Wi-Fi Deauthenticator and Deauth Detector

TEAM 17:

- Kuljeet Singh Bhengura
- Kevin Dsouza
- Disha Sanil

PROBLEM STATEMENT

1) Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking has many security issues.

2) Security is one of important challenge which is to be handled in the era of wireless technology these days. Current security standards have shown that security is not keeping up with the growing use of wireless technology. There are many security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Every now and then a new vulnerability comes in existence to the existing wireless standards.

3) Our objective is to investigate and perform a special type **Denial of Service (DoS)** attack against a vulnerability in 802.11 wireless networks. This attack is known as the **Deauthentication Attack**. When any wireless access point wants to disconnect a client or terminate all the connections, it sends special frames known as *Deauthentication or Disassociation* frames. Due to being **unencrypted**, these frames do not require an authenticated user. Hence, we as attackers can craft these frames and send them to the access point in such a way that the access point assumes the frames to be coming from the client and not the attacker. This attack can be launched easily using minimal resources.

4) Along with the offence we also present an efficient defence solution on **Detecting** the Deauthentication attacks.Our proposed module is lightweight and detects the attack with high accuracy & low false positive rate. Our technique can be easily deployed on open as well as encrypted networks. The module works for both **Deauthorization Attacks** and **Disassociation Attacks.** Therefore, we carry out an o**ffence and defence** strategy.

SCOPE OF THE PROJECT GOAL

OFFENCE:

1.One place where deauthentication can be particularly useful is at a *School or University*. By blocking cell-phone Wi-Fi Hotspots, students can be prevented by being distracted on their phones. In addition, they cannot cheat by sending text messages to one another during exams.

2.High security premises, such as prisons and detention centers, can also benefits from our module because it can prevent illicit communication between inmates and visitors.

3.Military Services: Prevent terrorist attacks by means of remote-controlled bombs. Any bombs can be disconnected from the master device using this *Deauther.*

4.Help achieve quietness and silence in a conference room during a meeting.

SCOPE OF THE PROJECT GOAL

DEFENCE:

1) Since wireless local area network (WLAN) management frames are often unencrypted, an attacker can potentially attack the WLAN infrastructure by spoofing the Media Access Control (MAC) address of a client device that is associated with the WLAN, and sending a deauthentication and/or disassociation frame using the MAC address of the associated client device. Because the WLAN infrastructure cannot determine that the deauthentication and/or disassociation frame is from an attacker or a valid client device, it will terminate the client device's connection to the WLAN. As a result, a valid client device will experience denial of service by the WLAN infrastructure.

2) Create awareness about 802.11w. The “w” protocol uses CCMP from 802.11i to provide integrity, confidentiality and sender authenticity for unicast management frames, and Broadcast Integrity Protocol (BIP) to provide integrity for broadcast management frames. In both cases, protection is only provided for management frames of subtype action, deauthentication and disassociation. If protection of management frames is enabled and an unprotected management frame of subtype action, deauthentication or disassociation is received, the frame is silently discarded.

FEATURES OF THE DEAUTHER

1) Once your Wi-Fi Deauther board is powered, you shouldn't need a screen to interact with it. While it's convenient to have a display to see what's going on, we can rely on the web interface to control the ESP8266 device as well.To access it, connect to the Wi-Fi network and enter the password "deauther" to join. Then, in a browser window, you can navigate to the default IP address of 192.168.4.1

2) The first page you'll find yourself on is the "Scan" page, which breaks down results into a few easy to understand categories. First, there are access points. This will give you a list of every device advertising a Wi-fi network in range.Further down the list, you'll see devices that are connected to a network, as well as which network they are connected to.

3) Select Target Networks: In the "SSIDs" section, we'll be able to clone networks, create fake networks, or simply Rickroll everyone.The top field is for specifying any fake network we want to create. This includes the SSID, or network name, whether or not the network uses WPA security, and how many networks you want to create.

4) Launch an Attack: Now, let's check out the attacks we can launch in the "Attacks" section of the menu. Here, we can see three primary kinds of attacks.

Deauth: This will attack any network in range, disconnecting it from Wi-Fi until you disable it. This makes it likely that you may unintentionally prevent yourself from connecting to the device to turn it off. If you find yourself disconnected and you can't get back in, you may need to unplug the board to get it to stop.

Beacon: This attack will create up to a thousand fake networks, either cloning nearby networks or creating entirely fake ones from scratch.

Probe: Here, the board will send probe requests asking for a network name that's in the list you specify. This will confuse some Wi-Fi trackers and also sometimes cause Wi-Fi attack tools to create fake networks in response to the network names contained in the probe requests.

FEATURES OF THE DEAUTH DETECTOR

1) We can define whether or not we want to Channel Hop or just stay on one channel by setting the "channelHopping" setting to "true." Depending on where we are, we can define the highest channel to scan to while channel hopping (Japan is 14, while the US only goes to 11), and the number of packets detected per minute which we will decide an attack is underway.

2) Next, we have a series of variables which keep track of things in the script. We have added two variables to keep track of deauthentication and disassociation packets, creatively named "dissoc" and "deauth."

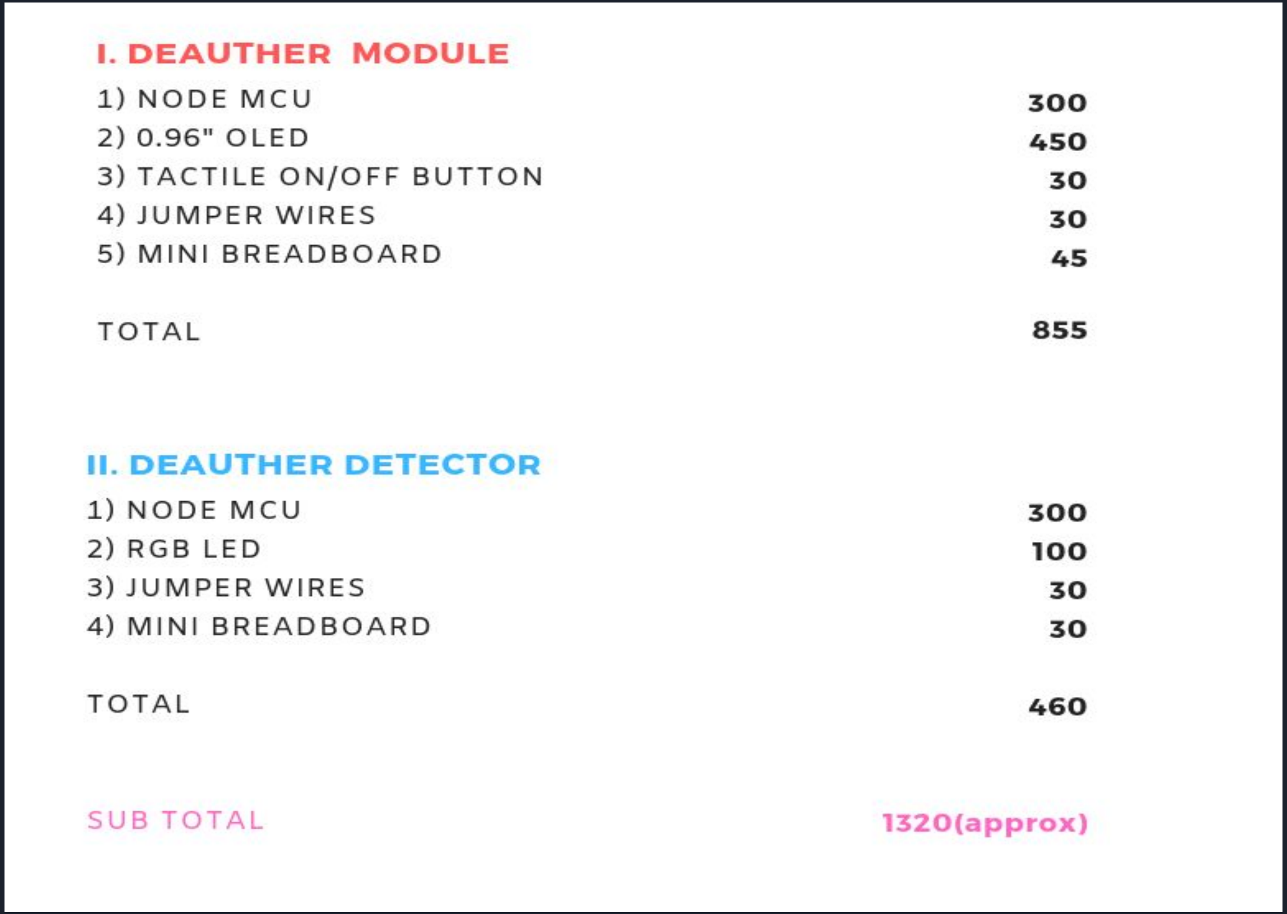
3) Next, we have a sniffer function, and an "if" statement that adds to the "c" counter, which is counting how many deauthentication or disassociation packets we have received. We ve commented this out because we will be tracking them individually.

4) Instead, we'll insert two "if" statements that will add to a cooldown timer. Whenever we detect disassociation packets, we'll turn on an LED by setting the cooldown timer to 500, and then subtract one from the timer one each time we scan a packet that isn't a dissociation packet. This means the light will stay on continuously when an attack is underway and turn off as soon as the attack stops and normal traffic resumes. The same logic is true for deauthentication packets, which we track in the second "if" statement.

```
if(buf[12] == 0xA0){dissoc = 500;}
if(buf[12] == 0xC0){deauth = 500;}
```

5) Now, our module decides what happens when the packet doesn't match, meaning it's a normal Wi-Fi packet and not one we're looking for. To handle this, we'll use an "else" clause that says that if the cooldown timer for "deauth" or "dissoc" is equal to or greater than one, subtract one from the timer. Otherwise, if the timer is already at zero, do nothing.

COST OF PROJECT



I. DEAUTHER MODULE

1) NODE MCU	300
2) 0.96" OLED	450
3) TACTILE ON/OFF BUTTON	30
4) JUMPER WIRES	30
5) MINI BREADBOARD	45
TOTAL	855

II. DEAUTHER DETECTOR

1) NODE MCU	300
2) RGB LED	100
3) JUMPER WIRES	30
4) MINI BREADBOARD	30
TOTAL	460

SUB TOTAL	1320(approx)

LITERATURE SURVEY: *Offence*

1) Signal Jamming

The most basic form of DoS attack is when another signal interferes with data transmissions as shown. Such interference can occur continuously or intermittently and arise from a variety of sources apart from malicious activity.

2) Disassociation Attack

A very similar vulnerability may be found in the association protocol that follows authentication. The IEEE 802.11 standard allows clients to associate with only one AP at a time.

3) Continuous Collision Jamming

Continuous collision jamming is effective but relatively expensive in energy terms and increases the probability that the attacker's location will be discovered. The study of Karhima et al. considered the effectiveness of continuous jamming signals against IEEE 802.11"b" and "g" networks [4].

4) Resource Depletion Attacks

Resource Depletion Attacks Resource depletion attacks normally target shared resources such as the AP to exhaust its processing and memory power so that it can no longer provide services to other (legitimate) stations. These attacks can be accompanied by more sophisticated attack such as introducing rogue access points to hijack the abandoned stations.

LITERATURE SURVEY:
Defence

1) Pseudo-Randomised Sequence Number

This study suggests a Pseudo Randomized sequence Number based solution to 802.11 Disassociation DoS attack. He suggests that the solution does not require any additional hardware and can be implemented in both wireless clients and Access Point via firmware upgrade. It was just mathematically implemented not physically.

2) Analysis and improvements of PEAP protocol

This paper showed that in recent years a large number of applications are developed for WLAN. But different types of issues related to security are also coming in WLAN. To provide security we need a secure authentication protocol like PEAP. This paper mainly talks about Protected Extensible Authentication Protocol (PEAP). The main concerns are its authentication process, what are the defects in EAP-PEAP and how we can improve PEAP so it can overcome through these defects

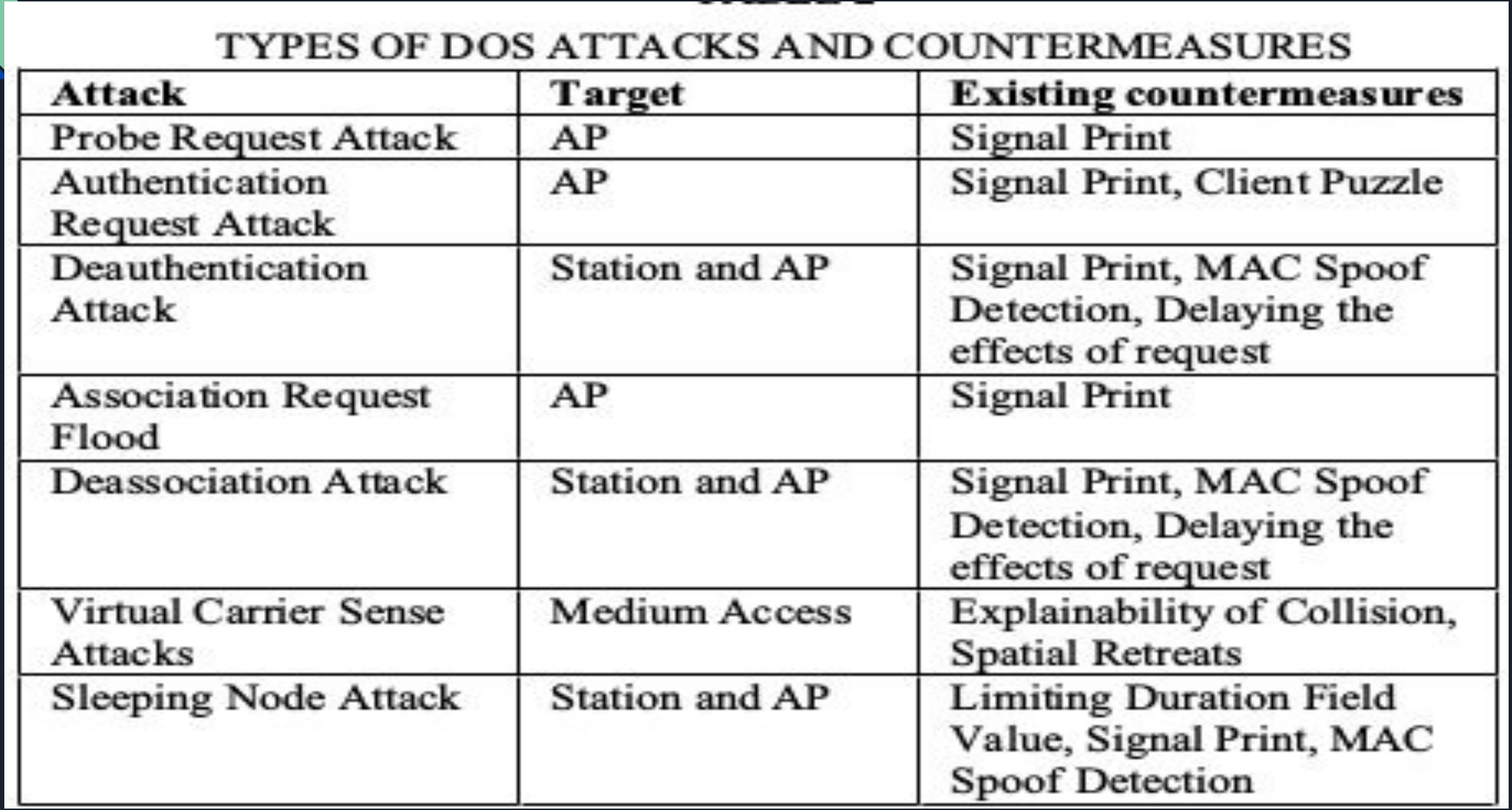
3) Static 4-Way Handshake

Floriano De Rango *et. al.*, [5] proposed static and dynamic 4 - way handshake solutions to avoid denial of service attack in WPA and IEEE 802.11i.

4) A Survey on Wireless Security protocols

This study presented a survey on wireless security protocols (WEP, WPA and WPA2/802.11i). Here WEP protocol types, weaknesses and enhancements, WPA protocol types, Cryptographic messages. Finally paper explained third generation of wireless security protocol as WPA2/802.11i.

LITERATURE SURVEY:



TYPES OF DOS ATTACKS AND COUNTERMEASURES

Attack	Target	Existing countermeasures
Probe Request Attack	AP	Signal Print
Authentication Request Attack	AP	Signal Print, Client Puzzle
Deauthentication Attack	Station and AP	Signal Print, MAC Spoof Detection, Delaying the effects of request
Association Request Flood	AP	Signal Print
Deassociation Attack	Station and AP	Signal Print, MAC Spoof Detection, Delaying the effects of request
Virtual Carrier Sense Attacks	Medium Access	Explainability of Collision, Spatial Retreats
Sleeping Node Attack	Station and AP	Limiting Duration Field Value, Signal Print, MAC Spoof Detection

REQUIREMENTS SPECIFICATION

HARDWARE REQUIREMENTS:

1.NodeMCU x 2

2.RGB LEDS x 2

3.OLED 0.96” I2C - IIC Interface

4.BUTTONS (TACTILE ON/OFF SWITCH)

5. BREADBOARDS x 3

6. JUMPER WIRES

7. POWER SUPPLY/ BATTERY

SOFTWARE REQUIREMENTS:

1)Arduino IDE

2) HTML to HEX Converter

REQUIREMENTS SPECIFICATION

HARDWARE REQUIREMENTS:

1.NodeMCU x 2

2.RGB LEDS x 2

3.OLED 0.96” I2C - IIC Interface

4.BUTTONS (TACTILE ON/OFF SWITCH)

5. BREADBOARDS x 3

6. JUMPER WIRES

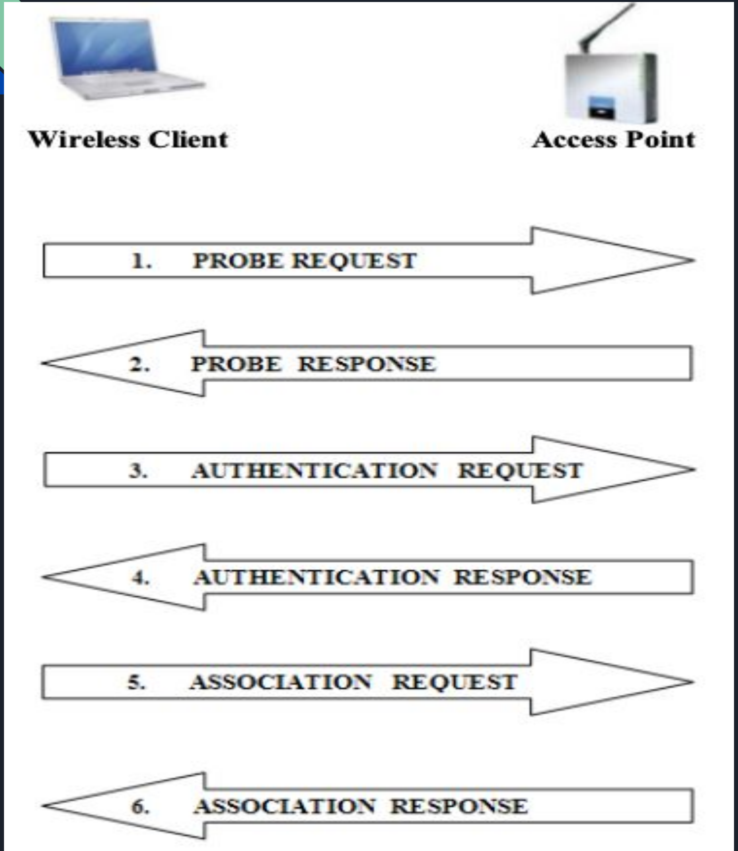
7. POWER SUPPLY/ BATTERY

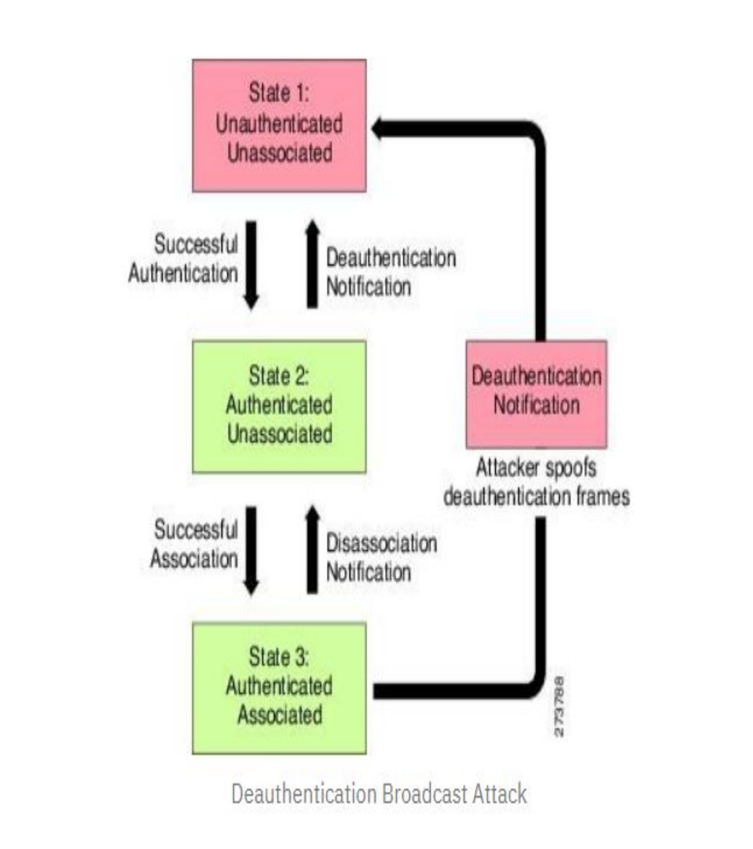
SOFTWARE REQUIREMENTS:

1)Arduino IDE

2) HTML to HEX Converter

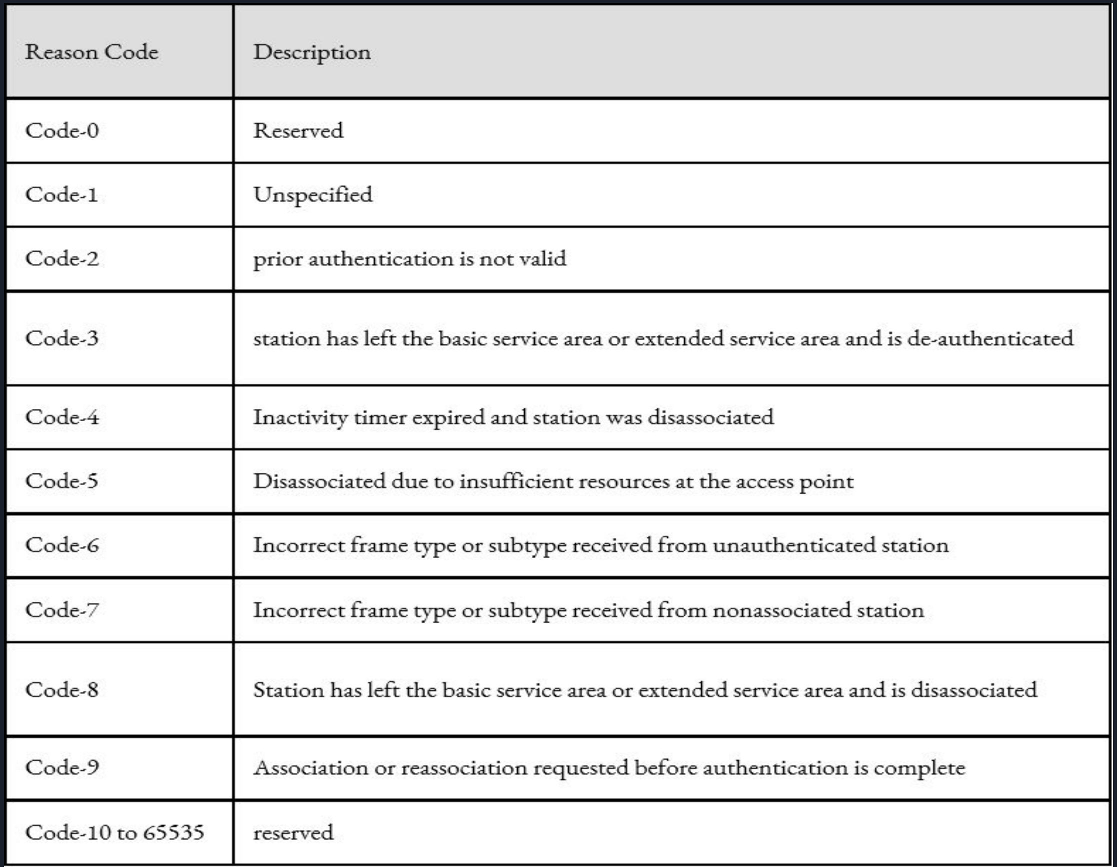
SCHEMATIC DIAGRAM





Deauthentication Broadcast Attack

REASON CODES



Reason Code	Description
Code-0	Reserved
Code-1	Unspecified
Code-2	prior authentication is not valid
Code-3	station has left the basic service area or extended service area and is de-authenticated
Code-4	Inactivity timer expired and station was disassociated
Code-5	Disassociated due to insufficient resources at the access point
Code-6	Incorrect frame type or subtype received from unauthenticated station
Code-7	Incorrect frame type or subtype received from nonassociated station
Code-8	Station has left the basic service area or extended service area and is disassociated
Code-9	Association or reassociation requested before authentication is complete
Code-10 to 65535	reserved

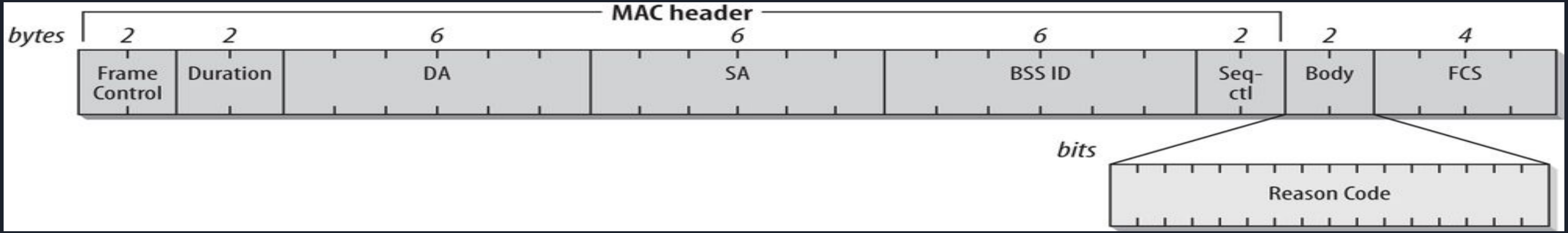
CONCEPTUAL EXPLANATION

There are **three** major types of frame used in IEEE 802.11 networks:

1) Data Frames: Data frames carry higher-level protocol data in the frame body.

2) Control Frames: Control frames assist in the delivery of data frames by providing area-clearing operations, channel acquisition and carrier-sensing maintenance functions, and MAC-layer reliability functions. Example: CTS, ATS, ACK

3) Management Frames: Management frames perform supervisory functions; they are used to join and leave the wireless network and move associations from access point to access point.



Body of Deauthorization Frame

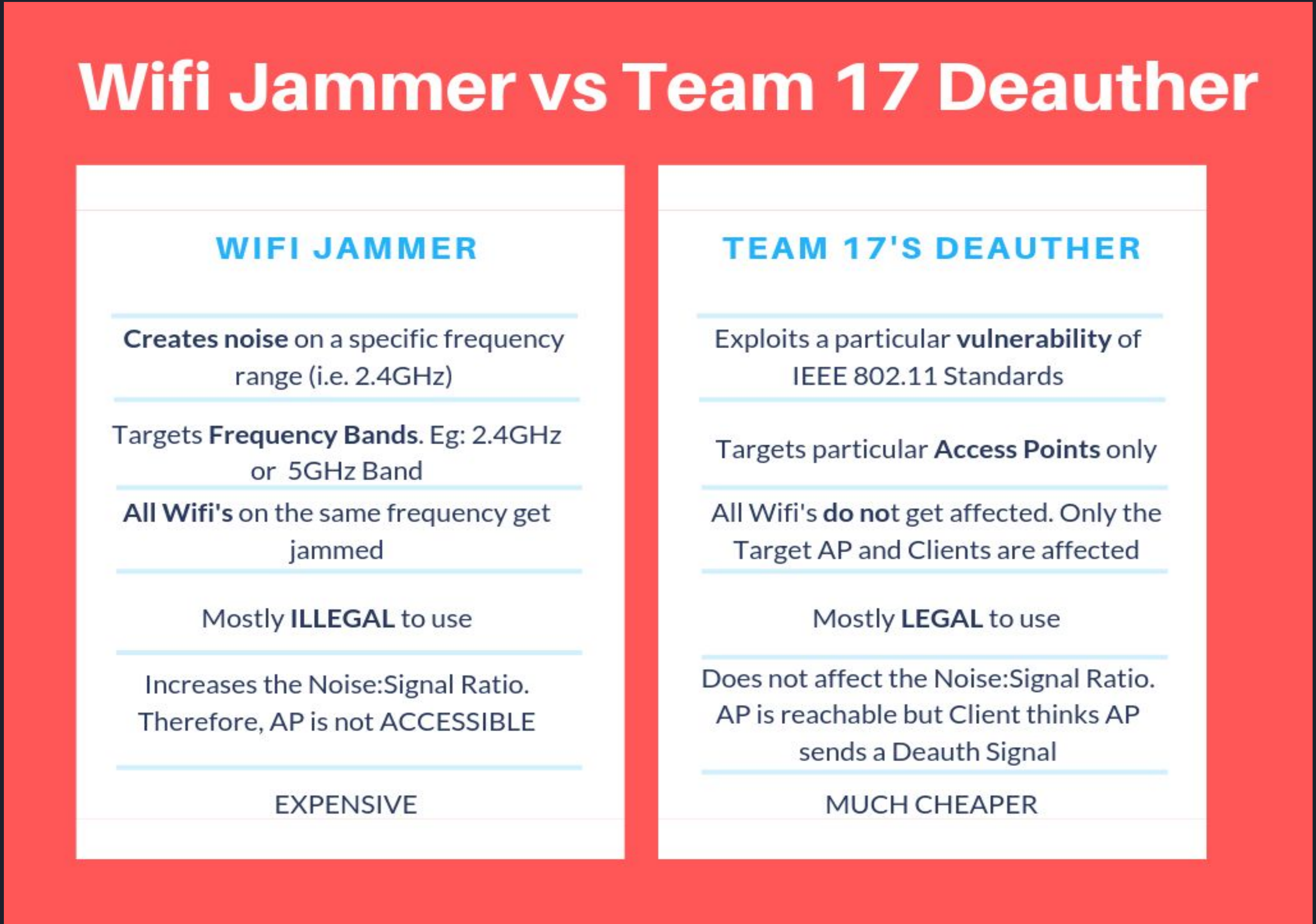
Detection of Deauthentication Frame:

(wlan.fc.type == 0) AND (wlan.fc.type_subtype == 0x0c)

Detection of Disassociation Frame:

(wlan.fc.type == 0) AND (wlan.fc.type_subtype == 0x0c)

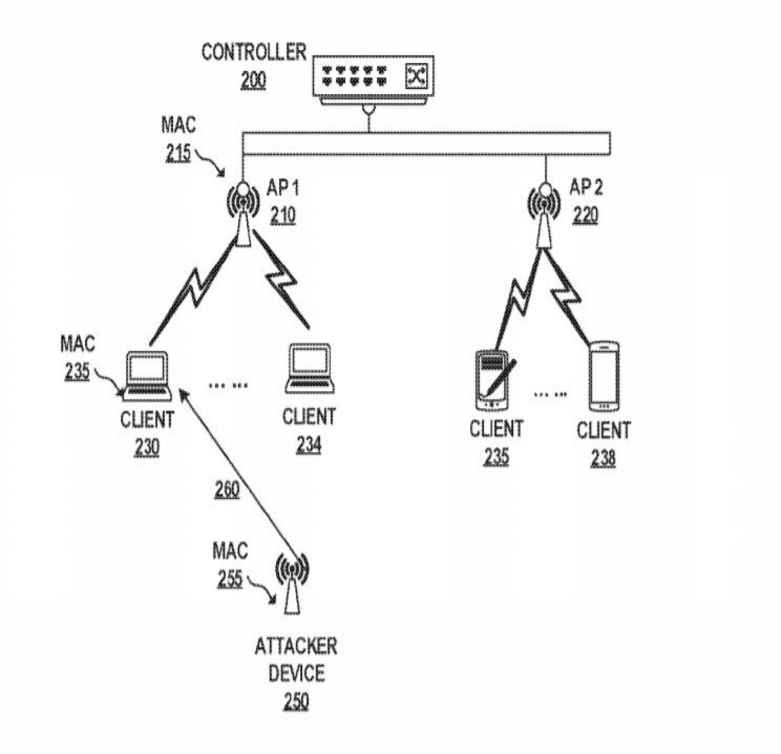
DIFFERENCE BETWEEN TEAM 17's DEAUTHER AND A WIFI JAMMER

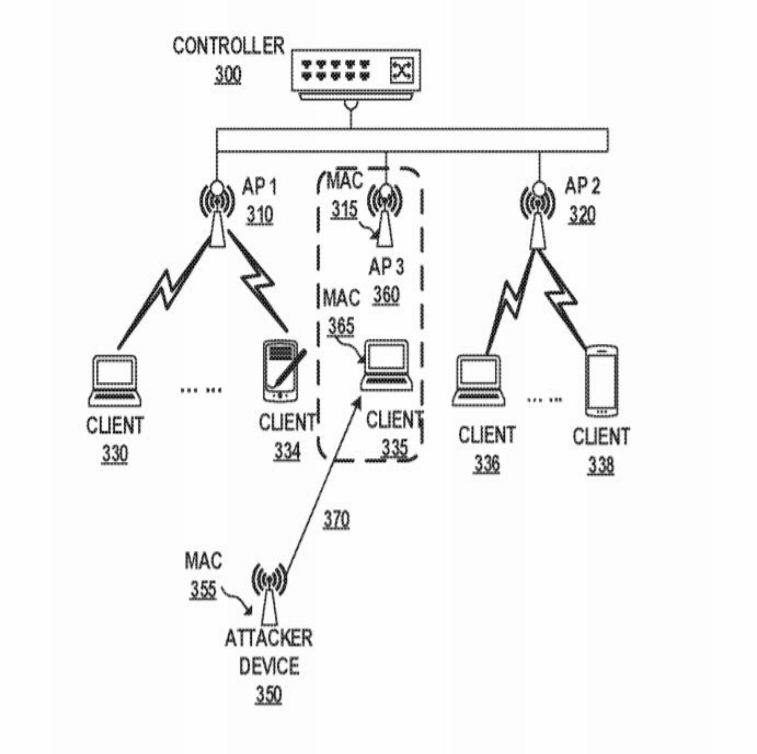


Wifi Jammer vs Team 17 Deauther

WIFI JAMMER	TEAM 17'S DEAUTHER
Creates noise on a specific frequency range (i.e. 2.4GHz)	Exploits a particular **vulnerability** of IEEE 802.11 Standards
Targets **Frequency Bands**. Eg: 2.4GHz or 5GHz Band	Targets particular **Access Points** only
All Wifi's on the same frequency get jammed	All Wifi's **do not** get affected. Only the Target AP and Clients are affected
Mostly **ILLEGAL** to use	Mostly **LEGAL** to use
Increases the Noise:Signal Ratio. Therefore, AP is not ACCESSIBLE	Does not affect the Noise:Signal Ratio. AP is reachable but Client thinks AP sends a Deauth Signal
EXPENSIVE	MUCH CHEAPER

WORKING OF THE MODULES

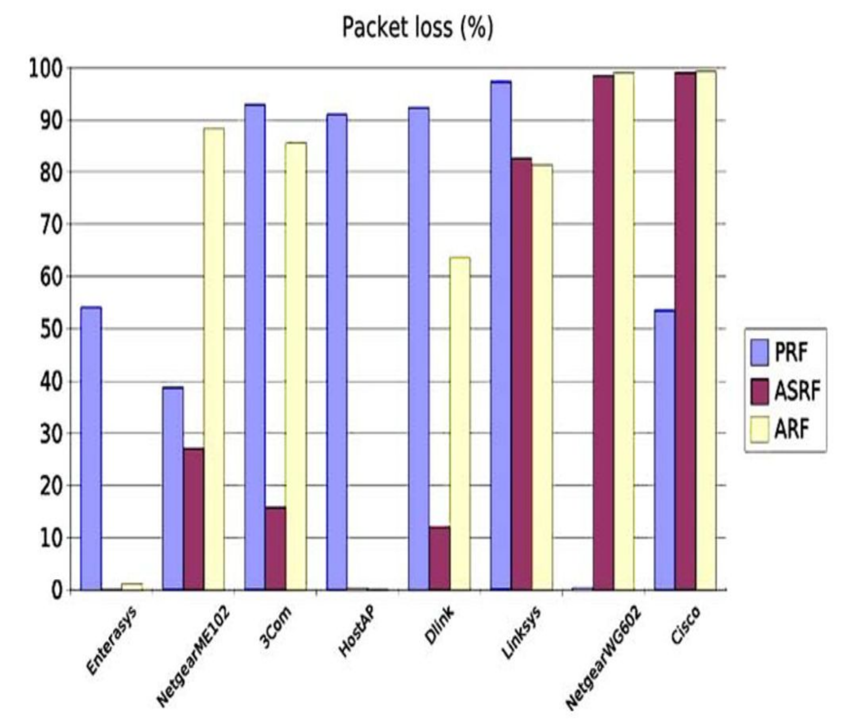


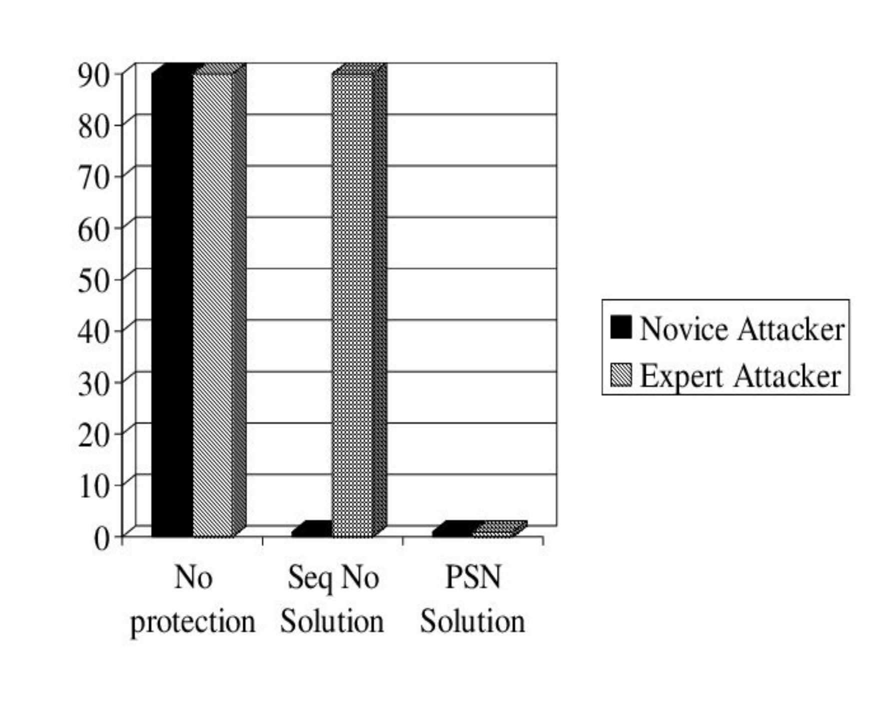


DEAUTH ATTACK

DEAUTH ATTACK DETECTION

ACCURACY OF THE ATTACK AND DETECTION



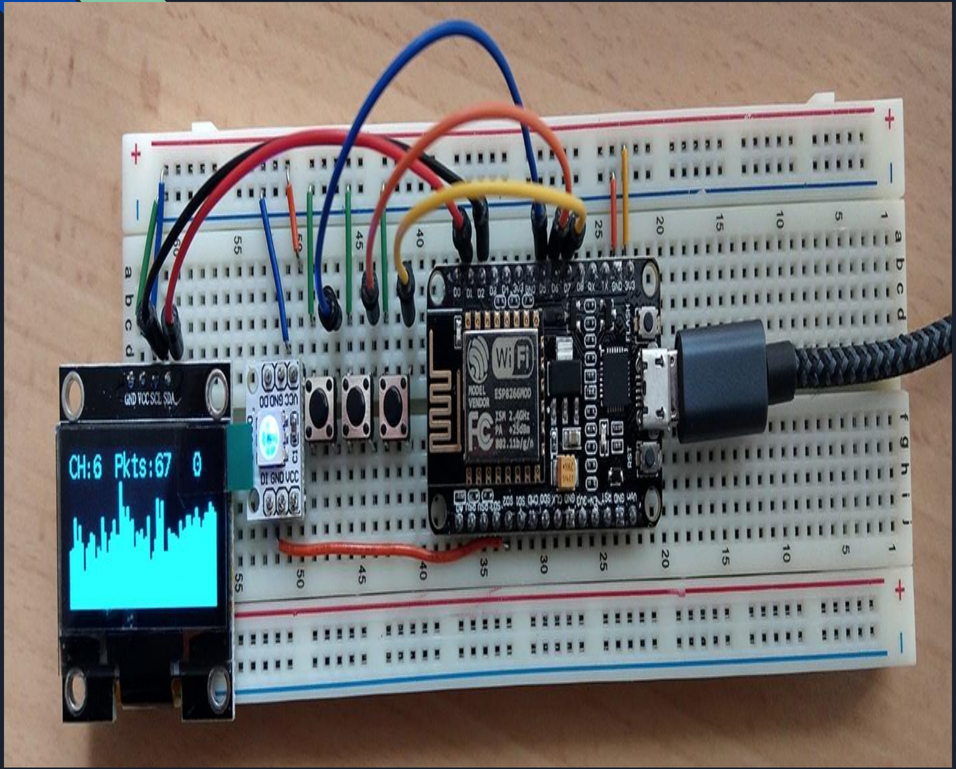


DEAUTH ATTACK %

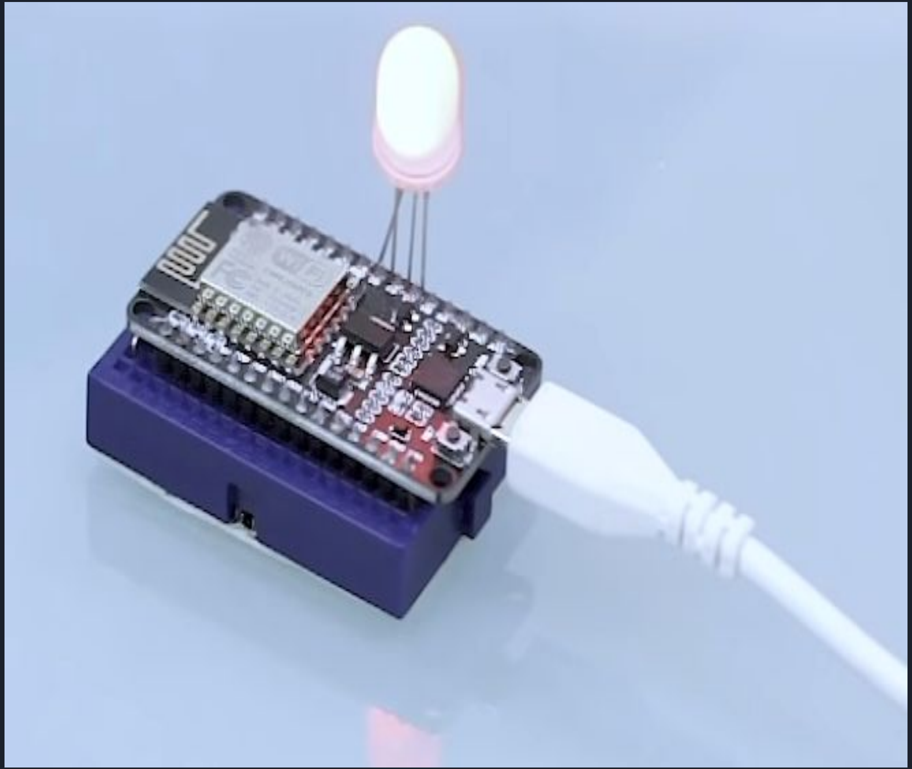
DEAUTH ATTACK DEFENCE %

**PRF: Probe Request Flood, ARF: Authentication Request Flood (ARF), ASRF: Association Request Flood (ASRF).*

IMPLEMENTATION

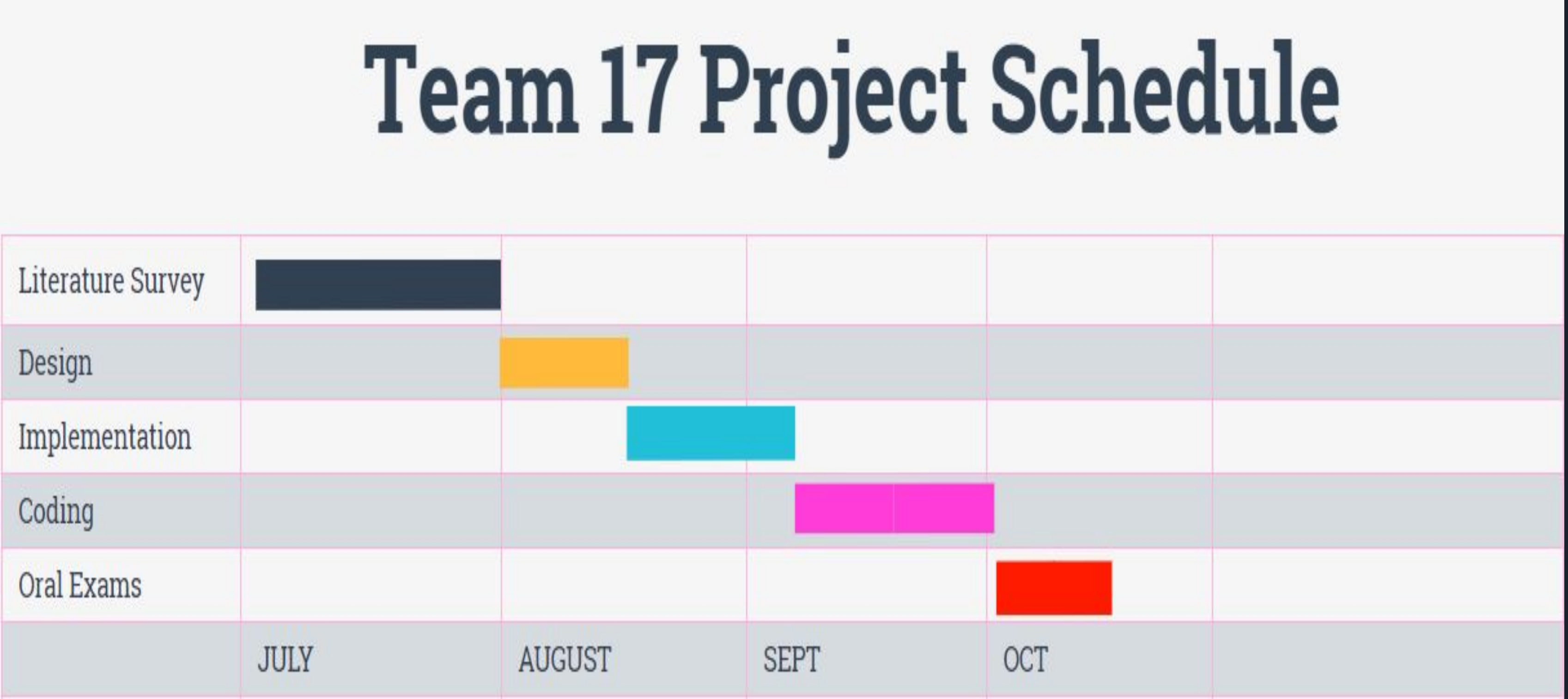


DEAUTHENTICATOR



DEAUTH DETECTOR

PROJECT PLAN



Team 17 Project Schedule

REFERENCES

[1] A. Atul, "Architecture and techniques for diagnosing faults in IEEE 802.11 infrastructure networks," MobiCom '04: Proceedings of the 10th annual international conference on Mobile computing and networking, pp. 30-44.

[2] M. Bernaschi, F. Ferreri, and L. Valcamonici, "Access points vulnerabilities to DoS attacks in 802.11 networks," Wirel. Netw., vol. 14(2), pp. 159-169, 2008.

[3] Prabhaker Mateti, The Handbook of Information Security. Dayton: John Wiley & Sons, Inc, 2005.

[4] Teemu Karhima, Aki Silvennoinen, Michael Hall, and Sven-Gustav Häggman. IEEE 802.11b/g WLAN tolerance to jamming. In *IEEE Military Communications Conference, 2004*, volume 3 of *MILCOM 2004*, pages 1364–1370, October 2004.

[5] De Rango, Floriano, Cristian Lentini, Dionigi, Marano, Salvatore, EURASIP Journal on Wireless Communications and Networking, "Static and Dynamic 4-Way Handshake Solutions to Avoid Denial of Service Attack in Wi-Fi Protected Access and IEEE 802.11i", 2006

[6] iperf network testing tool. Webpage. http://sourceforge.net/projects/iperf.

[7] tcpdump packet analyzer. Webpage. http://www.tcpdump.org.

[8] John Stratigakis. Hardware assist system and method for the timing of packets in a wireless network. US Patent 7233588, US Patent Office, June 2007.

[9] Stefan Kremser. Deauthentication and other wifi hacks. Webpage. https://spacehuhn.io

[10] Kody Bryan. Scan, Fake & Attack Wi-Fi Networks with the ESP8266-Based WiFi Deauther. Webpage. https://null-byte.wonderhowto.com/

[11]] Aircrack-ng, http://www.aircrack-ng.org

[12] Wireshark, http://www.wireshark.org

THANK YOU