PASSWORD MANAGEMENT USING DOODLES

Naveen Sundar G and Sriganesh Madhvanath
HP Laboratories India

HPL-2007-157
September 20, 2007*

doodles; password management

The average computer user needs to remember a large number of text username and password combinations for different applications, which places a large cognitive load on the user. Consequently users tend to write down passwords, use easy to remember (and guess) passwords, or use the same password for multiple applications, leading to security risks. This paper describes the use of personalized hand-drawn "doodles" for recall and management of password information. Since doodles can be easier to remember than text passwords, the cognitive load on the user is reduced. Our method involves recognizing doodles by matching them against stored prototypes using handwritten shape matching techniques. We have built a system which manages passwords for web applications through a web browser. In this system, the user logs into a web application by drawing a doodle using a touchpad or digitizing tablet attached to the computer. The user is automatically logged into the web application if the doodle matches the doodle drawn during enrollment. We also report accuracy results for our doodle recognition system, and conclude with a summary of next steps.

* Internal Accession Date Only
♦ ICMI'07, November 12-15, 2007, Nagoya, Aichi, Japan
Approved for External Publication

PASSWORD MANAGEMENT USING DOODLES

Naveen Sundar G, Sriganesh Madhvanath
Hewlett-Packard Labs
Bangalore, India
{naveensundarg, srig}@hp.com

ABSTRACT

The average computer user needs to remember a large number of text username and password combinations for different applications, which places a large cognitive load on the user. Consequently users tend to write down passwords, use easy to remember (and guess) passwords, or use the same password for multiple applications, leading to security risks. This paper describes the use of personalized hand-drawn "doodles" for recall and management of password information. Since doodles can be easier to remember than text passwords, the cognitive load on the user is reduced. Our method involves recognizing doodles by matching them against stored prototypes using handwritten shape matching techniques. We have built a system which manages passwords for web applications through a web browser. In this system, the user logs into a web application by drawing a doodle using a touchpad or digitizing tablet attached to the computer. The user is automatically logged into the web application if the doodle matches the doodle drawn during enrollment. We also report accuracy results for our doodle recognition system, and conclude with a summary of next steps.

Categories and Subject Descriptors

H.5.2 [**Information Interfaces and Presentation**]: User Interfaces - *Input devices and strategies.* K.8.3 [**Personal Computing**]: Management–*Password Information Management*

General Terms

Design, Experimentation, Human Factors

Keywords

Doodles, Password Management

1. INTRODUCTION

The average computer user needs to remember a large number of text username and password combinations for different applications on his or her local machine, intranet at work, and the internet. In particular, there are a large and growing number of web-based applications including online banking, travel websites and email that require users to authenticate themselves on a daily basis. Users tend to choose passwords which can be easily recalled, and hence are also easy to crack. For example, in [1], the authors report that out of 14000 passwords studied by them, nearly 25% were found in a dictionary of $3x10^6$ words. Furthermore, users also tend to write down their passwords and use the same password for multiple applications, leading to security risks.

Password management systems have been introduced to address the above concerns. A password management system is a system which manages multiple username and password combinations for the user, corresponding to different local or web applications. The username and password combinations can be accessed either through another password (master password) or through a biometric such as a fingerprint. Master-password based password management systems have some shortcomings. While biometric password management systems address these concerns effectively, they give rise to privacy issues. These issues are discussed in detail later in this paper.

In this paper, we describe the use of hand-drawn doodles for password management. This method involves recognizing doodles as sequences of (x, y) coordinates by matching them against stored prototypes using handwritten shape matching techniques. Doodle based password management systems can potentially overcome the limitations of text and biometric based password management systems. Furthermore, with touch screens, touch pads and other pen/touch input devices becoming more common on client devices, the hardware cost factor in using doodles for password management is becoming a non-issue.

The paper is organized as follows. In Section 2, we briefly discuss text and biometrics based password management systems, and some of their shortcomings. In Section 3, we introduce the idea of using doodles for password management and present relevant prior art. In Section 4, we describe a system that we have built which manages passwords for web applications through a web browser. Section 5 describes some of the experimental evaluation we are doing for benchmarking doodle recognition accuracy. We present some conclusions and discuss next steps in the final section.

2. PASSWORD MANAGEMENT SYSTEMS

As mentioned previously, password management packages are now available for remembering and managing the various username and password combinations for different applications. Versions of these are integrated into browsers such as Internet Explorer and Firefox, and available as stand-along packages. These are based on storing the password information for different applications in encrypted form, and securing them using a “master password”, which is again a text password. Text passwords are very popular due to a number of reasons. One among them is that no additional hardware is required for

ICMI’07, November 12–15, 2007, Nagoya, Aichi, Japan.

entering passwords into a computer. However, allowing single sign-on onto disparate systems using a single text password exposes those systems to the inherent disadvantages of using text passwords. Clearly more complex master passwords are needed for greater security, but are also more difficult to remember for end users. Easy to recall passwords are also easy to guess or hack. Text passwords may also be clandestinely captured via keystroke capturing spyware. Also, text passwords are difficult and time consuming to enter on small devices such as PDAs and mobile phones, since they typically are not dictionary words, and have to be entered a character at a time.

As an alternative to text passwords, biometrics, such as fingerprints have also been used to verify the user's identity and provide access to the stored password information. This solution requires a special sensor for the biometric. Also, since a user's biometrics are fundamental parts of his or her identity, and may also be used for many other purposes besides access to applications, the risks from this information being stolen or otherwise captured are extremely high. Once compromised, biometrics are difficult (if not impossible) to change. Further, biometrics, like fingerprints, can be traced back to the user and hence are not anonymous as text passwords. Though systems which store biometric information in a hashed form exist [6], they don't guarantee complete anonymity. Once we have a user's biometric information we can easily check whether the user is enrolled in a system.

3. DOODLE BASED PASSWORD MANAGEMENT

The key idea of this paper is to use a hand-drawn "master doodle" to access stored password information, instead of using text passwords or biometrics. The construction of the password management system and components such as secure storage of username/password information and associations with different applications, is similar to that of any password management system, and is hence not described here. At the time of setup, the user is asked to register his or her master doodle. The doodle can be drawn with a pen or a finger and requires a digitizer. With the proliferation of touchpad-enabled notebook computers and pen or touch-interfaces on mobile devices, we do not see this as a shortcoming of the solution. In fact any form of available mouse device may also be used, but in general these are less convenient for drawing with. The doodle in general may or may not have any interpretation (e.g. as a picture or signature), may use one or more strokes, may be short or long, and is restricted only by the size of the drawing area. The only criterion is that the user must select a master-doodle that he/she can recall subsequently.

In general, between one and three samples of the master doodle are collected at the time of enrollment. The doodle samples are stored as sequences of (x,y) coordinates along with pen-up and down events. When the user needs to access an application locally or on the web, he/she is prompted to draw his or her personal master doodle. The doodle is matched against the stored samples obtained during registration using standard handwritten shape matching techniques. Based on a threshold on the match score, the doodle is either accepted or rejected. If accepted, the password information corresponding to the application is retrieved, and the user is authenticated into the application.

The use of doodles in lieu of text passwords has been explored previously in other contexts. In [2], the authors propose graphical passwords as a novel form of authentication. The authors show that the space of all possible doodles is larger than the space of passwords. A brief survey of studies which show that pictures are easier to recall than words is presented by the authors. In [2] the authors report their findings from a user study based on doodles. It was found that users remember doodles as well as passwords if stroke order variations are not taken into account. Doodles have been proposed for "lightweight authentication" and personalization of public devices such as information kiosks in airports [7]. The authors use a large number of samples (ten samples per doodle) during training (i.e. registration). In a realistic scenario one cannot expect a user to enter more than a few samples during enrollment. In the experiments reported in this paper, we assume that a user enters only one doodle during enrollment.

Table 1 presents a comparison of different password management methods. Even without taking into account the fact the people use easy to guess passwords, the size of the possible doodle space is much larger than space of all possible text passwords [3]. Furthermore, unlike in the case of textual passwords, there exist no precompiled dictionaries for doodles which could the render the task of guessing a doodle easy. Using the above two arguments it can be argued that doodles are more secure than text passwords [3,5].

Table 1: Comparison of Password Management Methods

Passwd Mgmt	**H/W Cost**	**Security**	**Recall**	**Anony -mity**	**Ease of Use**
Text	Low	Low	Low	High	Med
Doodle	Low-Med	Med	Med	High	High
Biometric	Med-High	High	High	Low	High

Doodles are clearly more anonymous than biometrics and in general, more than text passwords, given that people often select familiar strings such as names and birthdays for text passwords. They are also significantly easier and faster to enter than text passwords, especially on touch-based interfaces where a soft keyboard is often the only option available for text input. Hardware cost is based on whether a user would require a hardware device that is used exclusively for the password management/authentication (and not used as an input device). Our assertion that doodles can be easier to recall than passwords is based on a number of studies which show that pictures in general are easier to recall than words [3]. However this assertion still needs to be validated in the specific case of doodles.

4. BROWSER DOODLES

We have implemented a system for managing passwords of web applications, which increasingly constitute the largest subset of commonly used applications for most users. In this system, a user chooses a master doodle for his/her account. All passwords of the user are protected by this master doodle. The master doodle can in turn be protected by a master password, if needed. One sample of the master doodle is collected during enrollment. Since our system is designed primarily to work on notebook computers equipped with integrated touchpads, visual feedback while doodling is provided using a separate doodle window.

When a user visits a password protected page, the user enters the username and password for that site into the system, for enrolling/registering that particular page with the password management system. The username and password are stored in a database along with web application's URL.

When the user visits the same page again, he can log into the system by the drawing his doodle using the entire touchpad, and using the doodle window for feedback (Figure 1). If the doodle closely matches the master doodle, the username and password for that website are retrieved from the database and the user is logged into the site automatically. In addition, the user may also directly enter the username or password instead.

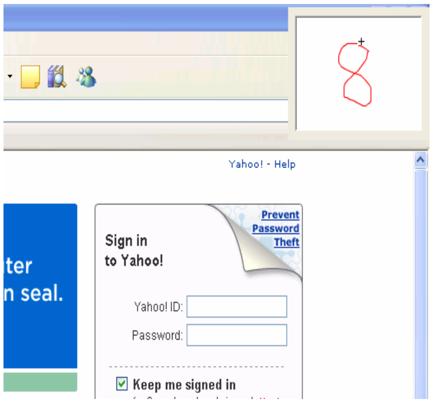

Figure 1. Application login using a doodle. Visual feedback while doodling is provided using a small window.

5. DOODLE RECOGNITION

The core problem in using doodles instead of passwords is that of matching hand-drawn shapes which exhibit some variability every time they are drawn.

During enrollment, one cannot expect a user to draw more than one or two samples of the master doodle. Ideally, the doodle matching system should be able to perform robustly with a single sample of the user's doodle.

For our initial experiments, we have used handwritten Tamil characters drawn from the Tamil isolated character dataset [8] as examples of doodles. We selected this dataset because of the availability of multiple samples per character for several users, and the presence of both single stroke and multi stroke characters, and abstract shapes. Although the data may not be representative of doodles users may come up with, and is collected using TabletPCs and PDAs rather than touchpads, it allows us to design and benchmark algorithms for doodle recognition.

One way to evaluate doodle recognition accuracy in the password management context would be to evaluate the False Reject and False Accept rates when doodle samples from a user, and random other doodles respectively are matched against one or more samples of the user's master-doodle.

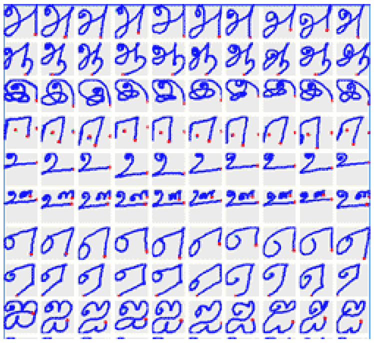

Figure 2. Sample characters from Isolated Handwritten Tamil Character Dataset hpl-tamil-iso-char.

Since our present focus is on comparing different sets of features for matching doodles, we have selected the first 50 character classes from the database, and cast the doodle matching problem as a 50-class recognition problem, rather than a verification problem. The hypothesis is that features that are intrinsically better at capturing the shape of the doodle in the identification (recognition) context will also work well in the verification context.

Data from ten different users was used in the evaluation, and the recognition accuracy was computed for each user separately and averaged. For each user, a set of prototypes was constructed by selecting one random sample per pattern class, for a total of 50 x 1 = 50 prototypes. The test set used for evaluating recognition accuracy for that user was composed of five samples (different from the one selected for training) for each class, for a total of 50 x 5 = 250 samples. Both training and test samples were subjected to the same preprocessing: they were normalized to a constant size, smoothed, and resampled uniformly along the trajectory to yield a fixed number of points. Multi-stroke characters were treated as single-characters by ignoring the stroke transitions and concatenating the strokes. All the characters were resampled to sixty points. We experimented with 1-nearest neighbor classification using different features and distance measures.

5.1 Features

The features we tried included x and y coordinates of the doodles (after preprocessing the sample as described), the normalized first and second derivatives [4], and the curvature value at each point. Let x_i and y_i be the i^{th} point in the input character/doodle. First derivatives x_i at and y_i are computed as:

$$x'_i = \frac{\sum_{i=1}^{r} i.(x_{i+1} - x_{i-1})}{2.\sum_{i=1}^{r} i^2} \quad , \quad y'_i = \frac{\sum_{i=1}^{r} i.(y_{i+1} - y_{i-1})}{2.\sum_{i=1}^{r} i^2}$$

where the value of r determines the number of neighboring points used in the computation. (We used r=2.) From the first derivatives the *normalized* first derivatives are computed as:

$$\hat{x}'_i = \frac{x'_i}{\sqrt{x'^2_i + y'^2_i}} \quad , \quad \hat{y}'_i = \frac{y'_i}{\sqrt{x'^2_i + y'^2_i}}$$

The normalized second derivatives are calculated in a similar manner. The curvature is computed as

$$\kappa_i = \frac{x'.y'' - x''.y'}{\left(x'^2 + y'^2\right)^{3/2}}$$

where *x′*, *y′* and *x″* and *y″* are the normalized first and second derivatives respectively.

5.2 Distance Measures:

We experimented with both Euclidean and Dynamic Time Warping (DTW) distance in our experiments. DTW is a technique which uses dynamic programming to find the optimal alignment between any two time series or sequences, by warping one of the time series non-linearly along its time axis. This warping based alignment between the sequences can then be used to find the dissimilarity/distance between them. Let *P* and *Q* be 2 time series of lengths *m* and *n* given by:

$$P = p_1, p_2, \ldots\ldots\ldots p_i \ldots p_m$$
$$Q = q_1, q_2, \ldots\ldots\ldots q_i \ldots q_n$$
$$\text{where } p_i = \{ x_{\mathrm{Pi}}, y_{\mathrm{Qi}} \}.$$

A 2 dimensional cost matrix *C* of size *m* by *n* is generated where the value at *C*(*i*,*j*) is given by:

$$C(i, j) = d(p_i, q_j) + \min(C(i-1, j), C(i-1, j-1), C(i, j-1))$$

$d(p_i,q_j)$ is the local distance between two points in the series. In our experiments we used the Euclidean distance between points as the local distance measure. The computation starts at *C(1,1)* and ends at *C(m,n)*. *C(m,n,)* gives the DTW distance between the two sequences. To speed up the DTW computations, the Sakoe-Chiba band constraint [9] was used with the width of the band set to 40.

5.3 Empirical Results:

Table 2 given below shows the recognition accuracies from using two different sets of features, and two distance measures (Euclidean and Dynamic Time Warping (DTW)).

Table 2: Doodle Recognition Results

Features	Distance Measure	Avg Accuracy (%)
X-Y	DTW	86.12
X-Y, Normalized First, Second Derivatives and Curvature	DTW	90.56
X-Y	Euclidean	77.48

From Table 2, it is clear that despite normalizing all samples to a constant number of points, DTW distance is a much better distance measure when compared to Euclidean distance, for doodle data. We were able to achieve an overall accuracy of 90.56 % on this dataset, which is very encouraging considering that (i) the final usage scenario involves verification with the possibility of rejection, (ii) this result is using a single training sample of each doodle, and that we can expect accuracy to improve significantly as more samples of the user's doodle become available as a byproduct of usage.

6. SUMMARY AND NEXT STEPS

In this paper, we have described a novel method of password management based on doodles. Doodle based password management systems can be potentially better than text or biometrics based password management system due to greater anonymity and ease of use. We also presented a browser based password management system that we have. This system allows users to sign in into websites using a single personal doodle, known as the master doodle.

We have presented preliminary results on doodle recognition based on a dataset of Tamil symbols, using a single sample for "training". These results illustrate the feasibility and security of doodle based password management based on only a few registration/enrollment samples. We are working on studying the impact of adaptation on accuracy using different adaptation schemes; we expect substantial increases in accuracy from a small number of additional training samples. We are also in the process of collecting real doodle samples using the notebook touchpad from a set of users over a period of time, to simulate the final application scenario.

Finally, we plan to conduct a large-scale user study with the final adaptation-enabled system in order to measure users' ability to recall doodles, and to understand usability and user acceptance of the proposed solution.

9. REFERENCES

[1] Klein, D. "Foiling the cracker: A survey of, and improvements to, password security". *In Proceedings of the 2nd USENIX Security Workshop*, August 1990.

[2] Goldberg, J., Hagman, J., and Sazawal, V., "Doodling our way to better authentication", *CHI '02 extended abstracts on Human factors in computing systems*, ACM Press, Minneapolis, Minnesota, USA, pp.868–869, 2002.

[3] Jermyn, I., Mayer, A., Monrose, F., Reiter, M., & Rubin, A., "The Design and Analysis of Graphical Passwords". *Proceedings of the 8th USENIX Security Symposium.* The USENIX Association, Washington, D.C., U.S.A, 1999.

[4] Pastor, A. Toselli, and E.Vidal, "Writing Speed Normalization for On-Line Handwritten Text Recognition", *Proc. of ICDAR'05*, Seoul, 2005, pp. 1131-1136.

[5] R. N. Shepard. Recognition memory for words, sentences, and pictures. *Journal of Verbal Learnings and Verbal Behavior*, 6: 156-163, 1967.

[6] U. Uludag, S. Pankanti, S. Prabhakar, and A.K. Jain, "Biometric Cryptosystems: Issues and Challenges," Proc. IEEE, vol. 92, no. 6, pp. 948-960, June 2004.

[7] Varenhorst, C. "Passdoodles: A lightweight authentication method" *http://oknet.csail.mit.edu/papers/varenhorst.pdf 2004*

[8] *http://www.hpl.hp.com/india/research/penhw/resources/tamil-iso-char.html*

[9] H. Sakoe and S. Chiba, "Dynamic Progamming Optimization for Spoken Word Recognition", *IEEE Trans. On Acoustics, Speech and Signal Processing, vol. 26, pp. 623-625, 1980*