The True Cost of Free (Public) Wi-Fi

By

Tafari Duncan

Final Draft

COMP 116 / Computer Science Security

Tufts University

Medford, Massachusetts

October 31st, 2016

ABSTRACT

As the world advances further into the digital age millions of people come online every year. In the United States alone, over 87 percent [1] of Americans connect to the internet frequently and use Wi-Fi to do it. But as even as more and more people connect to the internet, very few are aware of its security risks. The internet has many security considerations, some of which are far out of the scope of what an individual user can control. This paper, however, focuses on the risks that the average internet user could expect to encounter while using public wireless connections, and suggests ways that the user could protect themselves.

Table of Contents

1.0 Introduction

Eighty-seven percent of American consumers use public Wi-Fi at cafes, airports, or hotels [1]. In today's digital age, easy access to the internet is critical. Given that much of the information Americans interact with every day is online, no internet often means a total separation from one's emails, social media, news, and entertainment (and that's just the short list). It's no wonder then that the first reaction many people have when they enter a public place is to check for a Wi-Fi signal. Ironically, it is because public Wi-Fi is publically available for anyone to use that it is so dangerous. In the same sense that the privacy and security of your bedroom at home would never be considered equivalent to that of a city park or train station, public Wi-Fi is inherently more dangerous than your personal Wi-Fi connection at your own home. This means that it warrants additional protections when used. That's not to say by the way that your home Wi-Fi is safe, as most systems can be hacked just the same way that some public Wi-Fi can be, but it is to say that home Wi-Fi systems are far less likely to be a target in the first place [1].

Surprisingly, the biggest vulnerabilities on public Wi-Fi haven't changed in over a decade. Articles on the subject as far back as the early 2000s discuss the same dangers of public Wi-Fi usage and how easy it can be for one's data to be compromised as articles written today. However, even as millions of Americans have flocked to cafes (e.g. In the case of Starbucks alone, the number of Starbucks in the US doubled from 2005-2015 to around 13,000 and 2016 reports indicate that they each receive an average of 500 customers daily [2]), public awareness of the issue is incredibly small [1].

Here are a few of the specific techniques that every Wi-Fi user should be alerted for:

- Packet Sniffing (See Appendix A.a for my own basic example)
- Man In The Middle Attack (See Appendix A.b)
- Jamming
- War Driving. (See Appendix A.c)

Packet Sniffing, simply put, is when a hacker uses a tool like Wireshark to capture all of the data packets sent on a network. Every time a computer connects to the internet, it transmits data in the form of data packets, which can be used to find out exactly what the user of that computer was doing on the internet. This, combined with a Man In The Middle Attack described below, can allow a hacker to steal personal information.

Man In The Middle Attacks, which involve the hacker setting up a fake access point and forcing computers to route their internet traffic through the hacker-controlled network, are also prevalent. These attacks can come in two forms, the first in the sense of fake networks that are set up to look exactly like a legitimate one. Hackers may set up a wireless network that they control named “Coffee Shop 5G” for example. These attacks can be especially successful if the network they create is free and open, as many people will naturally prefer to connect to the free Wi-Fi connection over paid ones. This is the form shown in the Appendix. The second form comes in them hijacking an existing “secure” network by a method known as ARP Poisoning (where they use tools like Ettercap to reroute all traffic on the network through them). In both of these forms of Man in The Middle Attacks, the attacker can steal user passwords and personal information, especially if the user accesses sites that are not secured by SSL/TLS authentication.

Jamming is less likely to cost the user anything, as it involves the hacker shutting down access to the network. This attack method can be particularly damaging to businesses, however,

as the loss of Wi-Fi at a coffee shop, for example, may lead to a loss in customers. It could also be used to serve as damaging in other ways, as the loss of Wi-Fi for even a few minutes could be costly depending on the time and nature of the business or person being attacked.

War Driving is particularly interesting, as the term comes from "war dialing, where people would dial random phone numbers in search of modems" [3]. Essentially, this involves people traveling around specifically in search of unsecured networks. Drones have even been used to locate unsecured Wi-Fi networks in remote locations.

For my own research, I decided to visit a local Starbucks café and investigate how difficult it would be to actually sit down and hack the local Wi-Fi network. I stopped short of actually capturing any data (since doing so would violate Starbuck's fair use policy and potentially get me into trouble) but noted that it was incredibly easy to access the Wi-Fi network (which did not require a password) and setup the tools a hacker to use. No one questioned me as I google searched "Common Starbucks Wi-Fi vulnerabilities", or opened up Kali Linux and booted up Wireshark. I was also struck by the realization that even if someone in the café wanted to stop me, they would have no idea what to look for. I looked just as inconspicuous as everyone else around me, plugged into their laptops. I probably could have worn a shirt that says "Hacker" and no one would have questioned it.

2.0 To The Community

I choose this topic in part because it is one that I am constantly at fault for. Currently, this mostly comes in the form of my university Wi-Fi, which fortunately encrypts my traffic to add some protection. That said, I am a frequent user of café and airport Wi-Fi, and I used to be the first one to connect to whatever unsecured network I find when I am out with friends. It's convenient, but that convenience is why the problem is so widespread. I will never forget the day

my junior year of college when one of my housemates looked at me laughed and said, “You know I could capture all the Wi-Fi traffic in the house right now right?”. He was joking, but only because he would consider it unethical and was aware that it would violate several different school policies, not to mention federal law. But in that moment I realized, he could still do it. In fact, anyone could. The only thing that stopped him was his own willpower and sense of morals.

Anyone with a computer and a Wi-Fi card can configure their computer to intercept internet traffic from the other people using the network. Getting onto most networks is a simple as selecting it from the list of available providers in your area. Even systems that have passwords or login in screens can be bypassed using programs like Reaver, Aircrack-ng or oclHashcat. Once on the network, programs like Wireshark can be used to download the traffic between the router and the computers connected to it. Then using programs such as Ettercap the hacker can comb through the data and find passwords, credit card information, and other information from your browsing session. The good news is that many of the popular web services (e.g. Facebook, Gmail, Amazon, Instagram) are aware of this and do everything they can to secure your data. The bad news is, regardless of how secure their sites are, you are still at risk from other sites that you visit that don’t have similar levels of protection. The information a hacker can discover from monitoring your search history, for example, might help them guess that your password is probably Jesus64 or something similar. With that said, this is especially relevant for the elderly and adolescent internet users who might not even be remotely aware of the dangers of the internet. Almost every holiday, for example, when I go to visit my grandmother, I am consistently shocked to find several malware programs on her computer. When I ask her how they got there, she tells me she doesn’t remember or that my younger cousin (age 13) downloaded the software. She assumed that the antivirus would catch them if they were

dangerous, and while she noted that she found the pop-ups they caused annoying, she didn't realize what was causing them. All of this is something that happens daily across the world let alone the United States when people are using *their own* computers in *their own* homes on *their own* Wi-Fi. Now imagine how dangerous it can be to move to a café or other public Wi-Fi spot where you have no control over the network and anyone can access it.

3.0 Defenses

Fortunately, there are several different ways to protect one's self on public Wi-Fi. Services like VPNs and online proxies promise to shield your browsing sessions from prying eyes, and some locations offer encrypted networks that aim to make it harder for hackers to steal information from others on the network. There are multiple ways to strengthen your security online and make it harder for someone to compromise your data. But sometimes, the best solution is the simplest one.

3.1 Don't use public internet

First and foremost, the best way to protect one's self on public Wi-Fi is to simply not use it. As the cost of cell-phone data plans drop, this is increasingly easy and simple to do. It's worth noting that mobile data itself can still be hacked, but this is much more difficult to accomplish and rarely happens to the average phone user. Most modern cell phones come with the option of allowing you to connect your computer to your phone data plan, allowing you to hope on for quick sessions.

3.2 Use VPNs

When longer connections on public Wi-Fi networks are necessary, the next best course of action is to connect to a VPN (Virtual Private Network) or a Web Proxy. VPNs offer many

benefits, and can actually be used to help users surf the internet anonymously in addition to safely. The distinction here is that if one is concerned about their general privacy and being monitored by either the websites they visit or their actual internet provider, VPNs can help prevent this by allowing users to surf the internet anonymously. However, if you're concerned about a physical person nearby hacking into the Wi-Fi network and stealing your data for malicious purposes, I would consider that to be a need to browse the internet safely.

A VPN works by creating an encrypted connection to transmit your data through. They can reroute user data through different computer ports and IP addresses, even giving the impression that the user is in a different location than they actually are. As an added benefit, because the data is encrypted, it ensures that even if a hacker was to spy on you while you were browsing the internet at your local coffee shop, they wouldn't be able to decrypt the data they received.

3.3 Use HTTPS and SSL

Netscape Communications, the creator of one of the first internet browsers and founder of the Mozilla Organization (which created the Firefox Browser), created HTTPS for their Netscape browser in 1994 to add a layer of security to online browsing sessions. It works by using the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol to share with cryptographic keys with the browser that visits a website. These protocols also encrypt the data shared between the site and the user's computer, making it difficult for prying eyes to snoop on the connection. Unfortunately, a Google Audit earlier this year revealed that "that 79 of the web's top 100 non-Google sites don't deploy HTTPS by default, while 67 of those use either outdated encryption technology or offer none at all. The worst offenders include big names, like the *New York Times* and IMDB" [4]. To help compensate, there are several browser extensions

(e.g. *HTTPS Everywhere* is one example) that can be used to force the browser to try for an HTTPS connection. Also, most modern browsers make it easy to tell if your connection is using HTTPS. Below is an example from Firefox, where one can see the address bar displays a green lock when the connection is secured.

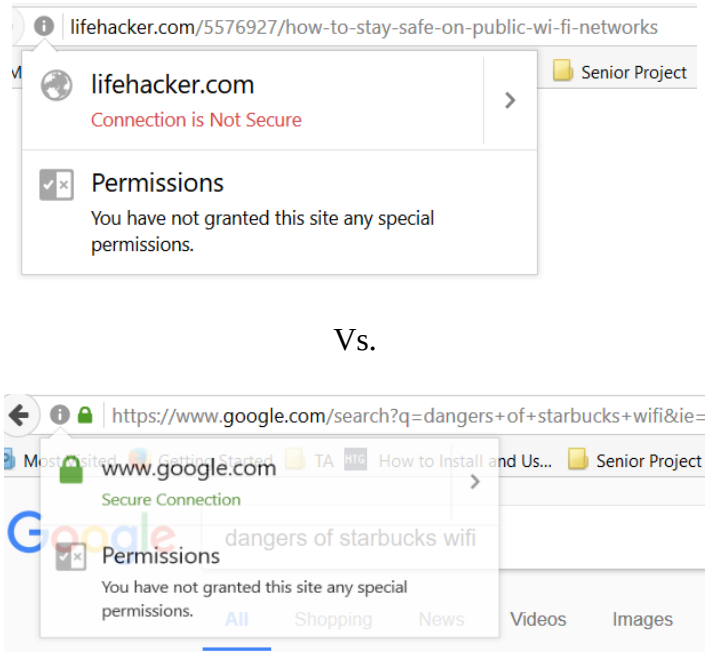


Figure 1

3.4 Turn off Local Area Network sharing

Most Mac and PC Laptops offer file sharing options for your local network. These settings by default are often configured to allow your computer to easily communicate with other computers, printers, and devices on your network. But these settings also make your computer discoverable on the network that it uses. Depending on the configuration, it might even allow others to access files on your computer without a password or prior authentication. It's important to remember to deactivate these file sharing permissions when you connect to public Wi-Fi.

Even on supposedly private networks, this can be an issue. Students at Tufts University, for example, frequently connect their computers and printers to the local Wi-Fi and set it as a trusted private network. This unknowingly permits their computers and printers to be open to anyone on the network, meaning that other students (or strangers with access to a student's login) can access their files or print from their respective computers. (See Appendix B.a)

Conclusion

Public internet is basically the wild west of the digital age. The majority of internet users have no idea the risks they run when they go online and are primarily focused just on getting online. When people connect themselves to public Wi-Fi, they expose themselves to the risks of being hacked by other people on the network. Fortunately, they can protect themselves by refusing to visit sites that contain sensitive data, using a VPN, or using their mobile data connection instead of the public Wi-Fi. However, given that the number of people at risk has continued to climb despite the fact that the challenges and risks that face public Wi-Fi users today are just the same as they were a decade ago, I strongly believe that a widespread public outreach and education campaign is urgently necessary to increase awareness of these concerns as quickly as possible.

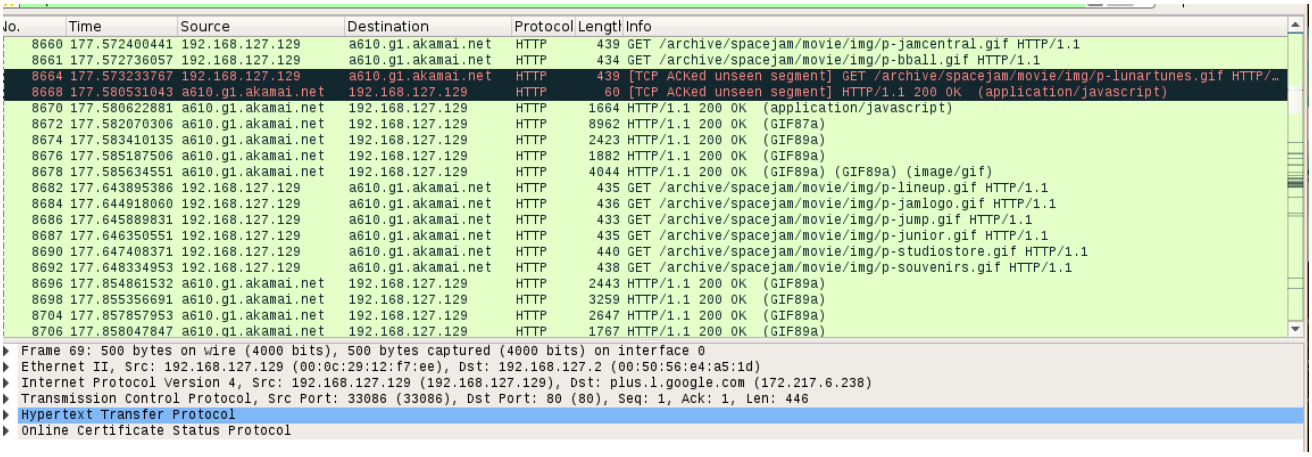
List of References

1. ‘Most People Unaware of the Risks of Using Public Wi-Fi’ <http://www.cnbc.com/2016/06/28/most-people-unaware-of-the-risks-of-using-public-wi-fi.html> [accessed 11 December 2016]
2. ‘Starbucks: International and U.S. Stores 2016 | Statistic’, *Statista* <https://www.statista.com/statistics/218366/number-of-international-and-us-starbucks-stores/> [accessed 10 December 2016]
3. ‘Types of Wireless Network Attacks | TechRoots’, *Phoenix TS,* 2016 <http://phoenixts.com/blog/types-of-wireless-network-attacks/> [accessed 10 December 2016]
4. ‘An (Updated) Hacker’s Toolkit’, *Private WiFi,* 2015 <http://blog.privatewifi.com/a-hacker%e2%80%99s-toolkit/> [accessed 10 December 2016]
5. Bajpai, Pranshu, ‘The Life of a Penetration Tester: How To Spoof DNS In Kali Linux / Facebook Phishing Page Using Social Engineering Toolkit In Kali Linux / BackTrack’, *The Life of a Penetration Tester,* 2013 <http://lifeofpentester.blogspot.com/2013/06/how-to-spoof-dns-in-kali-linux-facebook.html> [accessed 10 December 2016]
6. ‘How to Hijack Facebook Using Firesheep’, *PCWorld*, 2010 <http://www.pcworld.com/article/209333/how_to_hijack_facebook_using_firesheep.html> [accessed 11 December 2016]

7. Madmin, ‘Hack Lab Part 2: Exploring Your Home Computer Network with Kali Linux’ <http://blog.agupieware.com/2014/10/hack-lab-part-2-exploring-your-home.html> [accessed 11 December 2016]
8. ‘PII: B978-1-59749-073-3.50011-7 - Orebaugh_Wireshark_Chapter_6.pdf’ <http://cdn.ttgtmedia.com/searchNetworking/downloads/Orebaugh_Wireshark_Chapter_6.pdf> [accessed 9 December 2016]
9. Security, Author: Brian Barrett Brian Barrett, ‘Most Top Websites Still Don’t Use a Basic Security Feature’, *WIRED* <https://www.wired.com/2016/03/https-adoption-google-report/> [accessed 10 December 2016]
10. Tarantola, Andrew, ‘VPNs: What They Do, How They Work, and Why You’re Dumb for Not Using One’, *Gizmodo* <http://gizmodo.com/5990192/vpns-what-they-do-how-they-work-and-why-youre-dumb-for-not-using-one> [accessed 10 December 2016]

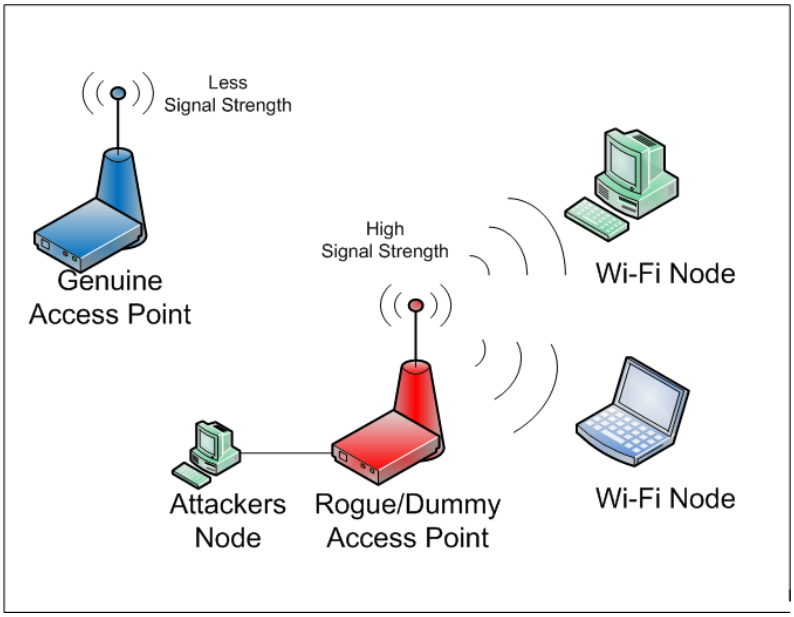
Appendix

A.a



An example of Packet Sniffing on my own network, showing sample data that shows a user's browsing habits.

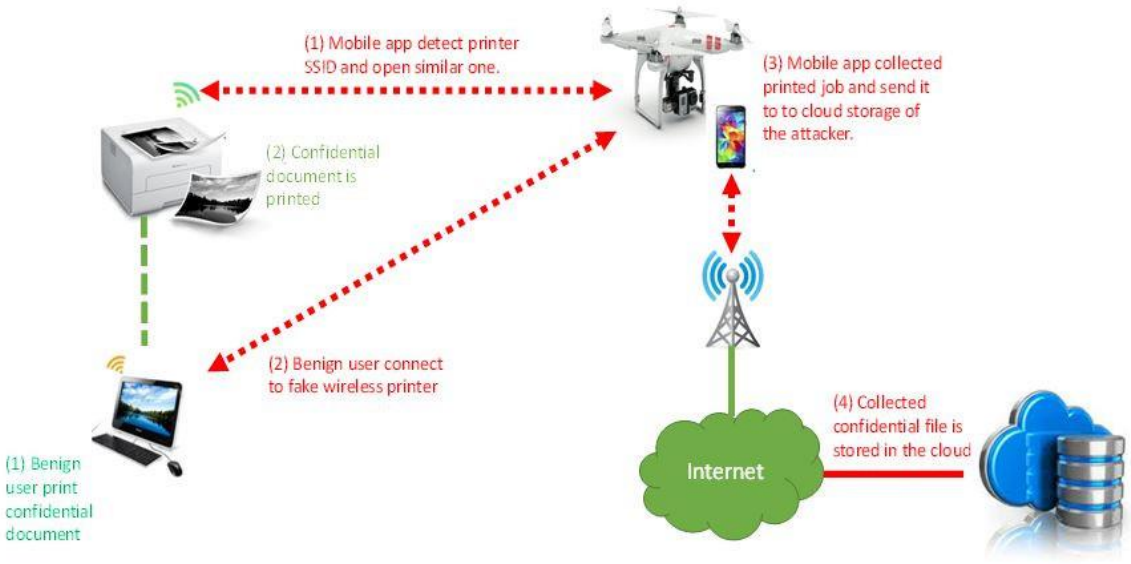
A.b.



Graphic Explaining Man In The Middle Attack, sourced from:

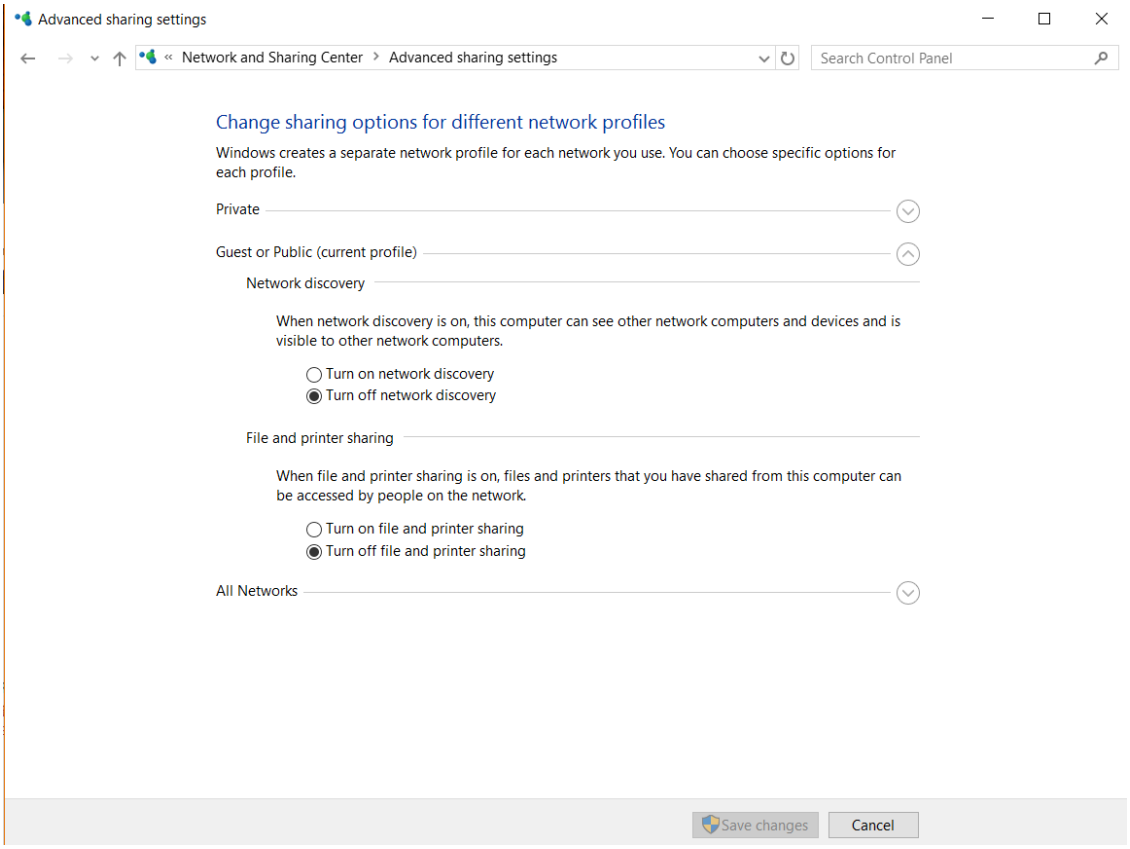
http://www.valencynetworks.com/images/wireless-attacks-1.png

A.c.



Graphic depicting Wi-Fi Driving Attack wherein a Drone is Used to Break Into Office Wi-Fi via a Printer, sourced from: http://icdn2.digitaltrends.com/image/drone-stealing-printer-939x517.jpg

B.a



The Network And Sharing Center on Windows PCs, which can be configured to disallow file sharing and PC discovery policies on public networks.

C