available at www.sciencedirect.com

ScienceDirect

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

Computers & Security

A Secure Identification and Key agreement protocol with user Anonymity (SIKA)

Kumar Mangipudi[1,*], *Rajendra Katti*

Department of Electrical and Computer Engineering, North Dakota State University, Fargo, ND 58102, USA

ARTICLE INFO

Article history:
Received 11 March 2005
Revised 6 March 2006
Accepted 19 May 2006

Keywords:
User identification
Authentication
Key agreement
Anonymity
RSA
Denial-of-Service (DoS) attack

ABSTRACT

Anonymity is a desirable security feature in addition to providing user identification and key agreement during a user's login process. Recently, Yang et al., proposed an efficient user identification and key distribution protocol while preserving user anonymity. Their protocol addresses a weakness in the protocol proposed by Wu and Hsu. Unfortunately, Yang's protocol poses a vulnerability that can be exploited to launch a Denial-of-Service (DoS) attack. In this paper, we cryptanalyze Yang's protocol and present the DoS attack. We further secure their protocol by proposing a Secure Identification and Key agreement protocol with user Anonymity (SIKA) that overcomes the above limitation while achieving security features like identification, authentication, key agreement and user anonymity.

1. Introduction

Whenever a user wants to establish a secure communication channel with the server, he initiates a service request during the login process. The server first identifies the user and then checks for the legitimacy of the user. Upon a successful identification they then negotiate a shared session key to secure the rest of the communication. Until now, numerous authentication and key agreement protocols employing a wide range of cryptography techniques have been proposed. Among them, Kerberos (Kohl and Neuman, 1993), SSL (Secure Sockets Layer) (Freier et al., 1996) and X.509 an authentication framework (ITU-T, 1997) are used to facilitate the user identification, mutual authentication and key exchange during a user's login process. Some of the other widely studied protocols that achieve similar functionalities are password based and are often referred as Password Authenticated Key Exchange (PAKE) protocols (Bellovin and Merrit, 1992; Bellare et al., 2000; Boyko et al., 2000; Katz et al., 2001; Goldreich and Lindell, 2001; Girault, 1991).

Transmitting the user's private information during a login process may be a cause of concern. This is because the sensitive information such as shopping patterns, individual preferences, etc., can be abused for marketing purposes (Bao and Deng, 2001) resulting in violation of user's privacy and can raise legal issues. As such user anonymity is a desirable security feature while requesting and accessing services. Unfortunately, user anonymity was not addressed in earlier authentication and key agreement protocols.

In 2000, Lee and Chang proposed a user identification and key distribution protocol that attains user anonymity based on public key cryptography (RSA) and hash functions.

* *Corresponding author*. Intel Corporation, 2111 NE 25th Avenue, Hillsboro, OR 97124, USA. Tel.: +1 503 712 4200.
E-mail address: narasimha.kumar.v.mangipudi@intel.com (K. Mangipudi).

[1] Disclaimer: This work was performed while the author was with North Dakota State University. The contents in this paper are the opinions of the authors.

0167-4048/$ – see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.cose.2006.05.002

However, Wu and Hsu (2004) cryptanalyzed Lee–Chang's protocol and exploited its vulnerabilities to launch an impersonation attack and also pointed out that given a previously agreed session key an attacker can disclose a user's identity. They further proposed a protocol to fix the aforementioned vulnerabilities. Later, Yang et al. (2004) showed a new weakness in Wu–Hsu's protocol, wherein the server obtains the user's secret token at the end of the login process, i.e., after a successful user identification and key agreement process. Possessing the user's secret information enables a server to impersonate the user at a later time. As such, Yang et al. (2004) proposed a protocol that overcomes the weakness of Wu–Hsu's protocol and achieves user anonymity, user identification and key agreement. As mentioned by Yang et al., these three protocols (Lee–Chang, Wu–Hsu and Yang) have the following attractive features apart from achieving user anonymity: (1) each user is required to maintain only one secret irrespective of the number of servers he is accessing; (2) the server is not required to maintain a list of passwords; (3) the system is scalable as new servers can be added without requiring to update the master key. More details on this protocol can be found in Yang et al. (2004).

Unfortunately, Yang's protocol despite possessing many attractive features is vulnerable to a Denial-of-Service (DoS) attack. In this paper, we show the DoS attack on Yang's protocol and propose a Secure Identification and Key agreement protocol with user Anonymity (SIKA). The rest of the paper is organized as follows: the next section reviews Yang's protocol. What follows next is the DoS attack on Yang's protocol. Further sections discuss our proposed SIKA protocol and its security and performance analysis. Finally, the last section concludes this paper.

2. Review of Yang's identification and key agreement protocol

In this section, we review Yang's identification and key agreement protocol. The main objectives of this protocol (as well as Lee–Chang's and Wu–Hsu's protocols) are to provide user identification, authentication and key agreement between the communication parties (a user and the server), while not disclosing the user's identity to the public. Since, it is necessary to know who is providing what services, the identity of the server is disclosed to the public. The user anonymity, however, is defined against the public rather than the server. This is because the server has to identify and verify the legitimacy of the user for accounting and billing purposes. In their protocol, there exists a trusted third party, the Smart Card Producing Center (SCPC) that defines the public parameters of the system and also issues secret tokens to the users and servers upon their request through a secure channel. During the login process a user and the server authenticate each other and agree upon a session key by using their respective secret tokens. The protocol consists of two phases. A key generation phase, where the SCPC issues a secret token to each of the participants (user/server) in the system via a secure channel and an anonymous user identification and key agreement phase, which is executed as and when the user logs in to the server for a service.

2.1. Key generation phase

In this phase, the SCPC chooses $N = pq$, where p and q are two large prime numbers; selects two integers e and d such that $ed = 1 \bmod \Phi(N)$, where $\Phi(N) = (p-1)(q-1)$; chooses a generator g in the field Z_N($g \in Z_N$), a hash function $H(m)$ on a message m, and a symmetric-key cryptosystem such as AES, where $E_K(m)$ and $D_K(m)$ represent encryption and decryption functions on a message m, respectively. The SCPC then publishes e, N, g, and $H(\cdot)$ as its public parameters and retains d, p, and q as secret. Each entity (user/server) first registers and then obtains a secret token P_i from the SCPC through a secure channel. The P_i is calculated as:

$$P_i = ID_i^d \bmod N, \tag{1}$$

where ID_i is the identity of a user U_i or the server S_i.

2.2. Anonymous user identification and key agreement phase

A user (U_i) and the server (S_j) execute the protocol shown in Fig. 1. The protocol is used to agree upon a common session key K_{ij}, identify the user and then authenticate, while maintaining the anonymity of U_i from the public. A brief description of the protocol is given below. U_i requests a service by way of $M1$. Upon receiving the request, S_j chooses a random number k; calculates

$$z = g^k P_j^{-1} \bmod N \tag{2}$$

and then sends it to U_i as $M2$. U_i now chooses a random number t and a time stamp T, and calculates the following,

$$a = z^e ID_j \bmod N \tag{3}$$

$$K_{ij} = a^t \bmod N \tag{4}$$

$$x = g^{et} \bmod N \tag{5}$$

$$p = g^t P_i^{H(x,T)} \bmod N \tag{6}$$

$$y = E_{K_{ij}}(ID_i) \tag{7}$$

and sends $M3(x,y,p,T)$ to S_j. (Note that K_{ij} is used as the common session key for encryption and decryption of the user's identity.) Upon receiving $M3$, S_j first checks validity

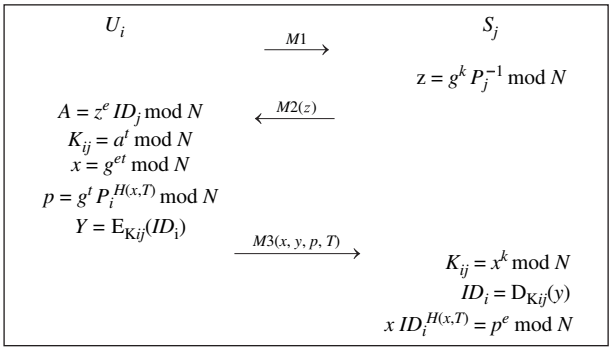

Fig. 1 – Anonymous user identification and key agreement phase.