Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Efficient end-to-end authentication protocol for wearable health monitoring systems[☆]

Qi Jiang[a,*], Jianfeng Ma[a], Chao Yang[a], Xindi Ma[a], Jian Shen[b], Shehzad Ashraf Chaudhry[c]

[a] *School of Cyber Engineering, Xidian University, Xi'an, China*
[b] *School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing, China*
[c] *Department of Computer Science and Software Engineering, International Islamic University, Islamabad, Pakistan*

ARTICLE INFO

Article history:
Received 9 March 2017
Revised 12 March 2017
Accepted 13 March 2017
Available online 7 April 2017

Keywords:
Wearable health monitoring systems
Authentication
Key agreement
Privacy
Quadratic residues
Smart card

ABSTRACT

Wearable health monitoring systems (WHMSs) will play an increasingly important role in future e-healthcare and enable smart and ubiquitous healthcare services. Given its sensitivity, the health data should be protected against unauthorized access. As a result, it is critical to design an end-to-end mutual authentication protocol that enables secure communication between the wearable sensor and medical professionals. Recently, Amin et al. proposed an anonymity preserving mutual authentication protocol for WHMSs. However, we identify that their protocol suffers from stolen mobile device attack, desynchronization attack, and sensor key exposure. Then we put forward an improved end-to-end authentication protocol based on quadratic residues. Comprehensive security analysis is conducted to show that the proposed protocol fixes these flaws of Amin et al.'s protocol and satisfies all desired requirements. The comparison with these existing protocols demonstrates that our protocol provides a practical end-to-end security solution for WHMSs.

1. Introduction

As one of the promising means to alleviate the issues associated with the increasing aging population and healthcare costs, as well as to improve healthcare quality, wearable health-monitoring systems (WHMSs) have attracted an increasing attention from both the industry and academia. WHMSs, which consist of various types of wearable or even implantable medical sensors, are enabling smart and ubiquitous monitoring of health condition of a mobile patient in a non-invasive way, from anywhere and at any time, and will potentially transform the future of healthcare [1].

Currently, advances in miniature sensors, wireless communications and cloud computing have made WHMSs a reality [1–3]. The architecture of a typical WHMS is shown in Fig. 1. The medical sensors and a personal mobile device, which can be a smart phone, a PDA, a pocket PC, etc., form a body area network (BAN) or body sensor network (BSN). These medical sensors sense significant physiological parameters, e.g., heart rate, blood pressure, body temperature, respiration rate, electrocardiogram, and transmit the data to the mobile device which acts as the intermediary to share this information over long distances. Then the intermediary sends the measured health data to a remote medical server or the medical professional's mobile device [1].

[☆] Reviews processed and approved for publication by Editor-in-Chief.
[*] Corresponding author.
E-mail address: jiangqixdu@gmail.com (Q. Jiang).

http://dx.doi.org/10.1016/j.compeleceng.2017.03.016

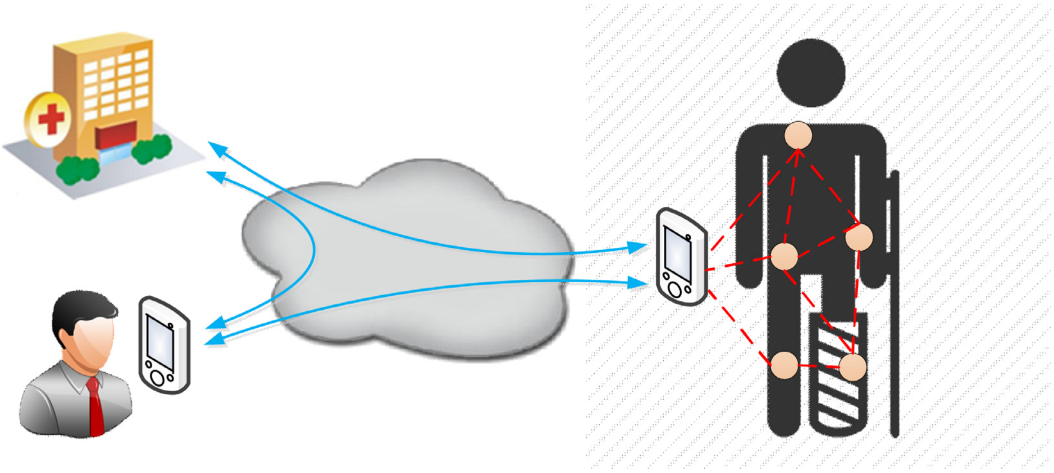

Fig. 1. Typical architecture of wearable health monitoring systems (WHMSs).

In WHMSs, the health data can be accessed by medical professionals anywhere and anytime through Internet and wireless networks. Specifically, a medical professional can access the health data in two ways. One is to access the data maintained by the medical server. The other is to access the real-time data measured by sensors directly. Given its sensitivity, there are laws stipulating privacy rules regarding electronic health data in healthcare systems, such as the Health Insurance Portability and Accountability Act (HIPAA) [4,5]. Thus there is strong awareness of the security and privacy of health data in WHMSs. Since the sensitive health information is transmitted through a path composed of various network devices and open channels, the information should be protected against various types of active and passive attacks [6]. In this paper, we mainly concern the design of an end-to-end mutual authentication and key agreement protocol between the wearable sensor and medical professionals to achieve end-to-end secure communication between them. Although several authentication protocols [7–16] has been proposed in the literature, all these protocols either fail to provide adequate security protection or suffer from various security vulnerabilities.

1.1. Architecture of WHMSs

In WHMSs, there are three types of participants, i.e., medical professional (doctor, patient, nurse, etc.), medical sensors and gateway. The medical sensor nodes sense the health condition of the patient and then send the health data to the gateway or medical professionals. The gateway is the brain of WHMSs, which provides registration to all the medical professionals and sensor nodes. The medical professionals can access the sensitive information of the patient from either the gateway or the sensor node to diagnose and monitor the patient's health conditions [7]. In traditional wireless medical sensor networks (WMSNs), the role of gateway is played by a smart device of the patients [7–9]. However, due to limited computing capability and power supply, mobile devices, such as smart phones and PDAs, are not suitable to perform expensive operations, such as providing registration services to medical professionals and sensors. In order to avoid this dilemma, we propose the slightly modified architecture, in which the role of registration center is played by a dedicated medical server in the medical center, as is illustrated in Fig. 1.

1.2. Related works

It is generally accepted that WHMSs must prevent unauthorized access to the sensitive health information and guarantee security and privacy of these participants. One more challenge that cannot be ignored is that power consumption of mobile devices and sensors should be minimized to lengthen the operational lifetime of WHMSs, since the power supply of sensors and mobile devices is relatively limited [1]. In this line, a number of two-factor authentication and key agreement protocols have been put forward. In such protocols, two different types of security credential, i.e., smart card and password, are needed for a user to corroborate his/her identity.

In 2012, Kumar et al. [8] suggested an authentication protocol for monitoring the health conditions of a patient and claimed that their protocol is capable of withstanding known security threats. Unfortunately, Khan and Kumari [9] found that Kumar et al.'s protocol has several security attacks. In addition, they proposed an enhanced protocol which is more efficient and secure against known attacks. He et al. [10] also showed that Kumar et al.'s protocol is vulnerable to some attacks and then put forward a user authentication protocol for healthcare applications using WMSNs.

In 2015, Wu et al. [11] showed that the protocol of He et al. [10] suffers from offline password guessing and impersonation attacks. Wu et al. [11] proposed an improved user authentication protocol using hash function to remove the loopholes of the protocol of He et al. Mir et al. [12] also showed that He et al.'s protocol is still susceptible to the offline password