Project Title: Wi-Fi Security Assessment Report
Student's Name: Juan, Andrew
Course: UCOS 3-1
Date of Submission: 11/16/2024

Introduction

Overview of Wi-Fi Security and Wardriving

With the rapid growth of wireless technology, Wi-Fi has become an essential component of both personal and professional environments, providing convenient internet access without the need for physical cables. However, Wi-Fi networks are inherently vulnerable to unauthorized access and attacks, especially if they are not properly secured. **Wi-Fi security** focuses on implementing protective measures like encryption, firewall settings, and network access control to prevent intrusions and protect data.

One of the notable security threats to Wi-Fi networks is **wardriving**. Wardriving is the practice of driving around with a device capable of detecting Wi-Fi signals to identify and exploit unsecured networks. Attackers can gather information about the network's location, SSID, and security type, sometimes accessing sensitive data or using the network for malicious activities. This practice highlights the potential risks of weak Wi-Fi security settings, emphasizing the importance of configuring Wi-Fi networks with robust security protocols.

Importance of Securing Wi-Fi Networks

Securing a Wi-Fi network is essential for protecting personal data, ensuring privacy, and preventing unauthorized access to the internet connection. An unsecured network can expose users to risks like data theft, unauthorized surveillance, and the use of internet resources by others without permission, which can lead to issues like slower speeds and potential legal consequences.

A secure Wi-Fi network can protect against unauthorized access by implementing strong passwords, disabling insecure settings like WPS, and using advanced encryption like WPA3. Regular assessments of Wi-Fi security can help users identify vulnerabilities, ensure that firmware and settings are up to date, and ultimately create a safer, more reliable network environment.

This report will provide a thorough assessment of my Wi-Fi network's security, the steps I took to address initial vulnerabilities, and recommendations for maintaining ongoing security.

Description of My Wi-Fi Network

I set up my Wi-Fi network using a **FiberHome HG6145F1 router**, which connects to the internet via a **fiber optic** line. This connection is configured with **Point-to-Point Protocol over Ethernet (PPPoE)**, which provides a reliable, secure link to my ISP.

My router supports **dual-band Wi-Fi**, allowing me to set up two separate networks: a 2.4 GHz network, which I labeled "worst wifi," and a 5 GHz network, labeled "best wifi in the world." The 2.4

GHz network offers broader coverage but lower speeds, while the 5 GHz band provides faster speeds but within a more limited range.

Initial Security Vulnerabilities Discovered

When I first assessed my Wi-Fi network, I identified a few security vulnerabilities:

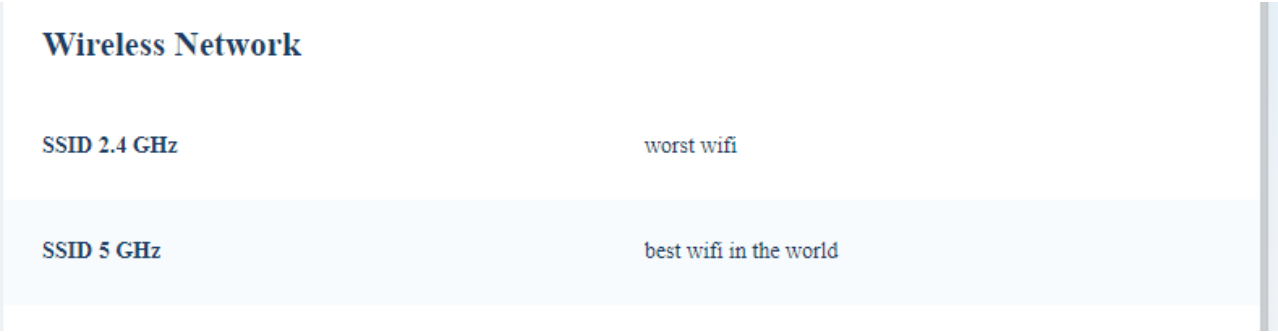
1. **Default SSID**: The SSID was initially generic and didn't provide any additional security. A recognizable SSID could allow attackers to identify my router's make and model, making it easier for them to exploit known vulnerabilities.
2. **Weaker WPA Encryption**: My network was initially secured with WPA encryption, which, although secure, is more vulnerable to attacks compared to the newer WPA3 standard.
3. **WPS Enabled**: WPS (Wi-Fi Protected Setup) was enabled by default, which can make it easier for unauthorized users to access the network by bypassing the Wi-Fi password with a brute-force attack.

Security Assessment

Detailed Findings of My Wi-Fi Network Security Settings

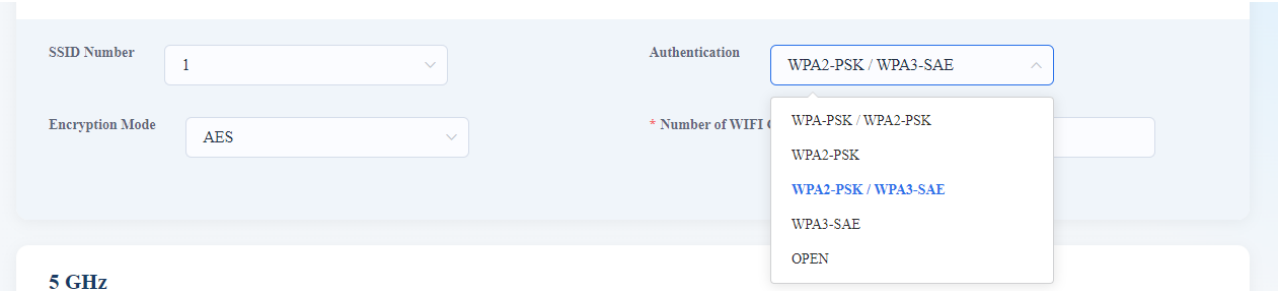
SSID Broadcast

Initially, my SSID was broadcasting with a name that didn't disguise my network well enough. I realized that while disabling SSID broadcast isn't a full security measure, customizing the SSID name helps prevent unwanted attention.



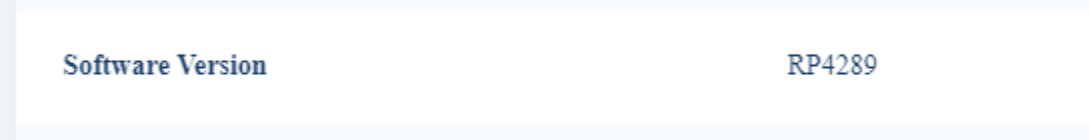
Wi-Fi Encryption

The router was initially set to **WPA encryption**, which has vulnerabilities that leave it open to several types of attacks. I upgraded to **WPA3** to benefit from its stronger encryption techniques.



Firmware Version

To make sure my router software was current, I reviewed the firmware version and confirmed it was up-to-date, which is essential for protecting against security vulnerabilities.



Explanation of Potential Vulnerabilities

I identified several potential vulnerabilities in my initial Wi-Fi setup:

- **SSID Name**: Using a default SSID can make it easier for attackers to determine my router model, which could reveal vulnerabilities. Changing the SSID helps reduce the risk.
- **WPS Vulnerability**: WPS was initially enabled, which made my network more susceptible to brute-force attacks. By disabling it, I closed this entry point.
- **Weak WPA Encryption**: WPA encryption, while more secure than WEP, is still vulnerable. By upgrading to WPA3, I improved the overall security and reduced the likelihood of unauthorized access.

Changes and Improvements

Description of the Changes I Made

1. **Changed the SSID Name**: I updated my SSID to a unique name to help protect my network from being easily identified by attackers.
2. **Updated Wi-Fi Password**: I created a new, complex password to ensure that only authorized users could connect to my network.
3. **Disabled WPS**: Since WPS is known for being a security risk, I disabled it to remove an easily exploitable entry point.
4. **Upgraded to WPA3 Encryption**: By switching from WPA to WPA3, I enhanced the level of encryption, making it harder for attackers to gain access.

Rationale and Impact of Each Change

- **SSID Name Change**:
  - *Rationale*: Changing the SSID helps mask the network from attackers who might otherwise identify the router model.
  - *Impact*: Reduced network visibility as a potential target.
- **Updated Wi-Fi Password**:
  - *Rationale*: Creating a strong password prevents unauthorized access.
  - *Impact*: Improved network security, limiting access to authorized users only.
- **Disabled WPS**:
  - *Rationale*: Disabling WPS mitigates the risk of brute-force attacks that could bypass the Wi-Fi password.

    - *Impact*: Strengthened security by closing a known vulnerability.
- **WPA3 Encryption**:
    - *Rationale*: WPA3 provides a higher security standard than WPA, with more advanced encryption.
    - *Impact*: Enhanced data protection and reduced likelihood of unauthorized access.

Conclusion and Recommendations

Summary of My Assessment Results and the Effectiveness of Improvements

In my initial assessment, I discovered several security vulnerabilities, including the default SSID, weaker WPA encryption, and enabled WPS. By changing the SSID, updating the Wi-Fi password, disabling WPS, and upgrading to WPA3 encryption, I significantly improved the security of my network.

Recommendations for Ongoing Wi-Fi Security

1. **Keep Firmware Updated**: I recommend checking for router firmware updates regularly to patch any new vulnerabilities.
2. **Monitor Connected Devices**: Regularly reviewing connected devices can help identify unauthorized users.
3. **Periodically Change Wi-Fi Password**: Updating the Wi-Fi password from time to time helps maintain security.
4. **Enable Extra Security Features**: I would enable additional options, like a guest network or advanced firewall settings, if needed.
5. **Review Security Settings Regularly**: I plan to periodically review my security settings to ensure they're up to date with the latest standard.