Josh Levy – EECS 349 HW3 P2 Lab report

This activity demonstrated that it is potentially possible for an app that does not have any elevated permissions to activate functionality in another that has permissions granted. I do not believe that this demonstration on its own is necessarily security vulnerability, however, because it still requires the user to activate the functionality from within the original app. This means that unless the malware app is able to somehow prompt the user into doing something potentially harmful, it cannot execute any attack.

I did see one note in the android developer documentation that noted it was considered a best practice to prefix the entries of extras in intents with the name of your app to avoid potential naming conflicts with other apps. This seems to imply that it is possible for other apps to modify the data in intents that your app creates, and I would be interested to see if this is a possible vector for an attack.