

S3PAS:A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme

Huanyu Zhao and Xiaolin Li
Scalable Software Systems Laboratory
Department of Computer Science
Oklahoma State University, Stillwater, OK 74078, USA
Email: {huanyu, xiaolin}@cs.okstate.edu

Abstract

The vulnerabilities of the textual password have been well known. Users tend to pick short passwords or passwords that are easy to remember, which makes the passwords vulnerable for attackers to break. Furthermore, textual password is vulnerable to shoulder-surfing, hidden-camera and spyware attacks. Graphical password schemes have been proposed as a possible alternative to text-based scheme. However, they are mostly vulnerable to shoulder-surfing. In this paper, we propose a Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme (S3PAS). S3PAS seamlessly integrates both graphical and textual password schemes and provides nearly perfect resistant to shoulder-surfing, hidden-camera and spyware attacks. It can replace or coexist with conventional textual password systems without changing existing user password profiles. Moreover, it is immune to brute-force attacks through dynamic and volatile session passwords. S3PAS shows significant potential bridging the gap between conventional textual password and graphical password. Further enhancements of S3PAS scheme are proposed and briefly discussed. Theoretical analysis of the security level using S3PAS is also investigated.

1. Introduction

The most common user authentication method is the text-based password scheme that a user enters a login name and a password. The vulnerabilities of this method have been well known. Users tend to pick short passwords or passwords that are easy to remember [1], which makes the passwords vulnerable for attackers to break. To resist brute-force search and dictionary attacks, users are required to use long and random passwords. Unfortunately, such passwords are hard to remember. Furthermore, textual password

is vulnerable to shoulder-surfing, hidden-camera and spyware attacks.

Graphical password schemes have been proposed as a possible alternative to text-based schemes, motivated partially by the fact that humans can remember pictures better than text [8]. In addition, the possible password space of a graphical password scheme may exceed that of text-based schemes and thus presumably offer higher level of security. It is also difficult to devise automated attacks for graphical passwords. As a result, graphical password schemes provide a way of making more human-friendly passwords while increasing the level of security. Due to these advantages, there is a growing interest in graphical password. However, existing graphical passwords are far from perfect. Typically, system requirements and communication costs for graphical passwords are significantly higher than text-based passwords. In addition, few graphical systems support keyboard inputs. More importantly, most current graphical passwords are more vulnerable to shoulder-surfing attacks than textual passwords.

To address the above issues, we propose a textual-graphical password system, named Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication System (S3PAS), which seamlessly integrates the textual and graphical passwords. S3PAS has the following salient features. (1) Shoulder-surfing, hidden-camera and spyware resistant. The secret can not be stolen even when an attacker watches or camera-records the victim enter the password. (2) Exactly match the conventional password and can go beyond. S3PAS can coexist with text passwords without changing the existing user profiles. Further, it can add more graphical pass-icons and sophisticated rules to further enhance the security level. (3) It is robust against brute-force attacks. (4) It supports both keyboard and mouse as input devices.

The rest of the paper is organized as follows. Section 2 presents related work in the area of both textual and graph-

ical passwords. Section 3 presents the basic S3PAS scheme and the enhanced variants. Section 4 analyzes and discusses the performance of the proposed scheme. Section 5 concludes the paper and envisions potential future work.

2. Related Work

Textual alpha-numeric passwords were first introduced in the 1960s as a solution to security issues that became evident as the first multi-user operating systems were being developed.

Blonder [2] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, a user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than textual passwords. The “PassPoint” system extended Blonder’s idea by eliminating the predefined boundaries and allowing arbitrary images to be used [13, 14, 15]. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticated, the user must click within the tolerance of the chosen pixels.

“Passface” is a technique developed by Real User Corporation based on the assumption that people can recall human faces easier than other pictures [3]. The basic idea is as follows. The user is asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user is presented with a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies all the faces.

Jermyn, et al. [5] proposed a technique, called “Draw a Secret (DAS)”, which allows the user to draw their unique password. When creating password, a user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn suggested that given reasonable-length passwords in a $5 * 5$ grid, the full password space of DAS is larger than that of the full text password space. Some further research based on DAS were conducted [7, 11, 12].

There is a common weakness in the above graphical password schemes: they are all vulnerable to shoulder-surfing attacks. To address this issue, Sobrado and Birget developed a graphical password technique [9]. In their scheme, the system first displays a number of 3 pass-objects

(pre-selected by a user) among many other objects. To be authenticated, a user needs to recognize pass-objects and click inside the triangle formed by the 3 pass-objects.

Man, et al. [6] proposed another shoulder-surfing resistant algorithm in which a user selects a number of pictures as pass-objects. Each pass-object has several variants and each variant is assigned a unique code. During authentication, the user is challenged with several scenes. Each scene contains several pass-objects and many decoy-objects. The user has to type in a string with the unique codes corresponding to the pass-object variants present in the scene as well as a code indicating the relative location of the pass-objects in reference to a pair of eyes. Hong, et al. [4] later extended this approach to allow the user to assign their own codes to pass-object variants. However, these methods force the user to memorize too many text strings, and their shoulder-surfing resistant property is not strong either.

More graphical password schemes have been summarized in a recent survey paper [10].

3. S3PAS System

S3PAS is designed to be used in client/server environments as most password authentication systems. Note that, the S3PAS system generates the login image locally and transmits the image specification (e.g., the coordinates of every character or icon in the image) instead of the entire image pixel-by-pixel from clients to servers, which greatly reduces communication overheads and authentication time.

3.1. Notations

To aid the presentation and analysis, we define the following notations to be used throughout the paper.

- T : The set of all the available password icons in a password scheme.
- $|T|$: The number of icons in the set of T (size of set T).
- T^* : The set contains all the combinations consisting of the elements in T . T^* is called “password space” in a certain password scheme.
- k : An element in the set of T^* . It is chosen by the user as a password, usually a string or a special order of several icons.
- $|k|$: The length of the user’s password k .

3.2. Single Set Scheme

S3PAS schemes include several variants, designed for different environments and different security requirements.

Single-set scheme is the basic S3PAS scheme. In this scheme, the available password icons set T is the set of all the printable characters just like the conventional textual password system, and $|T| = 94$. There is a string k which is user's password previously chosen and memorized by the user, which is named "original password". The characters in k are called "original pass-characters".

Initially, the system randomly scatters the set T in the login image as shown in Figure 1(a) and 1(b).

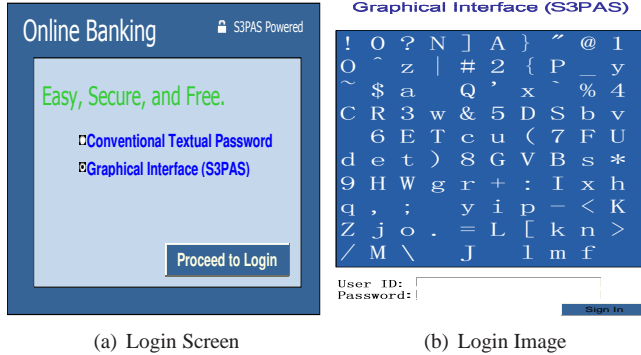


Figure 1. S3PAS Login Interface

To login, the user must find all his/her original pass-characters in the login image and then make some clicks inside the invisible triangles which are called "pass-triangles" created by 3 original pass-characters following a certain click-rule. Alternatively, the user can input/type a textual character chosen from inside or on the border of the pass-triangle area instead of clicking by mouse. Such character is called "session pass-character". Therefore, the final inputs could be either several session pass-clicks or several session pass-characters. These session pass-clicks or session pass-characters is a user's "session passwords".

Note that, there are two kinds of passwords in S3PAS system, the original passwords and the session passwords. Users choose their original passwords when creating their accounts. In every login process, users input different session passwords so that they can protect their original passwords from releasing.

The click-rule for single-set scheme is as follows. For the user's password string k , we number the first character in k as k_1 , the second k_2 , the third k_3 , etc. Then we have $k_1, k_2, k_3, \dots, k_{n-1}, k_n, n = |k|$. To login, users have to find out $k_1, k_2, k_3, \dots, k_{n-1}, k_n$ in the login image. Then the first click must be inside the pass-triangle formed by k_1, k_2 and k_3 . The second click must be inside the pass-triangle formed by k_2, k_3 and k_4 . Recursively, the i -th click must be inside the pass-triangle formed by $k_{i \bmod |k|}, k_{(i+1) \bmod |k|}$ and $k_{(i+2) \bmod |k|}, i = 1 \dots n$. This is the "basic click-rule."

To show the login process, let us follow an example.

Without loss of generality, we assume that the user Alice's original password k is "A1B3". Since the length of the password is, $|k| = 4$, based on the basic click-rule, Alice has to click four times correctly in the right sequence to be authenticated. The four combinations of password in order are "A1B", "1B3", "B3A" and "3A1". The login procedure consists of the following four steps and is also shown in Figure 2 (a) to (d).

1. Alice finds her pass-characters "A", "1" and "B", then clicks inside the pass-triangle or input a session pass-character inside $\triangle A1B$ (e.g., "P").
2. Alice finds her pass-characters "1", "B" and "3", then clicks inside the pass-triangle or input a session pass-character inside $\triangle 1B3$ (e.g., "D").
3. Alice finds her pass-characters "B", "3" and "A", then clicks inside the pass-triangle or input a session pass-character inside $\triangle B3A$ (e.g., "5").
4. Alice finds her pass-characters "3", "A" and "1", then clicks inside the pass-triangle or input a session pass-character inside $\triangle 3A1$ (e.g., "2").

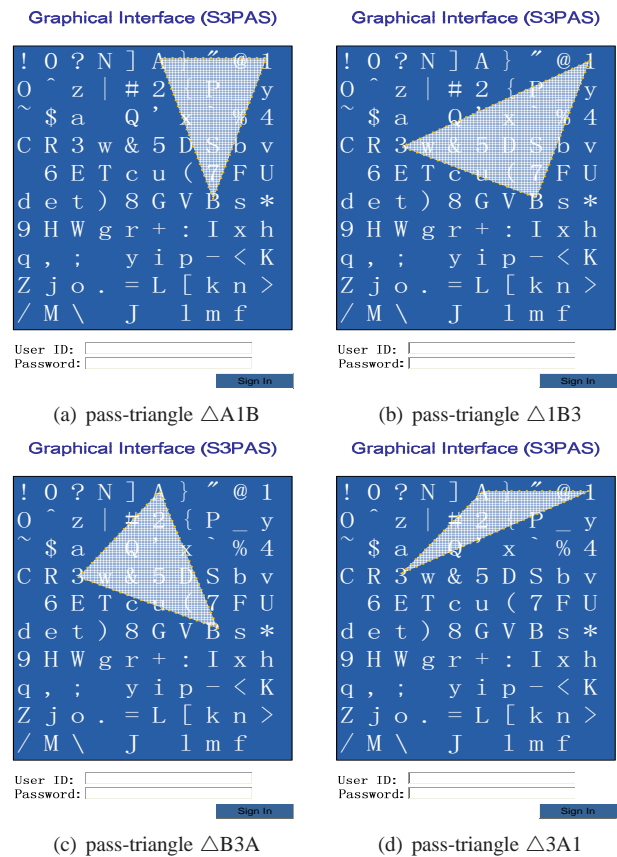


Figure 2. S3PAS Login Process

In this example, Alice’s original password is “A1B3”, and her session password is four clicks in sequence or textual password “PD52”. She has to click four times inside the invisible pass-triangles or input the session passwords “PD52” to be authenticated.

Two special cases need to be considered. If the two of those three pass-characters are the same, or even all of the three are identical, they can not construct a triangle. To address this problem, S3PAS requires that if two of the three characters are the same, users have to click in the invisible line formed by the two different characters. Similarly, if all of the three characters are the same, users have to click inside a certain circle area centered around this character.

To resist the brute-force search, we introduce the “change image” technique. If a user fails in clicking the correct areas, or a user inputs wrong session password for I (e.g., $I = 10$) times, the client automatically changes the session login image. How this idea resists brute-force search will be discussed in Section 4.

3.3. Enhancements

Three Set Scheme

Three-set S3PAS scheme is proposed to avoid the “common border problem.” In the single-set S3PAS scheme, the consecutive triangles share a common border. For example, in Figure 2(a) and 2(b), $\triangle A1B$ and $\triangle 1B3$ share the same edge “1B”. This common border problem might be exploited by attackers. In the three-set scheme, we randomly scatter three copies of the set T in the login image. Then there are $94 * 3 = 282$ characters on the login image. To distinguish the characters in different sets, we color the characters in the first set red, the second set green, and the third set blue. The detailed click-rule for three set scheme will be presented in our future publications.

Rule-Based Scheme

In the rule-based scheme, users are able to define their own click-rules when they creating passwords. The primary advantage is that rule-based scheme hides the click-rule. In the basic scheme, the click-rule is open to public, while in rule-based scheme, only the users themselves know their “pass-rules.” As a result, it becomes extremely hard for attackers to break user’s password using password analysis techniques. Further, the rule-based scheme hides the length $|k|$ of user’s password. In the basic S3PAS scheme, if Alice’s password is $|k|$ in length, she has to click $|k|$ times, which releases her password length to attackers. However, users can protect their password length information well by the rule-based scheme. Another benefit is that it can also avoid the common border problem. In addition, it could be easier for users to remember their own click-rules.

Enhanced Graphical Scheme

In the previous S3PAS schemes, the password is a textual string just like the conventional password. And the largest set of available password icons T is limited to the set of all the printable characters ($|T| = 94$). To enlarge the password space T^* and make the password easy to remember, we introduce the graphical S3PAS scheme. Our graphical S3PAS scheme is inspired by Sobrado and Birget’s work [9]. In this scheme, the available password icons set T is a set of “image icons” instead of “all the printable character.” So the size of T , $|T|$, can be much larger than 94. As a result, the password space T^* is enlarged greatly. This graphical S3PAS can be used in a high capability system to provide high level security.

4. Analysis and Discussion

4.1. Shoulder Surfing Resistant

Most textual and graphical password schemes are vulnerable to shoulder-surfing. However, our S3PAS scheme offers perfect resistance to shoulder-surfing, hidden-camera and spyware. After an attacker observes or records one click on the screen from the user, the attacker can not gain enough information of the user’s password. This shows that a shoulder-surfing attack is physically infeasible.

4.2. Random Click Attack and Triangle Area Approximation Analysis

In S3PAS schemes, users have to find out their pass-characters and then click inside the pass-triangle areas. However, attackers have the chance to click the right areas just by random-click even though they do not really know the password. This kind of attack is called “random-click attack.”

To resist random-click attack, users are required to click several times followed by some click-rule just like the basic S3PAS scheme. Recall the example shown in Section 3, if the password is “A1B3”, the user has to click four times to login. The problem is that whether four-character password is long enough to resist the random-click attack? If the attacker is “lucky” enough, he/she might be able to click inside the correct triangle regions correctly just by random-clicks. We observe that the size of the pass-triangle area greatly affects S3PAS’s security level. If the size of every pass-triangle area is too large, attackers are able to click inside the right areas with higher probabilities. To evaluate the security level, we should find out the expected average size of the pass-triangle areas, which is an important measure of S3PAS’s security level.

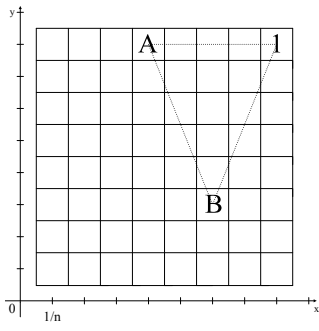


Figure 3. Analysis of Triangle Area

Consider the basic S3PAS scheme. Without loss of generality, we divide the login image region into $n*n$ grids. We assume that each character in the set T , which consists of all the 94 available password characters, is placed randomly in the center of every grid. In addition, we assume the length of the border of the login image is L . The three vertices of a pass-triangle hold coordinates: (X_1, Y_1) , (X_2, Y_2) , and (X_3, Y_3) . $X_1, Y_1, X_2, Y_2, X_3, Y_3$ are independent with each other. Each of them is distributed uniformly between L/n and L as shown in Figure 3.

The area of a triangle is given by,

$$S = \frac{1}{2} |(X_1 - X_2)(Y_1 - Y_3) - (X_1 - X_3)(Y_1 - Y_2)| \quad (1)$$

The expected average triangle area is,

$$E(S) = \sum_{f=1}^n \sum_{g=1}^n \sum_{h=1}^n \sum_{i=1}^n \sum_{j=1}^n \sum_{k=1}^n \frac{1}{2} \left| \left(\frac{f}{n} - \frac{g}{n} \right) \left(\frac{i}{n} - \frac{k}{n} \right) - \left(\frac{f}{n} - \frac{h}{n} \right) \left(\frac{i}{n} - \frac{j}{n} \right) \right| \frac{1}{n^6} \quad (2)$$

In the basic S3PAS scheme, we have 94 printable characters. As an example, $10 * 10$ grids are able to contain all the characters. Setting $n = 10$ in equation (2), we obtain, $E(S) = 0.7554300L^2 \approx 0.076L^2$. Based on $E(S)$, we know that the success probability using the random-click attack is given by $P(S) = 0.076L^2/L^2 = 0.076$. For a password k , the probability to get authentication just by random-clicks is $0.076^{|k|}$. Recall the former example, the length of the password is four. For attackers, the probability of click the right area for all the four times is $P(S)^{|k|} = 0.076^4 \approx 0.0000334$.

This probability is pretty low. It is extremely hard for attackers to get such a good "luck" to get authentication just by random-clicks. Attackers are forced to use brute-force search to break the password. That is, they hope to try many times, so that even though the probability to break the system for one time is pretty low, they can get the authentication by large number of tries. We will show later how S3PAS resists the brute-force search.

Let us go back to the expected average triangle area $E(S)$ in basic S3PAS scheme. Since the value of $E(S)$ determines the scheme's security level, we should try to reduce the value of $E(S)$. From equation (2), we observe that the parameter n is an important factor affecting $E(S)$. To show the relationship between $E(S)$ and n , we calculate several $E(S)$ value according to different n . We get the following results as shown in Table 1.

Table 1. The Area of Pass-Triangle as per the Grid Number n

n	Triangle area
2	$0.04687500L^2$
3	$0.06401463L^2$
4	$0.06994629L^2$
5	$0.07246848L^2$
6	$0.07379544L^2$
7	$0.07453787L^2$
8	$0.07501316L^2$
9	$0.07532504L^2$
10	$0.07554300L^2$
...	...

The table reveals a direct correlation between the grid number n and the triangle area; thus, we have the following conjecture.

Conjecture: *As the grid number n increases, the expected average area of a randomly-placed pass-triangle also increases; when n approaches infinity ($n \rightarrow \infty$), the expected average area of a triangle approaches a limit value.*

Based on the conjecture, to achieve the best security level, we should make the average size of the triangles as small as possible; thus, we should choose the smallest grid number that is large enough to host the set of all characters T .

4.3. Brute Force Search Resistant

In S3PAS systems, there are two kinds of passwords: the original passwords and dynamic session passwords. Therefore, there are mainly two ways to brute-force search S3PAS's passwords: brute-force search original passwords and brute-force search session passwords.

Brute Force Search Original Passwords Resistant

The main method used previously to defend brute-force search towards the passwords is to have a sufficiently large password space. Text-based passwords have a password space of $T^* (|T| = 94)$. Our basic S3PAS scheme has

been shown to provide a password space similar to text-based passwords. However, S3PAS schemes can provide a much larger password space by using the enhanced graphical S3PAS scheme.

Moreover, it is much more difficult to carry out brute-force attacks against textual-graphical passwords than text-based passwords. The attack programs need to automatically generate accurate mouse motion to imitate human inputs, which is particularly difficult for S3PAS. People can recognize a login image in less than one second, whereas computers spend a considerable amount of time processing millions of bytes of information regardless of whether the login image is a face, a landscape, or a meaningless shape.

Brute Force Search Session Passwords Resistant

S3PAS scheme is also efficient in resisting attacks on the session passwords. The primary reason is that we adopt “change image” technology. If a user fails in clicking the correct areas, or a user inputs wrong session passwords for I (e.g., $I = 10$) times, the client automatically changes the session login image. By doing this, there is no way for attackers to adopt brute-force search to break the session password because the session password will dynamically change after changing the image. As a result, all the attempts toward the previous image become useless. The attacker has to start a new search in the new image. Therefore, we argue that “change image” technique makes S3PAS immune to the brute-force search towards the session passwords.

Furthermore, the system might be broken once by chance under a tiny probability using brute-force attacks towards session password like any password system, but the attackers can not obtain the original secret passwords to completely break the system.

5. Conclusion

We proposed a scalable shoulder-surfing resistant password authentication system. S3PAS demonstrates desirable features of a secure authentication system being immune to shoulder-surfing, hidden-camera, and spyware attacks. Further, S3PAS is scalable in that it seamlessly matches the conventional text-based passwords and can accommodate various lengths of textual passwords, which requires zero-efforts for users to migrate their existing passwords to S3PAS. However, there are still some minor drawbacks in this system similar to other graphical password schemes. The major issues in S3PAS schemes include slightly more complicated and longer login processes. We plan to design a simplified version of S3PAS with a little lower security level to ease its adoption.

References

- [1] 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.
- [2] G. E. Blonder. Graphical passwords. *United States Patent 5559961*, 1996.
- [3] R. U. Corporation. How the passface system works, 2005.
- [4] D. Hong, S. Man, B. Hawes, and M. Mathews. A password scheme strongly resistant to spyware. In *Proceedings of International conference on security and management*, Las Vegas, NV, 2002.
- [5] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin. In proceedings of the design and analysis of graphical passwords. In *the 8th USENIX Security Symposium*, 1999.
- [6] S. Man, D. Hong, and M. Mathews. A shouldersurfing resistant graphical password scheme. In *Proceedings of International conference on security and management*, Las Vegas, NV, 2003.
- [7] D. Nali and J. Thorpe. Analyzing user choice in graphical passwords. In *Technical Report*, School of Information Technology and Engineering, University of Ottawa, Canada, May 27 2004.
- [8] R. N. Shepard. Recognition memory for words, sentences and pictures. *Journal of Verbal Learning and Verbal Behavior*, 6:156–163, 1967.
- [9] L. Sobrado and J. C. Birget. Graphical passwords. *The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research*, 4, 2002.
- [10] X. Suo, Y. Zhu, and G. S. Owen. Graphical passwords: A survey. In *21st Annual Computer Security Applications Conference (ACSAC 2005)*, Tucson, AZ, 2005.
- [11] J. Thorpe and P. C. v. Oorschot. Graphical dictionaries and the memorable space of graphical passwords. In *Proceedings of the 13th USENIX Security Symposium*, San Deigo, CA, 2004.
- [12] J. Thorpe and P. C. v. Oorschot. Towards secure design choices for implementing graphical passwords. In *Proceedings of the 20th Annual Computer Security Applications Conference*, Tucson, Arizona, 2004.
- [13] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon. Authentication using graphical passwords: Basic results. In *Human-Computer Interaction International (HCII 2005)*, Las Vegas, NV, 2005.
- [14] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon. Authentication using graphical passwords: Effects of tolerance and image choice. In *Symposium on Usable Privacy and Security (SOUPS)*, Carnegie Mellon University, Pittsburgh, 2005.
- [15] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon. Passpoints: Design and longitudinal evaluation of a graphical password system. *International Journal of Human Computer Studies*, 63, 2005.