Journal of Network and Computer Applications 60 (2016) 144–154

Contents lists available at ScienceDirect

Journal of Network and Computer Applications

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

A novel asymmetric three-party based authentication scheme in wearable devices environment

Sha Liu [a], Shun Hu [a], Jian Weng [a], Shuhua Zhu [b,*], Zhiyan Chen [c]

[a] School of Information Science and Technology, Jinan University, Guangzhou 510632, China
[b] Network & Education Technology Center, Jinan University, Guangzhou 510632, China
[c] International School, Jinan University, Guangzhou 510632, China

ARTICLE INFO

Article history:
Received 13 August 2014
Received in revised form
21 May 2015
Accepted 5 October 2015
Available online 31 October 2015

Keywords:
Authentication
Wearable devices
OOB
Secure device pairing
Mobile terminals

ABSTRACT

As we know, wearable devices record data generating from user's daily activities, and most of which are private data, such as health data and movement data. These information is usually stored in user's device. As more and more people started using wearable devices, some security problems have emerged and not been resolved perfectly, for example, how to keep the sensitive information safely in wearable devices and how to secure the user's privacy is becoming important issues in recent years. Considering the limitation of hardware of wearable devices, implementing authentication among three different parties (wearable devices, mobile terminals and users) would be a practical way to address these problems effectively. However, based on our study, traditional lightweight authentication schemes could not be applied for this new environment directly. In this paper, we proposed an asymmetric three-party based authentication scheme in this new environment. Drawing on the visual out-of -band (OOB) channel, two-dimensional code (QR code) and secure device pairing method, our scheme provides a mutual efficient authentication between wearable devices and mobile terminal. We made a new attempt to label the Bluetooth device address into a visual tag in order to reduce the time of Bluetooth connection. In addition, we took the multi-users condition into consideration and allowed primary user to add number of authorized users by authentication process. According to security and usability analysis, we proved that this scheme can not only resist known types of attacks but also can be practically applied in new environment. The experiment result shows thatperformance of the scheme meets our expectations.

© 2015 Elsevier Ltd. All rights reserved.

1. Introduction

In recent years, a growing number of intelligent wearable devices have stepped into people's daily life. With their portability and practicability, they gradually affect people's lifestyles and improve people's quality of life. For example, Nike smart watch could track distance, speed, time and energy consumption during user's running time. Google glasses adopt virtual reality technology to display messages and take photos. However, due to the limitation of hardware on these devices, they cannot provide precise and detailed analysis of users' data. So smart wearable devices usually work together with mobile terminals to implement data analysis and synchronization of sensitive information. In terms of the Samsung Galaxy Gear, it connects to a smart phone via Bluetooth to make a phone call, send or receive emails and SMS, track and manage personal information. Due to the fact that wearable devices mostly store personal healthy data and communication messages, the protection of users' privacy is a primary security problem people should solve in wearable environment.

The attacks against private data of wearable devices can be divided into two categories. The first is attacks against wearable device itself. This kind of attacks can be described as follows: when acquiring a wearable device, attackers will be able to get user's sensitive data compromised by wearable devices by some extreme methods, such as destroying the hardware. The second is that attacks aimed at the communication process between wearable devices and mobile terminals. This kind of attacks includes forge attacks, reply attacks and man-in-the-middle attacks. However, the former is out of the scope of our discussion. In this paper, we would focus on the latter kind of attacks and propose our novel authenication scheme based on this new environment.

2. Security requirements

Wearable devices environment is different from traditional environment, and after careful analysi, we make conclusions that the authentication scheme should have some unique requirements as follows:

* Corresponding author.
E-mail address: zsh@jnu.edu.cn (S. Zhu).

http://dx.doi.org/10.1016/j.jnca.2015.10.001
1084-8045/© 2015 Elsevier Ltd. All rights reserved.

1. Lightweight: Wearable devices normally have limited processing and storage capacity so that they can only operate the lightweight authentication;
2. Anonymity: Wearable devices need to be used combine with mobile terminal in public places. In order to prevent replay attacks, the wearable devices need to be anonymous;
3. Low delay: The data needed to be transmitted is much larger than these in WSN and RFID. In order to guarantee the quality of communication, the authentication scheme should be efficient and fast;
4. Availability: For the purpose of preventing the forward and backward attacks, each shared key in authentication process should be only effective for a short time in one authentication;
5. No trusted third-party device: Wearable device connects mobile terminal through unsafe WIFI or Bluetooth connection, there does not exist a trusted third-party equipment in the process of mutual authentication.

3. Related work

3.1. RFID authentication

The existing lightweight authentication protocols can be divided into RFID authentication and sensor authentication. RFID authentication protocols could also be divided into two categories: traditional RFID authentication protocols (Chien, 2007; Song and Mitchell, 2008) and the server-less RFID authentication protocols (Lee et al., 2012; Tan et al., 2008).

For traditional RFID authentication protocols, the process that reader and tag verify each other requires the participation of a trusted server. In Chien's scheme (Chien, 2007), reader first communicates with backend server through the security channel, and then gets initialization key shared with tag and initialization pseudonym IDS of tag. In Song and Mitchell (2008), reader transmits the message to trusted server through security channel after receiving message from tag. The server updates the tag information and sends validated data to reader after matching message successfully. This sort of authentication protocols cannot work in wearable devices environment, because there is no trusted third party and security channel in this unique environment.

Access Control List (ACL) technology is introduced in server-less RFID authentication protocols for the aim of reducing the participation of backend server. Tan et al. (2008) proposed a scheme that reader needs to authenticate itself in CA via safe channel and obtain its own access control list which contains information of legal tag in the setup phase before implementing mutual authentication. In Lee et al. (2012), reader firstly needs to verify itself in trusted backend server. Reader only authenticates tag whose ID in the ACL after downloading ACL. There is no need for backend server to participate in the process of reader and tag verifying each other. This kind of authentication protocols cannot be applied to wearable device environment for the similar reason thatthere is no trusted backend server and security channel to get ACL.

Wireless Sensor Network environment are regularly divided into static and dynamic WSN. In the static WSN, node-to-node authentication mainly depends on the MAC matching. Before starting authentication, each node will communicate with base station to gain a certificate and then one node can authenticate another (Vogt, 2004). Ren et al. (2008) proposed an authentication scheme based on geographical location information, but it does not meet the requirements of anonymity. Considering the dynamic WSN, node-to-node authentication should be cooperated with base station (Han and Shon, 2012). As a result, this method is not suitable for our environment as well.

3.2. Secure device pairing

With the popularity of personal wireless devices, Secure Device Pairing was proposed in recent years. It means that the process of building a secure channel between two previously unconnected devices based on some human-imperceptible communication channels. Due to the lack of trusted third-party the matching connection process is vulnerable to man-in-the-middle attacks (Li et al., 2011). To solve this problem, much previous work has combined cryptography protocols with different out-of-band (OOB) channels to provide more secure and efficient pairing schemes (Uzun et al., 2007; Kobsa et al., 2009; Prasad and Saxena, 2008). Balfanz et al. (2002) proposed a simple pairing protocol—"Talking to Strangers", which is based on one-way hash function and visual OOB channel-infrared communication. However, infrared transmission technology has already largely been replaced by other wireless transmission technologies and it is only available on some narrow fields. Gehrmann et al. (2004) proposed a manual authentication in wireless environment, which added the human factor into pairing process and regarded human as an auxiliary secure channel to transmit authentication messages. But both Balfanz et al. (2002) and Gehrmann et al. (2004) were based on a hypothesis that attackers cannot delay or replay any OOB information. Vaudenay (2005) firstly proposed a pairing protocol based on Short Authenticated Strings (SAS). It used commitment schemes to identify identity and needs 4 times of communication round to complete this certification process. The most important advantage of this protocol is that even if an attacker has delayed or replayed any OOB information, the success rate of attacking can also be limited to less than 2^{-k} if k-bit messages were transmitted. Laur and Nyberg (2006) and Pasini and Vaudenay (2006) proposed two variations based on Vaudenay (2005). McCune et al. (2005) proposed a scheme, so-called "Seeing is Believing (SiB)", in 2005. It adopted the concept of visual channel one device encrypts messages from OOB channel into two-dimension code (QR code) and displays it on the screen, then the paired devices read this code to get OOB information. Human are regarded as an auxiliary factor participating in authentication process. This method needs to meet the minimum requirement that at least one device has a camera and the other one has a display screen, so it is not suitable for low-end devices. Lately, based on McCune et al. (2005), Saxena et al. (2006) proposed a new method which is available for lower-requirements devices. This protocol used LED to transmit OOB information to the paired device. In addition, a kind of image comparison schemes was also proposed. The method encrypts OOB messages into image, then compares the two pictures on devices to check that whether they are the same (Goldberg and Fingerprint Code, 1996; Perrig and Song, 1999; Ellison and Dohrmann, 2003). However, these schemes have a high requirement for device revolution. There is also a series of schemes based on audio OOB channel (Goodrich et al., 2009; Soriente et al., 2008, 2007). However, at least one device needs to equip with a speaker or microphone and even sound is error-prone in noisy environment.

3.3. Bluetooth

Bluetooth technology is a form of wireless communication channels and it is widely used in varieties of industrial equipment. As many people know, it has some useful characteristics: a limited transmission distance (< 100 m) and a relatively wide bandwidth (Specification, 2001). During Bluetooth connection, the process that looking for mating-device is most time-consuming and it leads to the inefficiency of Bluetooth pairing. In order to reduce the time of Bluetooth connection, David et al. (Scott et al., 2005) proposed an idea of visual tags: it makes the Bluetooth device address as visual tags stored on the memory. When a device initiates Bluetooth connection request, it directly scans the visual tags displayed by the paired device, and then Bluetooth connectivity can be completed quickly.

Download English Version:

https://daneshyari.com/en/article/457171

Download Persian Version:

https://daneshyari.com/article/457171

Daneshyari.com