Fabian Ortiz

3/31/20

Dr. Tabernyk

802.11

802.11 is part of the IEEE (Institute of Electrical and Electronics Engineers Standards) 802 set of LAN protocols. Which essentially means it is the standard protocol for WIFI. Security wise, WEP or Wired Equivalent Privacy requires a passcode to authenticate and a passcode to encrypt the data. All 802.11 networks are open there is really nothing that can stop you from getting onto an open wireless network, especially if the network is unencrypted anybody can get on it. WEP had encryption but it used a streaming protocol called RC4. RC4 was great, but its issue was: it would keep sending the same data over and over again accidentally, when streaming something you have to use something called an initialization vector and the problem was that WEP was mathematically able to crack the key just by looking at the data that was going through it.

WPA+TKIP came next and fixed the initialization vector problem using TKIP. TKIP is Temporal Key Integrity Protocol, the idea is if WEP used a secret decoder ring, that kept getting incremented one click every time that we could predict every time, TKIP spun it or jumbled it and made it difficult to predict and a lot more robust. For users at home, I would use a VLAN. It is a virtual local area network, but it focuses a lot on scalability and security. This method can help with issues that we face with wireless security. Some issues we have are people can see all the networks that their device shows and can get onto any of them. This is a problem because someone could have a key that breaks the passcode that “protects” their connection. Another issue is someone sending viruses through the ethernet cables that goes into the router and then goes wireless and gets onto our devices. A VLAN is secure because it won’t show up as it is virtual and almost under the radar. It’s a network within a network, almost an inner circle type of feeling.

At home, with little kids on the devices and clicking on anything that pops-up, I would use a pop-up blocker or an anti-virus that protects from malware such as phishing or Trojan horses. Another way to add some protection is to adding parental controls or restrictions to what can be used by the user, your internet service provider can be contacted and you can also get a little hands on and block out certain cookies or websites that can damage your drivers and take your information.