CSCI 578 – ASSIGNMENT 0.5

Deadline: by 9am on Wednesday, February 3
Submission Information: Use Assignment 0.5 dropbox on D2L

GETTING TO KNOW ANDROID

In this assignment you are going to get to know about Android and its design, as well as its application structure. You can see an overview of Android architecture, already shown in class, in the diagram below. Our focus in this assignment is on the Applications and Application Framework layers. Application Framework in Android provides third-party developers with a set of tools, libraries, and APIs that allow them to design and implement their application in Android’s ecosystem.

To ensure security of the system, Android maintains a mutually distrusting relation between applications in the systems. It runs each application in its own sandbox, an isolated virtual machine. However, this does not mean that applications cannot communicate with each other.

Android’s application communication model further promotes the development of rich applications. Android developers can leverage existing data and services provided by other applications while still giving the impression of a single, seamless application. For example, a restaurant review application can ask other applications to display the restaurant’s website, provide a map with the restaurant’s location,
and call the restaurant. This communication model reduces developer burden and promotes functionality reuse. Android achieves this by dividing applications into components and providing a message passing system so that components can communicate within and across application boundaries.

Android provides a sophisticated message passing system, in which message objects called *Intents* are used to link applications. An Intent is a message that declares a recipient and optionally includes data. An Intent can be thought of as a self-contained object that specifies a remote procedure to invoke and includes the associated arguments. Applications use Intents for both inter-application communication and intra-application communication. Additionally, the operating system sends Intents to applications as event notifications. Some of these event notifications are system-wide events that can only be sent by the operating system. We call these messages system broadcast Intents.

Intents can be used for explicit or implicit communication. An explicit Intent specifies that it should be delivered to a particular application specified by the Intent, whereas an implicit Intent requests delivery to any application that supports a desired operation. In other words, an explicit Intent identifies the intended recipient by name, whereas an implicit Intent leaves it up to the Android platform to determine which application(s) should receive the Intent. For example, consider an application that stores contact information. When the user clicks on a contact’s street address, the contacts application needs to ask another application to display a map of that location. To achieve this, the contacts application could send an explicit Intent directly to Google Maps. Alternatively, the contacts application could send an implicit Intent that would be delivered to any application that says it provides mapping functionality (e.g., Yahoo! Maps or Bing Maps). Using an explicit Intent guarantees that the Intent is delivered to the intended recipient, whereas implicit Intents allow for late runtime binding between different applications.

Since Intents are exchanged between application components, we call this type of communication *Inter-Component Communication (ICC)*. To know more about components, you can look at the Android documentation on components. Alternatively, you can take a brief look at the Android applications overview. This type of communication is the result of design decisions that Android system architects have taken. As we know, a design decision may have deep effects on various aspects of a software system. One of them is security. In this assignment, you are going to find some security issues caused by Android's communication methods. These security issues can be exploited by attacks that are called *ICC attacks*.

### DELIVERABLES

Using the material mentioned above and in the class, try to find *at least two vulnerabilities* in the Android operating system that are caused by its architecture and, specifically, by the ICC mechanism it supports. You should

1. include a diagram for each attack
2. describe the diagram in detail, as follows:
   a. explain where each component resides (what type of application)
   b. explain how this attack can affect users and their data
   c. discuss whether this attack can be stopped and how

An example of the kind of diagram you should produce is provided below. Terms such as “broadcast” and “implicit invocation”, used in the below diagram, may not be entirely familiar to you (although you
should have heard them before). All of the terms you will need are discussed in the Android documentation you will review as well as in Chapter 4, which we will cover next week.