Analysis of Security Features and Vulnerabilities in Public/Open Wi-Fi

Jason E James
jason.james@indstate.edu
School of Criminology and Security Studies
Indiana State
Terra Haute, IN 47809

Abstract

As a student at a university or college, have you ever, whilst using the local wireless hotspot sitting in the campus common area, library, coffee shop, food court, or in classroom buildings, had the feeling that someone is looking over your shoulder at what you are doing on your computer? Indeed, someone might be, but it's not what you think. Hackers are looming everywhere looking to steal your personal information and identity. The author used Kali Linux and Ubuntu OS to discover and analyze students who use open Wi-Fi (Wireless Fidelity) and the security risks they are exposed to and associated safeguards they can take. In this paper, the author analyzed the security features and vulnerabilities of the open Wi-Fi's like Starbucks, McDonald's, Panda Express, and college campus free attwifi, by using both active and passive attack methods. For active attack, the author performed MAC address spoofing, SSL Stripping, and DHCP Exhausting attacks. For passive attack, the author captured the pcap file and used Wireshark for analysis.

Keywords: Open Wi-Fi, security, vulnerabilities, colleges/universities, Kali Linux

1. INTRODUCTION

In the age of technology, Wi-Fi has significantly changed the way we work and play, enabling us to interact with the digital world from anywhere in the physical world. In fact, elementary, middle and high schools, and colleges and universities are offering Wi-Fi. Some provide the networks with a required login access and/or open, unencrypted and free for anyone to jump on (Siciliano, 2017). The explosion of free, public Wi-Fi has been an enormous godsend for college and university students. In fact, many colleges and universities have free access points all over campus, including those provided by retail and service giants like Starbucks, Barnes and Nobles bookstores, Comcast, and AT&T and students are rarely more than a short trip away from access to a campus network. Unfortunately, the freedom of connectivity 24/7 comes at a price, though, students are at risk from hackers that are looking to steal their identity. Students and many users of open Wi-Fi truly do not understand the risks associated with these connections (Kapersky Lab, 2017).

Hundreds of thousands of students use campus or open public Wi-Fi every day, but are they protecting themselves when they use it? With growing needs for wireless networks in colleges and universities, problems created by an attacker exploiting the networks is also growing. Attackers exploit open Wi-Fi security networks and listen to the traffic and retrieve sensitive information. In fact, students using open Wi-Fi networks, particularly in a university setting, can have their personal information compromised and become a victim of identity theft before they even graduate and can cause issues when trying to gain employment. Lack of protection over open Wi-Fi and ignorance with wireless security may cause very big damage to sensitive data of an individual. So, it is very important to understand the vulnerabilities and the solutions in order to protect your identity and make it more complicated for attackers.

©2020 ISCAP (Information Systems & Computing Academic Professionals)

2. BACKGROUND ON WIFI

Wi-Fi is a type of wireless local area network (WLAN) technology that enables an electronic device, such as a laptop, tablet, or smartphone, wireless access to applications, data, information and media, without the constraints of physical hardware connecting the devices to the Internet using radio waves. The core technology behind Wi-Fi is a device called an access point (AP), which acts like a bridge between the wired network and the Wi-Fi network. The access point, in turn, typically connects to the Internet via a network router (Kasten, Okhrimets & Kharchenko, 2015).

Wireless is about convenience not being restricted by physical infrastructure of one location. It allows wireless enabled devices to access a network or other devices when within range of one another. Wireless networks can be created relying on wireless network technology. College and universities have increased Wi-Fi hotspots significantly over the past several years and are now offering free open Wi-Fi through companies like AT&T and X-Finity, as well as the college or university network. Wi-Fi eliminates the constraints of physical hardware and can result in a significant cost saving (Rudman, 2008).

Many colleges and universities provide Internet connection via APs throughout campus. This type of connection requires a login name and password to access. Most people, let alone students, think when they "login," their session is encrypted and secure. However, logging in with a user name and password doesn't necessarily mean it's a secure network. The traffic on many campus networks requiring a login is unencrypted, which means anyone who connects to the network with the right "sniffing" tools can see everyone's information (Siciliano, 2017).

In order to prevent attackers from stealing data, Wi-Fi includes a set of protocols for user device authentication and data encryption. The protocols, which reside on both the access point and the connecting device, use a pre-defined passphrase or other form of unique identification to authorize the user and encrypt data so that it can only be accessed by a designated device. WPA/WPA2, the currently recommended security standard, uses a pre-shared key (PSK) in the form of a series of text letters to authenticate users and encrypt data (Kasten, Okhrimets & Kharchenko, 2015).

When connecting to a campus network that requires a login and password, the easiest way to know if it has encryption is to view the list of wireless networks from your wireless control panel by looking at the properties by right clicking or just hovering over each with your mouse. If the Wi-Fi states a *WPA* or *WP2* password is required then the network has encryption. However, if it's labeled *WEP*, it also has encryption, but at an unacceptable level that is easily hacked. If the Wi-Fi does not state anything and just requires a login and password then it is unsecure (Siciliano, 2017).

The other type of Wi-Fi on campuses is provided by a third party free of charge such as AT&T, Comcast, and even Starbucks and Barnes and Nobles. This type of Wi-Fi connection requires no username or login credential and allows guests to access the Internet via unsecured access. Many colleges and universities offer this type of access to guests.

3. RISKS ASSOCIATED WITH OPEN WI-FI

In many colleges and universities, open public access points, called "hotspots," allow students Internet access. As discussed previously, those APs may be provided by AT&T, Comcast, and even Starbucks and Barnes and Nobles. In other words, if a student is sitting in a in a common area on campus or in the Starbucks café, they can access the one of these channels to connect to the Internet. Unfortunately, these open hotspots also allow anyone within the area to potentially read data that is not meant for them (Kasten, Okhrimets & Kharchenko, 2015).

The same features that make these free Wi-Fi hotspots desirable for students make them desirable for hackers; namely, that it requires no authentication to establish a network connection. This creates an amazing opportunity for the hacker to get unfettered access to unsecured devices on the same network.

The biggest threat to free Wi-Fi security is the ability for the hacker to position himself between you and the connection point. So instead of talking directly with the hotspot, you're sending your information to the hacker, who then relays it on.

While working in this setup, the hacker has access to every piece of information you're sending out on the Internet: important emails, credit card information and even security credentials to your business network. Once the hacker has that information, he can — at his leisure — access your systems as if he were you (Kapersky Lab, 2017).

Some of the ways a student's privacy can be invaded while on these open Wi-Fi hotspots include Network Sniffing, Wi-Phishing, Third Party Data Gathering, and Accidental and Malicious Access Points that use Page Spoofing and Evil Twin attacks to invade a student's privacy (Kasten, Okhrimets & Kharchenko, 2015).

Network Sniffing
If a hacker wants to steal a student's personal, financial information or identity, all they need is a "sniffing" application, like Wireshark or Kali Linux Kismet, that intercepts and gathers all visible traffic on a channel. Since open Wi-Fi does not have any security using a pre-shared key (PSK) like WPA2 where each connection is encrypted between a Wi-Fi network and a user's client, a hacker's job is already done since all is plaintext and not encrypted and can just "sniff" the network and grab student's personal information (Kasten, Okhrimets & Kharchenko, 2015).

Wi-Phishing
In Wi-Phishing, a hacker sets up a "soft" access point (or unauthorized devices) to get wireless-enabled devices to connect to it as a prelude to an attack to steal a user's identity (i.e. Id-spoofing). This can also take the form of a man-in-the-middle or insertion attack, where a hacker sets up a "soft" access point that acts as a relay to the "real" access point. When information flows through the "soft" access point, the attacker copies the data (Rudman, 2008).

Third-Party Data Gathering
Third-party data gathering is when sensitive unencrypted data or data encrypted with poor cryptography is intercepted, disclosed to unauthorized parties and stolen, deleted or lost while being transmitted between two wireless devices (Rudman, 2008).

Even without the presence of active data hackers, your privacy is never guaranteed when you access an open public hotspot. Often the biggest breaches of privacy are performed by the very establishments offering free Wi-Fi. Sometimes Wi-Fi is used to identify potential customers who are in the vicinity of the access point, and sometimes it's used to track the websites that users visit. Below are some common techniques that hotspot providers use to obtain information about Wi-Fi users.

- Asking visitors to leave their phone number or email in exchange for the PIN to access the Internet.
- Asking visitors to share something via a social network or give a program access to their social identity (e.g., to display targeted advertisements)
- Leveraging multiple access points to triangulate the visitor's physical location based on Wi-Fi signal strength (for example, to track their route through a store or to identify which establishments are currently the most crowded/popular)
- Injecting cookies into their browser to track their history (e.g., to display targeted advertisements) (Kasten, Okhrimets & Kharchenko, 2015).

Accidental and Malicious Access Points
Accidental association is when in a populated area, multiple wireless areas may overlap. A user may turn on a wireless device, which in turn connects to a wireless access point from a different overlapping network (other than the intended access point). Data from the overlapping network as a result of this could be exploited.

Malicious association, also known as a rogue access point, is when a hacker sets up an access point illicitly and looks like a legitimate access point using a cloned ID. The user believes he/she has gained access to a legitimate device. This access point is used to intercept data and can be used to bypass security controls (Rudman, 2008). Since there are often multiple networks to choose from, you often guess which hotspot belongs to a specific venue. Some Wi-Fi users will even connect to a completely unknown network simply because it is unlocked. Obviously, this practice poses some serious risks, especially if the access point is malicious or being manipulated by an attacker (Kasten, Okhrimets & Kharchenko, 2015).

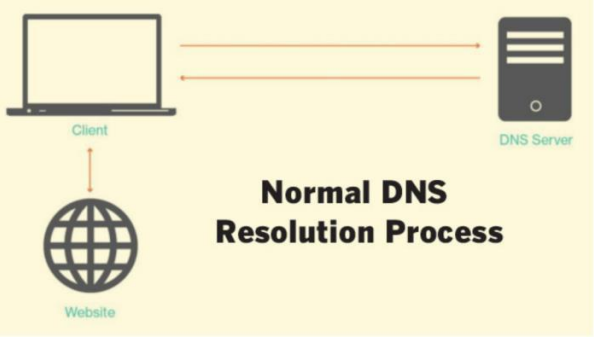

Fig. 1. Normal DNS Resolution Process (Kasten, Okhrimets & Kharchenko, 2015).

One of the biggest malicious association threats is "page spoofing," where a malicious access point controls a domain name resolution (i.e., how a domain name is translated into its numerical IP

address). In the normal DNS resolution process, a user's client will communicate with a server to connect to the Internet (Kasten, Okhrimets & Kharchenko, 2015).

In a spoofing attack, a hacker creates a fake version of a website to steal credentials. For example, you may be asked to "like" something on Facebook before you can access the Internet and then be directed to a fake Facebook login page that looks like the real thing. As you log in, this fake page would record your credentials, show a login error, and then redirect you to the real Facebook page for a "second attempt" at logging in. Before you're even aware of what has happened, your social identity has been stolen (Kasten, Okhrimets & Kharchenko, 2015).

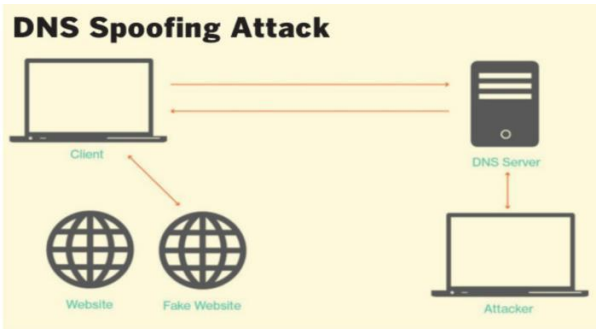

Fig. 2. DNS Spoofing Attack (Kasten, Okhrimets & Kharchenko, 2015).

Evil twin attack operates similarly. An attacker fools' wireless users into connecting to the attacker's network by placing an 'unauthorized' access point with a stronger signal in close proximity to the 'legitimate' wireless device. Users then log in to the attacker's network and unknowingly disclose data (Rudman, 2008).

This tactic is most often attempted in public parks or other large, unmonitored areas. Using a laptop with a wireless card, the attacker will access a legitimate access point to create an "evil twin" access point with a similar name. Imagine for a moment that you are at your local park, and your iPad detects a free Wi-Fi hotspot named "CityPark1." Many of us would probably connect to the network based on its name alone. However, by not confirming the legitimacy of an access point before connecting to it, you enable attackers to gather an even wider range of personal information (Kasten, Okhrimets & Kharchenko, 2015).

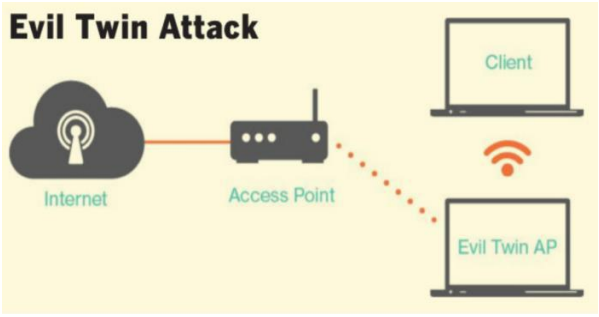

Fig. 3. Evil Twin Attack (Kasten, Okhrimets & Kharchenko, 2015).

These are the most common risks even though other risks such as denial-of-service attacks exist. Why do these risks exist? Three reasons exist for these types of attacks, each with different intentions. First are thrill seekers and drivers who are motivated by the thrill of electronic trespassing and in most cases, are harmless. Second are bandwidth thieves who use another's Wi-Fi to remain anonymous or to download software without paying for the software or bandwidth. The last reason, and the most common reason and the focus of this article are knowledgeable attackers or 'hacker who are out to steal data and information or steal someone's identity (Rudman, 2008).

4. PAST RESEARCH

The purpose of the literature review was to examine the existing literature for research on open Wi-Fi insecurity and if any research was conducted on college and university student access. Therefore, the review of the literature focused on literature related to Wi-Fi, security, and colleges/universities.

A second annual online survey was conducted by Norton by Symantec, although not specifically on college and university students, but rather a global study in order to better understand consumers' public Wi-Fi perceptions and practices and to unveil consumer misconceptions and worries about the safety of these connections. The survey explored consumers' knowledge about the safety of public Wi-Fi connections and while the use of public Wi-Fi is nearly universal, most consumers are unaware of the dangers when connecting to public Wi-Fi and continue to put their personal information at risk. The survey's findings provide consumers with much needed context to make better decisions about protecting their personal information while using public Wi-Fi.

In May 2017, Norton by Symantec (Norton by Semantec, 2017) surveyed 15,532 mobile device users who had connected to Wi-Fi to discover their attitudes to and behaviors using public Wi-Fi. The result was at least 1000 respondents from 15 global markets: Australia, Brazil, Canada, France, Germany, India, Italy, Japan, Hong Kong, Mexico, Netherlands, New Zealand, United Arab Emirates, the United Kingdom and USA. The research was conducted by Norton by Symantec and Reputation Leaders through international online panel company Research Now with data collected from May 18th to June 5th, 2017. The key findings included the following:

1. **Consumers are unable to resist a strong, free Wi-Fi signal.**
    a. More than half of consumers globally (55 percent) wouldn't think twice about exchanging, sharing or even doing something to get a strong Wi-Fi signal.
    b. 25 percent have accessed a Wi-Fi network without the Wi-Fi network owner's permission; 8 percent guessed or hacked the password
    c. 46 percent of consumers can't wait more than a few minutes before logging onto a Wi-Fi network or asking for the password after arriving at a friend's place, café, hotel or other location.
2. **Even when travelling, access to public Wi-Fi is a must.**
    a. Respondents say that access to a strong Wi-Fi signal is a deciding factor when choosing the following: A hotel/holiday/hostel rental (71 percent), a transport hub for traveling and/or commuting (46 percent), a place to eat or drink (café, bar, restaurant, etc.) (43 percent), an airline (43 percent)
    b. Nearly half (49 percent) of people say the most important reason for having access to strong public Wi-Fi is so they can use Maps, Google Maps or another GPS app to get around.
3. **Nevertheless, what some people choose to do over public Wi-Fi may surprise you.**
    a. One in six people admit to having used public Wi-Fi to watch adult content.
    b. Of those who admit to using public Wi-Fi to watch adult content, they've done so in the following locations: Hotel/Airbnb (40 percent), Café/Restaurant (30 percent), Work (29 percent), Airport (25 percent), On the street (24 percent), Train/bus station (18 percent), Public restroom/toilet (16 percent)
4. **Consumers' dependency on public Wi-Fi is putting their personal information at risk. What someone thinks are private on his or her personal device could easily be accessed by cybercriminals via compromised apps or Wi-Fi networks.**
    a. 60 percent feel their personal information is safe when using public Wi-Fi, yet 53 percent can't tell the difference between a secure or unsecure public W-Fi network.
    b. 75 percent of consumers don't use a Virtual Private Network (VPN) to secure their Wi-Fi connections, even though it's one of the best ways to protect your information.
    c. 87 percent of consumers have potentially put their information at risk while using public Wi-Fi.
5. **When consumers think about a hacker or malicious person stealing their personal information and posting it online, emotions run high.**
    a. 48 percent would feel horrified if the details of their bank accounts and financial information were posted online.
    b. 38 percent would feel angry if their photo library, including intimate, personal and family photos were posted online.
    c. 36 percent would be worried if their children's schedule, location or academic details were posted online.
    d. 21 percent would be embarrassed if the details of their private chats/texts conversation or closest secrets were posted online (Norton by Semantec, 2017).

Although no studies were found in the literature review search on open public Wi-Fi insecurity and college/university students, other studies were done on Wi-Fi and security.

In 2013, a study was done to propose a solution to monitor Wi-Fi networks that is under unauthorized access attack via rogue APs. The author provided the required user permissions to allow/block connect and access files on the secure ad-hoc client. The experiment results showed the effectiveness of the proposed solution (Sobh, 2013). Additionally, a study on the disadvantage of Wi-Fi networks (Chernukin, 2014) on offering low level of protection against unauthorized access and the problems related to such use of

the Wi-Fi technology, poses a threat to information security. Also, describes the causes for appearance of threats, drawbacks of legal character, and to substantiate the offers concerning improvement of legal and organizational measures for preventing the use of brand-new technologies for destructive purposes.

Sagers et al examined the relationship between wireless access points collected via war driving and a series of US Census socioeconomic variables in two communities in the United States (Sagers, Hosack, Rowley, Twitchell & Nagaraj, 2015). They found significant correlations between Wi-Fi security race/ethnicity, which may also correlate to education levels and income. Their findings suggest that a greater awareness and/or manufacturer-driven default security for wireless access points may be necessary to ensure better
security. Their presents a large-scale attempt to collect data from thousands of Wi-Fi networks to measure their security in two distinct geographic regions to determine what, if any, socio-economic factors affect the level of security and suggest a number of possible solutions to the gaps that exist in Wi-Fi security (Sagers et. Al., 2015).

Very few studies were found on open Wi-Fi insecurity and none were found as it relates to college/university students accessing open Wi-Fi on campus. This study utilizes Kali Linux to explore students accessing open public Wi-Fi one universities campus and the potential risk they are exposed to from attackers. The next few sections details the methodology used for this study, the results and solutions for security using open Wi-Fi on campus.

5. OPEN WI-FI SECURITY ANALYSIS

In this paper, the author considered analyzing the security features and vulnerabilities of the open Wi-Fi like Starbucks, McDonald's, Panda Express, and college campus free attwifi, by using both active and passive attack methods. The author was in no way hacking these devices in these places but rather emphasizing the issues of open Wi-Fi. For active attack, The author performed MAC address spoofing, SSL Stripping, and DHCP Exhausting attacks. For passive attack, the author captured the pcap file and used Wireshark for analysis.

MAC Address Spoofing

MAC address spoofing is technique for faking originally assigned Media Access Control (MAC) Address of a network device. MAC address spoofing is considered as a significant step for attacker to launch a variety of attacks on open Wi-Fi networks, such as man-in-the-middle, side jacking, and denial of service.

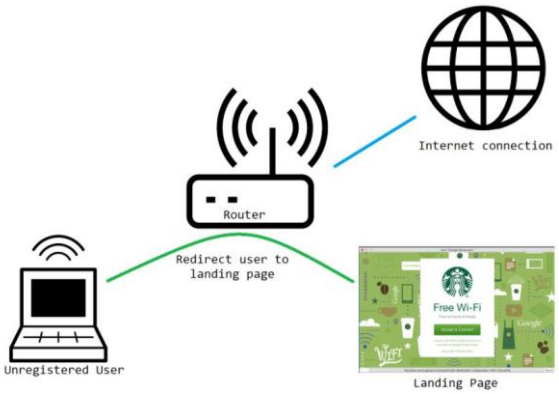

Fig. 4. Captive Portal Landing Page Structure [10]

The author tried to spoof the MAC address of the target machine to bypass the captive portal page of open Wi-Fi networks. Captive Portal works by intercepting, impersonating, and altering the connection between client and web server. Even though the author define the captive portal as a firewall for open Wi-Fi network, it is a man-in-the-middle attack. However, it has good intentions (for security reasons and safe environment) to filter the traffic. For example, to providing a safe and secure environment, adult contents are blocked in Google Starbucks Wi-Fi and McDonalds Wi-Fi (where they are combinedly more than 21,000 store locations in the U.S).

Even though the author, as an attacker, could duplicate the same MAC address of target who is already connected to an open Wi-Fi. The author was unable to bypass the captive portal using that MAC address spoofing. Additionally, the author experimented spoofing MAC address of Access point (AP) itself to bypass the captive portal. Even this time, results are negative. This could be because of 802.11 association process.

The 802.11 association process happens when a user tried to access Wi-Fi, i.e. the mobile station and AP will exchange a series of 802.11 management frames to get to an authenticated and associated state before connection is established. There are three 802.11 connection states: Not authenticated or associated, authenticated but not yet associated, and Authenticated and associated respectively. All these states conditions can be identified in the frame control fields.

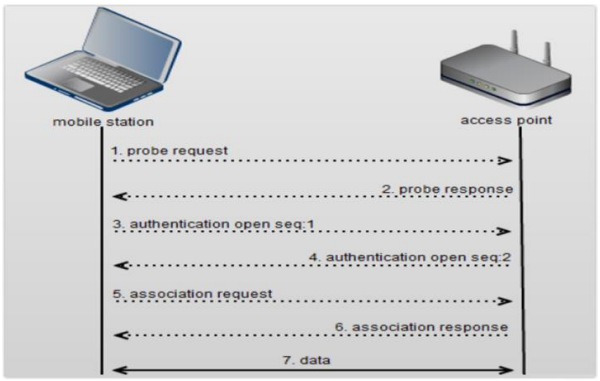

Fig. 5. 802.11 Association Process (Meraki, 2017)

Each frame includes frame control, duration, BSSID, Source MAC, Destination MAC, Sequence control, frame body, and frame control field.

Frame Control	Duration/ ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Frame Body	FCS
2 Bytes	2	6	6	6	2	6	0-2312	4

Fig. 6. Frame Control Field (Meraki, 2017)

So, by implementing devices with Sequence Number tracking, Operating System (OS) fingerprinting & tracking, and Received Signal Strength fingerprinting & tracking MAC address spoofing attack to bypass the captive portal can be prevented. Below Fig. 7. shows our Wireshark analysis of the 802.11 association process.

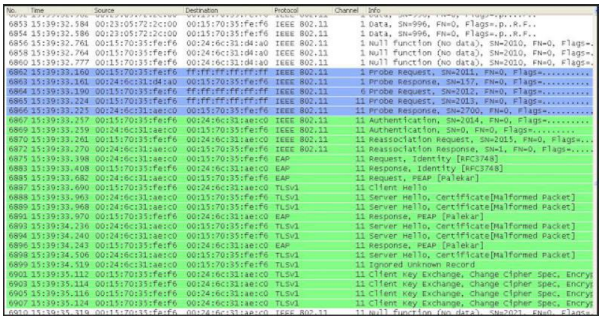
Fig. 7. 802.11 Association Process captured in Wireshark

SSL Strip

SSL Strip is a type of attack that tricks a victim's browser into communicating with an attacker in plain-text over HTTP. As a matter of fact, the author can identify SSL strip as a form of man-in-the-middle attack. The goal of SSL Strip when performed by attackers on open Wi-Fi, is to route all the traffic from the victim's machine via a proxy that is created by the attacker. To better understand the SSL Strip's concept, the author has to understand HTTP and HTTPS, which are application-layer protocols in TCP/IP model. In fact, when communicating over open Wi-Fi, HTTPS utilizes a secure tunnel to ensure data is transmitted in a secured way; this secure tunnel is commonly called as SSL.

Though, there are many ways to perform SSL Strip the author used ARP spoofing as a method of evaluation in our research. Indeed, through ARP spoofing the author was able to downgrade the connection established by the victim's browser from HTTPs to HTTP. In our scenario, a victim has connected to an open Wi-Fi and tried to connect to www.facebook.com using his credentials, while the attacker is running SSL Strip on another machine, which is a proxy server. The description of the attack's scenario is as followed:

- Victim tries to initiate a secure communication with www.facebook.com.
- The victim's browser that is connected to the attacker's machine requests a response from the Facebook's server (attacker acts as man-in-the-middle, by sending victim's request to server and await from response). Here, the Kernel forwards everything along except for traffic destined to port 80, which it redirects to 8080
- Attacker received secured feedback from Facebook's server and modified the response from the server from https to http and sends it to victim. At this point, the victim is provided with in insecure login http://www.facebook.com, and attacker can easily sniff all the data entered by the victim and see credentials (data is in plaintext format). Figure X below depicts the result of SSL Strip on a Facebook's user, connected to an open Wi-Fi.

DHCP Exhausting – A DoS Attack

DHCP is a critical part of the Layer 2 and Layer 3 link, as
well. Nowadays intelligent switches assign temporary IP addresses to hosts in networks. Most switches provide further configuration information such as a subnetwork mask, default gateway, and DNS services etc. Moreover, DHCP is an inherently insecure protocol. Some well-known attacks at Layer 2 utilizing DHCP are rogue DHCP servers, DHCP starvation, and DoS attacks among others. This project takes advantage to exploit the weakness by DHCP starvation in captive portal to exhausting its IP addresses. By issuing this command, Pig.py wlan0.

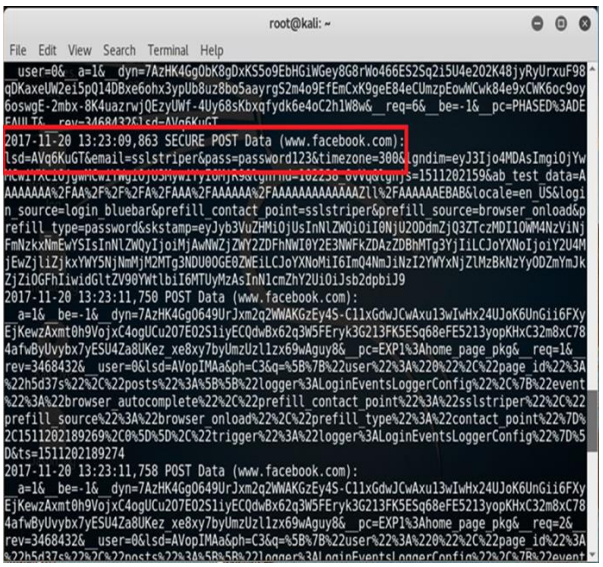

Fig. 8. SSL Strip Password capture

Below is a screen shot depicting a successful DHCP starvation on captive portal at McDonalds Café.

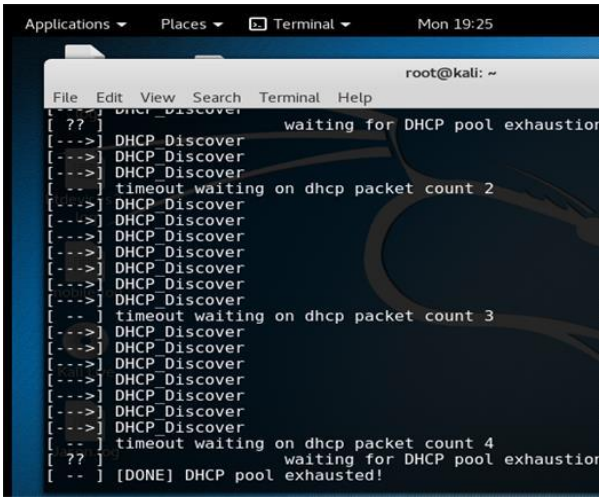

Fig. 9. DHCP Exhausting

The author was able to exhaust one subnet, but because the wireless access portal run on multi-subnets the effect of IP starvation was not achieved. Most captive portal mitigate such problems by putting in place measures such as:

- WLC (Wireless LAN Controllers) to terminate the user traffic and by examining DHCP requests to ensure that the client MAC address matches the chaddr. If the addresses do not match, the DHCP request is dropped.
- An H-REAP AP (Hybrid Remote Edge Access point) terminates the user traffic. The user VLAN is terminated locally, the DHCP request does not go through the controller, and an analysis of the chaddr cannot be performed.

DHCP Exhausting – A DoS Attack

The author did a ping response test in attwifi (Campus), Starbucks, McDonalds, and Panda Express open Wi-Fi. All of them provided us a same result "Destination host unreachable". The author did a quick research to understand the result. The wireless network has their firewall turned on to block ICMP packets from to help prevent DDoS Ping Flood attacks.

6. SOLUTIONS FOR SECURITY USING OPEN WI-FI

Even without an elaborate phishing scheme, it is impossible to completely secure a public hotspot. In fact, many times access points will only display an end-user agreement (EULA) or advertisement before allowing users to connect to the Internet.

Although there is no connection between the open public Wi-Fi network and a student's personal network (i.e., different SSIDs and IP addresses), there is still the concern that a hacker can connect to a network hosted on the user's device and exploit any potential vulnerabilities.

Students should never connect to open public Wi-Fi, since many risks exist as described earlier in this article, but since that is almost impossible, there are certain measures students can take to protect against attackers. Here are the most common precautions:

1. Always confirm the legitimacy of a Wi-Fi network before connecting to it; do not rely on the name alone. If there are multiple access points for the same venue, ask a staff member which one to use. Similarly, be sure to read that venue's Terms of Service carefully to ensure that your privacy will not be breached.
2. Ideally, you should only use public Wi-Fi to browse websites that do not require login credentials (e.g., news forums, etc.). However, if you do need to access sensitive data or enter login credentials (for, say, email), only go to websites that start with HTTPS (a more secure version of the standard HTTP web protocol). Just be aware that even if a website uses HTTPS for the majority of its content, the images on that website might still be distributed via HTTP since links are not typically encrypted. However, most current web browsers will warn you if this linked content is unsecure or when the certificate

from a secured HTTPS site is not valid or verifiable.

3. Never install software while using public Wi-Fi, as it could introduce viruses into your computer. For example, a common attack is to inform the user that his browser is using outdated Flash and then redirect the user to a fake Adobe website that will install a virus instead of the real software.
4. A good way to ensure security while accessing public Wi-Fi is to use a Virtual Private Network (VPN). A VPN essentially creates a tunnel between your device and a third-party server. All data that passes through this tunnel is encrypted and therefore hidden from both the Wi-Fi provider and anyone trying to sniff the network. If you cannot access a VPN through the school, consider installing a trusted third-party VPN like Cyber ghost.

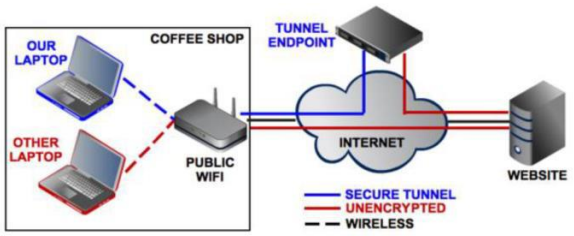

Fig. 10. Tunneled Traffic

5. If all else fails, students should use a personal mobile hotspot, either on their phone or with a separate device. In fact, many companies like AT&T offer unlimited plans so there is no limit on how much you can surf the Internet.

It is easy to take free Wi-Fi access for granted. Unfortunately, as public hotspots become more prevalent, so will hackers. Your best protection against data theft is a solid understanding of Wi-Fi and its vulnerabilities and taking a few commonsense precautions (Kasten, Okhrimets & Kharchenko, 2015).

7. CONCLUSION

Users of wireless hotspots are ultimately responsible for their own security. Although some tools give them enhanced security functionality when using a hotspot, the situation remains unpredictable and insecure for the majority of users. Operating system vendors and third-party software developers do not provide enough information and direction to users regarding the threats on wireless networks. The attacks against Wi-Fi are not terribly complicated, but without tools for triggering alerts and defensive measures aimed at hotspot users, there's little these users are able to do to protect themselves.

For all their utility and ease of use, hotspots are dangerous places. While every coffeehouse and lounge may not include an attacker lying in wait for victim hosts, the fact is attackers are likely to be successful. Users in enterprise environments have the luxury of a single point of control and administration that creates "security of scale" for wireless users. In open public hotspots, users are on their own. Despite the availability of tools and point solutions, most users represent easy prey for sophisticated attackers.

The state of the art with respect to wireless defense is behind the state of the art with respect to wireless attack. As technologies evolve, users will become better armed to deal with the threat posed in hotspots. In the meantime, it may be better to shut the laptop, enjoy the coffee, and keep an eye on the people nearby (Potter, 2006).

8. REFERENCES

Baul, P., Venkatachary, S., Balachandran, A. (2001). "Secure wireless Internet access in public places," ICC 2001. IEEE International Conference on Communications. Conference Record (Cat. No.01CH37240), Helsinki, 2001, pp. 3271-3275 vol.10.doi: 10.1109/ICC.2001.937274

Chernukin, I. (2014). NEW CHALLENGES TO INFORMATION SECURITY CAUSED BY THE INTRODUCTION OF WI-FI TECHNOLOGIES. *Information & Security, 31*(1), 79-86. doi:http://dx.doi.org.proxy.ulib.uits.iu.edu/10.11610/isij.3105

Cypriani, M., Lassabe, F., Canalda, P., Spies, F., (2009). "Open Wireless Positioning System: A Wi-Fi-Based Indoor Positioning System," 2009 IEEE 70th Vehicular Technology Conference Fall, Anchorage, AK, 2009, pp. 1-5. doi: 10.1109/VETECF.2009.5378966

Eslami, M., Karimi, O., Khodadadi, T. (2014). "A survey on wireless mesh networks: Architecture, specifications and challenges," 2014 IEEE 5th Control and System Graduate Research Colloquium, Shah Alam, 2014, pp. 219-222. doi: 10.1109/ICSGRC.2014.6908725

Hills, A. (1999). "Wireless Andrew [mobile computing for university campus]," in IEEE Spectrum, vol. 36, no. 6, pp. 49-53, Jun 1999. doi: 10.1109/6.769269

Jones, K., and Liu, L. (2007). "What Where Wi: An Analysis of Millions of Wi-Fi Access Points," 2007 IEEE International Conference on

Portable Information Devices, Orlando, FL, 2007, pp. 1-4.doi: 10.1109/PORTABLE.2007.45

Jyrki, T., and Penttinen, J. (2015a). "Future of Wireless Solutions and Security," in Wireless Communications Security:Solutions for the Internet of Things , 1, Wiley Telecom, 2015, pp.336-doi: 10.1002/9781119084402.ch10

Jyrki, T., and Penttinen, J. (2015b). "Security Risks in the Wireless Environment," in Wireless Communications Security:Solutions for the Internet of Things , 1, Wiley Telecom, 2015, pp.336-doi: 10.1002/9781119084402.ch8

Kapersky Lab. (2017). How to Avoid Public WiFi Security Risks. [Online]. Available: https://usa.3.com/resource-center/preemptive-safety/public-wifi-risks

Kasten, T. Okhrimets, A., and Kharchenko, A., (2015). Is it safe to use public Wi-Fi networks? [Online]. Available: https://www.networkworld.com/article/2904439/wi-fi/is-it-safe-to-use-public-wi-fi-networks.html

Kavianpour, A., and Anderson, M., C., Anderson (2017). "An Overview of Wireless Network Security," 2017 IEEE 4th International Conference on Cyber Security and Cloud Computing (CSCloud), New York, NY, 2017, pp. 306-309.doi:10.1109/CSCloud.2017.45

Meraki, C., (2017). 802.11 Association Process

Explained.[Online].Available:https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/802.11_Association_process_explained

Muppavarapu, R. (2015). Open Wi-Fi hotspots-Threats and Mitigations. [Online]. Available: https://dl.packetstormsecurity.net/papers/wireless/openwifimitigations.pdf

Norton by Symantec (2017). Norton Wi-Fi Risk Report: Report of online survey results in 15 global markets. [Online]. Available: https://www.symantec.com/content/dam/symantec/docs/reports/2017-norton-wifi-risk-report-global-results-summary-en.p

Potter, B. (2006). Wireless hotspots*. Association for Computing Machinery. Communications of the ACM, 49*(6), 50-56. doi:http://dx.doi.org.proxy.ulib.uits.iu.edu/10.1145/1132469.1132501

Ray, S., et al. (2017). "An efficient association of a mobile client in wireless mesh network," 2017 8th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 2017, pp. 497-500.doi: 10.1109/IEMCON.2017.8117225

Rudman, R. (2008). Wi-fi TECHNOLOGY: Is someone watching you? [Online]. Available: https://search-proquest-com.proxy.ulib.uits.iu.edu/docview/215225473?accountid=7398

Sagers, G., Hosack, R., Rowley, J., Twitchell, D., and Nagaraj, R. (2015). "Where's the Security in WiFi? An Argument for Industry Awareness," 2015 48th Hawaii International Conference on System Sciences, Kauai, HI, 2015, pp. 5453-5461

Siciliano, R. (2017). School WiFi Often Open and Insecure. [Online]. Available: http://www.huffingtonpost.com/robert-siciliano/school-wifi-often-open-an_b_4276082.html

Sobh, T. (2013). Wi-Fi Networks Security and Accessing Control. International Journal of Computer Network and Information Security. 5. 9-20. 10.5815/ijcnis.2013.07.02

Sosa, P. (2017). BREAK FREE! - BYPASSING CAPTIVE PORTALS. [Online]. Available: http://konukoii.com/blog/2017/03/07/break-free-bypassing-captive-portals