BITS 3353 Network Security Administration and Management,
5 November 2019

PUBLIC WIRELESS ACCESS

Wan Mohammad Faisal Bin Sammio, Soliseheaswar Sridaran, Nur Fadzilah Othman

Faculty of Information and Communication Technology, Technical University of Malaysia Melaka,
Malaysia

Abstract

Wi-Fi is a technology that uses radio waves to provide internet access to connected devices by the use of signals from nearby devices. We live in a modern age where being linked seems to be one of life's main aspects. Wi-Fi is a wireless networking abbreviation for wireless fidelity. WPA2 platform is commonly used for Wi-Fi communication since it is effective and safe against several wireless assaults. Organizations and network developer continually make a lot of cash and effort to secure wireless communication. Due to their various benefits, Wi-Fi is now popular. In addition to all of those benefits, Wi-Fi also faces the main safety issue, and so many individuals are looking to enhance safety via Wi-Fi because many businesses want to move sensitive information via Wi-Fi. Since the 1990s, Wi-Fi security algorithms have undergone many changes and upgrades to make them safer and more efficient. For home wireless network protection, different wireless security protocol types have been developed. The wireless security protocols are WEP, WPA, and WPA2 for the same purpose but are simultaneously distinct.

At some point in your day almost everybody uses Wi-Fi. Be online it's vital for us to update our social media status, buy a big pizza, hang on a taxi, book flights or train tickets or even use it to educate! In almost every café, restaurant and public space in the city, the world is completely invaded by the innovative Wi-Fi technology has become available to the general public. However, there are numerous of public Wi-Fi out there that provides free wireless connection to the users or clients in the place or organization. Do you know that accessing public wireless access or open Wi-Fi exposed you to the dangerous of being compromised? So, in this assignment we will discuss security issues related with usage of the public wireless access or hotspots and prevention strategies to overcome them.

Index Terms- Public wireless access, security, WI-FI security, Wi-Fi attacks, prevention strategies, privacy issues.

INTRODUCTION

Wi-Fi is a kind of remote system innovation used to connect to the Internet. In 1977, IEEE developed the first WLAN protocol, 802.11. It was the first WLAN Protocol. The frequencies at which Wi-Fi functions as 2.4 GHz and 5 GHz, no impedance with mobile phones is guaranteed, radio communications, TV receiving apparatus and two-way radios are experienced in the middle of transmission. 7 Basically, Wi-Fi consists of radio wave broadcast on a Wi-Fi router, where it detects and decipher the waves (Techopedia n.d.). This functions much like an AM / FM, but the interaction is a two-way stream. Wi-Fi works over longer distances than bluetooth and infrared, and is also ideal for mobile devices such as laptops and smartphones with low-power conceal technology.

Free Internet Wi-Fi access is available for free and is accessible in popular public areas such as airport, coffee shops, malls, restaurants and hotels. Those 'hotspots' are so popular and so ubiquitous that people often communicate with them without thinking twice. Although connecting and checking your social media account or reading some news articles sounds harmless, it is a risky business on public Wi-Fi to check your account or to conduct some operation involving authentication.

SECURITY ISSUES RELATED WITH USAGE OF THE PUBLIC WIRELESS ACCESS.

A. Rogue AP directed to Man In The Middle (MITM) attack.

According to Joshua Wright and Johnny Cache (2015) among all the security threats, one of the most threatening hazards is the prevalence of fake APs. The same features make it convenient for customers to use free Wi-Fi hotspots, namely, that no authentication is required to establish a network connection. It provides an incredible opportunity for the hacker to access unsecured computers on the same network without restrictions. A Man in the Middle (MitM) attack is one of the most common threats to these networks. A MitM attack essentially constitutes a form of eavesdropping. When a device logs into the Web, information is transmitted from point A (user) to point B (service / website), and an intruder may be able to "scan" such transmissions via vulnerabilities. So that's no longer what you thought was private.

The fake AP or known as Rogue AP is a malicious access point placed or setup intentionally by the attacker to deceive the victims to freely connect to the Rogue AP. The greatest threat to free Wi-Fi security is the hacker's ability to place himself between you and the point of connection. So instead of communicating to the hotspot directly, you send your info and data to the malicious hacker, who then relays it. The hacker can access all the data you send over the network while working in this setup: important emails, credit card valuable information and even security credentials for your organization network. Once that valuable information is available to the hacker, he can access your systems and pretending as if he were you to the system.

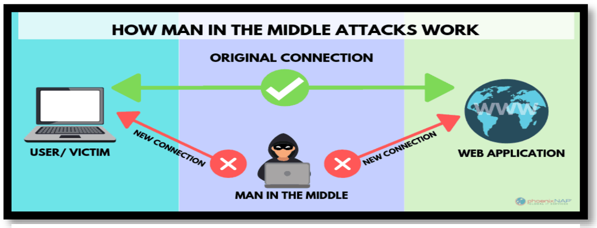


Figure 1. *How MITM attack work*

B. Malware distribution

Hackers could also distribute malware using an unsecured Wi-Fi connection. The hacker will easily plant the infected malicious software on your devices if you permit file sharing across a network. There are also forms, due to technology bugs, that hackers can slip malware on your devices without even thinking about it. A vulnerability in software is a security hole or weakness leakage found in a software or operating system. By manipulating code to target such specific vulnerability, hackers can exploit this weakness and then inject the malware into your device. Some intelligent hackers have successfully hack the link point itself, resulting in a window pop-up that appear during the connection phase offering an update to a common piece of software later. The malware is installed by clicking the window.

Figure 2*. How hacker inject malicious payload to distribute malware in order to gain victims' personal data*

C. Unencrypted networks

Encryption ensures that the messages sent between your device and the wireless router are in the form of a "secret code," so that no one who has the key to decrypt the code can interpret them. Most routers are shipped with default switched off encryption from the factory and must be switched on when the network is set up. If the network is set up by an IT professional, then it is likely that encryption is enabled. There's no way to tell if this happened, though.

D. Malicious attacks through ad hocs.

Ad hocs are peer-to-peer networks which connect two computers directly. When remote workers use a public Wi-Fi network, their devices are likely to be set to discover new networks, making it possible for hackers to connect directly to them. Malicious nodes are intended to deliberately disrupt the routing protocol's correct operation and deny network services where possible. These nodes can use or change sensitive information about the routing. For example, the distance metrics used in standard protocols, such as the number of hops, do not indicate the location of a destination. This is primarily due to the arbitrary distances in the routing protocol between routers. Nevertheless, with knowledge of each node's wireless range, it is feasible to use routing data to determine an upper limit on the physical distance between adjacent nodes, and thus infer information about a node's geographic location. This can help to block malicious nodes on their attacks.

E. Exposure to worm attacks

Worms behave with one key difference, much like viruses. To order to successfully penetrate a process, viruses must have a program to attack, while worms can wreak havoc on their own. You run the risk of a worm traveling from another device that is connected to your computer to the network when connected to a public Wi-Fi. Frequently, a computer network is used to propagate and depends on security vulnerabilities to be reached on the target computer. Worms almost always harm the network at least, even when bandwidth is consumed, while viruses almost always corrupt or change files on a targeted device.

Most worms are only designed to spread and do not seek to change their processes. Nevertheless, even those "free payload" worms can cause serious disruption through an increase in network traffic and other unintended consequences, as Morris and Mydoom have shown.

PREVENTION STRATEGIES TO OVERCOME THEM.

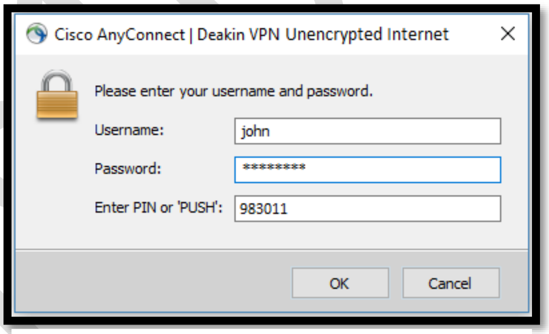
A. Use a VPN

When connecting to your business via an unsecured connection, such as a Wi-Fi hotspot, a virtual private network (VPN) connection must be used. Even if a hacker succeeds in positioning himself in between your connection, the data is strongly encrypted here. Since most hackers are looking for an easy target, the stolen information is likely to be discarded rather than placed through a long process of decryption. A VPN helps you to create a secure Internet connection to another network. VPNs can be used to access regionally limited websites, keep prying eyes from accessing your Internet access and more. These are a good choice for public Wi-Fi networks. The peace of mind and added security are worthwhile though they cost some money. Furthermore, most employers are equipped to connect their employees to a VPN network. And they ought, they ought to. Although workers have access to Wi-Fi networks to do their jobs, the company's data becomes highly vulnerable when they use a public network.

Figure 3. *VPN keep your connection safe from public.*

B. Do not engage any of your personally identifiable information (PII)

You don't treat it as important if you use data via a public Wi-Fi network. So avoid touching any PII at any expense, including account, social security numbers or home addresses if you are expected to use a public Wi-Fi network. Also, you may have to enter stuff such as phone numbers in some accounts when you sign up, so even if you don't also joining, you may have access to personal data unintentionally.



Cisco AnyConnect | Deakin VPN Unencrypted Internet

Please enter your username and password.

Username: john

Password: *********

Enter PIN or 'PUSH': 983011

Figure 4*. Do not enter any sensitive information using public Wi-Fi.*

C. Use SSL connections

If you have no VPN access. You aren't out of luck entirely. An encryption layer can still be added to your connection. Whenever browsing the web, make sure you allow or enable "Using HTTPS only" options on websites you regularly visit, including on all websites requiring you to input some form of credentials (most websites requiring an account or credentials have a "HTTPS" option in their settings). Note that hackers know that you recycle passwords so that your username and password may be the same as your bank or business network for some random forum and that sending them unencrypted might open your door for a smart hacker. The "HTTPS" method is used somewhere in your settings for many web sites needing account or credentials.

Figure 5*. Always use SSL connection to browsing for sensitive information.*

D. Turn Off Sharing

It's doubtful that you want to post anything when connecting to the Internet in a public place. If you first connect to a different, unsafe network, you can switch off sharing from the system preferences or the control panel depending on your OS or allow Windows to switch off it for you. You will want to switch off the features that make it possible for unfrictionally sharing files in your phones in a public network between strangers. On a PC, you can access the Network and Sharing Center, then change advanced sharing settings, then disable file and sharing printers. Go to System Preferences for Macs, then Share and unselect it all. Then go to Finder, press AirDrop, and choose Let me be found by: No One. Only locate and toggle AirDrop off for iOS in the Control Center. And that's it!. Nobody in the area may take your files, or submit one that you don't want.

E. Check What You're Signing Up For (Common Sense)

We know we are probably saying this in vain, before you connecting to a public Wi-Fi internet read the conditions attached. You may not always understand that word, but you should be able to detect any important red flags, particularly what data you collect from your session and what they do with it. If you find the policies involved completely impenetrable, a quick web search will highlight any known problems or problems for other users. Of course, nothing wrong with the terms and conditions they help the Wi-Fi provider secure too but don't just blindly click on any pop-up show. And if you are requested to install additional browser or application plugins, return quickly. Don't Give Away Too Much Info.

Figure 6. Use common sense for any suspicious activity

HOW TO KEEP YOURSELVES SAFE ON PUBLIC WI-FI

Don’t:

- Enable auto-connection to networks for your Wi-Fi.
- Sign into any account via an app containing sensitive information. Please go to the website and check that you use HTTPS before signing in.
- Visit pages that hold sensitive information like economic financial and medical reporting.
- Sign in a non-password protected network.

Do:

- Deactivate file sharing.
- If you do not use Wi-Fi or bluetooth, leave it off.
- Visit websites via HTTPS only.
- Sign out your accounts when you are done.
- To make sure your public Wi-Fi connections are private, use a VPN like Norton Secure VPN.
- Ensure that all remote workers have a firewall enabled on devices at all times.
- Make sure your network and all worker devices are covered by good anti-malware software--including anti-sniffing protection.
- Set up policies regarding the above, and periodically educate workers so they understand the risks and the importance of taking protective steps.

CONCLUSION

Wireless networks are becoming the most rapidly spread technology over the world; thus, they should be well protected, in order to prevent exploitation of confidential data. Public Wi-Fi is a blessing to us all for efficiency and ease, but not at the expense of it. Attackers can easily steal their login credentials, personal information and other data, and every day there is a growing range of software and new exploits. The security flaws increase as technology grows. Encrypt the drive, e-mails and text messages to make it harder for hackers. Hackers or scammers will go after low-hanging fruit and usually won't bother if they are aware of aggressive safety measures being taken by a user. Your data should remain more stable through rest and travel, removing many risks from insecure networks.

HERE I HAVE PROVIDE SOME USEFUL YOUTUBE VIDEO LINKS BELOW

i. How easy is it to capture data on public free Wi-Fi - https://www.youtube.com/watch?v=YzP3ZL4vlkY
ii. Rogue Access Point and Evil Twin - https://www.youtube.com/watch?v=FQ5mCHrC91A
iii. Tips to stay safe on public Wi-Fi by CNET - https://www.youtube.com/watch?v=OXXr5RCIuqE

REFERENCES

1. The risks of public Wi-Fi. (n.d.). Retrieved October 22, 2019, from https://malaysia.norton.com/internetsecurity-privacy-risks-of-public-wi-fi.html.
2. How to Avoid Public WiFi Security Risks. (n.d.). Retrieved October 22, 2019, from https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks.
3. Dolly, J., & IDG Contributor Network. (2018, January 9). Why you should never, ever connect to public WiFi. Retrieved from https://www.csoonline.com/article/3246984/why-you-should-never-ever-connect-to-public-wifi.html.
4. The Hidden Dangers of Public WiFi. (2014, October). Retrieved from http://www.privatewifi.com/wp-content/uploads/2015/01/PWF_whitepaper_v6.pdf.
5. What is Wi-Fi (Wireless Fidelity)? - Definition from Techopedia(no date) Techopedia.com. Available at: https://www.techopedia.com/definition/10035/wireless-fidelity-wi-fi (Accessed: May 26, 2019).
6. Wi-Fi Attacks(n.d) GreyCampus Initiative. Available at: https://www.greycampus.com/opencampus/ethical-hacking/wi-fi-attacks (Accessed: May 26, 2019).
7. Wright, Joshua, and Johnny Cache. *Hacking Exposed Wireless: Wireless Security Secrets and Solutions*. McGraw-Hill Education, 2015.
8. Kan, A. C. (n.d) Attacking WPA Enterprise Wireless Network, Pentest Blog. Available at: https://pentest.blog/attacking-wpa-enterprise-wireless-network/ (Accessed: May 26, 2019).
9. *(PDF) Malicious Attacks on Ad Hoc Network Routing Protocols*. https://www.researchgate.net/publication/228807723_Malicious_attacks_on_ad_hoc_network_routing_protocols.