The Journal of Systems and Software 85 (2012) 1157–1165

Contents lists available at SciVerse ScienceDirect

The Journal of Systems and Software

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

A graphical-based password keystroke dynamic authentication system for touch screen handheld mobile devices

Ting-Yi Chang[a,*], Cheng-Jung Tsai[b], Jyun-Hao Lin[a]

[a] Graduate Institute of e-Learning, National Changhua University of Education, No. 1, Jin-De Road, 500 Changhua City, Taiwan, ROC
[b] Department of Mathematics, National Changhua University of Education, No. 1, Jin-De Road, 500 Changhua City, Taiwan, ROC

ARTICLE INFO

Article history:
Received 24 May 2011
Received in revised form
26 December 2011
Accepted 26 December 2011
Available online 11 January 2012

Keywords:
User authentication
Keystroke dynamics authentication
Keystroke feature
Graphical-based password authentication

ABSTRACT

Since touch screen handheld mobile devices have become widely used, people are able to access various data and information anywhere and anytime. Most user authentication methods for these mobile devices use PIN-based (*Personal Identification Number*) authentication, since they do not employ a standard QWERTY keyboard for conveniently entering text-based passwords. However, PINs provide a small password space size, which is vulnerable to attacks. Many studies have employed the KDA (*Keystroke Dynamic-based Authentication*) system, which is based on keystroke time features to enhance the security of PIN-based authentication. Unfortunately, unlike the text-based password KDA systems in QWERTY keyboards, different keypad sizes or layouts of mobile devices affect the PIN-based KDA system utility. This paper proposes a new graphical-based password KDA system for touch screen handheld mobile devices. The graphical password enlarges the password space size and promotes the KDA utility in touch screen handheld mobile devices. In addition, this paper explores a pressure feature, which is easy to use in touch screen handheld mobile devices, and applies it in the proposed system. The experiment results show: (1) EER is 12.2% in the graphical-based password KDA proposed system. Compared with related schemes in mobile devices, this effectively promotes KDA system utility; (2) EER is reduced to 6.9% when the pressure feature is used in the proposed system. The accuracy of authenticating keystroke time and pressure features is not affected by inconsistent keypads since the graphical passwords are entered via an identical size (50 mm × 60 mm) human–computer interface for satisfying the lowest touch screen size and a GUI of this size is displayed on all mobile devices.

1. Introduction

Whenever people use services such as e-bank and e-mail, servers should have the ability to authenticate the users' identities. Otherwise, anyone can easily impersonate a legal user to login to the server. Password-based authentication schemes are simple and practical solutions to user identification because they allow people to choose their own passwords without any device to generate or store them. For personal computers, passwords consist of letters, numbers, and special punctuations on a standard QWERTY keyboard. This is called text-based (alphanumeric-based) password authentication. Handheld mobile devices do not have standard QWERTY keyboard to conveniently enter text-based passwords. Mobile devices often use numeric passwords, which is called PIN-based (*Personal Identification Number*) authentication. Though the password space size of text-based passwords is larger than that of PINs (i.e., the password space size of an 8-character text-based password and an 8-digital PIN are $64^8 \cong 2.8 \times 10^{14}$ and 10^8, respectively), text-based passwords are preferred natural language phrases that people can recognize easily and are therefore susceptible to dictionary attacks. On the other hand, PIN-based authentication is widely used in mobile devices, but it provides a small password space size and therefore compromises security.

The KDA (*Keystroke Dynamic-based Authentication*) system was first proposed by Gaines et al. (1980). It is a biometric measurement method to provide additional security for text-based passwords. Many studies (Araújo et al., 2005; Bergadano et al., 2002; Bleha et al., 1990; Boechat et al., 2007; Chang and Yang, in press; Haider et al., 2000; Harun et al., 2010; Hwang et al., 2009b; Killourhy and Maxion, 2009; Ru and Eloff, 1997; Shih and Lin, 2008; Xi et al., 2011) have been proposed to improve the text-based password KDA system utility. KDA systems confirm the correctness of passwords and also identify users based on individual password keystroke time features. The keystroke time features include the duration of a keystroke (keystroke hold time) and the interval of the keystrokes (keystroke latency time). Even if the password is revealed by dictionary attacks or shoulder surfing

[*] Corresponding author. Fax: +886 4 7211290.
E-mail addresses: tychang@cc.ncue.edu.tw (T.-Y. Chang), cjtsai@cc.ncue.edu.tw (C.-J. Tsai).

0164-1212/$ – see front matter © 2011 Elsevier Inc. All rights reserved.
doi:10.1016/j.jss.2011.12.044

attacks, the probability of breaking authentication is reduced. The KDA system has the following advantages. It is low-cost with no extra device to obtain the user's features, and does not require complex computations to capture the user's features. Since the process of capturing features is done when the user enters his or her password, it does not create any additional burden on users. Compared with other biometric authentication methods such as fingerprints, eye scan, iris, and signature, the KDA system is simple and useful for providing additional security in identity verification.

As is well known, mobile devices are widely used for accessing various data and information. Campisi et al. (2009) proposed a text-password KDA system that uses a cellular phone keypad. On the other hand, many studies (Clarke and Furnell, 2007a,b; Hwang et al., 2009a) have applied KDA systems to enhance the security of PIN-based authentication in mobile devices. However, the sizes or layouts of keypads of the mobile devices produced by different manufacturers are inconsistent. A user may not get used to entering his or her PIN or text-based password through different mobile devices. This will result in the user's features being entered inconsistently and KDA system verification failing if users enter their PINs or text-based passwords through difference mobile devices. Consequently, the KDA system utility for mobile devices (Campisi et al., 2009; Clarke and Furnell, 2007a,b; Hwang et al., 2009a) is worse than that for QWERTY keyboards (Killourhy and Maxion, 2009; Shih and Lin, 2008).

This paper develops a novel graphical-based password KDA system to improve PIN-based authentication for mobile devices. The password space size of the proposed system is larger than those of PIN-based authentication schemes. Regardless of the size of the user's mobile touch screen, users enter their graphical passwords through clicking or touching an identical human–computer interface. Therefore, the accuracy of users authentication is not affected by inconsistent keypads. In addition, this paper explores the pressure feature, which is a new biometric keystroke feature found in touch screens. The proposed graphical-based password KDA system is implemented in an Android-compatible phone. Serial experiments show the utility of the proposed graphical-based password KDA system is better than the related text-based password and PIN-based KDA systems (Campisi et al., 2009; Clarke and Furnell, 2007a,b). Moreover, when the pressure feature is applied in the proposed system, it further promotes system utility.

The organization of this paper is as follows. Section 2 reviews and discusses studies on graphical-based password authentication and the PIN-based KDA system, respectively. Section 3 proposes the architecture of the methodology, which includes the enrollment phase, the classifier building phase, and the authentication phase. The pressure feature is also introduced in this section. Section 4 presents the experimental results of this paper and compares them with other related studies. At the same time, the performance of the proposed system is presented. It is suitable for low-power mobile devices. Finally, conclusions are given in Section 5.

2. Related works

To improve on the drawbacks of PIN-based KDA systems, this paper first combines a graphical password with the KDA system. This section introduces these two related studies in Sections 2.1 and 2.2, respectively.

2.1. Graphical-based password authentication

The common method for identity authentication is text-based password authentication. In terms of security, a text-based password should consist of a string of eight or more random characters. However, a user is limited by the ability of his or her long-term memory to remember passwords. If the length of the text-based passwords is long, a user's memory load is heavy. Further, people may frequently forget and confuse their text-based passwords (Wiedenbeck et al., 2005a). Users typically cope with text-based password problems as follows. First, they write down their passwords. Second, they use one password for many systems. Third, natural language phrases are preferably used as passwords so they can be recognized easily. However, this leads to some text-based passwords becoming weak passwords that are vulnerable to dictionary and shoulder surfing attacks.

Graphical-based password authentication is an alternative method to withstand dictionary attacks, as originally described by Blonder (1996). Today, graphical-based password authentication can be divided into two categories: recognition-based and recall-based graphical passwords. Recognition-based systems authenticate the users' identities based on a sequence of images selected and remembered by users. These include the Passface system (Brostoff and Sasse, 2000) and Déjà Vu system (Dhamija and Perrig, 2000). However, they are vulnerable to shoulder surfing attacks. As such, Sobrado and Birget (2002) have developed convex-hull click, movable frame, and intersection to withstand such attacks (please see Sobrado and Birget, 2002 for more details). Further, Wiedenbeck et al. (2005a) extended Blonder's idea and developed the PassPoint system. In Weidenback et al.'s method, a user clicks on an image to create his or her graphical password and a tolerance around each chosen pixel is calculated. To authenticate identity, users must click within the tolerance of their chosen pixels and also in the correct sequence. Therefore, the password space size in Weidenback et al.'s method is larger than text-based passwords. On the other hand, the best known recall-based method is DAS (Draw-A-Secret), proposed by Jermyn et al. (1999). In their method, a user is asked to draw a simple picture on a 2D grid, and then the system authenticates the user's identity based on the order of the drawn picture. Moreover, Syukri et al. (1998) used a signature as a substitute for drawing a simple picture. The advantage of using the signature is it is self-given and difficult to copy. Unfortunately, most users require additional devices to finish their signatures since they are not used to writing their signatures with a mouse. Thus, this is inconvenient for users.

Recently, touch screen handle mobile devices have been becoming more widespread. A user inputs his or her password by clicking or touching the touch panel. Because the touch screen size is too small, Sobrado et al.'s and Weidenback et al.'s methods are unsuitable for authentication in mobile devices. Therefore, Jansen (2003) proposed a recognition-based graphical password authentication system for mobile devices. Jansen's system divides an image (e.g. sea, cat, etc.) into thirty thumbnail photos. A user selects several different thumbnail photos and the sequence of these thumbnail photos is the user's graphical password. Further, Jansen (2004) improved his method by allowing the thumbnail photos to be chosen repeatedly. Therefore, the password space size is larger than before. For example, a user chooses three photos and then the password space size is enlarged from $30 \times 29 \times 28$ to 30^3. However, Jansen's methods still cannot withstand shoulder surfing attacks.

The graphical-based password authentication has the following advantages. First, a person's long-term memory need not store all the images, but rather a meaningful interpretation (Mandler and Ritchey, 1977). Psychologists have shown images are remembered more easily than words or sentences (Mandler and Ritchey, 1977; Revett et al., 2005; Wiedenbeck et al., 2005a). In this case, a user is able to remember a complex password and then the password space size will be larger. Second, these graphical-based password authentication methods assume the number of possible images is sufficiently large. Thus, the password space size of the graphical passwords is larger than the text-based passwords. Third, it is able to withstand dictionary attacks. Since the recognition-based