AN ASSOCIATION-BASED GRAPHICAL PASSWORD DESIGN RESISTANT TO SHOULDER-SURFING ATTACK

Zhi Li[1, 2], *Qibin Sun*[1], *Yong Lian*[2], *and D. D. Giusto*[3]
[1] Institute for Infocomm Research (I^2R), A*STAR, Singapore 119613
[2] Dept. of ECE, National University of Singapore, Singapore 119260
[3]Dept. of EEE, University of Cagliari, Cagliari 09123, Italy
Email: {stuzl, qibin}@i2r.a-star.edu.sg; eleliany@nus.edu.sg; ddgiusto@unica.it

ABSTRACT

In line with the recent call for technology on Image Based Authentication (IBA) in JPEG committee [1], we present a novel graphical password design in this paper. It rests on the human cognitive ability of association-based memorization to make the authentication more user-friendly, comparing with traditional textual password. Based on the principle of zero-knowledge proof protocol, we further improve our primary design to overcome the shoulder-surfing attack issue without adding any extra complexity into the authentication procedure. System performance analysis and comparisons are presented to support our proposals.

1. INTRODUCTION

Textual password or PIN has been used for decades in spite of their well-known vulnerabilities. Today, the graphical user interface (GUI) has replaced the traditional command line I/O interface on most computers. Besides, in recent years, the prosperity of e-business based on mobile terminals also boosts the development of secure and convenient authentication solutions for touch screen devices. Many researchers thereby look at a more user-friendly approach – *graphical password* or *image based authentication* (IBA) in a broader sense. Besides the convenience of password input, it is deemed to be more "memorable" than the textual password or PIN which are *recall-based*. The basic theory is that our brain is more capable of storing graphical information than numbers/ alphabets and graphical password usually utilizes an easier and more human-friendly memorization strategy – *recognition-based* memory. In view of its potentials, JPEG (i.e., ISO/IEC JTC 1/SC 29/WG1) is considering to standardize such technologies [1].

We identify two mainstreams of state-of-the-art graphical password designs up-to-date: i) click-based approach [2, 3] and ii) image-selection-based approach [4, 5]. The former is based on sequential clicks of some points on an image, in which the presence of the background image helps the user to recognize the location of the secret clicks. In the latter approach, the user selects some "recognizable" secret images from a given image list. The whole authentication procedure consists of several rounds of such selections.

The common problem with both approaches is that the password entropy is relatively small (see the evaluation in Section 5). This motivates us to design a new graphical password scheme, which has large password entropy, and in the mean time, still preserve the user-friendliness. In this paper, inspired by a classic mnemonics – *Method of Loci*, we present a new design called *association-based* graphical password. The principal idea rests on the human cognitive ability of association-based memory. By creating "bounds" between the password elements, the mnemonic effect is enhanced. It is analogous to splitting a telephone number into chunks to aid memorization. Note that as will be addressed in Section 3, the password entropy is not necessarily reduced.

Another issue related to graphical password is the *shoulder-surfing (SS)* attack, i.e. the person behind you can observe and remember your input, and impersonate you afterwards. We realize that this problem is similar to the problems solved by the *zero-knowledge proof* protocols in cryptography [6]. We then present a slightly modified version of our previous design, which is resistant to this attack.

This paper is organized as follows. Section 2 introduces a typical application scenario using graphical password for user authentication. In Section 3 and 4, we propose the primary authentication scheme and the modified authentication scheme resistant to shoulder-surfing attack, respectively. Section 5 compares our designs with some prior related work. Section 6 addresses our future work and concludes the paper.

2. APPLICATION SCENARIO

Our application scenario involves three parties – Alice, Bob and the machine verifier (MV). Alice's objective is to authenticate herself to the MV via some input devices, such as the touch screen on an ATM machine, or a PDA, etc. The MV – either server or client-side – is to verify whether the person trying to authenticate herself/himself is Alice or another impersonator. Bob – the shoulder-surfer – is to obtain the password shared between Alice and the MV such that he could impersonate Alice. Assume Bob is capable of observing the full interactions between Alice and the MV. For example, he has set up a hidden camera besides the ATM machine such that he can capture all the details of the MV's display and Alice's input.

3. PRIMARY AUTHENTICATION SCHEME

3.1. Descriptions

In the user registration procedure, Alice is required to pick a desirable background image. The image is partitioned into some small regions, each partition being a locus. Define the locus alphabet as the set of all the loci $\mathbf{L}=\{l_1,l_2,\ldots l_{|\mathbf{L}|}\}$. Also define an object alphabet $\mathbf{O}=\{o_1,o_2,\ldots o_{|\mathbf{O}|}\}$ and a color alphabet $\mathbf{C}=\{c_1,c_2,\ldots c_{|\mathbf{C}|}\}$. The object alphabet consists of clip-arts images

0-7803-9332-5/05/$20.00 ©2005 IEEE

of objects, such as images of a cup, a bike, a cat etc. The color alphabet consists of colors like red, blue, green, cyan etc. To create her unique password profile, Alice is then required to create N triplets, each triplet with one element chosen from each alphabet $\phi_n=\{l_n', o_n', c_n'\}$, for $1 \leqslant n \leqslant N$. Note that Alice tends to choose some "salient points" as the pass loci, therefore, in practice, l_n' is selected from a subset $\mathbf{L}' \subset \mathbf{L}$.

Fig. 1 schematically illustrates the authentication procedure (Step 1->2->3A). The authentication phase consists of N rounds. Triplet ϕ_n serves as the "pass triplet" for round n, with l_n', o_n' and c_n' being the pass locus, pass object and pass color, respectively. In round n, Alice needs to click on the region of the background image associated with the pass locus l_n' (Step 1). After the click, a window pops up, showing a list of object elements $\mathbf{O}_1 \subset \mathbf{O}$, including the pass object $o_n' \in \mathbf{O}_1$. The remaining subset $\mathbf{O}_2=\mathbf{O}_1\backslash\{o_n'\}$ is called the decoy object set. Alice needs to select the pass object o_n' from the list (Step 2). After the selection, another window pops up, showing a list of color elements $\mathbf{C}_1 \subset \mathbf{C}$, including the pass color $c_n' \in \mathbf{C}_1$. Similarly, the remaining subset $\mathbf{C}_2=\mathbf{C}_1\backslash\{c_n'\}$ is the decoy color set. Alice needs to correctly select the pass color o_n' (Step 3A). This procedure repeats for N rounds. Alice is verified as authentic only when all the pass loci are correctly clicked, and all the pass objects and pass colors are correctly selected.

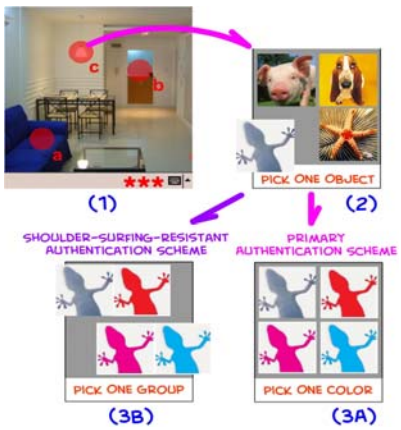

Fig. 1 Schematic diagram of the authentication procedure.

3.2. Analysis

As mentioned, user-friendliness and security are two mutually contradictory design goals for any user authentication system. We now analyze the primary authentication procedure based on these two criteria.

1) *User-friendliness* – Due to its nature, graphical password is considered advantageous over traditional textual password in terms of memorability. However, if the authentication procedure is too tedious (e.g. too many rounds of selection), it may still create memorization difficulties and annoy Alice. Our goal is to simplify the authentication procedure and create solid mnemonic effect, while still maintaining the password entropy large enough.

A classic mnemonic strategy called *Method of Loci* has attracted our attention. This method is described as follows:

First of all, choose a familiar place such as your own house. Take a mental walk through the rooms, and pay particular attention to the details that makes your mental images more vivid. Along the route create a list of loci, i.e. well defined parts of the room that you can use later to remember things, such as a door, a bed, an oven etc.

Now, when you are faced with a list of items to be memorized, you must form visual images of them and place them, in order, on the loci in your route. A loaf of bread sticking out of the letterbox; a giant apple in place of the door, etc. More striking the created image, more easily you will remember the thing.

This mnemonics can be dated back to the ancient Greeks, and has been proven to be surprisingly useful. E.g. in an experiment targeted at college students [7], the treatment subjects frequently recall two to seven times as much as the controlled subjects. In [7], Bower systematically studied the Method of Loci from a psychological point of view. He identified that the most essential part of this method is "the formation of imaginal associations between known cues and previously unknown list items at input, and use of these cues for recall."

In our proposed primary authentication scheme, two levels of association are created – the association between the locus and the object, and the association between the object and its color. By using mnemonics technique similar to the Method of Loci, Alice could remember the associated locus, object and color as a "bundle", rather than separately. In [7], Bower gives some very useful tips for establishing such associations – i) visualization must be conducted, no matter whether the user has witnessed the scene in real life. ii) The objects must be depicted in some kind of "interacting unity". For example, "a doll waving a red flag" is easier to be remembered than "a doll sits beside a flag that is red". Note that arbitrary associations may create some "bizarre scenes" (e.g. a blue banana in the bath), but remember that as addressed in the Method of Loci, more striking the created image, more easily you will remember the thing. Therefore, Alice is encouraged to create "bizarre scenes" to enhance the mnemonic effect. Another great advantage of this strategy is that the password can be unbiasly distributed among users and thus the password entropy can be maintained.

We argue that this association-based approach is superior compared to the recall-based approach, since associative memory is what the human is better at. On the other hand, it is superior compared to the recognition-based approach, because it leaves Alice much more choices of action to take, leading to much larger password entropy.

2) *Security* – We address two types of security measurement here: i) the password entropy, which measures the probability that Bob obtains the correct password based on random guessing; ii) resistance to shoulder-surfing attack, in terms of the number of observations Bob needs, in order to interpret the correct password.

The password entropy can be calculated as follows: for simplicity, assume all passwords are evenly distributed. Then the entropy is:

$$H(X_{std}) = N \log_2(|\mathbf{L}'||\mathbf{O}_1||\mathbf{C}_1|) \quad (1)$$

For a typical application, suppose the size of the salient point set

of an image |**L'**| is 30, |$\mathbf{O}_1$| and |$\mathbf{C}_1$| are both 4, and the number of rounds N is 4, the entropy is 35.6 bits, which is equivalent to the entropy of a 6-digit textual password. However, note that the above analysis is valid only under the following rule. In our scheme, the subsequent display of the object list $\mathbf{O}_1$ and the color list $\mathbf{C}_1$ after the locus selection may probably leak some information to Bob. For example, during Bob's random trials of the password, if Bob observes two different lists of objects displayed after the same input in two different trials, he may be able to interpret the pass object by intersecting the two lists. One useful rule to work against this attack is to make sure that the display of the object and color list must be "invariant", i.e., in Round n, $\mathbf{O}_1$ and $\mathbf{C}_1$ are deterministic functions of n and Bob's input (i.e. click or selection) in that current round only. More precisely, the object list can be determined by:

$$\mathbf{O}_1 = \begin{cases} \{o_n'\} \cup \mathbf{O}_2 \sim h_1(n, l_B), & \text{if } l_B = l_n' \\ \mathbf{O}_2 \sim h_2(n, l_B), & \text{otherwise} \end{cases} \quad (2)$$

where l_B is the locus Bob clicks on, and $h_1(\bullet)$ and $h_2(\bullet)$ are two one-way hash functions returning (|$\mathbf{O}_1$|-1) and |$\mathbf{O}_1$| elements, respectively. The color list can be derived in a similar way.

The above analysis presents the primary scheme's security level against random-guessing attack. Now for the shoulder-surfing attack, in this scheme, after Bob observes the authentication procedure once, the password is fully revealed, thus this scheme is susceptible to this shoulder-surfing attack as all other schemes previously mentioned. One solution to this problem will be presented in the next section.

4. AUTHENTICATION SCHEME RESISTANT TO SHOULDER-SURFING ATTACK

The shoulder-surfing attack urges us to look for a new approach to work against it, and in the mean time, we still want to preserve the primary authentication's user-friendliness.

In [8], a *challenge-response-based* graphical password scheme is proposed to counter the shoulder-surfing attack. However, the proposed procedure involves several rounds of jigsaw-puzzle-like challenges, which is practically not very workable. Another shoulder-surfing-resistant method based on PIN entry [9] is proposed recently. This scheme's feasibility is based on human's cognitive limitation on short term memory. However, we notice that to challenge human's memorability, the authentication procedure has to be intentionally tedious. Besides, they also proposed a *probabilistic cognitive trapdoor game* approach, which still suffers from the same tedious input procedure.

In this section, we propose a method that is only a slight variant of the method in Section 3, but the shoulder-surfing resistance property is nicely achieved.

4.1. Principle

We realize that the shoulder-surfing problem is similar to the problems solved by the zero-knowledge proof protocols in cryptography [6]. The principle of this protocol is: if Alice wants to prove to another verifier her knowledge of some secret information, but without revealing the secret's detail to the verifier, she can prove it by solving a "hard problem" – the "hard problem" is a special question that is easy to solve if the secret is known, and extremely hard if unknown. Therefore, by solving the problem, Alice can thereby prove her knowledge of that secret. Note that the "hard problem" must be carefully designed such that the verifier cannot get any information about the secret by observing Alice's solution.

The shoulder-surfing-resistant authentication involves a slightly different situation of the zero-knowledge proof protocol (see Fig.2). The basic idea is that if Alice can prove to the MV that she knows some secret information but without revealing it during the process of proof, she can authenticate herself to the MV, and in the mean time, avoid revealing this information to the shoulder-surfer Bob.

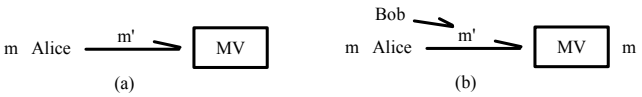

Fig. 2 Comparison of application scenarios of zero-knowledge proof protocol (a) and shoulder-surfing-resistant authentication (b), where m is the secret information (i.e. the password) and m' is the solution to the "hard problem" (i.e. the authentication input).

4.2. Descriptions

The next job is to design the "hard problem" which is secure and does not complicate the authentication procedure. We propose the following solution: randomly cluster the colors in the color list $\mathbf{C}_1$ into size-K subsets $\mathbf{C}_{1,i}$, for $1 \leqslant i \leqslant |\mathbf{C}_1|/K$, where $|\mathbf{C}_1|$ is the size of set $\mathbf{C}_1$. (For convenience, choose $|\mathbf{C}_1|$ and K such that K divides $|\mathbf{C}_1|$.) The "hard problem" is *to select the subset that contains the pass color c_n'*. Consider that Alice knows the pass color, so choosing the right subset is an easy job; however, since Bob does not know the pass color, he has no clue which subset to choose, but only can take his chance to guess. Note that this "hard problem" is not "perfect" because it is not fully secret-concealable – Bob still can get some information about the right pass color during the observation (i.e. narrowing down the possible pass colors to the subset selected by Alice). In the next subsection, we shall analyze the security level of this scheme.

The new authentication procedure is illustrated as Step 1->2 ->3B in Fig. 1. In step 3B, instead of asking Alice to select the correct pass color, now we ask Alice to select the correct subset that contains the pass color.

4.3. Analysis

Since this shoulder-surfing-resistant authentication is only a slight variant of the primary scheme, we assume they have the same level of user-friendliness. We focus on analyzing the system's security based on i) password entropy ii) resistance to shoulder-surfing attack.

The password entropy can be calculated as:

$$H(X_{ssr}) = N \log_2(|\mathbf{L}'||\mathbf{O}_1||\mathbf{C}_1|/K) \quad (3)$$

Compare to (1), we notice that the password entropy has reduced and thereby facilitated Bob's opportunity to interpret the password by random guessing. Nevertheless, this modified approach provides resistance to shoulder-surfing attack, so we could consider that this approach trades-off random-guessing security with shoulder-surfing security.

We then measure the resistance to shoulder-surfing attack in terms of how many times Bob needs to observe Alice's authentication procedure, in order to interpret the correct password. The best case happens to Bob when in the second observation, for every round, the random clustering puts the pass color in a totally different subset without any overlapping decoy colors as in the first observation. In this case, Bob needs to observe twice to interpret the right password; in the worst case, however, when there are always overlapping decoy colors, it takes infinite observations for Bob to discover the password.

We also want to know the average number of observations needed. Define $P_{rnd}(M)$ as the probability that Bob reveals the pass color for a single round after M observations. Then the probability of revealing all the pass colors in less or equal to M observations is:

$$P_{all}(m \le M) = \left[\sum_{m=1}^{M} P_{rnd}(m) \right]^{N} \quad (4)$$

Therefore the probability of revealing all the pass colors in M observations is:

$$P_{all}(M) = P_{all}(m \le M) - P_{all}(m \le M-1) \quad (5)$$

The average number of observations needed is:

$$\bar{M}_{all} = \sum_{m=1}^{\infty} m P_{all}(m) \quad (6)$$

To find a general $P_{rnd}(M)$ is difficult. Consider the case $|\mathbf{C}_1| = 4$ and $K = 2$, then $P_{rnd}(M)$ can be found as:

$$P_{rnd}(M) = (2/3) \times (1/3)^{M-2} \quad (7)$$

In our system, setting N=4, the average number of observations needed is computed as 3.3913. That is, on average Bob needs to observe more than three times in order to interpret the right password. In practice, the chance is rare for Bob. Therefore, we consider our system as secure against shoulder-surfing attack. Moreover, higher security level can be easily achieved by increasing the color list size (e.g. by setting $|\mathbf{C}_1|$=6 and K=3) or increasing the number of rounds N (e.g. by setting N=6).

5. COMPARISONS WITH PRIOR WORK

In this section, we compare our proposed schemes with some prior related work in literature.

The calculation of password entropy for various methods is in TABLE I. (For [8], due to its ambiguous nature, we will not give quantitative analysis and comparison here.) Fig. 3 presents a comparison of various methods in a 3D plot. The evaluation is based on i) user-friendliness, ii) security against random guessing iii) security against shoulder-surfing. Since the user-friendliness is subjective to users, we only present some qualitative analysis (by giving score 1 to 5, 5 being the most user-friendly) based on our understanding.

6. CONCLUSION

In this paper, we proposed a novel graphical password design resting on the association-based memory. We also presented a variant of the primary scheme which successfully overcomes the shoulder-surfing attack, but without adding extra complexity to the authentication procedure. Our future work includes conducting user studies and experiments to examine the effectiveness of our methods.

REFERENCES

[1] G. Ginesu, D. Giusto, T. Onali, "Image Based Authentication (IBA): A Review", N3461, *ISO/IEC JTC 1/SC 29/WG1*, Nov, 2004.

[2] G. Blonder, "Graphical Passwords", *United States Patent* 5559961 (1996).

[3] http://www.viskey.com

[4] "The science behind Passfaces", Real User Corporation (Sept. 2001) http://www.realuser.com

[5] R. Dhamija, A. Perrig, " Déjà Vu: User study using images for authentication", *9th USENIX Security Symposium*, 2000.

[6] B. Schneier, *Applied Cryptography*, New York: Wiley 1996.

[7] G. H. Bower, "Analysis of a Mnemonic Device," 496-510, *American Scientist*, Sep,Oct 1970.

[8] L Sobrado and J.C. Birget, ``Graphical passwords", *The Rutgers Scholar*, vol. 4, 2002.

[9] V. Roth, K. Richter, R. Freidinger, "A PIN-Entry Method Resilient Against Shoulder Surfing", *11th ACM Conference on Computer and Communications Security (CCS'04)*, Washington DC, USA, Oct, 2004.

TABLE I Comparison of Password Entropy

Password Scheme & Descriptions	Password Entropy (bits)
Textual. 6 numbers/alphabets	$6*\log_2 62 = 35.7$
PIN-based SS-resistant. 4 digits [9]	$4*\log_2 10 = 13.3$
Image-selection-based. 5 runs, in each run select 1 from 9 images [4,5]	$5*\log_2 9 = 15.8$
Click-based. 4 loci (30 salient points) [2, 3]	$4*\log_2 30 = 20.0$
Proposed primary authentication. 4 loci, 4 objects, 4 colors (30 salient points)	$4* \log_2(30*4*4) = 35.6$
Proposed SS-resistant authentication. 4 loci, 4 objects, 4 colors, K=2 (30 salient points)	$4* \log_2(30*4*2) = 31.6$

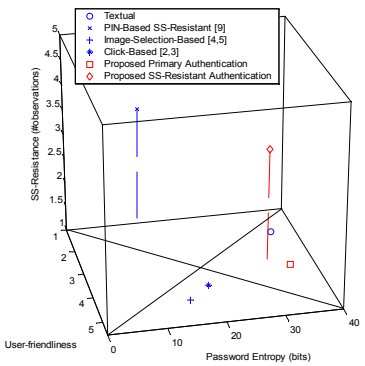

Fig. 3 Comparison of various methods in terms of user-friendliness, password entropy and shoulder-surfing resistance.