Wi-Fi monitoring on a budget

KEITH WALSH

Reason for purchase of new hardware

Back in CorkSec 53 I realised the usb wifi stick I was using was not great

- Cheap Chinese clone?
- Incorrect drivers?
- User error?

The cost of ‘good’ usb wifi cards had doubled in price at the time

What product did I pick and why?

- There was a Christmas sale at hackerarsenal.com
  - Their product WiMonitor (now WiMonitor Basic) was affordable
  - Easily available documentation
  - Honest reviews on the web about the product
  - Its only a re-flashed router, but would be getting something that ‘just worked’ for once
- I was looking for an excuse to use AddressPal from An Post

Why pay for shipping for only one item?

- As I was paying a flat rate for delivery, I also ordered the WiNX module.
  - “multi-purpose Wi-Fi attack-defense platform”
  - Different Firmware for different scenarios:
    - Wi-Fi Scanner
    - Wi-Fi Sniffer
    - Honeypot / Captive Portal
- We will come back to this later on

WiMonitor setup

- Requires 5v power via a micro usb socket
  - Cables and US psu provided
- Ethernet cable to connect the device to the laptop
- The device will boot and issue an IP address to the laptop
- Connect to the management web page on the device to configure it

WiMonitor setup

- From there set the destination to forward the captured packets to
  - Packets are encapsulated as ARUBA_ERM UDP packets
- Choose what channels to scan and how long to listen on each channel
- Configuration complete… well on the device anyway
  - Choose to disable auto refresh on the page as it generated unnecessary traffic

Client side config

- Launch Wireshark and listen on the correct interface.
  - You will see plenty UDP packets arriving on what ever port you specified
- Configure Wireshark to expect ARUBA_ERM packets on the given port
- Configure Wireshark to decode these packets back into Wi-Fi packets

Demo

- Configure device to scan all channels
- Configure device to scan a single channel
- Capture the 4 way EAPOL handshake
- Decode some packets (as I know what the wifi key is)

This video covers similar material to what was in the demo:
https://www.youtube.com/watch?v=BtJyEveciP4

Shiny toy #2 – the WiNX Module

- ESP 8266 based
- Documentation and firmware easily available
- Support scripts for Linux, OSX, Windows

WiNX –Example 1

- The module appears as an open Wi-Fi network
- SSID can be set to anything up to 30 characters long
- Users are faced with a captive portal on connection
- Any details entered are logged and stored on the device, these can be then retrieved over the serial console

This video covers similar material to what was in the demo:
https://www.youtube.com/watch? v=T9RBC86MYfY

WiNX –Example 2

- The module is re-flashed and becomes a Wi-Fi scanner

This video covers similar material to what was in the demo:
https://www.youtube.com/watch?v=DaeyGFDQKD4

WiNX –Example 3

- The module is re-flashed and becomes a Wi-Fi sniffer

This video covers similar material to what was in the demo:
https://www.youtube.com/watch?v=DsVVLNRilzI

Cost

- WiNX $20
- WiMonitor $45
- US Shipping $6.50
- AddressPal €15.99
- Customs etc €0
- Total ~ €73 to the door

Can it be done cheaper?

- Stock TP Link TL-MR3020 router is €30+post on Amazon UK
  - But its up to you to find the firmware and tweak it
- ESP 8266 modules are around € 6 delivered from China
  - I have bought one and will attempt to re-flash it and see what happens