NEPSEC
SYDNEY

All the communication in silence...

But is it?

•••

NepSec Sydney
Chapter 0x06 | 5th Meetup

@imhaxormad
@MrMeterpreter

About me

@MrMeterpreter - aka Neat

Security Enthusiast (Yes I test pens sometimes pencils too)

Sometimes builder but more into pulling things apart.

Working for [Redacted] Cyber Security company.

Not really the ‘hacker’ you would think of.

Red Teaming enthusiast.

Host of the podcast ‘Nepal got Hacked’. Yes that’s my voice!

Disclaimer - I shall not be liable for people getting excited and breaking stuffs and launching any unlawful activities. This knowledge is totally for educational and self defense purpose!

Agenda

All the stuffs in the air we breath.

How systems communicate Wirelessly.

Something to do with SDR, RFID, Zigbee and et. al.

Something to do with 802.11.x - the ‘WiFi’ - (If you can’t break into wifi-networks you aren’t a hacker. - as they say)

Theoretically we should be able to break them - shall we? (DEMO)

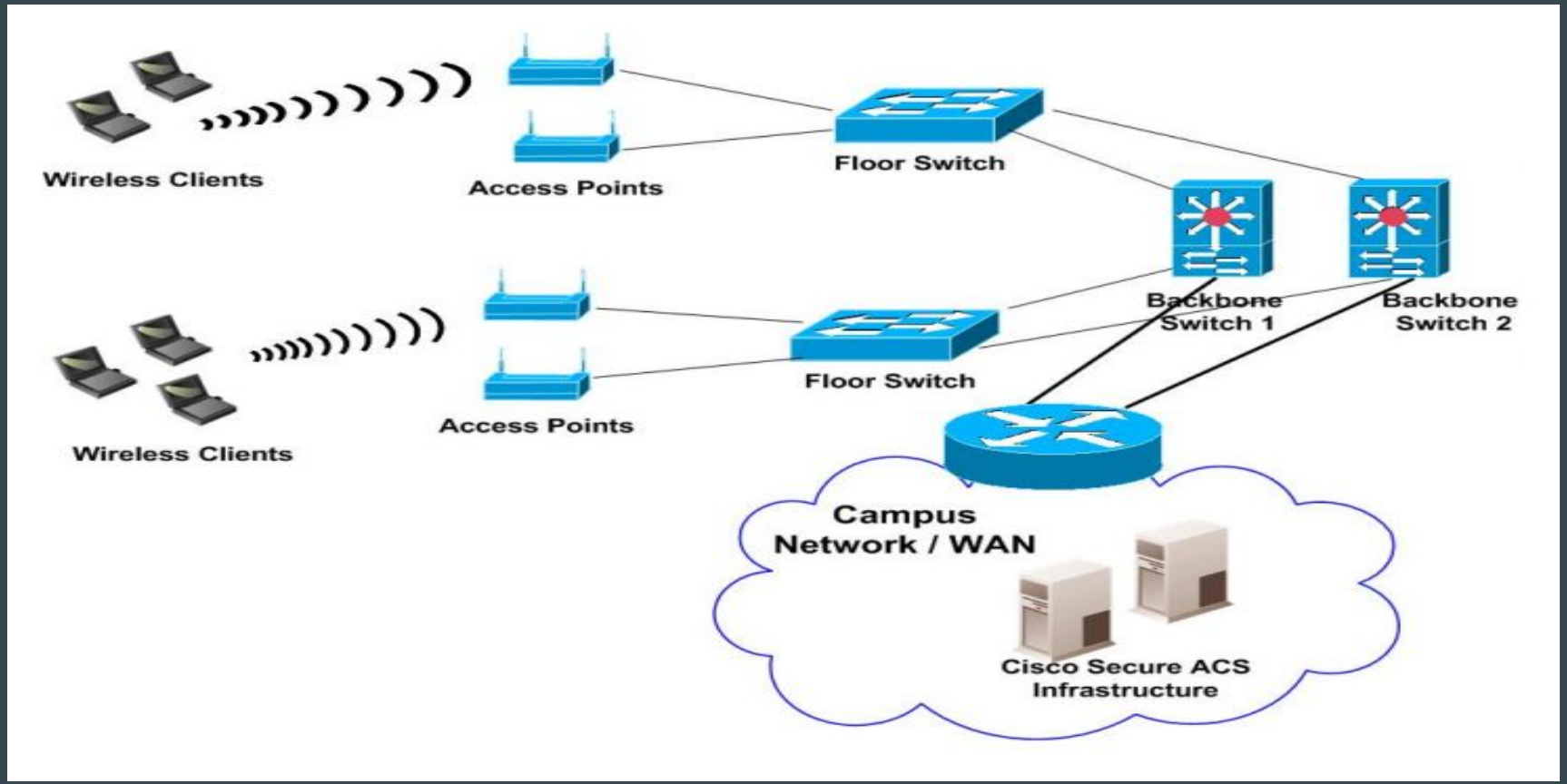
Takeaway

Working mechanism

As stated - “Wireless communication generally works through electromagnetic signals that are broadcast by an enabled device within the air, physical environment or atmosphere.” - Source

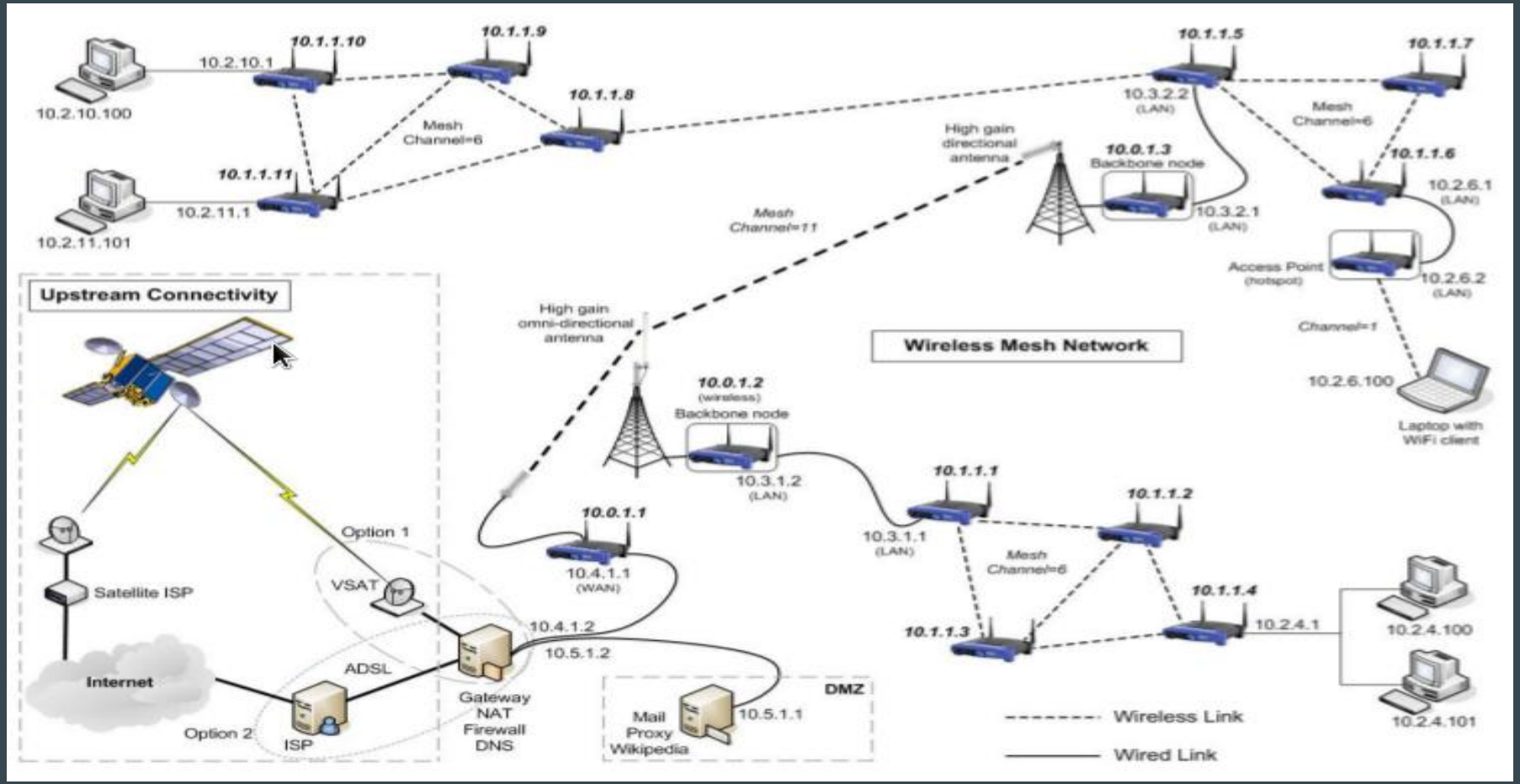
Source - https://www.techopedia.com/definition/10062/wireless-communications

Traditional Network (internal communication)

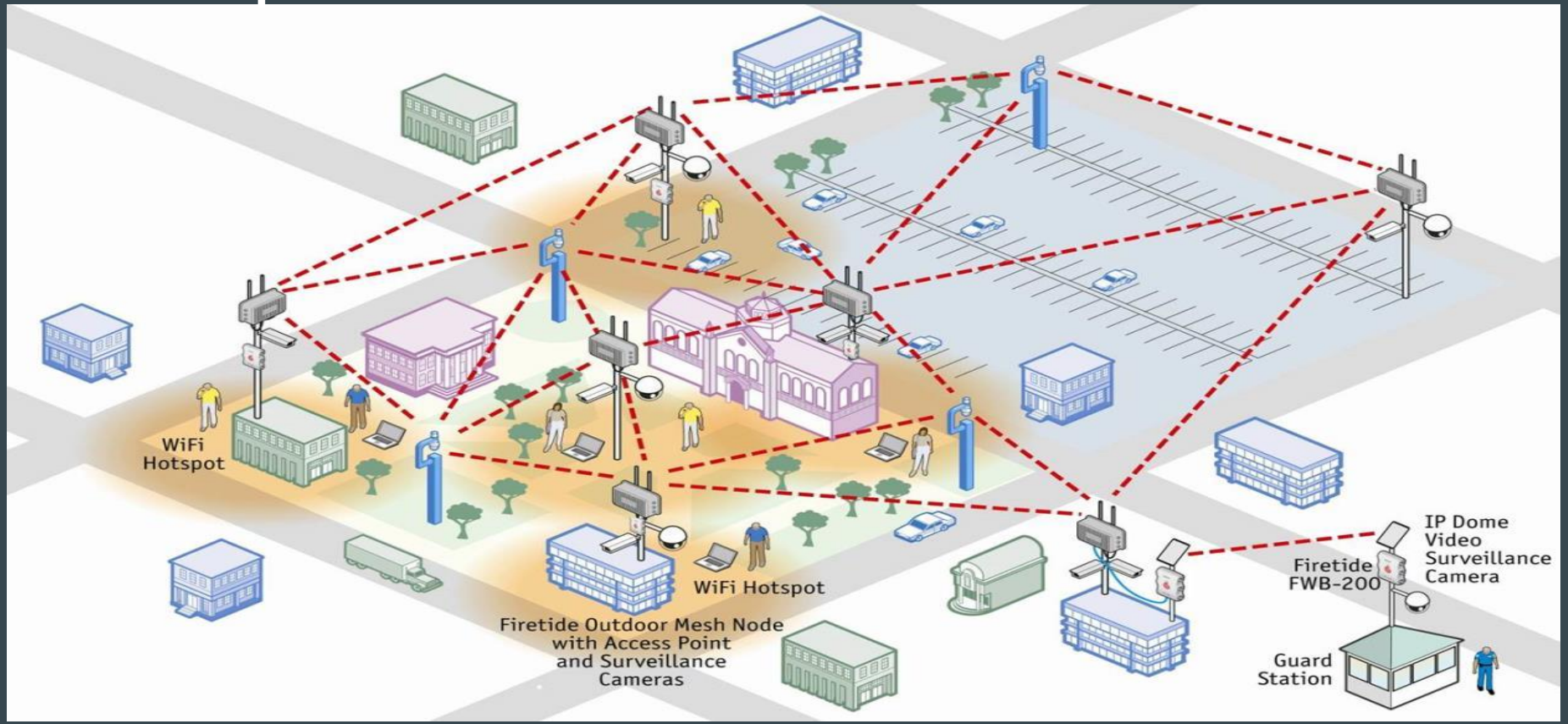


Source: https://www.cisco.com/c/dam/en_us/about/ciscoitatwork/downloads/ciscoitatwork/pdf/Cisco_IT_Wireless_LAN_Design_Guide.pdf

Traditional Network - with BTS, GSM station, satellite et. al.

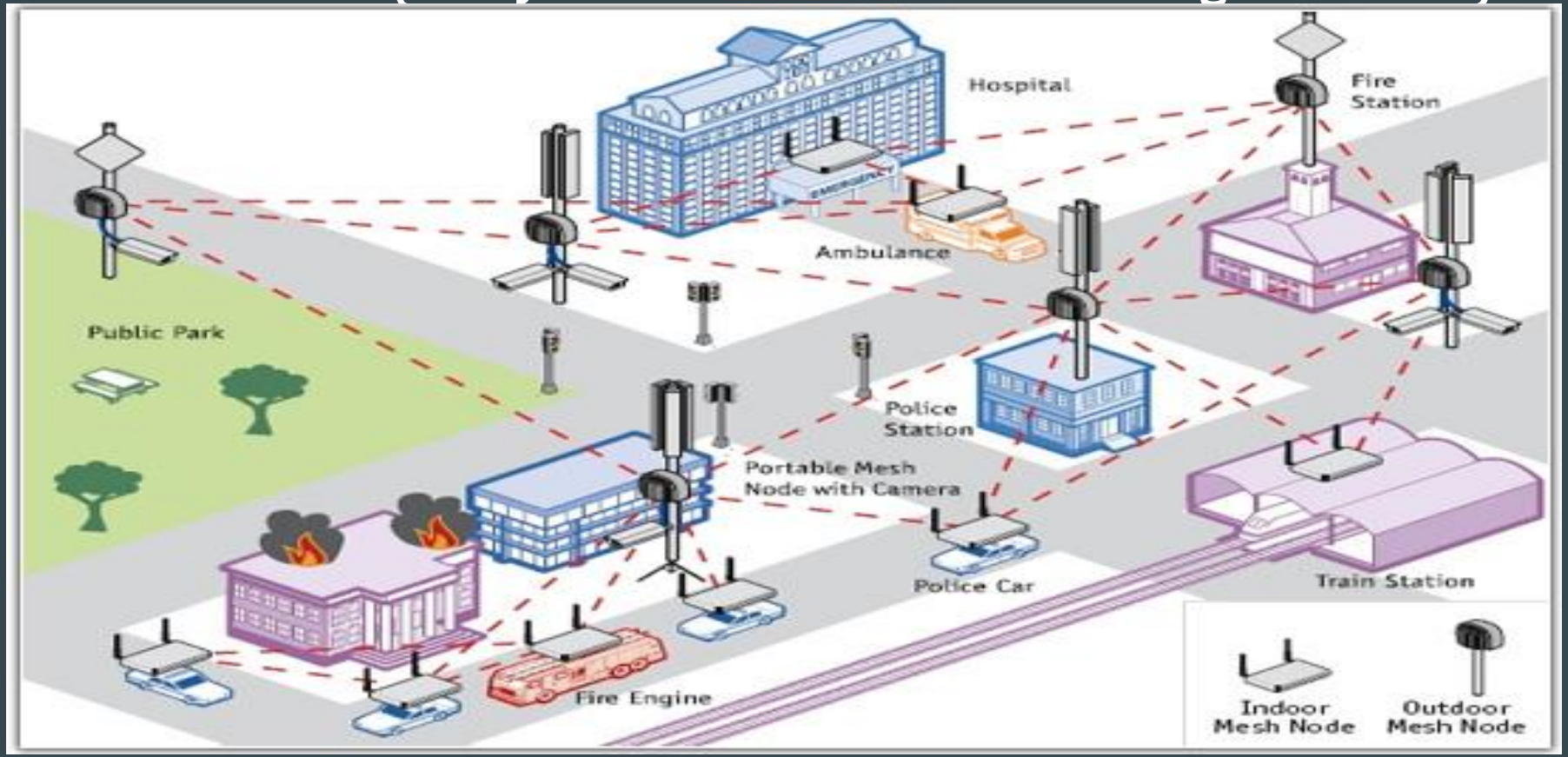


A broad picture of the wireless world...



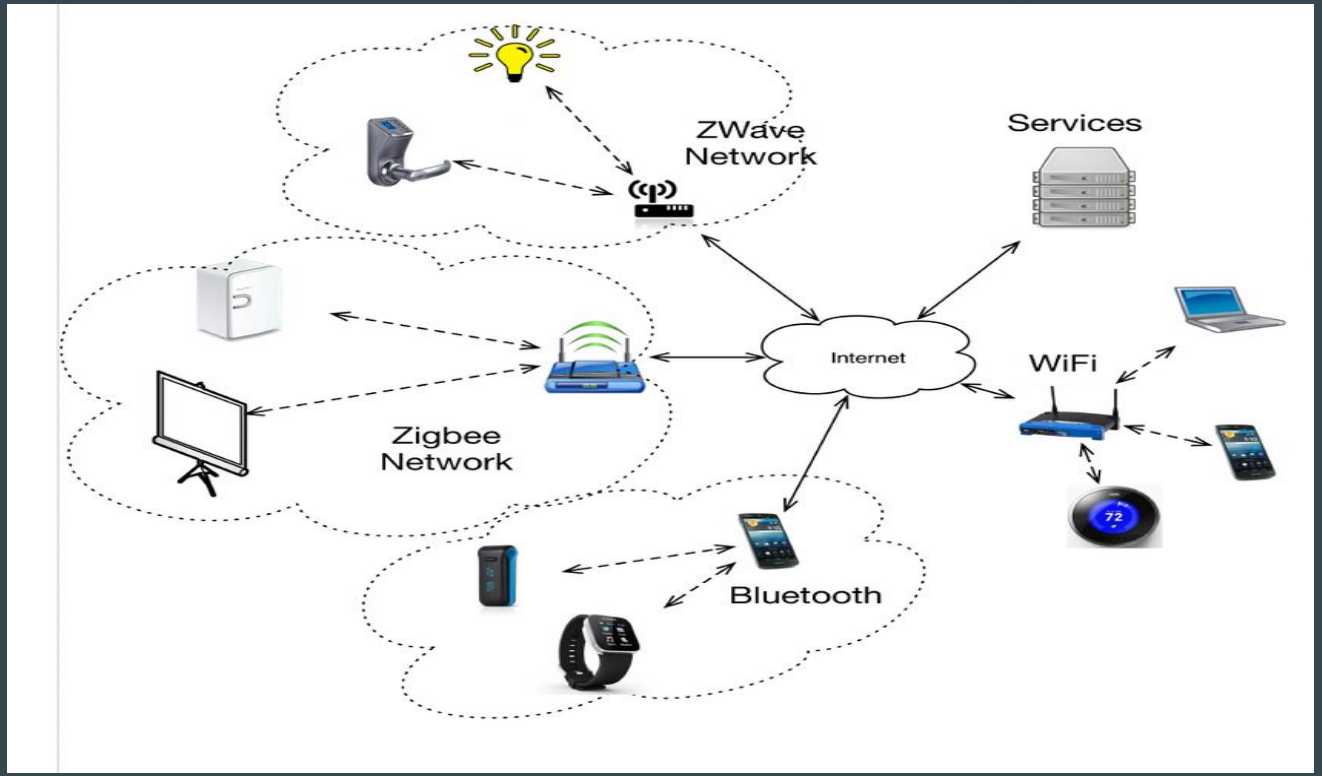
Source: https://scs-technologies.com/wi-fi-networks/

And this view... (everyone talks - even the buildings and cars)



Source: https://scs-technologies.com/wi-fi-networks/

The theoretical picture we see... - (kinda IOT architecture?)



Source: https://www.researchgate.net/figure/Present-state-of-IoT-network-architecture_fig2_267157426

Zigbee - The hidden attack surface

IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks (PAN) - smart home/cities.

Widely used in building management systems (BMS), connecting smart lights, wireless sensors, patient monitoring systems (Medicare systems), Traffic light control systems, Industrial control systems (SCADA) and much more.

An attack on a zigbee controlled systems could create a chaos on a certain environment under a given time frame and variable other factors.

Will show a video of a smart light being compromised remotely by replay attacks - in upcoming slides..

LoRaWAN (long range) - kinda similar to Zigbee but handles longer range communication.

RFID/NFC - The tag that you tagged

The cards (sorta) that let you into a building aye? - Used widely for access management, authentication and keeping track of stuffs!

It's in your bank cards, Passport, ETolls, Opal (for sydney folks), "Amazon Go Stores" (do your R&D there) and much more.

Examples - MIFARE (uses 13.56 MHz) - kinda easy to clone (the classic one)

Brute Force attacks on tag are popular - (PS: Most cards use default keys!)

R&D for y'all - @rfidiot - aka 'Major Malfunction' has got you covered!!

The hidden world of Bluetooth

Blue Borne came out probably couple years back or so...

Mousejacking - one of the coolest (practically achievable) exploit - hijacking wireless mouse and keyboards remotely (within radius).

If you can launch a mousejacking attack - you should be able to (under certain circumstances) remotely execute any sort of malicious codes on the remote system.

All you would need is a tiny little dongle - “Crazyradio PA”

Further read - https://www.mousejack.com/

So, what can an attacker gain - from the air...

Zigbee - Manipulate your home automation stuffs - https://www.youtube.com/watch?v=zcwz-lQtCwM

Zigbee - Manipulate your building management systems - https://www.youtube.com/watch?v=Ed1OjAuRARU

RFID - Digital Pickpocketing - https://www.youtube.com/watch?v=SPiyftJZ9jo

Launch MouseJacking attacks - https://www.youtube.com/watch?v=3NL2lEomB_Y

Software defined radio (SDR) - Probably listen to some radio's (as in - any RADIO/frequencies IYKWIM) with SDR - https://twitter.com/MrMeterpreter/status/1127214446709837825

Launch a War driving, war walking, war flying, war riding or just anything!

And even more... Things are not just limited to the Hollywood movies now!

My interesting finding (SDR)

Listening to tyre air pressure sensors https://twitter.com/MrMeterpreter/status/1098525706181476352

Listening to Automatic Dependent Surveillance Broadcast (A-DSB) ground station communication (Can't be public still - ongoing R&D) kinda radar communications and stuff.

Listening to Satellite transmissions (esp. Weather (weatherfax) information or you name it.)

and ... Shush! (Come to after meetup catch ups for demos!)

So - Let's just get the basics/most common stuff - (Something to do with 802.11.x)

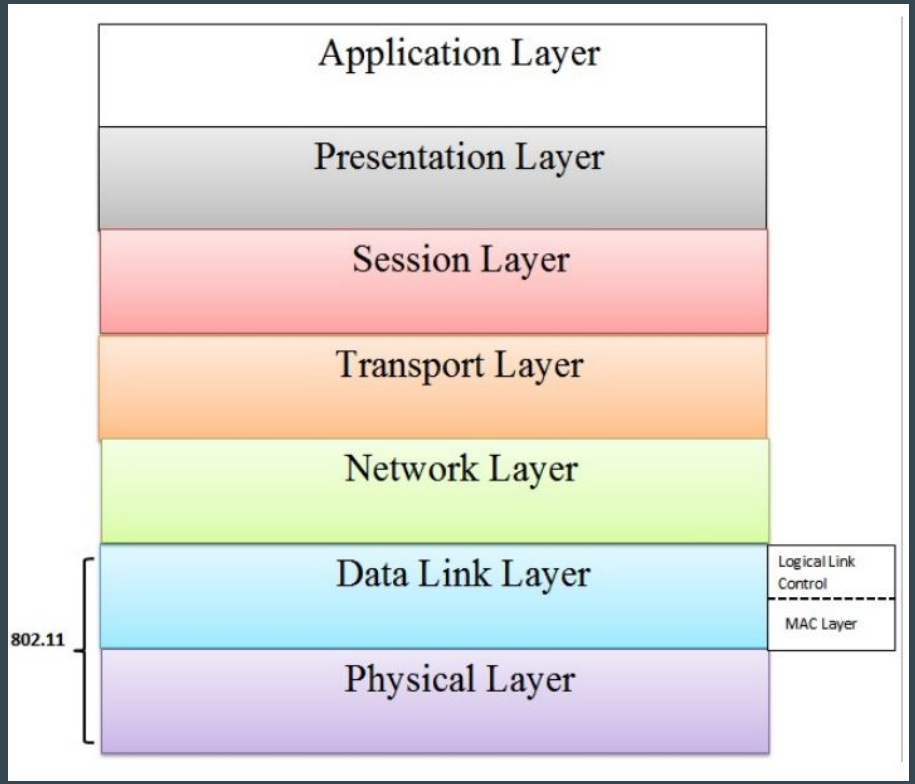
Wi-Fi standard uses the ISM (Industrial, Scientific and Medical) band - Free!!

Wireless Fidelity

Launched in 2.4GHz with transmission rates of 1-2mbps, Wi-Fi now works at 5GHz frequency also with transmission rate up to 54mbps at both frequencies. (Theoretically)

14 something channels - not sure (need to check on that)

The Technicalities - for 802.11.xx networks



Tools of trade

Aircrack-ng Suite - for replay attacks

Kismet - for wardriving and others

Wireshark/Tcpdump - for packet sniffing

KillerBee - for Zigbee replay attacks (Device - HackRF One)

Rtl_433, SDR#, GNU Radio and others - for RTL/SDR stuffs

Dump1090 - for Air Traffic Controller (ATC - used by Aeroplanes) traffic sniffing

Mfcuk - for RFID/NFC attacks

Demo Time!!!

A Lot of theory and excitement oey?

Let’s get some hands on!!!

Takeaway - Yoda wisdoms (lazy enough to paste from my old slide)

“Control, control, you must learn control!” i.e. Only hack what you own.

“Your weapons, you will not need them.” i.e. Installing Kali does not make you hacker.

“Much to learn you still have…my old padawan.” … “This is just the beginning!” i.e. Be curious, be passionate

“Always pass on what you have learned.” - You know what I mean.