A Survey on the Use of Graphical Passwords in Security

Haichang Gao, Wei Jia, Fei Ye and Licheng Ma
Institute of Software Engineering, Xidian University, Xi’an, P.R.China
Email: hchgao@xidian.edu.cn

***Abstract*—Beginning around 1996, numerous graphical password schemes have been proposed, motivated by improving password usability and security, two key factors in password scheme evaluation. In this paper, we focus on the security aspects of existing graphical password schemes, which not only gives a simple introduction of attack methods but also intends to provide an in-depth analysis with specific schemes. The paper first categorizes existing graphical password schemes into four kinds according to the authentication style and provides a comprehensive introduction and analysis for each scheme, highlighting security aspects. Then we review the known attack methods, categorize them into two kinds, and summarize the security reported in some user studies of those schemes. Finally, some suggestions are given for future research.**

***Index Terms*—Graphical Password, Security, Attacks**

I. Introduction

Today, authentication is the principal method to guarantee information security and the most common and convenient method is password authentication [1]. Traditional alphanumeric passwords are strings of letters and digits, which are easy and familiar to essentially all users. However, there are several inherent defects and deficiencies in alphanumeric passwords, which easily evolve into security issues. Due to the limitation of human memory, most users tend to choose short or simple passwords which are easy to remember [2]. Surveys show that frequent passwords are personal names of family members, birth date, or dictionary words. In most cases, these passwords are easy to guess and vulnerable to dictionary attack [3],[4]. Today users have many passwords for personal computers, social networks, E-mail, and more. They may decide to use one password for all systems to decrease the memory burden, which reduces security [5],[6]. Moreover, alphanumeric passwords are vulnerable to shoulder surfing attack, spyware attack and social engineering attack etc.

Motivated by the promise of improved password usability and security, the concept of graphical passwords was proposed in 1996 [7]. Like alphanumeric passwords, graphical passwords are knowledge-based authentication mechanisms. The main goal of graphical passwords is to use images or shapes to replace text, since numerous cognitive and psychological studies demonstrated that people perform far better when remembering pictures than words [8]-[11]. The most widely accepted theory explaining this difference is the dual-coding theory [12], suggesting that verbal and non-verbal memories are processed and represented differently in the mind. Assigned with perceived meaning based on direct observation, the images are represented in a way that retains the perceptual features being observed. The text is represented with symbols that convey associatively cognitive meaning. As a result, additional processing required for verbal memory renders a more difficult cognitive task. Thus it is easy for human being to remember faces of people, places they visit and things they have seen for a lengthy duration.

Research has been conducted on graphical passwords, with papers briefly summarizing categorizing schemes and reviewing numerous graphical password schemes while offering usability guidelines for their design [13], [14]. There are a plethora of papers on graphical passwords, some of which focus on specific schemes while others focus on concrete attacks [15][16]. Based on the current research of password security, we catalogued existing graphical passwords and conducted a comprehensive survey of security issues. This paper will be particularly useful for researchers who are interested in developing new graphical password algorithms as well as industry practitioners who are interested in deploying graphical password techniques.

The structure of our paper is organized as follows. In Section 2, we reviewed existing research and schemes closely related to our work. In Section 3, we classified all existing graphical password schemes into four main categories and gave a brief introduction to relevant schemes together with their characteristics. In section 4 and section 5, we introduced the existing attack types, and conducted an in depth analysis of the various threats faced by graphical passwords. In section 6, we offered four summary tables corresponding to four categories of graphical password schemes. Conclusion and Recommendations are addressed in Section7.

II. Literature Review

This research was supported by the National Natural Science Foundation of China (60903198) and the Fundamental Research Funds for the Central Universities.

Correspondence should be addressed to Haichang Gao, E-mail: hchgao@xidian.edu.cn

doi:10.4304/jsw.8.7.1678-1698

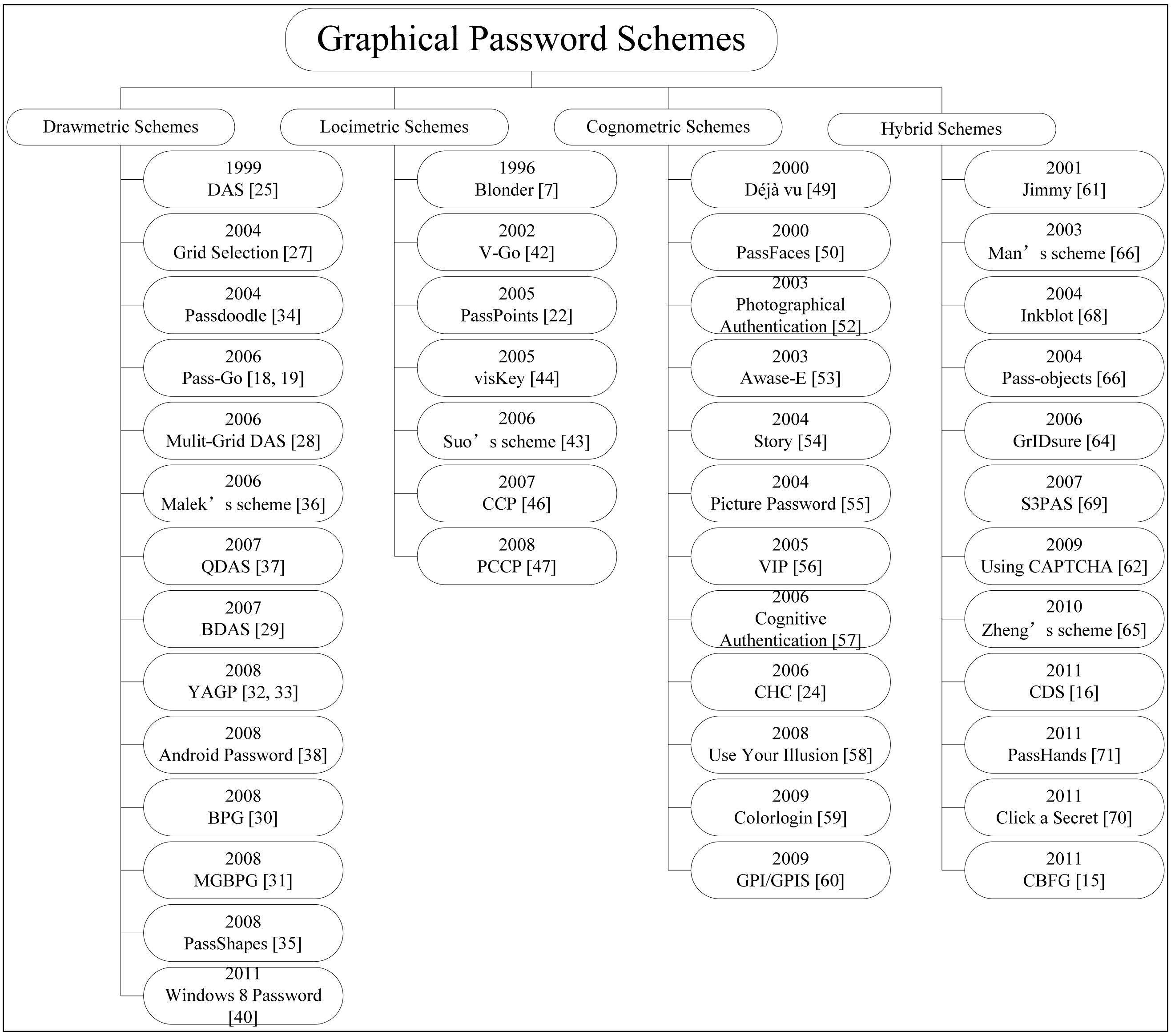


Figure 1. Classification of current Graphical Password Schemes

Several studies have been conducted on the security of graphical passwords. All of them have focused on specific schemes or concrete attacks. A detailed security analysis of DAS and Pass-Go has published by Thorpe and Tao et al. [17]-[21]. They pointed that 40% of passwords in Pass-Go fall into a subspace defined primarily by symmetry with respect to central vertical and horizontal axis, and 72% of passwords have only 4 or fewer strokes. Similar results were found in the DAS study. The security of password schemes is related more closely to the size of the effective password space rather than that of a theoretical password space. Therefore, dictionary attacks on Pass-Go and DAS require less effort to successfully crack users’ passwords. Oorschot et al. presented a graph-based algorithm dictionary attack for PassPoints [22] based on the hypothesis that users are more likely to choose click-points related to predictable preferences, e.g., logically grouping the click-points through a click-order pattern (such as five points in a straight line), and choosing click-points in the areas of an image where their attention is naturally drawn [23]. According to the results they provided, their automatic dictionary attack is easier to make whilst more scalable with systems using multiple images. Many graphical passwords are vulnerable to shoulder surfing attack. Due to the exposure of authentication interfaces, an attacker can capture a password by direct observation or by recording the individual’s authentication session. In order to overcome this problem, designers proposed several shoulder surfing resistant schemes. Wiedenbeck et al. [24] reported a game-like graphical password scheme named Convex Hull Click (CHC) which resists shoulder-surfing attack. Liu and his colleagues made a careful analysis of security issues on the CBFG they proposed [15]. Their result shows that CBFG has excellent capability against brute force attack, shoulder surfing attack and intersection analysis attack.

It should be noted that there have been two major summary literatures of graphical password studies. Suo et al. [13] conducted a comprehensive survey of the graphical password schemes existing between 1996 and 2005. They discussed the strengths and limitations of each mechanism and indicated future research directions in this area. Biddle et al. [14] provided a comprehensive overview of published research of graphical passwords over the first twelve years, analyzing both usability and security aspects, as well as system evaluation. They identified security threats that such systems must address and reviewed known attacks. However, both papers only gave a simple introduction of attack methods and did not provide an in-depth analysis combining specific schemes. These literatures provided us with a foundation on which to review and evaluate the security of the existing graphical passwords.

III. Categorization of Graphical Passwords

It has been 16 years since the first graphical password scheme, Blonder, was proposed [7]. With the development of graphical password, progressively more attention has been paid to this domain, and numerous studies have been undertaken. According to the authentication style, the current graphical passwords can be broadly classified into four general categories: Drawmetric schemes, Locimetric schemes, Cognometric schemes and Hybrid schemes. Hybrid schemes combine two or more of Drawmetric schemes, Locimetric schemes and Cognometric schemes. A detailed classification of schemes based on chronological order is shown in Figure 1. In this section we will review and discuss the existing schemes, particularly their security aspects.

A. Drawmetric Schemes

Drawmetric schemes are also known as recall-based schemes [55]. In Drawmetric schemes a user reproduces an outline drawing on a grid that he or she created or selected during the registration stage. DAS (Draw-A-secret) [25] was the first scheme in this category, and several others are improved versions of DAS, extending usability or enhancing security.

DAS was proposed by Jermyn et al. in 1999. In this scheme, a user is asked to draw a simple picture using a mouse or stylus. The drawing consists of one continuous stroke or several strokes separated by "pen-ups", on a *N×N* grid (usually a *5×5* grid). The picture is mapped to a sequence of coordinate pairs of the grid cells. For a successful login, the user needs to re-draw the picture. The historical significance of DAS is language independent, making it equally accessible to every user.

Users are liberated from remembering any alphanumeric string [25]. However, there are some restrictions on drawing which impact on the usability performance of DAS, such as ensuring every stroke is off the grid lines and redrawing in the exact position. According to a survey conducted by Nali [17], users tend to set predictable passwords which are vulnerable to dictionary attack. The survey showed that about 86% of passwords were centered or approximately centered and 45% of passwords were totally symmetric, thereby drastically reducing the effective password space. The concept of a graphical dictionary, introduced by Thorpe [26], was used to study the possibility of a brute-force attack. Their results also confirm that users incline to set certain types of passwords which may make dictionary attacks easier. Thorpe [27] further studied the impact of stroke-count and password length on the size of the DAS password space. Results suggested that increasing the grid size to increase the password space provides less security pay-back than increasing other parameters. Both stroke-count and password length significantly impact the effectiveness of password space, especially stroke-count. Attempts to improve the effective password space and the performance of the simple DAS have been undertaken.

Thorpe et al. proposed Grid Selection, which is composed of two parts: the drawing grid and the DAS password [27]. Users first select a rectangular region from a large and fine grained grid, and then draw the picture on the region, similar to DAS. Grid Selection increases the password space. However users have to remember the location of chosen region, increasing memorability difficulty.

Knowing that users tend to draw centering or symmetric lines and shapes in DAS. Chalkias et al. [28] proposed Multi-Grid, a modified version of DAS using uneven cell sizes. In Multi-Grid, the final grid could be composed from several internal grids. Users choose a grid from pre-defined multi-grid templates and then draw the picture on the grid. The study showed that centered passwords decreased to less than 50% and the scheme is more resistant to graphical dictionary attacks.

BDAS [29] proposed by Dunphy et al. is an extension of DAS where a background image is added to DAS. They reported that the background image could reduce predictable characteristics such as global symmetry or centering within the drawing grid and led users to choose stronger passwords. They do not mention whether the background image influences user's drawing such as possible hotspots or image-specific patterns which are vulnerable to dictionary attack.

As mentioned above, there are some restrictions on drawing such as keeping strokes off the grid lines and ensuring redrawing in the exact position which impact on the usability performance in DAS. Subsequent studies to diminish the restrictions and improve the usability performance were conducted. Inspired by the old Chinese game of 'Go', Tao designed a new graphical password

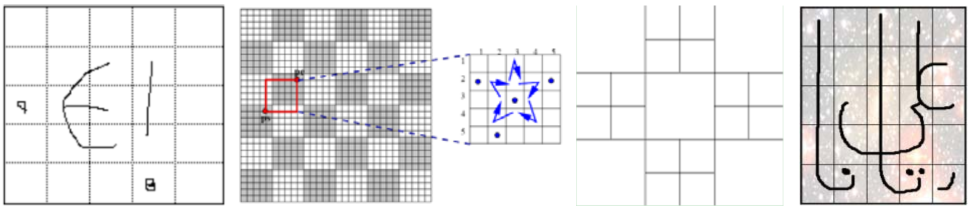
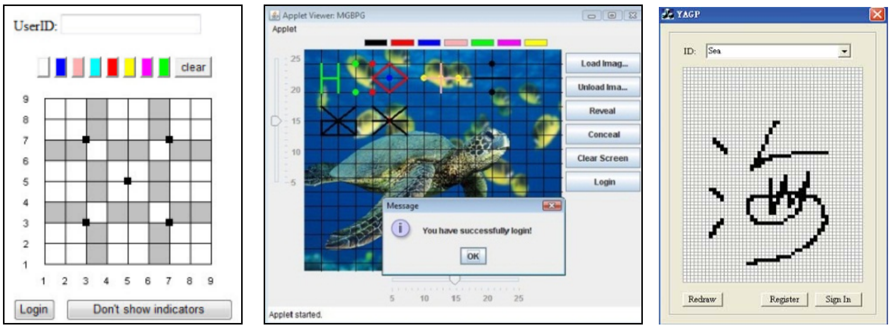


Figure 2. DAS, Grid Selection, Multi-Grid, and BDAS



Message

You have successfully login!

OK

ID: Sea

Figure 3. Pass-Go, Multi-Grid Background Pass-Go (MGBPG), and YAGP

scheme, Pass-Go [18],[19], in which a user drew the password using grid intersection points instead of cells. Consequently the coordinate system refers to a matrix of intersections, rather than cells as in DAS. Due to a finer grid structure, the theoretical password space of Pass-Go, which allows diagonal movements and pen color as optional parameters, is larger than DAS's.Thorpe and Tao et al. [17]-[21] demonstrated that 40% of passwords in Pass-Go fall into a subspace defined primarily by symmetry, with respect to a central vertical and horizontal axis, and 72% passwords have only 4 or fewer strokes. This significantly reduces the effective password space and dictionary attacks remain a concern. Background Pass-Go (BPG) [30], proposed by Por et al., added background images to Pass-Go to assist users in remembering their passwords and reducing the success rate of guess attacks, similar to the idea of BDAS. Por et al. presented Multi-Grid Background Pass-Go (MGBPG) [31] based on the inspiration of Multi-Grid DAS, Pass-Go and BPG. In MGBPG, users can select a personalized background image and grid line scaling to decrease memorability. The issue in MGBPG is to find a balance between a memorable password and higher security.

Gao et al. presented a novel graphical password scheme, YAGP [32],[33]. It adopted partial matching to relax the restrictions for users based on Levenshtein distance string matching and “trend quadrants” looking at the direction of pen strokes. A finer grid granularity was used to lead users to design a longer password which could enlarge the effective password space. It is hard for others to imitate since the trend quadrant sequence and block position of the password are significant characteristics. Moreover, graphical passwords can be drawn anywhere on the canvas to resist shoulder surfing to some extent.

Varenhorst [34] presented the Passdoodle, allowing users to create a freehand drawing as a password without a visible grid. A doodle should consist of at least two pen-strokes placed anywhere on the screen and can be drawn in a number of colors. The matching process in Passdoodle is more complex than in DAS. After reading the mouse input, the system begins to scale and stretch the doodle to a grid, and then compares the stretched doodle with the stored user data. Weiss et al. proposed PassShapes [35], a similar system to Passdoodle. PassShapes is simple geometric shapes constructed from an arbitrary combination of eight different strokes. During login, there is no grid and the password can be drawn in variable sizes or positions on the screen since only strokes and their order are evaluated. Although PassShapes provides better memorability, its password space is relatively small since each stroke is constructed from 8 possible choices.

Malek et al. [36] designed a scheme for resisting shoulder surfing attacks incorporating the sense of touch via haptic technologies. Parameters such as pressure and velocity can be handled as ‘hidden’ features to increase the resiliency of the scheme. Their experimental result showed that users applied very little pen pressure and rarely lifted the pen while drawing. Lin et al. presented a variation of the DAS, Qualitative Draw-A-Secret (QDAS) [37]. In this scheme, a stroke is mapped to its starting cell and the sequence of qualitative direction changes including “up”, “down”, “left” and “right”. So the user only needs to remember the starting cell index and the correct direction order of each stroke. QDAS uses qualitative spatial relations and dynamic grid transformations to reduce potential usability problems and shoulder surfing attacks. However, QDAS did not solve the issue of usability in DAS where the drawing cannot pass through a crossing point. It remains a concern whether the use of grid transformations will create new problems, such as cells decreased to a predefined minimum size, much smaller than the original.

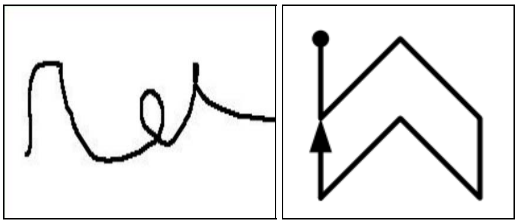


Figure 4. Passdoodle, and PassShapes

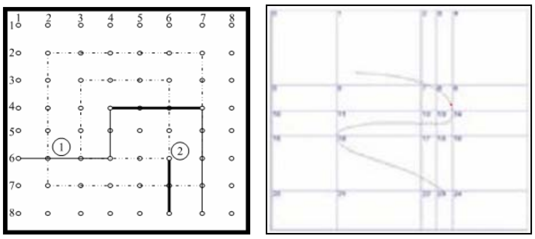
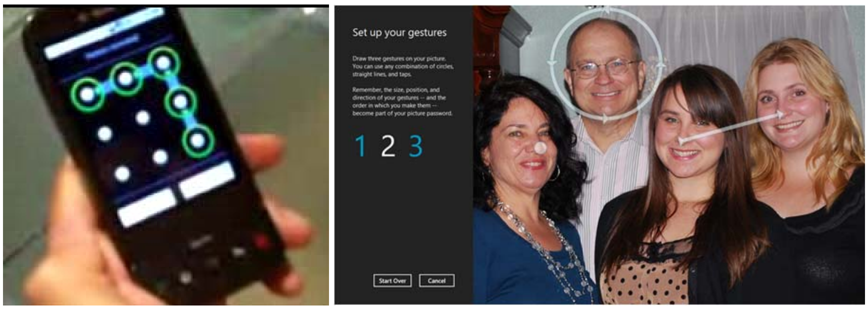


Figure 5. Malek’s scheme and Qualitative Draw-A-Secret (QDAS)



Set up your gestures

Draw three gestures on your picture. You can use any combination of circles, straight lines, and taps.

Remember, the size, position, and direction of your gestures -- and the order in which you make them -- become part of your picture password.

Figure 6. Android password and Windows 8 password

To date, there are only two commercial products of Drawmetric graphical password scheme. An unlock scheme resembling a mini Pass-Go has been used to unlock screens on Google Android cell phones [38]. A user can decide his own unlocking pattern by dragging his finger or stylus over several points in a *3×3* grid. The theoretical password space is only 2^{18} bits, yet is sufficient for phones which do not require a very high security level. However, the Android screen-unlock scheme has been proved to be susceptible to "smudge attacks" [39], where attackers get the password via the smudges on the screen. Aviv, et al. [39] examined the feasibility of such smudge attacks on touch screens for Smartphones using the Android platform. In the Window 8 system, Microsoft introduces a new graphical password [40].First a user is provided an image and then draws a set of gestures in the image. The three types of gestures offered include: circles, straight lines, and taps.Any combination of those gestures can be used for a password. Even though one study declares that guessing the correct gesture set based on smudging is very difficult, attack types like hotspots (i.e. dictionary attack) and shoulder surfing remain a concern. The two products of the Drawmetric graphical password scheme demonstrate clearly that commercial product schemes must be easy to remember, simple to operate, and apply to systems which require low security level.

B. Locimetric Schemes

Locimetric schemes, also called click-based graphical password schemes, are based on the loci method, an old and well-known mnemonic [41]. In Locimetric schemes, a user is provided with an image so that he or she can choose any point in the specified zone or any place in the image as a password click point. Successful authentication includes the right click points and their correct order. Locimetric schemes date back to Blonder's patent [7]. PassPoints, its successor, is a representative scheme of this category.

Blonder, the first graphical password scheme, was proposed in 1996, required the user to click on predetermined areas (or tag regions) of the predetermined graphical image in a predetermined sequence, as a means of entering a password [7]. This scheme possessed several advantages over alphanumeric passwords. First, people generally find images easier to recall than alphanumeric sequences, particularly images with personal meaning. Second, such password scheme provides higher security than alphanumeric passwords, and even a very coarse matrix of predetermined areas yields increased security. However, Blonder's authentication system had some disadvantages. For example, predefined regions should be readily identifiable and the number of predefined regions is small, perhaps a few dozen in a picture. The password may require many clicks for adequate security increasing tedium for the users. In addition, it is more vulnerable to shoulder surfing compared to alphanumeric passwords.

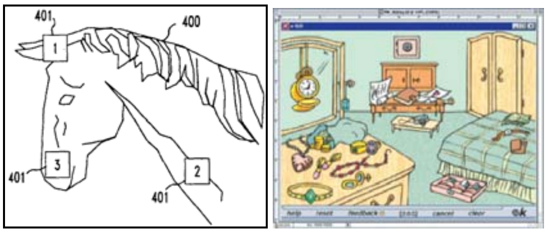


Figure 7. Blonder and V-GO

V-GO [42] is a commercial graphical password scheme developed by Passlogix based on Blonder's idea. In order to be authenticated, users must click on various items in a graphical image in the correct sequence [13]. Every candidate item in the image has an invisible borderline for detecting whether or not an item has been clicked by a mouse. Users can easily remember the password by using components. In order to ensure security, the image must consist of as many meaningful things as possible. V-GO is better than both the Blonder and alphanumeric schemes in memorability. However, the predefined selection areas are very small, greatly limiting the password space. Bounded items in image are so obvious that attackers can guess the items effortlessly. In addition, V-GO has no method of preventing users from selecting the most conspicuous objects as a password, which makes password insecurity.

PassPoints [22], proposed by Wiedenbeck et al., extended Blonder's idea by overcoming some of its main limitations. It eliminates predefined boundaries and allows any image to be used, e.g. natural images, paintings, etc. Users can click on any place in the image (as opposed to some pre-defined areas) to create a password. To log in, users must re-enter the chosen click points within a system-specified tolerance and also in the correct order. As an image may contain hundreds to thousands of potentially memorable click points, the theoretical password space of PassPoints is quite large. However, it has been noted that users find it difficult to ensure click points within tolerance and it take more time to enter a password than in alphanumeric passwords.

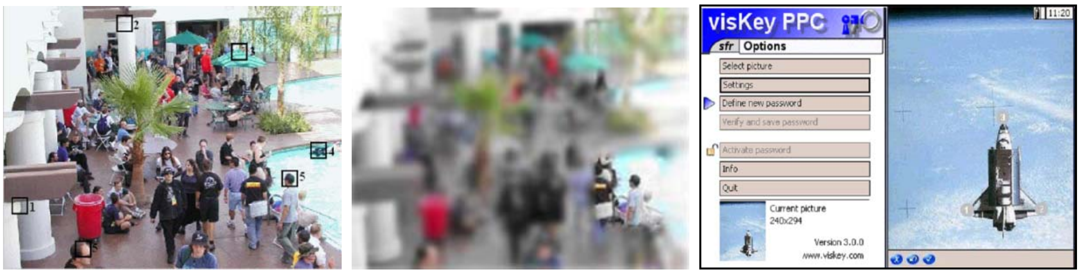


Figure8. PassPoints, Suo's scheme, and visKey

Moreover, PassPoints is vulnerable to shoulder surfing attack since attackers can observe the click points directly during authentication. Suo [43] proposed a shoulder-surfing resistant scheme based on PassPoints. During login, the image is blurred except for a small focus area. Users enter Y (for yes) or N (for no) on the keyboard, or use the right and left mouse buttons, to indicate if their click-point is within the focused area [14]. This process repeats 5 to 10 times. It is easily guessed by attackers if the click points are too few.

A similar technique, visKey, was developed by Sfr [44], and is a commercial version of PassPoints for the PPC (Pocket Personal Computer). This scheme is used for screen-unlock by tapping on a correct sequence of click-points with a stylus or finger. VisKey PPC combines easy handling with high security for mobile devices. Just a few clicks in a picture may offer a large theoretical password space.

To reduce hotspots and improve usability of click-based graphical password schemes, Chiasson et al. [45] proposed Cued Click-Points (CCP), a variation of PassPoints in which users click on one point per image for a sequence of images. The next image is displayed based on the location of the previous click-point, that is, each image after the first is a deterministic function of the current image and the coordinates of the user-entered click-point. If users click an incorrect point, a wrong image will be displayed. It is meaningless to attackers without knowledge of the correct password. However, analysis of user choice revealed that users tended to select click-points falling within known hotspots [46]. Chiasson et al. later designed Persuasive Cued Click-Points [46], added a persuasive feature to encourage users to select more random passwords. Specifically, during password creation the images are slightly shaded except for a small square viewport area randomly positioned on the image. Users are required to select a click-point within this viewport and not click outside of this viewport. They can press the "shuffle" button to randomly reposition the viewport as often as they want until a suitable location is found. During password login, the images are displayed normally without shading or the viewport and users are allowed to click anywhere. PCCP encourages and guides users in selecting more random click-points. It has been proven that PCCP is effective at removing major concerns related to common hotspots and patterns, thus increasing the effective password space, while still maintaining usability [47]. PCCP further reduces the hotspot effects. However, as it failed to address the issue of shoulder surfing attack, user's passwords of CCP and PCCP can still be broken as long as the attacker captures the login process or input sequence [15].

C. *Cognometric Schemes*

Cognometrics schemes, also called recognition based schemes or Search metrics schemes, involve identifying whether one has seen an image before. In Cognometric schemes, the user creates a password by choosing several images from a large portfolio of images, with the selected images becoming the user's password. During authentication, the user must successfully identify his/her password images from decoy images.

Dhamija et al. [48] proposed Déjà vu in 2000, where users selected a certain number of random art pictures from a set of pictures generated by a program in the registration phase. During authentication, the system displays a challenge set that contains both password pictures and decoy pictures. The user must identify which are the password pictures. It is convenient to store and transmit the art images generated by small initial seeds. Moreover, the art images make it difficult to record or share with others [48]. Déjà vu has several drawbacks, for example, an obscure picture is hard to remember and the password space is much smaller than that of alphanumeric passwords.

PassFaces [49] was proposed by Brostoff et al., motivated by the fact that human is familiar with faces. Users need to click on face images pre-selected in

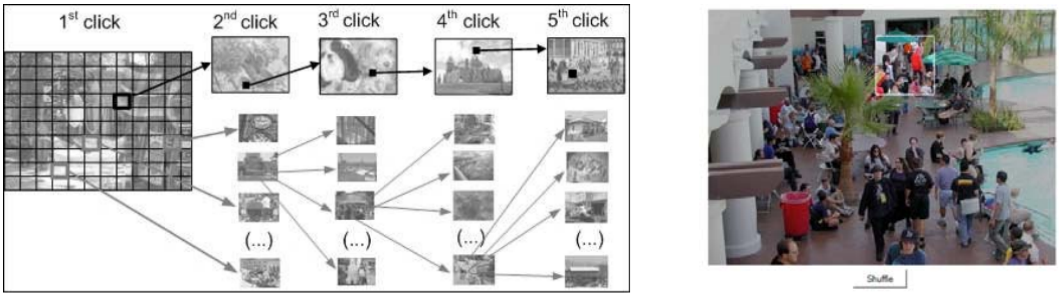


Figure 9. CCP and PCCP

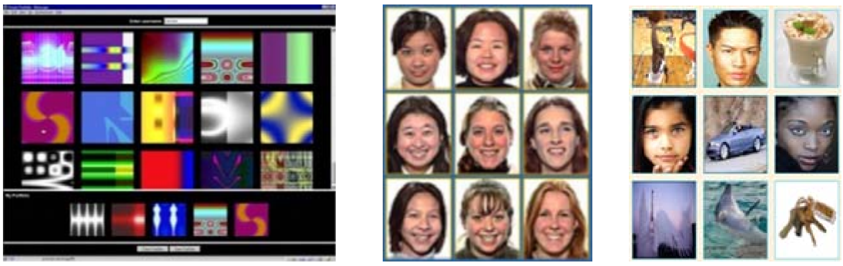


Figure 10. Déjà vu, PassFaces, and Story

registration for several such rounds. Relative literatures reported serious security problems in PassFaces [50]. It is vulnerable to shoulder surfing and spyware because face images are shown clearly. The probability of a guessing attack is high with few authentication rounds. In addition, there are some predictable images users are more inclined to select based on gender, race and complexion.

Photographic authentication [51] was proposed by Trevor Pering, et al. to work on distrusted public Internet terminals. Photographic authentication technique works with a trusted "home server" which stores users' photographs and account information. When users log into the system, the Web-service hosts receive the necessary credentials from the home server. The author establishes a prototype authentication system, with 4 images in a panel and 10 rounds. Users use their own pictures as passwords, while the system selects other pictures as decoy pictures. Base results demonstrate that photographic authentication is a viable technique that can reasonably withstand most replay attacks [51]. Awase-E [52] also uses a user's favorite pictures as the password. It gives another function-notification which gives users a trigger to handle malicious attempts. Awase-E shows P images with N rounds. Every round includes one or zero passimage. During login, according to the number of passimages in this round, users must select one or no passimage. With Awase-E both security and usability reach a higher level [52].

Similar to PassFaces, Story [53] only needs one round of authentication, but password images are a sequence of several unique images that creates a story to enhance memorability. When users authenticate, "tell a story" can string password pictures up. The story requires users to remember the order of images. So it is difficult for users who did not take the advice of using a story to guide their image selection to remember the password. For example, of the 236 incorrect password entries in Story, over 75% of them consisted of all the correct images yet with incorrect order [53]. So the importance of "make a story" should be emphasized to users. Picture Password [54] also authenticates only in one round, and this scheme is used in PDAs. Picture Password with *5×6* matrix displays 30 identically sized squares for its thumbnail images. There are two selection styles in Picture Password: individual selection and paired selection. Individual selection requires a quick single click on an image, while paired selection requires users to choose and link a pair of consecutively selected thumbnail images. Due to the two styles of image selection above, the password space increases from 30 to 930. VIP [55] has three versions: VIP1, VIP2 and VIP3. VIP1 displays images in the same locations. Users need to memorize a sequence of 4 images and enter them in a fixed order during login. VIP2 differs from VIP1 in that the 4 passwords images are displayed randomly. If authentication fails, the system will display the same visual configuration to avoid leaving any clue about the password. In VIP3, users need to identify 8 images and 4 images will be presented randomly together with 12 distracters on each attempt to authenticate. During login, users are allowed to select password images in any order. Compared with alphanumeric PINs, VIP takes more time to login, but it is more secure. As decoy images are changed at each authentication, attackers are able to recognize users' password images by comparing two screens. Therefore the VIP series are subject to shoulder surfing and phishing which occurs frequently during a normal ATM transaction.

Cognitive Authentication [56] is designed to resist spyware and shoulder-surfing. If a user stands on a picture belonging to the portfolio, then he will move down or move right until the right or bottom edge of the panel is reached, the label of row or column is recorded and a multi choice question which includes the label for the path's correct point is displayed for each round. The system computes the cumulative probability that the correct answer was not entered by chance after each round. When probability passes a certain threshold, authentication is success. The threshold enables the system to tolerate some user errors. An observer who

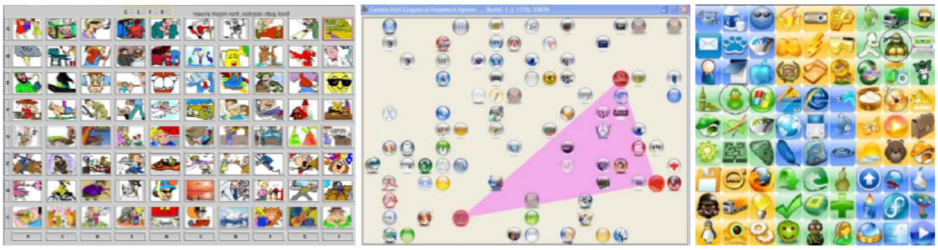


Figure 11. Cognitive Authentication, Convex Hull Click, and Colorlogin

records any feasible number of successful authentication sessions cannot recover the user's secret by the conjectured brute-force or enumeration method [56].

Convex Hull Click [24] also resists shoulder surfing in a public environment, where video recording and electronic capture are ineffective in this situation. Hundreds of icons displayed randomly in one panel and users choose and memorize several icons to create a password. Each panel includes at least 3 or more passwords icons. These three or more pass-icons together form a convex hull which is visual to users in mind. Users can click anywhere in the convex hull during login. Because users don't click the pass-icons directly, it resists shoulder surfing attack. Additionally, this scheme enjoys a large password space, with the negative consequence of increasing login time significantly.

Use Your Illusion [57] requires users to select distorted password images from decoys. The password images will be distorted after users have chosen their password images. It resists shoulder surfing attack and social engineering attacks because all pictures in the panel have been distorted. Colorlogin [58] is also designed for protection from shoulder surfing attack. When a user clicks on a row containing the pass-icon it means that he has chosen the correct pass-icons. All icons in that row are then replaced with lock icons. A round authentication will not be considered successful unless all pass-icons in one panel are correctly chosen. The background color decreases users' login time. Although the password space is large, once the pass-icon's color is revealed the password space shrinks sharply.

GPI (Graphical Password with Icons)/ GPIS (Graphical Password with Icons suggested by the System) [59] is designed aimed at solving the hotspot problem. In GPI, users select 6 icons from 150 icons as a password in one panel. With GPIS, the system generates a random password and displays it to users. If the user is not satisfied with the password the system generated, he can request the system generate new password until accepted. The main drawback of GPS is its unacceptable login time and small size of icons.

D. Hybrid Schemes

Hybrid schemes are typically the combination of two or more schemes or other authentications. These schemes are used to overcome the limitations of a single scheme, such as shoulder surfing, hidden camera, or spyware and so on. We will provide a detailed description of these schemes, focusing on memory mode and primary function.

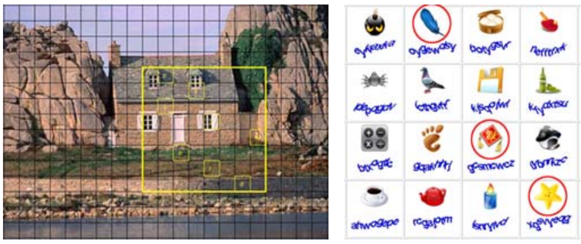
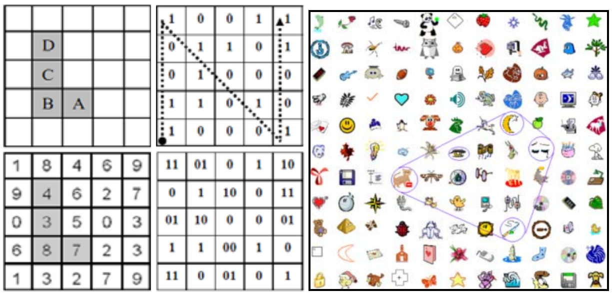


Figure 12. Jiminy and using CAPUCHA

Jiminy [60] uses image as a cue for helping users choose easy to remember passwords. In this scheme, users are provided with templates based on color that contain several holes. The user first selects an image, chooses a coloured template, picks a specific location inside the image, then clicks on the position to place the template and record the password [60]. During login, the users must select the right template, place it on the correct location on the image then enter the characters visible through the holes from top to bottom. Compared to remembering alphanumeric passwords, this scheme only requires users to remember the precise location of template on the image. However, experiments show that users have difficulty in remembering precise locations and their selections tend to be predictable, suggesting doubt about the efficacy of hotspot resistance [60].

Using CAPTCHA (Completely Automated Public Turing tests to tell Computer and Humans Apart) [61] [62], proposed by Gao el at., retains the advantages of graphical password schemes, while simultaneously raises the cost for adversaries by orders of magnitude. In the register phase, users select and remember images as their password images (pass-images). To be authenticated, the user needs to distinguish his pass-images as well as complete a test by recognizing and typing the adjunctive string below each pass-image. Although this scheme is almost impossible for automated programs, it could be in insecure if the adversary is a person and uses spyware as an assistant.

GrIDsure [63], a commercial product, is a graphical one-time PIN scheme, which makes PINs more resistant to shoulder-surfing attacks by using graphical passwords on a grid. During password creation, users choose and memorize the shape (e.g. an "L" shape) and the order that they want to enter the corresponding numbers (e.g. bottom to top) in a 5×5 grid, and enter the sequence numbers using a keyboard. The selected shape and order of cells is called the user's pattern, representing the secret they must remember in order to authenticate. Then on each subsequent login, the grid is populated by random numbers between 0 and 9. Users enter the numbers that appear in their pattern in the previously selected order (e.g. bottom to top). Security analysis reported that GrIDsure password is more secure than traditional PINs especially in shoulder-surfing attack resistance, with the level of security dependent on the context of use [63]. However, some users could not recall the shape's exact location or sequence of cells. A similar scheme was proposed by Zheng, et al., [64] with the difference being



	D			
	C			
	B	A		

1	8	4	6	9
9	4	6	2	7
0	3	5	0	3
6	8	7	2	3
1	3	2	7	9

1	0	0	1	1
0	1	1	0	1
0	1	0	0	0
1	1	0	1	0
1	0	0	0	1

11	01	0	1	10
0	1	10	0	11
01	10	0	0	01
1	1	00	1	0
11	0	01	0	1

Figure13. GrIDure, Zheng's, and Man's schemes

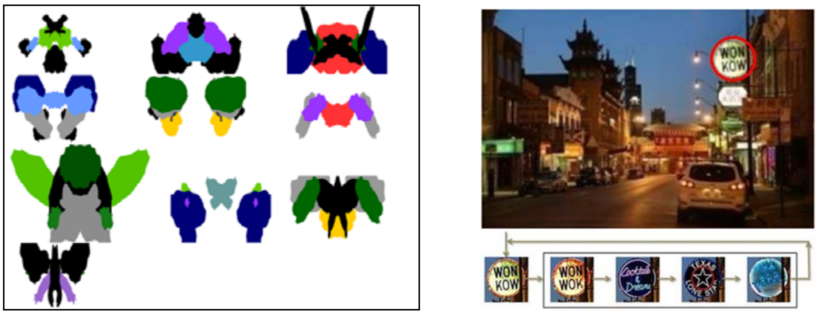


Figure 14. Inkblot and Click-a-secret

that in order to improve security, the authentication interface of this scheme varies in that one or more numbers (0 or 1) appear in each cell.

Man, et al. [65] proposed another shoulder surfing attack resistant scheme. In this scheme, users select several images as pass-objects which have many variants. Each variant is assigned with a unique code. During log in, users must enter a string with the unique code of the pass-objects' variants and a code indicating the relative location of the pass-objects in reference to a pair of eyes in several rounds provided by the system. This scheme is almost completely resistant to shoulder surfing attack, but it requires users to remember a substantial amount of code corresponding to the pass-objects variants. An improved scheme, Pass-Object [66], based on this one was later proposed by Hong, et al. allowing users to assign their own codes to the pass-object variants.

Inkblot [67] is a graphical tool for remembering text passwords, which aims to ensure that an easily remembered password is secure. During password creation, users are presented with a series of images which are computer-generated "inkblots", and asked to enter the first and last letter of the word or phrase that best describes each inkblot in sequence as a password [14]. Then on each subsequent login attempt, users see the same inkblots as cues and are asked to enter each of their 2-character responses. Experiments show that the security level of the passwords created by this scheme is sufficient. Even if an attacker sees the images, he could not guess the user's password.

Zhao and Li [68] proposed a Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication scheme (S3PAS). This scheme seamlessly integrates both textual and graphical passwords and is resistant to shoulder-surfing, hidden-camera and spyware attacks. During the registration phase, users select a string *k* as the original password. The length of k depends on different environments and different security requirements. In the login phase, they find their original password in the login image and then click inside the invisible triangles, called "pass-triangles", created by the original password.

"Click-a-secret" [69] proposed by M. Éluard et al., is a combination of Locimetric and Cognometric schemes that allows entering a secret though interaction with an image. Users create a personal image by replacing some particular regions of the original image with an alternate version. The particular region, named Gecu (Graphical Element Chosen by User), has a specific graphical element present in the original image (e.g. people, animals, vehicles, signs, architectural elements and so on). In register phase, the user clicks on Gecu in the original image, which is then replaced by an alternate version. When he thinks the current image is suitable, the user validates their personal image. This process continues for several rounds creating the user's password. In the login stage, the user clicks on Gecu in the initial image, until he finds all of his personal images. Although this scheme enhances the interaction with images, its usability is not high due to the limitation of its small theoretical password space.

Gao et al. [16] proposed a new shoulder surfing resistant scheme, called CDS (Come from DAS and Story), based on the inspiration of two representative graphical password schemes: DAS and Story. CDS adopts a similar drawing input method in DAS and inherits the association mnemonics in Story for sequence retrieval. In password creation, a user orderly selects several images from the register panel and then remembers the connection of the password images by mentally constructing a story. During login, a degraded version of the images is randomly arranged on the screen, which is difficult to distinguish from a distance or from a side view. The user should draw a curve across the password images orderly without lifting the stylus. The curve passes through both password images and decoys and the majority of the drawing trace would be cleared as the stylus slides, reducing the probability of passwords being revealed. Moreover, the curve must begin and end with given random images to avoid revealing the first and last password images. All of these measures enhance the properties of shoulder surfing resistance. When he thinks the current image is the correct one, the user validates his personal image. Nevertheless, its small theoretical password space and hotspots issues make it vulnerable to brute force attack and dictionary attack.

PassHands [70], designed by Gao et al., combines recognition-based graphical passwords with hand-based biometrics. It utilizes processed hand images instead of human faces, with similar authentication procedures as PassFaces. In the authentication phase, nine identically sized subimages which are processed by the same graphic processing method, placed randomly in a 3×3 grid where one of the images is a password image and the rest are decoy images. In addition, there is a schematic diagram of one hand on the screen, and a red square indicates the

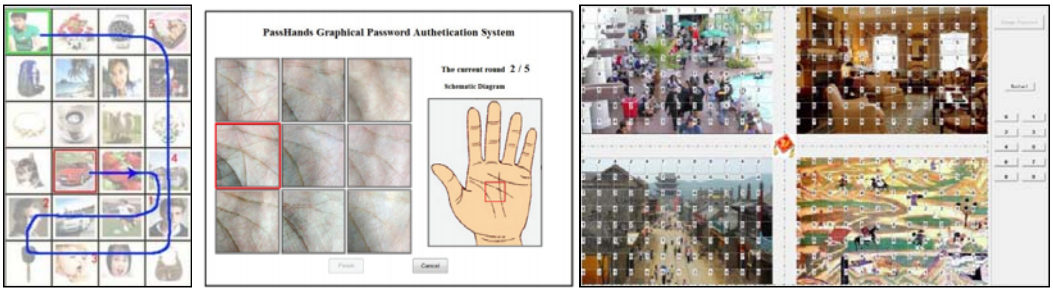


Figure 15. CDS, PassHands, and CBFG

corresponding location of the displayed subimages on the hand. During authentication, the user compares their left or right hand to the specific region with the generated image and then clicks the password image. However, the usability of PassHands is weak to other simple graphical password schemes, since the hand comparison process increases login time.

CBFG [15], a combination of Locimetric, Cognometric and alphanumeric schemes, inherits the basic principle of PassPoints and introduces the ideology of image identification. During registration, the system presents four background images and ten icons. Users must select at least one cell on each image as pass-cells and choose one icon as pass-icon. On the login screen, there are four background images with a random number (0~9) in each cell, one icon and ten numeric buttons representing 0 to 9. Users should click any numeric button until the icon is the pass-icon, and then click the numeric button corresponding to each pass-cell, with no need for specific pass-cell order. After authenticating the pass-cells, users should continue to click the remaining numeric buttons to ensure that all the buttons are clicked and until the system generates a successful or failed message. With multiple background images, CBFG provides a large password space. The visual information contained in each cell results in the existence of hotspots in user selection of pass-cells. Since the sequence entered each time has strong randomicity, and the start-time, end-time as well as password length are well hidden, it is still difficult for the attacker to guess the user's password even if he records the entire login process with a camera. They experiment results indicated that CBFG has strong capability against shoulder surfing and intersection analysis attack. However, some risks appear due to user behavior, such as the difference in the button click time interval.

IV. Attack Types Based on Password Space

An attack is the most serious risk for the security of password space. Attacks based on password space are common with the brute force search and dictionary attack the most common of these attacks. The following subsection provides a brief introduction to brute force search and dictionary attack and summarizes three universal password space formulas.

A. Password Space

Password space is the number of options in the scheme available to users for choosing a password. Graphical password schemes include two kinds of password spaces: theoretical password space and effective password space. Theoretical password space computes all possible passwords, while effective password space considers human factor, it only computes the passwords that users are most likely to choose as passwords. For example, in PassPoints, some areas like grass or sky have no memorable characters to click. So these areas can't be taken into account when computing effective password space.

The security of a password system heavily depends on password space. If the theoretical password space increased to a certain scale, brute force attack can be effectively resisted. On the contrary, if the theoretical password space is limited or insufficient, brute force attack will cause serious security issues. Password space must be a strong consideration in designing a password scheme. The effective password space differs from scheme to scheme, so it is difficult to analyze a universal formula. Here we summarize universal theoretical password space formulas for three kinds of schemes to provide a useful reference data for following research.

1) Drawmetric Schemes

Drawmetric schemes usually ask users to draw several strokes as a password on a given canvas. Every stroke contains information, for example in DAS every stroke consists of pen up, pen down, and the grids which the strokes cross. For schemes with no grids, every stroke includes the sequence of qualitative direction changes. So the formula of the theoretical password space for Drawmetric schemes can be analyzed by following steps. Assume P_i denotes password with i strokes (one password can include d strokes at most). So the theoretical password space T can be deduced by:

$$\mathrm{T} = \sum_{k=1}^{d} P_k \tag{1}$$

b_i is defined as the number of strokes with length i (stroke length can reach l at most), so the total number of stokes B_{total} can defined as:

$$B_{total} = \sum\nolimits_{i=1}^{l} b_i \tag{2}$$

For a password with i strokes, all possible password space can be repeated to take the i strokes arrangement. Namely:

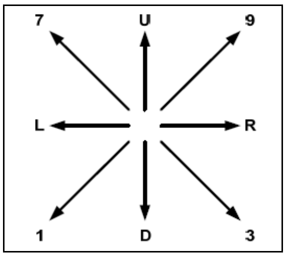


Figure 16. Eight directions in PassShapes

$$P_i = B_{total}^i \tag{3}$$

Combining the above formulas, we can draw the theoretical password space:

$$T = \sum_{k=1}^{d} (\sum_{i=1}^{l} b_i)^k \tag{4}$$

Here we list two examples to explain our universal formula. In gridded schemes (like DAS), b_i is defined as pen up, pen down, and the grids where the stroke crosses. Namely:

$$b_i = \sum_{(x,y)\in[1\ldots G]\times[1\ldots G]} n(x,y,i,G) \tag{5}$$

n(x,y,i,G) is the number of strokes with length *i* and end at the cell *(x,y)*. In a grid of $G\times G$, we can conclude:

$$n(x,y,i,G) = n(x-1,y,i-1,G) + n(x,y-1,i-1,G) \\ +n(x,y+1,i-1,G) + n(x+1,y,i-1,G) \tag{6}$$

While:

$$n(x,y,1,G) = 1$$

For gridless schemes (like PassShapes), b_i denotes the sequence of qualitative direction changes. There are eight different possible directions in PassShapes shown in figure 16. Clearly, $b_i = 8 \times b_{i-1}$, $b_1 = 8$.

2) Locimetric Schemes

Locimetric schemes ask users to select several regions as a password in a given picture. Some schemes use pre-defined selected regions. Assume *N* available regions in a scheme. Users select at most *d* regions as their password. The universal theoretical password space formula for this type of schemes is:

$$T = \sum_{i=1}^{d} N^d \tag{7}$$

Other schemes ask users choose dots as passwords in a given picture. Because users only click on a pixel, the system can set the pixel as center, and select a certain threshold value of S_0 as the password region. Users must remember the sequence in the password region. *S* denotes the area of the picture, and the theoretical password space is:

$$T = \sum_{i=1}^{d} \left(\frac{S}{S_0}\right)^i \tag{8}$$

For this example, we used a *451×331* picture, with a square size of *20×20*. The user can choose 5 to 10 points as a password. Using the universal theoretical password space formula and we can find the theoretical password space is:

$$T = \sum_{i=5}^{10} \left(\frac{451\times 331}{20\times 20}\right)^i \approx 5.23\times 10^{25} \tag{9}$$

3) Cognometric Schemes

Cognometric schemes differ from other graphical password schemes in that they display pictures for users to recognize, and for easy to recognize, the pictures must not be too small. At present, Cognometric schemes usually include an image library with size *N*. User's password pictures include *d* pictures at most. There are two kinds of circumstances in the password picture: orderly and disorderly.

The orderly theoretical password space is:

$$T_{order} = \sum_{r=1}^{d} P_N^r = \sum_{r=1}^{d} \frac{N!}{(N-r)!} \tag{10}$$

The disorderly theoretical password space is:

$$T_{disorder} = \sum_{r=1}^{d} C_N^r = \sum_{r=1}^{d} \frac{N!}{(N-r)!r!} \tag{11}$$

Using Story as an example, we assume the picture library has 150 images, and the user's password images are between 5 and 10. According to the formula, we can compute the theoretical password space:

$$T_{order} = \sum_{i=5}^{10} P_{150}^i \approx 4.27\times 10^{21} \tag{12}$$

From given examples and our analysis, we can conclude that the universal formulas are appropriate for concrete schemes and provide a general understanding of password space.

B. Brute Force Attack

Brute force attack is also known as exhaustive-search attack, since it involves systematically searching all possible elements in the theoretical password space until the correct one is found [71]. It is a strategy that can, in theory, discover all passwords with sufficient time and computing power. The brute force attack may be used when the theoretical password space is relative small or it is not possible to take advantage of other weaknesses which would make the attack easier. The most significant advantage of the brute force attack is simple to achieve. If the attacker gets the theoretical password space of the scheme, he would definitely crack the user's password. In theory, the greater theoretical password space the scheme has, the greater difficulty to crack it by brute force attack. Therefore, an effective method against brute force attack is to increase the theoretical password space, e.g. increasing the length of the password, increasing the number of images and so on. However, these strategies tend to increase the user's memory burden.

Alphanumeric password schemes have a theoretical password space of 64^N, where *N* is the length of the password, 64 is the number of printable characters excluding SPACE. If *N=8*, then the theoretical password space is $64^8 \approx 2.8\times 10^{14}$. In graphical passwords, the password spaces of different schemes vary greatly. Overall, graphical password schemes have been proved to provide a theoretical password space similar to or larger than those of alphanumeric password schemes [13], and Cognometric schemes tend to have smaller theoretical password spaces than other schemes. For example, for PassPoints with image size *1024×752* and grid square size *20×20* (all measured in pixels), the passwords consist of five click points, the theoretical password space size is $1925^5 \approx 2.6 \times 10^{16}$. The brute force attack programs must find the theoretical password space of the graphical password schemes to break a user's passwords, and automatically generate accurate mouse motion to imitate human input. For example, in PassFaces, in order to use brute force attack to obtain the use's password, the attack program must obtain all images in the system. The scheme has millions of images where each image appears in the interface randomly, so finding these images is quite difficult for brute force attack programs, and requires substantial time and computer power. Generally speaking, it is more difficult to use a brute force attack against graphical passwords than alphabetic schemes.

C. Dictionary Attack

Dictionary attack involves guessing passwords from an exhaustive list called a dictionary (from a pre-arranged list of values) which typically consisting of all passwords with higher possibility of being remembered easily, ordering from most to least probable [72]. Compared with the brute force attack, where all elements in theoretical password space are searched systematically, dictionary attack tries those possibilities most likely to succeed from the dictionary. Dictionary attacks may succeed as many users tend to choose from relatively small subsets of the theoretical password space known as weak password spaces, which are simple, easily predicted or relating to their personal information, and can be specified. The theoretical password space does not absolutely guarantee security. Another important factor is the effective password space containing passwords with predicted probabilities higher than a set threshold. So if the probability distribution of the passwords is non-uniform, the password scheme will be more vulnerable to dictionary attacks.

Dictionary attacks can be divided in to two categories: online and offline dictionary attacks. In online dictionary attack, an attacker tries to log in as a legitimate user and examines the validity of possible passwords by interaction with the live system [36]. The attacker simply inputs his guessed passwords and waits for the response of the live system. If the system rejects the password, he tries another guess until gaining successful login. For graphical or text passwords, the online dictionary attack can be thwarted by: clever use of CAPTCHAs [73]; limiting the number of incorrect attempts to per user account; increasing the delay of two consecutive error logs. However, these strategies are often frustrating to legitimate users who forget their passwords, they enable denial-of-service attacks, and are helpless against multi-account attacks [14]. In offline dictionary attack, an attack need not interact with the live system to verify guesses, and may access the database that contains hash values of the user's passwords [36]. An attacker makes a guess of the password first, evaluates the hash of his guess, then searches the entire password database for any match. If a match is found, the attacker imitates the legitimate user whose password is appropriately guessed. Else if a match is not found, he can repeat this guess process as many times as he want. Schemes are more vulnerable to offline dictionary attack than online attack, as offline attack is not visible, processing trial guesses can be quicker and pre-computed data structures or special hardware may be used [14].

For graphical passwords, successful dictionary attacks are mostly due to the predictable patterns in user choice, and these patterns are strongly association with the schemes users choose. Dictionary Generation Algorithms in different graphical password schemes are very different, but they are all closely related to user choice in the password creation phase. Replicating all details of user choice in every scheme is beyond our scope. Instead, our goal is give a brief description of user choice by giving some representative examples in each type.

Drawmetric schemes require users to draw their password on visible or invisible grids. In some Drawmetric schemes, user's drawings contain the predictable characteristics relating to symmetry, number of composite strokes, and centering within the grid [74]. Nali and J.Thorp analyzed user choice in DAS and Pass-Go, they reported that approximately 45% of users chose symmetric passwords, 2/3 of which are mirror symmetric (reflective); approximately 80% users chose passwords composed of 1-3 strokes; about 86% of the passwords are centered or approximately centered (meaning centered about a set of cells adjacent to the center grid lines) [74]. It could be seen from the choice of users that effective password space is often much smaller than the theoretical password space. So an attacker may take advantage of these features when user creates a password to generate dictionary for dictionary attacks. A successful dictionary attack on DAS requires less effort than the brute force attacks which search the full theoretical password spaces. Multi-Grid can decrease centered password to less than 50%, so this scheme is more effective against dictionary attacks.

Locimetric schemes usually use images as clues, in which users select and click a few points (e.g. select five points) on images as their passwords. In the process of selecting passwords, the user tends to follow predictable rules, known as hotpots and patterns. Hotpots [75] are popular points or areas in an image which a have higher probability of being chosen by user. Patterns are straight line or simple geometric shapes in a password. Studies show that 7% to 16% of passwords from two representative images use dictionaries of approximately 2^{26} entries (where the theoretical password space is 2^{43}) [76]. Patterns [77] are straight lines or simple geometrics formed by user choice in passwords. The attacks often take advantage of the weakness in the password creation phase to set up the dictionary, and then crack user's password. For example, in PassPoints, users will tend to choose the points that compose their click-based graphical password based on the order in which the points draw their visual attention, as Figure 17 shows.

Cognometrics schemes, which mainly use the human's ability of memory graphics, require users to identify and memorize the images selected during registration. There are many factors affecting users choice when they select images as their passwords, such as race, gender, and so

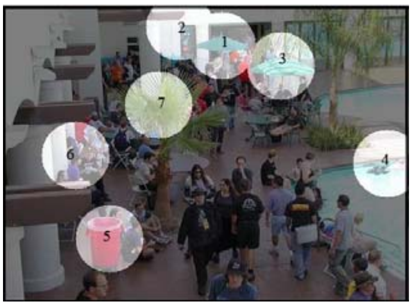


Figure 17. User choice in PassPoints

on. Research on PassFaces and Story explore the regular patterns and characteristics of users in selecting password images [78]. For PassFaces, experimental results show that the faces chosen by users were highly correlated to the race of the user, which usually easily select the race similar to themselves. Both male and female select female faces more often than male faces, and then select attractiveness more often than not. For Story, these features in choosing passwords still exist though to a lesser extent. In this study, the authors used these features to establish a dictionary, and then searched the dictionary to crack passwords. For PassFaces, 25% of user passwords could be guessed in 13 attempts, and the weakest 10% of males' passwords could be guessed in only two guesses. For Story passwords can be cracked by navigating the dictionary. Although the cost of attempts is increased, it is still far less than that of violent force attacks.

Hybrid schemes are a combination of two or more schemes or other authentications, and do not share the common characteristics of all schemes. However, it still has some characteristics or bias to specific schemes, such as hotpots in Jimmy or common patterns in Inkblot and so on. Although the cost of attacks increased, attacks could still make use of these characteristics or bias for dictionary attacks.

Generally speaking, dictionary attacks in graphical password schemes may require higher cost than textual schemes. Cognometric, Locimetric and Hybrid schemes offer more security than Drawmetric in dictionary attacks.

V. Attack Types Based on Password Capture

This section discusses attack types based on password capture. Common means of attack: shoulder surfing, intersection analysis, social engineering and spyware attack.

A. *Shoulder Surfing*

Shoulder surfing refers to someone using direct observation techniques to capture passwords [79]. For example, someone watches over the user's shoulder as the user enters a password or records the user's input with an external device, such as video cameras. Shoulder surfing is particularly effective in public places and is usually unknown to the legitimate user. Using shields that partially protect password entry terminals from the visual scope of cameras and other methods was proposed to counter shoulder surfing attacks in textual password schemes. Nevertheless, these techniques will not protect users from shoulder surfing when attackers clearly watch the passwords. Due to the visual interface, shoulder surfing has increased as a severe security threat for graphical passwords. Most of the current graphical password schemes are vulnerable to shoulder surfing [80]. Several approaches such as those where the user does not directly click the password have been developed to deal with this problem, but they have significant usability drawbacks, usually in the time and effort to log in, making them less suitable for everyday authentication.

As for Drawmetric schemes, the entire drawing is visible on the screen while it is being drawn, and passwords can be recovered from only one accurate observation of login process. It is believed that DAS would be susceptible to shoulder surfing since the entire drawing is visible on the screen while being drawn, so as BDAS and Pass-Go and picture password in Windows 8. It has been reported that only a few schemes are resistant to shoulder surfing. QDAS provides a high level of resistance to shoulder surfing through the use of a qualitative mapping between user strokes and the password, and the use of dynamic grids to both obfuscate attributes of the user's secret and encourage them to use different surface realizations of the secret [37]. Malek's scheme is more resistant to shoulder surfing attacks than any other previous Drawmetric schemes. They integrated an invisible attribute of the input device, pressure, into the graphical passwords in such a way that it increases the entropy of the graphical password and counters shoulder surfing attacks. In Passdoodle [34], reproducing the drawing may be difficult if drawing speed or acceleration is adopted as one of means to identify a password. Owing to the position-free element of drawings and the consideration of drawing trends, YAGP obtained a good performance in resisting shoulder surfing.

All of the Locimetric schemes are vulnerable to shoulder surfing because clicking on images on a large screen in an external physical environment may make user's actions easier to capture. Thus, Locimetric schemes are not appropriate for crowded places such as university libraries, airport kiosks and shopping malls. Researchers developed several Cognometric schemes which are strongly resistant to shoulder surfing. These schemes have common characteristic, in that they do not need to click the password images directly. Even though the attackers observe the entire authentication session, it is ineffective in helping them capture the user's password images. In CHC, users need to identify their pass-objects, visualize the triangle they form and click inside the convex hull [24]. Unlike CHC, the shoulder surfing resistant scheme proposed by Weinshall et al., involves remembering a number of images and computing a path through a panel of images according to certain rules. ColorLogin is resistant to shoulder surfing because of the selection of the row where the pass-icons are and the concealment of the clicked row. Each of the three schemes can provide good protection against shoulder surfing. Other schemes like Déjà vu, PassFaces and Story are subject to shoulder surfing because users click the password images directly.

Most of Hybird schemes are intent to enhance the security of graphical passwords by providing good protection against shoulder surfing. Man et al. proposed a scheme dependent on users remembering several images (pass-objects) and their corresponding text codes as well as coding the relative location of the pass-objects in reference to a pair of eyes [65]. For GrIDsure, if attackers don't know the shape of the password, the key sequence, which changes every time, is useless. So GrIDsure can resist shoulder surfing to some extent [63]. S3PAS's password is characters and numbers, with an authentication process similar to the CHC scheme [24] [68]. Zheng et al. proposed a scheme based on shape and text to overcome the shoulder surfing problem. It uses shapes of strokes on the grid as the original passwords and allows users to login with text passwords via traditional input devices which hide the shapes of strokes during authentication [64]. Other schemes (like Using CAPTCHA and CBFG) combine the image and text, which significantly resists shoulder surfing [15] [61]. CDS requires users to orderly draw a curve across their password images rather than click directly on them [16]. The drawing input trick along with complementary measures, (erasing the drawing trace, displaying degraded images, and starting and ending with randomly designated images), provide good resistance to shoulder surfing.

In practice, a shoulder surfing attack is closely related to the place where the schemes are used. Shoulder surfing is particularly effective in fixed places, especially where a miniature camera can be concealed in ceilings or walls to record the authentication session. Also, it is relatively easy to observe user's action in crowded places such as university libraries, cybercafés, airport kiosks without user's awareness. However, with portable devices, a user can avoid exposing the password by shielding the authentication interface by his hand or body or moving to less crowded areas when authenticating. Thus the measures available for portable devices significantly reduce the impact of shoulder surfing.

B. *Intersection Analysis*

First mentioned in Déjà vu, intersection attack is where all the password images are part of the challenge sets, and decoy icons are changed in each round. Intruders can use the intersection of two challenge sets to reveal the password images [48]. It is a common problem in existing graphical password schemes such as CHC and PassFaces using multiple images choice as pass objects.

An intersection attack is possible when the frequency of an image appearing at login can be used to determine its role as either a key or a decoy. The only practical method proposed in previous research to complicate the shoulder surfing threat is innately vulnerable to this attack [1]. In the VIP system the user is assigned a key image profolio, of which a random subset is exposed at each login. The effect of this is that observing key images at one login might not be useful when logging in at the next. In the described setup each decoy image is certain to appear at login, but due to the variation afforded by the key image portfolio each key image has a 50% chance. In this scenario an attacker can derive the key images without an attack that involves manipulation or observation of the legitimate user. Current wisdom to protect against this attack is not to implement a key image portfolio at all, to ensure every login challenge is the same. One side-effect of this solution is that the login trial is intuitively more vulnerable to observation, as everything the attacker learns is useful in an immediate replay attack.

In VIP3, the key pictures and decoy pictures are displayed randomly and therefore the intersection does not work. In PassFace each round contains a key picture, others are displayed randomly. The different probabilities create an intersection.

C. *Social Engineering*

Users are often labeled as the weakest link in a computer system [81] [82]. It is easy for hackers to collect confidential information from users through social engineering attack. Orgill's et al. [81] definition of social engineering: "Social Engineering is a technique used by hackers or other attackers to gain access to seemingly secure systems through obtaining the needed information (for example, a username and password) from a person rather than breaking into the system through electronic or algorithmic hacking techniques". The attacker makes use of the natural human tendency to trust to deceive the user into giving useful information. Tricking, Phishing and Pharming are typical and common social engineering attack techniques.

1) *Tricking*

Compared to text passwords, graphical passwords are more difficult to share with others. Given that a picture contains much more information than text, so it is more difficult for people to describe a picture accurately. Therefore, graphical passwords are less susceptible to Tricking. For Drawmetric schemes, making use of oral description to convey a password is relatively complicated, but users can share passwords to an attacker by drawing a sketch. However the difficulty of drawing a sketch of password differs for different schemes. For identical cell schemes like DAS, it is easy to redraw a password. But for schemes where cells are not identical schemes (multi-Grid), users can't redraw a password easily. Other schemes use background pictures, which makes description easier.

For Locimetric schemes, there are many spots which users select as password, and some of them have similar descriptions. In PassPoints, where there are many people in the Figure 8, users select several heads as the password. This makes users' descriptions of the password difficult, and so this scheme makes it harder for sharing passwords than Drawmetric schemes.

For Cognometric schemes, some schemes like Déjà vu and Use Your Illusion, the pictures are abstract. It is very difficult to describe them verbally and record them. For other schemes containing icons, like CHC, Colorlogin and GPI/GPIS, there are many icons, most of which can be described making these schemes relatively easy to share password with others. There are no icons picture in Story and VIP, but the picture can be easily described because the picture is different from others. Remaining schemes which use pictures e.g. PassFace and Cognitive Authentication Schemes, the picture is so similar in description that we can't share with others verbally, making Tricking ineffective.

Hybrid Schemes (like Using CAPTCHA) use icons which can be easily described. In Click a Secret, every part is different, so description is easy too, and therefore Tricking is easy. PassHands is based on Biometrics Recognition. It is difficult to find the palm-lines and finger knuckles. In schemes which mix text and shape like S3PAS, if hacker knows the theory of the scheme and gets the sequence of the text, it is easy for him to crack a user's password. CBFG is similar to PassPoints, and password description is difficult. Inkblot uses abstract images, making description and Tricking very difficult. Overall, picture passwords are more difficult to share and record than text passwords.

2) Phishing and Pharming

Phishing [83] is a way of acquiring confidential information such as usernames, passwords, and credit card details by posing as a trustworthy entity in a network. Phishing is mainly carried out via e-mail spoofing or instant messaging, and it often guides users to enter usernames and passwords on a fake website which looks and feels almost same to the legitimate one. Phishing is the main social engineering technique used to deceive users.

Pharming [84] is an advanced form of phishing. Pharming is a hacker attack which is intended to redirect a website's traffic to another bogus site. Pharming can be conducted either by changing the host file on a victim's computer or by exploitation of a vulnerability in the DNS server software. Compromised DNS servers are sometimes referred to as "poisoned". Pharming requires unprotected access to target a computer.

Lack of knowledge, visual deception and lack of attention are the keys to successful Phishing or Pharming. There are several methods to combat Phishing or Pharming. First is identifying the certificate, which is a public key binding a digital signature with an identity. When a certificate which has not been signed by a trusted certificate authority is met by the browser, a warning is issued to the user. Certificate Authority (CA) is an entity which releases certificates and attests that a public key belongs to a particular identity. Self-signed certificates are created and signed by some organizations such as banks. The browser issues a warning and at the same time allows the user to decide whether or not to accept the self-signed certificate. Second is HTTPS which indicates that the HTTP has been sent over Secure Sockets Layer (SSL) and Transport Layer Security (TLS). If users can't see a HTTPS prefix, then they can judge the web site is fake. And these traditional methods for text password are useful for graphical password.

Phishing or Pharming for graphical passwords is more difficult than for alphanumeric passwords. In an alphanumeric password scheme, attackers need not to know anything about user's password information and the theory of authentication, and the fake website will record user's input information since users will input username and password to login. So the hacker can easily obtain clear text accounts. But for graphical passwords, attackers must know how the graphical authentication works, and different graphical password scheme principles also differ.

For Drawmetric schemes like DAS, hackers have to know what the configuration of canvas is and how many grids in a scheme. What's more, for schemes like BDAS, background picture is additional needed. If the configuration of grid or picture for legal and illegal website is different, the user may doubt the authenticity of the website.

For Locimetric schemes like PassPoints, the hacker must know what the background picture is and whether the background is the same for every user. If the background differs, the work for attacking is more difficult.. The hacker records the coordinates, and analyses the coordinates' location in the picture. For other schemes like Blonder and V-Go, the hacker has to know the possible password region, otherwise the user may find the login is different and suspect the website. There is no doubt these greatly increase the hacker's difficulty, making Phishing or Pharming more difficult.

For one round Cognometric schemes, e.g. Story or Picture Password, hackers can record which picture users select. For multi rounds, such as PassFace and Awase-E, the login process implies the password. For schemes like CHC or Colorlogin, where users don't click the password directly, it is difficult to get passwords by Phishing or Pharming only once. Overall, Phishing and Pharming do not work well in Cognometric schemes.

For Hybrid Schemes, like GrIDsure, where the shape is drawn by users in the registration phase, hackers can get the shape and obtain the password. For Click a Secret, attackers must obtain the configuration of picture, record what users have clicked and then obtain the password. For CDS, users draw a line to authenticate, and the hacker may find possible passwords by recording this line. However, when using this method, attackers can only know parts of password on one login, similar to PassHands. For S3PAS and CBFG, which are similar to CHC, users don't click the password directly, therefore even if an attacker knows what is clicked, he cannot know the correct password. In general, phishing or pharming in graphical passwords is harder than that in alphanumeric passwords.

MITM (man in the middle) can retrieve and relay information from the legitimate site. With a MITM attack, attackers may log in to the legitimate site at least once by hijacking a single correct authentication response during the attack [14].

D. Spyware attack

Spyware [85] is a type of malware (malicious software) installed on computers that collects information about users without their knowledge. The presence spyware, which includes adware, Trojan horse, keystroke-loggers, mouse-loggers and screen-scrapers, is usually installed on a user's personal computer without permission, is typically invisible to the user and difficult to detect. Spyware can select almost any type of data, including personal information, internet surfing habits, user logins, and bank or credit account information, and is often used by attackers to steal information. In the field of password security study, we focus on a type the malware which secretly collects passwords.

1) Keystroke-loggers

Keystroke-loggers [86], which records the user's input using keyboard, is usually used by hackers to capture passwords and infiltrate target networks. It may be hardware, software, a combination of software and hardware, or any other form of keyboard spying. In general, passwords which are fixed and entered via the keyboard are easily attacked by keystroke-loggers. For example, alphanumeric password schemes are especially vulnerable to keystroke-loggers. Most of the graphical password schemes do not use the keyboard to input passwords and easily resist keystroke-loggers. However, they may be having other safety issues e.g. mouse-loggers. Graphical password schemes, which input fixed passwords using the keyboard, like Jimmy, Inkblot and Using CAPTCHA, are vulnerable to keystroke-loggers. But graphical password schemes (such as GrIDsure, Zheng's scheme, Man' scheme) also use the keyboard but input varied contents each login can resist keystroke-loggers.

2) Mouse-loggers

Mouse-loggers record the click position and trajectory of the mouse, and can be used to crack the user's password. The mouse-logger stores the information of each click position and the trajectory of the mouse in the form of coordinates. Mouse-loggers can only crack the schemes which input information by mouse, but are not a threat to keyboard alphanumeric schemes. Mouse-based schemes whose click points or drawing trajectory are fixed for every login, such as most of the Drawmetric schemes and Locimetric schemes, are easy to crack by mouse-loggers. Conversely, if the click points and drawing trajectory are not fixed, these schemes (PassFaces, Déjà vu, etc.), are hard to crack simply using mouse-loggers.

3) Screen-scrapers

Screen-scrapers intercept and capture screen content by taking and saving pictures of the screen. Unlike shoulder-surfing which requires direct external human or machine observation, screen-scrapers record the user's operation information by internally installed software. Screen-scrapers, once installed on a computer, can record all of the user's operating activities and are a more serious threat than shoulder surfing. Most of the graphical passwords can be cracked by using screen-scrapers. However, as it is difficult to install spyware on a user's computer without being noticed, screen-scrapers pose a less serious threat under normal circumstances. Schemes which use shielded input characters, such as Using CAPTCHA, Inkblot and most alphanumeric schemes resist screen-scrapers, Even if screen-scrapers capture the screen content, it cannot know what the "*" mean and therefore these schemes can resist screen-scrapers.

TABLE I.
DRAWMETRIC SCHEMES

Password space (bit)	**Dictionary Attack**	**Shoulder Surfing**	**Intersection Analysis**	**Tricking**	**Phishing or Pharming**
58	N	N	N	Easy	Easy
Unknown	N	N	N	Middle	Easy
Unknown	N	N	N	Easy	Easy
77	N	N	N	Easy	Easy
Unknown	Y	N	N	Middle	Easy
Unknown	Y	Y	Y	Easy	Difficult
48	Y	Y	N	Easy	Middle
58	N	N	N	Easy	Middle
300	N	N	N	Middle	Easy
18	N	N	N	Easy	Easy
Unknown	N	N	N	Easy	Middle
Unknown	Y	Y	N	Middle	Middle
Unknown	N	N	N	Easy	Easy
Unknown	N	N	N	Middle	Middle

TABLE II.
LOCIMETRIC SCHEMES

Schemes	Password space (bit)	Dictionary Attack	Tricking	Phishing or Pharming
Blonder	Unknown	Y	Middle	Middle
V-GO	Unknown	N	Difficult	Middle
PassPoints	43	N	Difficult	Middle
visKey	Unknown	N	Difficult	Middle
Suo's scheme	16/43	Y	Difficult	Middle
CCP	43	N	Difficult	Difficult
PCCP	43	Y	Difficult	Difficult

4) Other spyware

In reality, attackers rarely use only one attack method, and they often combine methods. For example, attackers may combine keystroke-loggers and mouse-loggers. In this way, they can record not only user's keyboard input information but also mouse click content and moving trajectory. In the same way, attackers can obtain both the screen content and the keyboard input information combining keystroke-loggers and screen-scrapers [87,88].

In order to protect user information, joint efforts are required both from users and password scheme designers. From a user's perspective, he should use security antivirus software, develop good surfing habits, not open unidentified web pages, not install suspicious plug-ins, and not use websites requiring sensitive personal information in an insecure environment. From a password scheme designer's perspective, he must make his password scheme more secure and reliable, using methods where: keyboard input or mouse click information not fixed for each login, add real-time SMS (Short Messaging Service) verification if necessary etc.

TABLE III.
COGNOMETRIC SCHEMES

Schemes	Password space (bit)	Dictionary Attack	Shoulder Surfing	Tricking	Phishing or Pharming	Spyware Attack
Déjà vu	16	Y	N	Difficult	Middle	Screen
PassFaces	13	N	N	Difficult	Middle	Screen
Photographic authentication	20	Y	N	Difficult	Middle	Screen
Awase-E	Unknown	Y	N	Difficult	Middle	Screen
Story	12	Y	N	Middle	Middle	Screen
Picture Password	Unknown	Y	N	Difficult	Middle	Screen
VIP	13	Y	Y	Difficult	Middle	Screen
Cognitive Authentication	10/73	Y	Y	Difficult	Difficult	Y
Convex Hull Click	32	Y	Y	Difficult	Difficult	Y
Use Your Illusion	11	Y	N	Difficult	Middle	Screen
Colorlogin	Unknown	Y	Y	Difficult	Difficult	Y
GPI/GPIS	43	Y	N	Difficult	Middle	Screen

VI. SECURITY SUMMARY

Table 1 to 4 summarizes the security of the 46 graphical password schemes we analyzed. ‘Y’ means it is resistant to that form of attack. ‘N’ indicates the scheme is open to attack. In the Tricking, Phishing or Pharming and Spyware Attack column, ‘Easy’ denotes that the Tricking or Phishing is highly effective. ‘Middle’ denotes that difficulty has increased. ‘Difficult’ means the Tricking or Phishing is difficult. In the Spyware Attack column, ‘Screen’ means screen-scrapers is can be used in the scheme, ‘Mouse’ or ‘Keyboard’ indicates it is open to mouse-loggers or keystroke-loggers or combination attacks. ‘Unknown’ means insufficient detail in the literature to complete the evaluation. It is noticed that for all mentioned drawmetric schemes, the screen-scrapers and mouse-loggers can both be used in the spyware attack. So the spyware attack was not listed in the table1. It was also the case in the table2.

For locimetric and cognometric schemes, all the mentioned schemes are open to the intersection analysis attack. And all the locimetric schemes are vulnerable to the shoulder surfing attack. So the intersection analysis was not listed in the table2 and table3, the shoulder surfing was not listed in the table2.

VII. CONCLUSION AND RECOMMENDATION

Since 1996, numerous graphical password schemes have been proposed as alternatives to alphanumeric password schemes. The main argument for graphical password is that it can reduce the burden of human memory, as studies have demonstrated humans tend to remember graphics and images better. The current graphical password schemes can be classified into four categories: Drawmetric schemes, Locimetric schemes, Cognometric schemes and Hybrid schemes. In this paper, we provide a comprehensive security overview of published research of existing graphical password schemes. We classified the existing attack types into two categories: password space based and capture based. For attacks based on password space, we focused on the brute force attacks and dictionary attacks. For capture based attacks, shoulder surfing, intersection analysis, social engineering and spyware attack were discussed in detail.

Preliminary analysis suggested that it is more difficult to break graphical passwords than to break alphanumeric passwords using the traditional attack methods such as brute force attack, dictionary attack and social engineering attack, especially in Drawmetric schemes. Because of the stronger visualization of graphical password schemes, shoulder surfing attack creates a significant threat, especially for the Drawmetric and Locimetric schemes. With the development of spyware, both alphanumeric password schemes and graphical password schemes are facing greater threat, particularly the spywares combine keystroke-loggers, mouse-loggers and so on. It is clear that the combination attack methods are trending up and pose an increasing threat to the graphical password security development. Combination attack methods overcome the limitations of a single method and so increase security threats.

In order to improve the security of graphical password

TABLE IV.
HYBRID SCHEMES

Schemes	Password space (bit)	Dictionary Attack	Shoulder Surfing	Intersection Analysis	Tricking	Phishing or Pharming	Spyware Attack
Jiminy	9	Y	N	N	Difficult	Middle	Screen
Using CAPTCHA	Unknown	Y	Y	Y	Difficult	Difficult	Y
GrIDsure	18	N	Y	N	Easy	Middle	Y
Zheng’s scheme	Unknown	N	Y	N	Easy	Middle	Y
Man’s scheme	Unknown	Y	Y	N	Difficult	Difficult	Y
Pass-Object	Unknown	Y	Y	N	Difficult	Difficult	Y
Inkblot	94	Y	N	N	Easy	Easy	Keyboard
S3PAS	Unknown	N	Y	N	Easy	Difficult	Y
Click-a-secret	Unknown	Y	N	N	Difficult	Difficult	Screen
CDS	Unknown	Y	Y	N	Middle	Middle	Y
PassHands	Unknown	Y	Y	N	Difficult	Difficult	Y
CBFG	Unknown	Y	Y	Y	Difficult	Difficult	Y

scheme, joint efforts are required both from users and password scheme designers. From a password scheme designer's perspective, he must make his password scheme more secure and reliable, using methods where:

- Focus on increasing password entropy without sacrificing usability and memorability.
- Minimize the pattern in the scheme.
- Keyboard input or mouse click information not fixed for each login.
- Add real-time SMS (Short Messaging Service) verification if necessary.

From a user's perspective, he should make his password more secure by:

- Avoid pattern and esay password when set a password.
- Use security antivirus software.
- Not open unidentified web pages.
- Nnot install suspicious plug-ins.
- Not use websites requiring sensitive personal information in an insecure environment.

For graphical password schemes, security and usability represent opposite ends of a spectrum: increasing security implies decreasing usability and vice versa. Therefore, a tradeoff is required based on user requirements. To meet user requirements we should contacts the two aspects with the special target environment when a new scheme is proposed or for selecting the appropriate scheme. For portable devices, such as mobile phones, which generally do not contain confidential information, we may pay more attention to usability as pect. However, for some systems which require high security levels, it is appropriate to sacrifice some usability to ensure the absolute security.

Overall, for graphical passwords to advance as a serious authentication alternative, more research must be conducted and presented. In this paper, we systematically analyze the security of existing graphical password schemes, and provided a reference for future research and designing of graphical password.

References

[1] K. Renaud. "Evaluating authentication mechanisms". In L. Cranor and S. Garnkel, editors, *Security and Usability: Designing Secure Systems That People Can Use*, chapter 6, pp.103-128. O'Reilly Media, 2005.

[2] 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.

[3] D. Feldmeier and P. Karn. "UNIX Password Security-Ten Years Later". *In Crypto'89*, August 1989.

[4] R. Morris and K. Thompson. "Password Security: A Case History". *Communications of the ACM*, 22(11):594-597, 1979.

[5] D. Florencio and C. Herley. "A large-scale study of WWW password habits". *In 16th ACM International World Wide Web Conference (WWW)*, May 2007.

[6] A. Adams, M. A. Sasse, and P. Lunt. "Making passwords secure and usable". *In HCI 97: Proceedings of HCI on People and Computers*, pp.1-19, London, UK, 1997. Springer-Verlag.

[7] G. Blonder. "Graphical passwords". *United States Patent*, 5,559,961, 1996.

[8] B. Kirkpatrick. "An experimental study of memory". *Psychological Review*, 1:602-609, 1894

[9] S. Madigan. "Picture memory". In J. Yuille, editor, *Imagery, Memory, and Cognition: Essays in Honor of Allan Paivio*, chapter 3, pp.65-89. Lawrence Erlbaum Associates, 1983.

[10] A. Paivio, T. Rogers, and P. C. Smythe. "Why are pictures easier to recall than words?", *Psychonomic Science*, 11(4):137-138, 1968.

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

[12] A. Paivio. "Mind and Its Evolution", *A Dual Coding Theoretical Approach*. Lawrence Erlbaum: Mahwah, N.J., 2006.

[13] X. Suo, Y. Zhu, and G. Owen. "Graphical passwords: A survey". *In Annual Computer Security Applications Conference (ACSAC)*, December 2005.

[14] R. Biddle, S. Chiasson, and P.C. van Oorschot. "Graphical passwords: Learning from the First Twelve Years". *ACM Computing Surveys*, 44(4), Article 19:1-41.

[15] X.Y. Liu., J.H. Qiu., L.C. Ma., H.C. Gao., etc., "A Novel Cued-recall Graphical Password Scheme", *In sixth International Conference on Image and Graphics (ICIG)*, pp.949-956, 2011.

[16] H.C. Gao., Z.J. Ren., X.L. Chang., X.Y. Liu., etc., "A New Graphical Password Scheme Resistant to Shoulder-Surfing", *International Conference on Cyberworlds (CW)*, pp.194-199, December 2010.

[17] D. Nali and J. Thorpe. "Analyzing user choice in graphical passwords". *Technical Report TR-04-01, School of Computer Science*, Carleton University, May 2004.

[18] H. Tao. "Pass-Go, a new graphical password scheme". *Master's thesis, School of Information Technology and Engineering*, University of Ottawa, June 2006.

[19] H. Tao and C. Adams. "Pass-Go: A proposal to improve the usability of graphical passwords". *International Journal of Network Security*,7(2):273-292, 2008.

[20] J. Thorpe. "On the Predictability and Security of User Choice in Passwords". *PhD thesis, School of Computer Science*, Carleton University, January 2008.

[21] P. C. van Oorschot and J. Thorpe. "On predictive models and user-drawn graphical passwords". *ACM Transactions on Information and System Security*, 10 (4):1-33, 2008.

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

[23] P. C. van Oorschot, A. Salehi-Abari and J. Thorpe. "Purely Automated Attacks on PassPoints-Style Graphical Passwords". *IEEE Transactions on Information Forensics and Security*, 5(3): pp.393-405, 2010.

[24] S. Wiedenbeck, J. Waters, L. Sobrado, and J. Birget. "Design and evaluation of a shoulder-surfing resistant graphical password scheme". *In International Working Conference on Advanced Visual Interfaces (AVI)*, May 2006.

[25] I. Jermyn, A. Mayer, F. Monrose, M. Reiter, and A. Rubin, "The design and analysis of graphical passwords". *In 8th USENIX Security Symposium*, August 1999.

[26] J. Thorpe and P. C. van Oorschot, "Graphical dictionaries and the memorable space of graphical passwords". *In 13th*

USENIX Security Symposium, August 2004.

[27] J. Thorpe and P. C. van. Oorschot, "Towards Secure Design Choices for Implementing Graphical Passwords", *in Proceedings of the 20th Annual Computer Security Applications Conference*. Tucson, Arizona, 2004.

[28] K. Chalkias, A. Alexiadis and G. Stephanides, "A multi-grid graphical password scheme". *In Proc. the 6th International Conference on Artificial Intelligence and Digital Communications*, Thessaloniki, Greece, Aug. 18-20, 2006, pp.80-90.

[29] Paul D. and Yan J., "Do background images improve Draw a secret graphical passwords?", *In Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS)*, 2007, 36-47.

[30] L. Y. Por, X. T. Lim, M. T. Su, and F. Kianoush. "The design and implementation of background Pass-Go scheme towards security threats". *WSEAS Transactions on Information Science and Applications*, 5(6):943-952, June 2008.

[31] L. Y. Por and X. T. Lim, "Multi-Grid background Pass-Go". *WSEAS Transactions on Information Science and Applications*, Issue 7, Volume 5, July 2008.

[32] H. Gao, X. Guo, X. Chen, L. Wang, and X. Liu, "YAGP: Yet another graphical password strategy". *In Annual Computer Security Applications Conference*, 2008, 121-129.

[33] X. Liu, H. Gao, L. Wang and X. Chang, "An Enhanced Drawing Reproduction Graphical Password Strategy". *Journal of Computer Science and Technology*, 26(6): 988-999. 2011.

[34] C. Varenhorst, Passdoodles: "A lightweight authentication method". *MIT Research Science Institute,* July 2004.

[35] R. Weiss and A. De Luca, "PassShapes - utilizing stroke based authentication to increase password memorability". *In NordiCHI*, pp.383-392. ACM, October 2008.

[36] M. Orozco, B. Malek, M. Eid, and A. El Saddik, "Haptic-based sensible graphical password". *In Proceedings of Virtual Concept*, 2006.

[37] D. Lin, P. Dunphy, P. Olivier, and J. Yan, "Graphical passwords & qualitative spatial relations", *in Proceedings of the 3rd Symposium on Usable Privacy and Security*, vol. 229. ACM, New York, NY, 2007, 161-162.

[38] "Android", http://beust.com/weblog/archives/ 000497.html, site accessed in Dec, 2012

[39] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M. Smith, "Smudge attacks on smartphone touch screens". *In USENIX 4th Workshop on Offensive Technologies*, 2010.

[40] "Signing in with a picture password" , in Building Windows 8 in the MSDN Blogs, http://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-with-a-picture-password.aspx, last accessed in Oct 2012.

[41] Higbee, K.L.: "Your Memory: How it Works and How to Improve it", *2nd edn. Prentice Hall Press,* New York (1988).

[42] "Passlogix", http://www.passlogix.com, last accessed in Oct 2012.

[43] X. Suo. "A design and analysis of graphical password". *Master's thesis, College of Arts and Science*, Georgia State University, August 2006.

[44] "Sfr", www.sfr-software.de/cms/EN/pocketpc/viskey/ index.html, site accessed in Oct, 2012.

[45] S. Chiasson, P.C. van Oorschot, and R. Biddle. "Graphical password authentication using Cued Click Points". *In European Symposium On Research In Computer Security (ESORICS),* LNCS 4734, September 2007, pp. 359-374.

[46] S. Chiasson, A. Forget, R. Biddle, and P. C. van Oorschot. "Influencing users towards better passwords: Persuasive Cued Click-Points". *In Human Computer Interaction (HCI),* The British Computer Society, September 2008.

[47] Chiasson, S., Stobert, E., Forget, A., Biddle, R., van Oorschot, P.C.: "Persuasive Cued Click-Points: Design, implementation, and evaluation of a knowledge-based authentication mechanism". *IEEE Transactions on Dependable and Secure Computing (TDSC)*,2012

[48] Dhamija R. and Perrig A., "Déjà vu: A User Study Using Images for Authentication", *in Proceedings of 9th USENIX Security Symposium*, 2000

[49] Sacha Brostoff, M. Angela Sasse, "Are Passfaces More Usable Than Passwords?:, *A Field Trial Investigation*, 2000

[50] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes", *in Proceedings of the 13th Usenix Security Symposium*. San Diego, CA, 2004.

[51] T. Pering, M. Sundar, J. Light, and R. Want., "Photographic authentication through untrusted terminals", *Pervasive Computing*, pp.30-36, 2003.

[52] T. Takada and H. Koike, "Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images", *in Human-Computer Interaction with Mobile Devices and Services*, vol. 2795: Springer-Verlag GmbH, 2003, pp. 347 - 351.

[53] Davis D., Monrose F., and Reiter M. K., "On user choice in graphical password schemes". *In Proceedings of the 13th Usenix Security Symposium*. San Diego, CA, 2004

[54] Jansen W., "Authenticating Mobile Device Users Through Image Selection". *First International Conference on the Internet Society*, May 2004

[55] A. De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems", *International Journal of Human-Computer Studies*, 63(1-2):128-152, 2005.

[56] Weinshall D., "Cognitive Authentication Schemes Safe Against Spyware". *In IEEE Symposium on Security and Privacy (S&P)*, 2006

[57] E. Hayashi, N. Christin, R. Dhamija, and A. Perrig., "Use Your Illusion: Secure authentication usable anywhere", *In 4th ACM Symposium on Usable Privacy and Security (SOUPS)*, Pittsburgh, July 2008.

[58] H.C. Gao, X.Y. Liu, R.Y. Dai, etc., "Analysis and Evaluation of the ColorLogin Graphical Password Scheme". *The 5th International Conference on Image and Graphics*, Sep. 20-23, 2009.

[59] K. Bicakci, N. B. Atalay, M. Yuceel, H. Gurbaslar, and B. Erdeniz, "Towards usable solutions to graphical password hotspot problem", *In 33rd Annual IEEE International Computer Software and Applications Conference*, 2009.

[60] K. Renaud and E. Smith. Jiminy: "Helping user to remember their passwords". *Technical report, School of Computing, Univ. of South Africa*, 2001.

[61] H.C.Gao, X.Y.Liu, S.D.Wang, R.Y.Dai. "A new graphical password scheme against spyware by using CAPTCHA". *In: Proceedings of the symposium on usable privacy and security,* 15-17 July, 2009.

[62] L.M.Wang, X.L.Chang, Z.J.Ren, etc.: "Against spyware Using CAPTCHA in graphical password scheme". *In: 24th IEEE International Conference on Advanced Information Networking and Applications*, pp. 760-767 (2010).

[63] Brostoff, S., Inglesant, P., &Sasse, A. M. "Evaluating the usability and security of a graphical one-time PIN system". *24th BCS Conference on Human Computer Interaction*.

pp.1-8. Dundee, Scotland. ACM Press: NY.

[64] Z. Zheng, X. Liu, L. Yin, Z. Liu "A Hybrid password authentication scheme based on shape and text", *Journal of Computers*, vol.5, no.5, 2010.

[65] S. Man, D. Hong, and M. Mathews, "A shoulder surfing resistant graphical password scheme", *in Proceedings of International conference on security and management*. Las Vergas, NV, 2003.

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

[67] A. Stubblefield, D. Simon. "Inkblot Authentication", *MSR-TR-2004-85. Technical report,* Microsoft Research, 2004.

[68] H. Zhao and X. Li, "S3PAS: A Scalable Shoulder-Surfing Resistant Textual-Graphical Password Authentication Scheme", *in 21st International Conference on Advanced Information Networking and Applications Workshops*, vol. 2. Canada, 2007, pp. 467-472.

[69] Eluard, M.; Maetz, Y.; Alessio, D.; , "Action-based graphical password: Click-a-Secret", *2011 IEEE International Conference on Consumer Electronics*, 2011, pp.265-266.

[70] H.C.Gao, L.C.Ma, J.H.Qiu and X.Y.Liu, "Exploration of a Hand-based Graphical Password Scheme", *Proceedings of the 4th international conference on Security of information and networks*, 2011.

[71] "Brute force attack", http://en.wikipedia.org/wiki/Brute_force_attack, last accessed in Oct 2012.

[72] "Dictionary attack", http://en.wikipedia.org/wiki/Dictionary_attack, last accessed in Oct 2012.

[73] B. Pinkas and T. Sander. "Securing passwords against dictionary attacks". *In 9th ACM Conference on Computer and Communications Security*, 2002.

[74] D. Nali and J. Thorpe. "Analyzing user choice in graphical passwords". *Technical Report TR-04-01, School of Computer Science*, Carleton University, 2004.

[75] A. Dirik, N. Menon, and J. Birget. "Modeling user choice in the Passpoints graphical password scheme". *In 3rd ACM Symposium on Usable Privacy and Security*, July 2007.

[76] P. C. van Oorschot, A. Salehi-Abari, and J. Thorpe. "Purely automated attacks on PassPoints-style graphical passwords". *IEEE Trans. Info. Forensics and Security*, 5(3):393-405, 2010.

[77] S. Chiasson, A. Forget, E. Stobert, P. C. van Orschot, and R. Biddle. "Multiple password interference in text and click-based graphical passwords". *In ACM Computer and Communications Security*, 2009.

[78] D. Davis, F. Monrose, and M. Reiter. "On user choice in graphical password schemes". *In 13th USENIX Security Symposium*, 2004.

[79] V. Roth, K. Richter, and R. Freidinger: "A PIN-entry method resiliant against shoulder surfing". *the 11th ACM Conference on Computer and Communications Security*, 2004.

[80] F. Tari, A. Ozok, and S. Holden: "A comparison of perceived and real shoulder-surfing risks between alphanumeric and graphical passwords". *In: Proceedings of the 2nd ACM Symposium on Usable Privacy and Security*, 2006.

[81] G. Orgill, G. W. Romney and P. M. Orgill: "The Urgency for Effective User Privacy Education to Counter Social Engineering Attacks on Secure Computer Systems". *In: Proceedings of the 5th Conference on Information Technology Education*. pp. 177-181,2004.

[82] B. Schneier: "Secrets and Lies". *John Wiley and Sons,* 2000

[83] "Phishing", http://en.wikipedia.org/wiki/Phishing, last accessed in Oct 2012.

[84] "Pharming", http://en.wikipedia.org/wiki/Pharming, last accessed in Oct 2012.

[85] "Spyware", http://en.wikipedia.org/wiki/spyware, last accessed in Oct 2012.

[86] B. Ross, C. Jackson, N. Miyake, D. Boneh, and J. Mitchell. "Stronger password authentication using browser extensions". *In 14th USENIX Security Symposium*, Baltimore, August 2005.

[87] R Padmavathy, Chakravarthy Bhagvati. "A Small Subgroup Attack for Recovering Ephemeral Keys in Chang and Chang Password Key Exchange Protocol". *Journal of Computers*, vol.6, no.4, 2011.

[88] Zuowen Tan. "An Authentication and Key Agreement Scheme with Key Confirmation and Privacy-preservation for Multi-server Environments", *Journal of Computers*, vol.6, no.11, 2011.

Haichang Gao is an associate professor in Xidian University and a member of the IEEE and CCF. He has published more than twenty papers. Now he is in charge of the project of the National Natural Science Foundation of China and the Fundamental Research Funds for the Central Universities. His current research interests include graphical password and intelligent computing.

Wei Jia, Fei Ye, and Licheng Ma are master candidates in computer science at Xidian University. Their current research interests are graphical password.