**CSCI 578 Homework 3**

Steps that were followed as part of this assignment:

1. Used COVERT to analyze a collection of 20 apk files, out of which, four apps belonged to me that were used in Assignment 2 to show attacks, and remaining 16 apps were downloaded from the resources given. The XML files generated by Covert are attached.
2. A python script ‘Parser.py’ was run on these 20 XML files to generate 20 JSON files with all the parsed data. It extracts all useful data such as Application Name, Components, Permissions, Intents, Actions and Senders.
3. Script ‘Interactions.py’ is used to parse all 20 JSON files and compare the Intents with Actions to find all the interacting components.
4. Myindex.html uses D3 library to generate a visualization from the data in the JSON file generated in the above step.
5. The visualization consists of 20 apps. Each app has its components and permissions shown. Hovering the mouse over each app, component and permission shows its name. All the components that interact with each other are joined.
6. There are 4 images attached for the visualization.
   1. Image1 shows an overall image of all 20 apps with its interactions.
   2. Image2 shows the name of an app SetWallpaper when mouse is hovered over the blue box.
   3. Image3 shows the name of the component when mouse is hovered over the white circle.
   4. Image4 shows the name of the permission owned by that app.

Instructions for running the code:

1. Parser.py takes in one XML file at a time, which is specified in line 6 of the code. Run this file in the terminal using

python Parser.py

1. Interactions.py takes in all 20 JSON files and all 20 XML files as an input array, specified in lines 6 and 10 of the code. Run this file in the terminal using

python Interactions.py

1. Open myindex.html in Google Chrome or Safari browser. (The entire image is best viewed on Google Chrome at 25% zoom.) (The D3 tooltip functionality does not seem to work on Firefox browser.)

Observations made:

1. Most of the inter-app communication takes place among larger apps such as Facebook, Twitter, Google Calendar, Go Weather, UC Cleaner, etc.
2. My malicious app AudioRecorder interacts through intents with Twitter and Facebook. This is an example for intent spoofing that may take place.