Wi-Fi Pentesting Notes

Contact

LinkedIn: https://www.linkedin.com/in/segev-eliezer/

YouTube: https://YouTube.com/@0xd4y

Website: https://0xd4y.com

GitHub: https://GitHub.com/0xd4y

Table of Contents

Contact
Table of Contents
Fragmentation and Hirte Attack
- Fragmentation
- Hirte Attack
- Hidden SSID
  - Detection Techniques
- MAC Filter
- WLAN Authentication
- Hotspot Attacks
- Hacking Isolated Clients
  - Client Authentication to Attacking Machine
  - MITM

        MITM SSL
    SSID
WEP (Wired Equivalent Privacy) Attacks
    Replay Attack
    Caffe Latte Attack
    Korek's ChopChop
Wi-Fi Gear
    External Wireless Card
WLAN Headers
    Terminology
    WLAN Packet Header
        Frame Control Field
        Duration / ID
        Address 1-4
        Sequence Control
        QOS Control
        Frame Body
        FCS
WPA2 -PSK
WPA-PSK
    Cracking WPA-PSK
        Dictionary Attack
    Keys
        WPA-PSK Authentication Further Explanation
Detecting Spoofing Attacks
    SSID Spoofing
    Mac Spoofing
Wireless IDS and IPS
Malicious SSID
    HTML Injection and XSS
    SQLi

Fragmentation and Hirte Attack

Fragmentation

- when large frame is to be transmitted but larger than maximum transferrable unit for network, the frame needs to be broken up into fragments

- located within the "Sequence Control" header field
    - see WLAN Headers

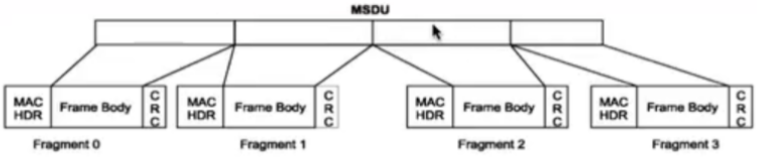
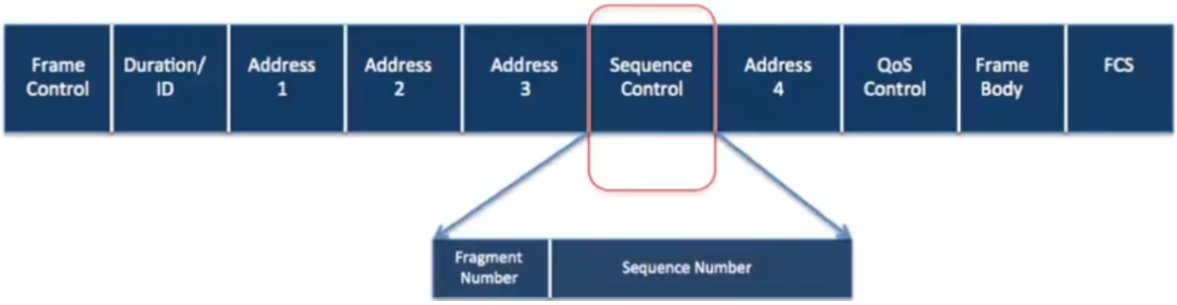
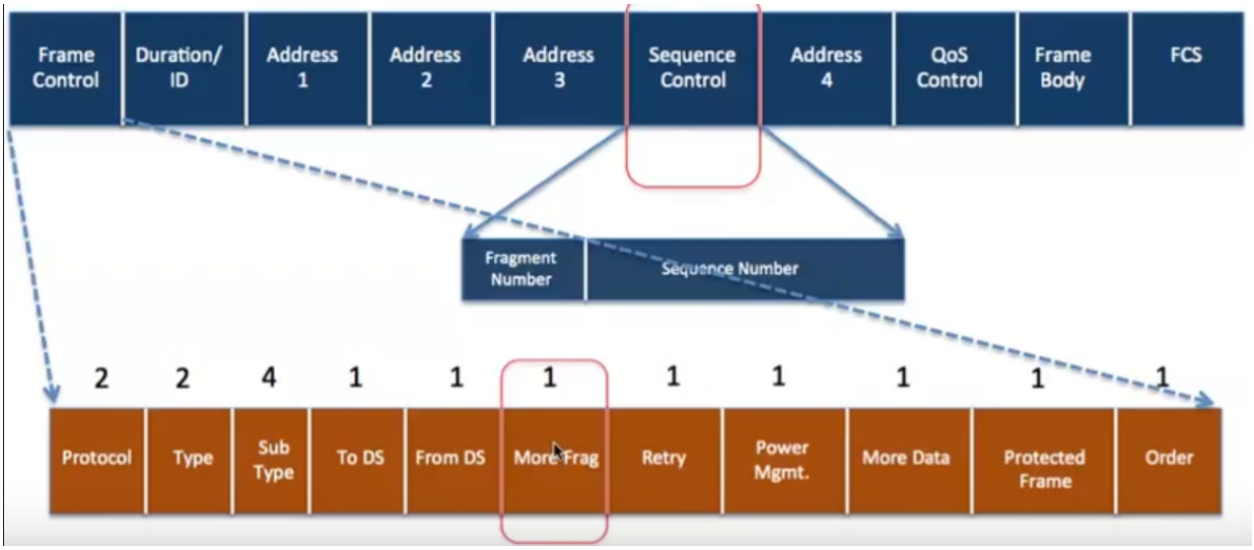


Figure 9-2—Fragmentation



- sequence number stays constant, but fragment number changes
- "more Frag" (more fragmentd) bit set to 1 for all fragmented packets except for the last one!
- indicates that more fragment packets are yet to be sent (receiver waits and doesn't reassemble packet until this bit set to 0)



Hirte Attack

1. Setup a fake WEP AP and wait for a client to connect
2. Upon connection of a client waits for auto-configuration IP address
3. Client sends an ARP packet
4. Obtain the ARP packet and convert it into an ARP request for the same client
    - relocates IP address in ARP header using fragmentation
5. Client replies
6. Collect these packets
7. Crack the WEP key# Hidden SSID, MAC Filter, and Authentication

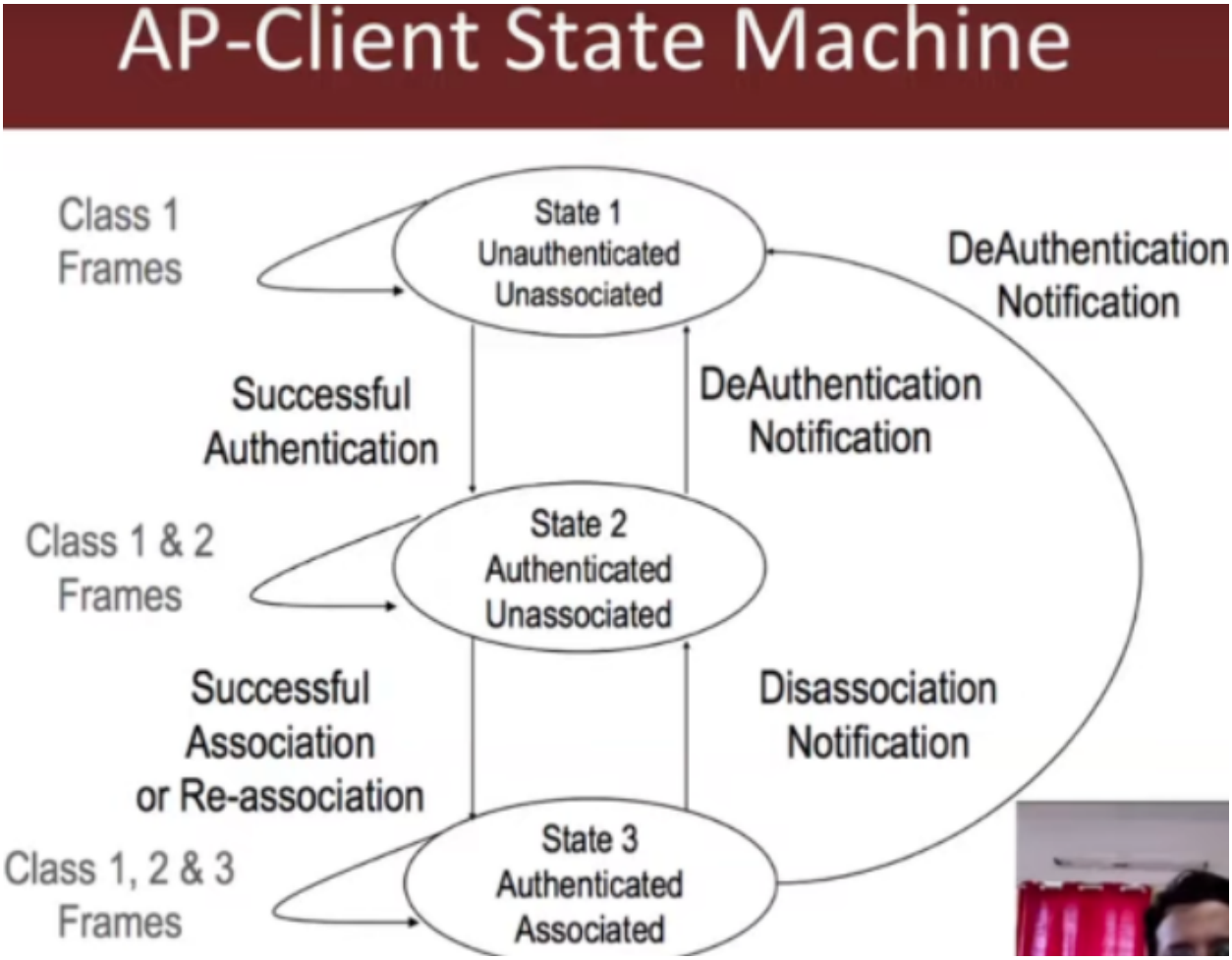
Hidden SSID

- SSID broadcasting off in beacon frames

Detection Techniques

1. Passive
    - monitor air for new client trying to associate with access point
    - look for connection to the hidden SSID by monitoring probe and association packets
        - the association and probe packets contain the SSID in the "Tag interpretation" parameter
2. Active
    - de-authenticate one or all clients and monitor reconnections
        - when clients are disconnected, they will try to reconnect and you can get the SSID as described in the "Passive" technique

How to Deauthenticate

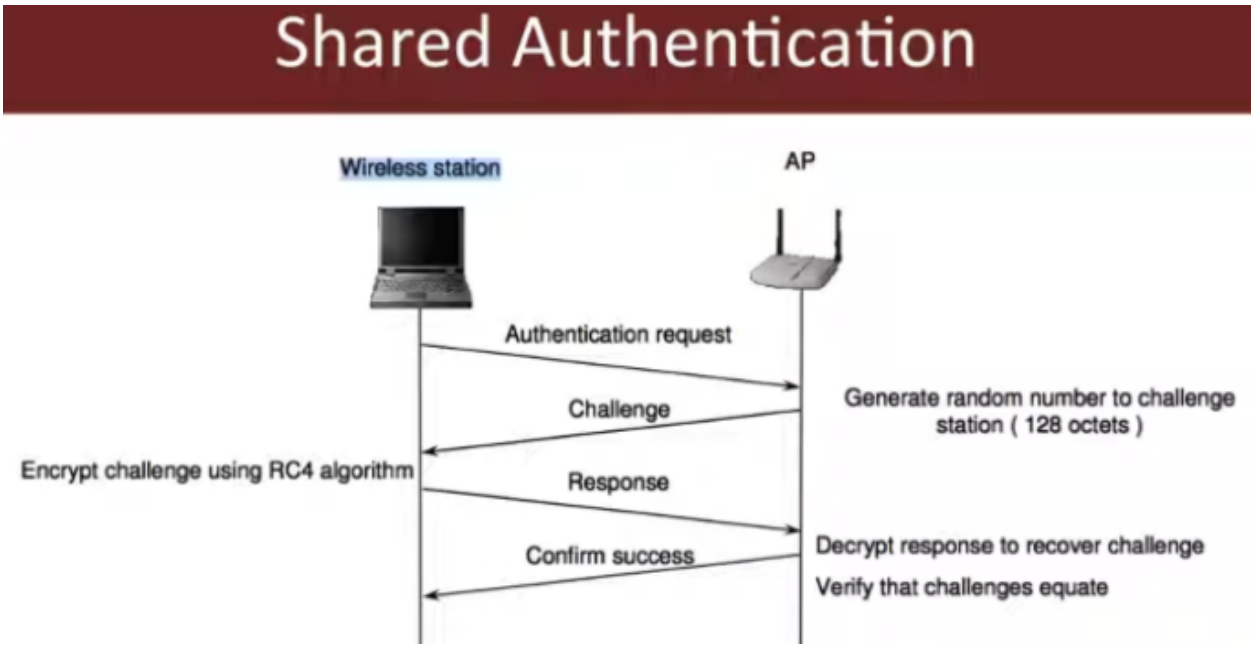


- when client deauthenticates, a management packet called "Deauthentication packet" is sent from AP to client

MAC Filter

- MAC filter typically used with switches and filtering devices and firewalls
  - feature to whitelist MAC address on specific port
  - MAC can be easily spoofed, so whitelist is not secure
- MAC filter is a network layer filter
- MAC addresses visible in plain text in WLAN header
- some access points use captive portals and add a device to a mac filtering list after it successfully authenticates

WLAN Authentication



1. STA asks to authenticate to AP
2. AP sends challenge response
3. STA encrypts challenge with WEP password
4. STA decrypts challenge with WEP password. If matches, grant access

- shared key authentication (SKA) is broken
    - possible to retrieve the key by reversing XOR operation# Hotspot Attacks and Hacking Isolated Clients (MITM)

Hotspot Attacks

- no encryption

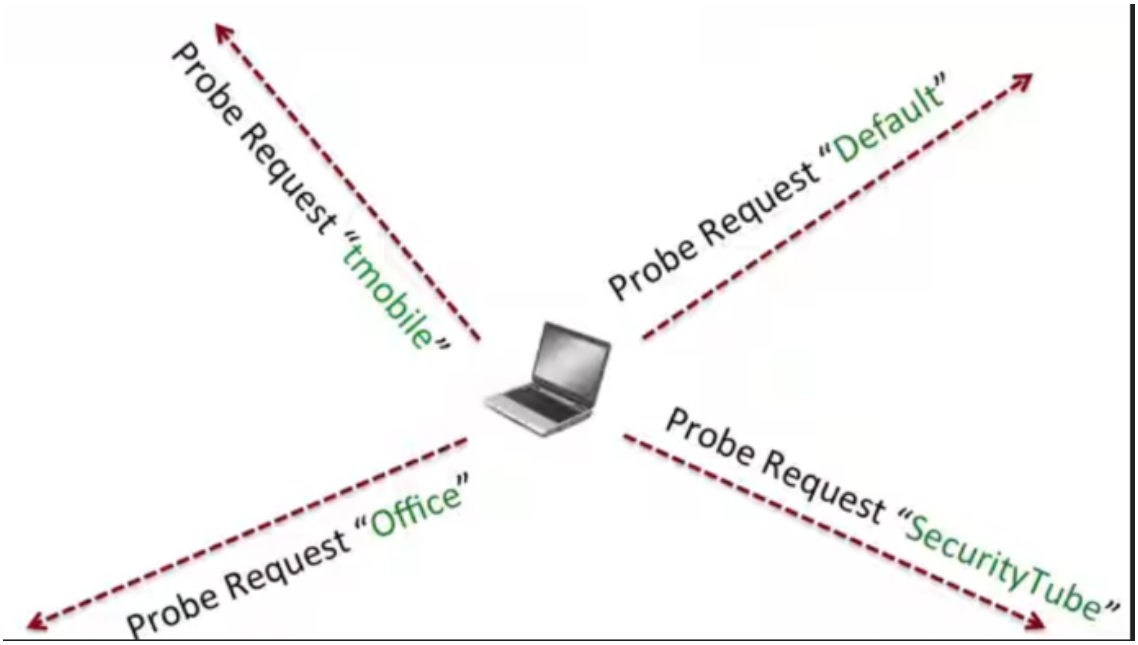
Soft AP: access point created entirely in software

- evil twin
    - same ESSID as target (can even set BSSID to be the same)
    1. Attacker sets up AP with same SSID as target AP then sends deauth packet to victim.

2. After victim is deauthenticated, their computer tries reconnecting to the SSID with same name and highest signal strength.
3. The victim will automatically connect to attacker machine.

Hacking Isolated Clients

- when client connected to SSID, that SSID is added to preferred network connection list
- client automatically connects to known SSIDs
    - client sends probe requests packets to locate known SSIDs in the preferred network connection list
        - Probe Request Packet: packet meant to locate available networks



- if true AP has no authentication, then making a malicious AP with same SSID will likely not make the client automatically connect
    - the client must manually connect to the malicious AP

Client Authentication to Attacking Machine

- client cannot authenticate AP

- SSID alone used to trust AP
- easiest with Hotspot as it is open authentication with no encryption

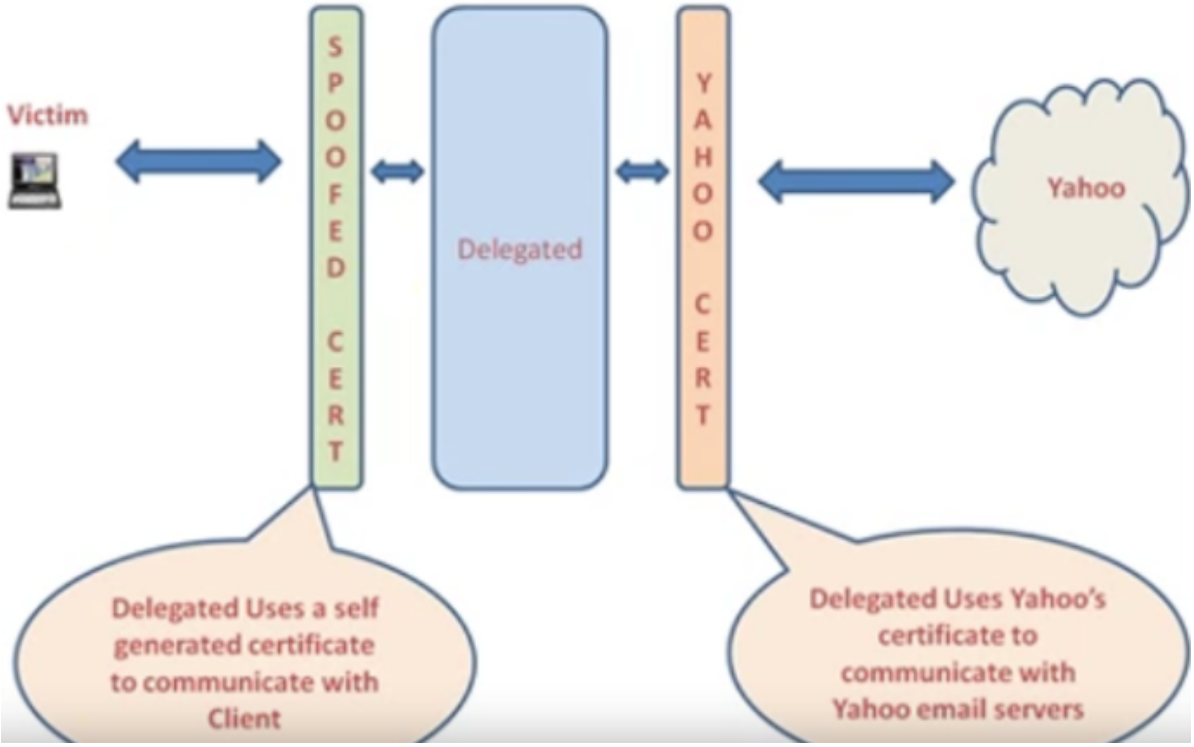
MITM

Man in the middle

- hacker connected to internet via eth0
- hacker has fake AP on mon0
- create bridge between mon0 and eth0
  - `brctl addbr <name of bridge>`
  - `ifconfig <name of bridge> up`

MITM SSL

- `dnsspoof -i <name of bridge>`
- victim will connect to spoofed DNS upon a DNS query, because dnsspoof will respond faste than true DNS
- attack works even through SSL, as client's requests are being encrypted using spoofed cert which is then decrypted by the hacker (note the hacker knows the encryption as they signed the certificate), and then the traffic is forward to the requested resource using the requested resource's certificate
  - this same traffic works in the reverse process when the requested resource responds to the request and sends the traffic back to the victim



  - note that there is a certificate error on victim device (due to BurpSuite using self-generated certificate instead of certificate of requested service)# Misc Information

SSID

- service set identifier (SSID)
- name given to an access point or network consisting of multiple access points
- beacon frames a.k.a broadcast frames are sent by access points to broadcast presence in current RF vicinity
  - this is how your computer finds nearby Wi-Fi networks to connect to
- using MDK3 tool, it is possible to spoof a network by sending beacon frames (it even appears as high signal strength)
  - easy to spoof 802.11 frames because there is no encryption# Network Devices OSI
- open systems interconnection model

- seven layers:
    1. Physical
    2. Data Link
    3. Network
    4. Transport
    5. Session
    6. Presentation
    7. Application

Switch

- layer 2 OSI device
- only communicate with local network devices
- uses application-specific integrated circuit (ASIC) chip
    - ASIC chip tells switch which ports a device is connected to

WAP

- wireless access point
- layer 2 OSI device
- only communicates with local network devices

MLS

- multilayer switch
- provides layer 2 switching services and layer 3 or high OSI model services
- most common MLS is layer 3 switch
- uses ASIC chip for switching and handling routing functions

Router

- layer 3 OSI device
- uses software for decision making

Firewall

- can be software based or network appliance
- functions at multiple OSI model layers (usually 2,3,4, and 7)
- blocks packets in 2 different ways:
    - *Stateless inspection*: examines every packet against set of rules
    - *Stateful Inspection*: examines state of connection between networks as general rules (e.g. firewall blocks any outgoing traffic on port xxxx)

Load Balancer

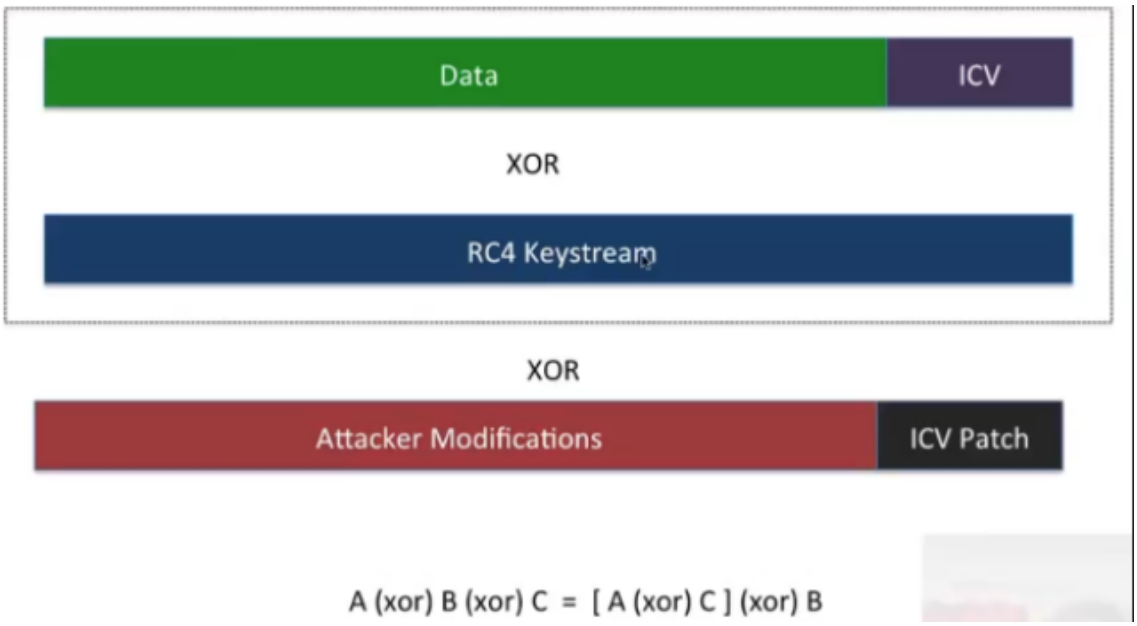
- also called content switch or content filter
- used to ensure no single gets overloaded with traffic

Proxy Server

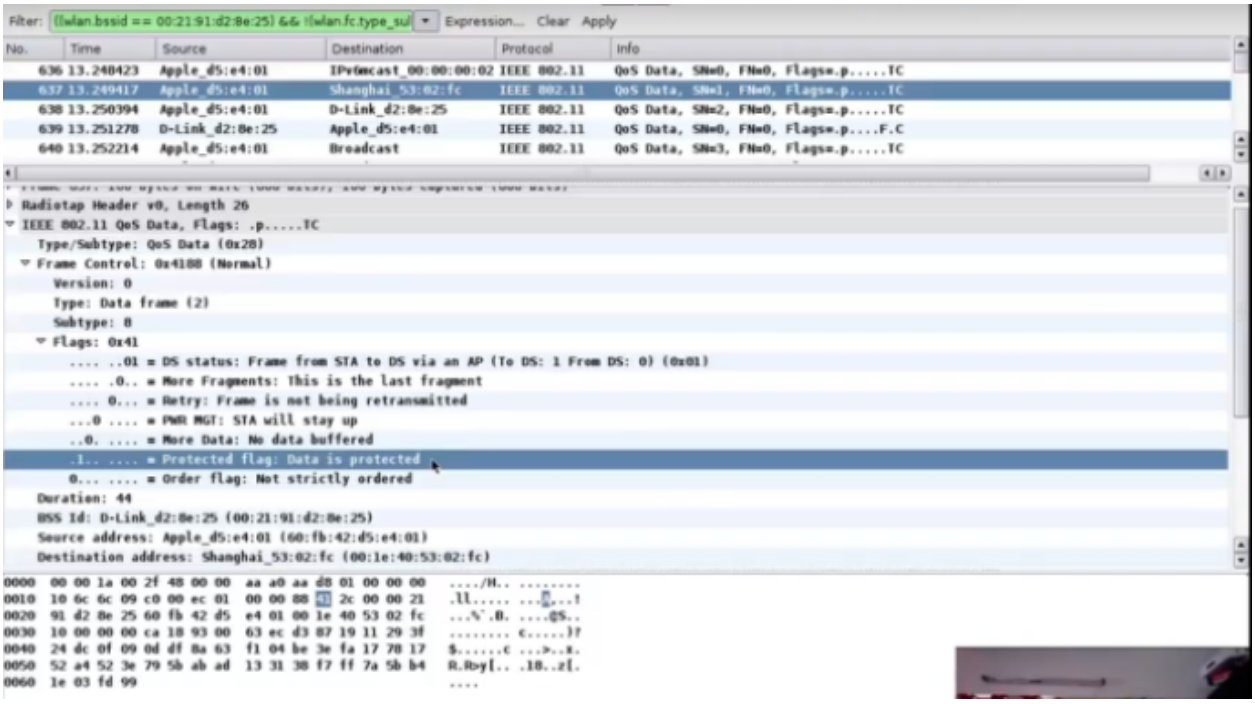
- often used to retrieve resources from outside untrusted networks
    - can also be used to filter allowed content# Useful Links
      SyllabusSequence Number

WEP (Wired Equivalent Privacy) Attacks

- first encryption scheme for Wi-Fi
- insecure (uses RC4 encryption)
    - symmetric encryption (transmitter and receiver have identical key for decrypting and encrypting)
    - possible to tamper data



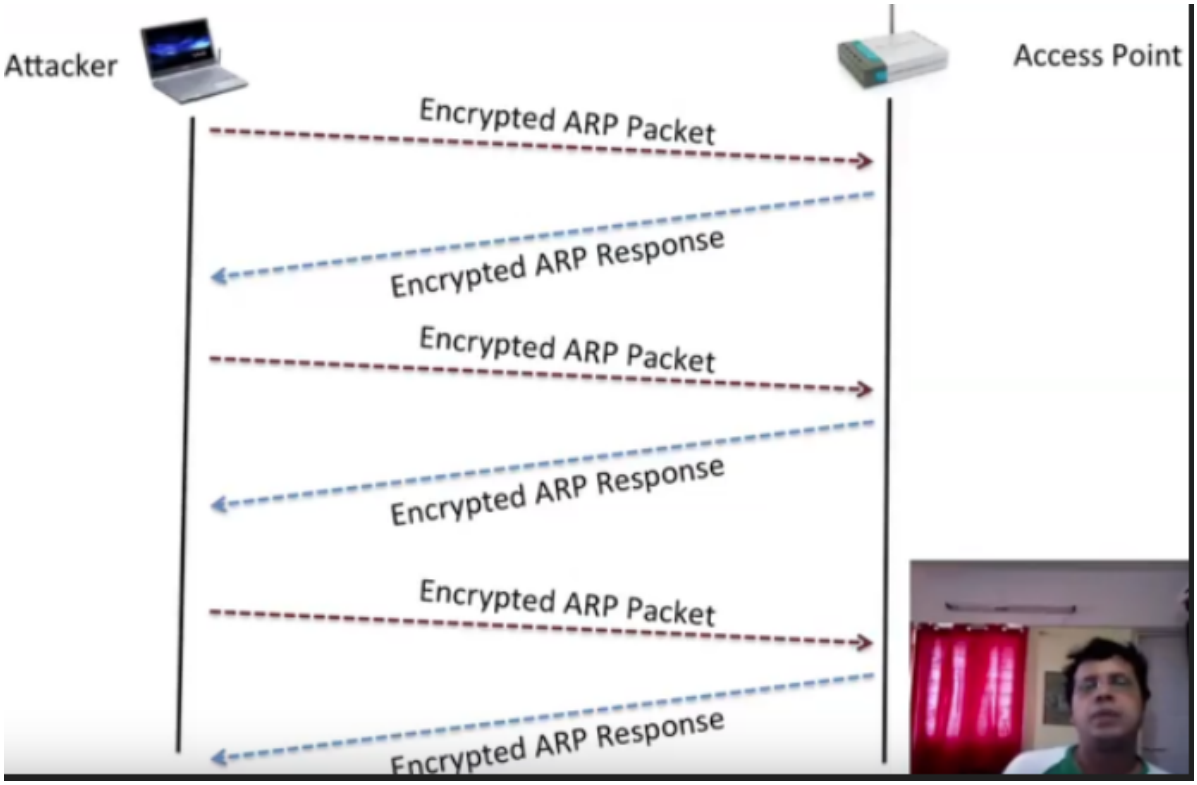
- check "Protected flag" to see if it is set (if set that means encryption is in place) Example of encrypted package:



Replay Attack

- noisy and easily detectable

- encrypted ARP packet can be identified due to its fixed length
    - these ARP packets are captured by hacker and constantly replayed to AP until the AP responds with enough weak IVs in the ARP responses to crack the key



Caffe Latte Attack

- this scenario assumes that the regular AP on which the client connects to contains a WEP key in its PNL

1. set up AP (evil twin) and deauth client
2. client tries to reconnect to AP with same SSID and highest signal strength
3. WEP key sent by client to malicious AP
4. malicious AP accepts all WEP keys and grants authentication

Korek's ChopChop

- last byte of encrypted data packet is chopped off. The byte of the data is then guessed and ICV is calculated. If guess is correct, ICV matches and encrypted data

is accepted

- process is repeated for all the bytes of the encrypted packet to obtain the full packet

Wi-Fi Gear

External Wireless Card

- allows for packet sniffing and packet injection
- wireless cards can only be on one channel at a time# Wi-Fi Sniffing
- WLANS operate in 3 different frequencies:
  1. 2.4 GHz (802.11b/g/n)
  2. 3.6 GHz (802.11y)
  3. 3.9/5.0 GHz (802.11a/h/j/n)
- 3 types of WLAN packets:
  1. Management
  2. Control
  3. Data

WLAN Headers

Terminology

Ad Hoc Network

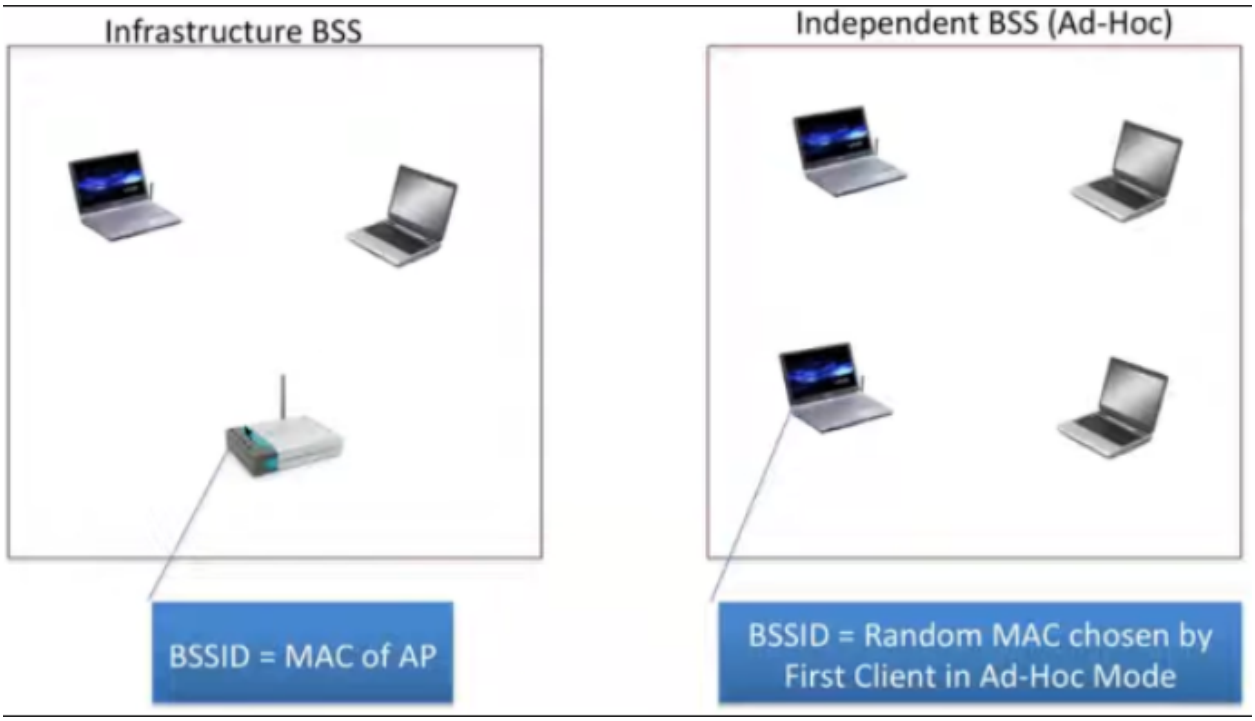
- decentralized network
- devices communicate directly with each other instead of using bridge (e.g. access point)
- communicates peer to peer (which is why ad hoc is also called peer to peer mode)
- cheap and quick, but performance decreases as more users join network
- can have some security risks

Infrastructure Network

- communicate with access point (typically covers between 100 to 200 feet)
- centralized network
- requires constant administration

STA: STAtion (wireless client)
BSS: set of wireless client nodes communicating with each other

- two types
- infrastructure BSS (AP and clients)
- independent BSS (Ad-Hoc Client)



ESS: set of connected BSSs
BSSID

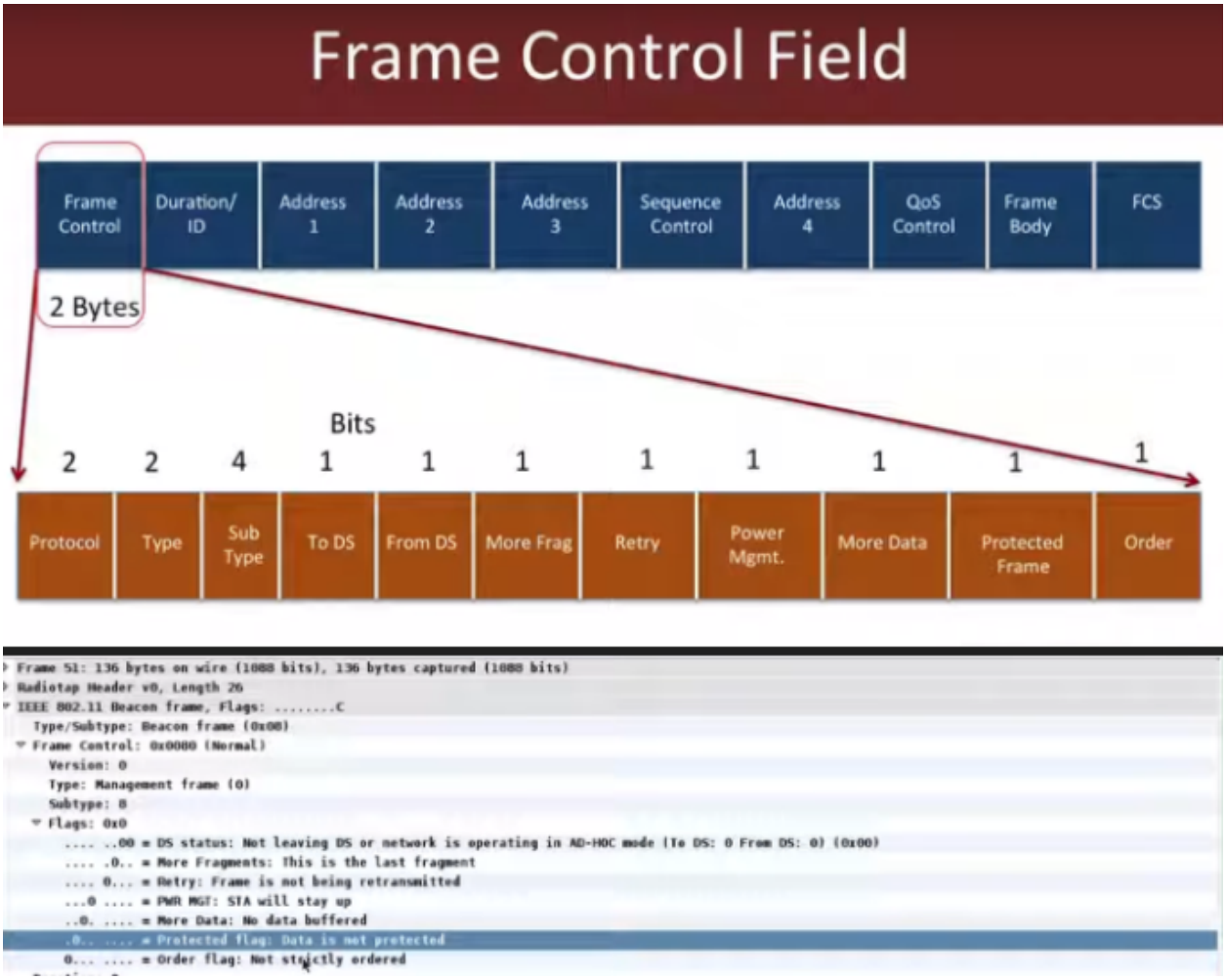
- basic service set identifier
- in the case of an infrastructure BSS it is the MAC address of AP
- in the case of an IBSS (independent BSS) it is the randomly chosen MAC address

Distribution System (DSU): connects APs in an ESS

WLAN Packet Header

Frame Control Field

- header starts at frame control which is two bytes (as opposed to two bits)



Protocol

- default to 0 value (may change when a major revision is incompatible with a previous version)

Type and Sub Type

- type
  - management, control, and data frames (each one of these has a sub type)
    - note each one of these fields is a bit

To and From DS

Retry Bit

- retry bit indicates if current frame is a retransmission

- applicable only to management and data frames

Power Management

- indicates if STA is in power save mode or active mode

More Data

- indicates to STA in power save mode that more data is to follow
    - such as in situations when data is to be sent, but sender is low on battery
- data is queued up on AP

Protected Frame

- 1 indicates Frame Body is encrypted
    - applicable to data frames and management frames of type authentication
- 0 indicates no encryption

Order

- indicates that all received frames must be processed in order

Duration / ID

- slash is there to indicate that this field could be used either as a duration field or ID field
- duration field used to set Network Allocation Vector (NAV)
    - NAV is the minimum amount of time a STA needs to wait before attempting transmission

Address 1-4

- WLAN has more than one address
    - Source Address
    - Destination Address
    - BSSID
    - Address 4 is used in a WDS

- value and presence of addresses 2-4 depend on type / subtype

Sequence Control

- broken up into two fields:
  1. Sequence number of packet
     - number of packet transmitted by wireless entity
     - Sequence Number
  2. Fragment number of packet
     - which fragment is current frame of larger packet (if applicable)

QOS Control

- quality of service related

Frame Body

- contains data payload
  - can contain management subheader of packet
- consists of Logical-Link Control (LLC) and Address Resolution Protocol (ARP)

FCS

- Cyclic Redundancy Check (CRC) over MAC header and Frame Body
  - detects accidental changes to raw data
- 4 bytes

WPA2 -PSK

- encryption algorithm in the probe response
- method of cracking is the same as in WPA-PSK
  - just as vulnerable as WPA-PSK if weak password is chosen #

WPA-PSK

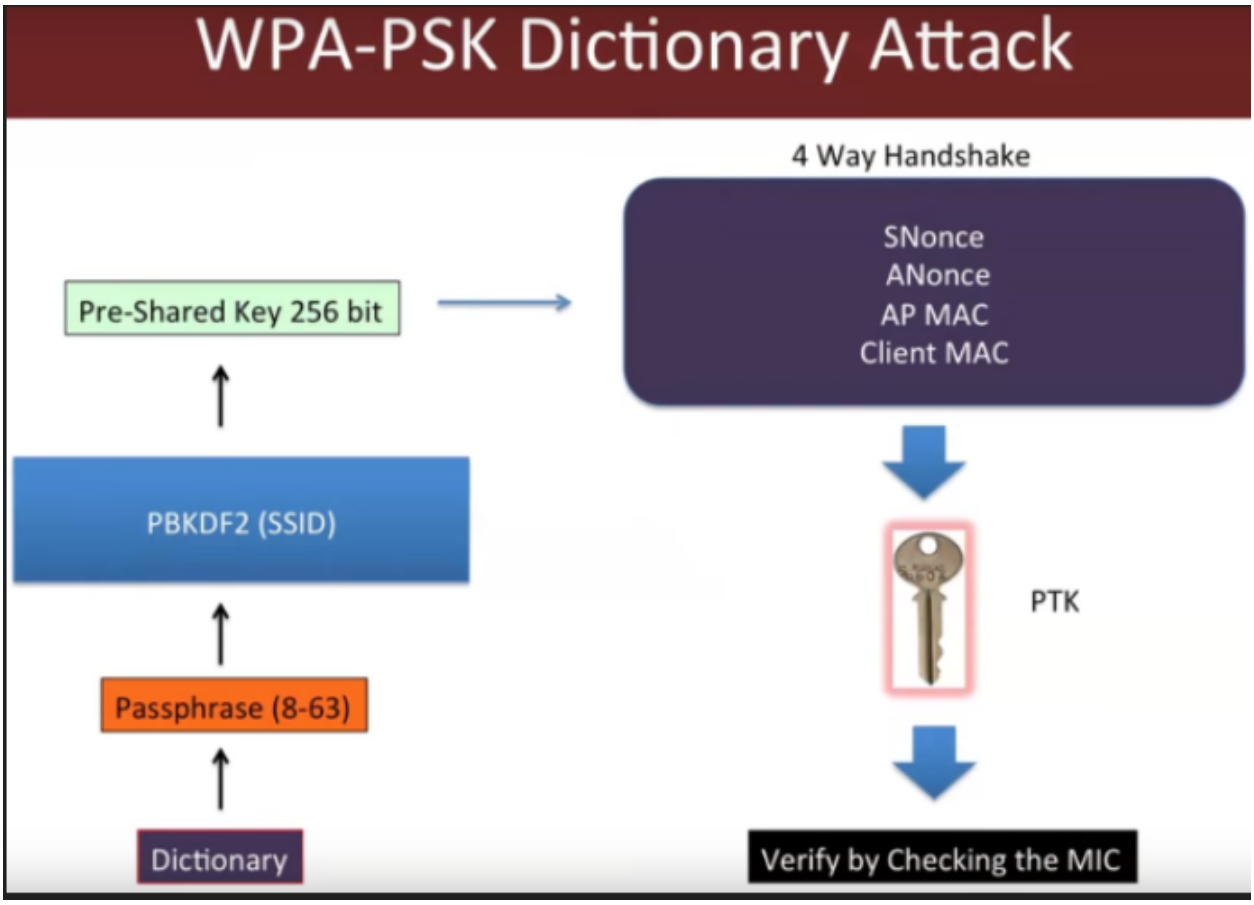
- used for personal use typically
- based on WEP
- uses TKIP (encryption method)
- personal networks typically use PSK while enterprise uses 802.1x + Radius
  PTK (Pairwise Transit Key)
- used for encryption of packets between client and AP

$$PTK = PMK + ANONCE + SNONCE + MAC(AA) + MAC(SA)$$

- PMK (Pairwise Master Key): comprised of SSID and passphrase
- ANONCE: random number AP has made
  - present in packets 1 and 3
- SNONCE: random number client has made
  - present in packet 2
- MAC(AA): MAC address of AP (authenticator)
- MAC(SA): MAC address of client (supplicant)
  - MAC(AA) and MAC(SA) present in all packets

Cracking WPA-PSK

Dictionary Attack



- reconstruct the MIC using the PTK, if MIC matches the one in packet, then the PTK is correct and the passphrase was successfully guessed
  MIC (Message Integrity Code)
  Value dependent on following parameters:
  1. message body
  2. PTK

Keys

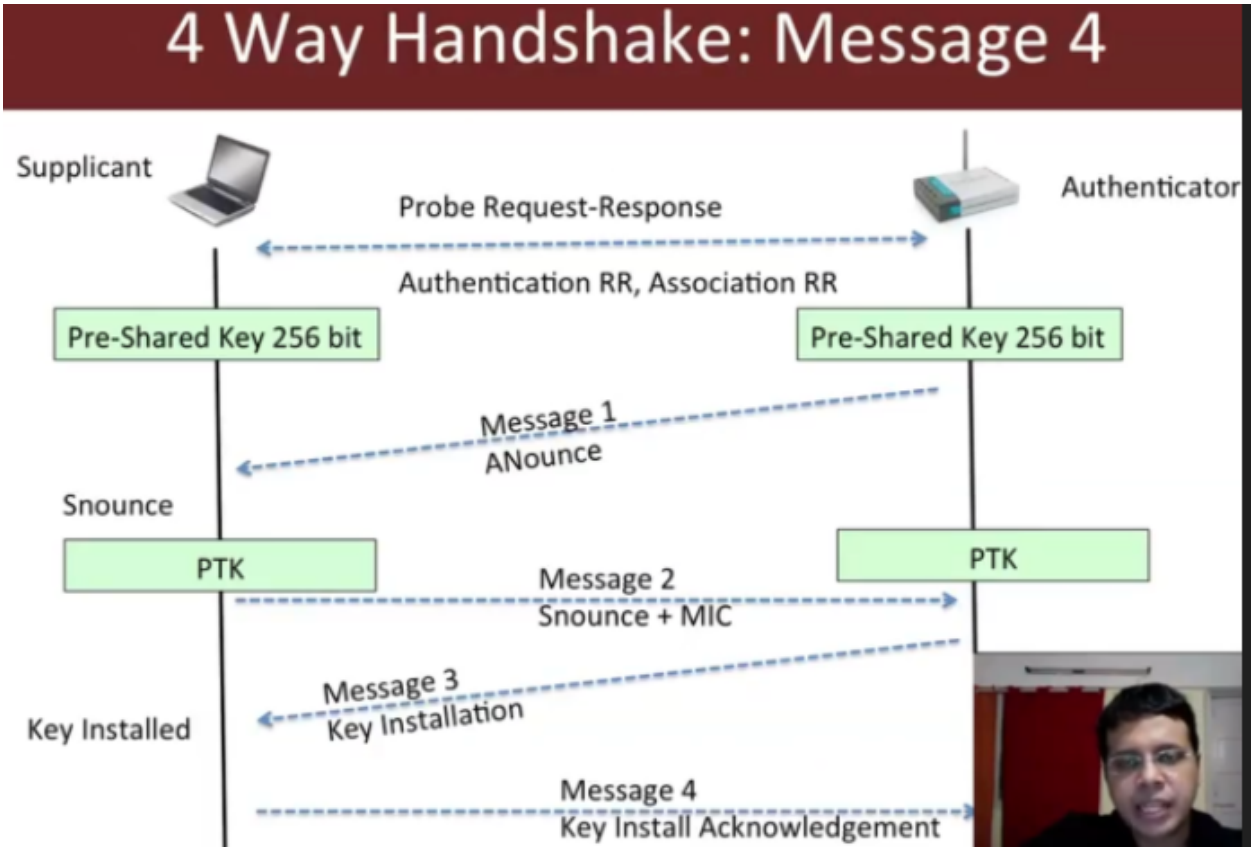
```
#! /usr/bin/env python
from pbkdf2 import PBKDF2

ssid = raw_input('SSID: ')
passphrase = raw_input('Passphrase: ')

print ("Pairwise Master Key: " + PBKDF2(passphrase, ssid, 4096).read(32).encode("hex"))
```

- PBKDF2 takes in the following five parameters:
    1. Passphrase
    2. SSID of AP
    3. SSID length
    4. 4096 - number of times passphrase is hashed
    5. 256 - intended key length of PSK (in bits)
- WPA uses dynamic keys for encryption
    - keys generated on per connection basis
- in WPA and WPA2 personal, the PSK and PMK is the same

WPA-PSK Authentication Further Explanation



1. Supplicant enters password and through the password a PSK is derived
    - note AP already has a PSK because AP knows its own password

2. AP sends to supplicant ANounce
3. Client uses ANounce and its own SNounce to generate PTK and MIC. SNounce and MIC is then sent to AP
4. AP uses the added SNounce information to generate the MIC and PTK and checks if the generated MIC matches the one that the client sent
5. If matches, the AP sends a key installation message to the supplicant and data transfer starts. Otherwise, the supplicant is deauthenticated.
6. Supplicant installs key and sends key acknowledgement to AP

Detecting Spoofing Attacks

SSID Spoofing

- when not spoofing the mac address, you can see multiple MAC addresses broadcasting the same SSID
    - not necessarily malicious, such as if a business has multiple access points with the same name, and would like to allow a client to roam around a building without having to manually reconnect to other APs
    - if the MAC address is not in a list of authorized MAC addresses, then it might be malicious (this only works if the attacker did not spoof the MAC address)
- could potentially be detected by monitoring the power usage of the real AP versus the potential rogue APs

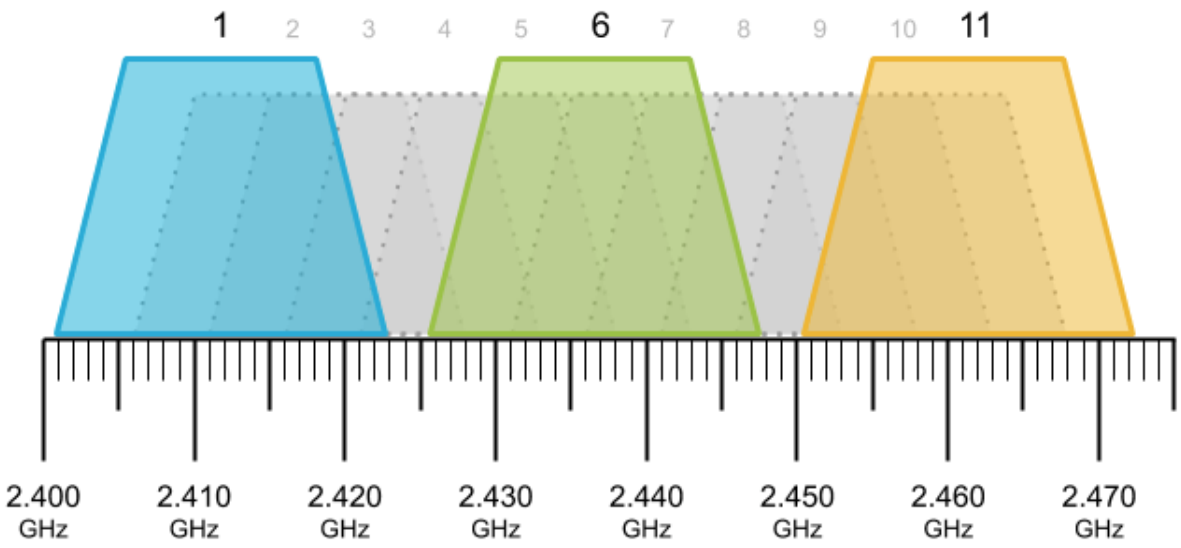
Mac Spoofing

- could still be detected if the length of beacon frames from the legitimate AP and illegitimate AP differ
    - the rogue AP will have the bare minimum information in the beacon frames, and will typically be less in length than the legitimate AP
- this could still in theory be bypassed by cloning the beacon frames, however there is no known tool (as far as I know) that does this

    - note that air*-ng does not perform this feature
- sequence numbers between the rogue and legitimate AP differ (typically by a lot e.g. rogue = 324 and counting while legitimate = 1235 and counting)

Wireless IDS and IPS

- the IDS and IPS detect when a client connects to an unauthorized AP, in which case it sends a deauth packet to the client to disconnect it
    1. This can be sort of circumvented by creating multiple rogue APs across multiple channels
    2. When the client gets disconnected from the rogue AP, it searches for another AP with the same ESSID, and automatically connects to it
- typically channels 1,6, and 11 are good channels to use as they do not overlap each other



Malicious SSID

HTML Injection and XSS

- insecure web consoles displaying SSID names could potentially be vulnerable to SSIDs with injected HTML code

SQLi

- an SQLi statement can be put as the ESSID to cause a monitoring device to reboot, or to delete all entries in a database