

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320-088X

IJCSMC, Vol. 3, Issue. 3, March 2014, pg.540 – 544

RESEARCH ARTICLE



DooDB: A Graphical Password Database Consist of Doodles and Pseudo Signature Based User Authentication

Miss. Yugandhara A.Thakare¹, Prof.A.S.Kapse²

¹CSE Department, P.R.Patil, COET, Amravati, SGBAU, India

²CSE Department, P.R.Patil, COET, Amravati, SGBAU, India

¹yugathakare@gmail.com ; ²kapse.arvind@yahoo.com

Abstract— Most of the computer user has to remember the alphanumeric password or PIN consist of combination of numbers, characters and symbols for different kind of application which may intern increases load of user in remembering per application username and password. This method has been shown to have significant drawbacks. For example, users tend to pick passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem and for reducing the cognitive load on the user we have presented DooDB containing Doodles and Pseudo Signature. Here the focus is upon doodle based password which is subset of recall graphical passwords. Users are authenticated by asking to draw with their fingertip a doodle on a handheld device touch screen which is captured and further used for verification. There were no restrictions regarding duration or shape.

Keywords— Doodles; Graphical password; Pseudo signature; DooDB

I. INTRODUCTION

Nowadays, user authentication is an important issue regarding security. Strong text-based password could provide certain degree of security to the user. Graphical password is an alternative solution to the text based password authentication scheme, motivated by the fact that humans can easily remember images better than text. Nowadays many internet based environments try to use graphical authentication scheme for user authentication. Due to their graphical nature they are easy to remember than alpha numeric password [1].

Doodle based authentication scheme is a lightweight user verification method. The use of graphical passwords for user validation is receiving an increasing interest in the last years as touch screen enabled devices proliferating in the market. In this paper we are focusing upon DooDB which consist of Doodles and pseudo-signatures. DooDB is subset of recall based graphical password. Users are authenticated by asking to draw with their fingertip a doodle on a handheld device touch screen which is captured and further used for verification. By taking quantitative analysis of forgeries & captured dataset, preliminary verification experiments using the two kinds of graphical are reported.

II. CLASSIFICATION OF GRAPHICAL PASSWORD BASED SYSTEMS

Graphical passwords schemes can be classified into four categories: Recognition based Systems, Pure Recall based systems, Cued Recall based systems & Hybrid systems. Recognition based techniques involve identifying whether one has seen an image before. The user must only be able to recognize previously seen images, not generate them unaided from memory. Second is Pure Recall based systems, in pure recall-based methods the user has to reproduce something that he/she created earlier during the registration stage. Third is Cued Recall a based system, in cued recall-based methods, a user is provided with a hint so that he/she can recall his/her password. Fourth is Hybrid systems which are typically the combination of recognition and recall based or textual with graphical password schemes.

III. RELATED WORK

There are different approaches have been proposed in the literature review starting from the survey to the unlock patterns used in Android which is a simplified version of the Pass-Go scheme. A survey of the techniques presented has been reported recently in [3].After that Draw-A-Secret system (DAS) [4] made another contribution in this field, in which a grid is provided for tracing the graphical password of user and sequence drawn by the user on grid is then stored and further used for validation purpose. User is validated only if current sequences of cell match the stored grid sequence. Hand-drawn doodle password ("passdoodle") and its verification system was later introduced in [5],[7].In this Users perceive passdoodles as easier to remember than alphanumeric passwords. This preliminary study was carried out by the group of 39 users. The doodle verification scheme Scribble-A-Secret (SAS) was later proposed [6].A verification scheme based on predefined visual cues is presented which is general common shapes are chosen by the user with the aid of a graphical interface. With these cues each user creates pseudo signature. Then from the pseudo-signatures Cryptographic keys are generated. Experimental results are reported using a database of 37 subjects, which includes forgeries is in [8]. In the so called Android

Unlock Pattern scheme, the user is presented a 3×3 grid and the secret (password) of a user is a drawing on that grid (i.e., a sequence of lines connecting the dots). During enrollment, a user has to choose a pattern and during the authentication phase, he has to recall his pattern and draw it on the screen. Here only the sequence of points is stored as a password. Various data analyses regarding doodle have been performed in [9].

IV. THE DooDB DATABASE

This database comprises two sub corpora: doodles and simplified signatures i.e. pseudo signatures. These data were produced by 100 users, who were asked to draw with their fingertips over a mobile device touch screen. There were no restrictions regarding duration or shape. Forgeries are also included in the database. In case of pseudo signature also participants are asked to draw their signature which the user can consider as graphical password. Acquisition can be done by examining the co-ordinates of fingertip position over a screen as user passes the screen. If we consider x and y as co-ordinates and t as discrete time and if co-ordinate values represent milli-inches then the values of x_t and y_t may range between $[0,2000]$ and $[0,3500]$. The time interval Δt between consecutive samples is also stored. Examples of doodles and pseudo signature are shown in Figure1. To avoid that users forgot their doodles the acquisition process was divided in to sessions in order to allow enough inter-session variability. The donors were allowed to practice their drawings until they felt comfortable with them. Forgeries have also been captured in this database. For performing forgeries, users had visual access to the doodle or pseudo-signature they had to imitate. The acquisition software replayed the strokes on the screen showing their dynamic properties e.g. speed. Till the user become confident with their forgery the animation was shown to users.

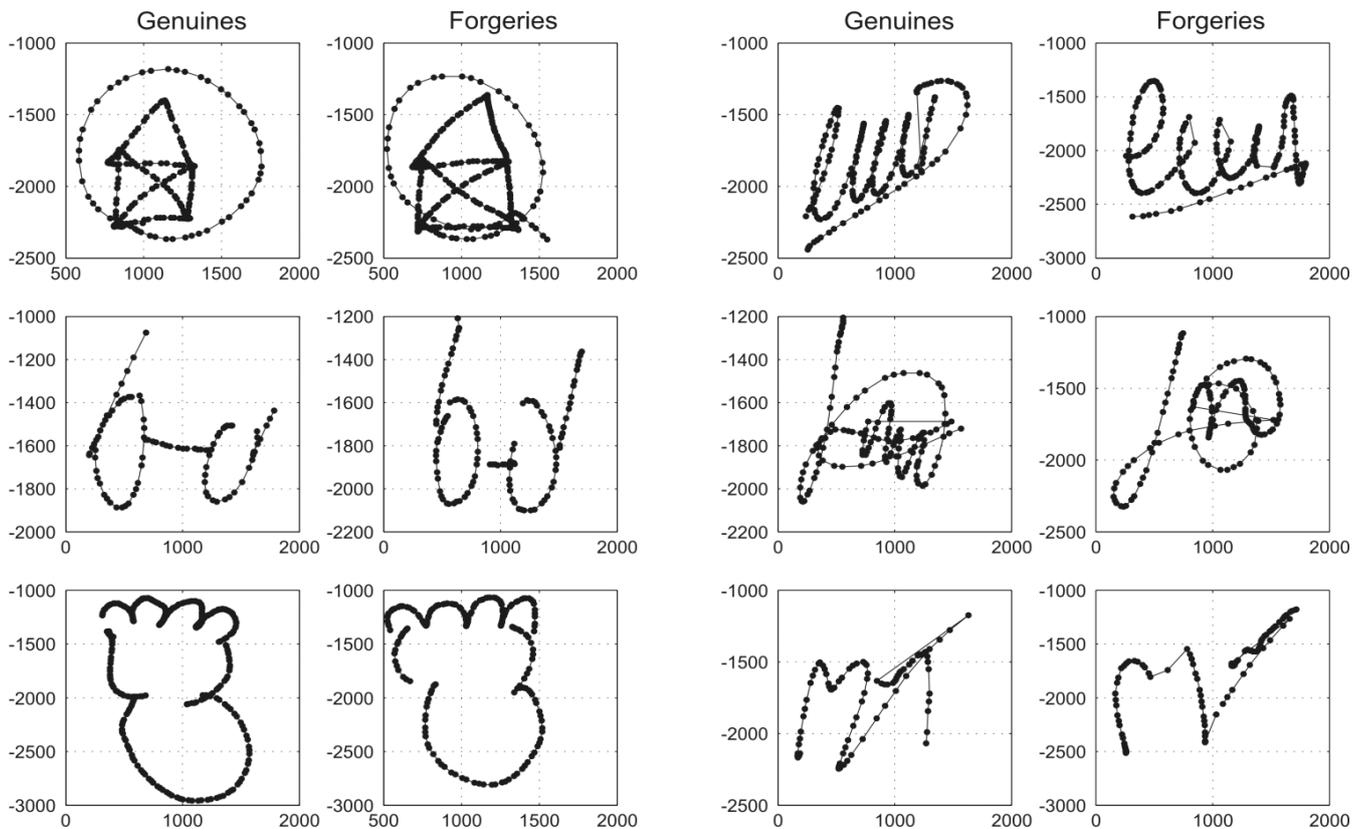


Figure 1. Examples of doodles (left) and pseudo-signatures (right)

V. CONCLUSIONS

DooDB a Graphical Password Database Consist of Doodles and Pseudo Signature has been presented. In which users are authenticated by asking to draw with their fingertip a doodle on a handheld device touch screen which is captured and further used for verification purpose. This database comprises doodles and pseudo-signatures from 100 users and skilled forgeries for all of them. The acquisition protocol has been described for verifying the doodles and pseudo signature for protection against forgeries. In most cases, users invented their own doodle at the time of acquisition, so, Doodle based authentication scheme is a lightweight user verification method.

REFERENCES

- [1] K. Renaud, ``*On user involvement in production of images used in visual authentication*,'' J. Vis. Lang. Comput., vol. 20, no. 1, pp. 1_15, 2009.
- [2] X. Suo, Y. Zhu, and G. Owen, ``*Graphical passwords: A survey*,'' in Proc. 21st ACSAC, 2005, pp. 463_472.
- [3] R. Biddle, S. Chiasson, and P. Van Oorschot, ``*Graphical passwords: Learning from the first twelve years*,'' ACM Comput. Surveys, vol. 44, no. 4, pp. 19:1_19:41, 2012.
- [4] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, ``*The design and analysis of graphical passwords*,'' in Proc. 8th USENIX Security Symp., 1999, pp. 1_14.
- [5] J. Goldberg, J. Hagman, and V. Sazawal, ``*Doodling our way to better authentication*,'' in Proc. CHI, Extended Abstracts Human Factors Comput. Syst., 2002, pp. 868_869.
- [6] M. Oka, K. Kato, X. Yingqing, L. Liang, and F. Wen, ``*Scribble-a-secret: Similarity-based password authentication using sketches*,'' in Proc. ICPR, 2008, pp. 1_4.
- [7] C. Varenhorst, ``*Passdoodles: A lightweight authentication method*,'' (2004) Res. Sci. Inst., Massachusetts Inst. Technol., Cambridge, MA, USA, Tech. Rep. [Online]. Available: http://people.csail.mit.edu/emax/public_html/papers/varenhorst.pdf.
- [8] J. Chen, D. Lopresti, and F. Monrose, ``*Toward resisting forgery attacks via pseudo signatures*,'' in Proc. 10th ICDAR, 2009, pp. 51_55.
- [9] Marcos Martinez-Diaz, Julian Fierrez (Member, Ieee), And Javier Galbally, ``*The DooDB Graphical Password Database*'' in Proc. IEEE VOLUME 1, 2013