PictureLock and Security Organizer

<Students' names redacted>
Department of Computer Science and Engineering
The Ohio State University
Columbus, OH 43210

Abstract

Traditional security measures require users to create passwords using a string of characters. However, recent technologies have enabled unauthorized individuals to obtain a password using a variety of techniques. Traditional character passwords are also difficult for users to remember. This paper introduces a new method of password authentication using pictures instead of a string. This new method of authentication, called PictureLock, is incorporated into an application, called Security Organizer, for storing usernames and passwords for online accounts. Similar pictograph methods that provide identity and authentication services are discussed. Together, the PictureLock and Security Organizer improve the security of traditional password authentication methods in a useful application while maintaining a low overhead. Although it provides countermeasures to known threats, it does have a few vulnerabilities it its design that need to be addressed. Future features for the application include adding an ability to create multiple databases, upload themes, and adding an intrusion detection system.

1. Introduction

In our digitalized world, we increasing rely on the Internet in our daily lives. Many people pay bills, shop, and check social sites online. These activities require users to have online usernames and passwords for these accounts to prove their identity. Advanced mobile technology is also allowing people to complete these tasks using their phones. However, as the number of accounts that we have increases, we are required to remember additional usernames and passwords. A phone application that remembers this information would be a useful tool for mobile users.

In this paper we propose a new Windows Phone 7 application that stores information, including the username, password, and URL for online accounts, called the Security Organizer. Since this application holds valuable information, it must be adequately protected and implement secure access control. Therefore, we also propose using a unique pictograph "alphabet" for the password to access the application called PictureLock. PictureLock provides several advantages over traditional passwords by its design, which will be discussed in the following sections.

We designed the PictureLock and Security Organizer with the following goals in mind:

1. To create a simple, intuitive application GUI to store online account information. This is the Security Organizer.

2. To implement an authentication system that would balance security and usability. It should be easy to use and remember, while still maintaining a low cost and improving security. This is the PictureLock.

2. Access Control

Access control is critical for any information system. It provides methods for controlling the users and processes that are allowed to access a system. It also controls what they are allowed to do with the information and data on that system.

Access control can be thought of as operating in layers. These layers are often divided into physical, administrative and technical controls. Technical controls are the hardware, software and devices that enforce policies on a system. The PictureLock authentication system is a technical control.

The process flow for an access control system is as follows:

· User identifies themselves to the system

· System verifies the users identity through authentication

· If authentication succeeds, the system checks to see if access is allowed through the authorization step.

· If the user is authorized, access is granted and the system may log the actions of the user through accounting. The components in the process are commonly known as Authentication, Authorization and Accounting (AAA). The PictureLock software is an authentication system. In the use case for a smart phone application, it is a single user application. It is assumed that if the user authenticates successfully, then they are authorized to use the data in the application.

2.1 Authentication

Authentication systems are commonly divided into three categories: something you know, something you have and something you are. Combining authentication from two or more of these is known as multi-factor authentication and is considered very strong. However, multi-factor authentication increases costs and in some cases, decreases usability.

2.1.1 Password Authentication

Common implementations of something you know are passwords and passphrases. However, a common problem with passwords is that users will often choose a password that is easy to recall rather than being sufficiently complex. The PictureLock authentication is also a form of this type of authentication using images in place of characters. For increased security, the images in PictureLock should only be meaningful to the user of the application.

2.1.2 Other Authentication Systems

Other systems implementing the other two forms of authentication include smart cards, security tokens and biometrics. While these system offer substantial improvements to security, they are often difficult and expensive to implement. In addition, they require special hardware on the device being used. The PictureLock system avoids this additional expense by not requiring any additional hardware.

2.2 Threats to Password Authentication

One of the main objectives of PictureLock is to allow greater security than traditional passwords without making access to resources significantly more cumbersome.

As this is the case, it is important to examine some of the threats faced by traditional passwords.

2.2.1 Shoulder Surfing and Snooping

One of the most common threats to password protection on a phone is shoulder surfing. Shoulder surfing is when an attacker observes a legitimate user while he or she performs a task to authenticate themselves with the system. By observing the characters entered, they attacker can attempt to reproduce the task and gain access to system resources. The effectiveness of a shoulder surfing attack depends directly on (1) the difficulty involved with observing the user performing authentication and (2) the attacker's ability to reproduce the authentication.

In the case of traditional passwords, it can be relatively easy to observe someone entering a password by simply watching the user press the buttons or keys required to enter it. Even though the attacker cannot see the keys that are pressed, they may be able to observe the password on the screen. Usually, passwords are obfuscated on the screen. However, the length of a password can still be clearly discerned. Knowing password length increases the odds that an attacker can guess the password. If a password is learned through shoulder surfing, it becomes trivial for any attacker with even a modicum of computer knowledge to reproduce it.

2.2.2 Brute Force Attack

Brute force attacks are defined as an attacker trying all possible password combinations to find the correct password. The effectiveness of such an attack depends entirely on the number of possible passwords. In the case of a traditional password, the strength is dependent on the length and randomness of the password. In the case of the pictograph authentication, the total number of possible passwords depends on the total number of images used. This assumes that the attacker is blindly selecting images and unaware of the use of themes of pictures and the number of themes.

2.2.3 Dictionary Attack

Dictionary attacks involve the use of common passwords in an attempt to guess a user's correct password. This varies from brute force attacks because they try to anticipate user behavior rather than simply exhaust the space of passwords. The effectiveness of dictionary attacks may have relative success against users of traditional passwords whose choices or policies do not protect them against this.

2.2.4 Forgotten Passwords

Forgotten passwords can prevent a user from accessing resources to which they are entitled. Most traditional password systems have some sort of system for recovering this password, but if such a system is compromised (the user's e-mail, for example) then their password may be compromised. There are a number of factors that affect the severity of this threat, including the existence and security of a password recovery system, but also the likelihood that a user will forget the information that they need to access the system.

2.2.5 Social Engineering

Social engineering is when an attacker attempts to persuade a user to divulge their password or other means of access to the system. Usually, this means posing as a person whom the user might expect to have legitimate need of the password. The effectiveness of this is based mostly on user awareness and policy.

3. Related work

Several other research projects and implementations using images exist to provide identity and authentication services. In some cases, the images are used to prove the identity of a particular machine or system to a human. A common implementation of this is known as SiteKey.

Another use is in CAPTCHAS, where the images can be used to prove to a system that the other endpoint is a human. Finally, images can be used for general authentication, proving the identity of an individual. User authentication is the task that PictureLock implements.

3.1 SiteKey System

According to a study submitted to IEEE in 2007, 100% of users failed to notice that HTTPS was disabled on website to which they were authenticating [1]. SiteKey attempts to add additional cues for the user to distinguish the actual website they wish to connect to from a fraudulent one. SiteKey works by having the user first presenting their identity to the website without any additional authentication. If this is the first time the user is visiting the website, they will be challenged with a security question or cognitive password, such as favorite color or mother's maiden name. If the user answers the question successfully, they are presented with a unique image which they chose when they enrolled. The purpose of asking the security question is to ensure attackers are not able to snoop the SiteKey image. Once the user verifies that the proper image is displayed, they may proceed to enter their regular password.

One problem with the SiteKey is that it requires users to notice the lack of the proper image being displayed and to realize that they may not be connected to the proper site. This is much like HTTPS where users are required to notice that HTTPS is not being used to realize it is not safe to proceed. In the Schecter et al study, 92% of users proceeded to disclose their authentication information despite the proper image not being displayed. [1]

3.2 Traditional CAPTCHA replacement

CAPTCHA systems are used to prove to a computer that the other end point is a human as opposed to another computer. This is often called a reverse Turing test.

Traditional CAPTCHA systems are implemented by scrambling alphabet characters in way that is easily distinguished by humans but is difficult for a computer to interpret.

Several systems have been researched that use image systems to replace these traditional character based systems. In research conducted by Gossweiler et. al, they discuss a system where images of arbitrary orientation are displayed to a user and the user is required to correct the orientation [2]. Similar research by Bai et. al. displays a series of images to the user and requires the user to determine which of the images are correctly oriented [3].

3.3 General user authentication

Images can also be used to uniquely determine the identity of an individual in a manner similar to traditional passwords. In research by Komanduri, a system was designed to authenticate users based on images instead of character based passwords [4]. This system had a one-to- one mapping with character based passwords in order to determine if passwords of the same complexity this were based on images improved the user's ability to recall their password. A common problem with character passwords is that as complexity goes up, the user's ability to recall this password goes down.

Komanduri also compares the effectiveness of requiring the users to recall the images and characters in order to user's ability to recall images and characters with no defined order. In both cases, the ability to recall the image based passwords was significantly higher than character based passwords. When requiring the proper sequence of images or characters to be recalled, the group using image based passwords improved from 50% correct recall to 66%. When not requiring any order, the group using images improved to 100% compared to 66% for the group using character based passwords. [4].

4. PictureLock and Security Organizer

In today's high tech world, many people have multiple online accounts. As demonstrated by the previously mentioned research, it can be difficult for people to remember the user names and passwords for each of these accounts. As a consequence, passwords are forgotten or people use the same password for multiple accounts -- reducing the security of these accounts. By having an application which keeps track of account information, users will be less likely to use the same password for multiple accounts and forgetting a password becomes impossible. However, the password to access this application must have tight security and be easily remembered. After reviewing current authentication methods, we wanted to create a system that is low-cost and easily remembered while still upholding tight security standards. We therefore decided to implement an authentication system using "something a user would know" and obfuscating the characters of the password by using images. Our application uses a pictograph that is more easily remembered and has improved security.

4.1 Concept and Design

To implement a password authentication method that improves upon current methods while averting threats and maintaining a low overhead, we designed an application that uses themes of pictures instead of ASCII characters. When the correct sequential combination of pictures is selected, access to the Security Organizer is granted. This organizer is a service that stores online account information, including URLs, usernames and passwords. The following sections detail the design for both the PictureLock and Security Organizer components of the application.

4.2 PictureLock

As an initial implementation, we used 12 different animal themes for the pictures. Each theme contains 12 representations of a defined animal, such as "cats", "dogs", "parrots", or "rats." At the login screen, a 3x4 grid of representations is displayed in random order. Every theme is not necessarily displayed in the initial presentation and duplicate themes may be presented. However, the application ensures that a representation of the first theme in the password is displayed in the initial presentation. This means that the PictureLock must have some knowledge of the password to ensure that the correct images are displayed. Once a picture is selected, the picture flips to reveal a new picture. Once the correct sequence of pictures is selected, access to the Security Organizer is granted.

While designing the PictureLock, we decided that we did not want to have all of the themes initially displayed for two reasons. First, if all of the themes were presented, we would be exposing our "alphabet" of themes and a user could determine the defined themes. For example, if picture 'A' is never shown with picture 'B', then they are likely in the same theme. Not displaying all of the themes together eliminates this risk. Second, by allowing duplicates or different representations of the same theme, we hoped to instill confusion if someone was trying to determine the themes. However, allowing duplicates increases the odds that the password can be guessed.

Additionally, some picture representations contain two animals, which should also cause confusion for someone trying to guess the password or determine themes. For example, one picture contains a rat on a cat's head. To someone unfamiliar with the themes, he would not know whether the representation was a part of the "rats" or "cats" theme. Only the user who uploaded the photos and set the password would know which theme the picture belonged to, thus increasing the security of the password.

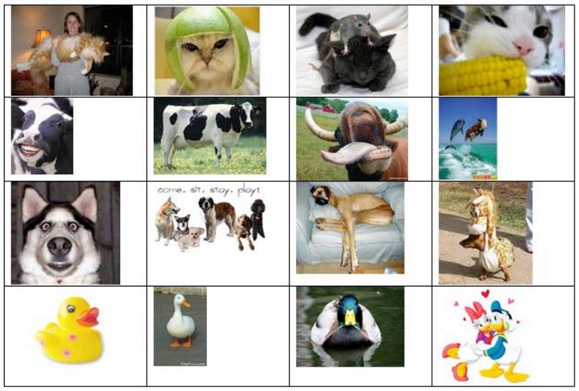


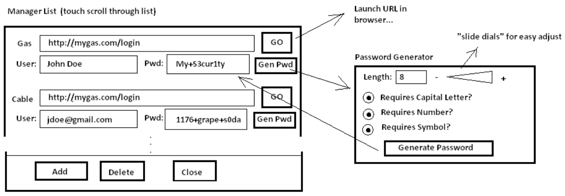
Figure 1

We also designed PictureLock so that not every theme in the password is necessarily presented in the initial display. It is possible for, say, the second theme in the password not to be in the initial display. If this happens, the second theme in the password would be revealed after the first selected picture flips over and shows a new picture. This eliminates the possibility for a user to continuously shuffle the initial pictures and guess the themes in the password by noticing which themes are always presented.

While the current implementation includes themes of animals, a production implementation of the application should include functionality so that users could upload their own pictures that having specific meaning to them. For example a user could create a theme for "family", "friends", "vacation photos", or "favorite teams" along with random photos of unknown people or objects. Thus, if a user had the "family" theme in her password, only she would know that the person in the picture selected is a family member. A 3rd party observer would not be able to differentiate between pictures of family members and pictures of random individuals.

4.3 Security Organizer

The Security Organizer is designed as a simple database that stores text fields for URL, user name, and password, for each entry or account name. It offers controls to edit, add, and delete accounts. Currently, a user needs to use the copy and paste functionality to enter user names and passwords from the organizer to online sites and to navigate to URLs in a browser. However, future implementations would use a "Go" button to launch URLs in the browser. We would also like to add the functionality to generate passwords for accounts. Figure 2 shows the design of the Security Organizer with current and planned future functionality.



Gas http://mygas.com/login
User: John Doe Pwd: My+S3cur1ty

Cable http://mygas.com/login
User: jdoe@gmail.com Pwd: 1176+grape+s0da

Length: 8

Figure 2

5. Countermeasures to Threats

The PictureLock and Security Organizer is an effective application for storing online account information. Additionally, it improves upon traditional authentication methods through the use of a pictograph alphabet. The design of the PictureLock and use of a pictograph alphabet provides effective countermeasures to the previously mentioned threats that traditional authentication methods face. These countermeasures are described in the next sections.

5.1 Shoulder Surfing Countermeasure

The use of images for a password naturally makes it more difficult for someone to shoulder surf. From a distance, the images are harder to distinguish than ASCII characters. The images are also randomly placed in the grid. So even if a shoulder surfer notices the placement of the image that are selected, he or she still does not know the password since the images will not be in the same location on the grid when the application is reopened. Additionally, if a shoulder surfer does see the images that are selected, it is not likely that the same images will appear when the application is reopened since there are multiple representations of each theme. For example, a shoulder surfer may see a user select an image of a rubber duck. When the shoulder surfer tries to select the same image in the PictureLock, he or she would be looking to select an image of a rubber duck and fail to realize that a rubber duck is a part of the "duck" theme. Therefore, he or she would not know to select the presented image of a duck in water.

5.2 Brute Force Countermeasure

Since images can be more difficultthan ASCII characters for a computer to analyze and recognize, a bot that attempts to snoop the PictureLock password can be forced to guess the password using a brute force attack. By obfuscating the alphabet, it is difficult to understand what characters are being presented and pressed. Ideally, this might reduce automated hacking performance to roughly that of an actual human. This would allow the use of shorter passwords (that are easier to remember), yet still present a sufficient obstacle for hackers.

For example, if there are 12 themes, the password length is 5, and a hacker makes 1 guess per second, then it would take up to 12^5/3600 = 69.12 days of continuous hacking to guess the user's password. Most hackers do not have the patience and dedication to do this. If the attacker has no knowledge of the theme based implementation, the attack would take significantly longer. For example if there are 12 themes and 12 images per theme, a brute force attack may take up to 144^5/3600 = 17199267.84 days.

Technologies such as Google Goggles demonstrate the ability of computers to analyze images to derive a meaning. Bots may be able to use image analysis techniques in brute force attacks to identify what the pictures are and learn the theme characters. In order to counter this, themes should be based on knowledge that only the intended user would likely know.

5.3 Dictionary Attack Countermeasure

Dictionary attacks are eliminated through the use of a pictograph. By using images, there are no characters or words on which to attempt a dictionary attack.

5.4 Social Engineering Countermeasure

Social engineering is difficult in pictograph authentication since the images are meaningful only to the user who created the password. Users are aware of which pictures and themes are in their password and therefore, if different images are presented, a false or look-alike log in is easy to detect. This decreases the likelihood that even an unaware user would divulge the information.

6. Application Pitfalls

The current implementation of the PictureLock and Security Organizer has some great features but it also contains pitfalls. Some of these pitfalls can be solved with future features. Below we discuss both the solvable and unsolvable pitfalls.

6.1 Forgotten Password

If the user forgets his or her password for the PictureLock, there is currently no way to recover it. However, not having a password recovery method ensures the security of the PictureLock and protects the data in the Security Organizer. In addition, the use of pictographs for authentication should improve the user's ability recall the password for the application. Currently, we do not intend to add a password recovery method since it may compromise security by adding another attack vector.

If users specifically requested a backup way of getting to their data, a retrieval method could be developed. For example a secure website could be set up that allows users to verify their identity and reset their password.

6.2 Unencrypted Pictures

The pictures used to represent password characters are currently not encrypted. Encrypting these images is a feature that would be important in the case of a physical security attack so that a hacker cannot get access to them to try and figure out the password.

6.3 Application Knows the Password

Another pitfall of the application is that PictureLock needs to know the password in order to ensure that it displays the correct pictures. However, a phone should not directly store any part of the password on it. The password to access the Security Organizer should be as isolated as possible. One possible solution to this is to use a one way hash of the images. Using a one-way hash for images is discussed at length in the Komanduri's research. [4]

7. Future Features

There are several future features that would increase functionality of the PictureLock and Security Organizer. The desired features are described below.

7.1 Create Multiple Databases

Users should be able to manage multiple databases. An initial screen to open an existing database, create a new database or delete and existing one would need to be added. Furthermore, once a user selects a database to be deleted, they should have to authenticate with the PictureLock and be presented with confirmation screen.

7.2 Upload, Delete, and Format Pictures and Themes

Maintaining and updating the images in the database for the PictureLock is another important future feature. This would allow the user to upload and delete pictures and themes. This would make the images meaningful only to the authorized user and prevent social engineering attacks and image analysis in brute force attacks. The user would also have the ability to format the pictures to make them easier to view. This includes controls for brightness, contrast, and rotating pictures.

7.3 Shuffle

If a user feels his or her password entry is being watched by someone else (shoulder surfing), a shuffle button could be added that randomizes the pictures to any third party observer. This is separate from the existing shuffle function which allows the user to restart the password entry process.

7.4 Null Pictures

In the current implementation, each password consists of a sequence of pictures. If a user feels they are being watched, they could select pictures that do not add to the password entry. These null pictures would lead the 3rd party observer to believe that the password is longer than it actually is. This makes the password harder to figure out and it also makes it more difficult for an observer to remember all of the images in the password.

7.5 Password Generator

Within the Security Organizer, it would be convenient to have some way that passwords could be generated at various complexities. The complexities can be controlled by a slider bar and could include options to include letters, numbers, capital letters, or other special characters.

7.6 Screen Lock

PictureLock is an access point for reaching the Security Organizer application. PictureLock doesn't have to limit itself to only this application and could be used for locking other applications as well. One obvious choice is PictureLock could be implemented as the lock screen for the phone. Unfortunately, the platform used for this implementation (Windows Phone 7) does not allow the phone's lock screen to be replaced.

7.7 Intrusion Detection System

In the event that someone obtains the phone and tries to guess the PictureLock password, an intrusion detection system could be used to detect this. To abate brute force password cracking, the number of attempts could be limited. Thus if the number of password attempts passes a set threshold, the phone would go into a timed lockout. In addition, if the number of attempts is exceeded, a notification could be sent to the owner such as sending an email.

7.8 Password Change

We would also like to add the functionality to change the PictureLock password once it has been set. This is an imperative feature that would also increase the security of the application. To change the password the user would need to type in the original password and then enter the new password twice to change it.

8. Conclusion

In this paper, we presented a new Windows Phone 7 application. The application is composed of two components: the Security Organizer for storing online account information and the PictureLock, which uses pictograph authentication to grant access to the Security Organizer. We discussed current access control methods and the threats that traditional authentication methods face. We also presented related work on the role of images in information security and the ability of users to recall images in similar pictographs. The design of the PictureLock attempts to improve upon traditional authentication methods while maintaining low overhead. The design of the Security Organizer is intuitive and stores all of the necessary information for online accounts. The PictureLock offers countermeasures to currently known threats and improves security. However, there are several flaws in the current implementation and future features needs to be added to provide additional functionality.

References

[1] Schecter et al. “The Emperor’s New Security Indicators.” In *IEEE Symposium on Security and Privacy*. Oakland, California, May, 2007.

[2] Gossweiler et. al. “What’s Up CAPTCHA? A CAPTCHA Based On Image Orientation.” *International World Wide Web Conference*. Madrid, Spain, Apr. 2009.

[3] Bai, Xiaole, et. al. “SCAP: Shape based CAPTCHA Design.” Source: Dong Xuan. Nov. 2009.

[4] Komanduri, Saranga. “Improving password usability with visual techniques.” *Bowling Green State University*. Bowling Green, Ohio, Dec. 2007.

Other General References:

Whitman, M. E., & Mattord, H. J. (2009). Principles of information security. Boston, MA: Thomson Course Technology.

Harris, S. (2010). CISSP exam guide. New York: McGraw-Hill.