# Mobile Device Authentication Instruction Manual

Contents

[Mobile Device Authentication Instruction Manual 1](#_Toc437328876)

[General Overview 2](#_Toc437328877)

[Deployment \ Installation 2](#_Toc437328878)

[Deployment 2](#_Toc437328879)

[Installation 4](#_Toc437328880)

[Overview 5](#_Toc437328881)

[Walkthrough 5](#_Toc437328882)

[Modify and Set the Accepted Tap Sequence 6](#_Toc437328883)

[Data Exportation 10](#_Toc437328884)

# General Overview

This document is summary review instruction manual for the Mobile Device Authentication application for the Android phone. The application was built using the Java framework with Android Studio as the IDE.

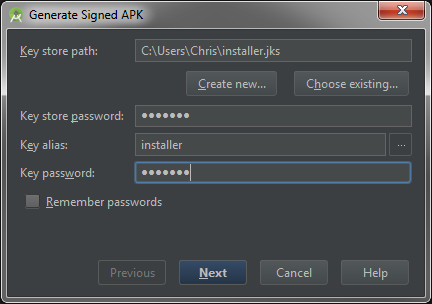
# Deployment \ Installation

In order to deploy and install this application, follow the steps below.

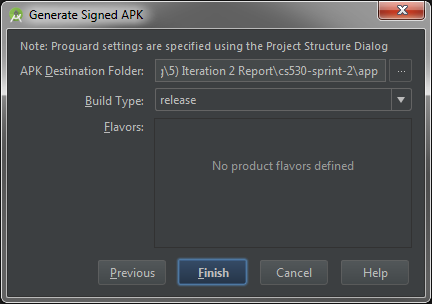
## Deployment

When the code in Android Studio is ready to be compiled and used, follow the steps below for building an APK installation file.

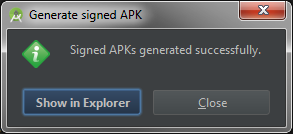
From the main menu, go to Build 🡪 Generate Signed APK. You should arrive at the window shown below. Here, you’ll need to specify a Key store path on the machine either by choosing an existing directory or creating a new one. If you are specifying a path for the very first time, you will need to set up a password.

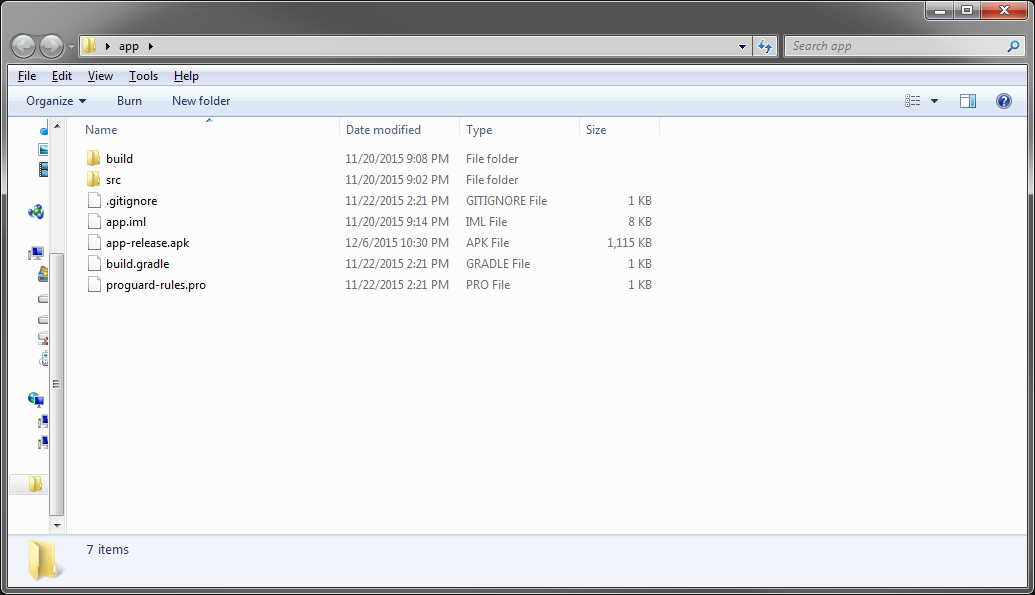


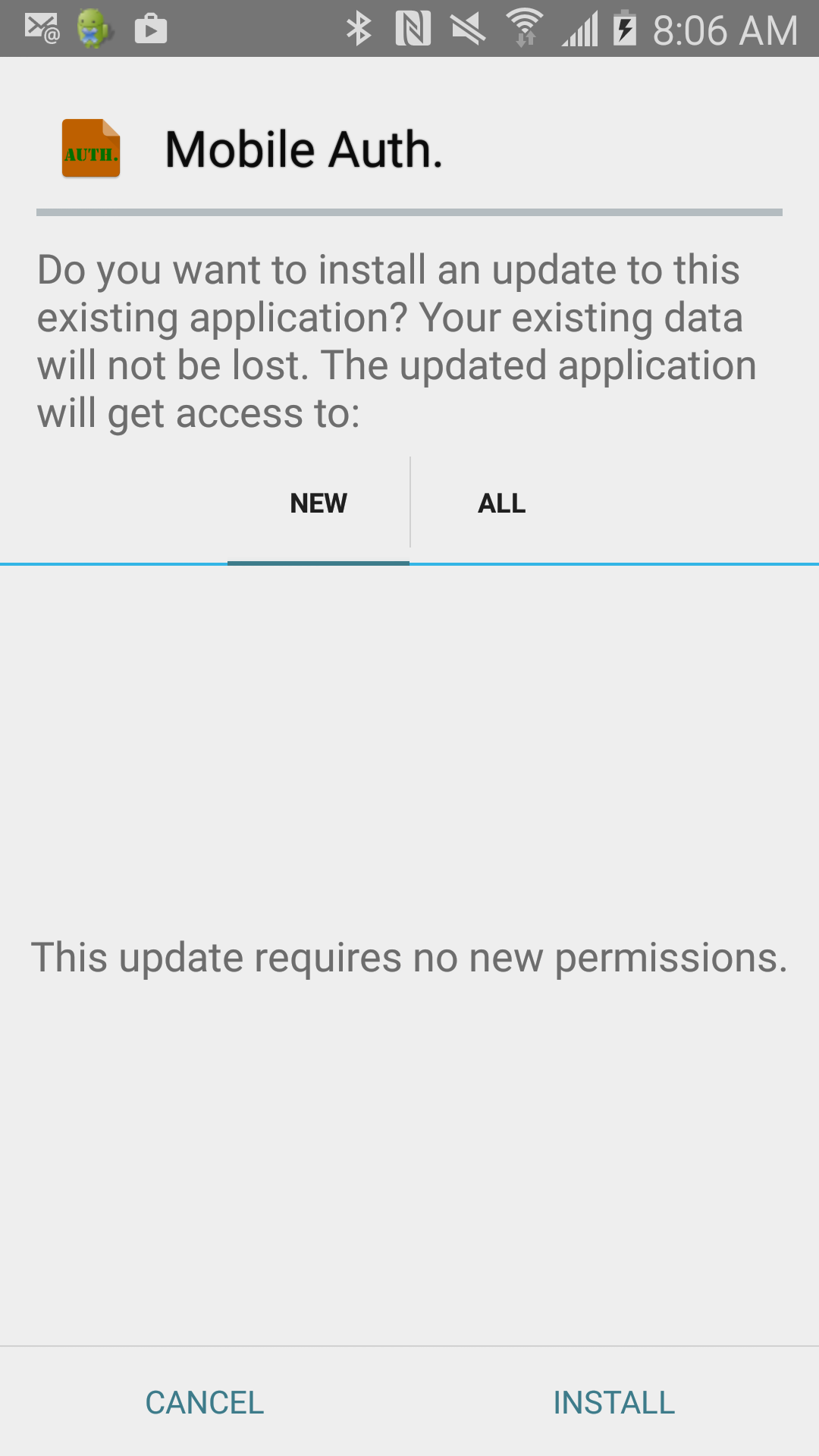
Once you select a path, click on next. On the following window, specify the destination folder. Leave the build type as ‘release’. Flavors are optional.



Click on finish. If Android Studio successfully created the APK file, then you should now be able to see it in the destination folder of the host machine. You can click on the ‘Show in Explorer’ button to see it:







## Installation

In order to install the application, connect your Android to the host machine via USB port. Once connected, copy and paste the ‘app-release.apk’ file to a location on the phone of your choice.

Once the APK file is on the phone, navigate to it from the actual phone (not the host machine that created the APK file), and open it to start the installation. NOTE: you may need to set some security settings on your Android to allow it to install applications that are not originally from the App store. Simply follow the on screen prompts to install the application.

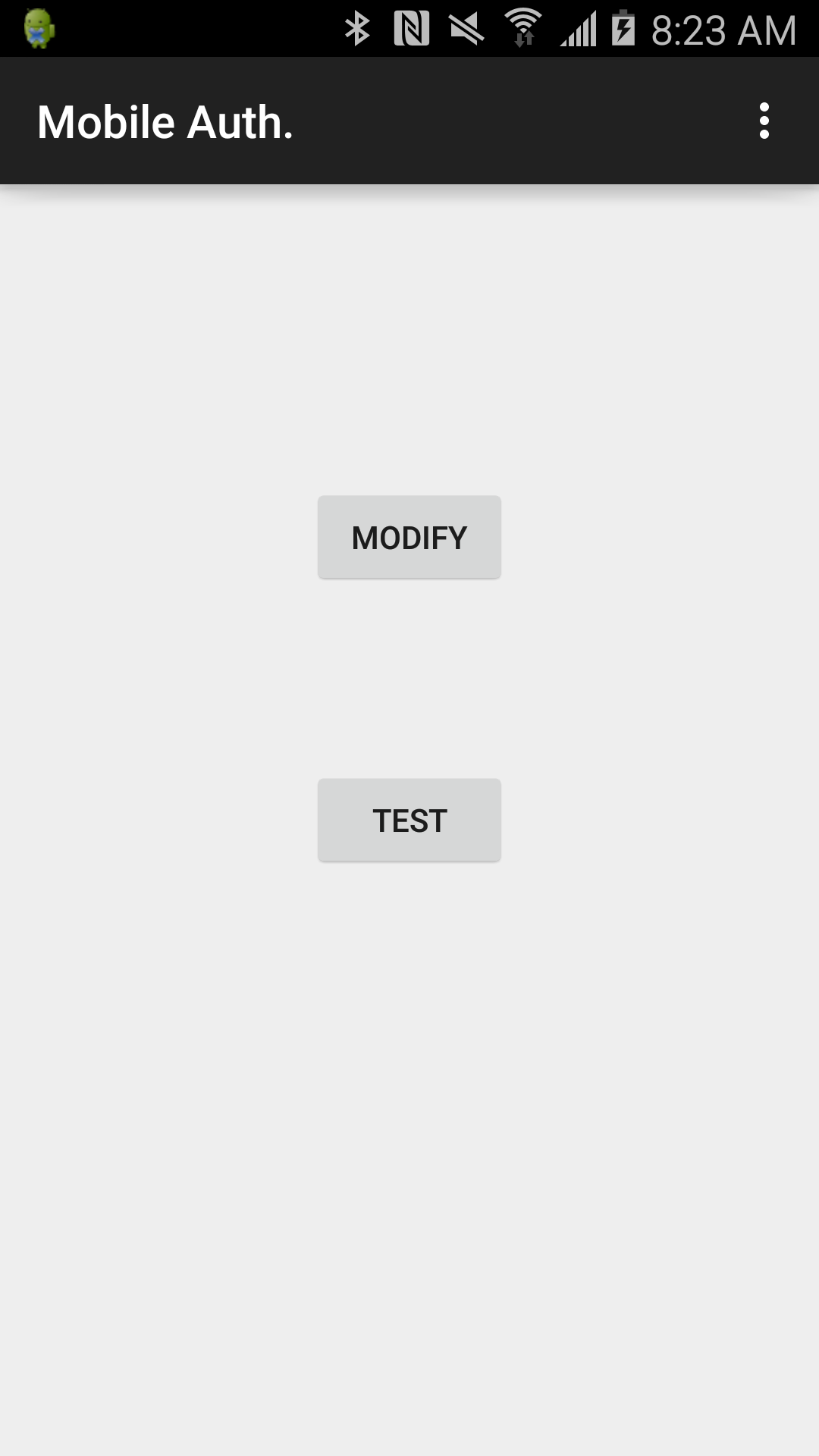
# Overview

The mobile authorization application is an application that can be used as a simple security interface on top of any phone application, or entry into the phone itself. The program is currently not tied to any direct application or phone in general, rather it is used to demonstrate the how it could be used for such reasons.

The application doesn’t use the common user name and password authentication process that is commonly used. Rather, it works by accepting a tap sequence from the user. The user is required to tap in a sequence pattern that will be remembered by the application. Then on future login attempts, the recorded pattern is compared to the pattern that the user is currently entering. If they match, access is granted. If not, then access is denied. The most important feature of the tap comparisons is not the location of the tap sequences on the phone screen, but rather the timing between each sequential tap.

Finally, the application will actually offload the data stored on it for the recorded tap sequences. The data is sent off to a CSV file that can be opened in Excel for viewing or audit purposes.

# Walkthrough



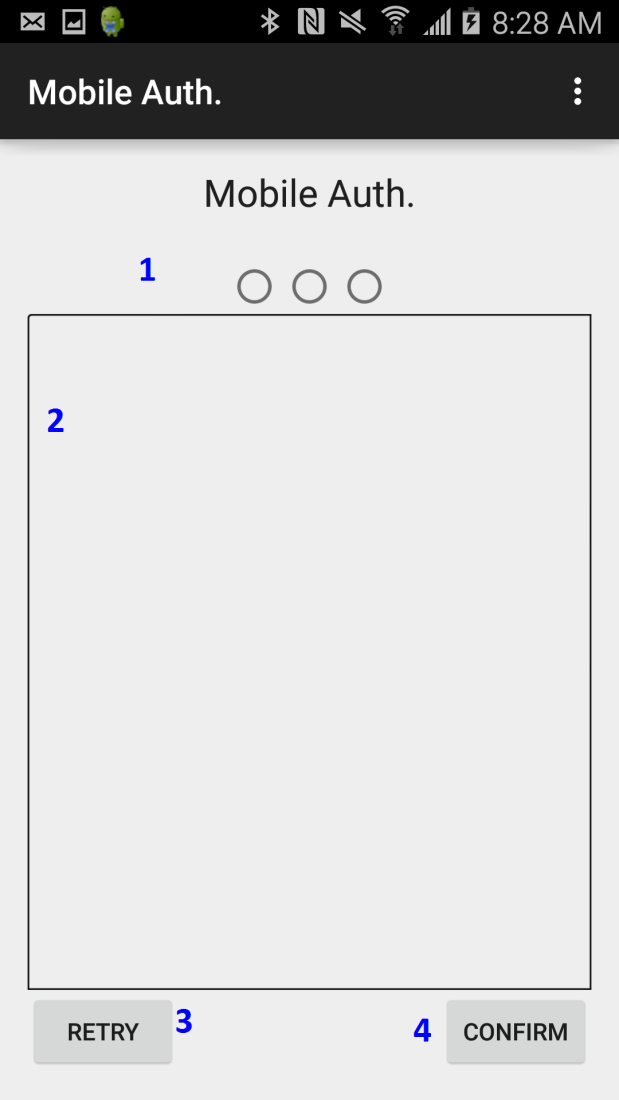
When you first start the application, you have two options 🡪 Modify and Test as shown here. Since this is probably the first time you are starting the application, click on the Modify button.

## Modify and Set the Accepted Tap Sequence

On the Modify screen, you will need to enter the tap sequence that you want to be captured as the authentication sequence. Please note two important things:

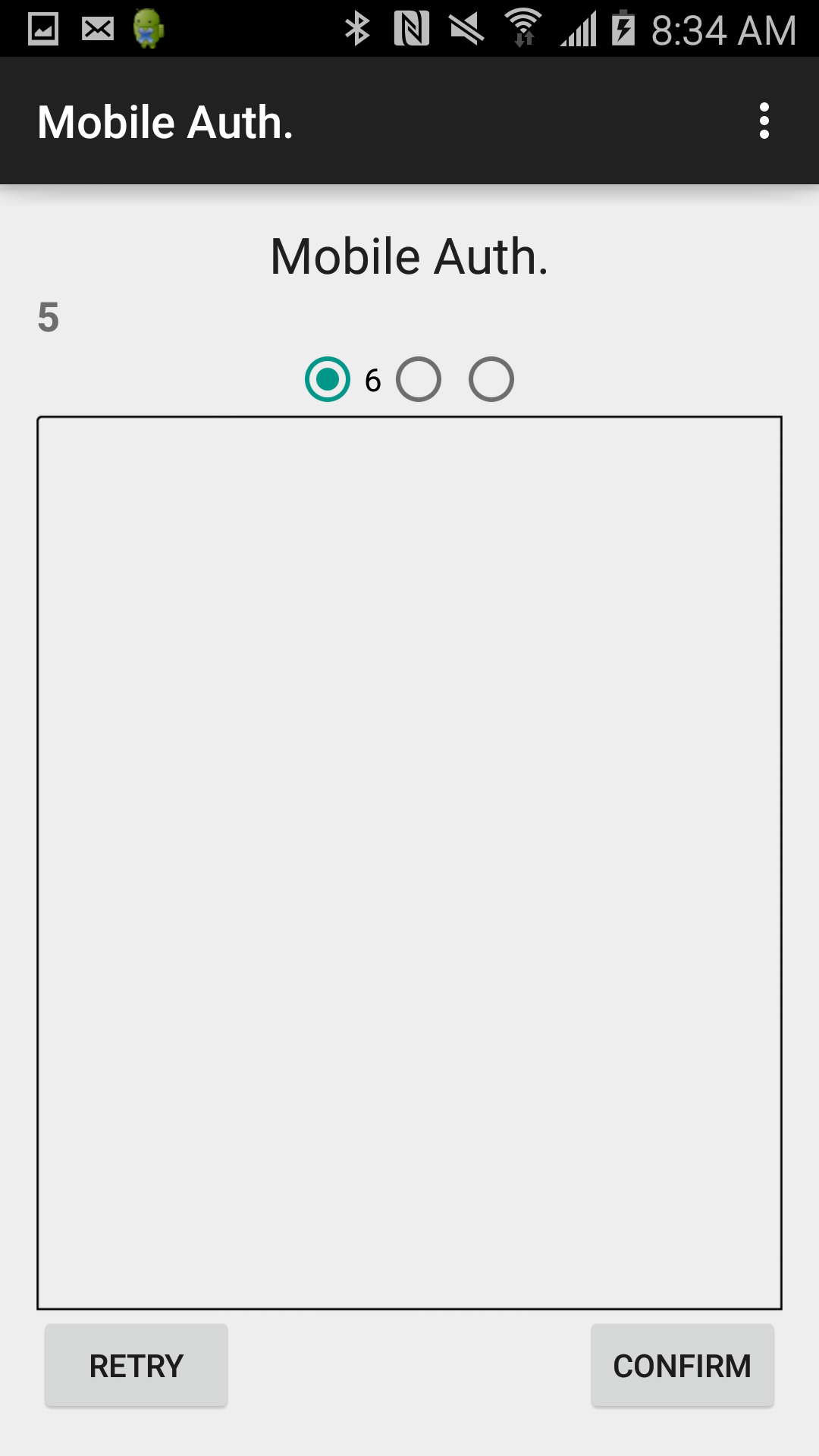
1. The sequence that you choose must be entered three times in total.
2. The sequence that you choose should be near identical for each set you enter. Otherwise, the authentication process will not be able to successfully compare future patterns.

Shown below is the Modify screen, along with what each part is doing.

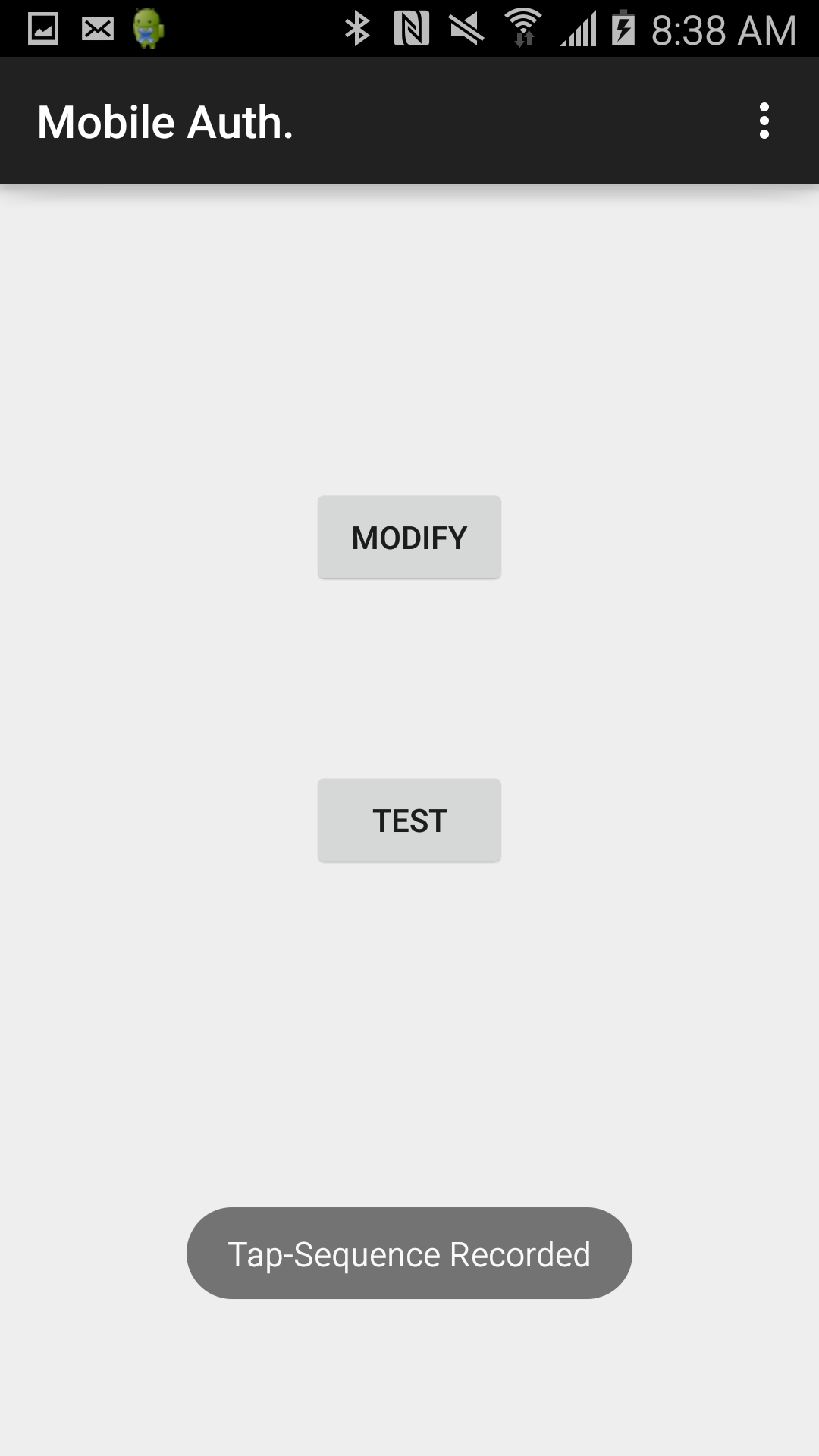


1. This is the radio button set that represents the three tap sequence sets that are entered by the user. They will all be turned on when done.
2. This is the entry plane on the surface for capturing your tap sequences.
3. This is the retry button. Use this to erase any captured tapping and tapped sequences and to start over.
4. This is the conform button. When you are done entering a sequence, press this button to save it.

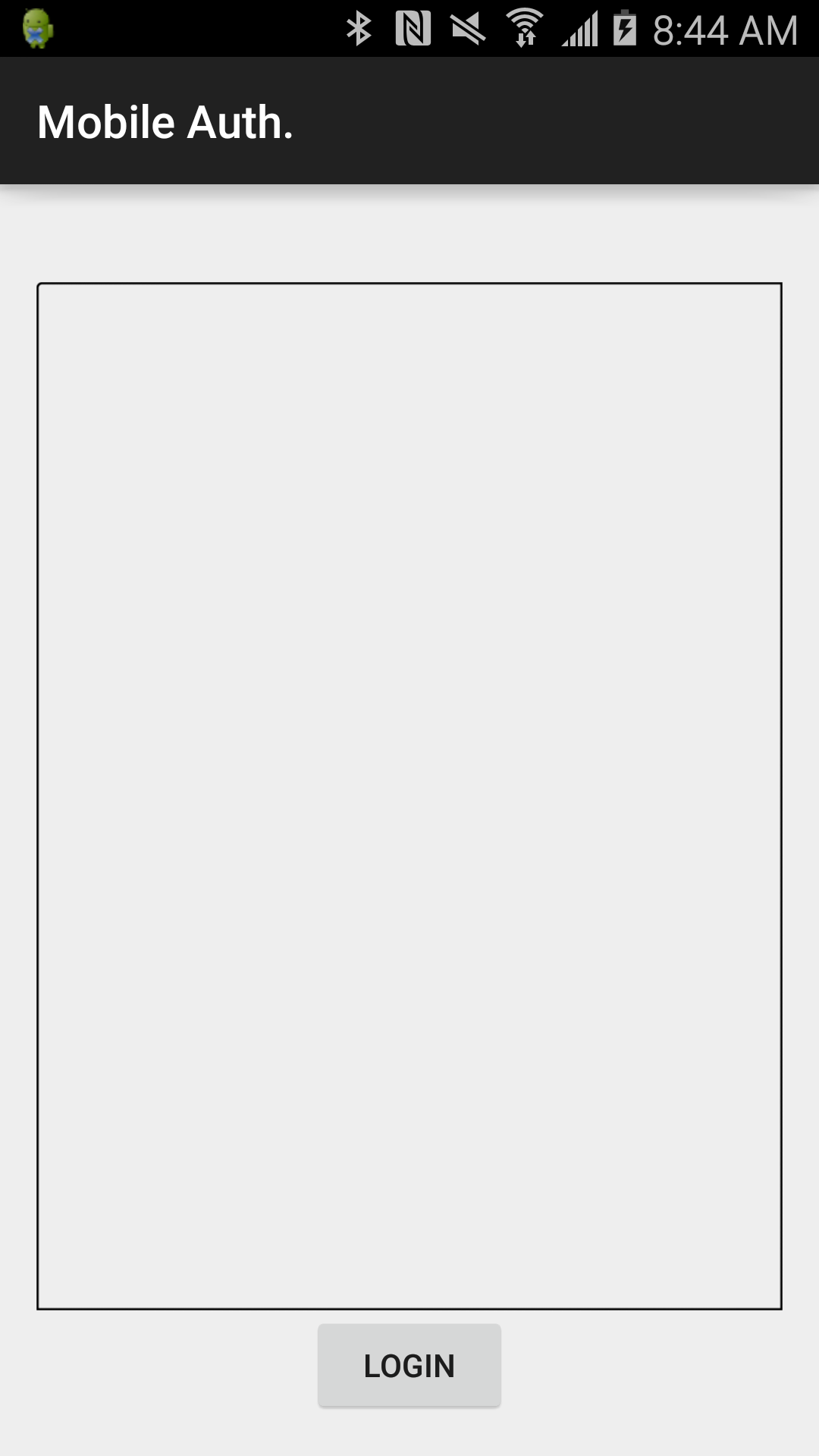
Shown below is the recording of the tap sequences in the middle of recording them. Notice the radio set filling up showing the number 6 for the count of tap sequences entered for the captured confirmed sequence. Also notice the number 5 representing the current taps that have been entered for the current sequence.



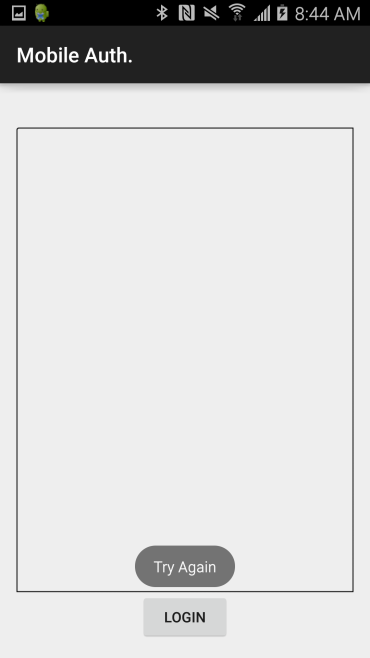
Once all three sequences have been entered, you will arrive back at the start of the application, and you should receive messages that the tapped data sets have been successfully captured and that they are ready to be used. Also, you receive a message that the data was successfully exported out to a CSV file.

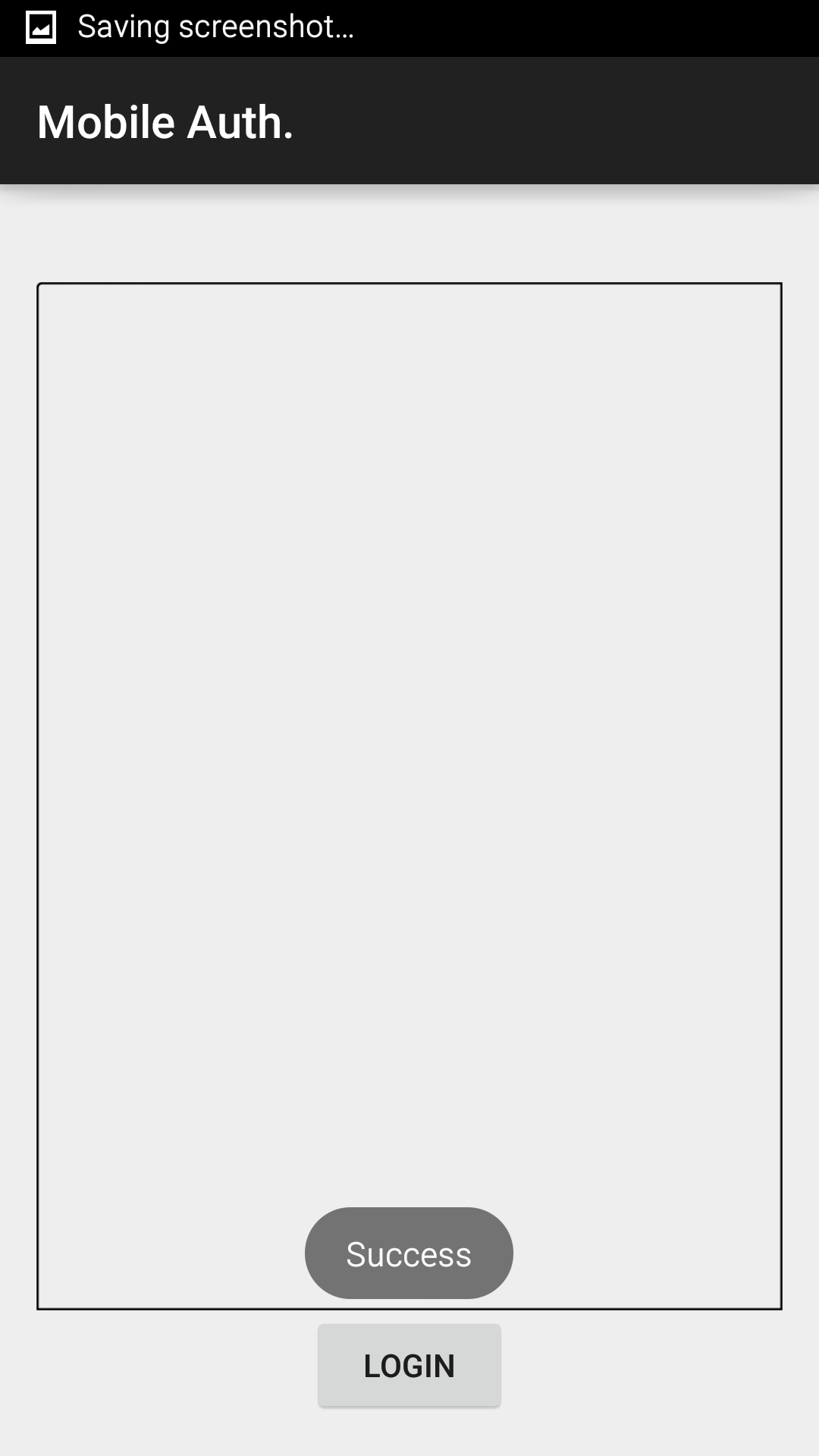


At this point, you can now click on the Test button. This part of the application is now the interface that will be used for authenticating a login attempt.



Enter the tap sequence, and when you are done, click on the done button. If the sequence entered by the user matches with a high precision rate, the application will show ‘Success’, otherwise, it will show ‘Try Again’ as both are shown below.





## Data Exportation

The recorded tap sequences that were used by the application as the pattern to match to are sent off to the ‘Mobile Auth.’ directory on the phone. The phone will create the directory if it doesn’t exist in the root. Shown below is a sample CSV file open in Excel that was created by the application.

