Week 9 recap for DADA

Mobile security

We were introduced to Fernando Ruiz this week who was a mobile malware researcher for Intel Security. He is from Santiago Chile and loves figuring out how security on phones can be improved and penetrated.

We started with the history of mobile phones and how the networks have evolved over the years, from the very primitive 1G networks of the past to the 4G and more recently finished 5G versions. Worldwide, Android phones have dominated the mobile phone markets for smart phones and continue to outclass apple. Apple gets props for starting the “smartphone revolution” in 2007 with their first iphone. There are many different mobile phone OS but the vast majority of them are android. Android runs on Linux and is coded through Java, which in my opinion is superior to ios XNU and C++. Android gives much more freedom for security control which is good for the user but also more dangerous for the tech-unsavvy user since third party installs are allowed with the right get-around methods.

After this history lesson we went into the evolution of malware on android. WinCE was the first mobile backdoor in 2004, and eventually SymbOS.Skulls starting its reign of terror by corrupting apps and replacing icons for spooky effect. Fernando then gave a demo of Skulls and how it worked which was cool. Latter came cadtrap and redbrowser, the latter of which got a demo as well. Soon self propagation and financially motivated malware began spreading as the viruses became more sophisticated. With new tech came new vulnerabilities, and in 2008 polymorphism in phones allowed for dangerous new possibilities. The first mobile botnet was detected with the Symbian worm, a dangerous silent virus that spread via SMS URL. IKEE was the first IOS malware, but could only attack jailbroken iphones. FakePlayer and Tapsnake were the first android malware found and were pretty basic, however proved even these new phones could be defeated.

The android malware revolution was about how mobile botnets and repackaged apps in official and third party app stores took advantage of users thinking they had a “safe space”. PJAPPS had the scary ability to intercept incoming SMS messages. DROIDREAM involved more than 50 applications compromised that would attempt to root android devices and silently install malicious APK. It had 50-200k installs within four days of starting! When google tried to create a killswitch enabling them to remotely remove malicious files, malware authors took advantage of this too and disguised their malware to be similar and target Chinese telecom carriers.

Next we talked about the android architecture Which would take a while to sum up here.

He also talked about some android basics such as intents and activities, which was cool because I am currently taking a mobile dev class.

Next was the lab which involved the analysis of samples and code. We looked at FakePlayer and Tapsnake. Next was a dynamic analysis of walktxt, which was cool. It was used to bait people wanting to pirate an app that normally costs 1 dollar, and it SMS bombs the user.k