Puzzle
April 6, 2018

It was recently claimed that the Facebook app on Android phones accessed messages sent through other apps, and uploaded them to Facebook. This occurred because the Facebook app was not appropriately confined.

This problem is not unique to Facebook's app. Most apps request access privileges to data and hardware devices on smart phones, without specifying what specific data or hardware they need to access to perform their task.

1. Why do you think app designers don't request permission for each set of data, and each device, the app needs to access?

2. In many cases, users can disable permissions. Why do you think users didn't do this with the Facebook app, and generally do not do this with other apps?

3. Why should the access provided to apps be the minimum needed to carry out their task?

4. How would you handle cases where the app needs to send the location of the phone to a server at a particular point in time, but not at other points in time?