CSE608 Project 2
Exploring Attack Surfaces in Android apps

[Background]

As mobile devices becoming one of the most popular personal computing platforms, attackers have come to realize the tremendous value they could gain by attacking these privacy-intensive, constantly-connected, and application-rich devices. In this project, you will have a chance to position yourself as an avid hacker who is set out to identify and exploit the attack surfaces that are exposed by common Android applications and preferably unique to Android or mobile devices.

[Scope and Goals]

Not to further limit your imagination, the scope of this project is loosely confined within the following three possible attacking targets:

(1) Web elements in Android apps;
(2) Native code and libraries in Android apps;
(3) The middleware layer (i.e., the java layer) in the Android OS.

You should select one (or more if you feel passionate) from the above targets as the base to start your investigation and exploration. The goals include, but are not limited to:

(1) A PoC (proof-of-concept) of your brilliant attack;
(2) A design and a rough implementation of a security mitigation that addresses certain non-trivial attacks (could be known previously);
(3) A comprehensive survey of previously known and unknown security flaws and exploitations;
(4) A comparison study of

[Deliverables]

You are supposed to turn in an academic-style technical report that describes your concrete goals, approaches, findings, designs (if any), related work, and conclusions. You should also submit your code, if any, along with the report.

[More note]

This project is intentionally made to be open-ended in the hope of exercising your skills of identifying open problems in reality and searching for solutions or conducting research on them. Although this is an individual project, it may later lead to collaborations among students who happen to study very related topics and want to extend their work together. The possible collaborations will be decided after this project is turned in. As always, please direct all your questions and discussions to BlackBoard.

[Android apps for experiments]

I provide a set of 200 free Android apps (*.apk) to you under the condition that you will never distribute any of the app outside of the class or use it for any purpose other than this project. If you agree on this condition, you can download the them from here:
http://ris3.cs.stonybrook.edu/cse608_200_apk.tar.gz

[Other Useful Resources]

http://developer.android.com/tools/index.html
http://developer.android.com/tools/sdk/ndk/index.html
https://code.google.com/p/android-apktool/
https://code.google.com/p/androguard/
http://source.android.com/