Journal of King Saud University – Computer and Information Sciences (2016) **28**, 68–81

King Saud University

Journal of King Saud University – Computer and Information Sciences

www.ksu.edu.sa
www.sciencedirect.com

A secure effective dynamic group password-based authenticated key agreement scheme for the integrated EPR information system

Vanga Odelu [a,b,*], **Ashok Kumar Das** [c], **Adrijit Goswami** [a]

[a] *Department of Mathematics, Indian Institute of Technology, Kharagpur 721 302, India*
[b] *Department of Mathematics, Rajiv Gandhi University of Knowledge Technologies, Hyderabad 500 032, India*
[c] *Center for Security, Theory and Algorithmic Research, International Institute of Information Technology, Hyderabad 500 032, India*

Received 24 July 2013; revised 10 March 2014; accepted 15 April 2014
Available online 7 November 2015

KEYWORDS

Cryptanalysis;
Integrated EPR information system;
Dynamic group;
Password;
Authentication;
Security

Abstract With the rapid growth of the Internet, a lot of electronic patient records (EPRs) have been developed for e-medicine systems. The security and privacy issues of EPRs are important for the patients in order to understand how the hospitals control the use of their personal information, such as name, address, e-mail, medical records, etc. of a particular patient. Recently, Lee et al. proposed a simple group password-based authenticated key agreement protocol for the integrated EPR information system (SGPAKE). However, in this paper, we show that Lee et al.'s protocol is vulnerable to the off-line weak password guessing attack and as a result, their scheme does not provide users' privacy. To withstand this security weakness found in Lee et al.'s scheme, we aim to propose an effective dynamic group password-based authenticated key exchange scheme for the integrated EPR information system, which retains the original merits of Lee et al.'s scheme. Through the informal and formal security analysis, we show that our scheme provides users' privacy, perfect forward security and known-key security, and also protects online and offline password guessing attacks. Furthermore, our scheme efficiently supports the dynamic group password-based authenticated key agreement for the integrated EPR information system. In addition, we simulate our scheme for the formal security verification using the widely-accepted AVISPA

* Corresponding author at: Department of Mathematics, Indian Institute of Technology, Kharagpur 721 302, India.
E-mail addresses: odelu.vanga@gmail.com, odelu.phd@maths.iitkgp.ernet.in (V. Odelu), iitkgp.akdas@gmail.com, ashok.das@iiit.ac.in (A.K. Das), goswami@maths.iitkgp.ernet.in (A. Goswami).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

http://dx.doi.org/10.1016/j.jksuci.2014.04.008

(Automated Validation of Internet Security Protocols and Applications) tool and show that our scheme is secure against passive and active attacks.

1. Introduction

In an integrated EPR (electronic patient record) information system of all the patients, the medical institutions and the academia with most of the patients' information in details for them, can make the corrective decisions and clinical decisions in order to maintain and analyze patients' health. In such systems, the illegal access needs to be avoided as well as the information from theft during transmission over the insecure Internet needs to be prevented.

A dynamic group key agreement protocol provides the mechanisms to process member addition and deletion. Several dynamic group key agreement protocols have been proposed in the literature. We can divide the group key agreement protocols into two categories (Lee et al., 2013). The first one is the group key agreement protocols with public key. For example, key agreement protocols proposed by Tzeng and Tzeng (2000), Tzeng (2002), Boyd and Nieto (2003), Kim et al. (2004), Lee et al. (2006), and Jeong and Lee (2007) employ the public key infrastructure (PKI) and provide higher security. However, they are required to maintain the complex and heavy public key systems and users must hold extra storage for keeping public/private key pairs. The second one is the group password-based key agreement protocols (GPKE) without public key. For example, key agreement protocols of Lee et al. (2004), Abdalla et al. (2006), and Dutta and Barua (2006) provide the same password to all communicating parties. That is, each user does not have his/her own private password, and thus, the user cannot have his/her privacy. However, Zhang et al. (2012) showed that Dutta and Barua's scheme (Dutta and Barua, 2006) is insecure, where their scheme does not satisfy the key independence property (Steiner et al., 2000) and any two malicious users whose logic indexes are not adjacent in the former execution of the protocol may mount a replay attack in new protocol executions. Hence, these password-based approaches are not much suitable for many practical scenarios (Lee et al., 2013).

Boyd and Nieto (2003) described the first conference key agreement protocol, which can be completed in a single round. However, their scheme lacks forward secrecy property. By the forward secrecy property, we mean that when a node (user) leaves the network, it must not read any future messages after its departure. Kim et al. (2004) proposed an efficient and secure constant-round authenticated key agreement protocol (AGKE) for dynamic groups in the random oracle model. Dutta and Barua (2006) proposed a variant of Kim et al.'s scheme (Kim et al., 2004). Dutta–Barua's scheme makes use of the ideal-cipher model, instead of a simple mask, and they claimed that their scheme is secure against dictionary attacks. Unfortunately, their scheme contains another source of redundancy that can be exploited by an attacker (Abdalla et al., 2006). In 2006, Abdalla et al. (2006) proposed the first provably-secure password-based constant-round group key exchange protocol. It is provably-secure in the random-oracle and ideal-cipher models, which makes use of the decisional Diffie–Hellman problem assumption.

Recently, Lee et al. (2013) have proposed a simple group password-based authenticated key protocol without the server's public key, called the SGPAKE protocol, for the integrated EPR information system. Their scheme is based on Abdalla and Pointcheval's scheme (Abdalla and Pointcheval, 2005). Lee et al.'s SGPAKE protocol does not use any long-term key or public-key system. Lee et al. (2013) claimed that SGPAKE protocol provides each user a unique private weak password and resists password-guessing attack, and thus their scheme provides user privacy and data privacy. However, in this paper, we show that any user U_i in a group S_n can derive the private password of the user U_{i-1} by setting the off-line password guessing attack, so that it does not provide the user's privacy. We aim to propose an improvement on Lee et al.'s SGPAKE protocol while retaining the original merits of Lee et al.'s scheme. Through the formal and informal security analysis, we show that our improved scheme provides user's privacy and perfect forward security, and also resists the offline password guessing attack.

The remainder of this paper is organized as follows. In Section 2, we provide the properties of the one-way hash function, discrete logarithm problem and group Diffie–Hellman problem. In Sections 3 and 4, we review Lee et al.'s SGPAKE protocol and then discuss the security flaws of Lee et al.'s SGPAKE protocol, respectively. We explain our improved scheme in Section 5. In Section 6, we provide the security of our improved scheme. Through the informal and formal security analysis, we show that our improved scheme is provably secure against an adversary for protecting the user's privacy and perfect forward security. In Section 7, we simulate our scheme for the formal security verification using the widely-accepted AVISPA (Automated Validation of Internet Security Protocols and Applications) tool and show that our scheme is secure. In Section 8, we compare the performances of our scheme with other related existing schemes. Finally, we conclude the paper in Section 9.

2. Mathematical preliminaries

In this section, we discuss the properties of the one-way hash function, discrete logarithm problem and group Diffie–Hellman problem, which are useful for describing Lee et al.'s SGPAKE protocol (Lee et al., 2013) and its security analysis as well as our improved scheme.

2.1. One-way hash function

A one-way collision-resistant hash function $h : \{0,1\}^* \rightarrow \{0,1\}^n$ is a deterministic algorithm (Sarkar, 2010; Stinson, 2006) that takes an input as an arbitrary length binary string $x \in \{0,1\}^*$ and outputs a binary string