International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 5, Sep - Oct. 2013 pp-3012-3019 ISSN: 2249-6645

A Survey of User Authentication Schemes for Mobile Device

Hezal Lopes[1], Madhumita Chatterjee [2]
**(Computer, Universal College/Mumbai University, India)*
*** (Department of Computer Engineering, Mumbai University, India)*

***ABSTRACT**: Personal mobile devices (PMDs) have become ubiquitous technology. There, steadily increasing computational and storage capabilities have enabled them to over an increasingly large set of services. Mobile devices offer their users lots of possibilities and a feeling of freedom. However, this freedom comes along with new security threats. Sensitive data might be stolen and abused, if an unauthorized person gets unrestricted access to such devices. Considering their significance, it's necessary to ensure that they aren't misused. Therefore, user authentication mechanisms are required. Unfortunately, a less effective and inconvenient PIN based authentication system is used to protect them against their misuse. So far authentication mechanisms like PINs and passwords do not take into account the limited capabilities of user interfaces of mobile devices. So, it is necessary to create and develop specially adapted mechanisms, which are designed to be usable under these restrictions. In this paper, we have tried to identify what are possible approaches for authenticating users on mobile device and highlight their pros and cons in terms of security and usability.*

***Keywords:** User authentication, Graphical method, Image based method, Audio based method.*

I. INTRODUCTION

Mobile devices support us in our everyday life. The main advantage of these devices is that we can take them with us and use them almost everywhere and at any time. We can check our e-mails, read online news, communicate via social networks and do many other things on the go. To support their owners mobile devices create and store a lot of sensitive personal data.

Today, mobile devices are ubiquitous, but are potentially accessible to unauthorized persons. To avoid misusage it is important to implement and use reliable authentication mechanisms. Widely used knowledge-based mechanisms like PINs and passwords are not well suited for mobile devices as the capabilities of user interfaces are very limited.

It is necessary to understand the capabilities and limitations of mobile devices beforehand. It is important to develop new authentication mechanisms specially adapted to the limitations and options of mobile devices.

In this paper we have discussed possible user authentication mechanisms for mobile devices their deficiencies.

II. A USER AUTHENTICATION SCHEMES

User authentication is the primary line of defence for a handheld device [1] 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.

Security of user authentication associated issues comes 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. 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 three broad classes. They are as follows:

- Graphical-based Authentication
- Image based Authentication
- Audio-based Authentication.

II.I 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. This scheme is divided into three categories. [1].

- Password with Graphical Assistance
- Draw-A-Secret
- 3D Graphical Password.

II.I.I Password with Graphical Assistance

Password with Graphical Assistance scheme is stronger than textual passwords [1]. Figure 1(a) shows, 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).

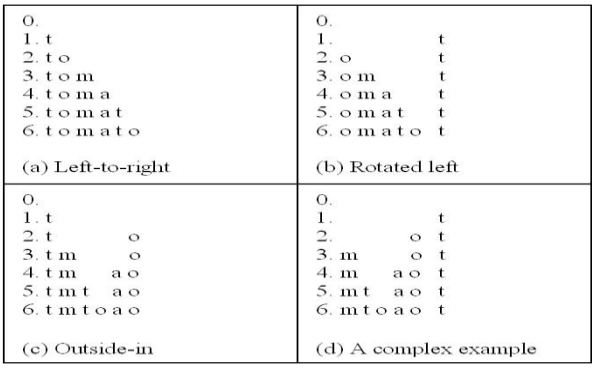


Figure 1: Password with Graphical Assistance [1]

Advantage

The power of graphical input abilities while yielding a scheme that is convincingly stronger than textual passwords.

Disadvantage

Long and random passwords are hard to remember also it has complex function.

III.I.II Draw-A-Secret

A technique, called "Draw - a - secret (DAS)", which allows the user to draw their unique password [2]. A user is asked to draw a simple picture on a 2D grid. The coordinates of the grids occupied by the picture are stored in the order of the drawing. During authentication, the user is asked to re-draw the picture. If the drawing touches the same grids in the same sequence, then the user is authenticated. Jermyn, et al. suggested that given reasonable-length passwords in a 5 X 5 grid, the full password space of DAS is larger than that of the full text password space.

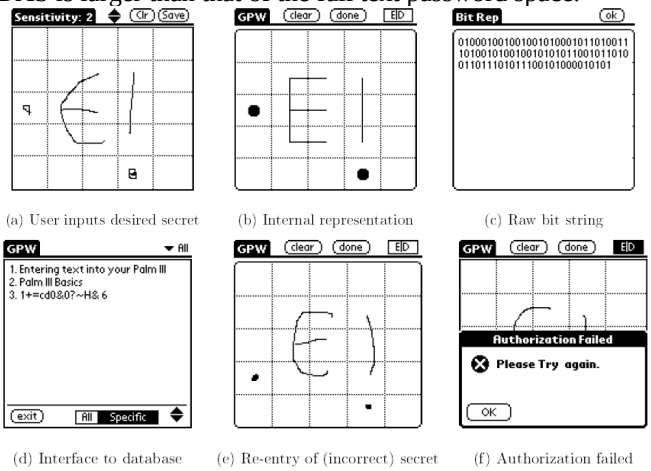


Figure 2: Draw a secret [2]

Advantage

DAS password scheme is hard to crack in practice than the conventional textual scheme.DAS passwords of length 8 or larger on a 5 x 5 grid may be less susceptible to dictionary attack than textual passwords. This approach is alphabet independent. Users are freed from having to remember any kind of alphanumeric string.

Disadvantage

DAS passwords (for some reasonable number of primitives) constitute a larger space than that of textual-based password.

II.I.III 3D-Graphical Passwords

A special feature in this scheme the user is permitted to rotate the drawing canvas (grid) [3]. The rotation is performed on the z-axis, which gives a 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. 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 modelled 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 equip-angular bi-directional rotations in-between strokes are encoded differently and generate a different password from drawing the same picture with no rotations at all.

(c) Rotation of -90° and another stroke drawn: (-90)(5,1)(5,2)(5,3)(5,4)(5,5)(6)

(d) Rotation of +90°, rotation of -45°, then another stroke drawn: (+90)(-45)(1,1)(1,2)(1,3)(1,4)(1,5)(6)

Figure 3: 3D Graphical Password [3]

Advantage

This scheme increases the password space to very large extent and hence promises to provide extended security. This scheme provides a higher level of security without compromising user convenience. The same mirror-symmetric drawings with different intermediate rotations are encoded as different passwords, making it difficult for the attacker to form the dictionary simply based on mirror symmetry. Also, rotation of the drawing grid introduces resistance to shoulder-surfing attacks. Consider where an attacker manages to get a glimpse of the final drawing on the canvas when the user is trying to log in. The attacker would try to guess the sequence in which the strokes were made (including the direction of the strokes) by the user while drawing the picture. (Knowing whether the user is right-handed or left-handed might help the attacker guess the direction of the strokes.) If the attacker guesses the sequence and direction of the strokes correctly, he would succeed in getting the user's password. However, the added dimension of rotation makes it significantly difficult for the attacker to guess the password by just looking at the final drawing on the canvas.

Disadvantage

Password space increases around 20 times than draw a secret.

II.II Image based Authentication

Images are more readily recalled than words [1] 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.

II.II.I Passface

To log in, users select their Passfaces from a grid of faces displayed on the screen [4]. This study uses the standard implementation of the Passfaces demonstration toolkit, requiring participants to memorise 4 faces, and correctly select all 4: one in each of 4 grids of nine faces (see Figure 4 for an example grid). The grids are presented one at a time on the screen, and the order of presentation remains constant, as do the faces contained in each grid. However, no grid contains faces found in the other grids, and the order of faces within each grid is randomised. These features help secure a user's Passface combination against detection through shoulder-surfing and packet-sniffing.

Figure 4: Passfaces [4]

Advantages

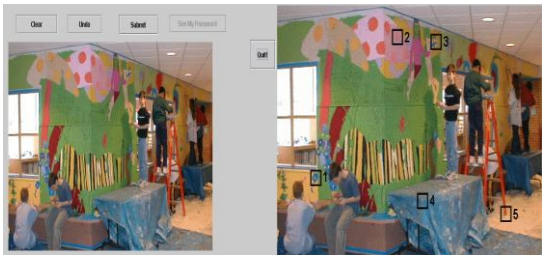
Passfaces have been shown to be very memorable than traditional passwords. Passfaces offer better performance than passwords for users who log in infrequently (less than once every two weeks). These features help secure a user's Passface combination against detection through shoulder-surfing and packet-sniffing.

Disadvantages

The increasing power of computing infrastructure is inevitable. As the increase occurs, the resources that Passfaces require will become ubiquitous. Passfaces should therefore be tested with up to date hardware and software facilities. If these facilities are not available, speed of the authentication mechanisms' responses to user input should be measured and included in analyses, and response times made similar by retarding the password mechanism. Pass face-based log– in process took longer than text passwords and therefore was used less frequently by users. However the effectiveness of this method is still 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.

1) II.II.II Passclick

A graphical password scheme in which a password is created by having the user click on several locations on an image [5]. 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 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.



Advantage

There are no multiple rounds of images, just a single image. In an implementation of this scheme the image had predefined click objects or regions that were outlined by thick boundaries. The users chose the password from these objects and logged in using them (although thick boundaries were not visible when logging in). A click anywhere within the boundary was considered correct.

Disadvantage

A problem with this scheme was that the number of predefined click regions was relatively small so the password had to be quite long to be secure (e.g., 12 clicks). Also, the use of pre-defined click objects or regions required simple, artificial images, for example cartoon-like images, instead of complex, real-world scenes. If we have some complicated or crowded image then it takes more time to scan the image to identify their password points. They probably also had to observe the area of their password points very carefully to identify the exact place to click. Consider figure 6 which is very complicated image. So here difficult to identify exact place user has click.

II.III Audio-based Authentication

Audio signal are one of the most useful and effective features for user authentication in mobile environments [1]. 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.

II.III.I Voice Verification

Voice Verification [1] presents 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. Voice verification, also known as speaker recognition, determines the identity of the speaker. Enrolment 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. 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.

Advantage

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. 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.

Disadvantage

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. 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 isometric 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 speaker's health (cold or laryngitis). 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. The mobility of system likes uncontrolled and harsh acoustic environments (cars, crowded airports), which can stress the accuracy.

II.III.II Audio and Image Authentication

In considering how both audio and visual 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 [6]. AVAP protocol is used for this type of authentication. AVAP is based on the following hypothesis: mnemonic associations between audio and visual information can be exploited to authenticate a user. A prototype was developed to authenticate users entering a particular website. The prototype records a number of associations during enrolment, and requests those associations to authenticate users for subsequent website accesses. Five image-sound associations were required. Users were given a randomly-selected sound and required to relate it to one of a corresponding set of 10 images. These associations have to all be recalled at subsequent site entries.. Audio controls were displayed to facilitate repeated audio activation. Audio clips were chosen deliberately to provoke an association within a particular image set, and tended to mirror the general mood of a category (e.g.,. epic orchestral music corresponding to dramatic imagery of the cosmos). Nine audio clips were associated with groups of 10 images, six of which were semantically similar (i.e., same subject matter) and three random. We expected that grouping semantic images together would increase security by reducing the predictability of an association. For instance, it may be trivial to guess that an individual may choose an image of plant life for a given piece of music, but it may not be so easy to select what type of plant life an individual would select from a set of ten semantically-similar images. The three random categories were included to measure the relative performance of associations made using a random image set to those made using a semantically-similar set.

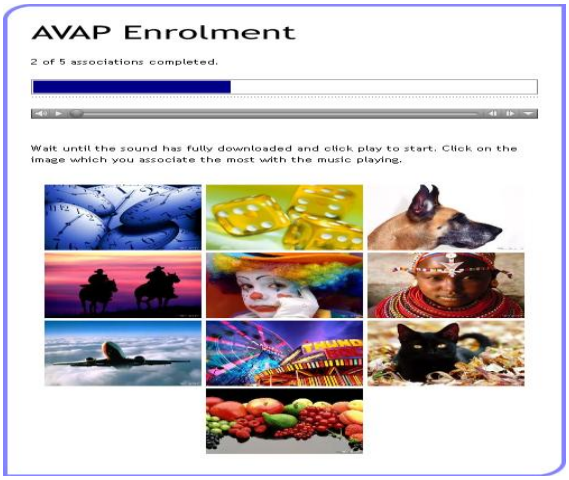


Figure 7: AVAP [6]

Advantage

Exciting and relaxing to use to be more enjoyable and relaxing. 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.

Disadvantage

Users did not always listen to the audio, but only chose pictures they liked. Users became irritated with the time taken for the images to download at each site access. Users struggled to distinguish between semantically similar images and thus made frequent errors. Images were deemed to be too abstract.

II.III.III Audio Visual Person Authentication Using Speech and Ear Images

Figure 8 shows multimodal person authentication system using speech and ear images [7]. Audio and visual data are respectively converted into feature vectors. Each set of features is matched with both a claimed person model and a speaker independent (SI) model. Then, audio and visual scores are integrated with appropriate weighting and a decision is

made whether he/she is a true speaker or an impostor. If the score is larger than a threshold value, the speaker is accepted as a claimed speaker.

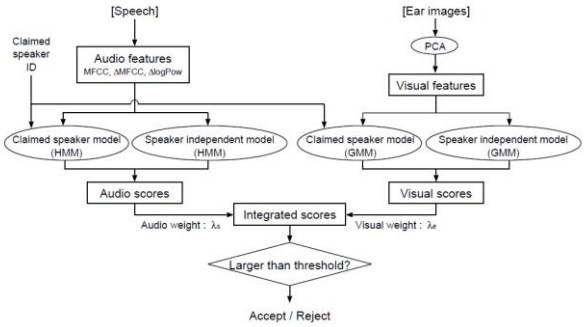


Figure 8: Multimodal Authentication Scheme[7**]**

Advantage

Although most of them use "face" information in combination with speech, the face features also change due to make-up, beard, hair styles and so on, and derives degradation of the performance. Therefore, it is worth investigating other biometric features with high permanence. ear shape hardly changes over time. Ear shape of person does not change over time that increases robustness of person authentication.

Disadvantage

Ear images are more changeable than face images by a tilt of the camera, since the ear surface is more irregular than face surface.

III. COMPARATIVE ANALYSIS OF USER AUTHENTICATION SCHEMES FOR MOBILE AND HANDHELD DEVICES

This table is used to give analysis of all user authentication schemes that we saw above.

	User Authentication Schemes	**Authentication process and usability**	**Memorability /Usability**	**Possible Attacks/ Security Issues**	**Analysis**
Graphical Based Authentication	Alphanumeric Password	Type the password	Complex function, Long and random passwords are hard to remember.	Brute force search, Spy ware, shoulder surfing, etc	Vulnerable to dictionary attacks(simple password)
	Draw a Secret	Users draw something on a 2D grid.	Drawing sequence is hard to remember	Guess, Shoulder Surfing, different password attack methods are not successful	Approach is alphabet independent, Users are freed from having to remember any kind of alphanumeric string
	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.	The drawing sequence is hard to Remember. 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.	Increase the password space to very large extent and hence promise to provides extended security
Image	Pass faces	Recognize and pick the preregistered	Faces are easier to remember, but the choices are	Dictionary (Face) attack, Face brute force	Images are more easily recalled than

Based **Authentication**		pictures; takes longer than text based password	still predictable. Memorability mainly depends on the total number of rounds in the process and the face selection	search, Guess, shoulder Surfing	words.
	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.	Instead of arbitrary images, user can click on any place on an image.
Audio **Based** **Authentication**	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, poems are easy to member.	Dictionary attack, Brute force search, Guess, spy ware, Shoulder surfing, etc.	Human ability to recall and recognize the audio signal is much higher than remembering words
	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 reduces memorability.	Brute force search, Guess, spy ware, Shoulder surfing, etc.	Environmental noise, pronunciation style, speech depends on speaker health, speaker system
	Audio-Visual Person Authentication using Speech and Ear Images	The image of ear shape of a user is integrated with user speech information, high 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.	Speech can go down by acoustic noise and feature changes over time. Ear shape of person does not change over time that increases robustness of person authentication.

IV. CONCLUSION

Authenticating users on mobile devices can be challenging and many solutions currently being used by mobile applications either compromise security or usability. When mobile devices connect to business networks, user and endpoint authentication play critical roles in preventing misuse, abuse and attack. With effective use of authentication methods, organizations and individuals can cost-effectively guard against current and emerging threats, while retaining optimal productivity and flexibility in their use of mobile devices.

The authors do not support for any particular solution here because the best solution depends on users application's requirements. For example, the security requirements for an online banking application that performs funds transfers are

different from the security requirements for student just using mobile for playing games. Additionally, the ultimate security of user application is depending on many implementation details.

REFERENCES

Journal Papers:

[1] M. N. Doja, Naveen Kumar,"User authentication schemes for mobile and handheld Devices", Jamia Millia Islamia - New Delhi,2007.

[2] 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.

[3] 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).

[4] 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.

[5] 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 July2005.

[6] 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.

[7] 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.