RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: SBX3-W1

Hunting and Tracking Rogue Radio Frequency Devices

Eric Escobar

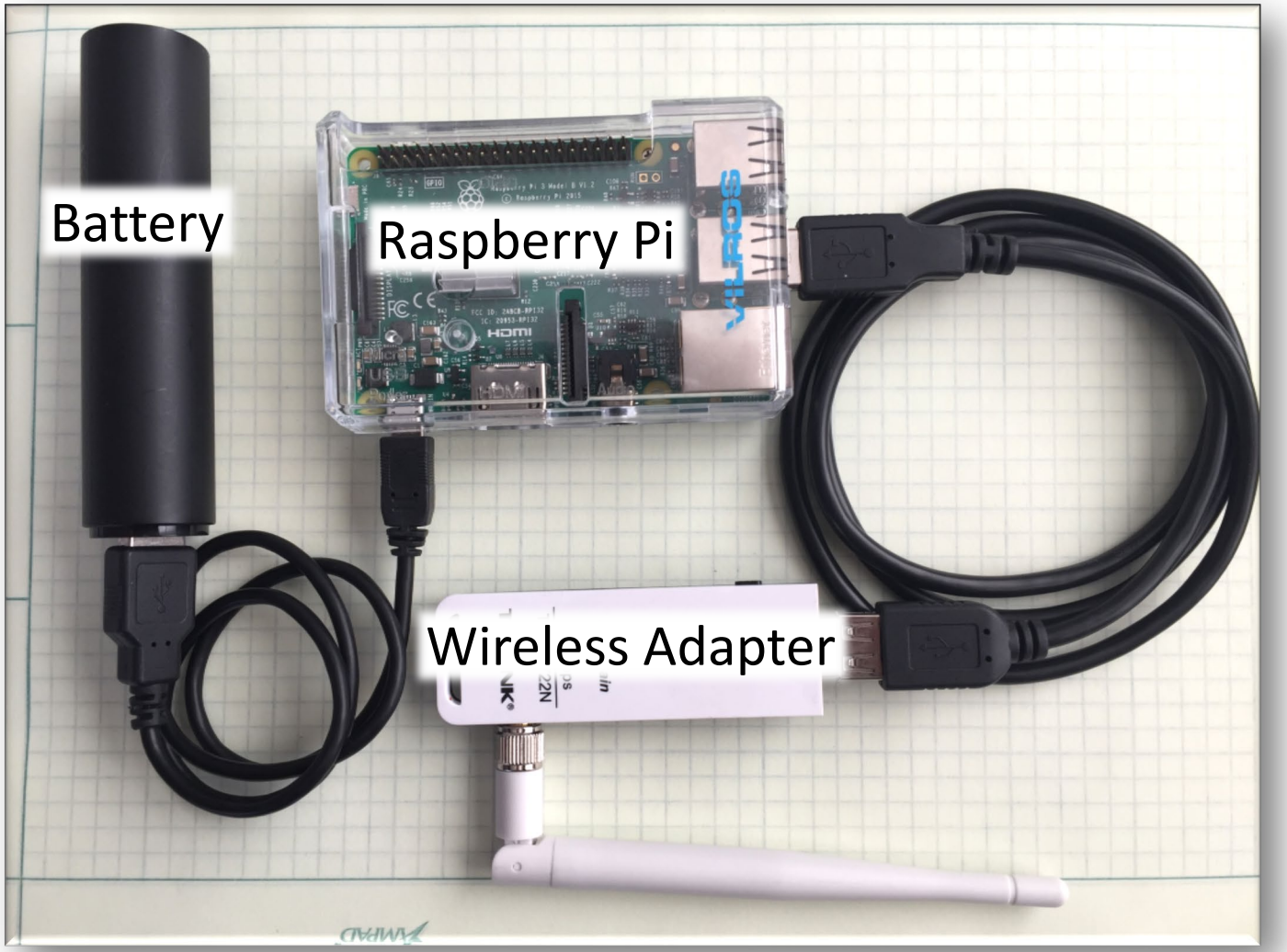
Principal Security Consultant
Secureworks
@EricEscobar

Story Time

- An employee cafeteria
- $60 in hardware from Amazon
- A Hacker & 10 years of R&D stolen

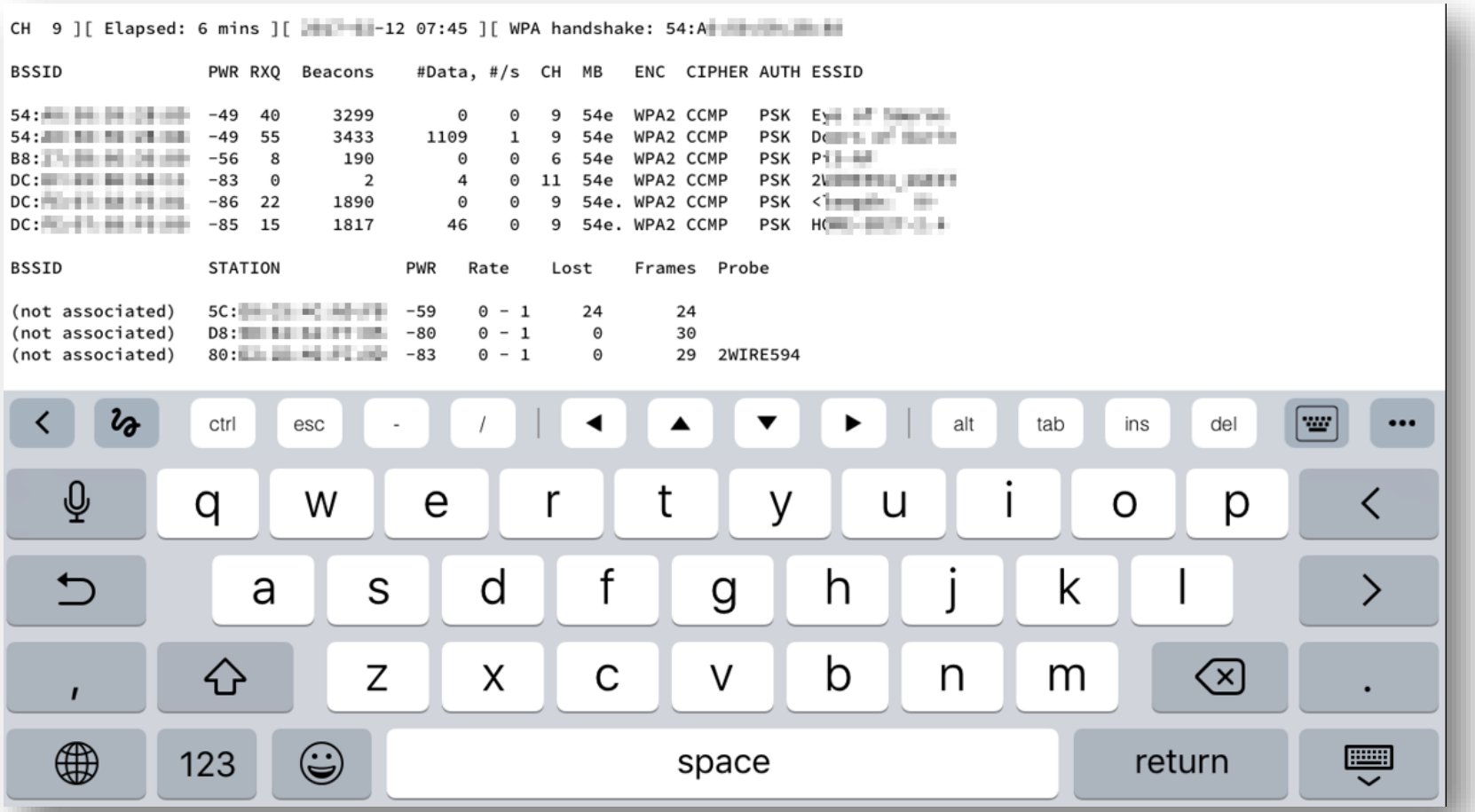
Story Time

The build.



Story Time

You can do everything from a phone.



RSAConference2019

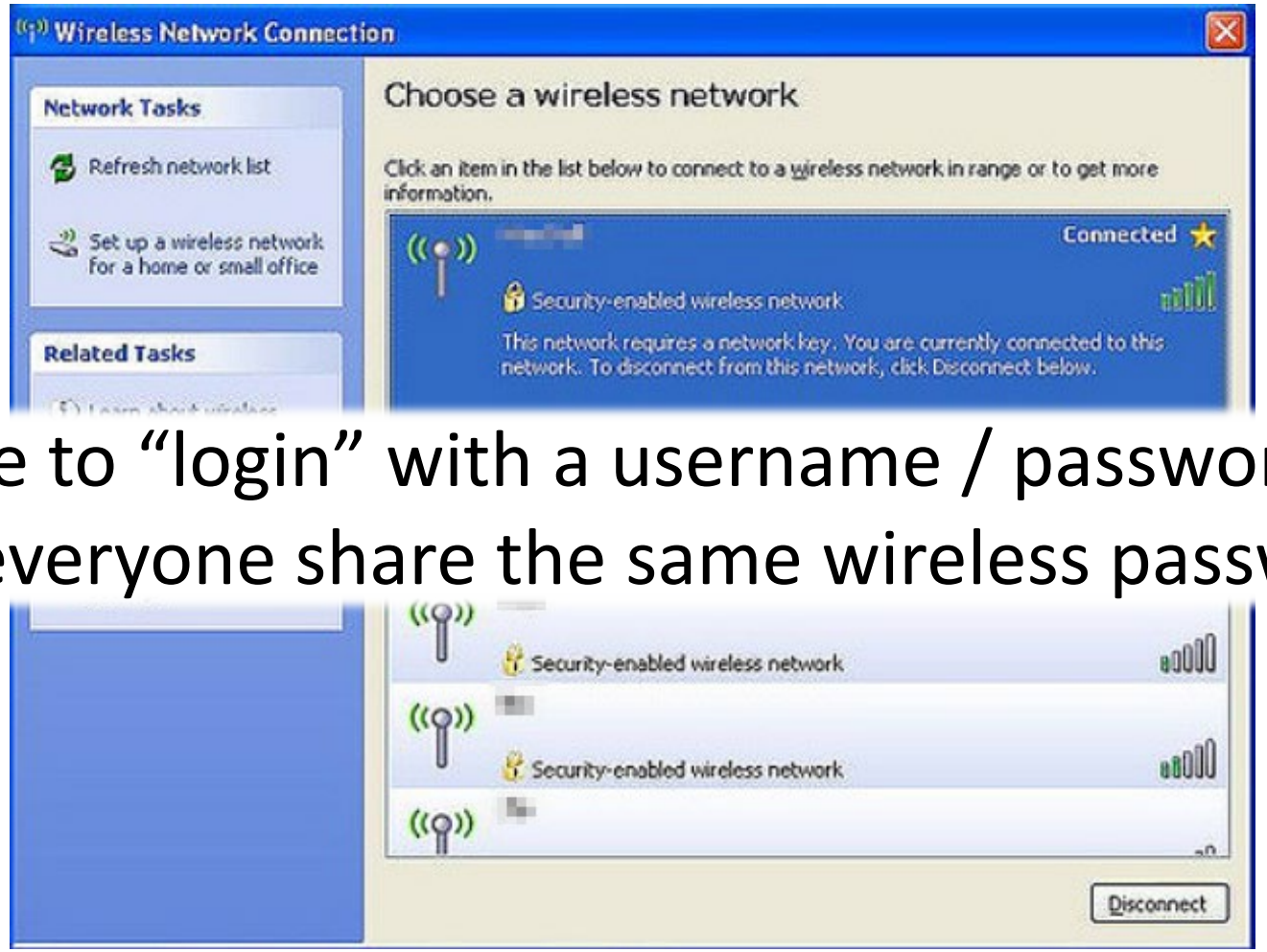
Questions to ask yourself…

(Because attackers already are)

Questions to ask yourself…

Does your company allow BYOD (Bring your own device)?

Questions to ask yourself…



Do you have to “login” with a username / password for WiFi?

Does everyone share the same wireless password?

Questions to ask yourself…

Is “Guest” WiFi on a separate network?

Questions to ask yourself…

Does anyone connect to the bootleg WiFi?

RSAConference2019

Why are Wireless Attacks attractive to an attacker?

Benefits of wireless attacks

- Typically no internal access is necessary.
- Easier to stay anonymous.
- Attackers can stay out of sight.

RSAConference2019

An Overview of Wireless Attacks

Real Life Examples of common RF attacks

A brief outline:

- Wireless Phishing
- Collecting device metadata
- Tracking a person or object
- Jamming alarms
- Opening Gates & Doors
- Wireless medical devices anyone?

Rogue Access Points

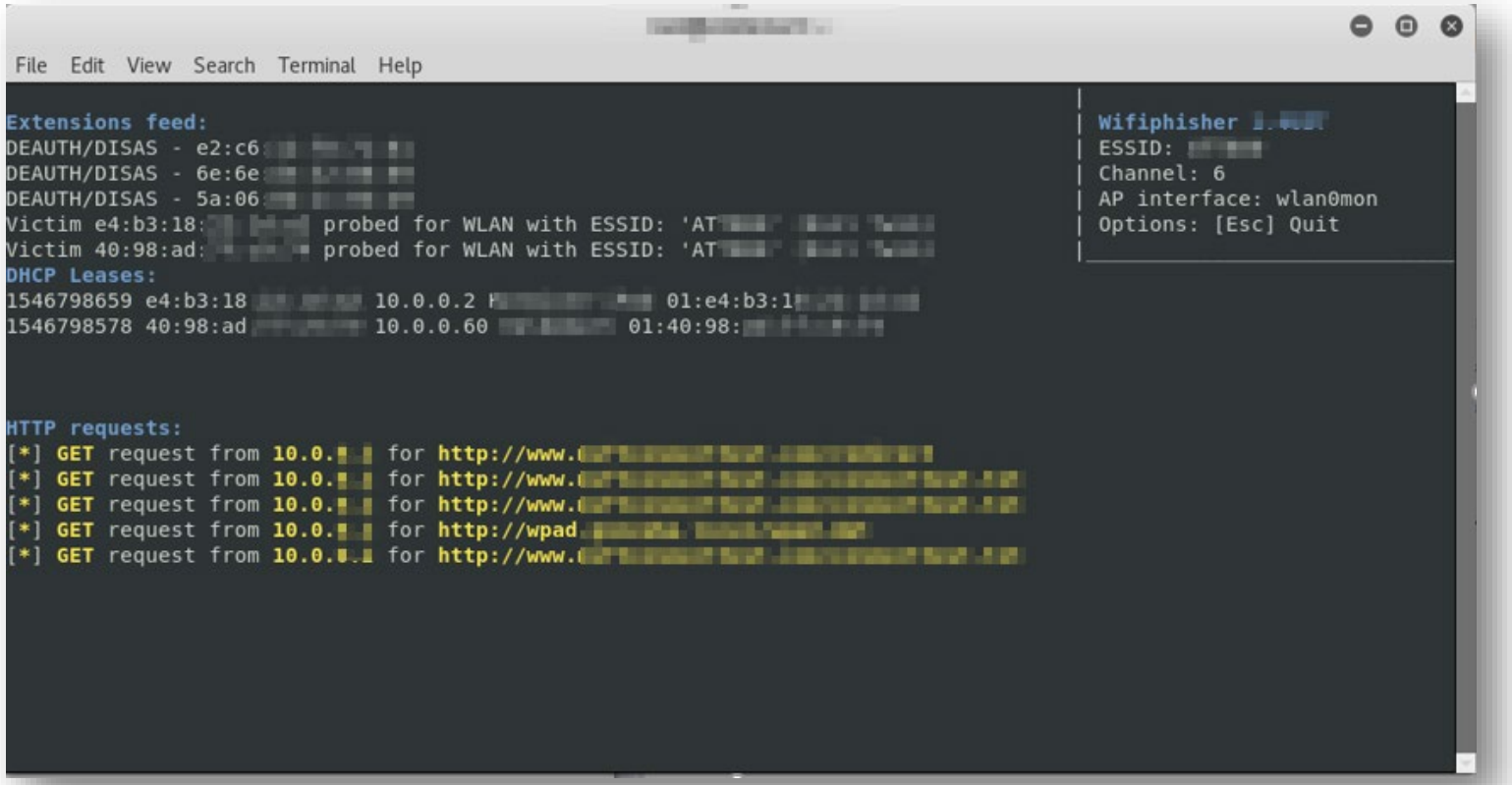
What is a Rogue Access Point (AP)?

- A wireless access point not within your control
- Technically any phone or hotspot could be a Rogue AP

Let’s see what a dangerous Rogue AP can do…

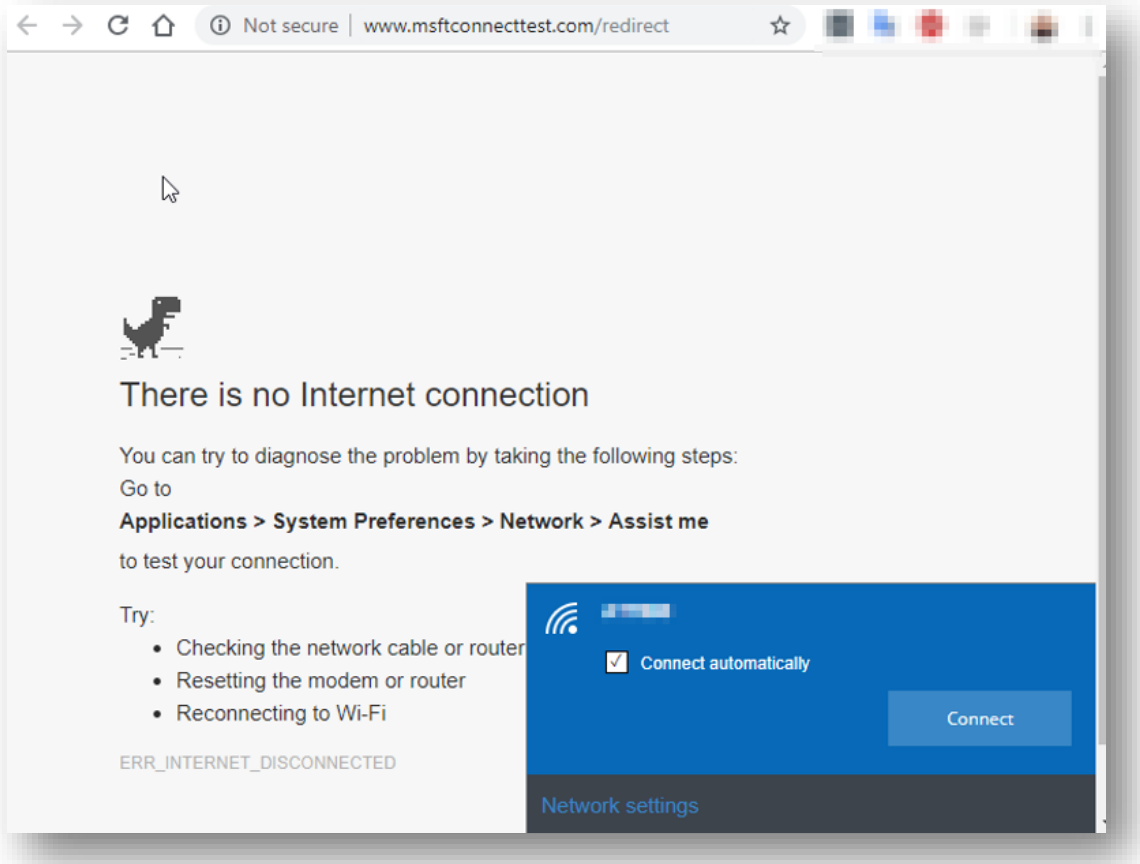
User Impersonation & Wireless Phishing

Rogue access points can create an unsuspecting trap.



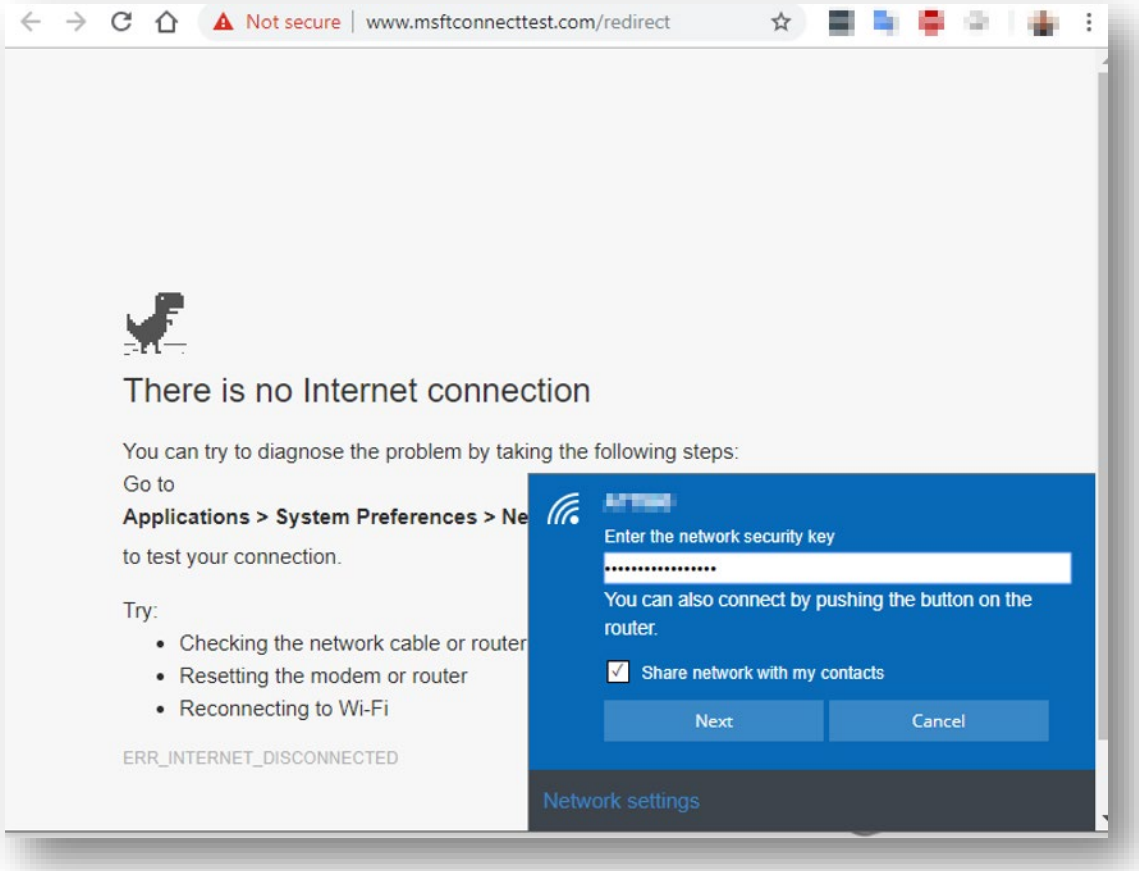
User Impersonation & Wireless Phishing

The fake login can trick users.



User Impersonation & Wireless Phishing

The fake login can trick users.



User Impersonation & Wireless Phishing

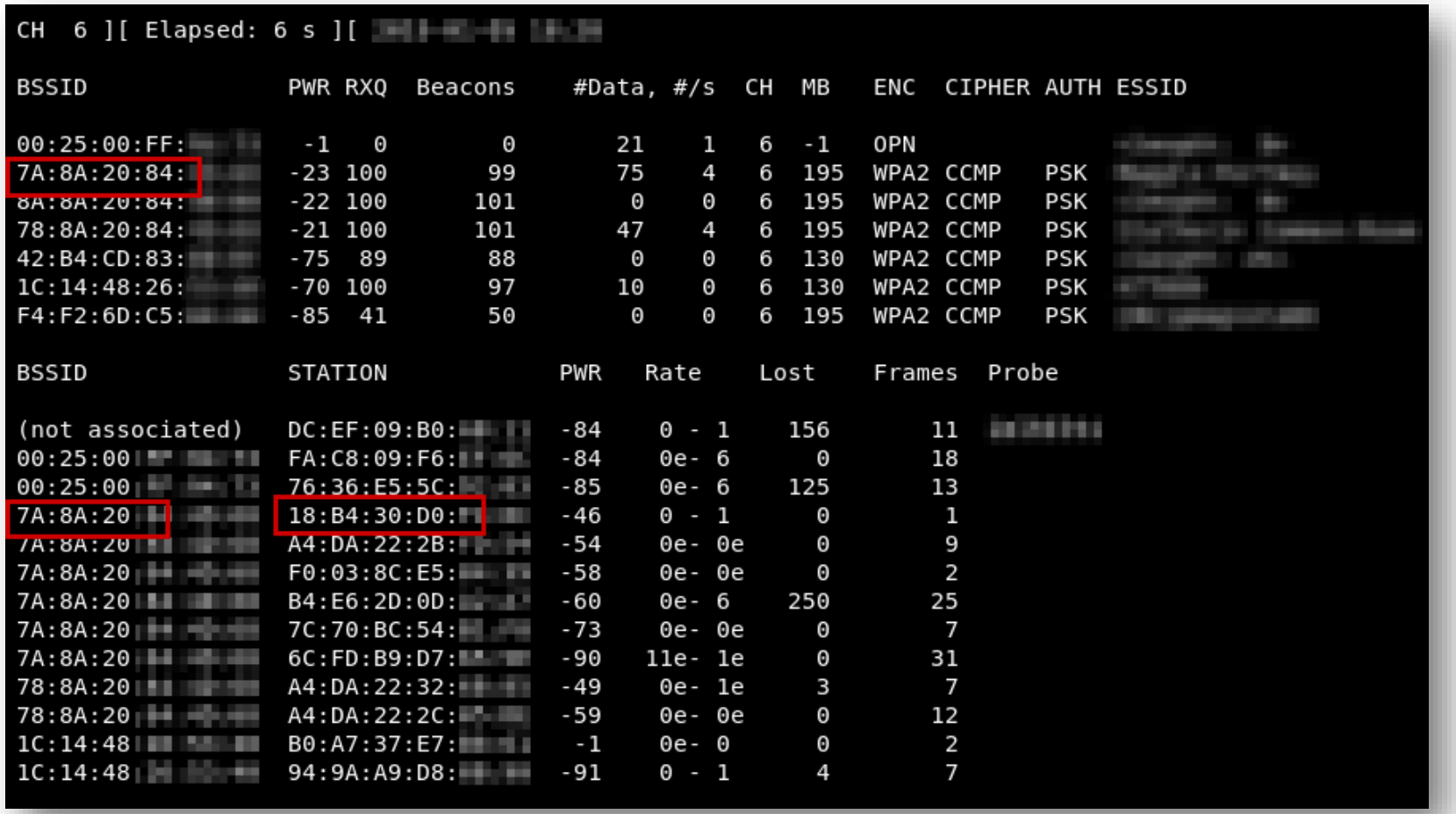
Rogue Access Points:

- Can lead to stolen credentials.
- Compromised workstations.
- Can exfiltrate data.
- Can allow users to circumvent corporate policies.

Attackers gather lots of Data

- Wireless devices emit tons of useful information.
- WiFi devices can allow for:
  - Users to be tracked.
  - Identification of device type.
  - Connected networks.
- Let's take a look at the output from the tool "Airodump-ng"

Collecting Device and User Metadata



```
CH  6 ][ Elapsed: 6 s ][ [redacted]

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:25:00:FF:[redacted]  -1   0        0       21    1   6  -1   OPN              [redacted]
7A:8A:20:84:[redacted]  -23 100       99       75    4   6  195  WPA2 CCMP   PSK  [redacted]
8A:8A:20:84:[redacted]  -22 100      101        0    0   6  195  WPA2 CCMP   PSK  [redacted]
78:8A:20:84:[redacted]  -21 100      101       47    4   6  195  WPA2 CCMP   PSK  [redacted]
42:B4:CD:83:[redacted]  -75  89       88        0    0   6  130  WPA2 CCMP   PSK  [redacted]
1C:14:48:26:[redacted]  -70 100       97       10    0   6  130  WPA2 CCMP   PSK  [redacted]
F4:F2:6D:C5:[redacted]  -85  41       50        0    0   6  195  WPA2 CCMP   PSK  [redacted]

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   DC:EF:09:B0:[redacted]  -84    0 - 1    156        11  [redacted]
00:25:00[redacted] FA:C8:09:F6:[redacted]  -84    0e- 6      0        18
00:25:00[redacted] 76:36:E5:5C:[redacted]  -85    0e- 6    125        13
7A:8A:20[redacted] 18:B4:30:D0:[redacted]  -46    0 - 1      0         1
7A:8A:20[redacted] A4:DA:22:2B:[redacted]  -54    0e- 0e     0         9
7A:8A:20[redacted] F0:03:8C:E5:[redacted]  -58    0e- 0e     0         2
7A:8A:20[redacted] B4:E6:2D:0D:[redacted]  -60    0e- 6    250        25
7A:8A:20[redacted] 7C:70:BC:54:[redacted]  -73    0e- 0e     0         7
7A:8A:20[redacted] 6C:FD:B9:D7:[redacted]  -90   11e- 1e     0        31
78:8A:20[redacted] A4:DA:22:32:[redacted]  -49    0e- 1e     3         7
78:8A:20[redacted] A4:DA:22:2C:[redacted]  -59    0e- 0e     0        12
1C:14:48[redacted] B0:A7:37:E7:[redacted]   -1    0e- 0      0         2
1C:14:48[redacted] 94:9A:A9:D8:[redacted]  -91    0 - 1      4         7
```

Collecting Device and User Metadata

- A quick search shows us a known Mac Address fragment.
- Attackers can use this to enumerate connected devices.

Results for MAC address 18:B4:30

Found 1 results.

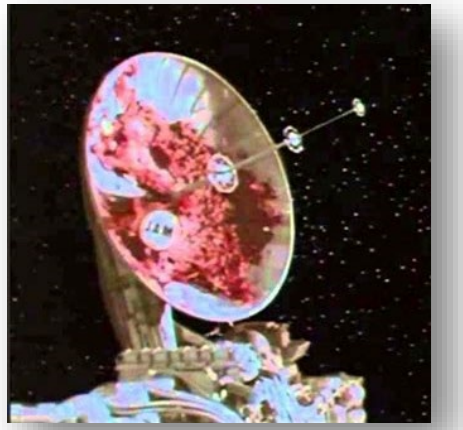
MAC Address/OUI	Vendor {Company}
18:B4:30	Nest Labs Inc.

Tracking People and Devices

- Wireless devices emit power level:
  - Can be used to track devices via trilateration.
  - “Blue Sonar” can track almost all Bluetooth devices.

Wireless Attacks extend past WiFi

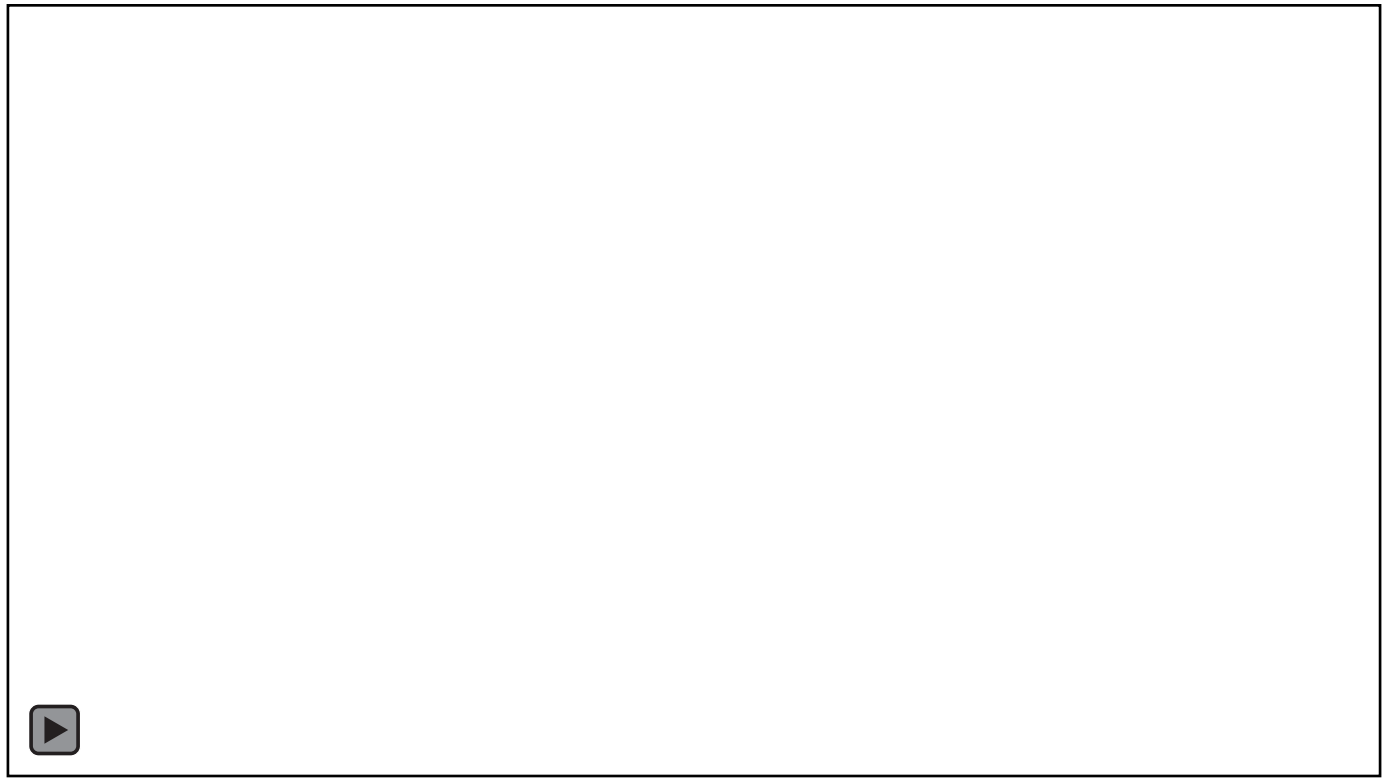
- Wireless attacks can extend to anything in the RF spectrum.
- Replay attacks:
  - A common vulnerability in many wireless devices
  - Allows for an attacker to resend a signal previously sent.



- Jamming:
  - Creates noise so a receiving station can’t make out a signal.
  - Effective at blocking communication.

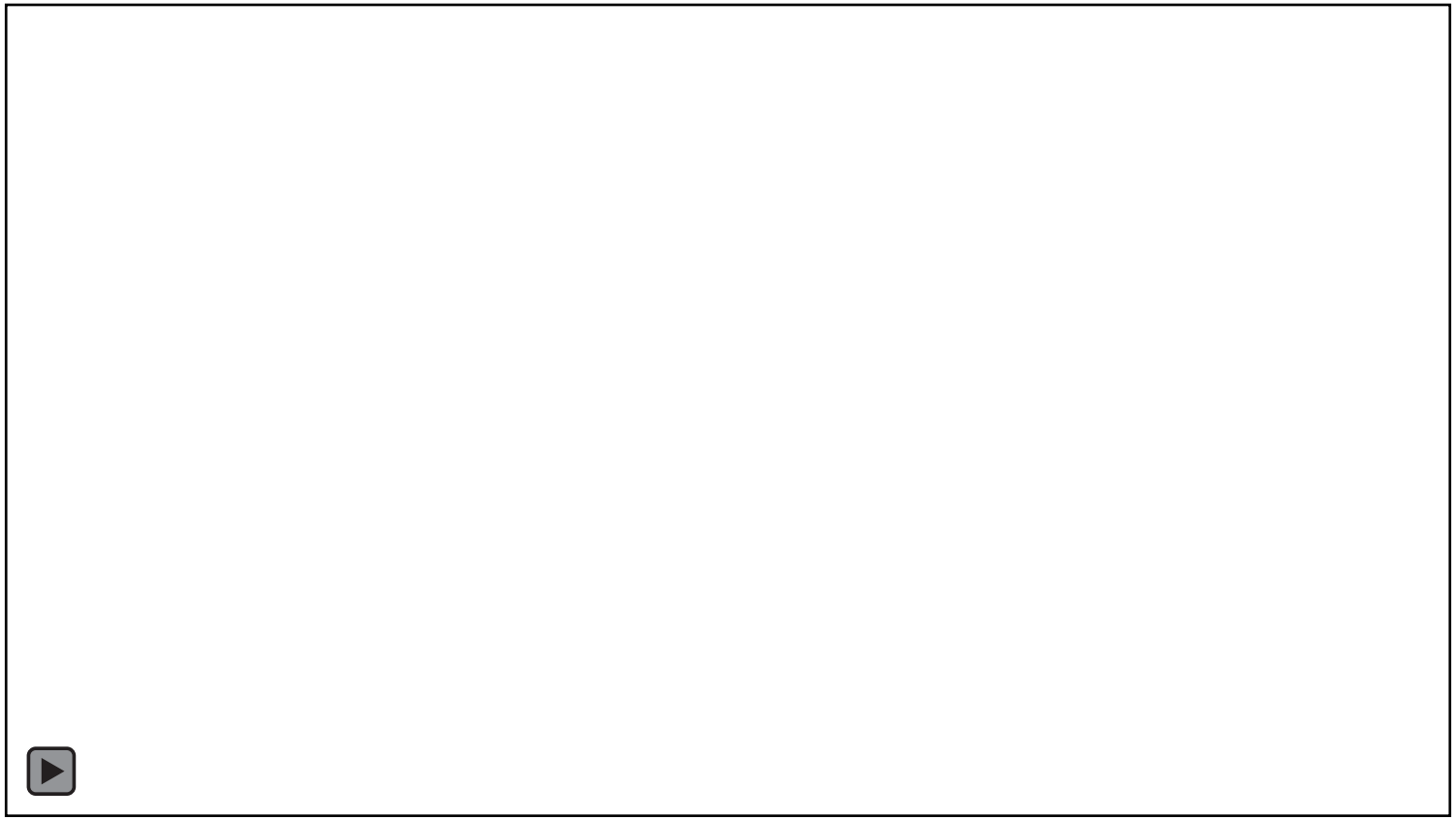
Opening Gates & Doors

- Replay attacks can be used to open secure gates.



Jamming Attacks

- Wireless noise can block transmissions.



Detecting and Locating

- So we've seen wireless attacks in action.
  - Now what?

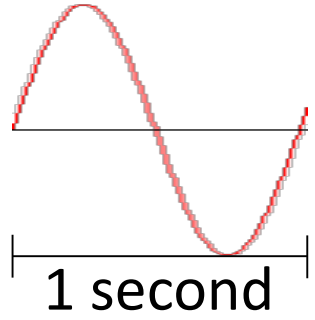
- Let's dig into Radio Frequencies (RF)
  - To detect and locate we need to know properties of radio signals.

RSAConference2019

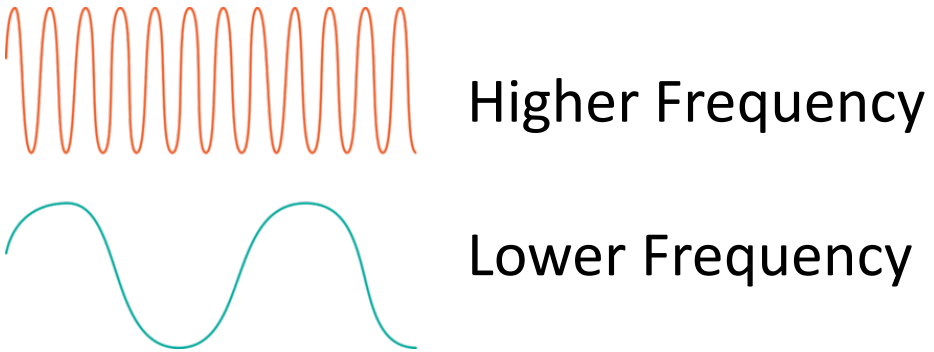
Radio Frequencies - 101

How do we measure Radio Frequencies?

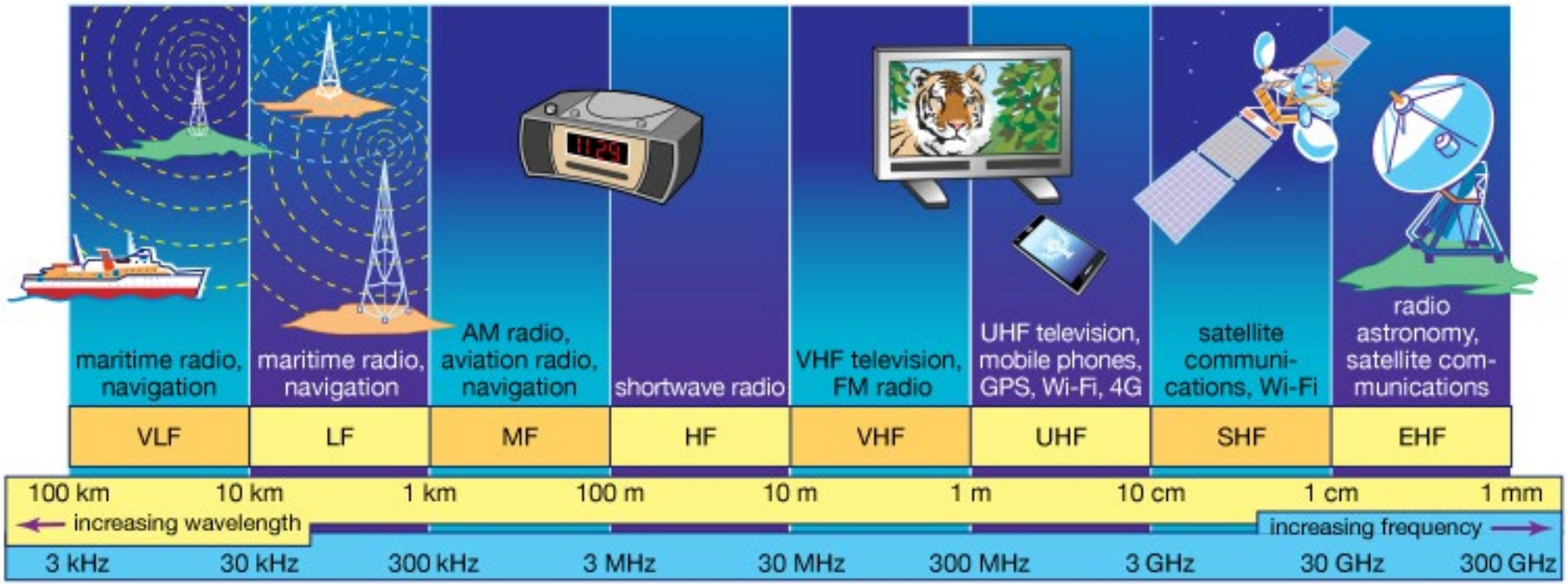
- Frequency Ranges
  - Measured in Hertz (one cycle / second)



  - Higher Frequency == More cycles / second
    - Wifi – 2.4Ghz (2.4 billion cycles/ sec)



Example Radio Frequencies



Radio Wave Propagation & Penetration

- Low frequencies can “diffract” signals
  - Allows signals to bend around objects
- Very low frequencies and penetrate deeper into objects
  - Typically means they can travel farther
- Medium wave (shortwave) frequencies can “refract” off the atmosphere
  - Allows signals to bounce around the globe
- High frequencies typically get absorbed quickly

Okay nerd, so what?

- Different radio frequencies have different capabilities.
  - Some frequencies can transmit lots of data at short distances.
  - Some can transmit a little data very long distances.
- Attackers can leverage properties of different frequencies to…
  - Exfiltrate data
  - Track a person or object
  - Eavesdrop on communications

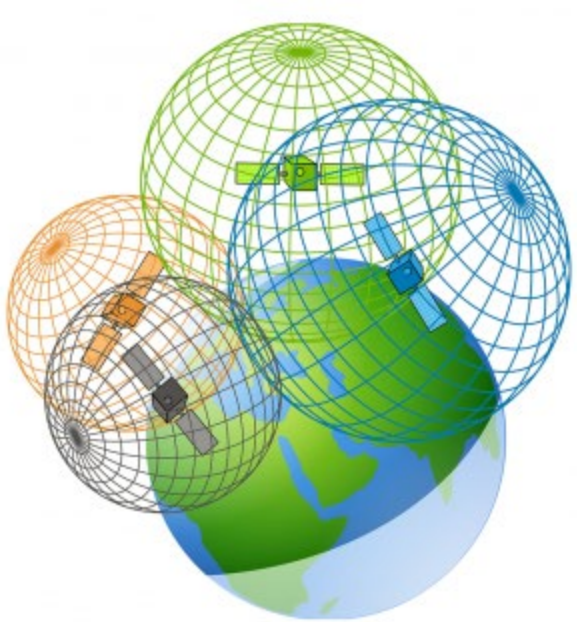
RSAConference2019

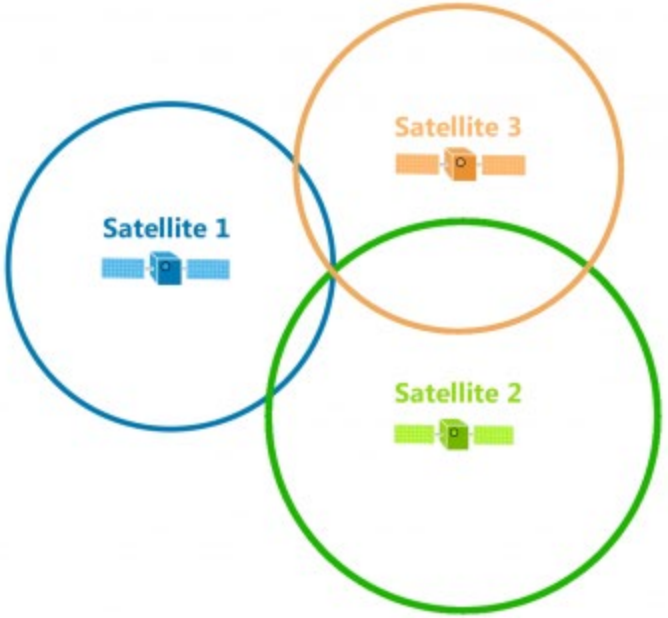
Just a little bit more Math & Science

Triangulation vs Trilateration

Triangulation vs Trilateration

- Most people mean trilateration when they say “triangulation”
  - I’ll quickly cover the differences with a story
- Trilateration uses distance.
- Triangulation uses angles.

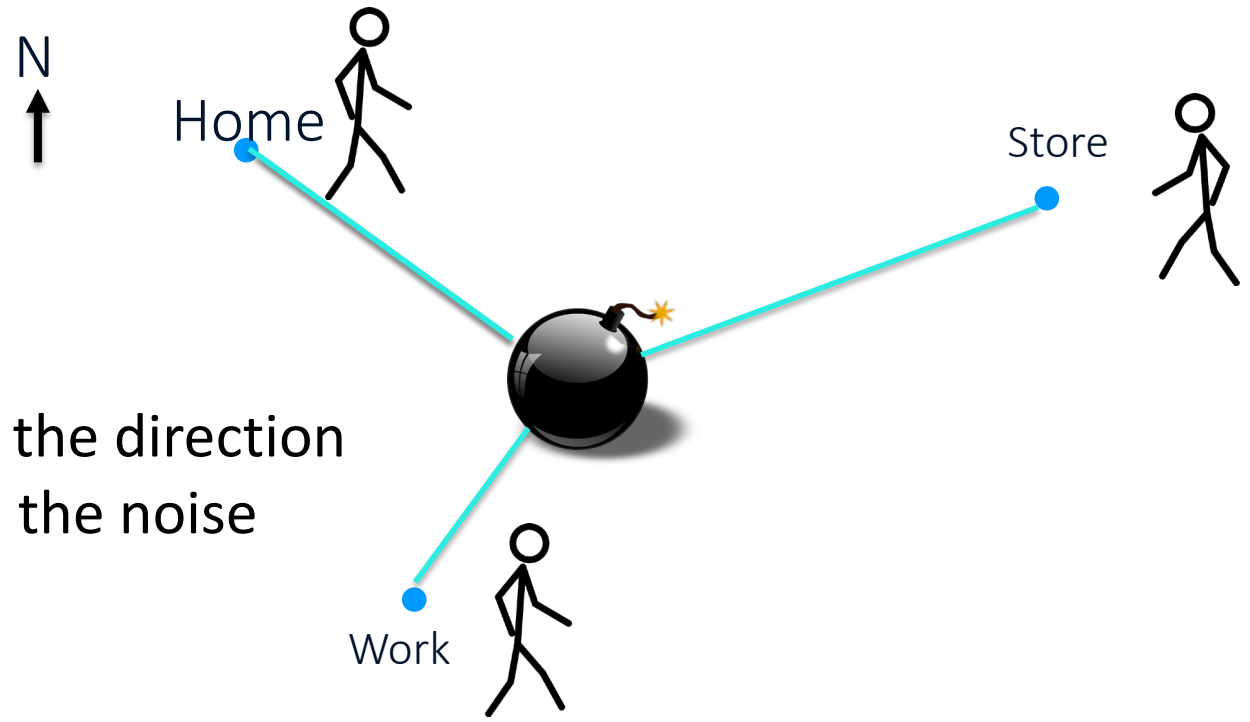




Triangulation

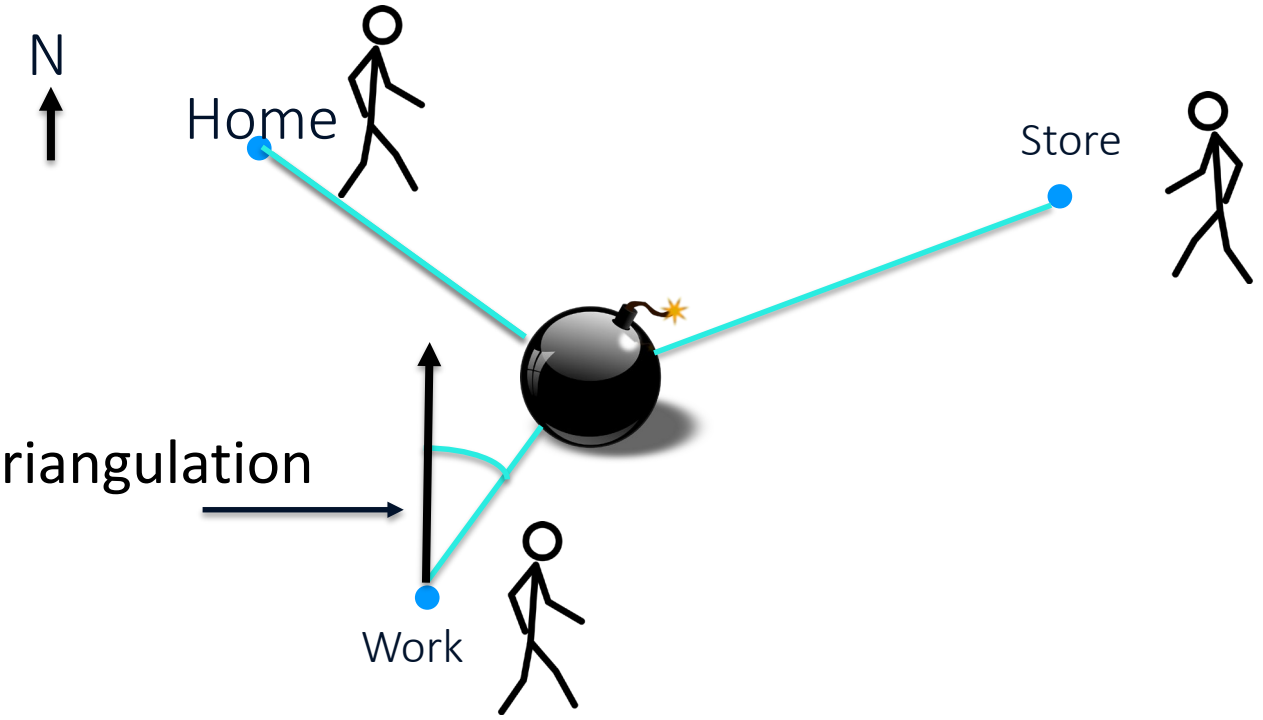
A loud boom goes off in the center of town…

Triangulation



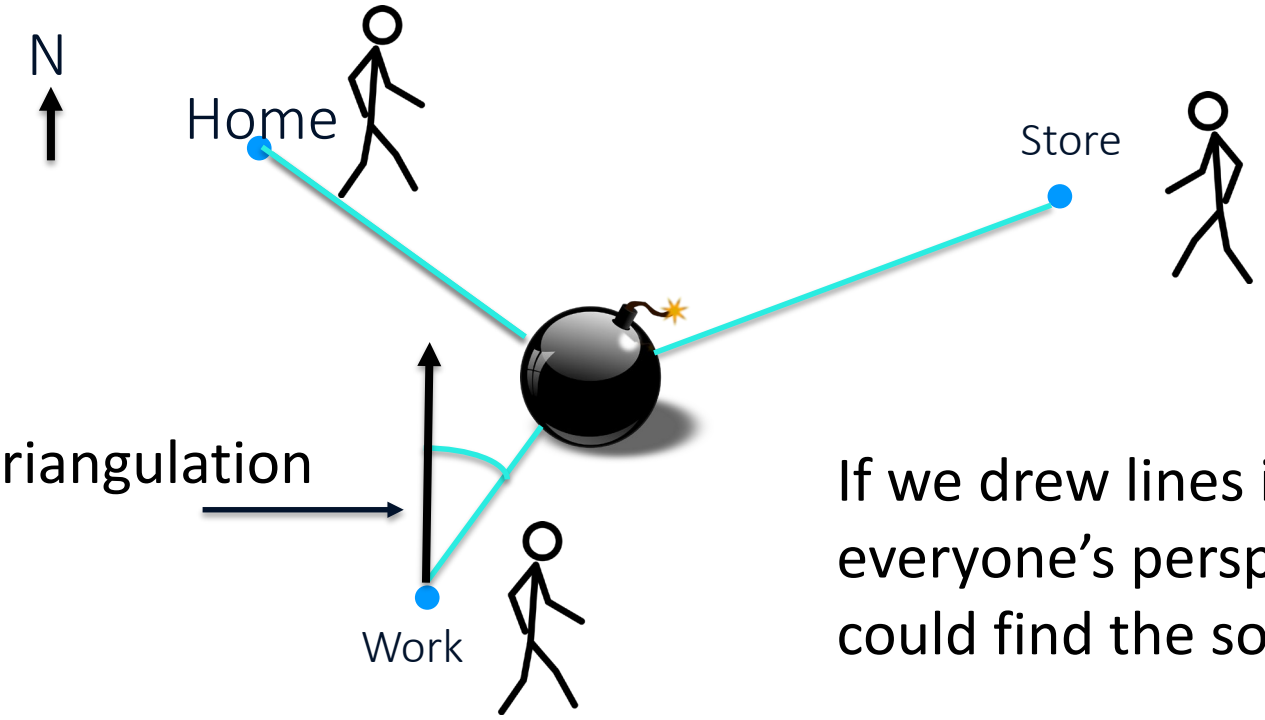
Everyone looks in the direction where *they* heard the noise

Triangulation



This is the “angle” in triangulation

Triangulation

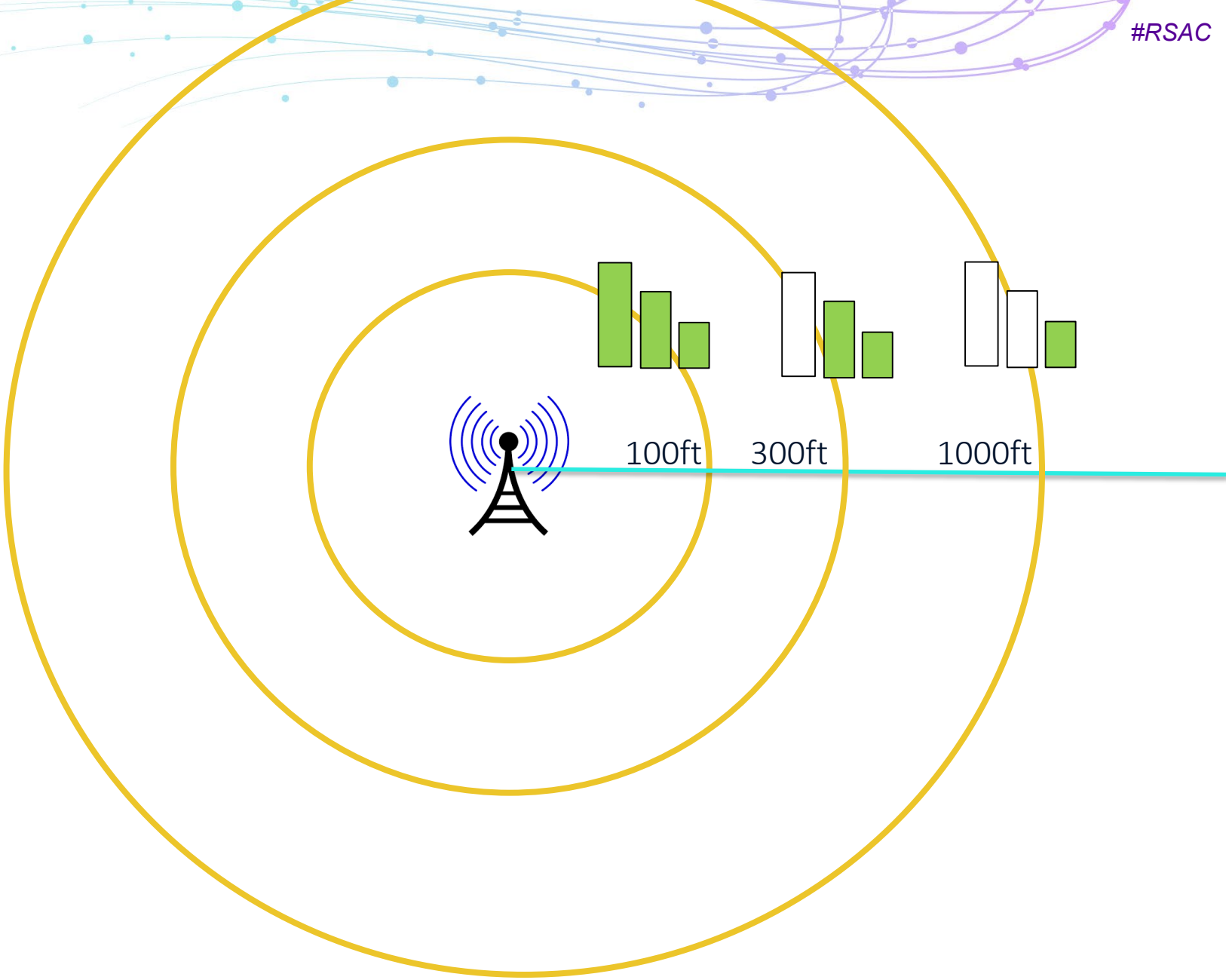


This is the “angle” in triangulation

If we drew lines in the direction from everyone’s perspective we could find the source.

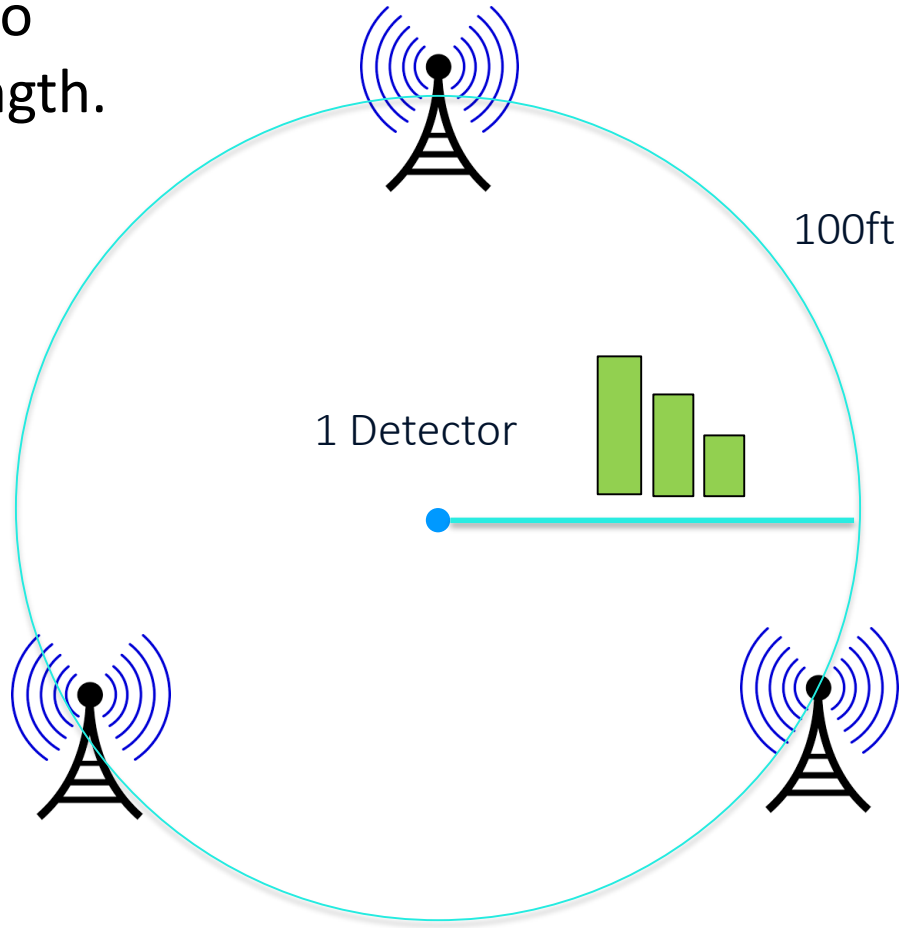
Trilateration

Trilateration works on signal strength and distance.



Trilateration

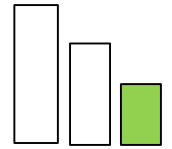
The closer you get to the radio source the higher signal strength.



Trilateration

If you're in one spot you can know only how far away a signal is.

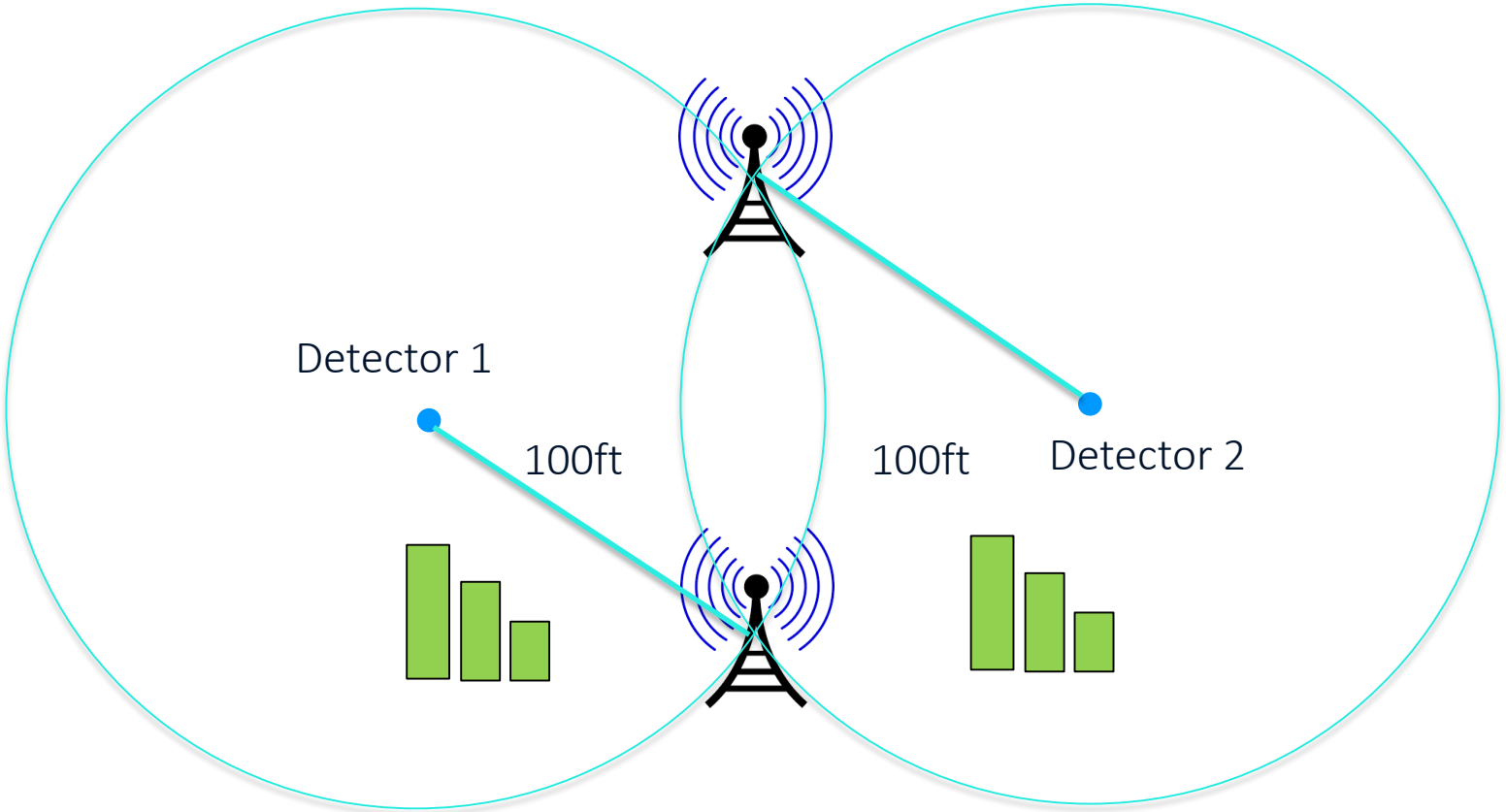
1 Detector



1000ft

Trilateration

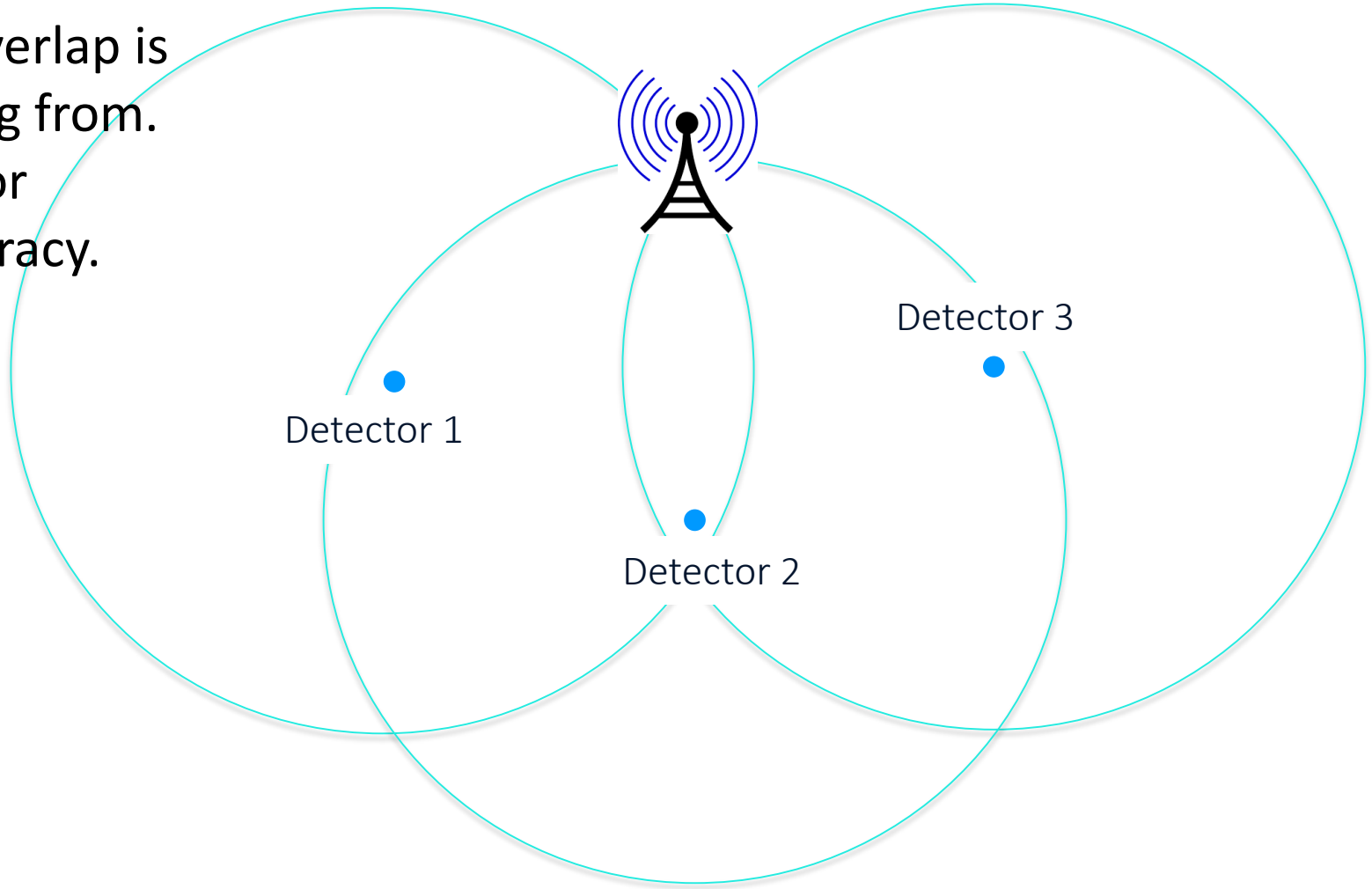
Where two detectors overlap, are where the signal can be coming from.



1 Detector

Trilateration

- Where three detectors overlap is where the signal is coming from.
- More “detectors” allow for error correction and accuracy.



RSAConference2019

How can you protect yourself?

How to find a solution for your company?

- Know your RF environment.
- Be aware of your devices and airspace.
- Have a logging solution in place.
- See if your existing hardware has WIDS & WIPS functionality.

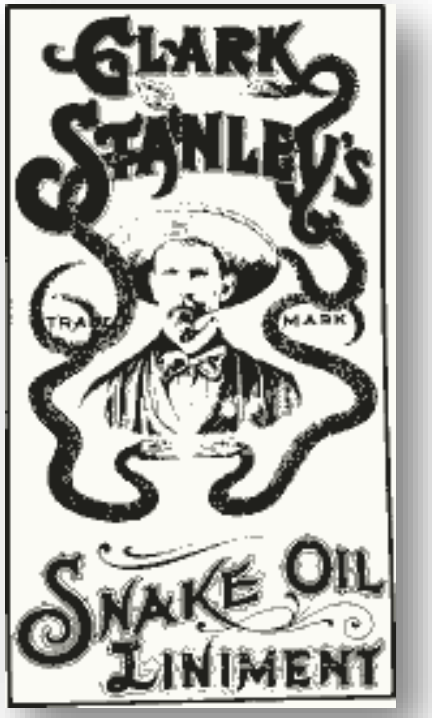
Tracking down rogue access points

- Know what access points are yours.
- Log surrounding MAC addresses.
- Know what you're looking for.
- Have employees be on the alert.

Rogue Access Point (IRL)->

How to find a solution for your company?

- Every solution is unique to your organization.
- Pros & Cons to every solution.
- WIPS & WIDS
  - WIPS (Wireless Intrusion Prevention System)
  - WIDS (Wireless Intrusion Detection System)
- Can detect deauthentication attacks & rogue APs

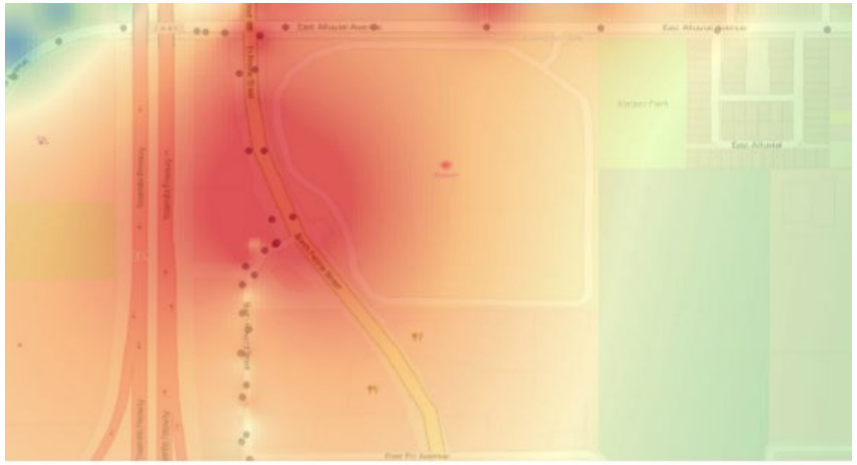


How to find a solution for your company?

- Know your RF environment.
- Be aware of your devices and airspace.
- Have a logging solution in place.
- See if your existing hardware has WIDS & WIPS functionality.

Wireless Protections

- A note on wireless penetration.
  - The distance your WiFi extends past your building is relative.
  - Great antennas can easily pickup WiFi from hundreds of yards away.
  - Specialty antennas can go even further.
- Your wireless network should not rely on distance for security.
  - Wireless heatmap ->



Apply What You Have Learned Today

- Next week you should:
  - See what existing protections you have in place.
  - Standup your own access point and see if anyone notices.
  - Identify all of your known wireless networks.
- In the next 90 days you should:
  - Be able to identify all of your access points across all of your sites.
- In six months you should:
  - Have removed all unnecessary wireless networks.
  - Be able to identify if a rogue access point.

RSAConference2019

Let’s play a game.

Put it into practice today.

Think you have the skills?

- Someone at the conference has a rogue access point!
- Find the rogue access point with the WiFi name of “FoxHunt”.
- If you think you’ve found the person carrying it, just ask.
- More questions? @EricEscobar 

RSAConference2019

Questions?