SportsFaces: A Graphical Password System based on Images of Sports Celebrities

Sajida Kalsoom, Sheikh Ziauddin and Muhammad Tahir

Department of Computer Science
COMSATS Institute of Information Technology, Islamabad, Pakistan

Abstract: In many cases, human-selected text passwords are either too easy to guess or too difficult to memorize. Graphical passwords reduce the memory burden of users by replacing the task of recalling the password to that of recognizing the password. In this paper, we present a graphical password scheme based on the images of sports celebrates. Experimental evaluation shows that the retention time of the proposed SportsFaces is greater than alphanumeric password systems.

1 Introduction

Entity Authentication refers to the set of techniques where users have to prove the claim of their identity to the identifier. Users can be authenticated in one of the following three ways: i) what they know (e.g., password) ii) what they have (e.g., smart card) and iii) what they are (e.g., biometrics). Most commonly used authentication schemes are password based schemes [HL00, YRY05, HS09, LLW10] due to their cost-effectiveness and need for minimal infrastructure. The other two techniques are costly and require sophisticated infrastructure especially biometric-based schemes [ZD10, Dau04, TP02].

Among password based schemes, alphanumeric passwords are most common but they have their problems too. Weak passwords are easily guessable (security issues) e.g. using dictionary attacks while strong passwords are generally difficult to memorize for a user (usability issues). Although different strategies are used to overcome these shortcomings e.g. users are asked to select alphanumeric password of some specific length, use combination of small and capital letters and choose some unpredictable special characters, etc. But despite of these tactics, the problems of security and usability are still there. Users generally ignore the recommendations to create secure password. Another major limitation is human memory and especially its two functions: information storage and information retrieval. These two functions vary widely from person to person and are affected by the choice of strings for passwords. Thus, alternative to text-based passwords, are the graphical passwords which are cost-effective and potential solutions to these problems.

Graphical passwords are relatively easier to retrieve as compared to text-based passwords because they involve "recognition rather than recall" [Nie94]. This recognition minimizes the memory load by making graphical objects visible. The fact that humans are quite efficient in recognizing and recalling visual objects, has been supported by many psycho-

logical studies [BK75, Sta73]. The intended purpose of graphical password is to reduce the memory load of user and still achieve the possible highest security. Thus graphical password schemes provide a way of making more secure and recognizable passwords.

1.1 Related Work

Jermyn et al. presented a graphical password authentication scheme named Draw A-Secret (DAS) [JMM+99]. In order to create a password, user has to draw a secret on a grid that serves as his or her password. Then during login time, user has to redraw the same secret for authentication. The problem with this scheme is that the users have to completely rely on their memory to recall the secret that they had created at registration time. Gao et al. proposed YAGP (Yet Another Graphical Password) [GGC+08] which is based on DAS scheme and eliminates the above-mentioned constraint of DAS. In addition, it offers more resistance against shoulder surfing attack and uses a larger password space. The major limitation of YAGP is that its similarity threshold is fixed and precise redraw of secret is difficult.

Blonder's patent [Blo96] is considered as the first cued recall based scheme. In this scheme, the user has to click on the predefined regions of the predetermined image to create a password. To authenticate successfully, user has to click on the previously selected region in the same sequence. One drawback is that the user still needs to remember the sequence of clicks which requires memory recall. Wiedenbeck et al. proposed PassPoints system [WWB+05a, WWB+05b] which is an improvement over Blonder's scheme. In PassPoints system, any image (instead of predefined image) can be used to create password with clear boundaries instead of predefined click region. The authors also used tolerance distance for click points in order to avoid the difficulty for users to click exactly at the same pixel. One problem with PassPoints system is that the image selection could be a tricky task. This is so because the image has to be rich enough to allow selection of many click points with negligible "hot spots" (i.e. the points with highest probability of being selected). Images with fewer click points lead to security issues.

Dirik et al. developed a model [DMB07] to identify the suitability of an image for PassPoints system by predicting the hotspots in the image. The system was evaluated by over hundred users and the results showed that the model could predict 70-80% accurately. Chiasson et al. presented a cued click points technique [CvOB08] in which users had to click one point on each image for a sequence of images. This scheme is more usable than PassPoints as it is easier to remember one point per image instead of sequence of points for a single image. Moreover, there is no need to remember the order of the selected password points.

2 Proposed Scheme

We proposed a new graphical password scheme named SportsFaces. In the proposed scheme, the password is based on images related to sportsmen. We have selected sports players because most of the users have some interest in one or the other sport. In addition, the idea can be easily extended to include non-sports categories such as movie stars, singers, etc. In our prototype, we used two categories: Cricket and Football. Our database consists of all the images of players and countries (flags) who have participated in the most recent major event in that sport, i.e., FIFA World Cup 2010 and ICC 20-20 World Cup 2010 for Football and Cricket, respectively. The Football players' images were collected from FIFA website [FIF] while Cricket players' images were taken from Cricinfo website [Cri]. There were 32 countries who participated in FIFA World Cup 2010 and the squad for each country consisted of 23 players. Similarly, ICC 20-20 World Cup 2010 had 12 teams and 15 players for each team. Therefore, our image database consisted of 916 images.

2.1 Registration Phase

In order to create a password, the user has to select nine images: three countries and three players for each country. At registration time, the user first selects a password category, i.e., i) Cricket Players or ii) Football Players.

When the user selects a category, flags of the countries belonging to the corresponding category appear on the screen (see Fig. 1). The user selects one of the displayed flags which results in appearance of the corresponding players' screen (see Fig. 2).

Abbildung 1: Flags for Cricket category

Next, the user selects three players from the list of displayed images. The above-mentioned process is repeated thrice resulting in selection of three countries and nine players. The identities of these twelve images make a password string. All the images in the password are displayed on the last screen of registration process (see Fig. 3) so that the user can look at his or her password carefully and absorb it.

Abbildung 2: Displayed players when Pakistan is selected from countries' screen

2.2 Login Phase

The login phase is quite similar to the registration phase except that there is no screen displaying the complete password at the end. The user enters his or her user id, selects the category, countries and players correctly in order to login successfully.

Users are not required to remember the sequence of the selected images. For successful authentication, the user only has to select the same country and players that he or she has selected during password creation. In the proposed system, the password string is not stored in the plain form in the database; instead a cryptographic hash of the password string is calculated and stored in the system. In addition, the images are shuffled every time they appear on screen in order to avoid shoulder surfing attack.

3 Experimental Evaluation

3.1 Participants

We conducted our lab study with 13 participants out of which 9 were male and 4 were female. All the participants were undergraduate students with their ages ranging from 18 to 24 years. All of the participants were regular computer users.

3.2 Procedure

We asked the users to work with two systems: our graphical password system and our implementation of a typical alphanumeric system. Lab study is conducted over three pha-

Abbildung 3: Last screen of registration phase, displaying twelve images which constitute user's selected password

ses namely password creation, password learning and password retention phase. Retention phase is sub-divided in three stages where retention is tested on the same day, after three days and after seven days of password creation.

3.2.1 Password Creation

Our lab study started with a demonstration to guide the users about the working of the proposed system. The demonstration lasted for about 10 minutes. For alphanumeric password system, the users were directed to select any "novel" password of eight characters having at least one uppercase letter, one lowercase letter and one digit. Then each user was asked to create his or her password for both alphanumeric password system and SportsFaces.

To create graphical password, each user has to select 3 flags and 9 players as detailed in section 2.1. To create alphanumeric password, each user has to enter a password of exactly eight characters including at least one uppercase letter, one lowercase letter and one digit. In addition, the user has to retype his or her password for confirmation and matching.

3.2.2 Password Learning

After password creation phase, learning phase started. Learning phase is conducted for our graphical password system only because users are quite familiar with typical alphanumeric systems and they don't need any practice for that system. We divided our learning phase into two activities namely cued sign in and trial sign in. In cued sign in, a cue is given (in the form of a text message) to the user if he or she selects any wrong image during password selection. In trial sign in activity, the user is asked to enter password until he or she achieves five correct submissions. During this activity, if a user forgets his or her password, he or she can see the password using show password link and try again to sign

in. The user can also use show password after submitting an incorrect input. At the end of learning phase, the users fill a questionnaire where they are asked to compare their comfort level when using SportsFaces and alphanumeric password systems.

3.2.3 Password Retention

The retention phase is similar to learning phase except the users are asked to do only one sign in here.

4 Results

4.1 Password Creation Phase

In the creation phase, users created their graphical and alphanumeric passwords. For each participant, we measured total number of attempts and amount of time required to create a valid password. Results show that, on the average, the users took longer to create a valid graphical password as compared to an alphanumeric one. The average time to create graphical and alphanumeric password was 3 minutes and 24 seconds and 2 minutes and 14 seconds, respectively. On the other hand, all 13 users created their graphical password in first attempt as compared to just 4 for alphanumeric one as shown in Table 1.

Tabelle 1: Number of users creating valid passwords in 1st, 2nd or 3rd attempts for SportsFaces and alphanumeric systems

Total Attempts to Create Password	No. of Users for SportsFaces	No. of Users for Alphanumeric System
1	13	4
2	x	7
3	x	2

4.2 Password Learning Phase

The learning phase was conducted for practicing graphical password. As mentioned earlier, learning phase was not conducted for alphanumeric system. This phase was divided into two sub-activities: cued sign in and trial sign in. To pass cued sign in, users were required to input correct password once. During lab tests, all the users were able to successfully sign in during cued sign in activity with an average sign in time of 1 minute and 18 seconds. The criterion to successfully complete the trial sign in was 5 correct password inputs. Eight out of 13 users completed trial sign in without any mistake, 4 users made one mistake and 1 user gave four incorrect submissions. The average trial sign in time (for 5 correct inputs) was 4 minutes and 6 seconds.

4.3 Password Retention Phase

Retention of passwords is measured at three times: at the end of learning phase, after 3 days and after one week. Criterion for completion of retention phase is one correct password submission. Table 2 shows the results of retention phase.

Tabelle 2: Results of retention phase

Retention Trial	System	No. of Users Giving Correct Password	Average Time (min:sec)
1	SportsFaces	11	01:39
	Alphanumeric System	13	00:29
2	SportsFaces	12	01:00
	Alphanumeric System	9	01:26
3	SportsFaces	11	01:07
	Alphanumeric System	8	01:04

4.4 Discussion on Results

The overall results are encouraging for SportsFaces graphical password system. All participants created their graphical password without doing any mistake as opposed to alphanumeric password. Although it took longer to create graphical password but this could be due to unfamiliarity of users with the graphical password system. During the first retention trial, alphanumeric system outperformed SportFaces getting a retention rate of 100% as compared to 85% for Sportsfaces. On the other hand, SportsFaces outperformed alphamnumeric system during retention trials 2 and 3. SportsFaces attained success rates of 92% and 85% as compared to 69% and 62% for alphanumeric password system in retention trial 2 and 3, respectively. From the results, we can make the following two conclusions:

- Memorability of alphanumeric passwords is better for short time (as shown in retention trial carried on the same day) but as the times passes, graphical passwords become more memorable than alphanumeric passwords (as shown in retention trials carried after 3 and 7 days, respectively).
- Memorability of alphanumeric passwords decreases continuously with the passage of time (100%, 69% and 62% for R1, R2 and R3, respectively) but the same is not necessarily true for graphical passwords (85%, 92% and 85% for R1, R2 and R3, respectively).

5 Security Analysis

5.1 Exhaustive Search and Guessing Attacks

In the proposed scheme, the users have two choices for category selection, i.e., Football and Cricket. After a category is selected, the users have to select 3 out of 32 flags for Football (resp. 3 out of 12 for Cricket); and for each flag, they have to select 3 out of 23 players for Football (resp. 3 out of 15 for Cricket). Therefore, an exhaustive search attack would require 2^{23} possible attempts to find the password. On the other hand, to carry a successful attack against 8-character alphanumeric passwords, an exhaustive search would require 2^{48} attempts. Though password space of alphanumeric system is larger but they are more susceptible to dictionary attacks as compared to SportsFaces. In general, for graphical passwords, this attack is not feasible because there is no dictionary that contains the images of all world objects. Alphanumeric systems are vulnerable to these attacks because dictionaries of commonly selected passwords are easily available.

5.2 Shoulder-Surfing Attacks

Shoulder-surfing attacks are those attacks where an attacker gets the secret information through direct observation when the user is entering his or her password. Alphanumeric systems are susceptible to shoulder-surfing attacks. In these attacks, typically the attacker gets a chance to observe the password entry for a short duration of time. As alphanumeric passwords are typically small, the attacker may see the secret by looking just for a while. In addition, many passwords consist of familiar words making it easier for an attacker to reconstruct the secret even if he or she knows only a few characters of the secret.

On the other hand, shoulder surfing attack is not feasible against SportsFaces as multiple levels of challenges are involved. The attacker has to observe the secret entry for longer period of time as first he has to see the category followed by the flags for the selected category followed by the players against each flag. In additions, the images are displayed in random order on all screens during the password entry thus making the shoulder-surfers task even more difficult.

6 Conclusions and Future Work

In this paper, we proposed a new graphical password system named SportsFaces. In the proposed system, the password consists of a combination of sports categories, country flags and players. The scheme provides a potential solution for the current problems faced by the other graphical password schemes. Lab results show promising results for Sports-Faces system. The proposed system provides both the security and the usability features. The usability results and the answers to questionnaire reveal that the users were comfortable in creating as well as remembering their password using the proposed system. System

is flexible in a way that more categories and corresponding images can be easily added to increase security of the system. Our current prototype involves two sports: cricket and football but we plan to add more sports categories in the future. In addition, we plan to expand our basic idea by adding non-sports image categories such as movie stars, models, music celebrities, etc.

Bibliography

[BK75] G.H. Bower und B. Karlin. Comprehension and memory for pictures. *Memory & cognition*, 3(2):216–220, 1975.

[Blo96] G.E. Blonder. Graphical password, September 24 1996. US Patent 5,559,961.

[Cri] ESPN Cricinfo. http://www.espncricinfo.com.

[CvOB08] S. Chiasson, P. van Oorschot und R. Biddle. Graphical password authentication using cued click points. *Computer Security–ESORICS 2007*, Seiten 359–374, 2008.

[Dau04] J. Daugman. How iris recognition works. *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1):21–30, 2004.

[DMB07] A.E. Dirik, N. Memon und J.C. Birget. Modeling user choice in the PassPoints graphical password scheme. In *Proceedings of the 3rd symposium on Usable privacy and security*, Seite 28. ACM, 2007.

[FIF] FIFA. http://www.fifa.com.

[GGC+08] H. Gao, X. Guo, X. Chen, L. Wang und X. Liu. Yagp: Yet another graphical password strategy. In *Computer Security Applications Conference, 2008. ACSAC 2008. Annual*, Seiten 121–129. IEEE, 2008.

[HL00] M.S. Hwang und L.H. Li. A new remote user authentication scheme using smart cards. *IEEE Transactions on Consumer Electronics*, 46(1):28–30, 2000.

[HS09] H.C. Hsiang und W.K. Shih. Weaknesses and improvements of the Yoon-Ryu-Yoo remote user authentication scheme using smart cards. *Computer Communications*, 32(4):649–652, 2009.

[JMM+99] I. Jermyn, A. Mayer, F. Monrose, M.K. Reiter und A.D. Rubin. The design and analysis of graphical passwords. In *Proceedings of the 8th conference on USENIX Security Symposium-Volume 8*, Seite 1. USENIX Association, 1999.

[LLW10] C.T. Li, C.C. Lee und L.J. Wang. A Two-Factor User Authentication Scheme Providing Mutual Authentication and Key Agreement over Insecure Channels. *Journal of Information Assurance and Security*, 5(1):201–208, 2010.

[Nie94] J. Nielsen. Enhancing the explanatory power of usability heuristics. In *Proceedings of the SIGCHI conference on Human factors in computing systems: celebrating interdependence*, Seiten 152–158. ACM, 1994.

[Sta73] L. Standing. Learning 10000 pictures. *The Quarterly Journal of Experimental Psychology*, 25(2):207–222, 1973.

[TP02] M.A. Turk und A.P. Pentland. Face recognition using eigenfaces. In *Computer Vision and Pattern Recognition, 1991. Proceedings CVPR'91., IEEE Computer Society Conference on*, Seiten 586–591. IEEE, 2002.

[WWB+05a] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy und N. Memon. Authentication using graphical passwords: Basic results. *Human-Computer Interaction International (HCII 2005)*, 2005.

[WWB+05b] S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy und N. Memon. PassPoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human-Computer Studies*, 63(1-2):102–127, 2005.

[YRY05] E.J. Yoon, E.K. Ryu und K.Y. Yoo. An improvement of Hwang-Lee-Tang's simple remote user authentication scheme. *Computers & Security*, 24(1):50–56, 2005.

[ZD10] S. Ziauddin und M.N. Dailey. Robust iris verification for key management. *Pattern Recognition Letters*, 31(9):926–935, 2010.