International Journal of Science and Research (IJSR)
ISSN: 2319-7064
SJIF (2022): 7.942

The Vulnerabilities, Threats and Counter measures in Wireless Network Security

Rakesh S Kale

rakeshkale. model[at]gmail.com

Abstract: ***The advent of wireless networking has brought about several advantages but also introduced new security risks that alter an organization's overall information security risk profile. Even though implementing technological solutions is the typical response to vulnerabilities and threats, wireless security is primarily a management issue. To effectively manage the threats associated with wireless technology, it is necessary to develop a plan to mitigate identified risks and conduct a comprehensive risk assessment. We have created a framework to assist managers in comprehending and assessing the various risks associated with using wireless technology. Additionally, we explore several approaches to prevent those risks.***

Keywords: Wireless Network, Wireless Security, Wireless Threats, Etc.

1. Introduction

The utilization of wireless networking provides numerous advantages, such as increased productivity due to easier access to knowledge resources, simplified and cost - effective network configuration and reconfiguration. However, wireless technology also brings about new security risks that alter an organization's information security risk profile. For instance, the risk of interception is higher in wireless networks due to communication occurring "through the air" using radio frequencies. If messages are not encrypted or are encrypted using an inferior algorithm, the confidentiality of the information may be compromised. Although wireless networking modifies the risks associated with various security threats, the fundamental security objectives of maintaining confidentiality, ensuring integrity, and preserving the availability of information and information systems remain the same. Wireless networks are prevalent due to their ease of integration with other networks and components, cost - effectiveness, and convenience. Nowadays, most consumer laptops come with pre - configured wireless networking technology, providing benefits such as convenience, mobility, productivity, deployment, expandability, and cost - effectiveness. Despite these advantages, wireless network technology also has its drawbacks and may not be suitable for certain networking scenarios due to inherent limitations. Security, range, reliability, and speed are among the shortcomings of utilizing a wireless network. Network administrators encounter various issues with wireless networks, including unauthorized access points, broadcasted SSIDs, unknown stations, and spoof MAC addresses. To address these concerns, most network analysis vendors provide WLAN troubleshooting tools or features in their product lines, such as Network Instruments, Network General, and Fluke.

Wireless Vulnerabilities, Threats and Counter measures:

Wireless networks consist of four key components: the transmission of data over radio waves, access points that connect to the corporate network and/or client devices (such as laptops and PDAs), and users. Each of these components presents a possible entry point for a potential attack that can compromise one or more of the fundamental security objectives of maintaining confidentiality, ensuring integrity, and preserving availability.

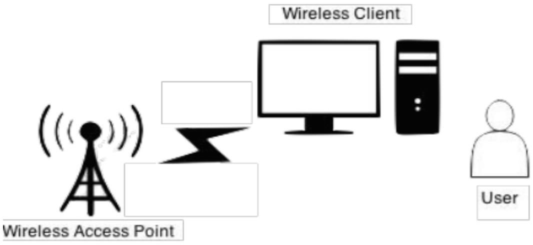

Figure 1: Wireless networking components

2. Network Attacks

2.1 Accidental Association: Unauthorized access to both wired and wireless business networks can occur through various means and motives. One of these methods is known as "accidental association," where a user unwittingly connects their computer to a wireless access point from an overlapping network of a nearby company. This result in a security breach, as sensitive company information, is unintentionally exposed, potentially creating a link between the two businesses. This risk is further compounded if the laptop is also connected to a wired network.

2.2 Malicious Association: "Malicious associations" occur when attackers purposely use their cracked laptops to connect to a company network instead of using a legitimate access point (AP). These laptops, also known as "soft APs, " are created when a hacker utilizes specific software to make their wireless network card appear to be a genuine access point. Once connected, the attacker can install Trojans, launch attacks on the wired network, and obtain passwords. While Layer 3 security measures, such as network authentication and virtual private networks (VPNs), can aid in security, they are ineffective for wireless networks as they operate at the Layer 2 level. Even wireless 802.1x authentications, which do enhance security, are still vulnerable to hacking.

2.3 Ad – hoc Networks: Ad - hoc networks can pose a threat to your security. These are peer - to - peer networks that allow wireless computers to connect directly without an access point in between. Ad - hoc networks are often insecure, but encryption techniques can be utilized to improve their security.

2.4 Non– traditional networks: Personal network Bluetooth devices and other non - traditional networks can be vulnerable to hacking and must be considered a security threat. Even devices like barcode readers, wireless printers and copiers, and handheld PDAs should be secured to prevent unauthorized access. IT personnel may overlook these non - traditional networks because they tend to focus primarily on laptops and access points.

2.5 Identity theft (MAC spoofing): MAC spoofing, also known as identity theft, is a type of attack in which a malicious actor can eavesdrop on network traffic and identify the MAC address of a device that has network privileges. To mitigate this, most wireless systems allow MAC filtering, which permits only authorized devices with specific MAC IDs to access the network. However, there are various software programs with network sniffing capabilities that can circumvent this. In addition, attackers can use other software to pretend that their device has any MAC address they want, making it easy for them to bypass this protection.

2.6 Man - in - the – middle Attacks: The technique known as a man - in - the - middle attack is when an attacker tricks computers into connecting to a computer that is acting as a soft access point. This allows the hacker to connect to a legitimate access point through another wireless card, which in turn creates a steady flow of traffic through the transparent hacking computer to the real network. Once the traffic is flowing, the hacker can intercept and analyze the traffic. The de - authentication attack is another type of man - in - the - middle attack that takes advantage of security vulnerabilities in challenge and handshake protocols. This attack forces connected computers to disconnect from the legitimate access point and reconnect with the attacker’s soft access point. The process of man - in - the - middle attacks can be automated by software like LANjack and Air Jack, which has made it easier for even novice attackers to execute these types of attacks. Hotspots are especially vulnerable to these attacks since they often lack security measures.

2.7 Denial of Service: When an attacker keeps sending bogus requests, premature successful connection messages, failure messages, or other commands to a targeted AP (Access Point) or network, it results in a Denial - of - Service attack (DoS). This type of attack can prevent legitimate users from accessing the network and can also cause the network to crash. These attacks take advantage of protocol vulnerabilities, such as the Extensible Authentication Protocol (EAP).

2.8 Network injection: A network injection attack is a type of attack that exploits access points that are vulnerable to non - filtered network traffic, particularly broadcasting network traffic such as “Spanning Tree” (802.1D), OSPF, RIP, and HSRP. The attacker injects fraudulent network reconfiguration commands that affect routers, switches, and intelligent hubs. This type of attack can cause a network to crash entirely, requiring a reboot or even reprogramming of all intelligent networking devices.

3. Securing Wireless Communications

Wireless communications pose three primary threats: Interception, Alteration, and Disruption.

3.1 Safeguarding Wireless Communications Confidentiality There are two countermeasures to reduce the risk of eavesdropping on wireless transmissions. The first method involves making it harder to locate and intercept wireless signals, while the second involves using encryption to maintain confidentiality even if the wireless signal is intercepted.

3.1.1 Concealing Signal Techniques to intercept wireless transmissions, attackers need to identify and locate wireless networks. However, organizations can take several measures to make it more difficult to locate their wireless access points. The following are the easiest and least expensive options: Turning off the broadcasting of the service set identifier (SSID) by wireless access points, Assigning cryptic names to SSIDs, Reducing signal strength to the lowest level that still provides requisite coverage, or Locating wireless access points in the interior of the building, away from windows and exterior walls. More effective but expensive methods for reducing or hiding signals include: Using directional antennas to constrain signal emanations within desired coverage areas or Using signal emanation - shielding techniques, also known as TEMPEST, to block the emanation of wireless signals.

3.1.2 Encryption encrypting all wireless traffic is the best way to protect the confidentiality of information transmitted over wireless networks. This is particularly important for organizations subject to regulations.

3.2 Preventing the Modification of Intercepted Communications Interception and alteration of wireless transmissions can lead to "man - in - the - middle" attacks. Two countermeasures can significantly decrease the risk of such attacks: strong encryption and robust authentication of both devices and users.

3.3 Countermeasures to Mitigate Denial - of - Service Attacks Wireless communications are vulnerable to denial - of - service (DoS) attacks. Organizations can take several steps to reduce the risk of such unintentional DoS attacks. Careful site surveys can identify locations where signals from other devices exist, and the findings of such surveys should be used when deciding where to locate wireless access points. Regular periodic audits of wireless networking activity and performance can identify problem areas, and appropriate remedial actions may include removing the offending devices or measures to increase signal strength and coverage within the problem area.

4. Securing Wireless Access Points

Wireless access points that are insecure or poorly configured can lead to unauthorized access to the network, and compromise the confidentiality of the transmitted information. To secure wireless access points, organizations should take the following three countermeasures:

1) Eliminating any rogue access points that are unauthorized or unmonitored;
2) Properly configuring all authorized access points to ensure they adhere to security standards and guidelines; and
3) Using the 802.1xs protocol to authenticate all devices accessing the wireless network. By taking these steps, organizations can minimize the risk of unauthorized access to their wireless networks and protect the confidentiality of their data.

5. Securing Wireless Client Devices

Wireless client devices face two significant threats: loss or theft and compromise. Losing or having laptops and PDAs stolen is a critical concern since they often contain confidential and proprietary data. Such an incident may result in the organization violating privacy regulations regarding the personal identifying information collected from third parties. Compromise is another threat that wireless client devices face, as attackers can use it to access sensitive data stored on the device or obtain unauthorized access to other system resources.

6. Securing Wireless Networks:

6.1 Encryption

One of the most effective ways to secure a wireless network is to encrypt communications over the network. Most wireless routers, access points, and base stations come with built - in encryption mechanisms, but it's important to ensure that the encryption feature is turned on. If your wireless router does not have an encryption feature, consider getting one that does.

6.2 Anti - virus and Firewall Protection

Computers on a wireless network require the same protection as those connected to the Internet. Install anti - virus and anti - spyware software, and keep them updated. Turn on your firewall if it was shipped in the "off" mode.

6.3 Training and Educating Users

Users are a vital component of wireless network security. As with wired networks, it's crucial to train and educate users about secure wireless behaviour. Regularly repeating user training and education is essential for ensuring effectiveness.

6.4 Network Auditing

Wireless network auditing is a crucial aspect of WLAN security policy. The network must be regularly audited for rogue hardware. Scanning and mapping tools such as nets tumbler and Waveland - tool can be used to identify all access points and WLAN nodes. Specialized tools like Air Snort can be used for WEP cracking and auditing the network for weak keys, key reuse, and WEP security settings. These tests are similar to those used by hackers to gain unauthorized access to the network.

7. Conclusion

Wireless networking has revolutionized the way organizations operate, providing cost - effective and efficient solutions to improve productivity. However, it also brings new security risks that require a systematic approach to assessing and managing risk. While it is impossible to eliminate all risks, this paper has outlined various countermeasures that can be used to mitigate those risks associated with wireless clients, access points, and the transmission medium. In addition, it emphasized the need to educate and train users in safe wireless networking procedures to maintain a reasonable level of security. By adopting these strategies, organizations can confidently embrace the benefits of wireless networking while protecting their valuable assets.

References

[1] Gupta, B. B., & Gupta, A. (2014). Wireless Network Security: Vulnerabilities, Threats, and Countermeasures. International Journal of Computer Applications, 97 (11), 14 - 18.

[2] Choudhary, P., & Choudhary, D. (2013). Security Analysis of Wi - Fi Protected Access II (WPA2). International Journal of Computer Science and Mobile Computing, 2 (4), 173 - 178.

[3] Singh, R., & Kumar, A. (2015). A Study of Wireless Security Protocols: WEP, WPA, and WPA2. International Journal of Computer Applications, 120 (6), 30 - 35.

[4] Sharma, S., & Singh, S. (2018). Wireless Security and Its Countermeasures: A Review. In Proceedings of the 3rd International Conference on Inventive Systems and Control (pp.1270 - 1274). IEEE.