authentication protocols. During communication, the static identity leaks out partial information about user's authentication messages to the attacker. Most of the password authentication protocols for multi-server environment are based on static identity and the attacker can use this information to trace and identify the different requests belonging to the same user. On the other hand, the dynamic identity based authentication protocols provide two-factor authentication based on the identity and password and hence more suitable to e-commerce applications. The aim of this paper is to provide a dynamic identity based secure and computational efficient authentication protocol with user's anonymity for multi-server environment using smart cards. It protects user's identity in insecure communication channel and hence can be applied directly to e-economic applications.

This paper is organized as follows. In Section 2, we explore the literature on existing dynamic identity based authentication protocols using smart cards and authentication protocols for multi-server environment. Section 3 reviews the dynamic identity based remote user authentication protocol for multi-server environment proposed by Hsiang and Shih (2009). Section 4 describes the susceptibility of Hsiang and Shih's protocol to replay attack, impersonation attack and stolen smart card attack. In Section 5, we present dynamic identity based authentication protocol for multi-server architecture using smart cards. Section 6 discusses the security analysis of the proposed protocol. The comparison of the cost and functionality of the proposed protocol with other related protocols is shown in Section 7. Section 8 concludes the paper.

2. Related work

A number of smart card based remote user authentication protocols have been proposed due to the convenience and secure computation provided by the smart cards. However, most of these protocols do not protect the user's identities in authentication process. User's anonymity is an important issue in many e-commerce applications. Therefore in 2004, Das et al. proposed a dynamic identity based remote user authentication protocol to authenticate the users that preserves the user's anonymity. Their protocol uses dynamic identity to achieve this purpose and user's identity is dynamically changed during each new authentication process. The server does not require to keep any verification table and the users can choose and change their passwords without server's help. Das et al. claimed that their protocol is secure against stolen verifier attack, replay attack, forgery attack, guessing attack, insider attack and identity theft. However, many researchers Chien and Chen (2005); Liao et al. (2005); Yoon and Yoo (2006); Liou et al. (2006); Shih (2008) demonstrated susceptibility of Das et al.'s protocol to different attacks. In 2005, Chien and Chen pointed out that Das et al.'s protocol fails to preserve the user anonymity effectively because the authentication messages belonging to the same user can be identified. They proposed an authentication protocol and claimed that the proposed protocol preserves user's anonymity more efficiently. Though their protocol preserves user's anonymity and secure against various attacks but it is highly computation intensive. In 2005, Liao et al. proposed an improved protocol that enhances the security of Das et al.'s protocol and achieves mutual authentication. In 2006, Yoon and Yoo demonstrated a reflection attack on Liao et al.'s protocol that breaks the mutual authentication. They also proposed an improved dynamic identity based mutual authentication protocol that eliminates the security flaws of Liao et al.'s protocol. In 2006, Liou et al. suggested a new dynamic identity based remote user authentication protocol using smart cards that achieves mutual authentication. They claimed that their protocol preserves the advantages of Das et al.'s protocol and overcomes the weaknesses of Das et al.'s protocol. In 2008, Shih demonstrated that Liou et al.'s protocol fails to achieve mutual authentication.

In 2000, Ford and Kaliski proposed the first multi-server password based authentication protocol that splits a password among multiple servers. This protocol generates a strong secret with the help of password based on the communications exchanges with two or more independent servers. The attacker cannot compute the strong secret unless all the servers are compromised. This protocol is highly computation intensive due to the use of public keys by the servers. Moreover, the user requires a prior secure authentication channel with the server. Therefore in 2001, Jablon improved this protocol and proposed multi-server password authentication protocol in which the servers do not use public keys and the user does not require prior secure communication channels with the servers. In 2000, Lee and Chang proposed a user identification and key distribution protocol for multi-server environment based on the hash function and difficulty of factorization. In 2001, Li et al. proposed a remote password authentication protocol for multi-server environment. This password authentication system is a pattern classification system based on an artificial neural network. The user has to register with registration center once and then can obtain services from multiple servers without needing to register individually with each server. The users can choose their passwords freely and the server does not require to keep any verification table. This protocol can withstand the replay attack effectively but it requires intensive communication and computation efforts.

In 2003, Lin et al. proposed a multi-server authentication protocol based on the ElGamal digital signature scheme that uses simple geometric properties of the Euclidean and discrete logarithm problem concept. The server does not require to keep any verification table but the use of public keys makes this protocol computation intensive. In 2003, Raimondo and Gennaro proposed two multi-server password authentication protocols in which the user has to communicate in parallel with all authentication servers. They proved that these protocols are provable secure in the standard model. The attacker has to compromise minimum threshold number of servers to gain any meaningful information regarding the password of the user. These two protocols differ in the way the client interacts with the different servers. In these protocols, the servers are equally exposed to the user as well as to the attacker. In 2003, Brainard et al. proposed a password based two-server authentication protocol in which only one server was exposed to the users. The use of public keys makes this system computationally intensive. Moreover, it uses Secure Socket Layer (SSL) to establish a session key between a user and the front-end server to provide authentication but it provides only unilateral authentication.