Mobile Device Security

Nowadays, information technologies are highly developed and are still thriving, which leads to the widespread use of mobile devices, such as smartphones, tablets, laptops, and other portable devices. What's more, the spreading coverage of WIFI makes it much easier for people to get access to the internet, thus they could use the mobile devices socializing, entertaining, doing online shopping, even communicating and working. Admittedly, all the above makes people's much easier than before. However, now the mobile device stores both personal and business information, which makes it a data center of its user. Such collection of data put the devices under new risks. Mobile device security becomes an increasingly important problem to be addressed.

From what is arguing above, mobile devices collect and store a big amount of information, which access must be controlled to protect the assets of the device's owner. I can simply narrow the assets that need to be protected down to two aspects. One asset is the privacy information, and the other is business information. Speaking of the privacy information, there are a lot of them stored on mobile devices, such as contact, text message, social media content, even account credentials. Certainly, we would like to keep all these private, which makes our security goal clear, that is no one could either break into the device when the device is exposed to them physically or hack into the device remotely through the internet. While for the business asset, most of them are working emails and data in the remote working applications. The security goal is also very straight forward, that is to prevent from unauthenticated access and unauthorized access.

If we dive deep in analyzing the potential adversaries and threats to mobile devices, we will find out several severe ones of them. The top concern is Device Lost. It is easy to think about because it happens to everyone, we lost items. If a person happens to leave our mobile phone in a taxi or at a restaurant, his privacy and business information will certainly at risk. The second one is Application Security. As we all know, there are a lot of mobile apps out there. Once someone install an app on his device, the app always requests many privileges to access to different kinds of data, such as the contact, calendar, location and even browsing history. And most of the time, the person will allow all such request without knowing the

potential risk of private data leakage. What's the worse, there are also some malicious apps that they could steal the sensitive data underground to a remote server, which is also a great threat. The third concern is Malicious Attack, which is mostly done through the internet. The connection to an unprotected public WIFI could put our data under risk. If the attacker hacks into the device, they could easily get access to email and even account credentials.

From the potential adversaries and threats that I referred, they are existing all because of the potential weaknesses the mobile devices. Firstly, the mobile devices are portable, which means they are of smaller size, and the size of the device has a trend of becoming much smaller. Small size makes the devices easier to be neglect, and thus easier to be lost, which leads to the top concern Device Lost. Secondly, most people do not take it seriously when an application asking for privileges to access its data, and can't tell malicious application from their appearance, which leads to the second concern. Thirdly, people need to access the internet so badly nowadays, so the everywhere public WIFI is certainly the thing they are looking for. Actually, most people do know the public WIFI is insecure, while they have no choice so to take the risk.

Here, it comes several potential defenses against the potential weakness. For Device Lost a good defense is to on one hand avoids lost and on other hand keeps the device from breaking in by enhancing verification method, like adding a second verify method such as Fingerprint Recognition. For Application Security, the defense could be improving people's awareness of allowing access to certain apps and people's recognition of malicious apps. For Malicious Attack, a potential defense is that install safety protection software and avoid accessing anonymous public WIFI.

In total, we could draw a conclusion that, mobile device security is an important topic for modern people. There are a lot of potential adversaries and threats out there, and it is time for people to take actions.