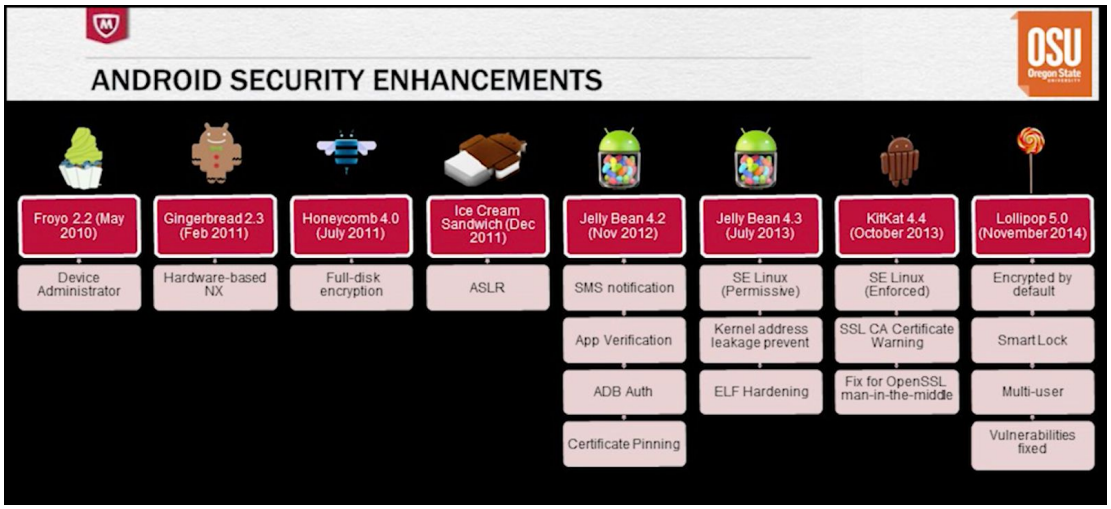
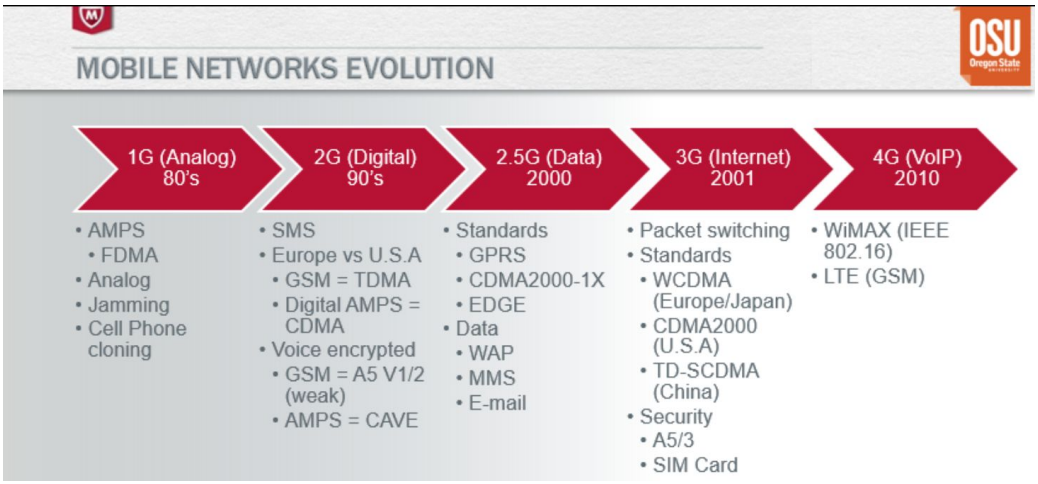
Nicolas Barraclough
12/6/20
CS373 - Defense Against the Dark Arts

Week 9/10 Write-up

Over the last couple of weeks, the class learned about mobile security. More specifically, we learned about a few mobile operating systems but focused on Android mobile security. I'm not gonna lie, it was pretty difficult to understand the lecturer in week 9. He gave us an overview of the security progression within Android mobile software from Froyo 2.2 back in 2010 and ending with Lollipop 5.0 in 2014. I always forget that the lectures took place half a decade ago. It would be nice to hear about more current things in this class but I guess this will give me things to research in my free-time. Yay!



I had known a bit about the different generations of networks for cell phones but I had no idea about all the different capabilities and security advancements that came along with the new generations of networks. With each new generation came new advancements in the network. 1G (analog) supported voice-only calling and supported a maximum speed of 2.4 Kbps. 2G introduced SMS and MMS for texting and multimedia messaging. 3G offered data to cell phones for internet access over cell service as well as video calling and much higher data transmission speeds. Now the standard which is not the latest in network technology, 4G. 4G offers everything that 3G has, except with much faster download speeds. The higher download speeds offer HD online video, more reliable online gaming, and better quality on phone and video calls. The next standard will be 5G which offers insane download speeds. This generation is so new, that it wasn't even mentioned in the lectures.



Terms in Mobile Networks Evolution:

- AMPS - Advanced Mobile Phone System
    - FDMA - Frequency Division Multiple Access
- Analog - (non-encrypted)
- Jamming
- Cell Phone Cloning
- SMS - Short Message Service
- TDMA - Time Division Multiple Access
- CDMA - Code Division Multiple Access
- CAVE - Cellular Authentication, Voice Privacy and Encryption
- GPRS - General Packet Radio Service
- EDGE - Enhanced Data rates for GSM Evolution
- WAP - Wet … jk Wireless Application Protocol
- MMS - Multimedia Messaging Service
- Packet Switching
- WCDMA
- TD-SCDMA - Time Division Synchronous CDMA (China)
- SIM Card
- WiMAX
- LTE - Long Term Evolution

Another thing that I didn't know much about was that malware is used on cell phones too. I had heard about jailbreaking and knew that there was some way for somebody to run unauthorized programs on a cell phone, but I chalked it up to magic or some tech wizardry. It makes sense now why so many people wanted to jailbreak their devices! Not only could you untie a phone from it's carrier in order to sell that device to somebody on a different carrier (the kids in my high school found that to be a great business and would steal

people's phones and sell them off), but you could jailbreak the phone in order to run third party software that otherwise couldn't be run on the device. Interesting stuff! I also never knew that doing something like that with an iPhone or iPod Touch could open the device to be accessed via SSH with a default password, 'alpine'. Good thing I could never figure out how to jailbreak my iOS devices without almost accidentally downloading a virus on my family computer.

Rooting for Android devices is similar to jailbreaking an iOS device. The purpose is to obtain root privileges so that you can run privileged operations and bypass restrictions put in place by the device manufacturer and the carrier. Android devices are a bit more susceptible to attacks because Android is open-source, whereas iOS is not. Open-source software is typically an easier target for a malicious attacker because they are able to work directly with the code to test/emulate their malware.