

Visual Security for Wireless Handheld Devices

Maria V. Duncan,* Murtuza S. Akhtari, and Phillip G. Bradford

Abstract

Everyday, passwords are used to access devices. Traditionally, passwords are alphanumeric, consisting of letters, numbers and symbols. Often, passwords are lengthy and have to be changed every few months to ensure computer security. This makes retention and recall difficult. Due to this problem, graphical passwords have been developed. This paper discusses a graphical password system designed and implemented as a summer project. In this system, passwords are made of pictures or symbols. Studies have shown that pictures are recalled more easily than words. Our research emphasizes that the linking of text to an image will enhance retention and therefore improve recall.

1. Introduction

Long and complex alphanumeric keyboard-typed passwords are everywhere. It is no wonder that people have a tendency to reuse passwords for different devices, limit the password to a few characters, and even write down the password. Longer and more complex passwords are often “stronger.” Unfortunately, they are difficult to remember. Visual passwords are an alternative to the traditional alphanumeric ones. Instead of numbers and letters, the passwords consist of images or pictures. Our research has a number of pictures, all of which contain a common secret that acts as the unseen password.

With wireless handheld devices, one does not have to work in the office anymore, but these handheld devices have special security needs. These include easy entry passwords, resilience to strangers observing password entry, and the prevention of writing down passwords. Visual passwords can help ensure computer security with wireless devices.

This paper shows that such visual and graphical password systems are easy to design and build. Such a system was built as an REU summer project at the University of Alabama. This paper discusses this system and other very recent industrial systems that share similarities.

1.1 Structure of this paper

In the introduction, wireless devices are introduced and how visual passwords can help improve computer security with regards to these devices. Some research into visual passwords is discussed, and a psychological view as to why pictures are better than words is presented in section 2.1. Section 2 also describes visual password software systems currently available for public use. Section 3 provides a discussion of our project and how it takes the visual password one step further by relating a word to a picture and more specifically link an attribute with a given geometric image. The advantages and disadvantages of visual security for wireless devices are discussed in section 4. Section 5 discusses the future avenues that can be tread to continually improve visual security.

1.2 Understanding the Visual Password System

There are three reasons for using a visual password system over an alphanumeric one:

- Personal input for cognitive retention
- Improve computer security
- Prevent “shoulder surfing”

Frequent password changes can be confusing. An individual might confuse new passwords that looked similar to the one that was issued to them months ago. With the use of graphical passwords and the use of themes, this is at least a partial solution. For instance, if the week’s theme for the staff is “3 + 4,” then this can be translated as to find three objects with four sides. This allows the individuals to pick out any object to their liking on the screen, as long as it is within the specified parameters. This will allow access to the staff even if two individuals choose different objects that lie within those parameters set.

More recently, many professors are turning to handheld data entry as opposed to the standard pen and paper to easily garner and access records. For instance, the medical staff uses check-off sheets on mobile devices while admitting a patient. Also, file entry is restricted to maintain confidentiality. A different password is given to an individual periodically to improve computer security. The individual might, on occasion, write down the password where others can see it. This can defeat the purpose of having an authentication method. Graphical passwords with “themes” that change prevent the user from writing the password. The change can be temporal or event driven. A temporal change is when a password is changed every week, and an event driven change occurs when passwords are changed upon completion of a particular project.

“Shoulder surfing” refers to someone looking over another person’s shoulder while they are trying to gain access into their system. This is important because in the business world, work is no longer limited to one’s PC. Many people use laptops, PDAs, and other mobile devices outside of their work area. For instance, a businessman is trying to access his company records while waiting for his flight at the airport. This increases the chances of shoulder surfing. Graphical passwords displayed randomly on touch sensitive screens allow the individual to impede shoulder surfing.

1.3 Challenge Response

Challenge response is a method of dynamically changing the level of security. Validating the authenticity of the user is important. There are several ways to perform a challenge response:

- The system itself can randomly propose questions based on its user database or other key time and/or sequence data
- An individual user can vary the attributes by adding subattributes

A user can surreptitiously add subattributes at different times by selecting visual keys that have common subattributes, where these subattributes are not necessary for the password.

2. Prior Graphical Password Research Developments

2.1 Pictures and Words: Memory Retention and Recall

Are words easier to recall than pictures or vice-a-versa? What role does this play in research and development of password systems? Studies in the past have shown that pictures are more readily recalled than words, according to Paivio, Rogers and Smythe

(4). Alphanumeric passwords are harder to remember, especially if they are changed every few months. Instead of letters and numbers for passwords, pictures are selected. This gives the user the ability to apply a personal touch to his password.

Does a caption aid in remembering a picture? Some pictures are hard to understand. For example, what is the relationship between these two pictures: the first one consists of several horizontal lines and the second one consists of wavy lines with a couple of circles. Would you have guessed that the first picture is uncooked pasta and the second one is spaghetti and meatballs? A nonsensical picture is one in which an individual cannot make an easy interpretation, described by Bower, Karlin and Dueck (5). This makes recognition and retention difficult, thereby making recall difficult. When a word or a sentence is displayed with a picture, a nonsensical picture begins to make “sense.” In our research, selecting icons with a common attribute creates the password. Therefore, a shoulder surfer might only see a display of non-related pictures but the user sees his password hidden within.

Age is also a considered factor in the research of memory retention and recall. Comparison studies of colored pictures, black and white pictures, and words show that colored pictures are recalled more easily than black and white pictures and words for various age groups, according to Borges, Stepnowsky and Holt (6). An important observation is that adults are better in recalling pictures, due to increased knowledge and organizational skills. It is this knowledge that will help prevent children from gaining entry to their parents’ important files.

2.2 Déjà vu

Dhamija and Perrig (2) give a visual password called Déjà vu. Instead of using alphanumeric passwords, the user chooses five geometric art images out of a series of twenty-five images. There are three phases:

- Portfolio Creation Phase
- Training Phase
- Authentication Phase.

In the Portfolio Creation Phase, the user chooses a subset of images to be used for his password. In the Training Phase, the user becomes more familiar with the subset of images. In the Authentication Phase, the user picks out his portfolio images from a display of images consisting of his portfolio and decoys.

There are three factors that motivate the development:

- Creating a password that can be recognized without precise recall
- Creating a password that can be used internationally
- Making authentication more secure

A Personal Identification Number (PIN) or a password requires precise recall. If the user fails by being off one letter or number, then he is denied access. The visual password allows the user to recognize their portfolio images without worrying about other images looking similar. Unfortunately, seeing the portfolio images constantly with the decoys upon authentication phase can possibly create confusion. The user might mistake a decoy as one of his portfolio images. Furthermore, such an imaging system is language neutral. Déjà vu is language independent. Some people write down their passwords and give them to their co-workers. This jeopardizes the computer security,

which is a major concern. The images make it hard for users to write them down and describe it to others.

The downside is that it takes longer in the creation of a personalized visual password compared to making a PIN or a regular password that people use to quickly log on. Further research in making the phases of visual password authentication quicker is being considered. On a promising note, studies have shown after a week, there have been less failed logins with Déjà vu compared to using PIN and regular passwords. In our research, we are taking it one step further. There exists the possibility of mistaking decoy images with portfolio images, but the use of attributes with the images decreases the likelihood of making that mistake.

2.3 Graphical Passwords

Currently, there are a few commercial graphical password software systems in existence. There is one in particular where clicking a specific point on a picture creates the password. The downside is that anyone who notices a few login sessions will know the password. Sobrado and Birget (3) use the concept of challenge response to deter shoulder surfing. Challenge response authentication is when the user must prove to the server that he has the needed information that a third party is not privy to.

In their system, a set of N objects is randomly displayed on the screen with a subset of K objects. The K objects are the pass-objects that the user has chosen. The user clicks on certain objects depending on the scheme. They propose three schemes:

- Triangle Scheme
- Movable Frame Scheme
- Special Geometric Configuration Scheme

In the first scheme, the user will find three of the K objects that form a triangular region. The user must click within this convex hull, defined by the three objects. In the second scheme, three of the K objects are presented within the N set. Only one of the K objects falls within a rotating line. The user must rotate the entire frame of objects in order to get a second K object to fall within the same line. In the last scheme, the user must find four K objects and click within their intersection. The user envisions the four objects' intersection and clicks within the area.

2.4 Sentence based Visual Login System:

PointSec™ offers a currently available sentence based visual login system (8, 9), and it provides a wide range of functionality:

- Real-time Encryption
- Removable Media Encryption
- Media Encryption Policy
- Enforceable Mandatory Access Control
- Central administration with PointSec™ profiles
- User account lockout
- User transparent encryption

The system also makes it easier to remember the Picture PIN and Quick PIN with customizable symbols or pictures. Alternatively, numeric or alphanumeric passwords can also be used. As an added security feature, it also has a predefined number of login attempts before the system locks out.

It uses a fast AES algorithm with a key length of 128 bits and provides automatic encryption without user intervention. Email attachments and notes are stored encrypted and are decrypted in real time when the user wishes to access them. It prevents unauthorized synchronization and access to data. All data stored on removable media is encrypted before storage, and it also allows usage of both encrypted and un-encrypted removable media.

However the PointSec™ software cannot be uninstalled, and the user is restricted to it even if he does not wish to utilize it. Also, the PointSec™ software is designed to function only with a particular type of OS (i.e., a different software has to be built if the user wishes to use it in a different machine with a different OS environment).

2.5 Picture Based Visual Login Systems:

Picture based systems are offered by VisKey or visual key (10). This system uses a single picture wherein the user has to click predefined spots on the picture that serves as the password. This password has to be selected previously by the user. For example, the picture of a house could be displayed wherein the user has to click on the chimney, the door, the window, and the roof in that order. The makers of VisKey claim that a regular four-character password has a possible ten thousand combinations, whereas the corresponding four clicks on a picture offer 1,000,000,000 different combinations. It also allows the user to use any of their favorite pictures, or it provides the user with a variety of downloadable pictures to choose from. VisKey is currently available in three versions for the PPC, the PC, and the Palm OS. The only difference between the PPC and PC versions is that the first one uses different pictures or a set of pictures to create a password, and the second one generates a password by selecting different positions on a single picture.

2.6 Real User PassFaces: The Passface™ User Authentication System

Real User's Passface™ system (11, 12) is a revolutionary method of personal authentication that provides significant benefits in security, reliability, usability and cost over traditional password based systems. The principal behind the Passface™ system is that people are extremely good at *recognizing* faces - even though they may be bad at *recalling* names and even worse at *recalling* random sets of characters or numbers. The Passface™ system harnesses this innate human ability as a means of personal authentication. Real User's Passface™ personal authentication solution combines the benefits of scalability, reliability, security, and usability.

3. Our Results and Implementation

3.1 Visual Display

A “password screen” drives this system in which the screen displays several lists from which the user chooses the attributes. Graphical icons are displayed as buttons and the user chooses, say, five icons that contain the selected attributes. The positions of the buttons randomly change upon login. This will hinder shoulder surfing based on key position.

Software patterns used in development are Event Model, Factory, and Subject/Observer. These patterns are dependent on each other. The Event is when

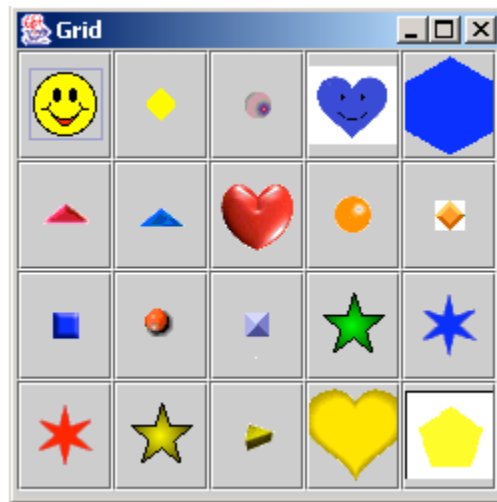
specific buttons are pressed. The Subject (user) sends the Events to the Observer (Factory), and the Factory creates instances of the icons with its related attributes.

3.2 Icons and Attributes

It is noted that after a week, there are less failed logins with graphical passwords compared to using PIN and regular passwords. The long-term use of Déjà vu might create confusion between what is a decoy image and a portfolio image. With our research, the use of attributes with the images decreases the likelihood of making that mistake.

The icons are the geometric shapes displayed as buttons. Associated with each icon is a set of attributes. The points, sides, color, and animation of a given icon characterize these attributes. The attributes serve as visual cues to help enhance the retention of specific images. The user personalizes the password when selecting a specific attribute.

The screenshot that follows shows the main login screen of our program. It displays a number of icons/images, some of which can be pre-assigned to be the user's password. At this screen the user keys in his password in the correct order, and the buttons that he clicks are stored in a list, which is then compared to the stored password. If the correct password has been entered, then the user is given access to his files. If not, then an error message pops up and takes the user back to this screen for him to re-enter his password. The user gets three tries before the system locks him out.



3.3 Implementation

The JAVA™ (Sun Microsystems) language was used for implementation of this project. JFrame, which is a subclass within the Java language package, gave us features that met our projects needs. Some features included a title bar, more control of the screen objects, JButton, and JList.

Preexisting geometric clip art shapes were used as images (7) and were chosen because they are found in nature as well as manmade items. Our project was more appealing because it was language independent and therefore can be used internationally.

The package consists of four classes:

- ChangePassword Class

- Grid Class
- IconAndAttributeFactory Class
- IconNAttributes Class

In the ChangePassword class, the user determines what the password is by choosing a given attribute of geometric object. The attributes are the points, sides, color and animation. For example, a triangle has three points, three sides, a specific color (depending on the icon), and will be either stationary or animated. The user chooses the attributes from the JLists displayed. The Grid class displays the icons as buttons, and it is within this class where the third class name originates. The IconAndAttributesFactory class creates instances of these icons. The data retrieved in creating these icons come from a metaFile which references to a controlFile. This controlFile contains the reference for the images (gif) and its related attributes. The Icon and attributes are then stored within the IconNAttributes class as a LinkedList.

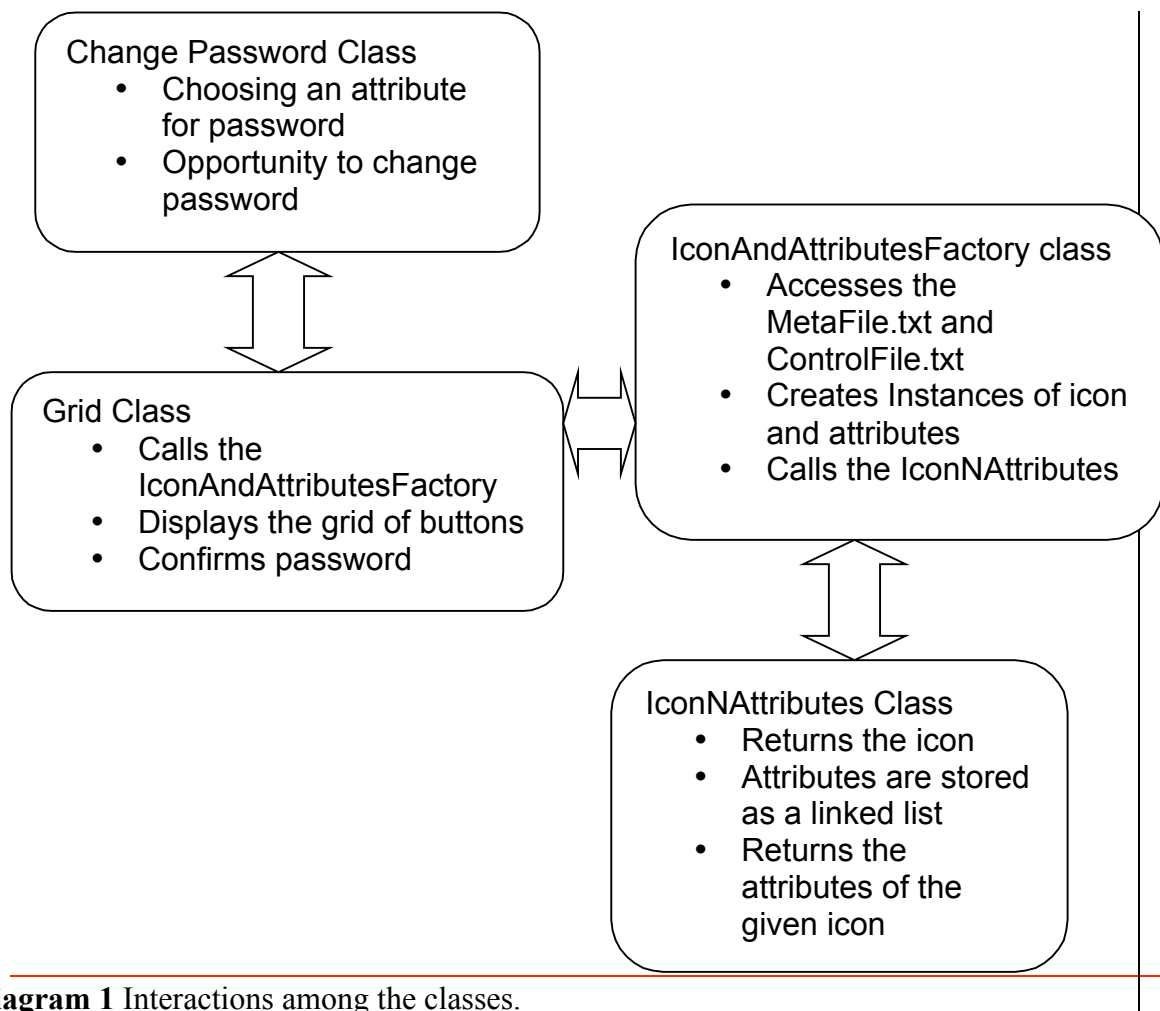


Diagram 1 Interactions among the classes.

4. The Pros and Cons of Alternative Security for Wireless

For handheld wireless devices, there are certain issues considered. Passwords are hard to type, especially those that are long and complex, and the user is limited to one-handed typing. Authentication of the user needs to be quick and easy. Shoulder surfing is also a bigger problem with these devices because someone can gain access with ease. This makes it easy for an attacker to gain access as well. Due to portability, handheld devices can also be misplaced, so it is important to know where your device is at all times. Sensitive information should never be saved on wireless devices because if stolen, the thief has the opportunity to access the files.

Auditory passwords are also being considered as alternatives to the conventional password system. This allows the individual to select his/her password by selecting distinct sounds that are linked to "themes." For example, if you chose nature as your theme, you would pick noises like birds chirping, frogs croaking, and a rippling brook. Unfortunately, there are a few disadvantages. Background sound is a factor, when using wireless devices. Being in a subway, it would be difficult to separate them from the distinctive sounds for the password. Another factor is user authentication itself. It would take time to learn and recognize the distinct sounds before choosing the right ones for your password.

5. Future Directions

Our graphical password scheme is based on text associated with pictures, therefore different from the systems previously discussed. The goal of our research is to provide a faster and more secure approach for user authentication. In other words, provide a password to be easily recalled, but less likely for a hacker to guess it. As previously mentioned, further research in making the phases of visual password authentication quicker is being considered.

References

1. Adrian Perrig and Dawn Song: "Hash Visualization: a New Technique to Improve Real-World Security," International Workshop on Cryptographic Techniques and E-Commerce (CrypTEC '99).
2. Rachna Dhamija and Adrian Perrig: "Déjà Vu: A User Study Using Images for Authentication," 9th Usenix Security Symposium, August 2000
3. Leonardo Sobrado, J.C. Birget: "Graphical passwords," *The Rutgers Scholar*, vol. 4 (2002). <<http://RutgersScholar.rutgers.edu/volume04>>
4. A. Paivio, T. B. Rogers, and P. C. Smythe: "Why are pictures easier to recall than words?" *Psychonomic Science*, 11:137-138, 1968.
5. G. H. Bower, M. B. Karlin, and A. Dueck: "Comprehension and memory for pictures," *Memory and Cognition*, 2:216-220, 1975.
6. M. A. Borges, M. A. Stepnowsky, and L. H. Holt: "Recall and recognition of words and pictures by adults and children," *Bulletin of the Psychonomic Society*, 9:113-114, 1977.
7. Images were found from the following sites: <<http://www.fg-a.com/gifs/html>>, <<http://www.gifanimations.com>>, and <<http://wilsoninfo.com/gifs.html>>
8. <<http://www.pointsec.com>>
9. <http://www.pointsec.com/solutions.pdf/datasheet_ppc_a4_2003.pdf>

10. <<http://www.viskey.com/>>
11. <<http://www.realuser.com>>
12. <<http://www.realuser.com/published/ScienceBehindPassfaces.pdf>>

* NSF Research Experience for Undergraduates at the University of Alabama