**Investigation and Analysis of Wireless Attacks**

Corbin Osman

American Public University System

ISSC456 – Digital Forensics: Investigating Wireless Networks and Attacks

Mike Lewis

04/23/2023

**Abstract**

The protection and security of systems, locations and information is important in the world that we live in today. With modern advancements in technology there are many reasons to secure devices, networks and systems from potential attacks and threats. Many developments help to aid in positive uses of technology, though there are some who use devices to take advantage of others. One of the ways this is performed is through the use of wireless attacks.

The focus of this paper will be on the investigation and analysis of different wireless attacks. The scope and goal are to grow in knowledge and understanding of how wireless attacks are performed, what types of accounts, systems, networks and devices may be targeted, and what methods and practices are available to help with mitigating the effects of attacks. The purpose and intent are to help readers be more aware of and understand what network attacks are, what information and data may be at risk of being attacked, how to recognize and counter specific wireless attacks, and how to protect and secure against the attacks and efforts of malicious actors.

**What are Wireless Attacks?**

Within the field of technology there are many ways to perform attacks on systems, accounts and networks. Some digital attacks focus on gaining access to systems and servers that house confidential and sensitive data to capture the information for personal gain and benefit, and others may be performed with the intent to disrupt or destroy systems and networks to interfere with another’s ability to function digitally. With the vast world of technology used worldwide there are many different types of attacks and reasons for one to utilize technology to attack another.

One avenue of attacks is known as wireless attacks, which is where malicious actors usually attack wireless devices and networks to change, delete, or steal data and information (Forcepoint). These attacks can be performed against a personal wireless device or network such as a home router or personal phone or against business and professional devices and networks. These attacks can be further narrowed down between active or passive attacks. Active wireless attacks usually involve modifying data, disrupting systems and services, and deleting or stealing information. Passive wireless attacks are often more focused on monitoring devices and networks and accessing accounts or systems without making changes or disrupting services (Forcepoint).

**What Information and Systems are at Risk from Wireless Attacks?**

Before learning about different forms of wireless attacks it can be beneficial to understand what might be targeted. With much of the world relying on digital technology a lot of our personal information is stored and shared in an online environment. Email accounts can contain confidential information that is shared with others, and social media accounts can contain personal information such as one’s date of birth, their profession, where they live, potential relatives, and other data. This information can be used by attackers to affect the lives of others and should be secured where possible.

Information and data more commonly targeted in wireless attacks are those which can be useful in the hands of an attacker. One example of data can be personally identifiable information such as one’s social security number, date of birth, debit and credit account information, address and medical history. These can be used by attackers to access and withdraw funds from accounts, apply for new credit or debit accounts, open utility accounts, and many more unauthorized actions. Another example of data that can be targeted is confidential business and corporate information. Examples of this can be business plans, client and employee personal information, and important documents and files containing sensitive information.

Information and data are one part of the targets in wireless attacks. Other common targets are business and personal systems and servers which run services and contain information that may be needed to perform certain functions. A few examples of this are as follows. An attacker can write an email posing as the true individual if they gain access to their personal email account. A website clients use to log in to their account is attacked and inaccessible for a period of time. Systems and devices that protect networks from suspicious incoming traffic are disrupted and not working as intended. These are examples of ways wireless attacks can hinder organizations and individuals with their involvement with technology.

**Types of Wireless Attacks**

With an understanding of why wireless attacks are performed and what their purpose and targets may be, let us now explore different types of wireless attacks. The following are several common wireless attacks that should be considered and prepared for. The first couple of attacks will be more passive in nature and the latter will be active attacks.

Freeloading is the act of an unauthorized user accessing a wireless network to gain free access to network services (Wilkins, 2011). This can be done without malicious intent, though there can be unintended consequences and effects through doing so. A few possible downsides can be experiencing a slower internet or network connection, confidential information may be viewed or accessed by unauthorized users, and dangerous software and data may be transmitted to or from the host network. These actions could result in disruptions or harm to the host network and its legitimate users.

Another attack that can be performed is passive capturing or eavesdropping. This occurs when wireless networks and devices are monitored or scanned for data and services that can be accessed. An example of eavesdropping can be through wardriving, which is where an actor drives around a specific area scanning for wireless connection points or devices that are unsecured and can be easily accessed (CT Wifi, 2017). Eavesdropping or passive capturing can also be utilized to listen in to the data communications occurring within a network to capture sensitive information.

Moving on from passive attacks, we will look at a few examples of active and aggressive attacks. A denial of service (DoS) attack occurs when an attacking party sends a large amount of data to increase the amount of incoming or outgoing traffic for various reasons. One such reason can be to interrupt the services or connections of a service or network, and another reason can be to disrupt security services allowing the attackers to gain access to resources or accounts (Wilkins, 2011). Denial of service attacks can also be performed by implementing viruses or worms into data packets that are then received or distributed by networks, resulting in the malicious software affecting the network or devices.

Rogue access points or evil twin attacks are performed through the use of a router or wireless connection point that poses as a legitimate connection point. These will generally be located in an area where they are to appear to be the real wireless connection point when it is in fact a clone or replacement (Wilkins, 2011). The intent behind such an attack is to trick users into believing it is the true network, and in connecting to the rogue access point they may share confidential information that can then be captured by the malicious host.

Peer-to-peer attacks are accomplished through using a device or networks to attack other devices or networks that are connected to the same access point (CT Wifi, 2017). These devices may contain software which can be used to launch attacks such as packet sniffing, password cracking and data capturing on other devices also connected to the same network. This can prove fatal as it may be more common on publicly accessible networks where many users connect their own personal devices daily. In utilizing less secure connection points users risk their devices and information being compromised through peer-to-peer or similar attacks.

**How to Recognize and Protect Against Wireless Attacks**

With a knowledge of different types of wireless attacks, it is important to understand how to recognize them and protect against their effects. Detecting wireless attacks can prove to be difficult if one does not know what to look for. Implementing a firewall onto devices or networks you use can help to detect potentially suspicious data and prevent it from entering and affecting the device or network. Utilizing wireless network analyzing tools such as Wireshark can also be useful in monitoring network traffic and detecting unwanted data and information.

Securing a network and the devices connected to it is important to ensure that data and information is secure from unauthorized access and viewing. Utilizing a strong wireless encryption such as WPA2 or WPA3 will help ensure that a stronger encryption method is employed. Additionally, the default home network name and Wi-Fi password should be changed to ensure that unauthorized users cannot access the network through the default credentials (Malviya, 2021). The same should be performed for the router console page, ensuring that the default username and password are changed as well.

To help protect against unauthorized users locating a wireless connection point it can be helpful to disable SSID broadcasting. While it can be convenient for it to appear on its own when attempting to connect a device to the network, this can prove to be a vulnerability as this will also allow others to see the network when nearby. Disabling SSID broadcasting will help to ensure that the network remains hidden from those not actively connected to it (Waqas, 2022).

**Strong Practices in Securing Wireless Networks and Devices**

In both personal and professional environments there are many strong practices that can be employed to better secure wireless networks and devices from potential wireless attacks. With all devices and networks, it is important that they be kept up to date with the latest patches and software updates to ensure that security policies and features are working as intended. Additionally, it can prove useful to disable both remote access and remote administration tools as they can result in vulnerabilities for a network or device (Waqas, 2022).

In professional environments it is important that strong security policies and procedures are in place to ensure that systems, accounts and networks are secured from potential vulnerabilities and attacks. Proper training and monitoring of employees can help introduce new policies and raise awareness of the importance of securing wireless networks and devices. Security administrators should routinely monitor networks and their features to ensure that security levels are where they are intended and find any potential vulnerabilities to wireless attacks.

Whether at home or in a business environment ensure that users utilize strong passwords for accounts, servers and networks. This can help to prevent parties attempting to crack passwords and access resources. Further, ensure that policies governing the sharing of files are in place. Confidential and sensitive work information that may be transmitted outside of the work area should be done so with proper encryption and only on trusted networks to ensure that unauthorized individuals and parties do not gain access to the information or data.

**Conclusion**

In review of wireless attacks and strong practices to protect against them, it is important to recognize the impact they can have and how common they are in today’s world. Wireless attacks can come at any time and their intent and purpose may be for varying reasons. Whether the wireless attack be performed against a home or personal network or against a business network, similar practices and policies can be followed to secure against such attacks and exploits. By recognizing wireless attacks and securing networks and devices in advance, users can secure their confidential information and data and protect themselves and those around them from wireless attacks.

**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.

Malviya, N. (2021, February 2021). Wireless Attacks and Mitigation. *Resources.infosecinstitue.com*. https://resources.infosecinstitute.com/topic/wireless-attacks-and-mitigation/

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

Wilkins, S. (2011, November 2). Be Aware of These 7 Common Wireless Network Threats. *Pluralsight.com*. https://www.pluralsight.com/blog/it-ops/wireless-lan-security-threats