GeoCapture- A two way authentication App

Apurva Abhyankar, Prasad Hirlikar

1. Introduction

With the advancements in smart phone technology, today, anything and everything can be done via your smart phone. Be it pizza order, emails cloud access or even online money transfer. With growing power of smart phones, the need for better and robust authentication techniques has risen drastically. If a malicious user breaks in to your smart phone, it can surely cause harmful damage.

Also, our additional objective is to increase the ease of authentication process by reducing the work that the user does to unlock the phone.

Thus we propose a novel authentication technique that will use the powers of smart phone itself to make it robust against malicious human intruders.

2. Related Work

In recent times there are various authentication techniques that have come up. We discuss a few important and famous ones:

a. Pin, Password and Pattern: These are the mostly commonly used techniques to unlock the smart phone. In regards to this authentication techniques, there are two issues that can be brought up.
   i. Robustness: One can easily hack into your password by shoulder surfing or even by observing the screen (At times, your finger print marks are indicator of your password). Also you have to keep changing your password regularly to keep it secure.
   ii. Ease of unlock: Although it takes much less time to put in the pattern or pin, it takes some effort from the user side. Also, for people who continuously use or check the phone for notifications, this method is not compatible.

b. Face unlock(By Google):
   Face unlock technique was introduced by Google first in in the Android 4.0(Ice Cream Sandwich). The idea was to recognize the user through the front camera every time it tries to unlock. The major flaw in the app was that the phone used to get unlocked even if a picture of the person is displayed in front of the camera. This was a major blow to the robustness of the authentication technique.
   Later, in Android 4.1.1(Jelly Bean), Google tried to overcome the previous flaw by putting in the liveliness check. Now, the user was asked to blink while unlocking the phone. This made sure that the image captured is real and not just an image of the user. Although this new version did overcome the previous flaw but even then, it is breakable. A simple use of photo shop can help you close the eyes of the image. All one needs to do now is to switch between the images while displaying it to front camera. By this method one can easily unlock into the phone. Here are two links to the video o that break through both the version of the face detection unlock technique:
   i. Bypassing android
   ii. Facial Recognition

c. Touch ID(By Apple)

Introduced apple in iOS 8, apple introduced touch ID which was a huge leap in cell phone security. The phone could identify the user by detecting the fingerprint when the user places its hand on the home button. This is by far one of the most sophisticated techniques and also highly robust. Biometric means of authentication have always showed that they are much robust than the pin and password techniques it is not easy to duplicate and neither it can be lost since you carry it with you.

The issue with Touch ID is that it is only limited to apple products and not to android. It is going to be difficult for google to replicate touch ID on android phones since absence of home button and using finger print detection via image scan would make it less robust and vulnerable.

3. Proposed Work

After discussion with the Professor, we came up with the idea of using a location and the environment as a password. As mentioned before our objective is not only to give a robust authentication technique but also provide a user friendly technique.

MAIN IDEA (Novelty): The password to unlock will change according to the location of the user and that password will be a particular image of an object that is specific to that location. The object will be detected by capturing the image from back camera and using simple object recognition algorithms.

Let us consider a use case to understand the procedure better: Let's say, a person is sitting in his office. His office has general objects such as a laptop or a white board or even a photo frame of his family. Now, our application will know that the current location of the user and for the current location it will be pre-defined that it is office. Thus, while unlocking the cell phone, our app will look try to look for the object (using the camera) that the user has predefined for his office environment. Similarly, when he is at home, the object to look for will be different.

The reason for such an approach is that it is user friendly. The user will have to just press the unlock button by pointing the camera towards the object. Also, it tries to combat shoulder surfing since other people will be unaware that that the camera is being used. Also the object to be detected will be different for each location. As an addition, if the object recognition fails, we can set a location specific password that is a password according to the location.

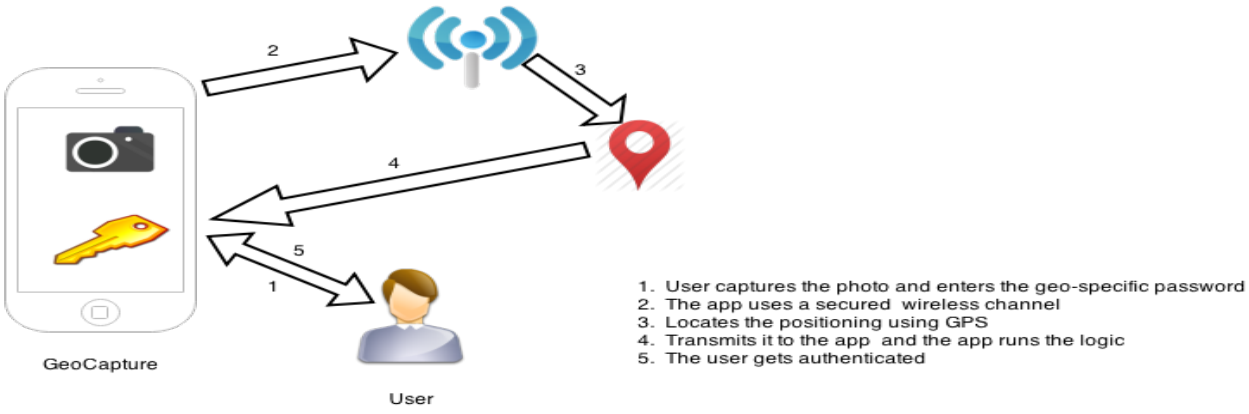
The approach of going about this project would be to first fetch to GPS location of the cell phone and try to set a certain location (example office, home). Thus every time the app collects the longitudinal and latitude data, it should detect if the cell phone is in a known place.

Also, in parallel, we can research on algorithms that can help in image matching. We will have to look for an algorithm that can process the image very quickly and provide results on whether it contains the object in the pre stored image. Also there, might be multiple objects for same location. Thus, it is more important for the algorithm to be fast than accurate. Once that is done. We can look at integrating both the modules and see if the outcome is feasible enough.

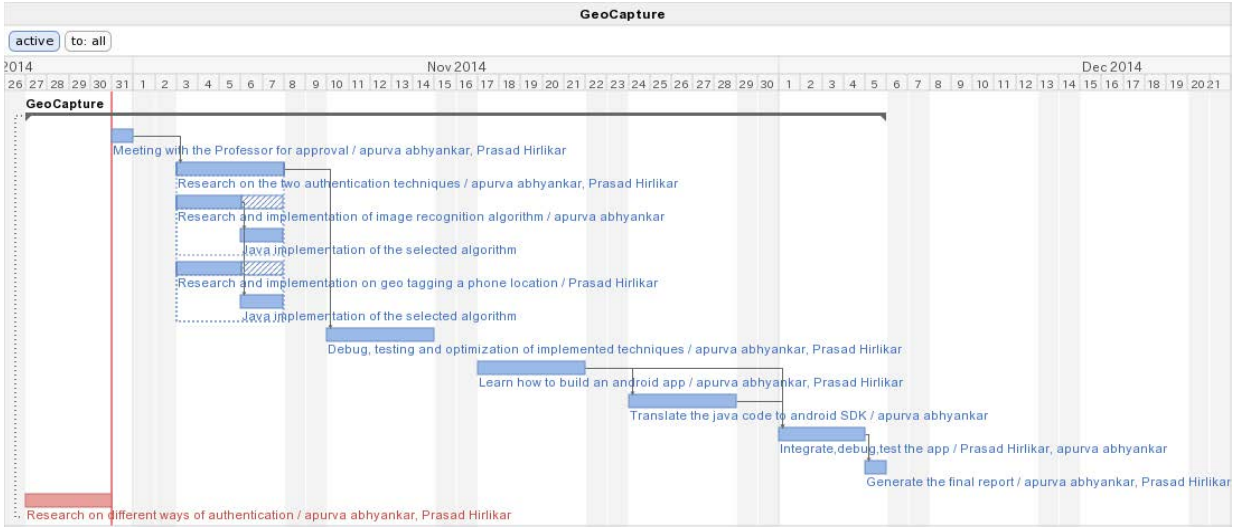
4. Expected Outcomes

We believe that the first step in secure an ecosystem starts from the user device itself. The more the user feels safe while using the device, more he will delve in the system and use it efficiently. For s secured system, user identity is very important and it is important to hide or protect the device from any kind of malicious attack. In this project, we ambitiously attempt to create an authentication technique which aims at making the device more secure by thwarting any malicious attack by any person which is not the authorize user of a device. To make the authentication technique, we make it robust by making it a two-step process. When the user wants to access his device, he will be authenticated by our app. The app will detect a specific image the user has provided for authentication. The image will be authenticated based on the location of the user. The user then has to enter the geo-specific password. If both the authentication techniques are successful, the user will be able to access his device.

Thus, we show that two-step authentication helps in detecting the authorized user increasing the security of the device, user data and identity.



Block Diagram



Timeline