Information Sciences 238 (2013) 242–249

Contents lists available at SciVerse ScienceDirect

Information Sciences

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

Provably secure three party encrypted key exchange scheme with explicit authentication

Hao-Chuan Tsai [a], Chin-Chen Chang [b,c,d,*]

[a] Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 621, Taiwan, ROC
[b] Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan, ROC
[c] Department of Information Engineering and Computer Science, Asia University, Taichung 41354, Taiwan, ROC
[d] Department of Biomedical Imaging and Radiological Science, China Medical University, Taichung 40402, Taiwan, ROC

ARTICLE INFO

Article history:
Received 8 April 2008
Received in revised form 25 February 2013
Accepted 4 March 2013
Available online 13 March 2013

Keywords:
3PEKE
Password
Off-line guessing attack
Provably secure

ABSTRACT

In 2007, Lu and Cao proposed a simple, three-party, password-based, authenticated key exchange (S-3PEKE) protocol based on the chosen-basis computational Diffie–Hellman assumption. Although the authors claimed that their protocol was superior to similar protocols from the aspects of security and efficiency, Chung and Ku pointed out later that S-3PEKE is vulnerable to an impersonation-of-initiator attack, an impersonation-of-responder attack, and a man-in-the-middle attack. Therefore, Chung and Ku also proposed a countermeasure with a formal proof to remedy the security flaws. Unfortunately, we have determined that Chung and Ku's protocol cannot withstand an off-line password guessing attack. In this paper, we briefly review Chung and Ku's protocol, demonstrate its weakness, and propose an enhanced version that is provably secure in the three-party setting.

1. Introduction

Providing private and reliable communications among clients over a public communication channel are great challenges for cryptography. A common way to solve these problems is to encrypt and authenticate clients' messages in order to protect the privacy and authenticity of their messages. In general, two mechanisms have been used to achieve this goal. The first is a public key cryptosystem to either encrypt or sign the messages [12,15,16,22]. Although a public key cryptosystem provides better security, its communication costs can create a heavy burden for certain applications. The second mechanism that has been used extensively is to establish a common session key via a key exchange scheme to encrypt messages for securing later communications. Passwords are the most popular way of protecting key exchange schemes over network environments because they are memorable and simple to use [2,6,11,13].

Bellovin and Merritt proposed the first well-known, two-party password based on the encrypted key exchange scheme [5]. In the recent decades, many two-party, password-based, authenticated key exchange schemes (2PAKE) have been proposed [2,6,13,25]. However, 2PAKE is only suitable for either client-to-server or client-to-client architecture. If a client needs to communicate with many other clients, the number of shared passwords that he or she would need to memorize would be linearly related to the number of communicating parties. That is, if there are N parties in a group who want to establish session keys with each other individually, C_2^N passwords are needed for each party to establish session keys. Due to this

* Corresponding author. Address: Department of Information Engineering and Computer Science, Feng Chia University, 100 Wenhwa Rd., Seatwen, Taichung 40724, Taiwan, ROC. Tel.: +886 4 24517250x3790; fax: +886 4 27066495.
E-mail addresses: tsaihc@cs.ccu.edu.tw, alan3c@gmail.com (H.-C. Tsai), ccc@cs.ccu.edu.tw (C.-C. Chang).

0020-0255/$ - see front matter © 2013 Elsevier Inc. All rights reserved.
http://dx.doi.org/10.1016/j.ins.2013.03.010

disadvantage, the server must be involved with the establishment of session keys among clients (3PEKE) [7,18,19,23,26]. This seems to be more realistic since a client only would have to memorize the password shared with the server rather than all of the multiple passwords of the other clients. Although 3PEKE is superior to 2PEKE in terms of reducing information that must be memorized, two potential problems remain. The first problem is that the privacy of the communication with respect to the server may not be ensured. The server is only required to establish a common session key between clients, and, even if the server shares some secrets with clients, an established session key should not be revealed to the server. The second problem is the insider attack. A legitimate, but malicious, client can impersonate other clients even if the system involves complete authentication to clients.

To resolve these problems, Lu and Cao [17] proposed a new, simple 3PEKE (S-3PEKE) protocol based on the chosen-basis computational Diffie–Hellman assumption [1]. However, Chung and Ku [8] pointed out that S-3PEKE has several weaknesses, including an impersonation-of-initiator attack, an impersonation-of-responder attack, and a man-in-the-middle attack, and they proposed countermeasures to remedy these security flaws. Unfortunately, we have determined that Chung and Ku's scheme is still vulnerable to an off-line guessing attack. This is due to the fact that the identities of clients are not always guaranteed; a legitimate, but malicious, client can modify the transcripts to get a response from the server and then derive other clients' secrets. Thus, we propose an enhanced version with novel architecture with the following characteristics:

(1) A session key assisted by the server available only to communication clients, and such a session key would not be revealed to either the server or others.
(2) Reduced computational load for clients and the server because, unlike previous 3PEKE schemes, the proposed version does not involve public-key cryptosystems, symmetric encryption/decryption systems [20,24], or other heavy burden operations [14,21] in the phase of establishing a session key.
(3) The server must authenticate the communication clients to avoid insider attacks and vice versa.
(4) Computation and round efficiencies can be provided for both communication parties.

The rest of this paper is organized as follows. Section 2 reviews Chung and Ku's 3PEKE scheme and also shows its security flaw. The preliminaries needed in the proposed scheme are described briefly in Section 3. And the enhanced scheme and the formal security analysis are given in Section 4 and Section 5, respectively. Our conclusions are presented in Section 6.

2. Review and weakness of Chung and Ku's 3PEKE scheme

Before reviewing Chung and Ku's 3PEKE scheme, we first depict the security basis on which their scheme relies.

2.1. DEFINE: computational Diffie–Hellman assumption

A $(t,\varepsilon)-\mathrm{CDH}_{g,G}$ is a probabilistic Turing machine Δ running in time t, with a prime order q and a generator g in a finite cyclic group G, such that its successful probability $\mathrm{Succ}^{\mathrm{cdh}}_{g,G}(\Delta)$ is greater than or equal to ε:

$$\mathrm{Succ}^{\mathrm{cdh}}_{g,G}(\Delta)=\Pr[\Delta(g^x,g^y)=g^{xy}]\geqslant\varepsilon,$$

when given the elements g^x and g^y to compute g^{xy}. Let $\mathrm{Succ}^{\mathrm{cdh}}_{g,G}(t)$ be the upper bound that adversaries have within time t. The Computational Diffie–Hellman (CDH) assumption is that $\mathrm{Succ}^{\mathrm{cdh}}_{g,G}(t)\leqslant\varepsilon$ for any t/ε is not extremely large.

The so-called chosen-basis computational Diffie–Hellman problem (CCDH) is a variant of the CDH assumption [9] that can be stated as follows: an adversary is given two random elements U and X as inputs. Next, the goal of an adversary is to output the value $K=CDH_{g,G}(X,Y/U^r)$, where r is the password mapping into G. The main idea of this assumption is that an adversary may compute either X or Y/U^r, but not both. That is, $\mathrm{Succ}^{\mathrm{ccdh}}_{g,G}(t,n)$ can be bounded by the probability $1/n$, where n is the size of the password mapping into G.

2.2. Chung and Ku's 3PEKE scheme

Assume that two clients A and B request to establish a session key by resorting to the server S. The steps of Chung and Ku's 3PEKE scheme can be described as in the following:

Step 1a: A chooses a random element $x\in_R Z_p$ and then computes $X\leftarrow g^x\cdot M^{pw_A}$, where M and pw_A denote the element in G and a password shared between A and S, respectively. Eventually, A sends X to B along with her or his identity, i.e., $A\|X$.

Step 1b: After receiving $A\|X$, B then also chooses a random element $y\in_R Z_p$ to compute $Y\leftarrow g^y\cdot N^{pw_B}$, where N and pw_B denote the element in G and a password shared between B and S, respectively. Next, B sends $A\|X\|B\|Y$ to S.

Step 2a: Upon receiving $A\|X\|B\|Y$, S utilizes the shared passwords pw_A and pw_B to retrieve $g^x\leftarrow X/M^{pw_A}$ and $g^y\leftarrow Y/N^{pw_B}$, respectively. In addition, S chooses a random element $z\in_R Z_p$ and the retrieved results to compute $g^{xz}\leftarrow(g^x)^z$ and $g^{yz}\leftarrow(g^y)^z$. Eventually, S computes $X'\leftarrow g^{yz}\cdot H(A,B,S,g^x)^{pw_A}$ and $Y'\leftarrow g^{xz}\cdot H(B,A,S,g^y)^{pw_B}$, where $H(\cdot)$ is a collision resistance one-way hash function, and then sends $X'\|Y'$ to B.