Computers and Electrical Engineering 000 (2017) 1–14

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server☆

Fan Wu[a], Xiong Li[b,*], Lili Xu[c], Saru Kumari[d], Marimuthu Karuppiah[e], Jian Shen[f]

[a] Department of Computer Science and Engineering, Xiamen Institute of Technology, Xiamen 361021, China
[b] School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan, 411201, China
[c] School of Information Science and Technology, Xiamen University, Xiamen 361005, China
[d] Department of Mathematics, Chaudhary Charan Singh University, Meerut, 250005, Uttar Pradesh, India
[e] School of Computer Science and Engineering, VIT University, Vellore 632 014, India
[f] School of Computer and Software, Nanjing University of Information Science and Technology, Nanjing 210044, China

ARTICLE INFO

Article history:
Received 20 November 2016
Revised 13 April 2017
Accepted 14 April 2017
Available online xxx

Keywords:
Mutual authentication
Wearable device
Anonymity
De-synchronization attack
Cloud server

ABSTRACT

As a popular technology for Internet of Things (IoT), wearable devices are accepted widely by people. Classic wearable devices including glasses and watches collect wearers' information which is usually private. Often, a single wearable device is not enough to see the data of the user and a mobile terminal such as a smart phone is used to match the wearable device. Also, the gathered data are often stored in the remote cloud server. Security issues become the emergent tasks and they have not been solved perfectly. Until now, there are weaknesses in traditional authentication ways, and such ways are not fit for the communication. Therefore, we propose a new and lightweight authentication scheme for wearable devices with help of cloud server. This scheme reaches mutual authentication and keeps anonymous for the devices. Compared to two recent schemes of the similar kind, ours is more secure and applicable.

1. Introduction

With the conception of Internet of Things (IoT) appearing, the applications of this notion turn to be flourished more and more. IoT means that the world can be connected by series of sensors which collect the information from everything in the world. There are many sorts of IoT applications , like wireless sensor networks [1], radio frequency identification (RFID) [2], etc. Among them, wearable device is an important part. A host of wearable devices for human beings have come into our daily life in recent time. An example is that many smart watches with the middle and low level prices sold on the sales web often have the functions like showing step numbers, energy consumption of walking and running, and reminding of short messages. In the current stage, wearable devices can only exchange messages with other devices in short distance through short-range wireless communication way, e.g., bluetooth. Also, they have constrained computation and communication resources so that only some fast algorithm can be used on them [3]. And usually a cloud server is required for data storage. So how to protect the data in the brittle wireless channel is a hot issue nowadays. The classic system architecture containing wearable devices is illustrated in Fig. 1. There are four entities in the system: a user, a smart

☆ Reviews processed and recommended for publication to the Editor-in-Chief by Guest Editor Dr. Debiao He.

* corresponding author.
E-mail addresses: conjurer1981@gmail.com (F. Wu), lixiongzhq@163.com (X. Li), saryusiirohi@gmail.com (S. Kumari).

http://dx.doi.org/10.1016/j.compeleceng.2017.04.012
0045-7906/

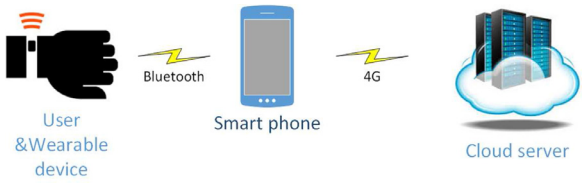

Fig. 1. Architecture of cloud-assisted wearable device system.

phone, a wearable device and the remote cloud storage server. First we assume the user may have one or more wearable devices with different purposes. The user only does some harmless operations to the communication, such as reading data from the wearable device and smart phone. Second, as a necessary device owned by a person, the smart phone is the media which connects the wearable device, usually by bluetooth, and the cloud server, usually by Wireless Fidelity (WiFi) or the 4th Generation communication system (4G). It has more energy and ability than the wearable device, in order to communicate with the cloud server. Generally, an App is a necessary component installed in the smart phone and plays the important role for transmitting information between the wearable device and the cloud server. The third is the wearable device such as the smart watch, smart bracelet, etc. It collects the user's personal body information like running steps and time cost, or even shows data containing the above items and short messages received by the smart phone. The last is the cloud server, which we can consider to be trustful due to its own security mechanism. Every time the data collected from the wearable device should be stored in the cloud server, so as to ease the storage burden of the smart phone and the wearable device.

1.1. Related work

Information encryption [4–14], as an important security issue, has always attracted researchers. The information transferring process is a hot part. Generally, user's identity, password and a portable device storing user's information issued by the trusted server are all critical elements for authentication. Sometimes the user's biometrics is also employed as one authentication factor [1]. The authentication mechanism for wearable devices is relatively new in the research scope and there are several papers about the topic [15–18] published in 2015 and 2016.

Diez et al. [15] presented an authentication scheme for self-authenticable wearable devices. In that scheme, authentication between a wearable device and another device can be done. Then the authentication process based on Extensible Authentication Protocol (EAP) [19] is introduced. Moreover, Butun et al. [16] showed a Cloud-centric MULti-level Authentication (CMULA) scheme between the wearable devices and wearable network coordinator. They claimed that the scheme made the IoT devices integrate the cloud server perfectly. In the scheme, the user directly accesses the cloud server, but does not gets data from a media device, like a smart phone. The two schemes seem to be far from common and simple work mode of wearable devices used by the masses. Liu et al. [17] used quick response (QR) code to transmit identity and address of wearable device via a secure out-of-band (OOB) channel, and then a scheme with two channels was proposed. But only some high-level wearable devices employ QR code to denote themselves on the smart phone. Moreover, there is also a password for wearable devices, which is unfit for common wearable devices. Liu et al. [18] proposed a yoking-proof-based authentication scheme with cloud server as the assistant for wearable devices. Yoking proof is first applied in RFID authentication scheme [20]. In such schemes, two tags are simultaneously scanned and verified.

Moreover, among the above schemes, only [17,18] show the whole authentication process in details. But some problems still exist in the schemes.

1. Inapplicability. Both schemes in [17,18] have a hypothesis that the wearable device and the smart phone/mobile terminal share a long-term key at the beginning. It is impossible to do that. For example, either of the them is newer than the other, e.g., a time span of two years. Also, they may be made in different companies. Moreover, for the scheme in [17], inputting password is meaningless for a lot of common wearable devices. And cloud server usage is the tendency [21]. And for the scheme in [18], it is common that one person has only one wearable device, like a smart bracelet for sport data recording.
2. De-synchronization attack. It is obvious in [18]. We explain the cases: if the message $\{C_{Db}||M_{Db}||N_{Db}\}$ is lost, the smart phone cannot verify whether C_{Db} is correct and S_{Db} and PID_{Db} will not be updated; if $\{C_{Da}||N_{YP}\}$ is lost, like the last case, S_{Da} and PID_{Da} will not be updated; finally, if $\{YP\}$ is lost, S_{Da}, S_{Db}, PID_{Da} and PID_{Db} stored in the cloud server will not be updated. The result is that the records of the wearable devices stored in the smart phone or the cloud server cannot be changed in time. Next time the authentication will be failed undoubtedly.
3. Unsuitable model. A secure OOB channel is used during the authentication process in [17]. This hypothesis is odd in the authentication, since generally a secure channel is only used in registration at first.

Based on the above analysis, a secure and practical authentication scheme for wearable devices, including complete pairing and authentication phases, is proposed. Via the famous tool Proverif, we make the formal verification and it is clear that

Please cite this article as: F. Wu et al., A lightweight and privacy-preserving mutual authentication scheme for wearable devices assisted by cloud server, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.04.012