Homework 4 (Due 12/11 Monday)

Introduction:

Many social network apps and location-based services require or encourage users to post their geo-location information. While enabling interesting features in mobile applications, disclosing location information may lead to privacy breaches.

In this homework, you will explore the location privacy issue in mobile applications. The demo app has two tabs: USER and ATTACKER. In USER tab, the app mimics the movement of a user and posts messages at a set of pre-defined locations associated with the location information. In ATTACKER tab, the app displays the view of an attacker after crawling the user's messages with the location information. Then you will identify the privacy issues and explore the possible mitigations by using geofencing and adjusting the location granularity in user reports.

Objectives:

1. Understand how to load GPX/KML files with a sequence of mock locations in Android emulators to test with user mobility.
2. Understand the privacy threat of posting location information.
3. Investigate two mitigation/defense schemes, enforcing geofencing and adjusting location granularity.

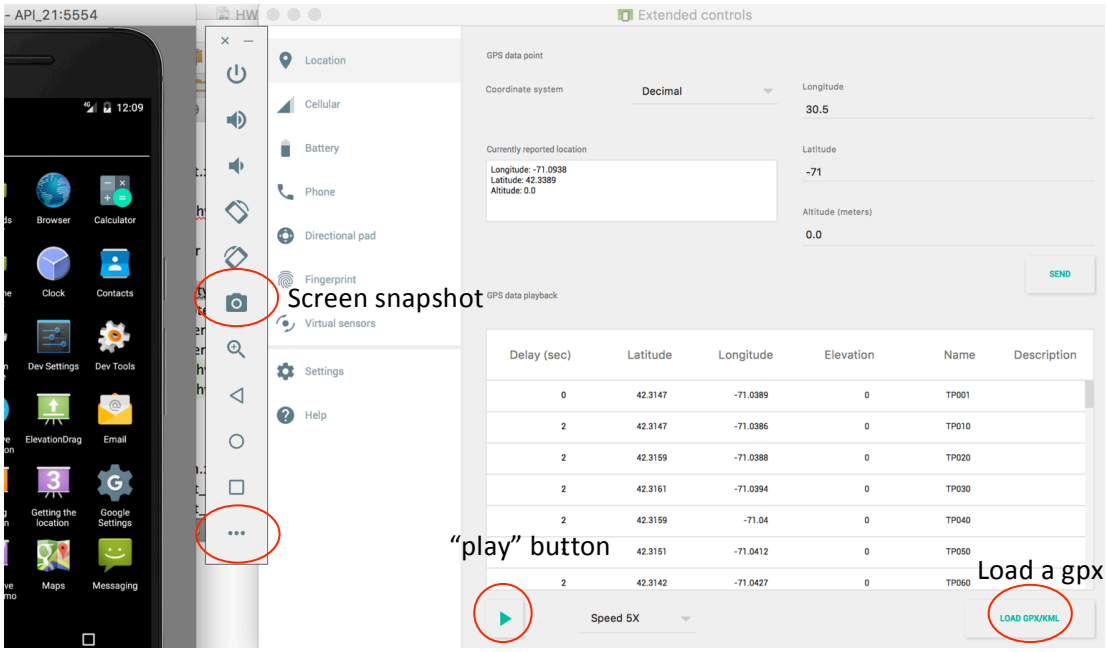
Detailed Steps:

Download **hw4_base.zip** and **Quinn2MFA.gpx** from the course web page. Upzip hw4_base.zip, and open it in Android Studio. Compile it and run the app in your emulator.

1. Open the app, choose USER tab (default tab), and check "Coordinate" option. This is the default option for reporting the geo-location with the messages where the exact GPS coordinates will be attached with each message.

2. Load the provided gpx file (Quinn2MFA.gpx) into the emulator (see the figure below). This file includes a sequence of GPS coordinates, and will be used to emulate the user's movement. You can select the play speed, and then press the play button (the green triangle). The GoogleMap fragment will show the movement of the user. Along the movement, you will see some toast messages indicating that some messages are posted by the user with the location information. In this app, those message/location data are actually stored in a file ("/sdcard/Download/data.txt").

3. When the movement stops, you can switch to ATTACKER tab, and click "Update" button. You will see 7 markers representing the messages that the user posted and have been crawled by the attacker. Apparently, the attacker can easily trace the movement of the user.



4. Next, you will try two mitigation schemes to protect the location privacy. Assume the user consider "JFK/UMASS Station" and "Boston Medical Center" (message 3 and message 5) are two sensitive locations that shouldn't be disclosed to others.

5. **Geofencing**: Switch back to USER tab and select "Geofencing" option. In this option, the app will setup two circular regions as geo-fences. Once the user enters the regions, the app will not post any messages to protect the location privacy. In this app, the two center points have been hard-coded to be the location of "JFK/UMASS station" and "Boston Medical Center". You need to type in a radius value (in the unit of meters) and press the button. The GoogleMap fragment will show the two regions. Then repeat the user movement in step 2 (the gpx file should have been loaded, and you just need to press the "play" button to start). Repeat step 3 and observe from the attacker's view. Adjust the radius value and repeat this step. Find the appropriate radius values for protecting each of the two locations, and answer question Q1.

6. **Region:** In the "Region" option, every location will be reported as a circular region. The center point is randomly selected and its distance to the actual location is no longer than the radius. Type in a radius value and press the button. And then launch the movement process again (step 2). When it ends, repeat step 3 to observe the disclosed location information. Adjust the radius value and answer question Q2.

Submission:

Complete the answer sheet and rename the file as

your_firstname.your_lastname-hw4.docx

And email it to the TA (SonNam.Nguyen001@umb.edu)

Answer Sheet

Our goal is to prevent the attacker from realizing that the user has visited the two sensitive locations: (**loc1**: “JFK/UMASS station”) and (**loc2**: “Boston Medical Center”). Think about the possible strategies that an attacker may use to make a conclusion/guess based on the available location information.

Q1. When using Geofencing scheme, what radius value can protect loc1? What radius value can protect loc2? Why? (Please attach two screen snapshots, one for each case, from the ATTACKER tab)

Q2. When choosing Region scheme, what radius value can protect loc1? What radius value can protect loc2? Why? (Please attach two screen snapshots, one for each case, from the ATTACKER tab)

Q3. Compare loc1 and loc2, which location is easier to protect (i.e., harder for the attacker to identify), and why?

Q4. Compare Geofencing and Region options, which scheme do you think is more effective for protecting the location privacy and why?