A Security Scheme for Textual & Graphical Passwords

Shaik Nazeer,
Dept. of CSE,
Bapatla Engineering College, India

Dr. P. Premchand,
Dept. of CSE,
Osmania University, India

Abstract:-Authentication is the process of identifying an individual, usually based on username and password. Authentication merely ensures that the individual is who he or she claims to be. This forestalls the activities against confidentiality and integrity. Shoulder surfing is the main problem of graphical passwords. To overcome the problem of shoulder surfing we introduced a novel Scheme. This scheme provides the login screen to the user at every time the user logs in, this login image consists of set of characters. User with his password clicks some pass characters which are different for different sessions and explained in proposed scheme. To provide better results Neural Network is used for the authentication.

Keywords: *Authentication, Shoulder Surfing, Back Propagation Learning Algorithm, Feed Forward Neural Network.*

*****

1. Introduction

Before explaining the current state of graphical techniques as one of the possible alternatives for user authentication, numbers of psychological studies explaining the „picture superiority effects‟ towards words and verbal are presented in the next paragraphs.

Shepard [59] conducted a study to examine the level of recognition for pictures. He used 600 pictures where each of them was displayed for a few seconds to the participants. Later on, participants were asked to recognize and determine whether the displayed images were original (images that on the list during initial experiment) or fake (images that not on the list during initial experiment). Overall, it was reported that participants managed to recognise 98% of the images.

In 1968, Nickerson [60] conducted a study to determine the effect of long term recognition memory towards pictorial materials. In his study, a total of 200 images were used in which each of the images was displayed for 5 seconds. During the test, participants had to determine the displayed images either 'old' (displayed to them during the first task) or 'new' (only displayed to them during the test). The testing were implemented in four phases; namely day 1, day 7, day 28 and day 360. Overall, the results showed that the probability of success rate decreased from day 1 up until to the day 360. However, considering the factors such as time (up to a year) and the way the experiment was conducted, they concluded that the long term recognition memory for pictorial images were still better than words.

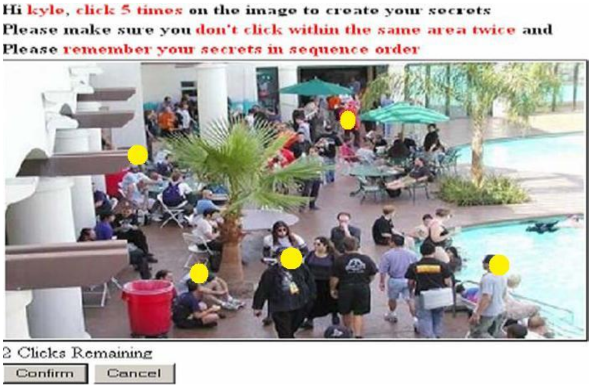
Standings et al., [61] conducted 4 experiments to examine the relationship between perception and memory. The first two experiments were about memory recognition for pictures. Experiment 1 used 1100 pictures taken from the magazines, with Experiment 2 used 2560 pictures obtained from the photographers (both amateur and professional). Overall, they found that participants scored up to 95% success for Experiment 1 and for Experiment 2, participants still scored 85% recognition success even after 4 days time. The last two experiments were about the effect of duration and the effect of reversing and orienting the pictures during viewing. From the results, it were summarized that participants still managed to score above 90% success rate even the images were reversed. However, with regard to the image orientation, participants scored slightly low (average of 55%). On the whole, they concluded that participants managed to obtain higher success rate for picture recognition.

In 1973, Standings [62] investigated the memory capacity and retrieval speed for both pictures and words. There were a total of 4 experiments conducted and he summarized that for both memory capacity and retrieval speed, using pictures were still superior to the words or verbal. This proven when using larger set of images (he used up to 1000 images), changing the method of recognition (images were displayed sequentially rather than simultaneously) and finally different forms of testing (using visual words, normal picture and auditory words), participants still performed significantly well.

1.1Graphical authentication schemes

Based upon user memory tasks, GA can normally be classified into two; namely recognition-based and recall-based, with a further classification of cued-recall sitting between the two. Looking upon users‟ action when they authenticate into the system, this thesis classifies GA into four main categories; namely click-based, choice-based, draw-based and hybrid. Click-based requires users to click anywhere they prefer in a given image. These secret click points are the users‟ „password‟. The choice-based approach requires users to select their chosen images from a set of decoy images. The image selection can be continued for several rounds depending on the system settings, while the draw-based method requires users to draw their secret on the provided grid/screen. In this case, the drawing is interpreted as the password in order to be authenticated. The graphical schemes are grouped into hybrid-based method if they combined at least two of the aforementioned categories.

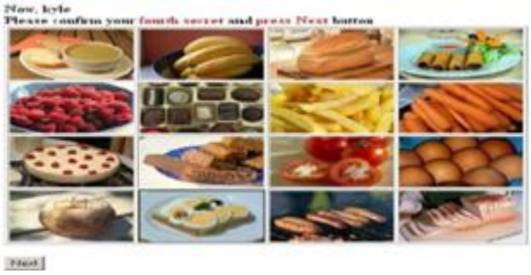
Figures 1-1 to 1-3 illustrate three main methods of authentication using images, with an example of secret created/chosen/drawn from the user is given. Within this section, a graphical scheme within their classification is introduced and if exist, their enhancement studies are reviewed and explained.



Hi kyle, click 5 times on the image to create your secrets
Please make sure you don't click within the same area twice and
Please remember your secrets in sequence order

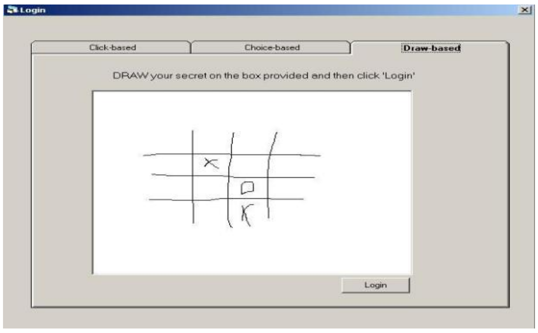
2 Clicks Remaining

Figure1-1:Example ofthe click-based graphical method



Now, kyle
Please confirm your fourth secret and press Next button

Figure 1-2: Example of the choice-based graphical method



DRAW your secret on the box provided and then click 'Login'

Figure 1-3:Example ofthe draw-based graphical method

2. Proposed Method

Considering the above schemes and understanding the flaws here it is proposed a new scheme

Notation for graphical Password Protocol

C	Claimant
V	Verifier
U	User Name of the Claimant
PW	a Set of images or letters selected by the user as a password
N	Nonce
E	Environment, which is a grid of images of symbols provided to the user to select. Positions indicators:
L	Left
R	Right
B	Bottom
T	Top
LT	Left Top
RT	Right Top
LB	Left Bottom
RB	Right Bottom

Location table

LT	T	RT
L	symbol	R
LB	B	RB

Sample *grid* shown below.

A	A	k	O	g	C	l	F	d	r
1	n	2	T	m	L	v	c	X	y
N	w	G	Z	b	5	V	7	K	p
H	3	f	6	o	W	z	e	Q	D
x	j	U	M	I	4	u	R	8	S
s	B	P	t	h	J	Y	q	E	i

This grid contains letters a-z ,and capital letters A-Z and digits 2-9,

We assume that the grid is foldable (or rollable) so that the side edges, touch each other whenever necessary . i.e. first column will touch last column if you roll (or fold).similarly first row will touch last row if you fold. Let us assume a user has selected top ‘ T’ as his position indicator.

Suppose the password of that user is RAMA. Then from this grid he has to enter the letters as “eB6B”. He always enters a letter which is on the top of the letter required by him. (on the top of “R “ the letter “e” is there , so instead of R he has to enter e).

Protocol:

The claimant must send his user name. If the user name is already selected by somebody else then server (verifier) will not accept the same name. After this she has to select a password.

a) *Registration*

Here the claimant or user receives a set of symbols. He randomly selects a subset of symbols and sends them to the server or verifier as his password. These symbols along with their selection order will serve as a password to the claimant. This is stored at the server.

i) C→V: U through secure channel
ii) V→C: Location table through secure channel
iii) C→ V : PWD ,position indicator through secure channel

Here the user selects the position indicator from the location table securely

b) Login

Here the user enters the user name and it is passed to the verifier along with nonce. Then the verifier challenges the claimant with an environment. This environment is populated randomly every time.

C →V : U,N
V → C: E

The user (or Claimant) enters the set of password images (or letters) as per the preselected position indicator from the latest grid he received.

C →V :PW

If this is a valid password then verifier accepts else rejects.

3. Explanation:

Here each time the claimant is using an encrypted symbols as his password. This encryption is highly random because the environment E is populated with symbols which are positioned differently. The entropy for this encryption is very high.

Depending on the user's name it sends his password symbols and those symbols will be populated randomly in the grid. The remaining symbols may be changed by verifier to further increase the entropy. This model has high resistance to shoulder surfing attack. The position indicator (i.e the indicating position for symbol) may be changed by the user occasionally. He may change his password also. Here the encrypted password (encryption done by this grid because of the preselected position indicator) will be used as a session password. Here it is again the one time password that is working which has a very high entropy.

4.Conclusion

By using S3PA Scheme we successfully overcome the drawback of attacks relating to shoulder surfing. As this Scheme generates the image randomly it was resistant to screen capture and key logger attacks, we are making a user to enter his session password with the help of his known password.

We could provide security at the server side, during the registration phase. The neural network was trained and stored weights of the network used for our mapping. Even though an intruder attacks the system and accesses this information he cannot interpret the data as he cannot find the normalized data values. We provided connectivity between our two schemes and successfully provided security at the server side and the client side. For back propagation we performed training with variants of learning rate (ŋ) and momentum term (α).

References:

[1]. HaichangGao, Xiyang Liu, Sidong Wang, Honggang Liu, Ruyi Dai, "Design and analysis of a graphical password scheme," 2009 Fourth International Conference on Innovative Computing, Information and Control, ICICIC, 7–9 Dec. 2009, pp. 675–678.

[2]. D. Hong, S. Man, B. Hawes, and M. Mathews, "A password scheme strongly resistant to spyware," Proceedings of International conference on security and management. Las Vergas, NV, 2004.

[3]. A.P. Sabzevar, A. Stavrou, "Universal Multi-factor authentication using graphical passwords," in: IEEE International Conference on Signal Image Technology and Internet Based Systems, 2008, SITIS "08, Nov. 30 2008–Dec. 3 2008, pp. 625–632.

[4]. G. Horng, "Password authentication without using password table," Inform. Processing Lett., vol. 55, pp. 247–250, 1995.

[5]. S. Wiedenbeck, J. Waters, J.C. Birget, A. Brodskiy, N. Memon," PassPoints: design and longitudinal evaluation of a graphical password system," International Journal of Human-Computer Studies 63 (2005) 102–127, Special issue on HCI research in privacy and security.

[6]. SadiqAlmuairfi, PrakashVeeraraghavan, Naveen Chilamkurti, "A novel image-based implicit password authentication system (IPAS) for mobile and non-mobile devices," Department of Computer Science and Computer Engineering, La Trobe University, 3086, Melbourne, Australia.

[7]. A. Gilbert, "Phishing attacks take a new twist," CNET News.com, May 04,2005.

[8]. A. Adams and M. A. Sasse, "Users are not the enemy: why users compromise computer security mechanisms and how to take remedial measures," Communications of the ACM,42:41–46, 1999.

[9]. L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[10]. J.D. Pierce, Jason G. Wells, Matthew J. Warren, David R. Mackay," A conceptual model for graphical authentication,"1st Australian Information security