



Protocols

Project Requirements



Tim Fielder



November 6, 2024

Introduction

A significant requirement for projects 4 and 5 for this class is accurate implementation of *secure* versions of the WPA2 or WPA3 handshake, and the Bluetooth or Zigbee pairing process.

While I could dig through dozens of web pages that *mostly* agree about how these things work and put together something that resembles an accurate step-by-step protocol, I think that it would be more beneficial for all of you to take that journey with me.

So instead, I will fill this slideshow with links to the resources I find that we can then use to build an understanding together, and so that you can have a say in what the expectations are for these projects.

WPA2

- NetworkLessons.com
- Cyberpunk.rs
- Netbeez.net
- Wifi-Professionals.com
- [WLAN Blog](#)
- [SE Post on MIC gen](#)
- [Python implementation of handshake](#)
- [Praneeth's Blog on auth/assoc](#)
- [Praneeth's Blog post on deauth](#)
- [WLAN Blog post on the handshake](#)
- [MRN Blog post on Beacon frames](#)
- [MRN Blog post on assoc frames](#)
- [MRN Blog post on auth frames](#)

WPA3

- [IEEE.org](https://www.ieee.org)
- [WPA3 Blog](#)
- [HU-Berlin.de](https://www.hu-berlin.de)
- [WLAN Blog](#)
- [Praneeth's Blog](#)



UTPB

Bluetooth

- [Bluetooth.com Part 1](#)
- [Bluetooth.com Part 2](#)
- [Bluetooth.com Part 3](#)
- [Bluetooth.com Part 4](#)
- [Bluetooth.com Part 5](#)
- [SO Post](#)
- [AllAboutCircuits.com](#)
- [BlackHat Paper](#)

Zigbee

- [GeeksForGeeks.org](https://www.geeksforgeeks.org/)
- [Digi.com](https://www.digi.com/)
- [Silabs.com](https://www.silabs.com/)
- [Github Post](#)
- [Zigbee 3.0 User Guide](#)



Questions

