Computers and Electrical Engineering 000 (2017) 1–8

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Personal identification number entry for Google glass☆

Hwajeong Seo[a,*], Jiye Kim[b], Howon Kim[c], Zhe Liu[d]

[a] IT Convergence Engineering, Hansung University, Seoul, Republic of Korea
[b] Computer security, Sejong University, Seoul, Republic of Korea
[c] Computer engineering, Pusan National University, Pusan, Republic of Korea
[d] College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, China

ARTICLE INFO

Article history:
Received 7 October 2016
Revised 27 April 2017
Accepted 6 May 2017
Available online xxx

Keywords:
Google glass
User authentication
Personal Identification Number
Usability
Shoulder surfing attack

ABSTRACT

In this paper, we introduce secure and efficient Personal Identification Number (PIN)-entry technologies for representative Augmented Reality (AR) devices (e.g. Google glass). The AR device supports an overlay screen, which displays the AR images and information. Since the overlay screen is only practically visible to the device holders, the screen can be used to deliver the secret parameters without loss of information. By taking advantages of the new secure medium, we present PIN-entry technologies for AR devices. In the method, we display a password layout consisting of random numbers on the screen. The users correct the input password through the voice or touch gesture. When the password input layout is properly corrected, the users enter the current input password. To evaluate the proposed methods, we implemented the prototype products and tested their performances in terms of usability and security. The novel methods achieved high security levels against shoulder-surfing attacks together with practically high usability.

© 2017 Elsevier Ltd. All rights reserved.

1. Introduction

Rapid developments of wearable and ubiquitous computers enable the Augmented Reality (AR) services in practice. The most representative AR platform is Google glass released at February 2013 by Google. Unlike traditional computer environments, users can easily interact with the devices through the voice without time and space restrictions. Particularly, Google glass has small screen over the glass lens, which displays the additional and useful information to the users. However, the private and personal services in industry may handle the confidential information through Google glass platforms. To ensure the secure services, the access permission should be given to only authenticated users. The secure user authentication is usually performed with Personal Identification Number (PIN). Before the service access, the user need to present his identity and corresponding PIN information. When the identity and information are valid, the user can get the service access permission. However, traditional PIN-entry methods can be vulnerable to shoulder-surfing attacks. Even though users hide the password numbers, the adversaries can extract the password numbers from the user's gestures during PIN-entry and pre-knowledge of target layout. Many studies have been conducted to ensure the secure PIN-entry techniques over traditional mobile platforms [1–3]. The methods exploit the unique features of mobile platforms to hide or mask the password input

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

* Corresponding author.
E-mail addresses: hwajeong84@gmail.com (H. Seo), graekim@gmail.com (J. Kim), howonkim@pusan.ac.kr (H. Kim), sduliuzhe@gmail.com (Z. Liu).

http://dx.doi.org/10.1016/j.compeleceng.2017.05.006
0045-7906/© 2017 Elsevier Ltd. All rights reserved.

Please cite this article as: H. Seo et al., Personal identification number entry for Google glass, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.05.006

Table 1
Specifications of Google glass.

Features	Description
CPU	OMAP 4430
Display	Prism projector, 640 × 360 pixels
Controller	Touchpad
Camera	5 Megapixel photos, 720p video
Connectivity	WiFi, Bluetooth
Power	570 mAh
Weight	36 g

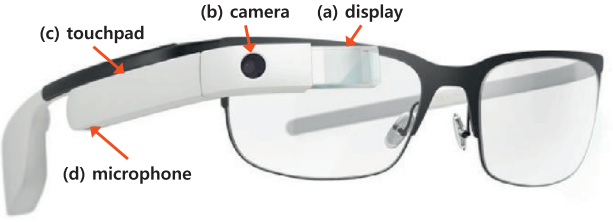

Fig. 1. Design of Google glass, (a) display, (b) camera, (c) touchpad, (d) microphone.

values. However, the emerging AR platforms have different features and user interfaces, which introduce new challenges in PIN-entry technologies.

In this paper, we present the PIN-entry methods for Google glass platform. The methods exploit the small overlay screen to display the secret values, since the screen is very small and cannot be practically captured by the adversaries. For Google glass authentication, we introduce the masked password, which only delivers the offset numbers to correct the input password. To evaluate the proposed method, we implemented and tested the prototype products. The novel methods achieved high security levels against shoulder-surfing attacks together with practically high usabilities.

This paper is organized as follows. In Section 2, we introduce the target AR device, namely Google glass, and the previous PIN-entry technologies on Google glass. In Section 3, we present the new PIN-entry methods for Google glass. In Section 4, we introduce prototype implementations and evaluate the performance in terms of usability and security against shoulder-surfing attacks. Finally, we conclude the paper in Section 5.

2. Related work

In this section, we explore the basic features of Google glass devices. Afterward, we introduce the previous authentication techniques for Google glass platforms.

2.1. Google glass

Google glass is developed by Google and manufactured by Foxconn. The device has become the most promising head-mounted augmented reality platforms [4,5]. The shape of device is a pair of eyeglasses and the input interfaces consist of built-in touch-pad, microphone, camera and various sensors. The touch-pad which receives swiping and tapping gestures from the user's fingertip, is located on the side of the Google glass devices. The camera located in front of Google glass has the ability to take photos and record 720p HD video. Google glass has very small LED illuminated display, which shows the overlay images over real user's view. This new feature enables the augmented reality application in practice by projecting the useful information through the screen. The body is lightweight and users can equip Google glass for long period without any burdens on the neck. However, the embedded battery power is very limited, which requires frequent power recharges to operate the devices. The device can be connected to the Internet or other platforms through WiFi and Blue-tooth networks. The detailed features and design of Google galss are given in Table 1 and Fig. 1, respectively.

2.2. PIN-entry method for Google glass

Since Google glass is emerging augmented reality platform, there are very few PIN-entry methods available. The first authentication method for Google glass is Blulletproof. The method allows the users to customize the combination of unlock gestures with single tap, long tap or fling left/right [6]. In December 2013, the official glass lock screen also became available after XE12 updates. This lock screen application allows a number of gestures including swiping forwards/backwards with one or two fingers, hook swipes and tapping with one/two fingers. When the users forget the password combinations, the password initialization is available through MyGlass website. Above approaches, however, do not ensure the security against shoulder-surfing attacks. If the adversaries can observe the user's gesture, the passwords are easily extracted from

Please cite this article as: H. Seo et al., Personal identification number entry for Google glass, Computers and Electrical Engineering (2017), http://dx.doi.org/10.1016/j.compeleceng.2017.05.006

Download English Version:

https://daneshyari.com/en/article/6883648

Download Persian Version:

https://daneshyari.com/article/6883648

Daneshyari.com