

# Walkthrough

## Exploring Wi-Fi Security – WPA2 vs WPA3

**Group Members:** Arunima Negi (30281210), Huma Naiman (30303242), Karanveer Singh (30282286), Pradip Ghimire (30303867)

Hey there!

Have you ever wondered how your Wi-Fi protects your data or precisely what really happens when you type in a password to connect? And most importantly, how do hackers sometimes still manage to break in?

If you're curious about how wireless security works, this teaching aide is for you. Exploring Wi-Fi Security Protocols – WPA2 vs WPA3 takes you behind the scenes of how your devices communicate securely over the air, how they stay safe, and how things could still go wrong.

This teaching aide is designed to make it simple to learn about Wi-Fi security in visually descriptive and engaging ways. You don't need to be a cybersecurity expert to follow along, just a curious mind and willingness to explore how everyday technology keeps you safe.

### How to Access & Use the Material

Our project comes with three parts: Walkthrough, Teaching Aide with Annexure, and Demo Presentation. Start with the Walkthrough; it gives you a quick overview of what to expect and how everything connects. Then, move on to the Teaching Aide for a deeper dive into the concepts and visuals. The Annexure is your quick reference guide for all the key terms and cryptographic concepts mentioned throughout the TA. New terms and jargon are hyperlinked in the whole document to Annexure, which helps supplement the user's effort. Finally, the Demo Presentation walks you through our live lab demo, showing exactly how the WPA2 handshake was captured and analyzed. Together, these pieces make it easy to follow along, learn the theory, and see it all in action.

### Overview of Content

We begin with a clear overview of Wi-Fi security and why encryption is important in an interconnected world. From there, you'll explore the development of wireless security from WEP to WPA, then WPA2, and eventually WPA3, with each protocol building on the previous one, yet facing new challenges.

Here's how the content flows:

The background part explains technical specifications like IEEE 802.11, key terms like SSID, and each version of Wi-Fi has a distinctive design, function, and protection measures.

Then we move into the main sections:

You'll discover how WPA2's architecture and 4-Way Handshake process authenticate devices and encrypt data. We explain how attackers exploit weaknesses in the handshake and how WPA2 improved upon WPA while still leaving some weak points.

You'll also learn the difference between Pre-Shared Key (PSK) and Extensible Authentication Protocol (EAP), cryptographic algorithms and key exchange systems are used, and how they underline Wi-Fi security in the modern environment.

We then cover real world attacks on WPA2 which have affected users and industry on multiple surfaces proceeding to WPA3 and how it redefines protection levels and fixes WPA2's vulnerabilities. You'll learn what changed in its architecture, how the Simultaneous Authentication of Equals (SAE) handshake replaces

WPA2's method, and why this change closes major security gaps. We also cover algorithms that WPA3 employs, the improvements to key exchange, and how it achieves forward secrecy to protect past messages even if future keys are compromised.

To bridge theory and practice, we present a hands-on demo that shows how WPA2's 4-way handshake can be captured and cracked using Aircrack-ng. The demo was performed in a controlled, authorized lab environment, where every access point and device was owned by the presenter. To visualize the attack, our slides walk you through each command, capture file, and Wireshark analysis of the EAPOL packets that make up the handshake. You'll see how a password like hello123 can be cracked in seconds, revealing the practical weakness of WPA2-PSK. We then compare this with WPA3's SAE handshake, which blocks the same exploit. By seeing how these attacks function, you gain an understanding of why it's so important to upgrade to WPA3 to secure personal and organizational networks.

## **What Makes This Teaching Aide Stand Out?**

We don't only tell you about concepts, we illustrate them. Our PowerPoint presentations include a live attack simulation with screenshots, step-throughs, and in-depth explanations so that complex ideas become easier to grasp. You'll exactly see how those vulnerabilities occur in WPA2 and how WPA3's enhancements prevent those same breaches. If you're new to computer science or cybersecurity, our Annexure is your new best friend. It's written in plain language and explains every key term used in the documents. It also helps you understand the mathematical computations behind encryption, authentication, and key exchange, so you don't get lost in math equations.

## **Why This Matters**

Understanding what Wi-Fi protocol you have on your network, isn't just for IT professionals, but for everyone who goes on to the internet. This teaching aide illustrates how WPA3 was created, how it secures users in an age of emerging cyber threats, and how future protocols like WPA4 are being designed with forward secrecy and stronger encryption in mind.

By the end of this, you will have a good background on how Wi-Fi security has evolved and why it matters. You'll be ready to dive into the full teaching aide, explore our attack demos, and gain a deeper appreciation for the technology that keeps your connections safe.