**Recognizing and Protecting Against Wireless Network Hacking**

Corbin Osman

American Public University System

ISSC459 – Hard Disk and Operating Systems

Mike Lewis

07/23/2023

**Abstract**

In today’s age of technology and its many advances, wireless devices and networks are used in households, vehicles, aircraft, hospitals, and other places of business. The world relies on the ability to connect to the internet and other networks to communicate with others, send and receive communications, store and analyze information, and secure confidential and sensitive information. Due to its nature, along with the valuable information that is secure and shared, networks and devices are often the targets of attacks. Malicious actors seek to perform attacks against others with the intent of personal gain or gratification, which at times leaves their victims in unfortunate situations.

With attackers seeking to steal or destroy data, systems and networks, it is important for users to understand how their attacks work and what can be done to protect against them. With wireless networks being a common target for attackers, it is important for users to understand what wireless attacks are, how they are performed, what information and data may be at risk of being attacked, how they can recognize and counter specific attacks, and how to mitigate and protect against the attacks of malicious actors.

**What are Wireless Attacks?**

Wireless networks can cover a wide range of fields and definitions. In turn, wireless attacks can also have varying definitions and may envelop different areas. To better understand what a wireless attack entails, it can be helpful to understand what a wireless network or device is. In an article by Margaret Rouse on wireless networks, the author defines wireless networks as “computer networks that are not connected by cables of any kind. The basis of wireless systems are radio waves.” (Rouse, 2023). These networks allow users to connect devices such as phones, laptops and desktop computers to the internet and other devices that may also be connected to the network. This grants users the ability to communicate with others and access information and resources online in a quick and simple manner.

While wireless networks offer incredible tools and utility to users, they are often the target of attacks by malicious parties. Wireless attacks are executed with the usual intent to steal, alter, or destroy data, systems, and network resources (Forcepoint). There are two main types of wireless attacks: active and passive. In active wireless attacks, malicious actors generally seeks to modify, decrypt or destroy data and systems. Passive attacks are more docile in nature by accessing networks and devices with the intent to monitor or steal information and data without making changes to systems, accounts and settings (Forcepoint).

**What Information is Targeted in Wireless Attacks?**

Now that a basic understanding of wireless attacks is established, we can look further into the intent of a malicious party and learn what their targets are when deploying wireless attacks. A few of the areas that are targeted are personal and home environments, business and professional locations, and public areas such as libraries, airports, and restaurants. We will look at each of these areas briefly and explore some of the common targets of these attacks.

In home and personal environments, confidential and sensitive information are often present. Personally identifiable information such as one’s social security number, date of birth, medical records and bank information are sometimes shared online with others who are authorized to handle such data. Malicious parties may attempt to capture this information as it is being shared across the network or online with others. Ravi Sen, a cybersecurity researcher, shares that personally identifiable information can be used in identity theft, and is unfortunately common after one’s personal information is compromised (Sen, 2021). Additionally, attackers sometimes try to access a network to use it for personal gain, such as sending communications, downloading data in bulk, and passively monitoring internet traffic.

Malicious actors often target public locations with the same intent as those who attack home networks. Locations such as libraries, restaurants, and airports often offer a network access point for visitors to connect their devices to so that they can access the internet. While these offer a convenient way for users to access the internet from their personal devices, it also invites attackers to visit these locations and try to capture incoming and outgoing internet traffic. This can be done with the hope of capturing confidential personal information and communications, and usually occurs without the victim knowing that their information was exposed.

The final of these commonly targeted locations are business and organizational environments. These locations regularly store and share both sensitive client information and confidential business plans and data. The quantity of data that is shared and secured makes these environments a prime target for malicious parties, as they may be able to gain access to a large amount of information with minimal effort. Additionally, attackers may also target systems and administrator accounts that have elevated privileges with the intent of making changes to settings and other features. In each of these environments, it is critical that users and administrators understand what is at risk and know how to recognize and respond to wireless attacks,

**Types of Network Attacks and Hacking Methods**

With a better knowledge of common targets of wireless attacks, let us now explore specific types of attacks that are often performed. We will first look into attacks that are passive in nature and then move on to more active attacks.

The first category of attacks cover a range of passive wireless hacking methods which malicious parties employ. A common attack that is often used in public locations is Wi-Fi spoofing, also known as a rogue access point. This is performed by setting up a wireless access point that poses as a legitimate available network which users can freely connect to (Ranjan, 2023). The intent of setting up and employing such a network is the hope that users will connect to the network and offer up their incoming and outgoing traffic unknowingly. The unsuspecting victim may use this rogue connection point for personal tasks such as logging into accounts and sending text or email communications, and the party behind the attack is able to use tools to capture the information as it is in being transferred. This action is also known as packet sniffing, where the malicious actor monitors traffic for specific packets of data or information that can be of value. To protect against falling victim to a rogue access point, it is recommended to avoid public wireless connections when possible. A fake access point can often appear to be legitimate, which is why many users fall for its scheme. If you have to use a public connection point, it can be helpful to utilize services such as VPNs that help to encrypt network traffic, further securing it from others who may be attempting to capture information.

Another similar passive attack is the act of searching for wireless access point connections that can be exploited and accessed. A malicious actor may search within a set area for connection points that are less secured or utilizing less advanced encryption with the intent to later attempt to access these wireless networks. A few common instances of these attacks are wardriving, warwalking, war-cycling, and war-flying. As can be deduced, each of these involves moving around an area in a vehicle, on foot, or on a bicycle while scanning for vulnerable networks. The latter is often performed with an aerial machine such as a drone or plane, which can allow for the scanning of a large amount of wireless networks in a short time. To help prevent attackers from scanning your network, it is smart to use strong encryption algorithms and set up a complex password for the network to prevent easy intrusion. One personal devices are connected to a home network, it can also be helpful to turn off the broadcasting of your network to keep it from being visible to others.

Moving on, we will now explore a few common active attacks which users should look out for. The first basic group of attacks are direct encryption attacks on wireless networks. A few examples of encryption algorithms are WEP, WPA, and WPA2. These encryption methods utilize keys to encrypt information so that it is unreadable to those who do not have the key to decrypt the information (Ranjan, 2023). This practice helps to keep confidential and sensitive information secured should it be viewed or accessed by unauthorized parties. Once a malicious actor has captured or has access to the data and information, they can then begin to use tools and services that work to decrypt the original contents of the data. It can be difficult to protect against this type of direct attack on data once it is in the hands of an attacker, so to secure information it is recommended to use networks and sites that are trusted so that data is at a lower risk of being captured.

Another category of active attacks are those which disrupt or damage wireless network connections. An example of this type of attack is a denial-of-service attack, also known as a DOS attack. These attacks are designed to generate a strong enough signal or enough traffic to intentionally cause interference (CT WiFi, 2017). There are many reasons as to why one might use such an attack against a network, and denial-of-service attacks can actually occur unintentionally as well. It may be difficult to prevent one of these attacks, but measures can be taken to help prepare for such an incident by having a recovery or response plan.

The final type of attack to be discussed in this paper is focused on social engineering. This type of attack works by manipulating individuals into providing information to the malicious party, such as account credentials, personal information, business plans, and more. These attempts relate to wireless networks when the target of such an attack is a specific wireless network or device. The attacker may use social engineering techniques to coerce the victim into sharing information about the network, such as what the network login credentials are, what type of encryption is being used, what devices are connected to the network, etc. This gives the attacker knowledge about the network which they can then use when attempting to later launch an attack. The best way to protect against social engineering attacks is to look for warning signs from communications. Whether the attack be attempted by phone, text, email, or even through the mail, it is important to remain educated on securing confidential information and not sharing private information (CT WiFi).

**Strong Practices for Protecting Against Wireless Attacks**

With a greater understand of the types of wireless attacks and general ways to protect against them, let us now look at strong practices to teach and employ to further protect against these attacks.

The first step to securing a wireless network access point is to ensure that it is not using default settings and credentials. Keeping the default username and password for an access point allows knowledgeable intruders to easily connect to your network, as these default logins are readily available online for attackers to search. As previously mentioned, it can also be helpful to disable SSID broadcasting to protect against attacks such as wardriving (Waqas, 2022). This will hide the network and keep it hidden from other parties who may be searching for networks and their potential vulnerabilities.

As with all devices and networks, utilizing the strongest available encryption methods and algorithms is a crucial step in securing against wireless attacks. Encryption such as WPA2 or higher will strengthen a wireless network and make it more difficult for attackers to gain access to the network (Waqas). In both personal and business environments, it is also good practice to have all users routinely update their passwords and other login credentials, as this helps ensure that unauthorized parties cannot maintain access to a network or device should they know a set of credentials. Additionally, where possible, it can be helpful to implement two-factor or multi-factor authentication to further ensure that only authorized users can access the network as intended.

Finally, the utilization of security software can help to secure a wireless network and the devices connected to it. Using a firewall on a router helps to block traffic that is not authorized, whether it be incoming or outgoing. The types of data that are and are not allowed can be configured by the user or administrator deploying the firewall, which can be adjusted to meet certain needs. Another piece of software that can help secure a device or network is antivirus software. This helps to secure and sanitize a device or network after an attack may have been performed, searching for potentially harmful data. They can also run in real-time to regularly monitor data and information as it is downloaded.

**Conclusion**

In summary, it is important for all users to consider the risks and vulnerabilities their wireless networks and devices have. Wireless attacks and hacking attempts are very common in today’s world, especially due to how often our confidential information is shared. Attacks and data breaches cause millions of individuals’ information to be leaked and accessed each year, which places them at greater risk of events such as identity theft and account takeovers.

Protecting and securing wireless networks and devices should be at the forefront of the minds of both users and administrators, in all types of environments where technology is used, and information is stored. Wireless attacks can occur at any time and vary in form and severity, which is why it is important that users learn what type of attacks to look out for, what information may be at risk of being targeted, and what they can do to protect against the hacks of these attackers.

**Resources**

CT WiFi. (2017, June 13). Types of Wireless Attacks. *Blog.ct-networks.io*. https://blog.ct-networks.io/types-of-wireless-attacks-9b6ecc3317b9

Forcepoint. (n.d.). What is a Network Attack? *Forcepoint.com*. https://www.forcepoint.com/cyber-edu/network-attack#:~:text=Network%20attacks%20are%20unauthorized%20actions,gain%20access%20to%20internal%20systems.

Ranjan, A. (2023, March 21). Types of Wireless and Mobile Device Attacks. *Geeksforgeeks.org*. https://www.geeksforgeeks.org/types-of-wireless-and-mobile-device-attacks/

Rouse, M. (2023, June 16). What Does Wireless Network Mean? *Techopedia.com*. https://www.techopedia.com/definition/26186/wireless-network

Sen, R. (2021, May 13). Here’s how much your personal information is worth to cybercriminals – and what they do with it. *Theconversation.com*. https://theconversation.com/heres-how-much-your-personal-information-is-worth-to-cybercriminals-and-what-they-do-with-it-158934

Waqas. (2022, February 9). Wireless Network Security Best Practices. *Hackread.com*. https://www.hackread.com/wireless-network-security-best-practices/