Yousef Kassira

CS 141

11/2/2017

Cyber Fair Poster Summaries

Mobile System – Android (Ashish Pulikkal and Yiyang Matt Yan)

Mobile Systems are currently in a major boom period. Everyone and anyone owns some sort of cell-phone, and most cell-phones today are running some sort of smart Operating System such as Android, iOS etc. With this boom in the Mobile Systems industry, the more attackers there are in the cyber industry as a whole. Most people think that all their information on their cell phone is completely safe and nobody can get to it because viruses only exist on computers. Most people fail to realize that these phones are now just as powerful as some computers. People are starting to get rid of their laptops because they don’t really need them anymore. One of the major things a smartphone does, that a computer cannot, is hold contacts. These contacts, if accessed by some cyber-hacker can be misused. These hackers have several different ways of getting into your phone. The focal point of this poster was the Android OS, which is widely regarded as a very open sourced Operating System. People can get into these phones through Bluetooth, Unsecured WIFI Networks and even cracked apps from straight off the Google Play Store. Everyone is always at risk, so we must be aware what we are getting into, and we must do whatever we can to fight these hackers.

Exploiting Hardware Policies (Joe Needleman)

Most department stores have a no questions asked return policy for many of their products. They don’t realize that this opens the door wide open for cyber hackers. A hacker can buy a router, implant some sort of malware on to the device, then return the device and do whatever they want to the next person who buys it. They are able to track IP addresses and take a lot of sensitive information from people. Although return policies are necessary, they are dangerous.

Free WIFI

Plenty of people are unaware of the dangers that Free WIFI has. With unsecured networks, your private information is accessible by hackers. There are hotspots that people go to connect to wifi such as Starbucks, McDonalds or even Airports. The presenter recalls of a time that he and a friend went to a Starbucks and decided to connect to the WIFI. From just this one case, he was able to access five separate peoples Social Security Numbers and Credit Card Information. He then proceeded to tell the Starbucks manager to tell their team that their network is ver unsecure and they should work on it. Cyber – Security is a very fast growing field and it is perhaps one of the best fields to get into at the moment. There is plenty of money going around in the space, and some even consider it to be somewhat simple of a career option.

Hacker Tracker (Jonathan Maxwell)

Jonathan Maxwell conducted an experiment to see how many attackers would try to access a “HoneyPot” computer, a computer that serves as bait, and then try and track the IP Addresses of these attackers. In the short period the HoneyPot was available, Maxwell had over 1.5 million hits from Attackers and tracked back their IPs that come from all over the world. Interestingly enough, China was a major spot for these hackers. Some of the most common attacked services were Telnet, VNC and even SSH, which our Computer Science department uses for Putty. There are attackers coming from everywhere, and there are a lot of them. So it is important we do whatever we can protect our devices from them.