USER AUTHENTICATION SCHEMES FOR MOBILE AND HANDHELD DEVICES

M. N. DOJA[1]
NAVEEN KUMAR[2]

Department of Computer Engineering
Jamia Millia Islamia - New Delhi
P.O. Box 110025 - India
[1]ndoja@yahoo.com [2]naveenkumar@rediffmail.com

Abstract. User authentication is a difficulty for every system providing safe access to precious, private information, or personalized services. It is a continual problem, particularly with mobile and handheld devices such as Personal Digital Assistants (PDAs). User authentication is the primary line of defence for a handheld device that comes into the hands of an unauthorized individual. Password or Personal Identification Number (PIN) based authentication is the leading mechanism for verifying the identity of actual device users but this method has been shown to have considerable drawbacks. For example, users tend to pick PIN or passwords that can be easily guessed. On the other hand, if a password is hard to guess, then it is often hard to remember. To address this problem in handheld devices, some researchers have developed comparatively more secure, affordable and memorable authentication schemes based on graphical assistance, images and audio. In this paper, we conduct a comprehensive survey and analysis of such existing user authentication schemes for mobile and handheld devices. The complete analysis of these schemes in term of usability and security are also discussed in this paper. This paper will be useful for information security researchers and practitioners who are interested in finding an alternative to password based authentication schemes.

Keywords: User Authentication, Mobile Security, Handheld Devices, Usability and Computer Security

(Received February 08, 2007 / Accepted December 08, 2007)

1 Introduction

All security access methods are based on three fundamental pieces of information: who you are, what you have, and what you know [3], which also corresponds to biometric authentication, token-based authentication and knowledge-based authentication respectively. For proving who they are, users can provide their name, email address, or a user ID. Since this information provides no assurance of identity, some users are beginning to use biometrics as methods of user identification. For proving what they have, users can produce service cards (i.e., ATM cards), physical keys, digital certificates, smart cards, or one-time login cards such as the Secure ID card [8]. For proving what they know, users can provide a password or pass phrase, or a personal identification number (PIN). This information is essentially a secret that is shared between the user and the system. Password authentication is the foremost mechanism for verifying the identity of computer users, even though it is well known that people frequently choose passwords that are vulnerable to dictionary attacks. The motivation for addressing the security and shortcomings of traditional password-based authentication is that users tend to choose passwords that are easy to remember, which in the case of textual passwords usually implies that they are easy to obtain by searching through a carefully formed dictionary" of candidate passwords. For example, in one case study of over 14,000 UNIX passwords, almost 25 percent of the passwords were found by searching for words in a dictionary [5]. The security and usability problem associated with alphanumeric passwords is referred as The password problem[27]. The problem arises because passwords are expected to comply with two fundamentally conflicting requirements:

- Passwords should be easy to remember, and the user authentication protocol should be executable quickly and easily by humans.

- Passwords should be secure, i.e., they should look random and should be hard to guess; they should be changed frequently, and should be different on different accounts of the same user; they should not be written down or stored in plain text.

Fulfilling these requirements is virtually impossible for users. As a result, users ignore the requirements, leading to poor password practices. This problem has led to innovations to improve passwords. Different scheme those are more secure than traditional approaches are being developed for improving the security of user authentication process. Biometric authentication, such as fingerprints, voice recognition, iris scans, and facial recognition are not yet widely adopted. The major drawback of this approach is that such systems can be expensive, and the identification process can be slow and often unreliable. However, this type of technique provides the highest level of security. High cost of hardware, processing and memory requirements are the major arguments to circumvent these technologies in mobile and handheld devices at present. We have studied and analyzed the cost effective user authentication schemes those are mainly based on what you know like alphanumeric password with graphical assistance, visual key, draw-a-secret, passfaces, passclick and audio authentication, these schemes are especially relevant to mobile and handheld devices that interact via a touch screen, keyboard, voice recorder and stylus.

2 Background

The recent development in mobile computing has encouraged the acquisition of handheld devices such as Personal Digital Assistants (PDAs). The use of mobile and handheld devices within the place of work is growing rapidly. Most handheld devices can be configured to send and receive electronic mail and browse the Internet. These devices are no longer viewed as stylish gadgets for early technology adopters, but have become as an alternative tools that offer competitive business advantages for the mobile workforce [9]. Handheld devices are characterized by small size, limited computing capability and small battery life, and the way for exchanging data with a more capable laptop or desktop computer. They also support interfaces oriented in the direction of mobility, for example, a touch screen and a microphone in place of a keyboard. One or more wireless interfaces, such as infrared (e.g., IrDA) or radio (e.g., GSM/GPRS, Bluetooth, WiFi), are usually integral for both local and wide area interactions. They offer efficiency tools in a compressed form and at fairly low cost, and are rapidly becoming omnipresent in today's business surroundings. These devices provides lots of advantages, however, they also generate new risks to an organizations security, not only from the private information held and the organizational networks reachable by them, but also from their propensity to become physically separated from the user and reach to intruder. Enabling user authentication is the first row of defence in opposition to unauthorized utilization of a mobile and handheld device.

Password systems are easy to implement on most devices however it is not very effective, users tend to undermine them by using straightforwardly remembered character strings as their password (e.g., User often choose his/her name), which an intruder may easily guess or systematically match against dictionaries of such commonly used strings [22],[5]. To battle weak passwords, organizations apply procedures that force users to include special, uppercase, and numerical characters in their password string, to change passwords regularly (e.g., every 60 days) with completely different strings, and to avoid common or easily guessed strings [7]. Unfortunately, the procedures put in place to guarantee strong passwords generally result in complex and meaningless passwords that users often need to record to recall promptly.

3 User Authentication Schemes

Security of user authentication associated issues come into view over the use of mobile and handheld devices; handheld devices progressively build up sensitive information and over time gain access to wireless services and organizational intranets. Because of their small size, handheld devices may be misplaced, lost, or stolen, and thus out in the open to an unauthorized individual. If user authentication is not enabled, a general default, the devices contents and network services fall under the control of whoever holds it. Even if user authentication is enabled, the authentication mechanism may be weak (e.g., a four number PIN) or easily guessed

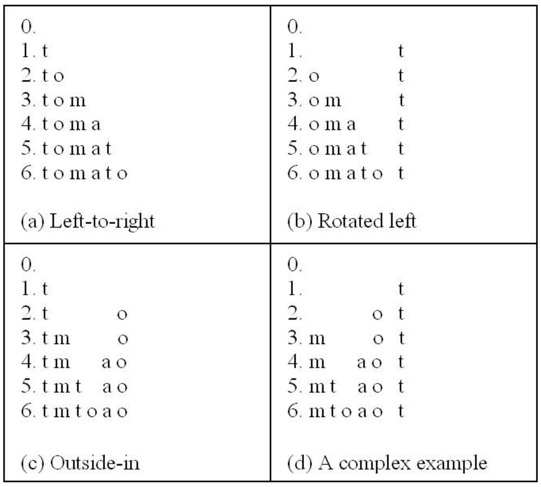
[11]. Typing passwords are difficult especially those that are long and complex, and the users are limited to one handed typing. Shoulder surfing attack is also a bigger problem with these devices because someone can gain access with ease. User Authentication schemes for mobile and handheld devices can be divided into two broad classes: software-based and hardware-assisted. Software-based authentication schemes work in combination with the integral hardware on the device and need no extra hardware components. They completely rely on additional software to be installed on the device. In comparison, hardware-assisted authentication schemes use at least one extra hardware module connected to the device, along with software that captures and processes input from that peripheral and controls the authentication process. Since the additional hardware required, hardware-assisted authentication solutions normally cost considerably more than software-based solutions. The remainder of the paper discusses the details of various authentication schemes that have been designed or could be modified for mobile and handheld devices, grouped into the three main classes graphical based, image based and audio based authentication.

4 Graphical-based Authentication

Many of the deficiencies of password authentication systems arise from the limitations of human memory. If humans were not required to remember the password, a maximally secure password would be one with maximum entropy: it would consist of a string as long as the system allows, consisting of characters selected from all those allowed by the system. Some passwords are very easy to remember, but also very easy to guess with dictionary searches. In contrast, some passwords are very secure against guessing but difficult to remember. We have selected three schemes in this category Password with Graphical Assistance, Draw-A-Secret and 3D Graphical Password.

4.1 Password with Graphical Assistance

Password with Graphical Assistance scheme demonstrate the power of graphical input abilities while yielding a scheme that is convincingly stronger than textual passwords [14]. Suppose that the user is presented with a simple graphical input display consisting of, say, eight positions into which to enter a textual password, as illustrated in Figure 1(a). In this figure, step 0 is the initial row of blanks, and steps 1-6 indicate the temporal order in which the user fills in the blanks. The password can be placed in the normal", left-to-right positions as shown in Figure 1(a). Due to the graphical nature of the input interface, however, the user could enter the password in other positions, as well. For example, Figure 1(b) shows a modification in which the user enters the password in a left-to-right manner, but starting from a different initial position than the leftmost. Figure 1(c) shows entering the password in an outside-in" strategy. And, of course, these variations can be combined in the obvious way, as shown in Figure 1(d). In this scheme, each k-character conventional password yields, m!/(m-k)! graphical passwords, where k is the password length and m is the given password positions and indeed this is the factor by which the size of the graphical password space exceeds the k-character conventional password space.



0. 1. t 2. t o 3. t o m 4. t o m a 5. t o m a t 6. t o m a t o (a) Left-to-right	0. 1. t 2. o t 3. o m t 4. o m a t 5. o m a t t 6. o m a t o t (b) Rotated left
0. 1. t 2. t o 3. t m o 4. t m a o 5. t m t a o 6. t m t o a o (c) Outside-in	0. 1. t 2. o t 3. m o t 4. m a o t 5. m t a o t 6. m t o a o t (d) A complex example

Figure 1: Alphanumeric with Graphical Assistance

4.2 Draw-A-Secret

In this draw a secret (DAS) the password is a simple picture drawn on a grid [10]. This approach is alphabet independent, thus making it easily accessible for users know any language like Hindi, Chinese, etc. Users are freed from having to remember any kind of alphanumeric string. Consider an interface consisting of a rectangular grid of size G X G. Each cell in this grid is denoted by discrete rectangular coordinates (x; y), which is subset of [1; :: :;G] X [1; : : :;G]. Suppose that the user is given a stylus with which s/he can draw a design on this grid.

The drawing is mapped to a sequence of coordinate pairs by listing the cells in the order, which the stylus passes through them; with a distinguished coordinate pair inserted in the sequence whenever the stylus is

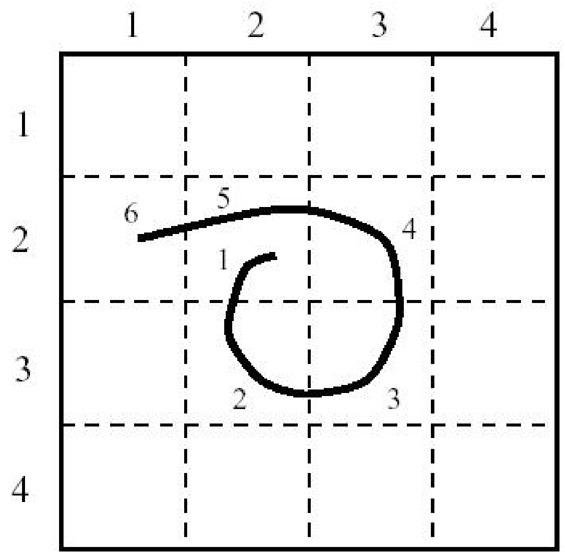


Figure 2: DAS password on a 4 X 4 grid

lifted from the drawing surface. For example, consider the drawing in Figure 2. Here, the coordinate sequence generated by this drawing is (2; 2); (3; 2); (3; 3); (2; 3); (2; 2); (2; 1); (5; 5). Where (5; 5) is the distinguished pen up indicator. If there were a second stroke in this example, then its sequence would be appended to the end of the sequence above, and similarly for subsequent strokes. In this way, we divide the space of possible drawings into equivalence classes, two drawings being equivalent if they have the same encoding, or in other words if they cross the same sequence of grid cells, with the breaks between strokes occurring in the same places.

4.3 3D-Graphical Password

It is a recall-based graphical scheme similar to the DAS scheme [24]. As a special feature in this, the user is also permitted to rotate the drawing canvas (grid). The rotation is performed on the z-axis, which gives an noticeable clockwise or counter-clockwise motion using either mouse or stylus. The grid is displayed in the window and the user may draw directly on it. The slider may be dragged up or down to adjust the existing rotation angle of the grid. In contrast, the DAS scheme, a stroke can be modeled as an event separated two pen-up events. In this scheme, rotation is an optional event, which occurs between the pen-up event and the stroke event. Any consecutive rotations in the same direction are aggregated as single rotation. Suppose the user rotates the canvas at an angle of, say in the clockwise direction and then for an angle of 90 in the same direction. This is equivalent to (has the same encoding as) a single rotation of 135 in the clockwise direction. However, if the user switches direction, the consecutive rotations are modeled as two distinct events. Hence, rotating the canvas, say in the clockwise direction for 45 and then rotating equivalent to not rotating at all. Such equi-angular bi-directional rotations will be encoded differently and will generate a different password than drawing strokes without rotating at all. This scheme increase the password space to very large extent and hence promise to provides extended security.

5 Image based Authentication

Studies in the past have shown that images are more readily recalled than words, according to Paivio, Rogers and Smythe [16]. Alphanumeric passwords are harder to remember, especially if they are changed every few months. Instead of letters and numbers for passwords, images can be selected as password in Image-based authentication schemes, these schemes suits to handheld devices those have special security needs. These include easy entry passwords, resilience to strangers observing password entry, and the prevention of writing down passwords. Image-based authentication is an emerging technology that may offer a feasible solution to the password problem. Mainly we have studied Passface, Déjà vu, Passclicks, Passlogix, Passpoints, VisualKey and PointSec, these schemes are further explained in the following section.

5.1 Passface

Passface is a technique developed by Real User Corporation [20]. The basic idea is as follows. The user will be asked to choose four images of human faces from a face database as their future password. In the authentication stage, the user sees a grid of nine faces, consisting of one face previously chosen by the user and eight decoy faces. The user recognizes and clicks anywhere on the known face. This procedure is repeated for several rounds. The user is authenticated if he/she correctly identifies the four faces. The technique is based on the assumption that people can recall human faces easier than other pictures. However the effectiveness of this method is still uncertain. Davis, et al. [6] studied the graphical passwords created using the Passface technique and found obvious patterns among these passwords. For example, most users tend to choose faces of people from the same race. This makes the Passface password somewhat predictable. This problem may be alleviated by arbitrarily assigning faces to users, but doing so would make it hard for people to remember the password. Another similar schemes Déjà vu [19], also works through recognizing several images in repeated rounds of selection (five rounds in this case), but uses abstract images and photographs rather than faces. The results of a small study of Déjà vu suggest that choosing the images that will make up the password takes longer than choosing PINs and alphanumeric passwords, but the images are easier to remember over time. To obtain security similar to that of an eight-character alphanumeric password (over an alphabet of 64 characters), 15 or 16 rounds with nine images each would be required. This would make the login slow and tedious, and most likely, the login would also be perceived by the user as slow and tedious.

5.2 Passclick

Blonder [2] designed a graphical password scheme in which a password is created by having the user click on several locations on an image. During authentication, the user must click on the approximate areas of those locations. The image can assist users to recall their passwords and therefore this method is considered more convenient than unassisted recall (as with a text-based password). The PassPoint system by Wiedenbeck, et al. [26],[28]extended Blonders idea by eliminating the predefined boundaries and allowing arbitrary images to be used. As a result, a user can click on any place on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. In order to be authenticating, the user must click within the tolerance of their chosen pixels and also in the correct sequence. This technique is based on the discretization method proposed by Birget, et al. [1].

5.3 Passlogix

Passlogix [17]has developed a graphical based authentication scheme, in their implementation; users must click on various items in the image in the correct sequence in order to be authenticated. Invisible boundaries are defined for each item in order to detect whether an item is clicked by mouse. Visual Key [25] is a similar scheme that uses cells of a single graphical image as the password elements. A user selects a specific sequence of image areas (e.g., objects in the image) from the display to authenticate. A selection grid, kept hidden from the user, logically divides a single image into individual cells. The strength of the password depends on the effective size of the password alphabet, which directly corresponds to the number of cells that make up the image. This yields a smaller size alphabet than that available with alphanumeric passwords. Another limitation is that, because the cell boundaries are invisible, no visual cues exist to help determine areas of the image to select, if a selected object in the image encompasses more than one cell.

5.4 PointSec

PointSec for Pocket PC [18]is a commercial product that includes several authentication-related components that can be managed centrally. PicturePIN is a graphical counterpart to a numeric PIN system, which uses pictograms rather than numbers for entering a code via a keypad, because any picture can be used and because a picture may contain hundreds to thousands of memorable points, the possible password space is quite large. Wiedenbeck, et al. conducted a user study [1], in which one group of participants were asked to use alphanumerical password, while the other group was asked to use the graphical password. The result showed that graphical password took fewer attempts for the user than alphanumerical passwords. However, graphical password users had more difficulties learning the password, and took more time to input their passwords than the alphanumerical users.

6 Audio-based Authentication

Audio signal are one of the most useful and effective features for user authentication in mobile environments. Human ability to recall and recognize the audio signal is much higher than remembering words, hence different user authentication schemes are being developed using audio and voice signal. The voice signal conveys many levels of information to the listener. At the primary level, speech conveys a message via words, but at other levels speech conveys information about the language being spoken and the emotion, gender, and, generally, the identity of the speaker. While speech recognition aims at recognizing the words spoken in speech, the goal of automatic speaker recognition systems is to extract, characterize, and recognize the information in the speech signal conveying speaker identity. In this section brief overview of audio authentication schemes like Voice authentication system, Voice Verification, Audio and Image Authentication and Audio-Visual Person Authentication using Speech and Ear Images are given.

6.1 Voice Authentication System

Voice authentication system is a cognitive recall mechanism for password verification [4]. A user is enrolled for password verification by receiving a first voice input from the user representing the password prompt and a second voice input representing a correct response to the password prompt. The first and second voice inputs may be stored as waveforms, as voice prints, recognized speech data, or a combination thereof. During verification, the identity of the user is verified by outputting the user-provided password prompt and evaluating a response to password prompt against the correct response. Thus, the user is able to select his/her own password prompt to facilitate cognitive recall of the password during a subsequent verification phase.

6.2 Voice Verification

Voice Verification present a user with a series of randomized phrases to repeat so the system can verify not only the voice matches but also the required phrases match [21]. Voice verification, also know as speaker recognition, determines the identity of the speaker. Enrollment requires an individual to say a set of specific words, typically a numeric value, in succession and usually repeated several times. A template is extracted from this input using an acoustic model, which defines the characteristic of the voice [15]. Once enrolled, authenticating to the system is done by prompting the individual to speak into a microphone and vocalize a randomly drawn set of digits, as they appear in the display. While many handheld devices incorporate a built-in sound card and microphone, they typically lack the processing power (i.e., floating point hardware) to perform the needed calculations quickly enough. The main reason for this is that voice-modeling algorithms rely heavily on floating point arithmetic, whose execution must be emulated in software.

Other drawbacks to this type of solution include environmental sounds, individual speaker variability in pronunciation (e.g., for the number 12, saying one-two versus twelve), the significant amount of time needed for enrollment compared to other biometric mechanisms, and the larger size templates that are needed. On the other hand, speech is a behavioral signal that may not be consistently reproduced by a speaker and can be affected by a speakers health (cold or laryngitis). Also, the varied microphones and channels that people use can cause difficulties since most speaker verification systems rely on low-level spectrum features susceptible to transducer/channel effects. Furthermore, the mobility of system likes uncontrolled and harsh acoustic environments (cars, crowded airports), which can stress the accuracy.

6.3 Audio and Image Authentication

Audio-Visual Associative Protocol (AVAP), an authentication scheme relying on the previously proven efficacy of pictorial passwords and on the benefits of non-speech audio, thus exploiting previously untapped human associative-memory strengths [13]. In considering how both audio and visual/image information can be used to authenticate a user, it was assumed that an individual would make a visual association when a particular piece of music is heard. Since such associations would theoretically be based on each individuals personal life experience, it was hoped that such associations would vary sufficiently to authenticate users uniquely. To expedite this scheme, a number of these associations would be recorded for an individual at enrollment. Subsequent authentication is achieved by having the user recall the same associations. The beauty of this scheme is that it is harder for the user to record their password, thus it increases the security of the scheme. Grouping semantic images together would increase security by reducing the predictability of an association. No attention was paid to the order in which users calibrated their associations when prompting recall.

6.4 Audio Visual Person Authentication Using Speech and Ear Images

This scheme proposes a biometric user authentication method using speech and ear images to attempt to improve the performance in mobile environments [12]. It is well known that the performance of person authentication using only speech is deteriorated by acoustic noises and feature changes with time. Since the ear shape of each person does not change over time, integrating its image with speech information increases robustness of person authentication. Experiments are conducted using audio-visual database collected from 38 male speakers at five sessions over a half year period. Speech data are contaminated with white noise at various Sound-to-Noise-Ration (SNR) conditions. Experimental results show that the authentication performance is improved by combining the ear image with speech in every SNR condition [12].

7 Security and Usability Analysis

An authentication system includes all of the hardware, software, and associated infrastructure needed to perform the authentication process. For broad user acceptance, the prime considerations for any handheld device authentication method are how convenient it is to use and how well its design utilizes the capabilities of the core hardware. For example, the time required to perform various functions, such as enrollment and verification, should be minimal and the procedure straightforward. Any difficulty due to large attachments, slow performance, or error-prone display is generally not acceptable. Some of the general obstacles faced include (1) Computationally demanding authentication schemes (like Voice Verification) especially those involving floating point operations, can overwhelm the processor capabilities and turn out slow performance. (2) Power consumed by any extra hardware for user authentication must be least to avoid discharging the battery of the device quickly. (3) Powering off a handheld device suspends the processes, rather than shutdown. This feature is convenient to the user but requires the developer to assert the authentication mechanism when the device is powered on, as well as during system reboot.We have conducted a comparative analysis of existing user authentication schemes that have been designed or could be modified for mobile and handheld devices, grouped into the three main classes graphical based, image based and audio based authentication.

8 Conclusions

Handheld devices, being designed for mobile workers, offer unique opportunities for user authentication. Several suitable authentication mechanisms exist as password replacements for mobile and handheld devices. As the understanding of security is explored not only in term of technical aspect but also in term of usability, interest in using alternative schemes of user authentication are developed. Text-based authentication schemes are inherently insecure as they are subject to a trade off between usability and security, however they remain popular as their concept corresponds to an existing common model world view making them an easy to understand concept. In this paper, we have conducted a comprehensive survey and analysis of the existing user authentication schemes that have been designed or could be modified for mobile and handheld devices. These user authentication schemes are presented in Table 1. Although the main argument for these schemes is that people are better at memorizing these schemes than text-based passwords, the existing user studies are very limited and there is not yet convincing evidence to support this argument. Our analysis suggests that it is more difficult to break the security of these schemes using the traditional attack methods such as brute force search, dictionary attack. However, since there is not yet wide deployment of these schemes, the vulnerabilities of these schemes are still not fully understood. According to the security and usability analysis the most promising authentication mechanisms are Passfaces, Draw a Secret, Passclick, Voice verification and Audio and Image authentication. Overall, these schemes are immature but as more and more research will be conducted to understand the usability of these schemes we will find higher levels of security in user authentication with usability.

Table 1: Comparative Analysis of User Authentication Schemes for Mobile and Handheld Devices

User Authentication Scheme	**Authentication Process and Usability**	**Memorability / Usability**	**Possible Attacks / Security Issues**
Alphanumeric Password With Graphical Assistance	Type the password; however additional graphical input improves the authentication Process.	Depends on the password and function selected in graphical assistance. Complex function, Long and random passwords are hard to remember.	Brute force search, Spy ware, shoulder surfing, etc
Draw a Secret	Users draw something on a 2D grid.	Depends on what users draw. User studies showed the drawing sequence is hard to remember.	Guess, Shoulder Surfing, different password attack methods are not successful.
3D Graphical Password	Users draw something on a 3D grid and allowed to rotate the drawing canvas on z axis in clockwise or counter-clockwise motion.	Depends on what users draw. User studies showed the drawing sequence is hard to remember. However the password space increase around 20 times than draw a secret scheme.	Guess, Shoulder Surfing, because this scheme include graphical input different password attack methods are not successful.
Pass faces and Déjà vu	Recognize and pick the preregistered pictures; takes longer than text based password.	Faces are easier to remember, but the choices are still predictable. Memorability mainly depends on the total number of rounds in the process and the face selection.	Dictionary (Face) attack, Face brute force search, Guess, shoulder Surfing.
Pass clicks like Blonder scheme Passlogix, passpoint,visual Key.	Click on several pre registered locations of a picture in the right sequence.	If the selected image has limited memorable points in it, pass clicks can be hard to remember. Memorability depends on the image selection.	Guess, brute force search, shoulder surfing. Because this scheme include graphical input different password attack methods are not successful.
PointSec	Uses pictograms rather than numbers for code.	Depends on what users selection , but the choices are still predictable.	Dictionary attack,Brute force search, Guess, shoulder Surfing.
Audio Authentication (Voice system and Voice Verification)	Voice signal work as password, voice may be speech or any audio. Process can be fast or slow depend on user.	Depends on the Voice password. Long and random passwords are hard to remember, but long song, poem are easy to member.	Dictionary attack, Brute force search, Guess, spy ware, Shoulder surfing, etc.
Audio and Image Authentication	Images can be associated with a particular piece of music as a password	The Images and music association. Number of associations chosen by user improve security but reduce memorability.	Brute force search, Guess, spy ware, Shoulder surfing, etc.
Audio-Visual Person Authentication using Speech and Ear Images	The image of ear shape of a user is integrated with user speech information, which increases the robustness of user authentication.	Not Applicable.Comes under the biometrics user authentication.	Speech is deteriorated by acoustic noises and time. Ear shape feature changes with time.

References

[1] Birget, J.C., Hong, D. and Memon, N. Robust discretization, with an application to graphical passwords, Cryptology ePrint archive 200307.

[2] Blonder, G. E. Graphical passwords, in Lucent-Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[3] Brostoff, S. and Sasse, M. A. Are Passfaces more usable than passwords: a field trial investigation, in People and Computers XIV - Usability or Else:Proceedings of HCI. Sunderland, UK: Springer-Verlag, 2000.

[4] Campbell, J. and Schroeder, J. Eds. Special issue on speaker recognition, Digital Signal Proces., vol. 10, Jan. 2000. Last accessed in January 2008.

[5] Daniel, K. Foiling the Cracker: A Survey of, and Improvements to, Password Security, Proceedings of the 2nd USENIX Unix Security Workshop, pp. 5-14, August 1990.

[6] 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.

[7] Eugene, Spafford. OPUS: Preventing Weak Password Choices, Computers Security. 11(3), pp. 273-278, May 1992.

[8] `http://www.rsasecurity.com/products/securid/`. Last accessed in January 2008.

[9] Jansen, W. Authenticating Mobile Device Users Through Image Selection, in Data Security, 2004.

[10] Jermyn, I., Mayer, A., Monrose, F., Reiter, M.K., Rubin, A.D. The design and analysis of graphical passwords, In: Proceedings of the Eighth USENIX Security Symposium, pp. 114, 1999.

[11] Kingpin and Mudge. Security Analysis of the Palm Operating System and its Weaknesses Against Malicious Code Threats, Proceedings of the 10th USENIX Security Symposium, August 2001.

[12] Koji Iwano, Tomoharu Hirose, Eigo Kamibayashi, and Sadaoki Furui. Audio-Visual Person Authentication Using Speech and Ear Images, Tokyo Institute of Technology, Department of Computer Science, 2-12-1 Ookayama, Meguro-ku, Tokyo, 152-8552 Japan.

[13] Liddell, J., Renaud, K. and De Angeli, A. Using a combination of sound and images to authenticate web users. Short Paper HCI 2003. 17th Annual Human Computer Interaction Conference. Designing for Society. Bath, England. 8-12 Sept 2003.

[14] Newman Fabian Monrose. Towards Stronger User Authentication, dissertation, Doctor of Philosophy,Department of Computer Science, New York University, May 1999, pp74-78.

[15] Nicky Boertien and Eric Middelkoop. Authentication in Mobile Applications, CMG, Telematica Instituut, The Netherlands, January 2002, `https://doc.telin.nl/dscgi/ds.py/Get/File-23314/VH_authenticatie.pdf`. Last accessed in January 2007.

[16] Paivio, A., Rogers, T. B. and Smythe, P. C. Why are pictures easier to recall than words, Psychonomic Science, 11:137-138, 1968.

[17] Passlogix,`www.passlogix.com`. Last accessed in January 2008.

[18] Pointsec for Pocket PC, Pointsec Mobile Technologies,November2002,`http://www.pointsec.com/news/download/Pointsec_PPC_POP_Nov_02.pdf`. Last accessed in January 2008.

[19] Rachna Dhamija and Adrian Perrig. Déjà Vu: A User Study Using Images for Authentication, 9th Usenix Security Symposium, August 2000.

[20] RealUser. `www.realuser.com`. Last accessed in January 2008.

[21] Reynolds, D.A., Quatieri, T.F. and Dunn, R.B. Speaker verification using adapted gaussian mixture models, Dig. Signal Proc., vol. 10, pp. 181202, Jan. 2000.

[22] Robert Morris and Ken Thompson. Password Security: A Case History, Communications of the ACM, 22(11), pp. 594-597, November 1979.

[23] SafeGuard PDA, Utimaco Safeware AG, March 2003, `http://www.utimaco.com/eng/content_pdf/sg_pda_eng.pdf`. Last accessed in January 2008.

[24] Saikat Chakrabarti, George V. Landon, and Mukesh Singhal. Graphical Passwords: Drawing a Secret with Rotation as a New Degree of Freedom.

To appear in The Fourth IASTED Asian Conference on Communication Systems and Networks (AsiaCSN 2007).

[25] Visual Key Technology, sfr GmbH, 2000, http://www.viskey.com/technik.html. Last accessed in January 2008.

[26] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. Authentication using graphical passwords: Basic results, in Human-ComputerInteraction International (HCII 2005). Las Vegas, NV, 2005.

[27] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. Authentication using graphical passwords: Effects of tolerance and image choice, in Symposium on Usable Privacy and Security (SOUPS), at Carnegie-Mellon Univ., Pittsburgh, 6-8 July 2005.

[28] Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. PassPoints: Design and longitudinal evaluation of a graphical password system, International J. of Human-Computer Studies (Special Issue on HCI Research in Privacy and Security), 63 (2005) 102-127.