WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Wireless Network Security: Vulnerabilities, Threats and Countermeasures

Ajay Radhakrishnan Nair

Keraleeya Samajam Model College Dombivli (W) Email: nair.ajayr99@gmail.com

ABSTRACT :

Wireless networking offers numerous benefits, but it also introduces new security threats and changes the overall risk profile of an organization's information security. Addressing wireless security threats typically involves implementing technological solutions, but fundamentally, managing wireless security is a leadership responsibility. Effective management of wireless technology risks requires a comprehensive and well-informed risk assessment specific to the environment, followed by the formulation of strategies to mitigate identified risks. This document outlines a framework designed to assist managers in understanding and evaluating the diverse threats posed by wireless technologies and suggests various strategies to counter these threats.

Keywords : Wireless Network, Wireless Security, Wireless Threats, Signal-Hiding

Introduction

Wireless networking brings numerous advantages, enhancing productivity through more accessible information resources. It simplifies network configuration and reconfiguration, making these processes quicker and more cost-effective. However, wireless technology also introduces new security threats and modifies the existing risk profile of information security. For instance, since wireless communication uses radio frequencies, it is more susceptible to interception than wired networks. If data is not encrypted or only weakly encrypted, it risks being intercepted, compromising the confidentiality of the information. While wireless networking changes the nature of some security risks, the core objectives of maintaining confidentiality, integrity, and availability of information and systems remain unchanged. This paper aims to equip managers with a foundational understanding of the various threats posed by wireless networking and the countermeasures available.

Wireless networks are widely adopted for their convenience, cost-effectiveness, and seamless integration with other networks and components. The majority of consumer computers now come with built-in wireless networking technology. The primary advantages of wireless networks include convenience, mobility, productivity, easy deployment, expandability, and cost-efficiency.

Despite these benefits, wireless network technology has its drawbacks. In certain networking contexts, the disadvantages may outweigh the advantages. These disadvantages stem from the inherent limitations of the technology, including issues related to security, range, reliability, and speed.

For network managers, wireless networks pose several challenges. Issues such as unauthorized access points, broadcasted SSIDs, unrecognized stations, and spoofed MAC addresses are common problems that need addressing in WLAN troubleshooting. Several network analysis vendors like Network Instruments, Network General, and Fluke provide WLAN troubleshooting tools and functionalities within their product offerings.

Wireless Vulnerabilities, Threats and Countermeasures

The wireless networks consist of four basic components: The transmission of data using radio frequencies; Access points that provide a connection to the organizational network and/or the Client devices (laptops, PDAs, etc.); and Users. Each of these components provides an avenue for attack that can result in the compromise of one or more of the three fundamental security objectives of confidentiality, integrity, and availability.

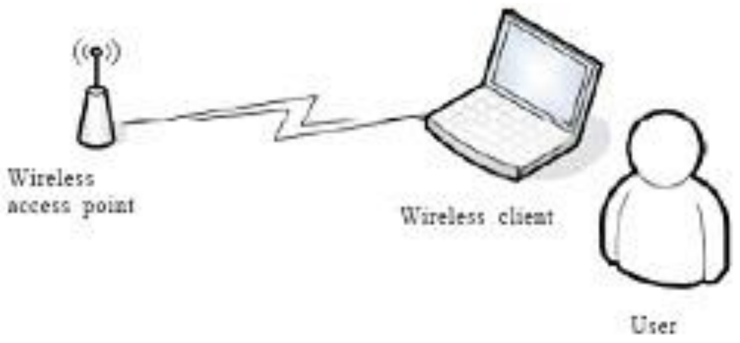

Fig. 1 Wireless networking components

Wireless Network Attacks

Accidental association

Unauthorized access to corporate wireless and wired networks can occur through various methods and for different reasons. One common method is known as "accidental association." This happens when a user's computer automatically connects to a wireless access point from a nearby company's network that overlaps with their own. Often, the user might not even realize this connection has occurred. This scenario poses a security risk as it could expose sensitive company information and potentially create an unintended link between the two companies' networks. This risk is particularly significant if the computer is simultaneously connected to a wired network.

Malicious association

Malicious associations" occur when hackers use their laptops to create fake access points, known as "soft APs," to trick wireless devices into connecting to them instead of legitimate company access points (APs). By running software that makes their network card appear as a genuine AP, hackers can infiltrate the network. Once connected, they can steal passwords, launch attacks on the wired network, or install trojans. Wireless networks, which operate at the Layer 2 level, are vulnerable because traditional Layer 3 security measures like network authentication and virtual private networks (VPNs) are ineffective against these attacks. While Wireless 802.1x authentication does provide some level of protection, it is still susceptible to these kinds of security breaches. Typically, the hacker's objective with this type of attack is not necessarily to penetrate VPNs or other security defences but rather to gain control over the client device at Layer 2.

Ad-hoc networks

Ad-hoc networks, which are direct connections between wireless computers without an intermediary access point, can present security risks. These networks typically lack robust security measures, making them vulnerable. However, implementing encryption methods can enhance their security and protect against unauthorized access.

Non-traditional networks

Non-traditional networks, including personal Bluetooth devices, barcode readers, handheld PDAs, and wireless printers and copiers, also pose security risks and are susceptible to hacking. Despite their ubiquity in daily operations, these devices often receive less attention from IT personnel who may primarily concentrate on securing laptops and access points. It's crucial to extend security measures to cover these non-traditional networks to prevent unauthorized access and data breaches.

Identity theft (MAC spoofing)

Identity theft, often through MAC spoofing, happens when a hacker monitors network traffic to capture the MAC address of a computer with network privileges. Many wireless systems use MAC filtering as a security measure, restricting network access to computers with specific, pre-approved MAC addresses. However, the effectiveness of MAC filtering can be compromised by the availability of network "sniffing" programs. These tools, combined with software that allows a hacker to emulate any desired MAC address, can enable unauthorized access, effectively bypassing the MAC filtering security.

Man-in-the-middle attacks

A man-in-the-middle (MITM) attack occurs when a hacker sets up a computer to act as a fake access point (soft AP), tricking other computers into connecting to it. Once connected, the attacker then links this soft AP to a legitimate access point using another wireless card. This setup allows the hacker to facilitate a steady stream of data between the victim's computer and the real network, enabling them to intercept ("sniff") the traffic.

One common form of MITM attack exploits vulnerabilities in challenge and handshake protocols to conduct a "de-authentication attack." This type of attack disrupts the connection between computers and their legitimate access point, forcing them to reconnect through the hacker's soft AP.

The complexity of executing MITM attacks has been significantly reduced by tools like LANjack and AirJack, which automate many of the steps involved. As a result, even less technically skilled individuals, often referred to as "script kiddies," can carry out these attacks. Public Wi-Fi hotspots are especially susceptible to MITM attacks due to their typically minimal security protections.

Denial of service

A Denial-of-Service (DoS) attack targets an access point (AP) or network by overwhelming it with a flood of bogus requests, premature successful connection notifications, failure messages, and other disruptive commands. This barrage of data can prevent legitimate users from accessing the network and, in severe cases, may even cause the network to crash. DoS attacks often exploit weaknesses in network protocols such as the Extensible Authentication Protocol (EAP), taking advantage of protocol-specific flaws to magnify the impact of the attack.

Network injection

In a network injection attack, a hacker targets access points that are exposed to non-filtered, broadcast network traffic, such as that used in "Spanning Tree" (802.1D), OSPF, RIP, and HSRP protocols. By injecting false network re-configuration commands, the attacker can manipulate routers, switches, and intelligent hubs. This can lead to a severe disruption where the entire network may collapse, necessitating a reboot or comprehensive reprogramming of all affected network devices.

Caffe Latte attack

The Caffe Latte attack represents a method for compromising WEP security, notable because the attacker does not need to be within the network's vicinity to execute it. This attack specifically targets the Windows wireless stack. The technique involves sending a flood of encrypted ARP requests to the client. The attacker exploits vulnerabilities in the shared key authentication and message modification flaws inherent in the 802.11 WEP protocol. By doing so, the attacker manipulates ARP responses to extract the WEP key, often in less than six minutes.

Securing Wireless Transmissions

The nature of wireless communications creates three basic threats: Interception, Alteration and Disruption.

Protecting the Confidentiality of Wireless Transmissions

There are two main strategies to mitigate the risk of eavesdropping on wireless transmissions. The first strategy involves techniques that make it harder for unauthorized parties to locate and intercept wireless signals. This might include measures such as decreasing signal strength to limit range or using directional antennas to focus the signal more precisely. The second strategy centers on the use of encryption to ensure that, even if a wireless signal is intercepted, the information it carries remains confidential. Encryption converts the data into a secure format that only authorized parties can decode, providing a strong layer of protection against eavesdropping.

Signal-Hiding Techniques

To prevent attackers from intercepting wireless transmissions, organizations can take various steps to make it more difficult for unauthorized users to locate their wireless access points. Here are some straightforward and economical approaches:

Turning off SSID broadcasting: This prevents access points from broadcasting the network name, making it less visible to outsiders.

Using obscure SSID names: This strategy involves naming SSIDs in a way that doesn't reveal their purpose or affiliation, thus confusing potential attackers.

Reducing signal strength: Adjusting the signal strength to the lowest necessary level helps confine the network's reach to only essential areas.

Positioning access points away from perimeters: Placing access points centrally within buildings, rather than near windows and exterior walls, minimizes the chance of the signal reaching outside the intended area.

For more comprehensive security, though at a higher cost, organizations might consider:

Utilizing directional antennas: These antennas direct the signal more precisely to required areas, limiting where the signal can be intercepted from outside those areas.

Applying advanced shielding techniques: Employing methods like TEMPEST to block the emanation of signals can further secure wireless networks against external threats.

Encryption

The best method for protecting the confidentiality of information transmitted over wireless networks is to encrypt all wireless traffic. This is especially important for organizations subject to regulations.

Preventing Alteration of Intercepted Communications

Interception and alteration of wireless transmissions represents a form of "man-intermeddle" attack. Two types of countermeasures can significantly reduce the risk of such attacks: strong encryption and strong authentication of both devices and users.

Countermeasures to Reduce the Risk of Denial-of-Service Attacks

Effective strategies are essential to safeguard wireless communications from potential denial-of-service (DoS) threats, including unintentional disruptions. Here's how organizations can strengthen their wireless networks:

1. Conducting Comprehensive Site Surveys

Objective: To create a detailed map of the wireless signal environment, detecting areas with potential interference or weak signal spots.

Method: Utilize advanced tools to assess signal strengths, check for channel overlaps, and identify physical barriers that could affect signal propagation.

Benefits: Enables optimal placement of wireless access points, enhancing network efficiency and minimizing conflicts with other wireless signals, crucial in densely populated settings.

2. Regular Wireless Network Audits

Objective: To continuously evaluate the health and security of the wireless network.

Method: This includes scanning for rogue access points, verifying network performance against benchmarks, and spotting unauthorized devices that might cause disruptions.

Benefits: Helps maintain network performance at peak levels and quickly identifies sources of disruptions, allowing for immediate resolution.

Additional Preventive Measures

a. Implementing Strong Security Measures

Details: Adopt the latest encryption standards like WPA3, consistently update all network devices with the latest firmware and software patches to close security loopholes.

b. Frequency Management

Details: Monitor and adjust the frequencies used by the wireless network. Use tools to avoid channel overlaps with neighboring networks, which can significantly reduce interference and improve network reliability.

c. Physical Security Enhancements

Details: Protect access points from physical tampering or unauthorized adjustments, which can also lead to network disruptions.

By embracing these methods, organizations can significantly mitigate the risk of both intentional and unintentional DoS attacks, ensuring their wireless networks remain robust and reliable.

Securing Wireless Access Points

Insecure, poorly configured wireless access points can compromise confidentiality by allowing unauthorized access to the network.

Countermeasures to Secure Wireless Access Points

Here's an original explanation of the steps organizations can take to reduce the risk of unauthorized access to their wireless networks:

4.1.1 Eliminating Rogue Access Points

1. Detect and Remove Unauthorized APs: Utilize tools such as wireless intrusion detection and prevention systems (WIDS/WIPS) to monitor for and quickly remove any unauthorized access points. These unauthorized devices can be covertly installed and used to bypass network security.
2. Conduct Regular Network Reviews: Regularly review and audit the wireless network to ensure all access points are authorized and documented. This helps maintain control over the network infrastructure.
3. Implement Strict Policies: Develop and enforce strict policies regarding the installation and management of wireless access points. Train staff on these policies to ensure they understand the importance of securing the network and the risks associated with unauthorized access points.

4.1.2 Properly Configuring All Authorized Access Points

1. Secure Default Configurations: Immediately change default factory settings on new access points, including default passwords and usernames, to prevent easy access.
2. Enable Advanced Encryption: Activate advanced encryption standards like WPA3 to protect the data transmitted across the network. If WPA3 is unavailable, ensure the strongest available encryption is used.

4.1.3 Using 802.1x for Device Authentication

1. Implement 802.1x Authentication: Deploy 802.1x, an IEEE Standard for network access control. It provides an authentication framework that allows only authenticated devices to connect to the network, reducing the risk of unauthorized access.
2. Configure for All Devices: Apply 802.1x configuration to every device that connects to the network to ensure consistent security across all access points and reduce potential vulnerabilities.
3. Continuous Monitoring and Updating: Regularly update and monitor the 802.1x setup to keep up with new security challenges and to ensure that the authentication measures are functioning correctly.

Securing Wireless Client Devices

For Loss or Theft:

- Encrypt data to secure information even if the device is lost.
- Enable remote wipe to clear data from lost or stolen devices.
- Use physical locks and secure storage when devices are unattended.
- Deploy tracking software to locate and potentially recover devices.

For Compromise:

- Regularly update systems to patch vulnerabilities.
- Use secure Wi-Fi connections and avoid public Wi-Fi without VPNs.
- Install firewalls and antivirus software to block and detect threats.
- Implement multi-factor authentication to strengthen access controls.
- These measures enhance device security and protect sensitive information against common threats.

Securing Wireless Networks

Use of Encryption

- Choose an Encrypted Router: Opt for a router that supports WPA3 encryption.
- Enable Encryption: Access your router's settings to activate WPA3 or WPA2 encryption.
- Set a Strong Password: Use a complex mix of characters, avoiding simple words or patterns.
- Regularly Update Firmware: Keep your router's firmware up-to-date to patch vulnerabilities.
- Disable WPS: Turn off Wi-Fi Protected Setup to increase security.
- Use Wired Connections for Setup: Manage settings via a wired connection for added security.

Use anti-virus and anti-spyware software, and a firewall

To protect computers on a wireless network:
Install Security Software: Equip all devices with reliable antivirus and anti-spyware programs.
Update Regularly: Keep security software up-to-date to defend against new threats.
Enable Firewall: Turn on the firewall to block unauthorized access and configure it according to your security needs.

Turn off identifier broadcasting

Disabling SSID broadcast on your wireless router can enhance security by making the network name less visible to unauthorized users and hackers. This makes it harder for them to detect and target your network.

Change the identifier on your router from the default

Changing the default identifier (SSID) and setting a strong password are essential steps in securing your wireless network. Here’s a concise guide:

- Change the Default SSID: Avoid using the manufacturer's default SSID. Create a unique SSID that isn't easily associated with you or your location.
- Set a Strong Password: Use a password that’s at least 10 characters long, combining upper and lower case letters, numbers, and symbols to enhance security.
- Configure Devices: Ensure all your devices connect to the newly named network with the updated password.

Change your router’s pre-set password for administration

Absolutely, always change your wireless router's default password to a unique, strong password. Aim for at least 12-16 characters, mixing upper and lower case letters, numbers, and special characters to enhance security and make it difficult for hackers to gain access.

Allow only specific computers to access your wireless network

MAC address filtering is a feature on many wireless routers that allows you to specify which devices are allowed to connect to your network based on their unique MAC addresses. However, since MAC addresses can be spoofed (imitated) by hackers, relying solely on MAC filtering isn't foolproof for network security. It's best to use it as just one part of a multi-layered defence strategy, including strong passwords, updated firmware, and encryption.

Turn off your wireless network when you know you won’t use it

Turning off your wireless router when it's not in use is a simple yet effective security measure. This practice minimizes the window of opportunity for hackers to target your network since the router is inaccessible and not transmitting data when powered down. It’s particularly useful during extended periods of non-use, such as overnight or when away from home. This not only enhances security but can also save energy.

Don’t assume that public “hot spots” are secure

It's common for many public places like cafés, hotels, airports, and other establishments to offer free wireless networks for the convenience of their customers. While these networks provide easy internet access and are useful for staying connected on the go, they can also pose security risks. Since public Wi-Fi is often less secure, it's important for users to be cautious about the information they access and share on these networks. Using VPNs, avoiding sensitive transactions, and keeping your devices updated are a few ways to enhance security when connecting to public Wi-Fi.

Training and Educating Users

Indeed, user education is crucial for wireless network security. Regular training helps users understand security risks, recognize threats, and follow best practices like using strong passwords and VPNs. Effective training, updated periodically, empowers users to act responsibly and maintain secure network environments.

Network Auditing

Wireless network auditing is essential for WLAN security, involving regular scans and mapping of the network to detect unauthorized devices. Tools like NetStumbler can identify all access points and nodes, and this data is then compared with previous audits to spot new and potentially rogue hardware. Additionally, specialized tools like Airsnort are used to audit for vulnerabilities such as weak WEP keys, helping ensure the network's defences are robust against potential hacking attempts.

Conclusion

Wireless networking indeed enhances productivity and can lead to cost reductions; however, it also introduces specific security risks. While it's not feasible to eliminate all risks entirely, organizations can manage these risks effectively through a systematic approach:

Risk Assessment: Regularly assess the risks associated with the three fundamental components of wireless networks: clients, access points, and the transmission medium.

Countermeasures: Implement commonly available security measures to mitigate identified risks. This includes secure configurations, encryption, and the use of advanced technologies for monitoring and defense.

User Education: Emphasize the importance of training users in secure wireless networking practices. Educated users can significantly reduce security risks by following established protocols and recognizing potential threats.

By combining these strategies, organizations can achieve a reasonable level of security that protects both data and network infrastructure from potential breaches in a wireless environment.

REFERENCES

1. Graham, E., Steinbart, P.J. (2006) Wireless Security
2. Cisco. (2004). Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, July 19.
3. CSI. (2004). CSI/FBI Computer Crime and Security Survey.
4. Hopper, D. I.(2002). Secret Service agents probe wireless networks in Washington.
5. Kelley, D. (2003). The X factor: 802.1x may be just what you need to stop intruders from accessing your network. Information Security, 6(8), 60-69.
6. Kennedy, S. (2004). Best practices for wireless network security. Information Systems Control Journal (3).
7. McDougall, P. (2004, March 25). Laptop theft puts GMAC customers data at risk. Information Week Security Pipeline.
8. Nokia. (2003). Man-in-the-middle attacks in tunnelled authentication protocols.
9. Paladugu, V., Cherukuru, N., & Pandula, S. (2001). Comparison of security protocols for wireless communications.
10. Slashdot. (2002, August 18). Wardriving from 1500ft Up.
11. Stoneburner, G., Goguen, A., & Feringa, A. (2002, July). Risk management guide for information technology systems. NIST Special Publication 800-30.
12. Wailgum, T. (2004, September 15). Living in wireless denial. CIO Magazine.