Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Selective disclosure and yoking-proof based privacy-preserving authentication scheme for cloud assisted wearable devices

Hong Liu[a,b], Huansheng Ning[c,*], Yinliang Yue[d], Yueliang Wan[b], Laurence T. Yang[e,f]

[a] School of Computer Science and Software Engineering, East China Normal University, China
[b] Research Institute, Run Technologies Co., Ltd., Beijing, China
[c] School of Computer and Communication Engineering, University of Science and Technology, Beijing, China
[d] Institute of Information Engineering, Chinese Academy of Sciences, China
[e] School of Electronic Engineering, University of Electronic Science and Technology of China, China
[f] Department of Computer Science, St. Francis Xavier University, Canada

HIGHLIGHTS

- Both local and remote authentication modes are considered for cloud assisted wearable devices.
- Selective disclosure mechanism and Chebyshev chaotic map are applied to achieve authentication.
- Yoking-proofs are established for simultaneous verification in a remote authentication mode.

ARTICLE INFO

Article history:
Received 1 August 2016
Received in revised form 25 January 2017
Accepted 7 April 2017
Available online xxxx

Keywords:
Authentication protocol
Security
Wearable device
Yoking-proof
Selective disclosure

ABSTRACT

Along with the development of user-centric wireless communications, wearable devices appear to be popular for real-time collecting a user's private data to provide intelligent service support. Compared with traditional short-range communications, the wearable devices confront more severe system vulnerabilities and security threats during interactions. Considering the limitations of computational capabilities and communication resources, it brings more challenges to design privacy-preserving authentication schemes for the resource-constrained wearable devices. In this work, local authentication and remote authentication are respectively designed for cloud assisted wearable devices. In the local authentication mode, hash based selective disclosure mechanism and Chebyshev chaotic map are jointly applied to achieve mutual authentication between a wearable device and a smart phone. In the remote authentication mode, Merkle hash tree based selective disclosure mechanism is designed to improve the structure of data fields in the certificate, and a yoking-proof is established to realize interactions between two wearable devices and a smart phone, and is further transmitted to the cloud server for simultaneous verification. Meanwhile, security formal analysis is performed based on the BAN logic for proving that the proposed remote authentication protocol has theoretical design correctness. It indicates that the proposed authentication scheme is available and flexible for ubiquitous wearable devices.

1. Introduction

Along with the development of user-centric wireless communications, wearable devices appear to be popular for real-time collecting a user's private data to provide intelligent service support. These wearable devices are mainly based on short-range wireless communication technologies (e.g., WiFi, Bluetooth, and near field communication (NFC)) to realize data perception and computing [1–4]. Currently, wearable devices are still in the infancy, and confront several open issues due to the limitations of computational capabilities and communication resources. The wearable devices are attached with a user's sensitive information (e.g., body signs, tracking, and preferences), and have been gradually deployed in the scenarios of health, sport and entertainment. It brings severe security challenges via wireless and open communication channels [5,6].

There are several researches worked to enhance security protection for the wearable devices in user-centric networks [7–12]. Thereinto, user privacy is a typical issue for cloud assisted wearable devices, and secure interactions are established to achieve authentication. Due to the resource limitations, the wearable devices usually transmit the frequently collected personal data into remote cloud server for advanced analysis [13–15]. It turns out that the

[*] Corresponding author.
E-mail address: ninghuansheng@ustb.edu.cn (H. Ning).

http://dx.doi.org/10.1016/j.future.2017.04.014
0167-739X/© 2017 Elsevier B.V. All rights reserved.

Please cite this article in press as: H. Liu, et al., Selective disclosure and yoking-proof based privacy-preserving authentication scheme for cloud assisted wearable devices, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.04.014.

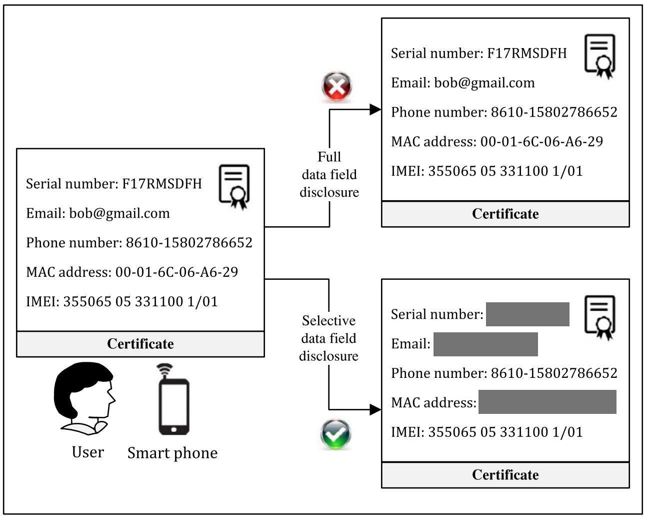
Serial number: F17RMSDFH
Email: bob@gmail.com
Phone number: 8610-15802786652
MAC address: 00-01-6C-06-A6-29
IMEI: 355065 05 331100 1/01
Certificate
User
Smart phone
Full data field disclosure
Selective data field disclosure
Serial number: F17RMSDFH
Email: bob@gmail.com
Phone number: 8610-15802786652
MAC address: 00-01-6C-06-A6-29
IMEI: 355065 05 331100 1/01
Certificate
Serial number:
Email:
Phone number: 8610-15802786652
MAC address:
IMEI: 355065 05 331100 1/01
Certificate

Fig. 1. An example of selective disclosure.

wearable devices may have two interactive modes, referring to a local interaction (interaction between a smart phone and one or more wearable devices), and a remote interaction (interaction among a smart phone, one or more wearable devices, and a cloud server). There are dissimilar requirements for the two interactive modes, diverse authentication protocols should be designed for the cloud assisted wearable devices. It is necessary for designing suitable security solutions to address security issues of wearable devices in both local and remote interactions.

During interactions between a smart phone and a wearable device, it is unavoidable for exchanging information for identification and advanced service support (e.g., location-based services). Generally, the smart phone could perform authentication based on a certificate covering full data fields. While some of data fields may not have to be published for authentication, and only partial data fields are adequate for working. Fig. 1 illustrates an example, in which a user's smart phone owns a certificate including serial number, email, phone number, MAC address, and IMEI. When the smart phone publishes its certificate for identification, it is recommended for disclosing partial insensitive data fields instead of disclosing the full data fields in the certificate. It becomes essential for designing selective disclosure mechanisms for a smart phone to freely publish certain data fields to the associated wearable devices.

Based on above security and privacy requirements, a suitable authentication scheme should be designed for cloud assisted wearable device contexts with the following security properties [16]. (1) *Data confidentiality and data integrity*: The exchanged messages between any two legal entities should be protected against an illegal access, tampering and modification, and any sensitive information cannot be revealed or destroyed. (2) *Mutual authentication*: The untrusted entities should pass the legal entities' verification so that only the legal entity can access the systems for obtaining the detailed information. (3) *Forward security*: Any attackers cannot correlate any two ongoing communication sessions, and also cannot derive the previous interrogations according to the current interactive session. (4) *Privacy preservation*: The entity cloud freely decide which data field could be published, any sensitive information cannot be obtained by an unrelated entity, and anonymity should be achieved to avoid identity and data guessing.

In this work, local authentication and remote authentication are respectively considered for the cloud assisted wearable devices. In the local authentication mode, hash based selective disclosure mechanism and Chebyshev chaotic map are jointly applied to achieve mutual authentication between a wearable device and a smart phone. In the remote authentication mode, Merkle hash tree based selective disclosure mechanism is designed to improve the structure of data fields in the certificate, and a yoking-proof is established to realize interactions between two wearable devices and a smart phone, and is further transmitted to the cloud server for simultaneous verification. Note that the concept of yoking-proof is first proposed in the radio frequency identification (RFID) applications, and yoking-proofs or grouping-proofs based protocols are designed to realize that two or multiple tags are simultaneously authenticated within a reader's range during an interactive session [17,18]. In existing RFID schemes, simultaneous existences of two or multiple tags can be regarded as a pair or a group to be verified by a reader (or a database). It indicates that such RFID scenarios are similar to wearable device scenarios, in which one or more wearable devices establish authentication with a smart phone (or a cloud server). Here, we have identified a unique security issue for the cloud assisted wearable devices, and focus on both secure authentication and simultaneous identification during local and remote interactions. The main contributions are as follows:

- The semigroup property and chaotic property of Chebyshev chaotic map are applied to achieve a smart phone authenticating the validity of a wearable device in both local and remote authentication mode. The Chebyshev polynomials are adopted to enhance anonymous message transmission.
- Hash and Merkle hash tree based selective disclosure mechanisms are respectively designed for the local and remote authentication, which realizes that a smart phone's sensitive data fields can be freely selected for sharing with the wearable devices along with privacy-preserving authentication.
- A yoking-proof is established by involving two wearable devices into one session in a remote authentication mode, which realizes that two wearable devices establish yoking relationships, and a cloud server simultaneously verifies the validity of the associated wearable devices.

The rest of this paper is organized as follows. Section 2 introduces the related security studies on the wearable devices. Section 3 describes the system model. Section 4 presents the proposed authentication scheme, including a local authentication mode and a remote authentication mode. BAN logic based security formal analysis is performed in Section 5. Implementation and performance analysis are presented in Section 6. Finally, Section 7 draws a conclusion.

2. Related work

Diez et al. [10] focused on self-authenticable wearable devices to propose a point-to-point authentication protocol, which enables secure mutual authentication between a wearable device and other entities (e.g., another wearable device, a mobile phone, and a remote server). The proposed authentication protocol could easily be extended to include the exchange of a session key to ensure a secure channel. Secure communications are established among remote wearable devices through the Internet to achieve information sharing. It is identified that existing security solutions address the secure authentication issues for wearable devices, which are more concerned about authenticating the user holding the wearable device than the device itself. Meanwhile, the related technologies such as NFC, smart cards, point-to-point protocol, extensible authentication protocol, and imprinting are introduced for the wearable devices. Different security levels (i.e., low, intermediate, and high) oriented scenarios are described according to sensitivity of information handled by the wearable devices.

Please cite this article in press as: H. Liu, et al., Selective disclosure and yoking-proof based privacy-preserving authentication scheme for cloud assisted wearable devices, Future Generation Computer Systems (2017), http://dx.doi.org/10.1016/j.future.2017.04.014.