**EMCS2430: Human Factors: People and Software**

3. Permissions in iOS and Android

Brian Russel Davis, [brian\_davis@brown.edu](mailto:brian_davis@brown.edu)

Part I: Combining Permissions  
Combinations of permissions are especially important. Why? Can you give an example? Wear your “attacker’s hat” to think about how you might exploit a combination of “innocent” permissions to create something malicious.

Any app that is asking for permission to read information from the user’s personal data and act on behalf of the user is very dangerous. I have seen this in action on many apps. The app wants permission to read text messages for example so the user doesn’t have to copy a verification code. But then all wants persmission to access the file system to add files, read files, etc. So the app can now message an attack and then save it to the file system?   
  
Part II: Approaching the Problem of Permissions  
You already may, or may someday, supervise a team that builds apps. What principles should your team follow? How would you go about formulating a “statement of principles” for how they should approach the problem of permissions?

The first principle is the idea of being user-centric and creating some sense of empathy. Imagine if this was your phone number, user id, ss# that we were passing around from REST call to DB and from DB to wherever. Second engineers ( just like product managers ) need to understand the Job-To-Be-Done. What “job” is the user trying to do. If we think about this task without technology and apply technology in the context of making the task safer, faster, more accurate or more efficient.