Building a De-authenticator:

Sarah's Café

Whoami

- Security Consultant @ NCC Group
- Security Queen
  - Shameless plug - We have a talk tomorrow <3
- Ladies of Cheltenham Hacking Society Administrator
- Bsc (Hons) Forensic Computing and Security graduate
- Bsides London 2019 Rookie Track winner!
- (Basically a workshop rookie)
  - This workshops inspiration from the London2600
- Lover of travelling

LLHS

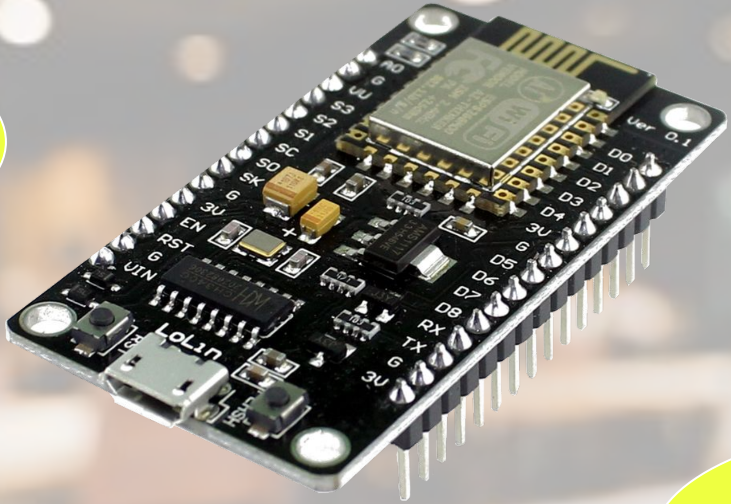
@G1nGe98

SECURITY QUEENS

What are we doing?

Building a de-authenticator by programming one of these bad bois.

Disconnecting devices connected to that router.



Impersonating a router.

Taking advantage of weaknesses in wireless communications.

DISCLAIMER

Jammer

vs

Deauther

DISCLAIMER

Wi-Fi Workings

1 Devices needing to connect to the internet will be connected to the router.

2 The wireless devices will talk to the router using radio waves to transmit data.

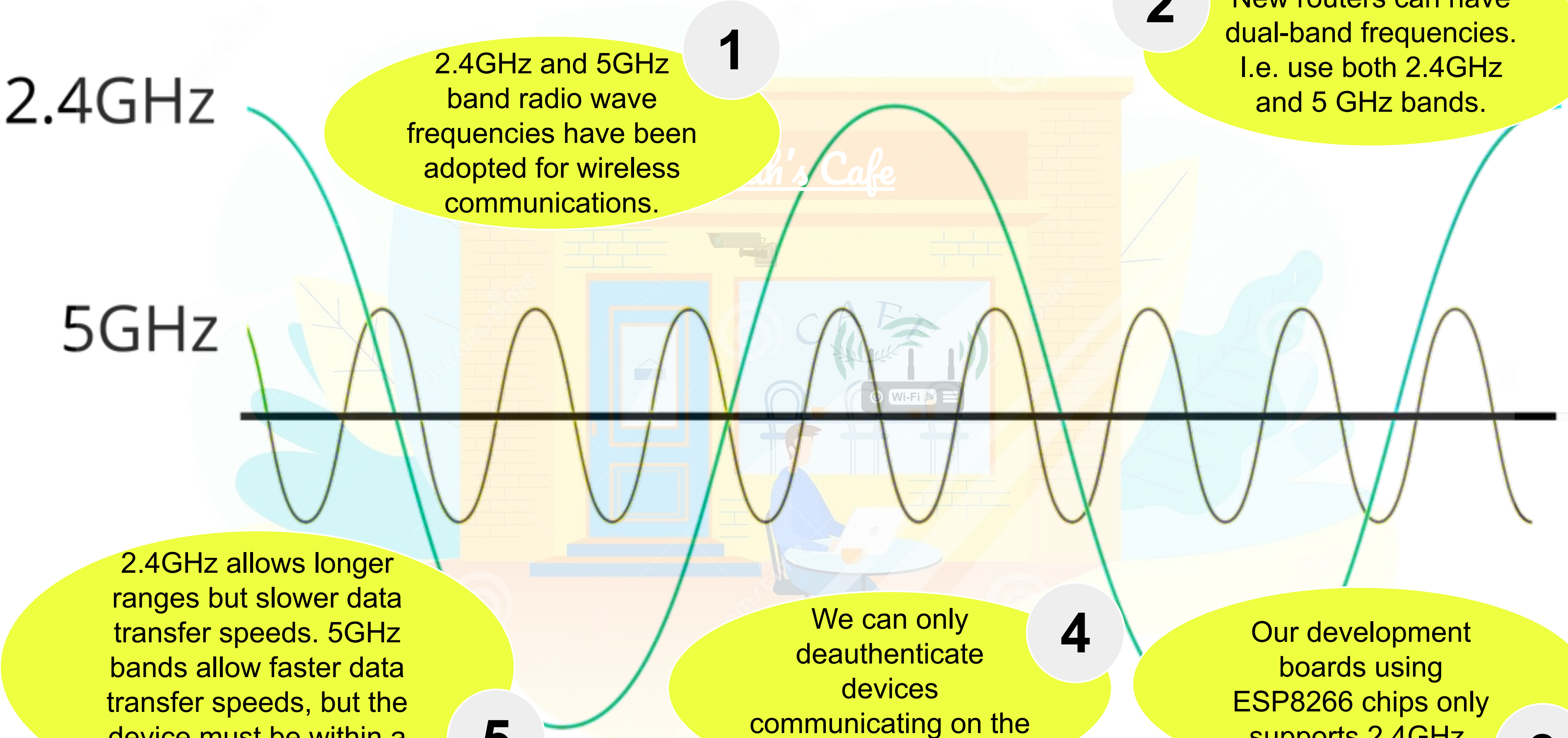
3 Radio wave frequencies are used to communicate. These frequencies contain channels.

4 A channel can only send communications of one device at a time, but multiple devices can communicate over one channel.

5 Interference can be experienced on overlapping Wi-Fi channels. E.g. when device communication overlaps another device.

6 Certain channels do not allow frequency overlap and can reduce interference.

What are wireless frequencies?



1 2.4GHz and 5GHz band radio wave frequencies have been adopted for wireless communications.

2 New routers can have dual-band frequencies. I.e. use both 2.4GHz and 5 GHz bands.

3 Our development boards using ESP8266 chips only supports 2.4GHz.

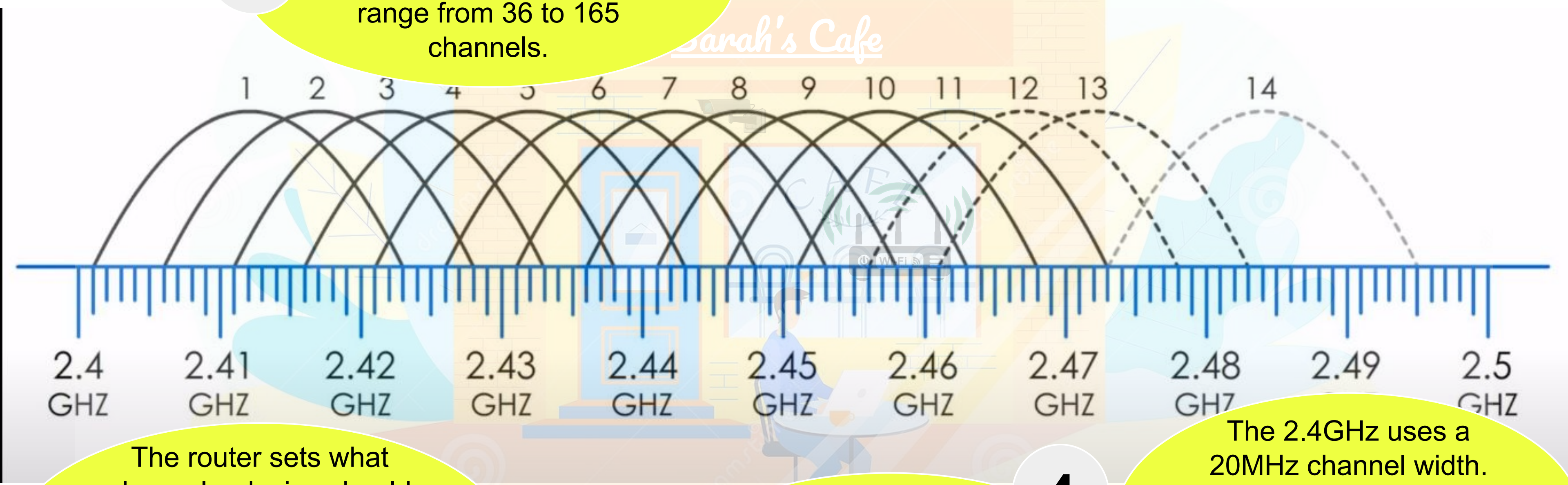
4 We can only deauthenticate devices communicating on the 2.4GHz band.

5 2.4GHz allows longer ranges but slower data transfer speeds. 5GHz bands allow faster data transfer speeds, but the device must be within a closer range.

What are wireless channels?

1 2.4GHz bands have 14 channels worldwide, whereas 5GHz bands range from 36 to 165 channels.

2 Channels 1, 6 and 11 do not have overlapping frequencies.



3 The 2.4GHz uses a 20MHz channel width. 5GHz bands use larger channel widths for faster data transfer rates.

4 Channel widths dictate how much data can pass through.

5 The router sets what channel a device should use. The more devices connected on a channel, the more data that needs to be transferred.

Wi-Fi standards

We know how things communicate, but we need to define **how** they communicate.

Method on how a connection can be made by the devices.

If standards are supported on one device and not another the cannot communicate… Unless the standards are compatible

Wi-Fi standards

Standard	Frequency	Max Data Rate**	Modulation	
802.11	2.4GHz	1-2Mb/s	DSSS,FHSS	Introduced in 1997.
802.11a	5GHz	54Mb/s	DSSS	1 S
802.11b	2.4GHz	11Mb/s	OFDM	1 th
802.11g	2.4GHz	54Mb/s	DSSS,OFDM	2 e conflict issues.
802.11n	2.4GHz, 5GHz	600Mb/s	OFDM	2 in a
802.11ac	5GHz	6.92Gb/s	OFDM	2014. Denser signal modulation = faster data transfer. 8 MU-MIMO streams to multiple devices at the same time.
802.11ax (2019)	2.4GHz, 5GHz	1201Mb/s	QAM?	2019. Splits one channel into sub channels to allow multiple users to communicate. Uses MU-MIMO - access point to address multiple devices at the same time.

OFDM - Orthogonal Frequency Division Multiplexing (how they create channels).

Better utilises the bandwidth by allowing signals to overlap.

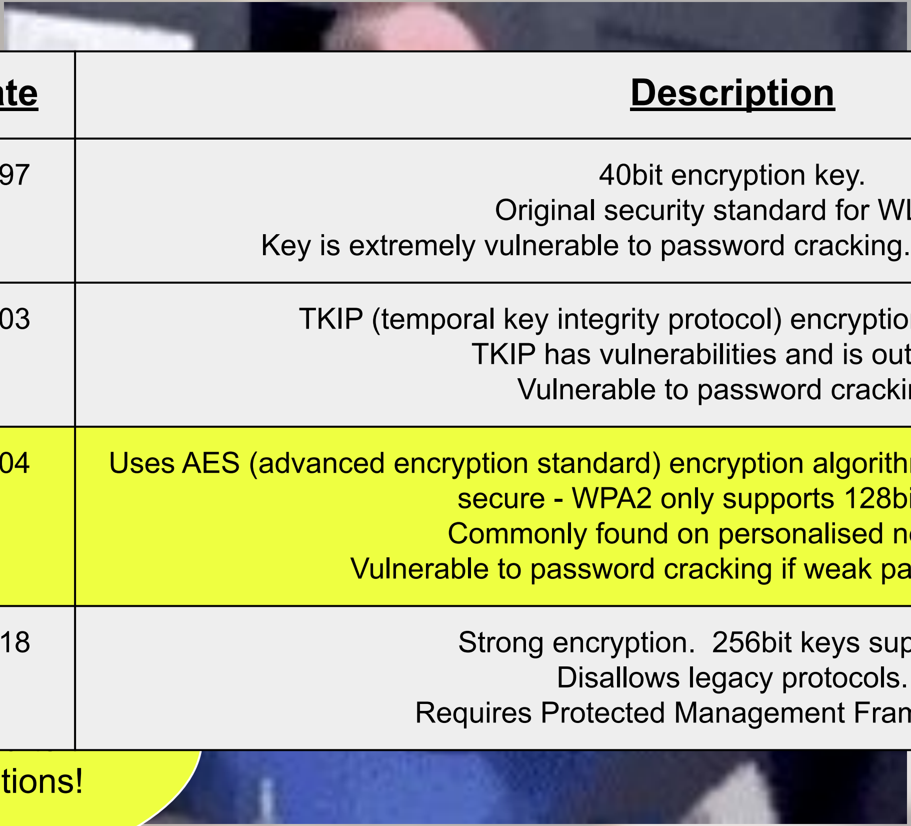
Different signals can communicate over the channel due to multiplexing.

DSSS - Direct Sequence Spread Spectrum (spreads signals over frequency band).

** Real world throughput varies greatly out in the wild. E.g. interference may slow speeds down.

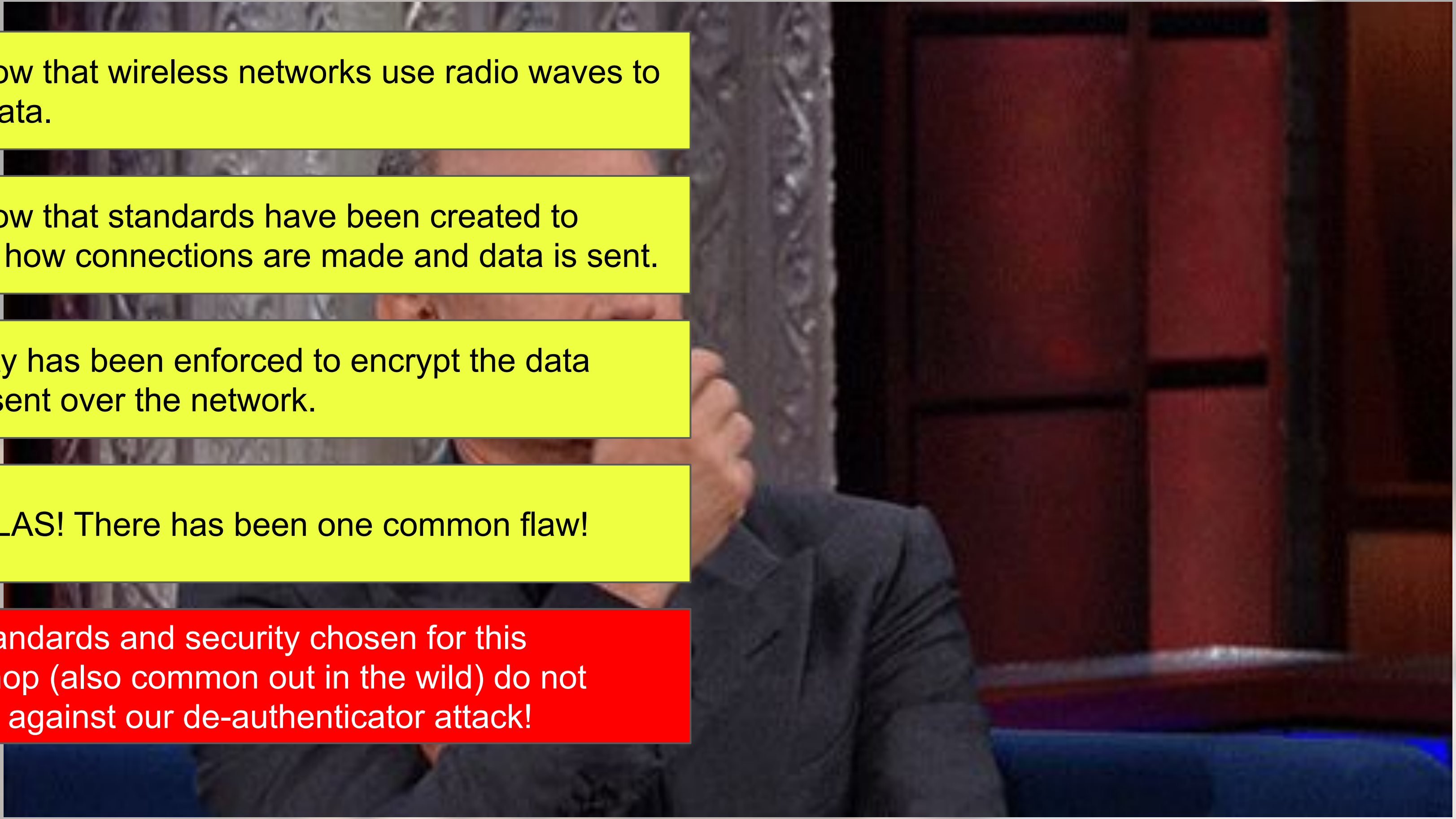
Wi-Fi security standards

Standard	Date	Description
WEP Wired Equivalent Provacy	1997	40bit encryption key. Original security standard for WLAN. Key is extremely vulnerable to password cracking. Uses RC4 encryption.
WPA WiFi Protected Access	2003	TKIP (temporal key integrity protocol) encryption method with RC4. TKIP has vulnerabilities and is outdated. Vulnerable to password cracking.
WPA2 WiFi Protected Access (v2)	2004	Uses AES (advanced encryption standard) encryption algorithm, industry standard. 256bits most secure - WPA2 only supports 128bit keys.. Commonly found on personalised networks. Vulnerable to password cracking if weak password is used.
WPA3	2018	Strong encryption. 256bit keys supported. Disallows legacy protocols. Requires Protected Management Frames (PMF).



secure our communications!

So let's recap...



We know that wireless networks use radio waves to send data.

We know that standards have been created to dictate how connections are made and data is sent.

Security has been enforced to encrypt the data being sent over the network.

BUT ALAS! There has been one common flaw!

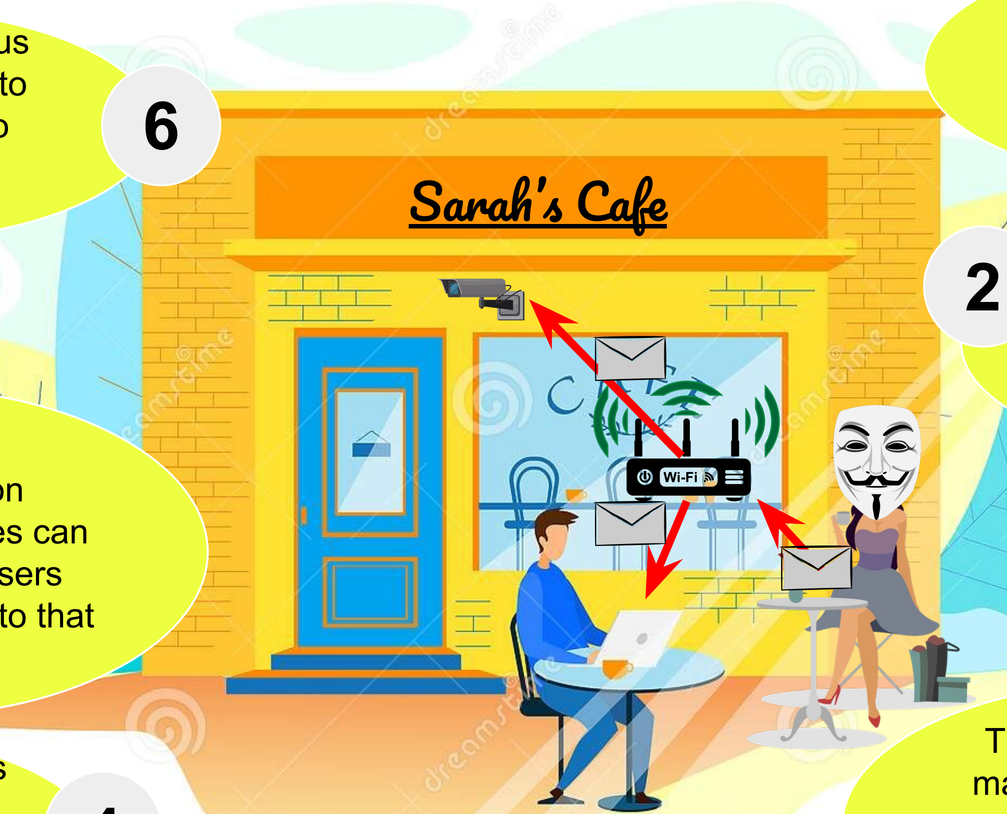
The standards and security chosen for this workshop (also common out in the wild) do not protect against our de-authenticator attack!

But WHY?!

Wi-Fi security standards, implementing encryption, do not add security to something called management frames. These are communicated unencrypted, as all clients must understand them.

Only data packets are encrypted with these security standards.

How does a deauther work?



1 A scope or specific AP needs to be identified.

2 The attacker will spoof the MAC of the AP identified for the scope.

3 The deauthentication management from to a single device or broadcast it to all devices connected to the AP.

4 A reason code needs to be specified to notify the client of why they are being deauthed.

5 Broadcasting deauthentication management frames can cause a DoS of users wanting to connect to that access point.

6 A spoofed/ malicious AP may be set-up to force the user into connecting to a different AP.

But what is a deauthentication frame?

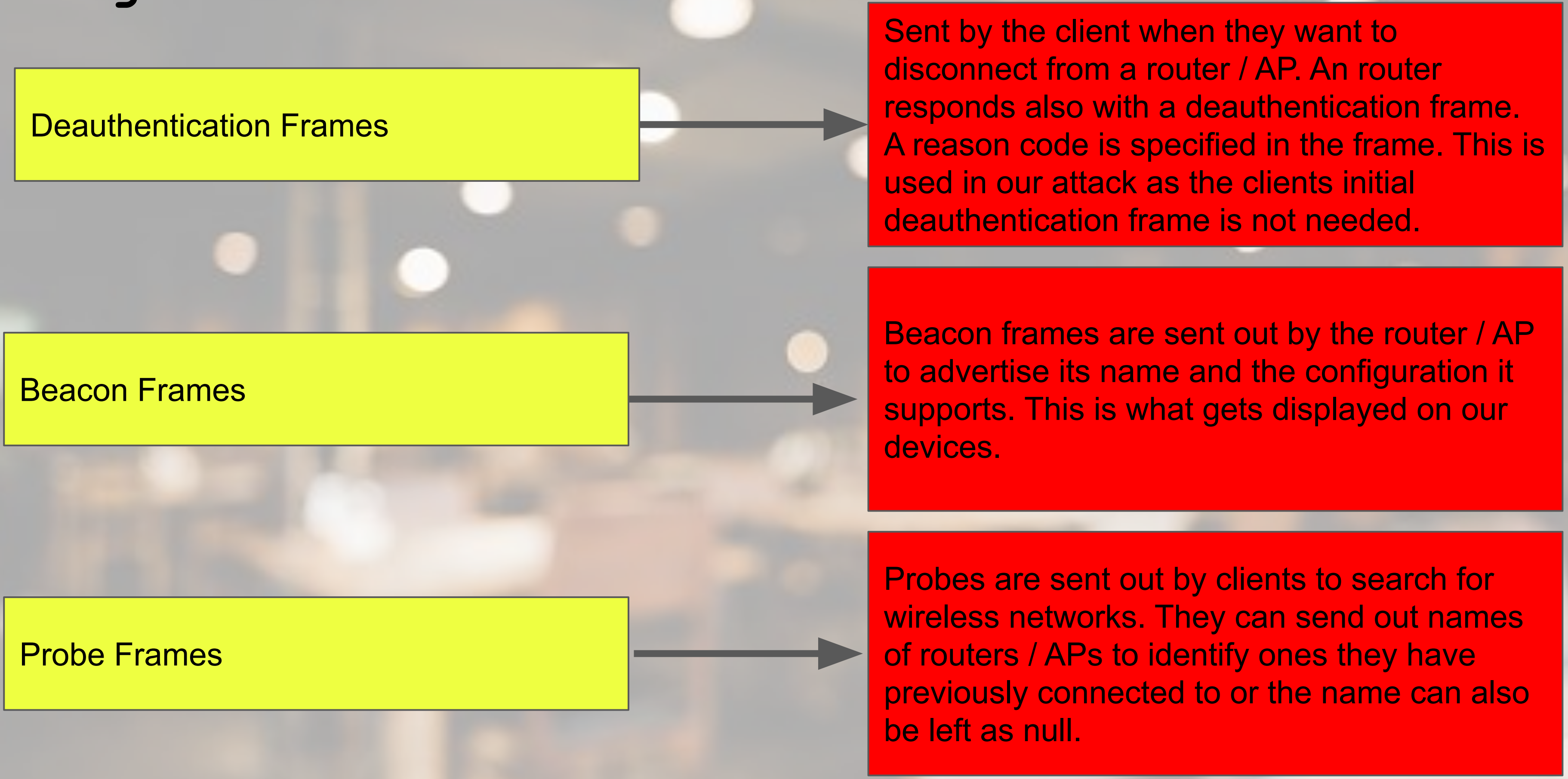
Wi-Fi Frames

Management -
Used to manage the base station. Such as becoming, probing, client association, client de-authenticating, etc.

Control -
Controls the access to the devices. E.g. an ACK frame is a control frame, confirming the receipt of data.

Data -
Data frames used to transfer data or trigger an event. Data frames can also be null.

Management Frames



Deauthentication Frames

Sent by the client when they want to disconnect from a router / AP. An router responds also with a deauthentication frame. A reason code is specified in the frame. This is used in our attack as the clients initial deauthentication frame is not needed.

Beacon Frames

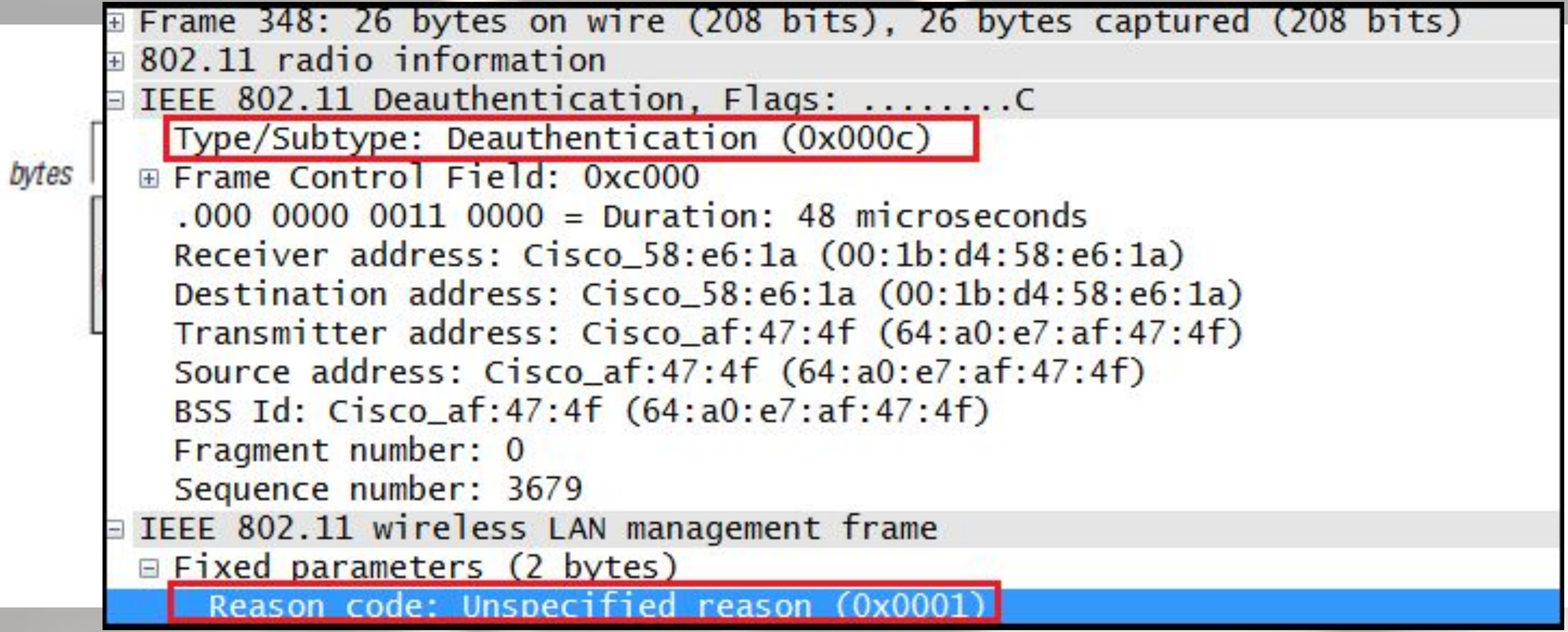
Beacon frames are sent out by the router / AP to advertise its name and the configuration it supports. This is what gets displayed on our devices.

Probe Frames

Probes are sent out by clients to search for wireless networks. They can send out names of routers / APs to identify ones they have previously connected to or the name can also be left as null.

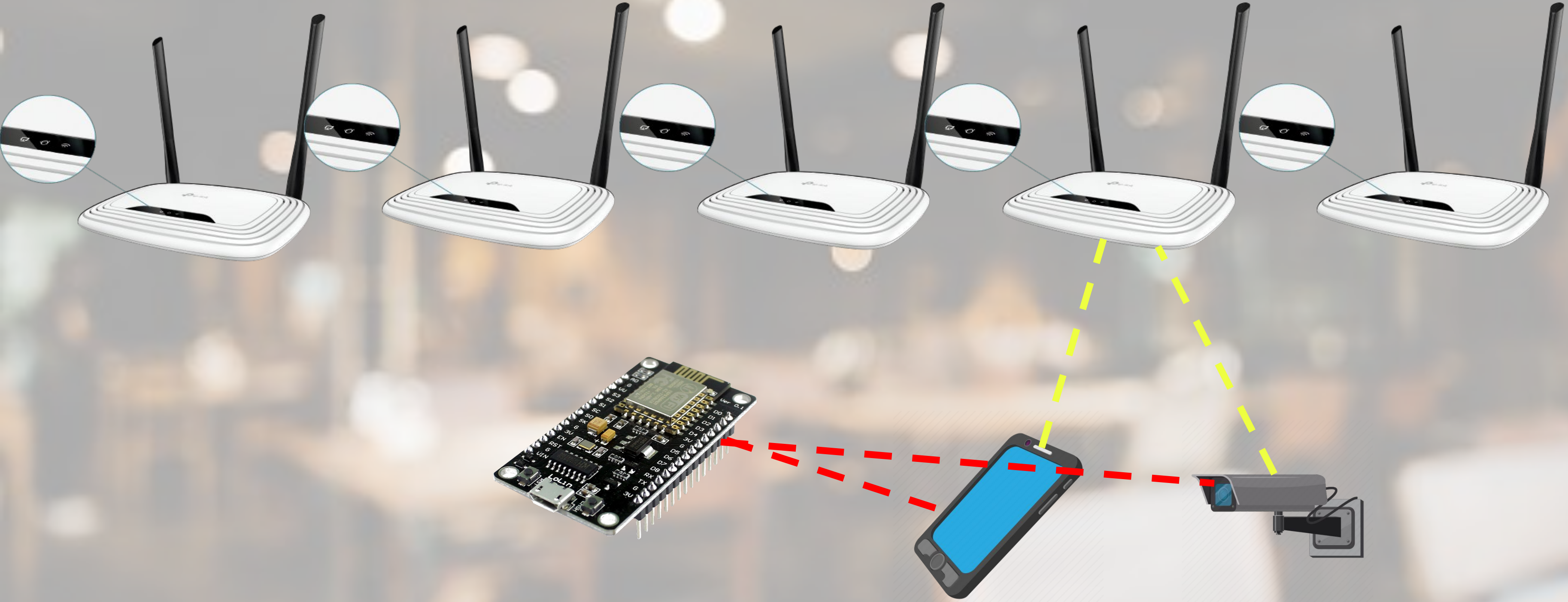
Deauthentication Frame

Deauthentication management frame is used to acknowledge the deauthentication of a device connected to a station or AP.

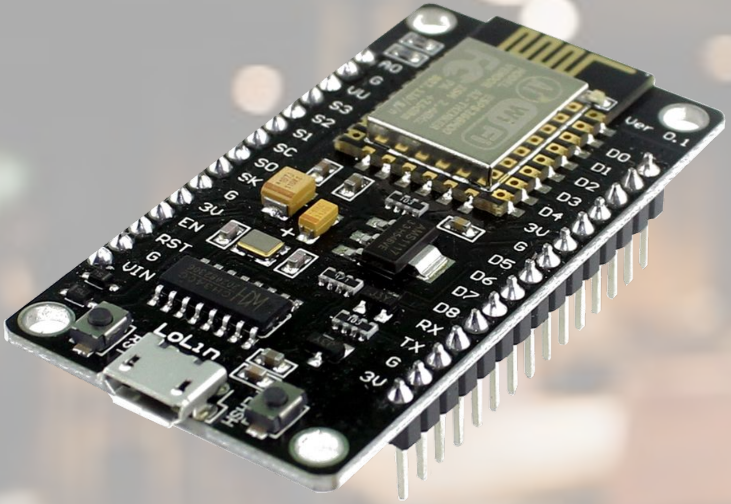


```
⊞ Frame 348: 26 bytes on wire (208 bits), 26 bytes captured (208 bits)
⊞ 802.11 radio information
⊟ IEEE 802.11 Deauthentication, Flags: ........C
    Type/Subtype: Deauthentication (0x000c)
  ⊞ Frame Control Field: 0xc000
    .000 0000 0011 0000 = Duration: 48 microseconds
    Receiver address: Cisco_58:e6:1a (00:1b:d4:58:e6:1a)
    Destination address: Cisco_58:e6:1a (00:1b:d4:58:e6:1a)
    Transmitter address: Cisco_af:47:4f (64:a0:e7:af:47:4f)
    Source address: Cisco_af:47:4f (64:a0:e7:af:47:4f)
    BSS Id: Cisco_af:47:4f (64:a0:e7:af:47:4f)
    Fragment number: 0
    Sequence number: 3679
⊟ IEEE 802.11 wireless LAN management frame
  ⊟ Fixed parameters (2 bytes)
      Reason code: Unspecified reason (0x0001)
```

Building a De-authenticator!



Ingredients to building a de-authenticator



Ingredients

ESP8266 chip development board

Data transfer cables

Arduino IDE

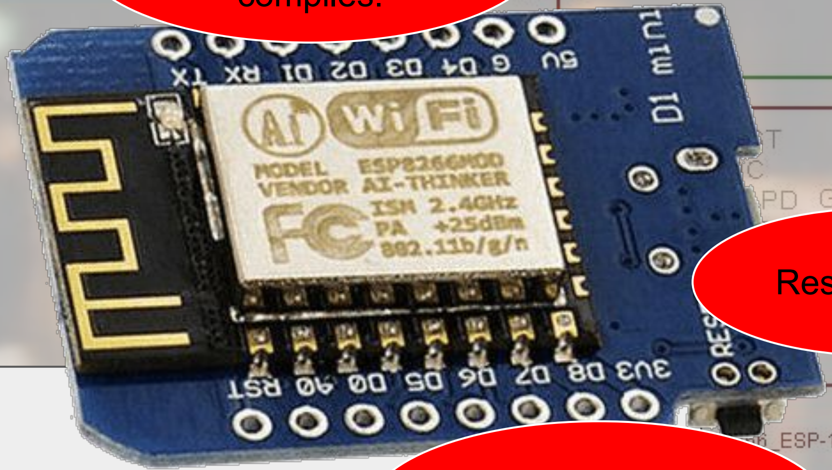
Router

Spacehuhns code

Development Board Types

Wemos D1 Mini Development Board with ESP8266 Chip

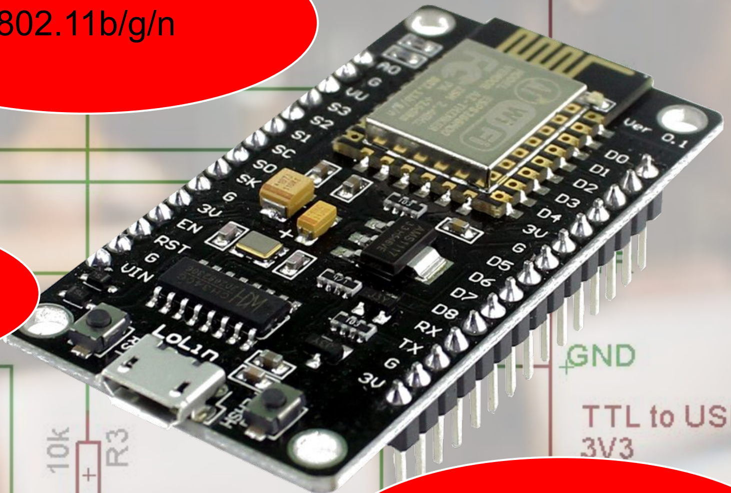
NodeMCU Development Board with ESP8266 Chip



Only difference is the way the code compiles.

Reset button!

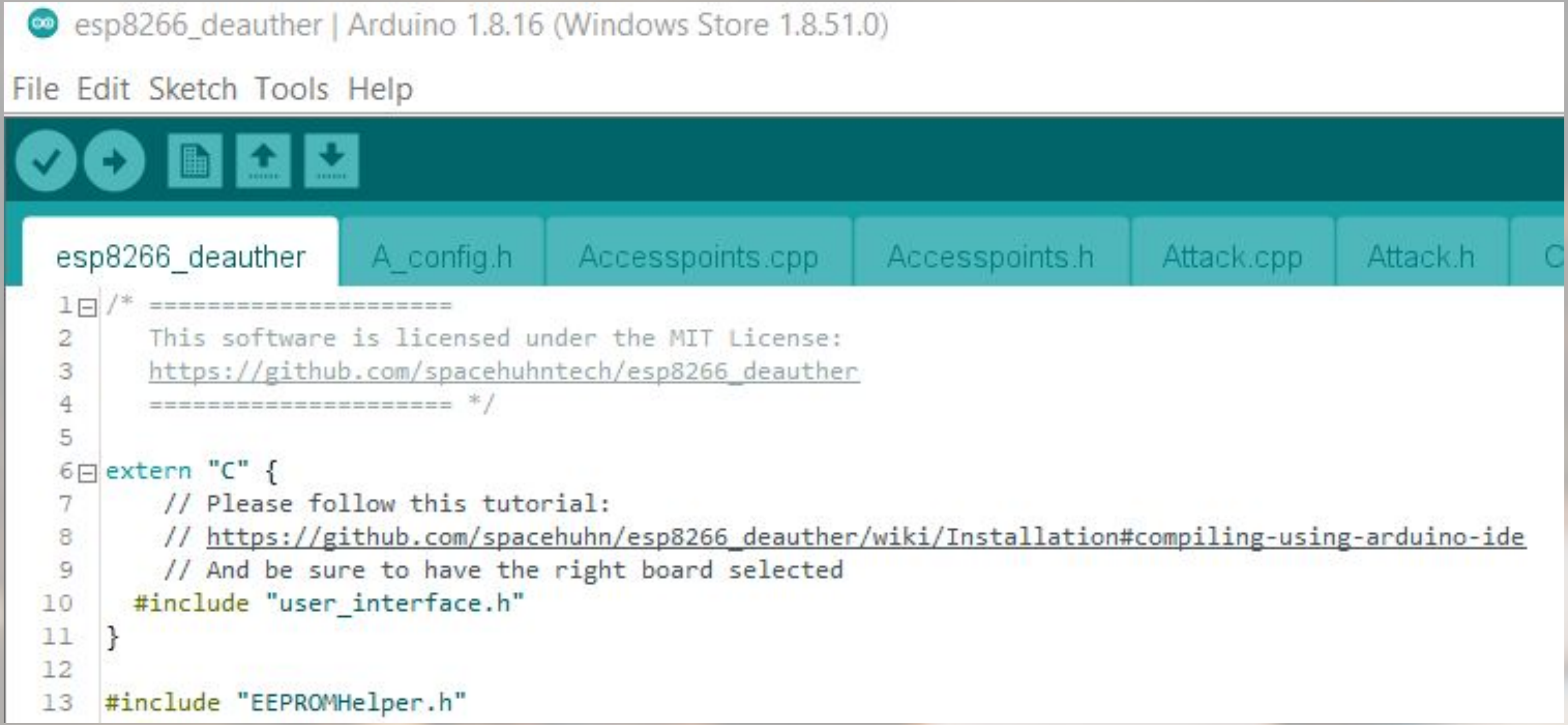
Micro-usb port for connectivity.


LoLin
Ver 0.1
D0 D1 D2 D3 D4 3V G D5 D6 D7 D8 RX TX G 3V
A0 G VU S3 S2 S1 SC SO SK G 3V EN RST G VIN

802.11b/g/n

2.4GHz frequency band.

Arduino IDE

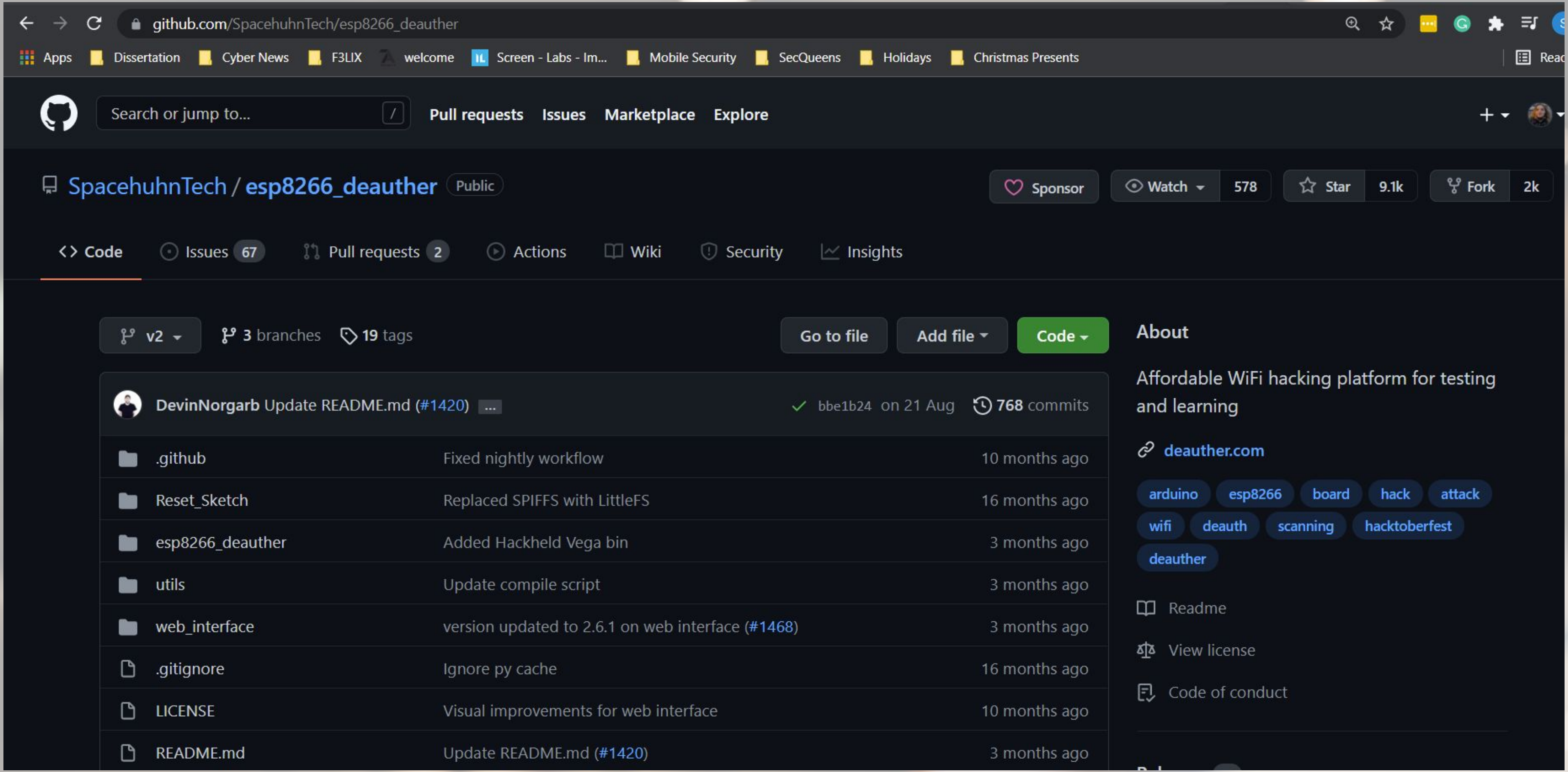

esp8266_deauther | Arduino 1.8.16 (Windows Store 1.8.51.0)
File Edit Sketch Tools Help
esp8266_deauther
A_config.h
Accesspoints.cpp
Accesspoints.h
Attack.cpp
Attack.h
C

```
/* =====================
   This software is licensed under the MIT License:
   https://github.com/spacehuhntech/esp8266_deauther
   ===================== */

extern "C" {
    // Please follow this tutorial:
    // https://github.com/spacehuhn/esp8266_deauther/wiki/Installation#compiling-using-arduino-ide
    // And be sure to have the right board selected
  #include "user_interface.h"
}

#include "EEPROMHelper.h"
```

Spacehuhn's Code



SpacehuhnTech / esp8266_deauther Public

DevinNorgarb Update README.md (#1420) ... ✓ bbe1b24 on 21 Aug 768 commits

.github	Fixed nightly workflow	10 months ago
Reset_Sketch	Replaced SPIFFS with LittleFS	16 months ago
esp8266_deauther	Added Hackheld Vega bin	3 months ago
utils	Update compile script	3 months ago
web_interface	version updated to 2.6.1 on web interface (#1468)	3 months ago
.gitignore	Ignore py cache	16 months ago
LICENSE	Visual improvements for web interface	10 months ago
README.md	Update README.md (#1420)	3 months ago

About

Affordable WiFi hacking platform for testing and learning

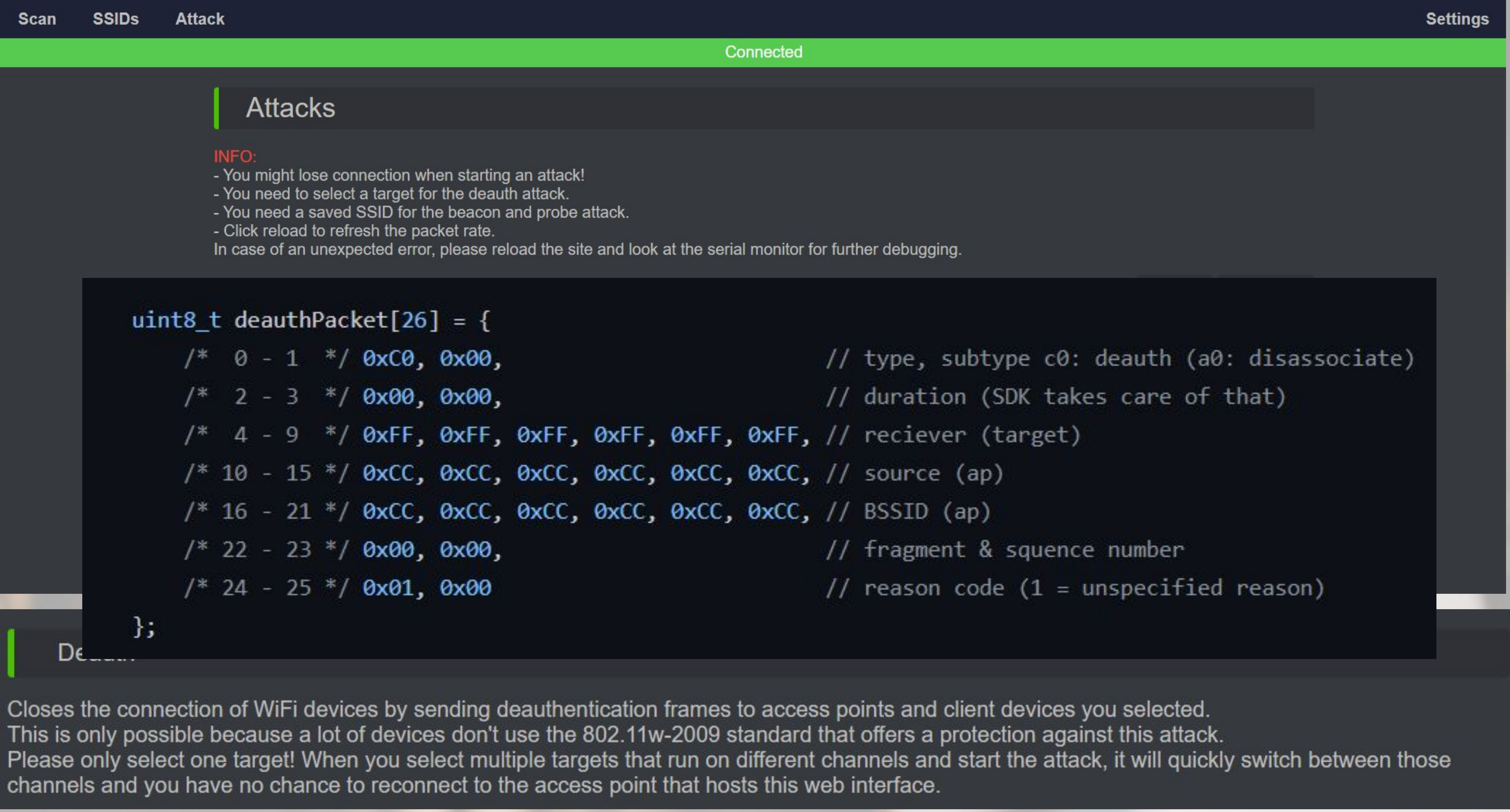
deauther.com

arduino esp8266 board hack attack wifi deauth scanning hacktoberfest deauther

Readme

View license

Code of conduct



Attacks

INFO:
- You might lose connection when starting an attack!
- You need to select a target for the deauth attack.
- You need a saved SSID for the beacon and probe attack.
- Click reload to refresh the packet rate.
In case of an unexpected error, please reload the site and look at the serial monitor for further debugging.

```
uint8_t deauthPacket[26] = {
    /*  0 - 1  */ 0xC0, 0x00,                         // type, subtype c0: deauth (a0: disassociate)
    /*  2 - 3  */ 0x00, 0x00,                         // duration (SDK takes care of that)
    /*  4 - 9  */ 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, 0xFF, // reciever (target)
    /* 10 - 15 */ 0xCC, 0xCC, 0xCC, 0xCC, 0xCC, 0xCC, // source (ap)
    /* 16 - 21 */ 0xCC, 0xCC, 0xCC, 0xCC, 0xCC, 0xCC, // BSSID (ap)
    /* 22 - 23 */ 0x00, 0x00,                         // fragment & squence number
    /* 24 - 25 */ 0x01, 0x00                          // reason code (1 = unspecified reason)
};
```

De

Closes the connection of WiFi devices by sending deauthentication frames to access points and client devices you selected.
This is only possible because a lot of devices don't use the 802.11w-2009 standard that offers a protection against this attack.
Please only select one target! When you select multiple targets that run on different channels and start the attack, it will quickly switch between those channels and you have no chance to reconnect to the access point that hosts this web interface.

Wireless Router:

TP-Link TL-WR841N 300 Mbps Wireless N Cable Router

2.4GHz only supported band.

Supports 11/b/g/n Wi-Fi standards.

Tplink settings default to automatically (auto) setting a channel to communicate over.

Aim and why

- Highlights the flaws in current wireless devices and standar
- 802.11w is not implemented in many Wi-Fi networks and m be supported in routers - such as the TPLink router.
- Allows us to build our own hacking tools cheaply.
- It’s good fun!

Routers are not as secure as you might think.

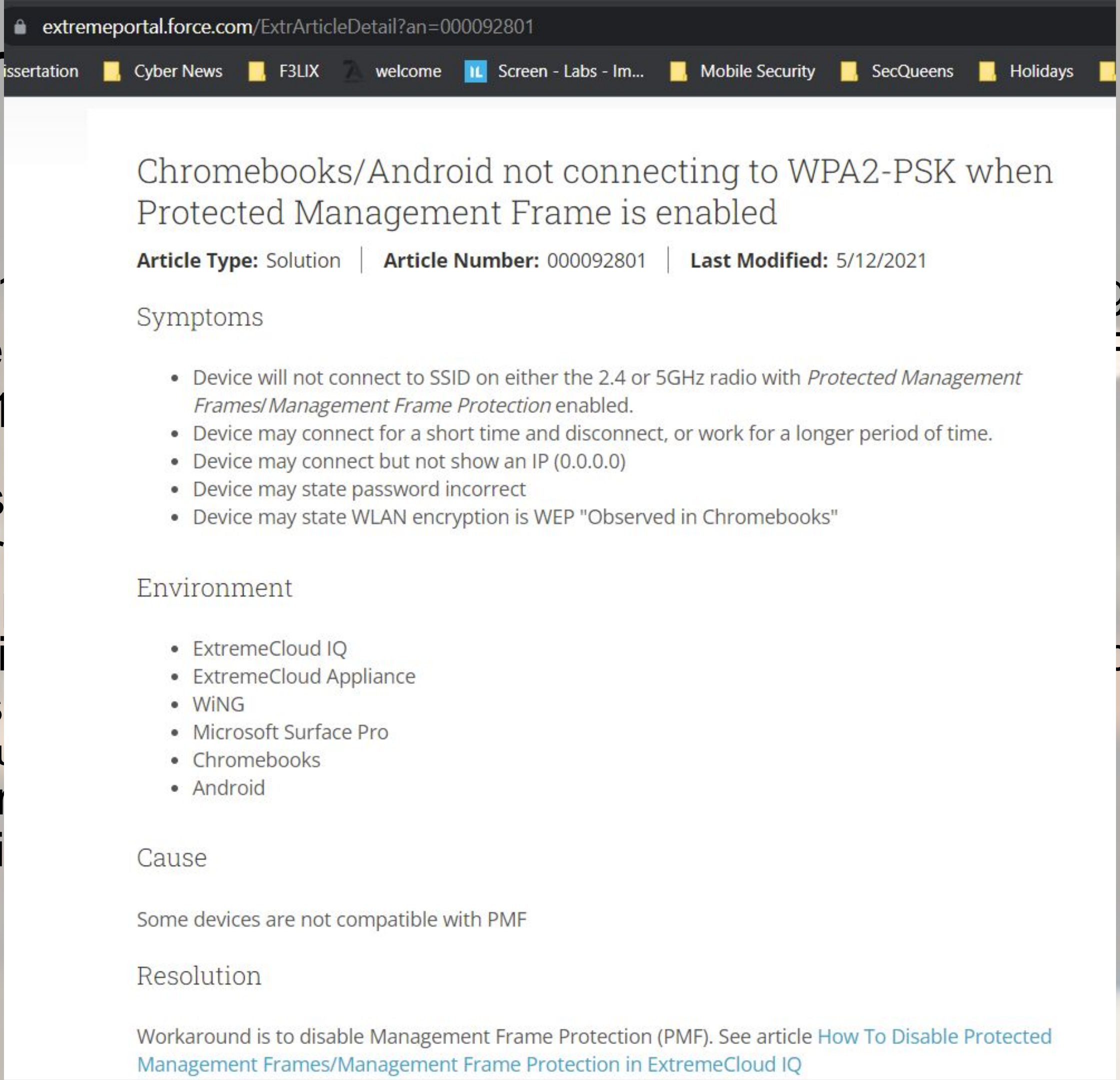
Management interfaces when left unconfigured are also vulnerable!

Not many support the latest standards.

Protectio

The IEEE 802.1 … grity checking in
the manageme … F) service was
based on 802.1

- 802.11w is
- PMF enfor … frames, which
means a s
- 802.11w ai … oofing, e.g.
prevent us
  - Makes u
- Helps to pr
- AP and Cli



Chromebooks/Android not connecting to WPA2-PSK when Protected Management Frame is enabled

Article Type: Solution | **Article Number:** 000092801 | **Last Modified:** 5/12/2021

Symptoms

- Device will not connect to SSID on either the 2.4 or 5GHz radio with *Protected Management Frames/ Management Frame Protection* enabled.
- Device may connect for a short time and disconnect, or work for a longer period of time.
- Device may connect but not show an IP (0.0.0.0)
- Device may state password incorrect
- Device may state WLAN encryption is WEP "Observed in Chromebooks"

Environment

- ExtremeCloud IQ
- ExtremeCloud Appliance
- WiNG
- Microsoft Surface Pro
- Chromebooks
- Android

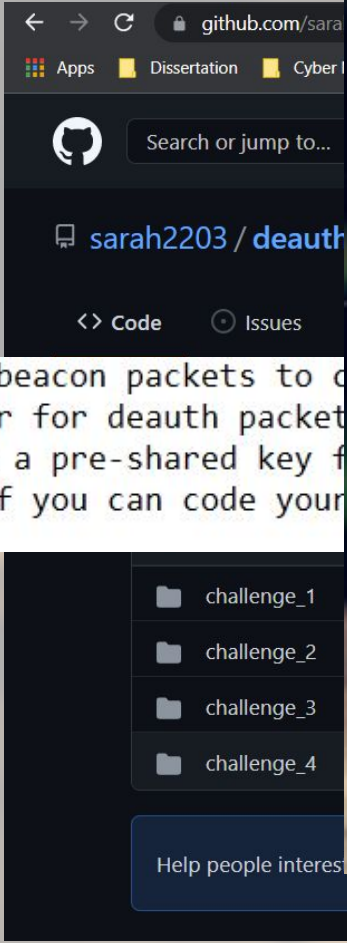
Cause

Some devices are not compatible with PMF

Resolution

Workaround is to disable Management Frame Protection (PMF). See article How To Disable Protected Management Frames/Management Frame Protection in ExtremeCloud IQ

Additional challenges and demo



challenge_1	1 hour ago
challenge_2	9 minutes ago
challenge_3	9 minutes ago
challenge_4	8 minutes ago

Help people interes

1. Spam beacon packets to c
2. Filter for deauth packet andshake in the PCAP file
3. Crack a pre-shared key f
4. See if you can code your

Work in yo
are going t

Remembe
clients atta

If you are c
you to try :

Before flas
change the
you. The fi

esp8266_deauther - A_config.h | Arduino 1.8.16 (Windows Sto

https://github.com/sarah2203/deauther_workshop