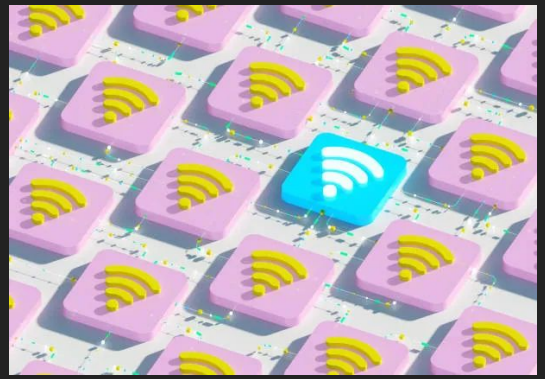
# CS 114: Wireless Security

**Ron Thompson - Spring 2024**
***Slides courtesy of Prof. Micah Sherr & Prof. Daniel Votipka***



Tufts UNIVERSITY | SCHOOL OF ENGINEERING Computer Science

Tufts Security & Privacy Lab

# Review

Dan will be doing a quick review of routing etc next class (Thursday)

# Quick intro for those who don't know me

PhD Candidate in Dan's lab focusing on security for  Medical Device & Industrial Control Systems

- How do we design secure systems?
- How do we evaluate and triage vulnerabilities?

Some relevant career highlights, spent ~10 years working before PhD:

- Cybersecurity Consultant for Medical Device Manufacturers
- CISA ICS Cybersecurity Certified - 301V & 301L
- Founded a startup that built tech for USASOC
- Ran security operations for a presidential campaign
- Defense contractor, built applications for the US Navy & US Army

Ron "zenw00kie" Thompson

# Wireless ≠ WiFi - Everything wants to connect

**Amateur Radio**

*Varies*

**Radio Telescopes**

*608 to 614 MHz*

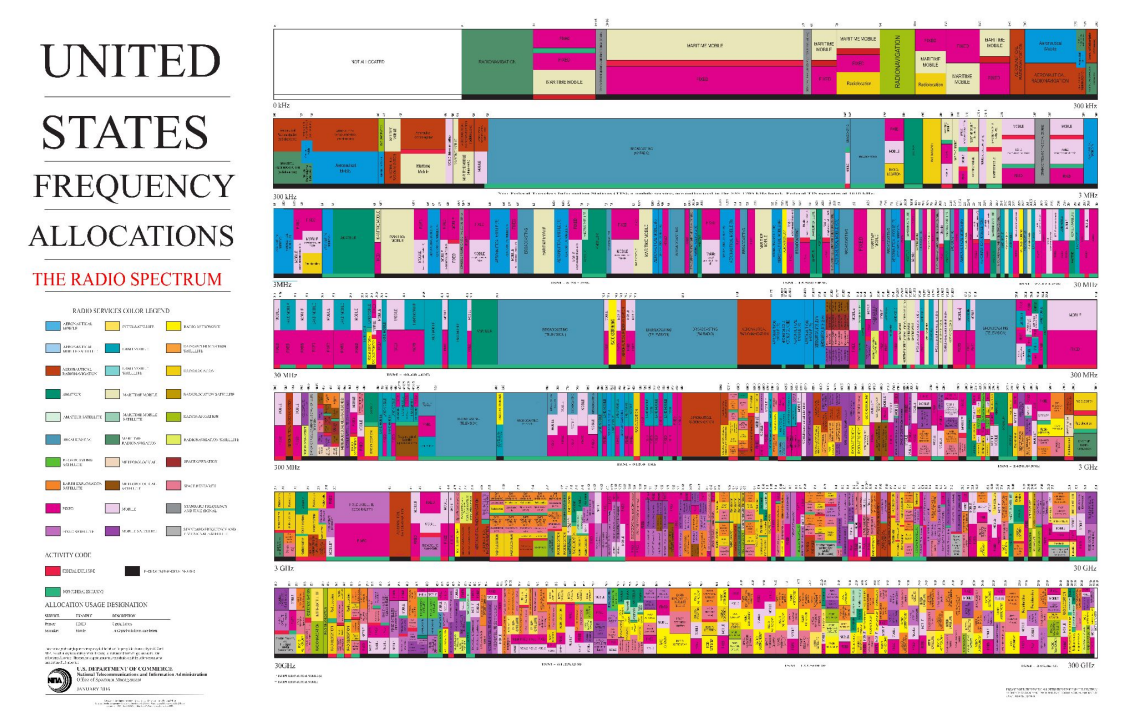
*same as some medical telemetry

**MBTA**

*470 MHz*

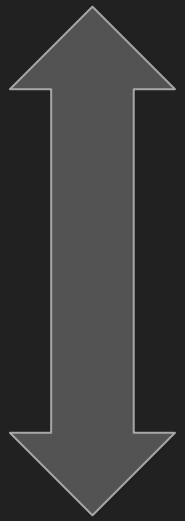
*from 2007 so may not be accurate anymore

# Networks, networks everywhere...



# Some common frequencies you might recognize

| Frequency | Devices |
|---|---|
| 108 - 330 MHz | Aviation, instrument landing systems, Air Training Command |
| 900 MHz | Cordless phones, wireless industrial controls |
| 2.4 GHz | WiFi Routers, Bluetooth, Zigbee, RC toys |
| 5.8 GHz | WiFi Routers, printers, cell phones |



Lower Frequency:
Less power, less data, less interference, more distance

Higher Frequency:
More power, more data, more crowded, less distance

# Connecting & Using Wireless Communications

- Access points (APs) may periodically broadcast *beacon frames* to advertise its presence (and some configuration parameters)
- Authentication:
  - client sends *authentication frame* to AP
  - if successful, client sends *association request frame* to AP, requesting allocation of resources
  - if successful, AP responds with *association response frame*
- Data sent via *data frames*
- Session Termination:
  - AP sends *disassociation frame* and *deauthentication frame*

# Interference is an opportunity for attackers

Wireless signals are subject to jamming

**Analog Jamming**: decrease signal-to-noise ratio by flooding with radio waves

- basic techniques easy to detect -- just listen for jamming signals
- more advanced techniques leverage features of the communication system (e.g., FM) to undetectably jam
- standard defenses: spread spectrum, channel hopping

**Digital Jamming**: exploit multiplexing scheme to consume all channel bandwidth

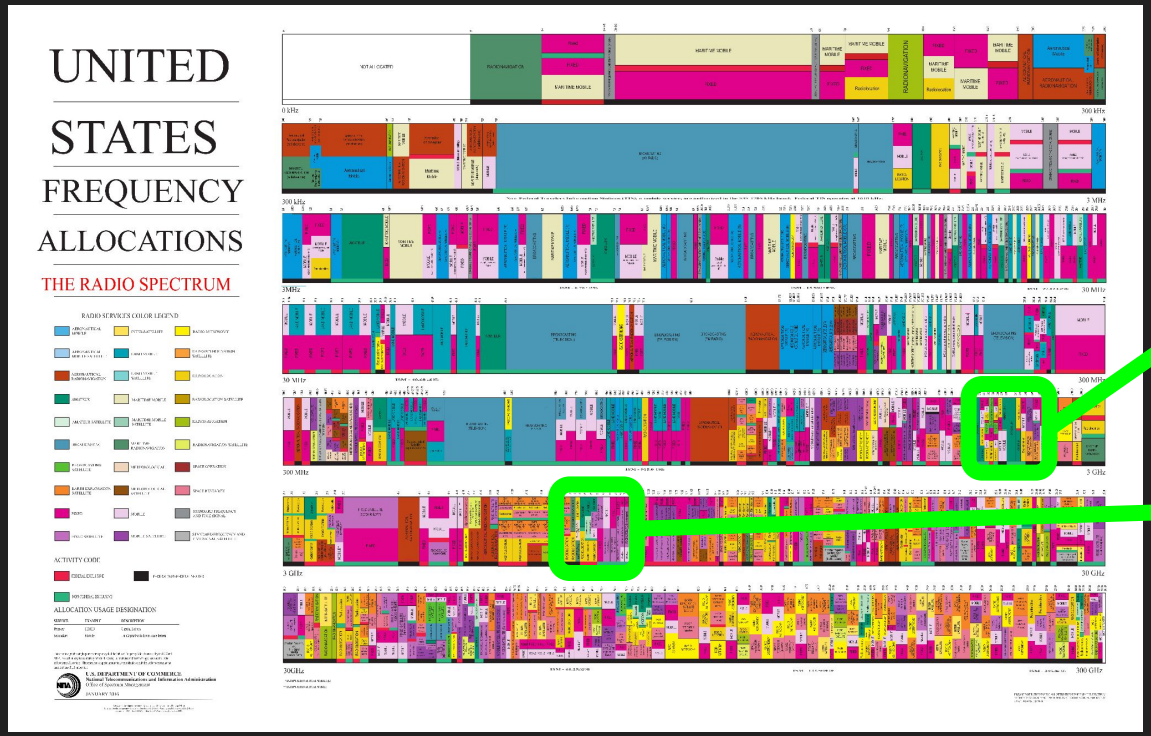
Natural crowdedness makes it easier to attacker to jam popular bands

# Even simpler attacks can also be done

With $30 of equipment, two teens were able to shut down more than 20 trains in 2023

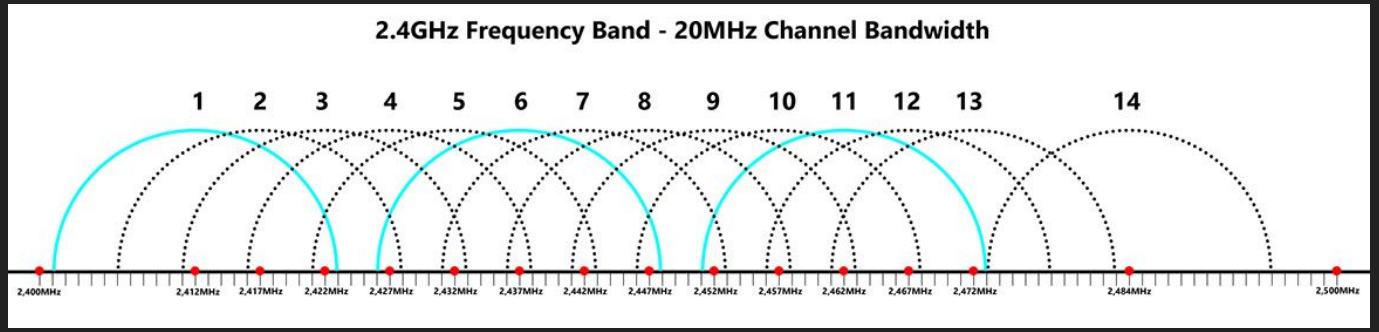
Simply by sending “stop” command on the frequency

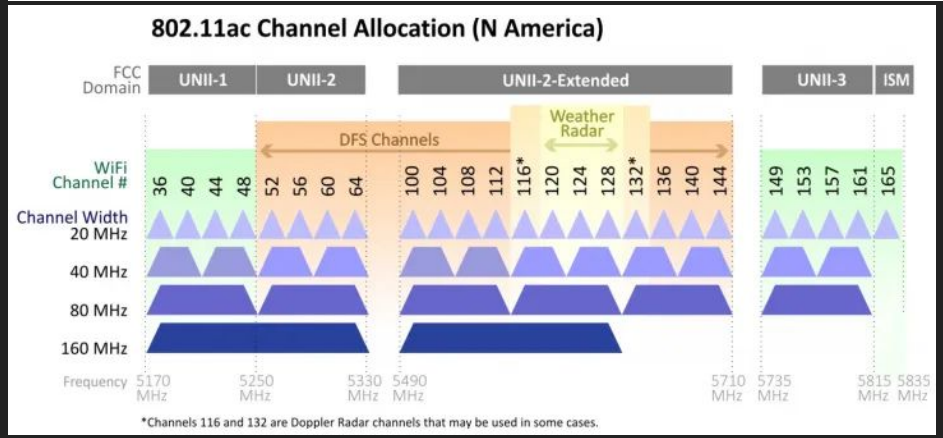
# focus on small part for this class





# We're focusing on protocols defined in IEEE 802.11



# Hey, can someone check their WiFi connection?

# Hey, can someone check their WiFi connection?

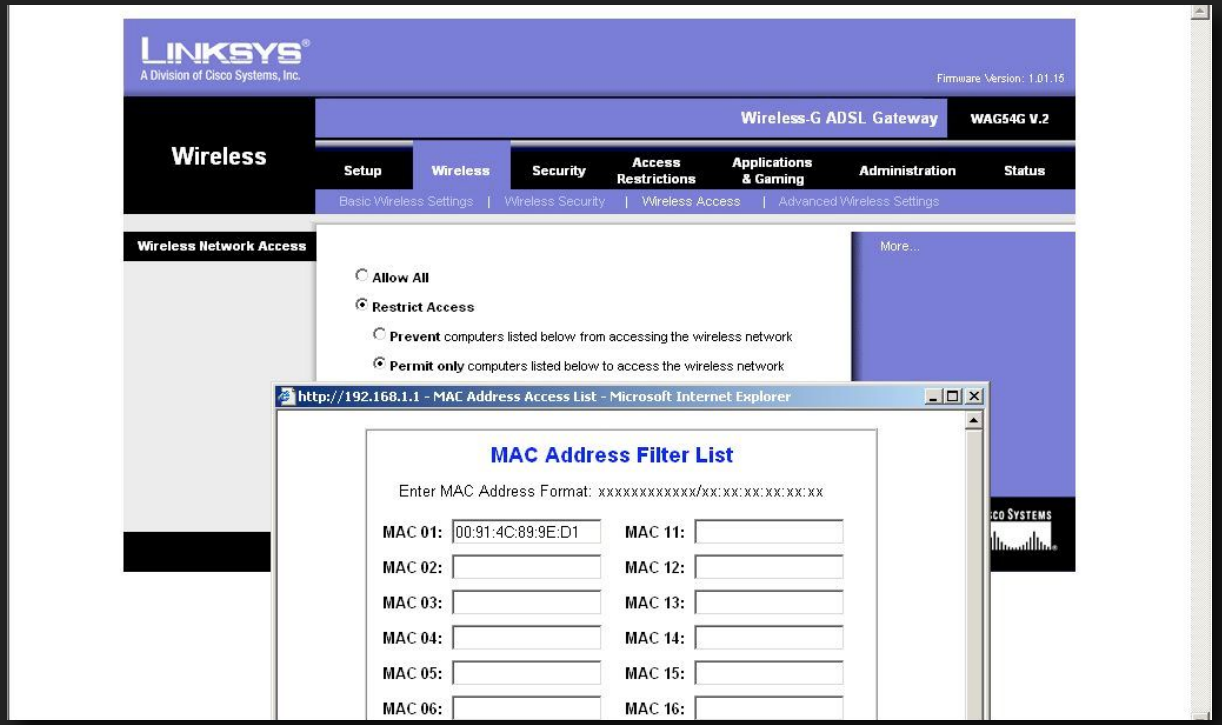
# You get a connection, you get a connection, everyone can connect

# All it takes is one coffee machine...

In 2017 a smart coffee maker was inadvertently added to an internal control network at a German petrochemical plant...

only figured out because coffee maker displayed same ransom message as the workstations.

# Hey you’re not on the list



# Well we can change our MAC address


MAC address of your choosing

sudo ifconfig eth0 hw ether 00:12:34:56:78

# evil twin [man-in-the-middle]

attacker can create a rogue AP that calls itself tufts_eecs

all Eve has to do is have a stronger signal than the AP she's trying to hijack...in fact I think she's trying to do that right now

*in a proper attack, we would connect our rogue AP in repeater mode and piggy back on the real network

Q: What are some places you think this is more readily done?

# evil twin and more out of the box - wifi pineapple

specific product from Hak5 that makes setup v easy



hooli

# hide yo ssid!

- APs broadcast **Service Set Identifiers (SSIDs)** to announce their presence
- In theory, these should identify a particular wireless LAN
- In practice, SSID can be anything that's 2-32 octets long
- To join network, client must present SSID
- Security mechanism for preventing interlopers:
  - Don't advertise SSID
  - Problem:
    - To join network, client must present SSID
    - This is not encrypted, even if network supports WEP or WPA

# Demo time!

# probing

used for reconnaissance (as a way to setup evil twin for instance)

when device isn't connected to a network but WiFi is still on it will send out probes looking for networks it already knows (can do this with other protocols as well such as Bluetooth)

did we see this during airodump?

# Taking this type of network scanning on the road

wardriving! (or warbiking for the more eco-inclined)

- what networks are broadcasting?
- can be done with other protocols such as bluetooth
  - a collaborator found that one of the most common devices sending BLE beacons in San Diego were CPAP machines [Givehchian et al. Evaluating Physical-Layer BLE Location Tracking Attacks on Mobile Devices]
- WiGLE.net shows maps of found networks

# Time to bolt on security...again

# Wired Equivalent Privacy (WEP)

- Part of original 802.11 standard
- Uses stream cipher:
  - WEP uses RC4 - supports seed up to 256 bits
    - seed = 24-bit IV + WEP key

- In WEPv1, key was 40 bits ➡ 64bit seed
- Later versions supported seeds of 128 and 256 bits

Problem: I can see everyone's communications

# Wired Equivalent Privacy (WEP)

Generate keystream (S) using RC4 with seed of IV and Key

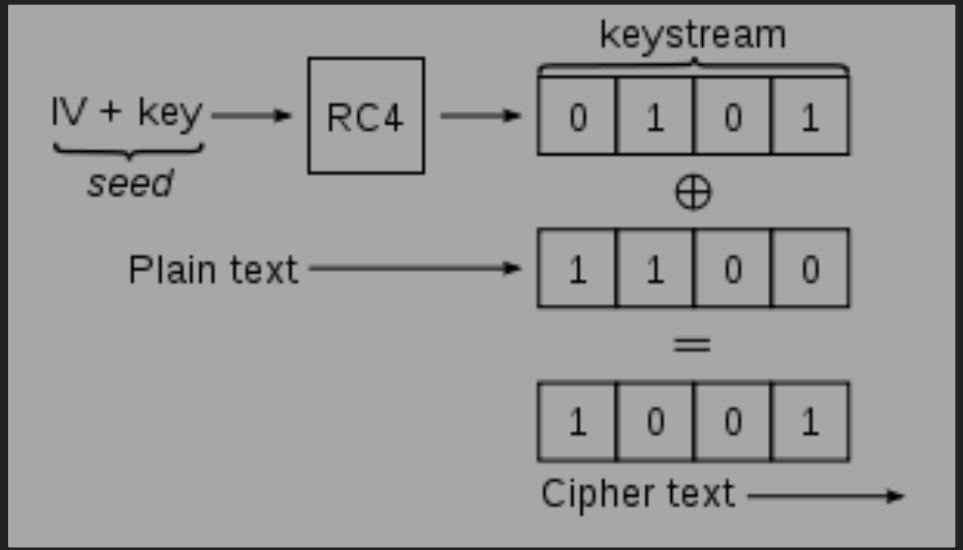
S = f(IV,K)

Keystream is then XOR'ed with plain text message to produce cipher text

C = M ⊕ S

Send IV and C frames

Only IV and Key are needed to decrypt



# WEP Authentication Modes

- Open System:
  - client doesn't need to provide any credentials
  - immediate association with access point
  - but can only send and receive info if using correct key

- Shared Key:
  - client must prove knowledge of  WEP key before associating
  - AP sends client plaintext challenge; response is challenge encrypted with the correct key

- Q:  Which is more secure?

# WEP Shared Key Vulnerability

Random Challenge: “jk4533hfdsa9”
Response: {IV, “jk4533hfdsa9” ⊕ RC4(K,IV)}
here, RC4(K,IV) denotes RC4 encryption using a key derived from key K and IV

Eavesdropper can observe plaintext challenge and encrypted response, and can produce:
challenge ⊕ response = RC4(K,IV)
RC4(K,IV) sufficient to authenticate:
next challenge: “abcdef”
Eve responds (without knowing K!): {IV, “abcdef” ⊕ RC4(K,IV)}

# I got 99 problems, and IV Collisions are one

IVs are too small… likely collision(s) after a few hours

- when IVs are the same, $C_1 \oplus C_2 = M_1 \oplus M_2$
  - statistical analysis will then yield plaintexts
  - redundancy in IP packets makes this easy!
  - knowledge of protocols further limits the possibilities
  - or, attacker sends message thru Internet to a wireless client in a manner that will result a known response (e.g., ping message)

- if multiple messages share same IV, once one is recovered, others can be trivially/immediately recovered --**WHY**?

# Oh yeah, and RC4 also has weaknesses

- RC4 has a weakness:  first few bytes of keystream are sometimes not particularly random looking [Fluhrer, Mantin and Shamir Attack; 2001]
- Mathematical result:  Given enough keystreams, it's possible to construct the key  [ciphertext-only attack]
- Attacker's goal:  Get a lot of keystreams!
  - Basic approach:  replay a bunch of ARP packets
  - AP will respond to replayed ARP
  - Sufficient number of AP's encrypted packets will yield key
- Standard RC4 fix:  discard first n bytes of keystream (usually n ≥ 3072)

# All you need is a little bit of patience

- TJX (TJMaxx + Marshalls + Bob's) main database compromised in 2007
  - ~94M credit and debit cards stolen
- Scanning devices, cash registers, and PCs in Minnesota Marshalls wirelessly communicated to server, which communicated to backend database
- Wireless data encrypted using WEP
- WEP key stolen from a parking lot.  Uh-oh.

- **Lesson:  Don't use WEP!**

# Wi-Fi Protected Access (WPA)

- Engineered to be the “secure replacement” for WEP
- Authentication stages:
  - Shared secret used to derive encryption keys
  - Client authenticates to AP
  - Encryption keys are used to produce keystreams for encrypting traffic

Two Modes:

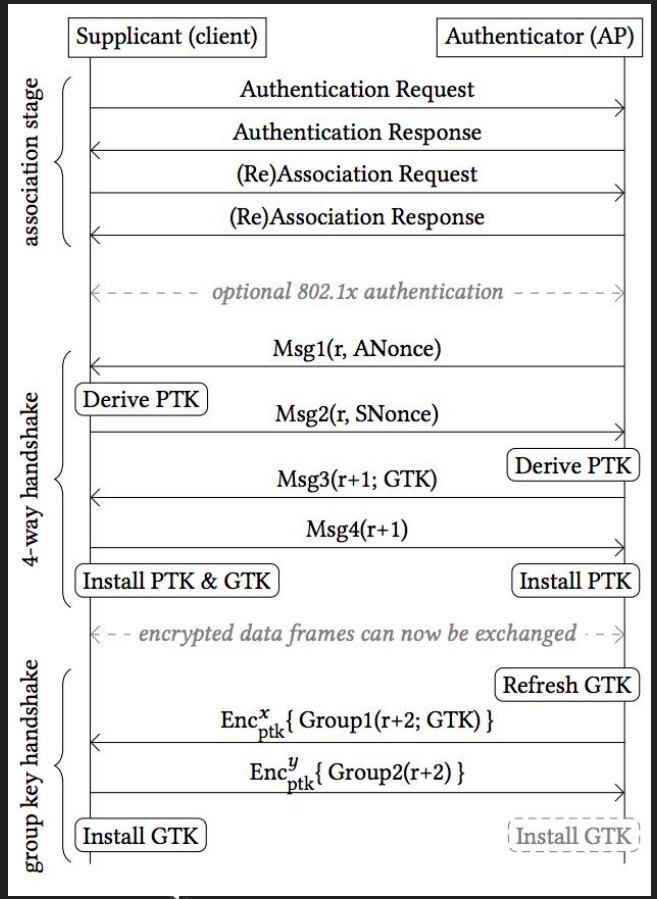
- PSK (Pre-shared Key) - “WPA Personal”
  - shared secret manually entered into all devices
  - designed for home use
  - e.g. tufts_eecs
- 802.1x Mode - “WPA Enterprise”
  - authentication handled by backend service (e.g., RADIUS server) via Extensible Authentication Protocol (EAP)
  - may make use of certificates
  - e.g., Tufts_Secure

# Wi-Fi Protected Access (WPA)

Both sides also compute a Pairwise Transit Key (PTK) using a Pre-Shared Key (PSK)

PTK = f(PSK, ANonce, SNonce, AP MAC address, Client MAC address)

PSK is the WiFi password for WPA Personal, whereas it's handled by EAP exchange for WPA Enterprise



# Wi-Fi Protected Access (WPA) - Encrypting Traffic

Temporal Key Integrity Protocol (TKIP):

- uses RC4, but designed to improve upon WEP's shortcomings
- increases size of IV to 48 bits
- rather than just concatenate IV, uses more complex key mixing routine

AES:

- supported in newer WPA2 protocol
- runs AES in stream-cipher like way (e.g., using something similar to counter mode)

# Attacks on WPA

- WPA is a lot stronger than WEP
- Most attacks rely on weak passwords
  - user-supplied keys are either entered as 256-bit string (64 hex digits) or as password
  - password is hashed to produce key using 4096 iterations of HMAC-SHA1 with SSID of AP as salt
  - there exists dictionaries of pre-hashed keys for most popular SSIDs (“linksys”, “yankeessuck”, etc.)

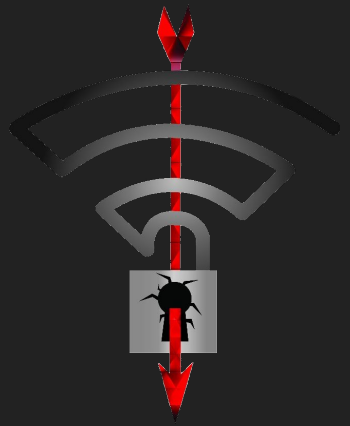
# Some other attacks - deauth

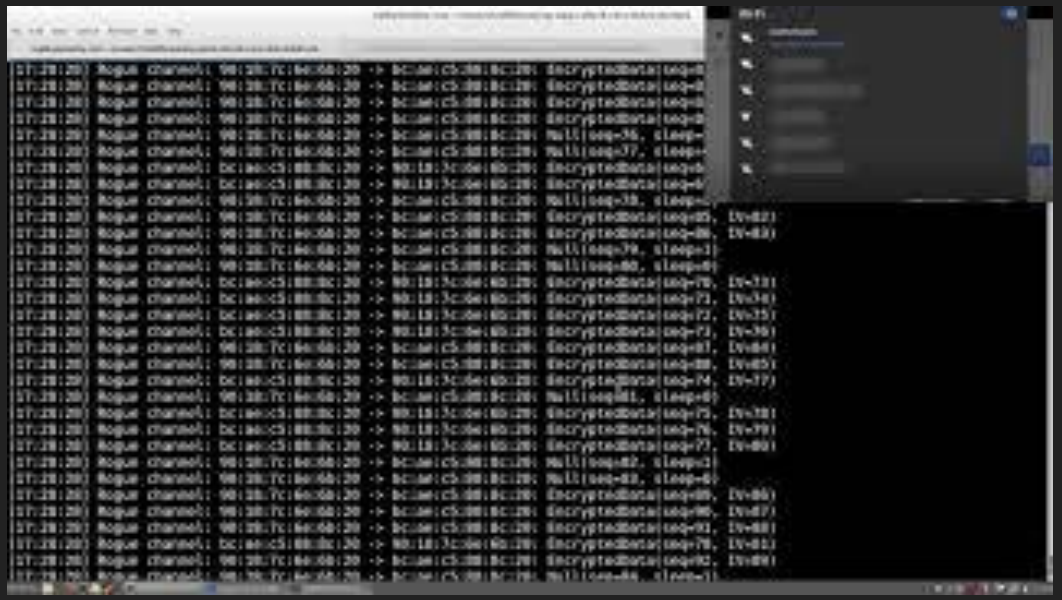
affects availability by sending a deauthentication packet for a spoofed MAC address, cutting access for that user

can multiply affects by finding all MAC addresses on network and sending deauth for all of them

# Some other attacks - KRACK

krackattacks.com - found by researchers at KU Leuven in 2017





# time permitting - look how easy it is!



lots of tools make it very easy to do these attacks

**WORD OF WARNING** only do this on networks you control/have explicit permission to test on - some attacks can also spillover and have unintended consequences, so be wise

**especially true if you are looking at other parts of the radio spectrum**


# Summary

Wireless basics

Attacks

- Eavesdropping
- Wardriving (and others)
- KRACK
- Jamming

Defenses

- Configuration-based: MAC filtering, SSID hiding
- Crypto-based: WEP, WPA2