Brian Powers

December 8, 2016

Professor Chi So

ITP 125

Public WiFi – High Capabilities and High Risk

Developing technology has the goal of increased capabilities and convenience which in turn results in increased productivity. The invention of the internet connected the world in ways never before seen, and this model has been improved ever since. Wires provide the core connection between computers and ultimately between humans in this internet system, but the removal of wires on a local basis has greatly increased flexibility and convenience of accessing the internet, mainly through WiFi. This invention creates wireless networks that allow for most physical, internet-accessible devices to be physically disconnected from a network, but still remain connected wirelessly. Although many advances have made WiFi extremely reliable and attractive, security vulnerabilities exist that threaten users in a variety of ways. These risks and their feasibility will be examined in this paper. A growing trend and development is the implementation of public WiFi network that cover a large area and are accessible to everyone. These networks and their future, as long as related threats, will also be examined.

Wi-Fi stands for wireless fidelity, and is a way for devices to communicate in a close distance setting. Wi-Fi is extremely similar to a LAN or Local Area Network, and is a wireless version of such. The method of data transmission between devices is through radio waves that are sent in the gigahertz range. This is similar to the range of wavelengths used by a microwave oven. During the process, a computer’s or device’s wireless adapter will convert data into a radio signal that is sent to a wireless router (Fitzpatrick). The wireless router acts as a sort of hub for all Wi-Fi and wireless traffic in an area/network. The router has a physical, usually Ethernet connection to the internet that it uses to communicate the data translated from wireless signals received. Likewise, the reverse process can also happen and the router can transmit wired data received from internet to wireless radio signals that are communicated to devices (Escobar).

In order to more efficiently send large signals, a procedure called orthogonal frequency-division multiplexing is employed in which the large signals are chopped into many smaller signals which reduces the chance of interference during this sending process. As a result, large amounts of data can be sent at extremely quick speeds. Wi-Fi is constantly being upgraded. Today, the newest update, using the 802.11ac networking standards, is currently being developed and this type of signal will be able to send nearly a gigabit of data per second. Additional techniques used to reduce signal interference include frequency hopping and complementary code keying. Frequency hopping consists of jumping in between different frequencies during the sending of data, while complementary code keying consists of using a mathematical algorithm to fit more data into packets of signals. In a home or business setting, wireless routers allow signals to be sent at different frequencies that allow many devices to be connected to the same router at the same time. There are, however, limitations to this number, and certain routers have higher signal outputs which translates to higher capacities for electronics.

Because Wi-Fi presents a very open interface for wireless communication, security measures are important to ensure that undesirable devices cannot intercept or send information to or from other devices. WEP, or Wired Equivalency Privacy was an early form of Wi-Fi security that attempted to make Wi-Fi communications as secure as wired communications. This method works by encrypting data sent to and from the router in order for the packets to be correctly processed. The algorithms used for this encoding are usually easily able to be cracked by hackers, however. WPA (WiFi protected access) is the new standard for internet security. It works in a similar style to WEP, but has a much more complicated encryption mechanism and is thus harder to break. WPA2-PSK, a new version of WPA security, is said to be nearly impossible to break currently due to the randomness of the codes that it generates.

Even with security measures in place, many threats exist in using Wi-Fi and involving the data transmitted among it. Data interception, denial of service, and unusual network traffic/strangers are common threats to WiFi security. Data interception is one of the most common forms of interference and can be dangerous because sensitive pieces of information (such as personal information, credit card numbers, or passwords) are transmitted over WiFi and could become cyber weapons if intercepted and placed in the wrong hands. Denial of service is another threat that doesn’t allow a device or multiple devices to connect to a router. Wireless intruders are devices within the signal airspace of a wireless network that are able to interfere with signals and can sometimes be dangerous. Many procedures are employed by networks to ensure that all network traffic is normal or not unusual. As WiFi networks cover larger areas as their capacities grow, security is becoming a larger and more important issue in their operation. Larger networks correlate with increased vulnerabilities, and security improvements are constantly necessary to make large public Wifi systems feasible (Fitzpatrick).

Public WiFi began being offered as a service between 2008 and 2010, with Yahoo and Google being the first major researchers/developers into the idea. Hundreds of cities and villages around the world now offer this service, and its implementation continues to expand. The system is usually created and constructed by a private firm in conjunction with the city government. Most of the costs for the network come during this construction. The operation of the network is usually fairly cheap and is paid for by advertising or by small fees per usage by customer. Santa Monica, California is an example of a city that has initiated a free-city wide WiFi network with relatively fast speeds and increasing usage since its implementation (Weedmark). The European Union has announced plans of intent to get public WiFi to its entire range, starting with major cities and towns, but eventually spreading to all populated areas (Wong). In addition to city-wide public WiFi, over 750,000 hotspots exist around the world. These are just smaller-scale versions of public WiFi that only exist at a certain location (Weedmark).

The ease of connecting to these public wifi hotspots has increased productivity and lowered costs of such services all over the world, and their use is very common on an everyday basis. However, these networks may be convenient but they are far from secure. Many direct security threats exist as a result of these networks being open and accessible by anyone. Certain hotspots have been set up that record all data sent through the network. This is very easy for hackers to successfully pull off. All that is necessary is the constructing of a network of this style that has an attractive and innocent sounding name, or even a name that is the same as an already established hotspot at a location. After the establishment of this type of network the administrator/hacker simply has to wait for people to use the network, and the data will automatically be captured and recorded. It is recommended that one refrain from sending sensitive information over any type of network that doesn’t require a password, as this information is unencrypted and capable of being interfered with in the ways just described in addition to in other ways (Kovacs).

Snooping consists of simply monitoring others’ WiFi traffic through the use of programs and scripts, and is fairly easy for someone with a knowledge of computers to pull off in a public WiFi setting. This person can see exactly what websites people in the area that are also connected to the same hotspot are viewing. More advanced knowledge can allow a hacker to see deeper into these web sessions including what users are doing on each website and what data they are inputting or reading (possibly sensitive information). There are ways around this threat, however. Using a VPN is a great defense as hackers will not be able to see what websites one is accessing, but simply that they are using a VPN. Additionally, using https websites will encrypt all data sent and received and make it unreadable to anyone snooping in the area. Despite these measures, it is still highly recommend not to partake in online banking on public WiFi networks (Fitzpatrick). Using a VPN is the best defense against most attacks that could occur in this setting, but the ease of setting up malicious networks or performing other attacks on information sent and received is too great to make up for the convenience of banking through these free networks.

As wires disappear and technology advances, the use of wireless internet networks will positively increase, and as a result, further developments will be made in their complexity and capabilities. This will include security increases. However, with any security increase, there are increases in the capabilities of hackers and others to infiltrate systems with newly devised methods. At some point in the future, power and electricity may very well move to wireless stages, and at that point, attacks of a similar nature may be implemented to intercept electricity and cause related problems. Despite security vulnerabilities with internet traffic, however, the overall security for private and encrypted systems is extremely satisfactory, and results in great ease of use and increase in convenience and thus productivity for all those that use it.

Works Cited

Escobar, E. (2015). How Does Wi-Fi Work? Retrieved December 07, 2016, from <https://www.scientificamerican.com/article/how-does-wi-fi-work/>

Fitzpatrick, J. (n.d.). The Difference Between WEP, WPA, and WPA2 Wi-Fi Passwords. Retrieved December 07, 2016, from <http://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/>

Kovacs, J. (n.d.). Why Using a Public Wi-Fi Network Can Be Dangerous, Even When Accessing Encrypted Websites. Retrieved December 07, 2016, from <http://www.howtogeek.com/178696/why-using-a-public-wi-fi-network-can-be-dangerous-even-when-accessing-encrypted-websites/>

Weedmark, D. (n.d.). How Do Wi-Fi Hotspots Work? Retrieved December 07, 2016, from http://smallbusiness.chron.com/wifi-hotspots-work-61746.html

Wong, J. I. (2016). It's looking more likely everyone in the EU will get free wifi—except those in the UK, thanks to Brexit. Retrieved December 07, 2016, from http://qz.com/853283/free-eu-wifi-everyone-in-the-eu-is-getting-free-wifi-except-those-in-the-uk-thanks-to-brexit/