Discussion-4 security concerns and solution Wi-Fi

Discussion Topic:

Wireless is expanding rapidly, but the challenges of securing it remain. What would be your main security concerns, and how would you address them? Discuss strategies and tools that you would utilize to secure your WiFi network.

My Post:

Hello Class,

In recent decades, wireless technology has infiltrated every aspect of daily life, becoming an integral part of how most of us communicate, access information, work, and interact with the world. Wireless technology refers to any technology that enables communication or data transfer without the use of wires or cables (Hasons, 2024). This post explores the widely used wireless technology Wi-Fi, how it relates to other wireless technologies, the challenges and security concerns associated with it, and how to address them.

Type of Wireless Technologies and How They Relate to Wi-Fi

Wireless technologies enable telecommunication, that is the transfer of information between two or more devices without the use of physical media such as wires and optical fiber. The five main types of wireless technology commonly used to transfer data today are cellular networks for mobile communication, Bluetooth for short-range device connection, satellite communication for broad coverage, and Wi-Fi for local area networking. All these technologies use radio waves instead of other electromagnetic signals such as infrared light used by remote controls or visible light used for Li-Fi as radio waves allow for longer ranges and better penetration through obstacles such as walls.

Wi-Fi is the most used telecommunication technology within Wireless Local Area Networks (WLAN). It uses specific radio frequencies (2.4GHz, 5GHz, and 6GHz) and has protocols optimized for creating local area networks. In other words, it can provide internet access locally (within a limited range) making it ideal for homes, offices, and public spaces. Wi-Fi has evolved and continues to evolve by increasing data rates and bandwidth. The table below shows the different Wi-Fi standards and how they have evolved.

Table 1

Wi-Fi Standards

Generation	IEEE Standard	Release Date	Features
Wi-Fi 1	802.11b	1999	11 Mbps data rate, 2.4 GHz frequency
Wi-Fi 2	802.11a	1999	54 Mbps data rate, 5 GHz frequency
Wi-Fi 3	802.11g	2003	54 Mbps data rate, 2.4 GHz frequency

Wi-Fi 4	802.11n	2009	600 Mbps data rate, 2.4/5 GHz frequency
Wi-Fi 5	802.11ac	2013	6.9 Gbps data rate, 5 GHz frequency
Wi-Fi 6	802.11ax	2019	9.6 Gbps data rate, 2.4/5 GHz frequency
Wi-Fi 6E	802.11ax	2020	9.6 Gbps data rate, 2.4/5/6 GHz frequency

Note: data from "The Evolution of Wi-Fi Networks: From IEEE 802.11 to Wi-Fi 6E" By Links (2022).

On a side note, Li-Fi is a relatively new technology, it is "bidirectional wireless system that transmits data via LED or infrared light. It was first unveiled in 2011" (Iberdrola, n.d., p. 1). Li-Fi is cheaper, faster, and has a larger data volume capacity than Wi-Fi. However, it cannot communicate through walls or other opaque materials as Wi-Fi does, because it relies on visible or infrared light instead of radio waves.

Wi-Fi Security Concerns

Wireless networks have many advantages such as eliminating the need for physical cables (low installation cost), allowing greater flexibility in device placement, and providing mobility to users. However, unlike wired networks, where access is physically restricted by cables, in wireless networks electromagnetic signals such as radio waves can be intercepted by anyone within range using a compatible wireless device. Networks using Wi-Fi technology are practically vulnerable to unauthorized access (rogue access points), data interception (eavesdropping), Denial of Service (DoS) attacks, and malware. The table below illustrates the most common Wi-Fi risks and solutions

Table 2

Wi-Fi Security Risk and Solutions

Security Risk	Description	Solutions
Unauthorized Access - Rogue Access Points	Attackers gaining access to a network without permission, often through rogue access points or by exploiting weak passwords or security settings. A rogue access point is an unauthorized Wi-Fi access points installed on a network, often mimicking legitimate APs (Evil Twins).	- Network monitoring for unauthorized devices - Wireless intrusion detection/prevention systems (WIDS/WIPS). - Regular network scans
Data Interception	Attackers capturing data transmitted over a network (eavesdropping or sniffing).	- Strong encryption (WPA3). - VPN usage, especially on public Wi-Fi. - Use of secure protocols (HTTPS, SSH).
Denial of Service (DoS)	Attackers flooding a network with traffic, making it unavailable to legitimate users.	- Network monitoring for unusual traffic patterns. - Intrusion detection and prevention systems (IDPS). - Rate limiting/traffic shaping.
Malware	Malicious software that can infect wireless devices and spread through the network.	- Antivirus and anti-malware software on all devices. - Regular software updates and patches.

		- User education on safe computing practices.
Man-in-the-Middle (MITM)	Attackers secretly intercept and possibly alter communications between two parties.	- Strong encryption (WPA3) - VPN usage - Regular security audits
Password Cracking	Techniques like brute-force, dictionary, and rainbow table attacks are used to crack network passwords.	- Strong password policies - Multi-factor authentication - Account lockout policies - WPA3 encryption
Jamming	Disrupting Wi-Fi signals by emitting radio waves on the same frequencies.	- Using different frequency bands (e.g., 5 GHz instead of 2.4 GHz) - RF shielding - WIDS/WIPS to detect jamming activity

Note: data from "Exploring Common Wi-Fi attacks: A deep dive into wireless network vulnerabilities" by ITU (2024) and "Introduction to Wireless Networks" by Grigorik (2016).

Wi-Fi Security Protocols

As shown in Table 2, Wi-Fi networks are vulnerable to attacks if not secured properly. The IEEE 802.11 Wi-Fi standard provides various types of authentication protocols. Thus, it is essential to understand the difference between them to choose the right one that meets the security needs of specific wireless networks. For example, the WPA3 protocol offers the strongest security but requires new and expensive hardware. WPA2 provides AES encryption, it is the most recommended access protocol for users as it provides compatibility between older and newer security devices. The table below provides a description of the different main authentication protocols associated with the Wi-Fi standard, as well as their strengths, and weaknesses.

Table 3

Wi-Fi Security Access Protocols

Protocol	Description	Strengths	Weaknesses
WEP (Wired Equivalent Privacy)	An older protocol that is no longer considered secure.	Easy to set up.	Uses a static key that can be easily cracked by modern tools.
WPA (Wi-Fi Protected Access)	An improvement over WEP, but still has vulnerabilities.	Uses a dynamic key that is harder to crack than WEP.	Susceptible to various attacks and may have compatibility issues with some devices.
WPA2 (Wi-Fi Protected Access 2)	The most common protocol, offering strong security with AES encryption.	Strong encryption and widely compatible with most modern devices.	Requires more processing power and may have compatibility issues with older devices.
WPA3 (Wi-Fi Protected Access 3)	The latest protocol with enhanced security features.	More resistant to attacks and offers better protection for weak passwords.	Requires modern hardware and is not yet as widely adopted as WPA2.

Note: data from various sources (Freda, 2022; Raphaely, n.d.; Basan, 2024; AscentOptics, 2024)

Not only is it important to understand the difference between the different Wi-Fi security protocols, it is also essential to keep informed about the latest security vulnerabilities and updates. For instance, at the beginning of 2024, a new Wi-Fi vulnerability was discovered by researchers (Migliano). The CVE-2023-52424 vulnerability affects all operating systems, it is categorized as a Service Set Identifier (SSID) Confusion attack, where Wi-Fi clients can be tricked to connect to an untrusted network. The table below describes what type of network and authentication are vulnerable to CVE-2023-52424.

Table 4

Types of Wi-Fi Networks Vulnerable to SSID Confusion Attacks

Wi-Fi Network Type	Authentication Type	Vulnerable
Home	WEP	✓
Home	WPA1	✗
Home	WPA2	✗
Home	WPA3	✓
Enterprise	802.11X / EAP	✓
Mesh	AMPE	✓
Other	FT	✗
Other	FILS	✓

Note: from "New WiFi vulnerability explained: Protecting against SSID confusion attacks" by Migliano (2024).

To defend against this new vulnerability the 802.11 Wi-Fi standard needs to be updated to incorporate the SSID as part of the 4-way handshake when connecting to protected networks, and the beacon protection needs to be improved to allow a client to store a reference beacon containing the network's SSID to verify its authenticity during the 4-way handshake (Lakshmanan, 2024).

In conclusion, since wireless technology, more specifically the Wi-Fi standard, has become an indispensable part of modern life, it is important to understand the associated security risks, their solutions, and the authentication protocols used to secure Wi-Fi and other wireless networks. Ultimately, prioritizing security by proactively addressing wireless network vulnerabilities is essential for the safe use of this indispensable technology.

-Alex

References:

AscentOptics. (2024, January 9). *WEP, WPA, WPA2, WPA3: Classifying and comparing wireless protocols*. AscentOptics Blog. https://ascentoptics.com/blog/wep-wpa-wpa2-wpa3-classifying-and-comparing-wireless-protocols/

Basan, M. (2024, April 29). *Wireless Network Security: WEP, WPA, WPA2 & WPA3 Explained*. eSecurity Planet. https://www.esecurityplanet.com/trends/the-best-security-for-wireless-networks/

Freda, A. (2022, February 14). WEP, WPA, or WPA2 — *Which Wi-Fi security protocol is best? WEP, WPA, or WPA2*. AVG. https://www.avg.com/en/signal/wep-wpa-or-wpa2

Grigorik, I. (2016, April 27). *Performance of wireless networks: Introduction to wireless networks.* High Performance Browser Networking. https://hpbn.co/introduction-to-wireless-networks/

Hasons (2024, February 26). *Wireless Technology – What is Wireless Technology?* Hasons. https://hasonss.com/blogs/wireless-technology/

Iberdrola (n.d.). *What is LiFi technology? LiFi, the internet at the speed of light*. Iberdrola Group. https://www.iberdrola.com/innovation/lifi-technology

ITU (2024, February 7). *Exploring Common Wi-Fi attacks: A deep dive into wireless network vulnerabilities.* ITU Online IT Training. https://www.ituonline.com/blogs/common-wi-fi-attacks/

Lakshmanan, R. (2024, May 16). *New Wi-Fi vulnerability enables network eavesdropping via downgrade attacks*. The Hacker News. https://thehackernews.com/2024/05/new-wi-fi-vulnerability-enabling.html

Links, C. (2022, May 19). *The Evolution of Wi-Fi networks: from IEEE 802.11 to Wi-Fi 6E*. Wevolver. https://www.wevolver.com/article/the-evolution-of-wi-fi-networks-from-ieee-80211-to-wi-fi-6e

Migliano, S. (2024, May 14). *New WiFi vulnerability explained: Protecting against SSID confusion attacks*. https://www.top10vpn.com/research/wifi-vulnerability-ssid/?utm_source

Raphaely, E. (n.d.). *A complete guide to wireless (Wi-Fi) security*. SecureW2. https://www.securew2.com/blog/complete-guide-wi-fi-security