I article I investigate was “Mobile Attacks and Defense” by Charile Miller. The point of this article was to explain why and how an attacker could attack either an iOS or Android mobile phone. The author argues that because phones are so powerful now and hold such personal data they are tempting for a hacker to attack. He then goes on to describe what sort of defenses each platform has against attacks. They both have a centralized place for app downloads, but they are implemented differently. iOS probably being the more secure because it requires signed code from Apple to run on a device. Another really interesting thing that they use is sandboxing. This is where the operating system only allows the application to access certain parts of the phone. I have owned both kinds of phones and never really knew that they did this. Apple has a set of rules that all applications play by while Android gives more flexibility to the app and in exchange requires the user to permit the app to access those parts. This technique of sandboxing seems like a really good idea that would help prevent malicious apps from being able to access very much. I think that is very important because of an attacker isn’t able to access very much, they might not even try to attack it in the first place.

I learned a lot that I didn’t know in this article. I knew about the marketplace restrictions by Apple and I knew that Google didn’t really put these restrictions in Android, but I didn’t know about the sandboxing technique. I have heard about sandboxing for web browsers on PCs though. It seems like a very powerful security
method to prevent much damage from being done. I think that is the most interesting part of it, it doesn’t really attempt to block access or to make it super hard to get in (although I am sure there are many other measures that do try to make it that hard). It simply restricts access when you are in so it doesn’t matter so much if someone did. It would be like a desktop operating system allowing a guest login but not being able to launch applications, browser the file directory, or change any settings. This is a pretty advance technique but I could use it in software I write to allow for communication to the outside, but only allow someone to touch my product instead of allowing them to get further into the operating system.

I would be curious, however, to see how this affects Apple’s developers. It seems like since iOS takes the approach of one size fits all and allows all applications the same access to things, that there might be some difficulties in developing legitimate software for the device. I could see how this could be a concern. I would also be curious to see how many Android users simply just click through the messages about allowing or denying an application from accessing certain parts of a phone. Certainly it could be a powerful tool, for example the author points out that a Tetris game that needs access to the Internet would seem fishy. But at the same time it could be a real feature in a valid game. It could be used for sharing high scores, so it could be hard for the end user to be able to make the call as to whether the problem is good or malware. The other big question that I have is how many attacks are actually occurring at this present time. I recall reading an article saying that within a rather short period of time an unprotected computer that was connected to the Internet would become infected. I wonder if this rate of attacks are happening on these phones, or if the attacked simply
are quite there yet. There is no denying that they will come, I merely wonder if they are present already. If they are happening then there for sure is call for concern and the issue needs to be monitored closely and action needs to be taken to prevent users. If it isn’t happening at an alarming rate yet, Google and Apple need to take this time to get the security far ahead of the attackers.