OFFENSIVE WIRELESS SECURITY

WITH A REVIEW OF RF PRINCIPLES

whoami

- Maxine “Freqy”
  - @FreqyXin
- Pentester / Wireless security researcher
- US Army Veteran
- B.S. Info Assurance & Cybersecurity
  - Minor: Law & Policy
- Master’s Cybersecurity and Leadership
- GSEC, GCIH, GPEN, GAWN

LEGAL DISCLAIMER

The information included in this presentation is intended for educational purposes only, and should not be used in an illegal manner.

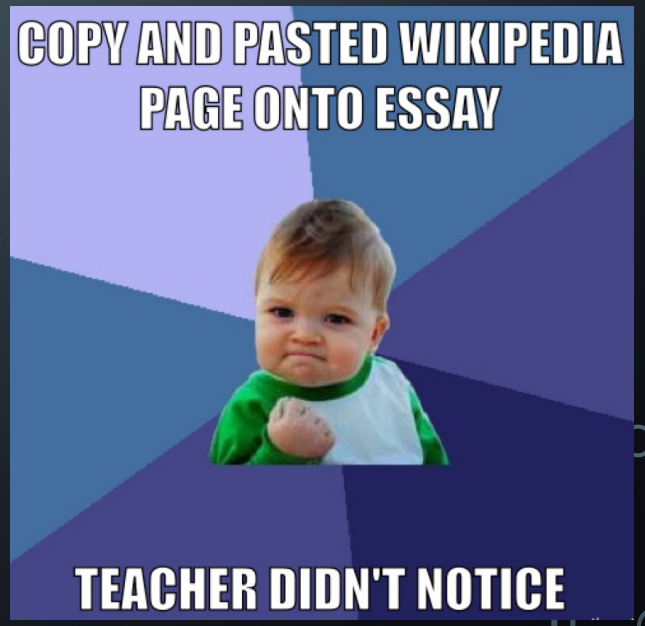
Don’t Be Evil!

OUTLINE

- Basic RF
- WiFi
- BLE
- ZigBee
- SDR
  - MouseJack

WHAT IS WIRELESS SECURITY?

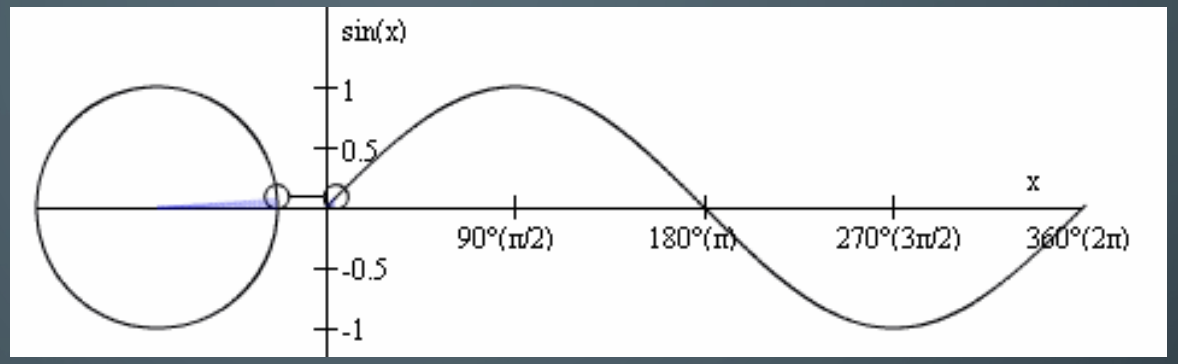
- "…the prevention of unauthorized access or damage to computers or data using wireless networks." – Wikipedia
- "As the number and availability of wireless-enabled devices continues to increase, itis important for organizations to actively test and secure their enterprise wireless environments. Wireless scans can help organizations determine corrective actions to mitigate risks posed by wireless enabled technologies." – NIST SPUB 800-115

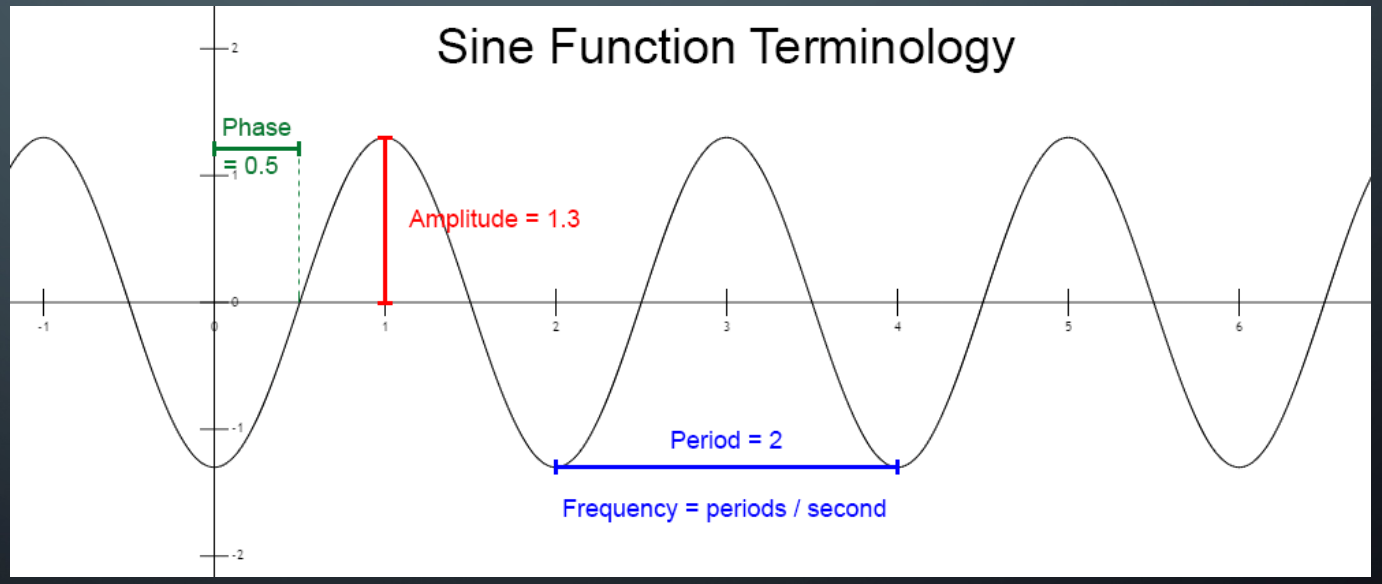


RF INTRO

WAVEFORMS

- A – Amplitude
- f – Frequency
- φ -- Phase

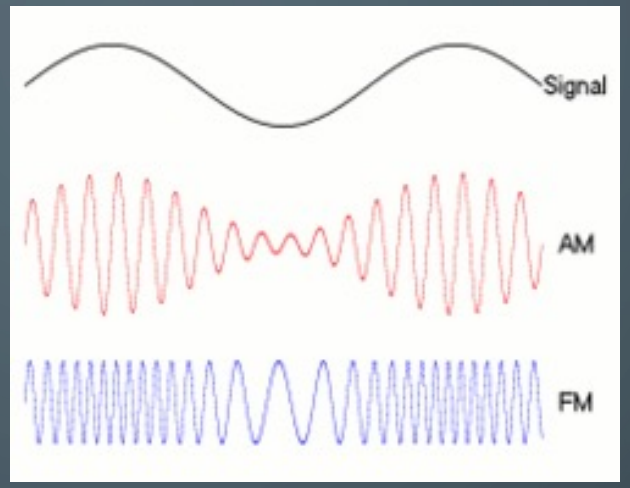




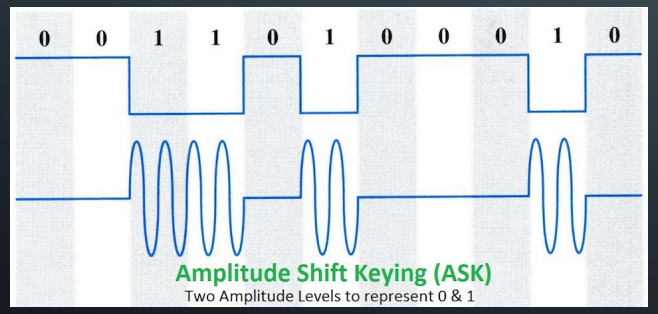
https://www.broad-strokes.com/2016-05/make-floating-rocks-with-the-power-of-math-part-2/

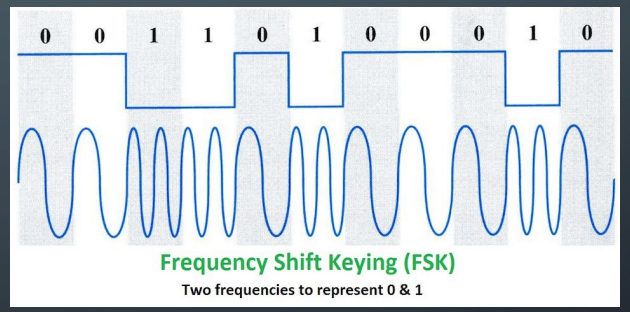
MODULATION

- Analog
  - AM – Amplitude Modulation
  - FM – Frequency Modulation

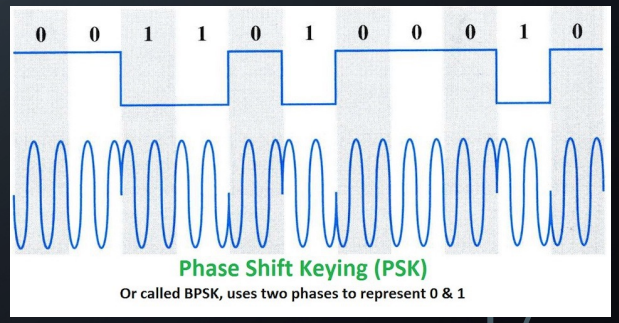


- Digital
  - ASK – Amplitude Shift Keying
    - OOK – On-Off Keying





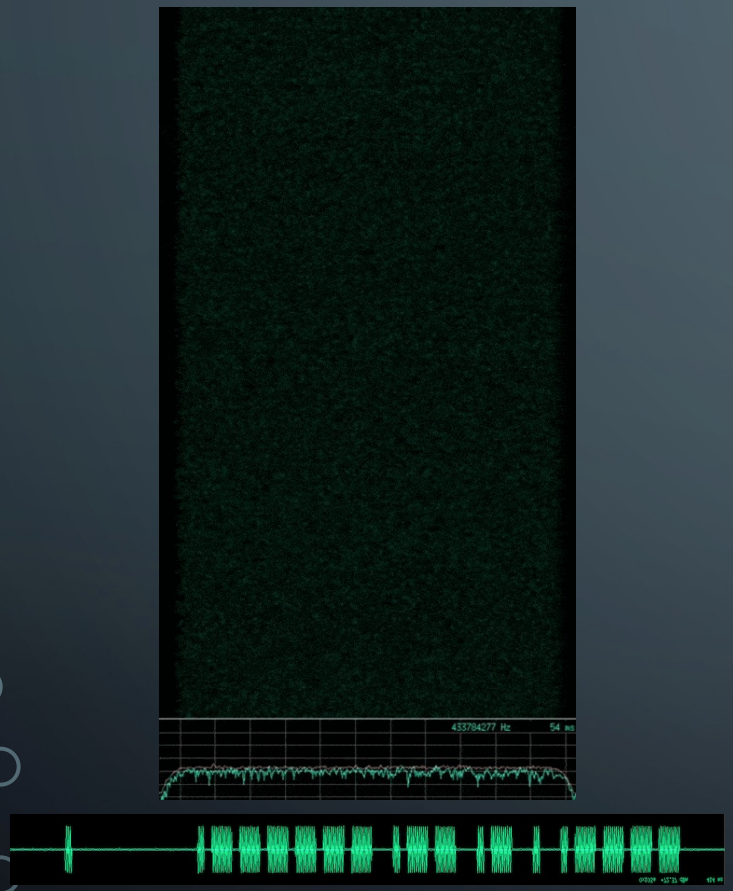
- FSK – Frequency Shift Keying
  - Binary FSK

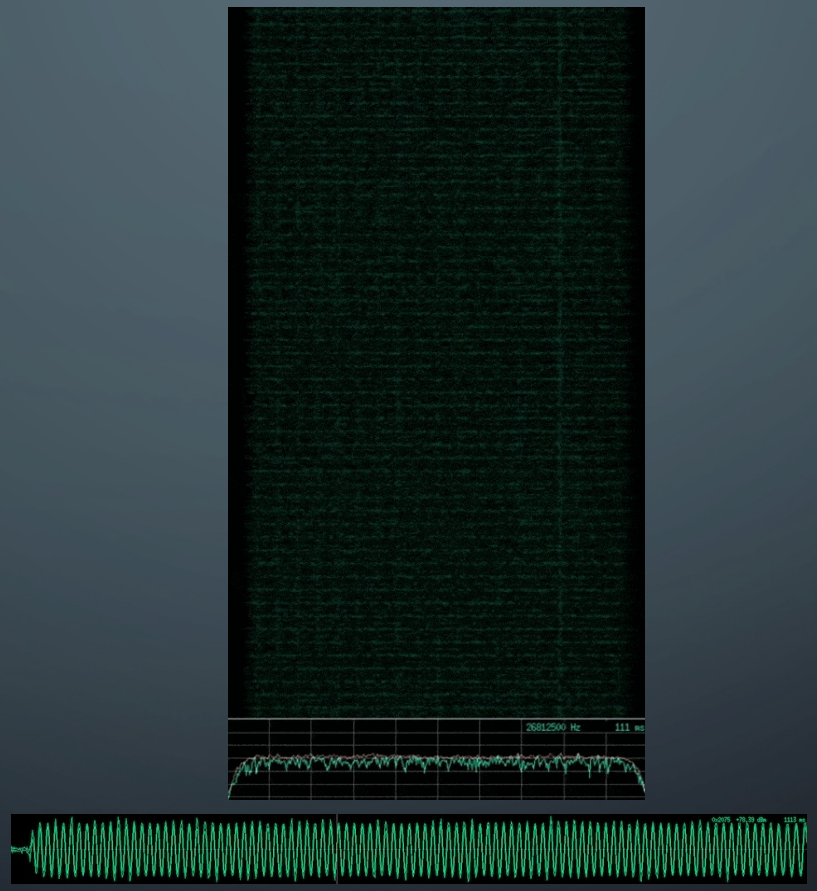


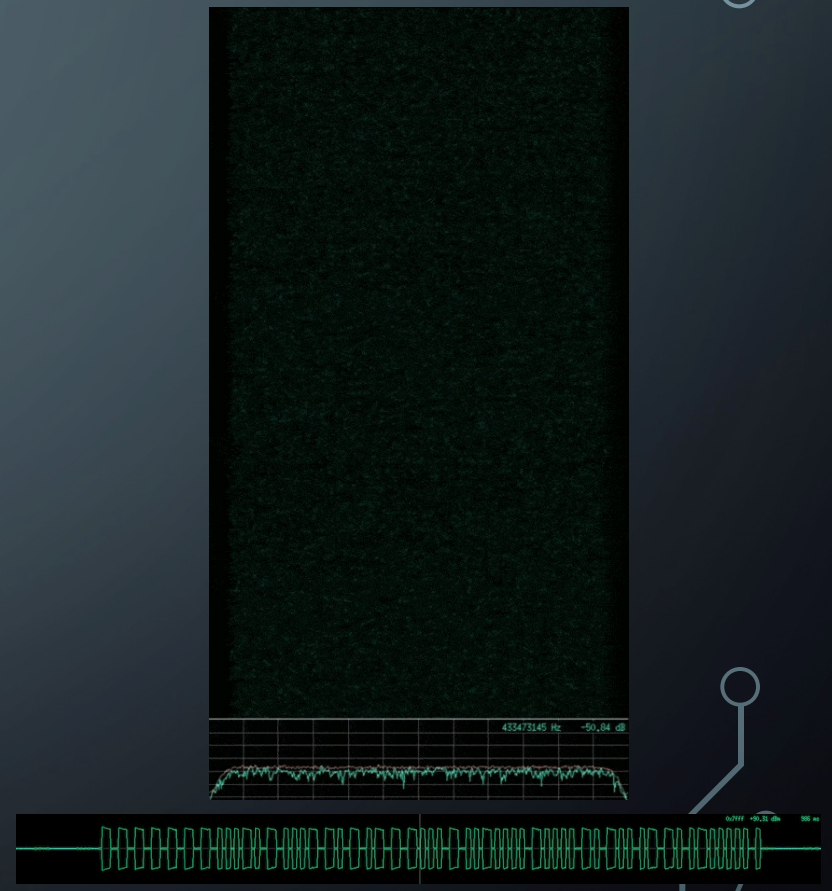
- PSK – Phase Shift Keying

https://www.elttam.com.au/blog/intro-sdr-and-rf-analysis/

ASK – OOK & PDM



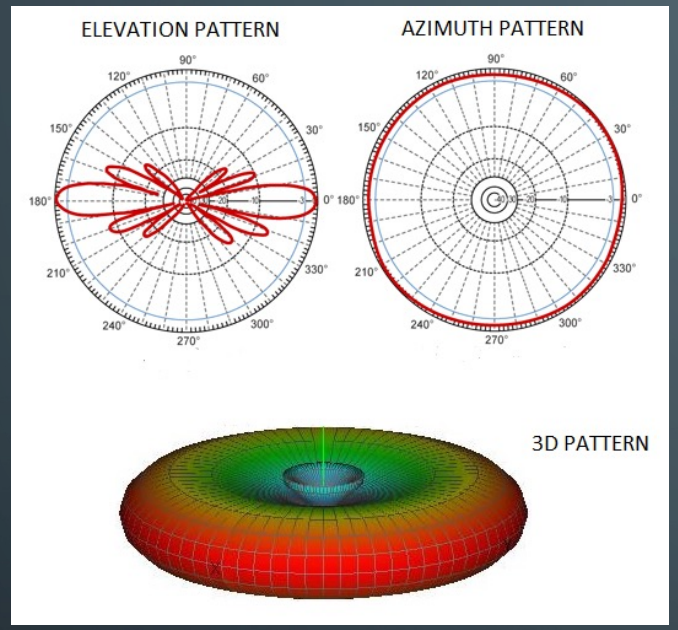




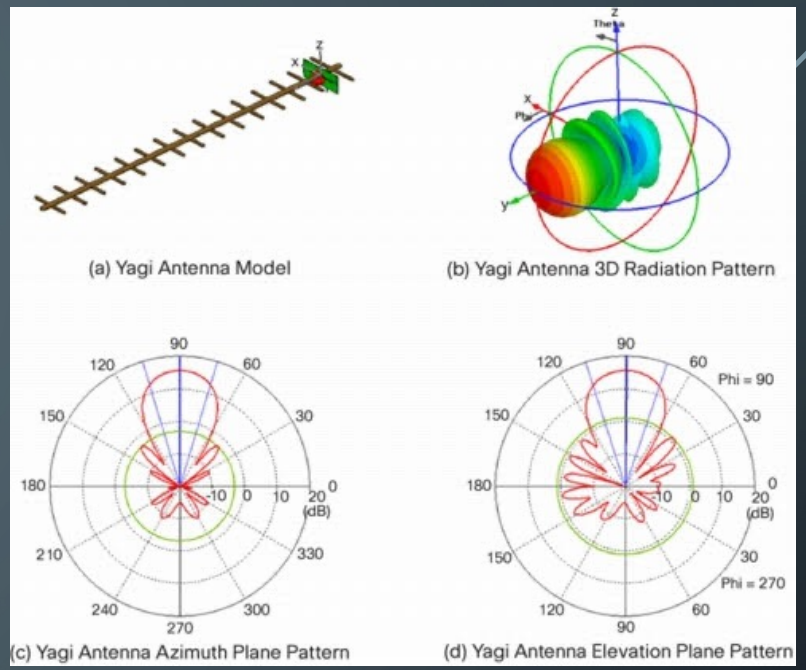
https://www.elttam.com.au/blog/intro-sdr-and-rf-analysis/

ANTENNAS

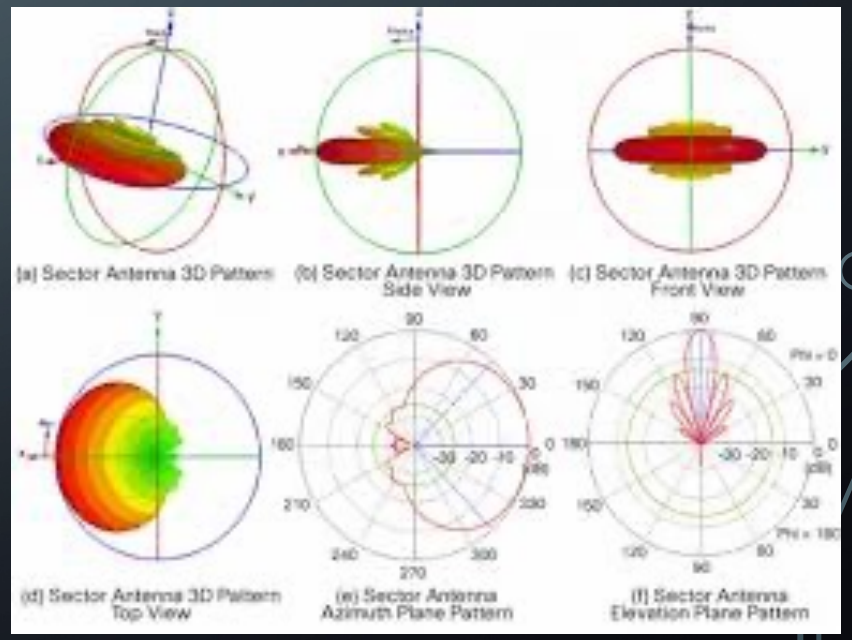
- Omni-Directional



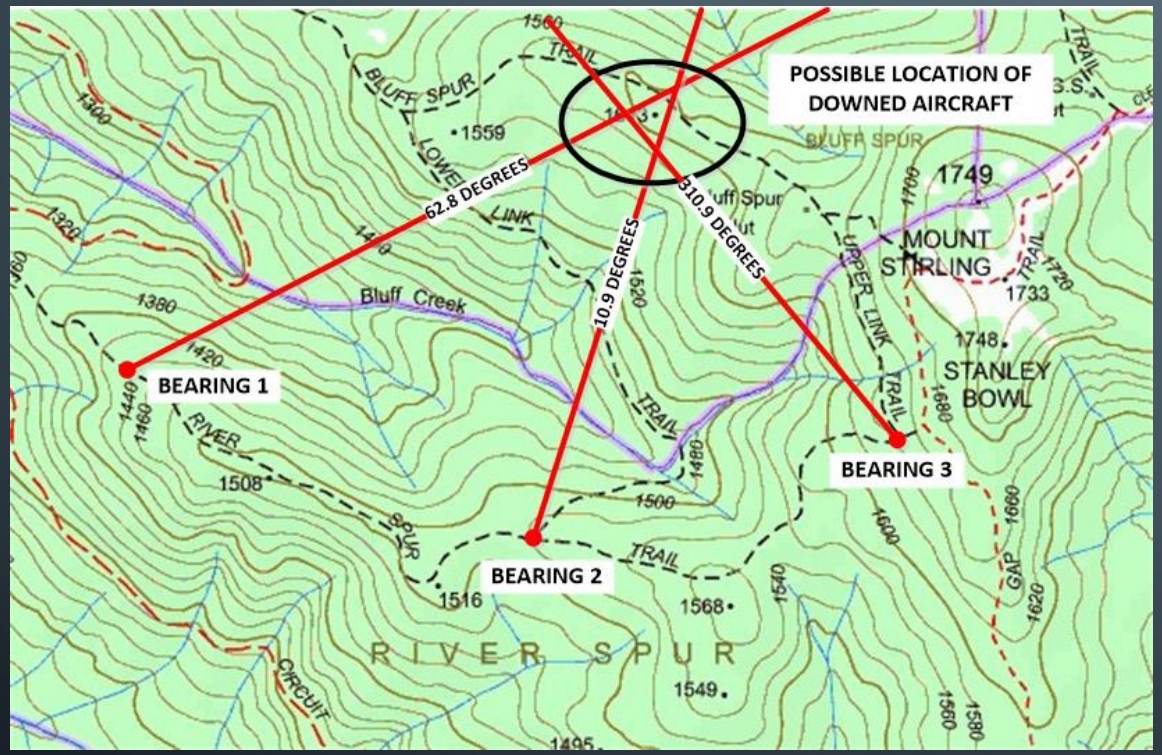
- Directional
  - Yagi

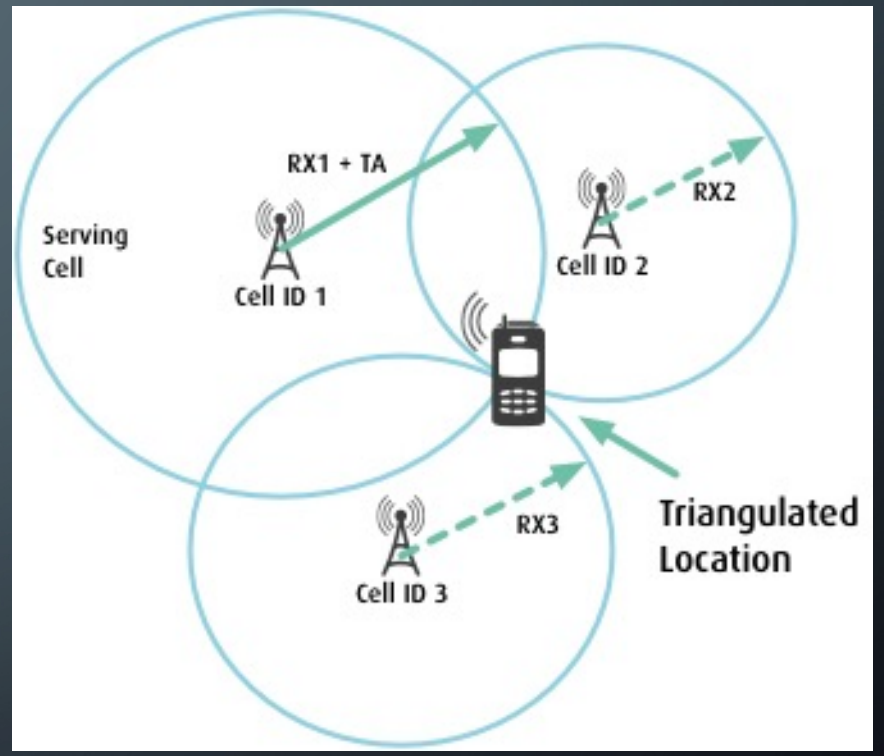


  - Sector



TRIANGULATION





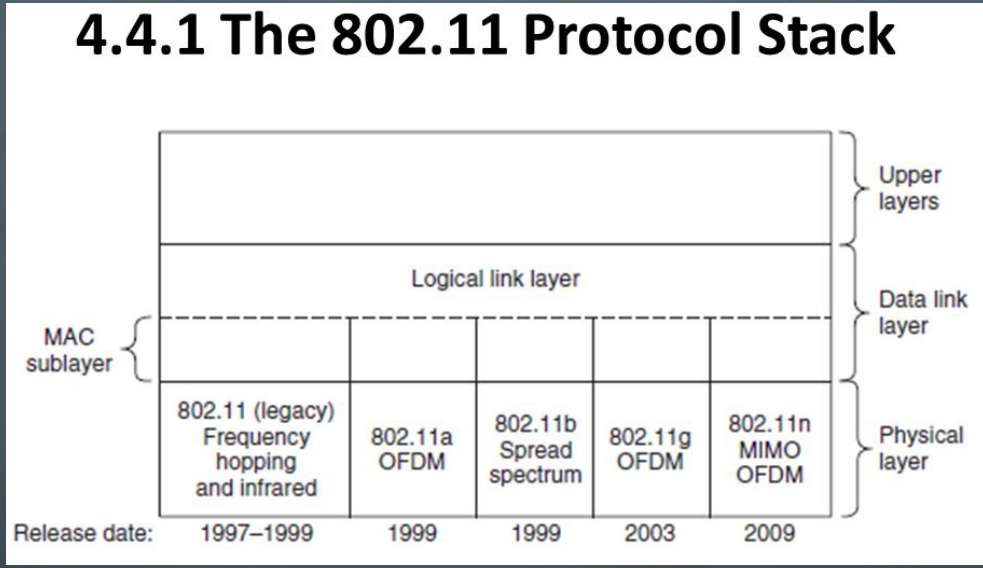
FREQUENCY JAMMING VS PROTOCOL JAMMING

- Frequency Jamming
  - VERY ILLEGAL
- Protocol Jamming
  - i.e Deauthentication
  - Legal to use on equipment you own

RF APPLICATION PT. 1

WI-FI

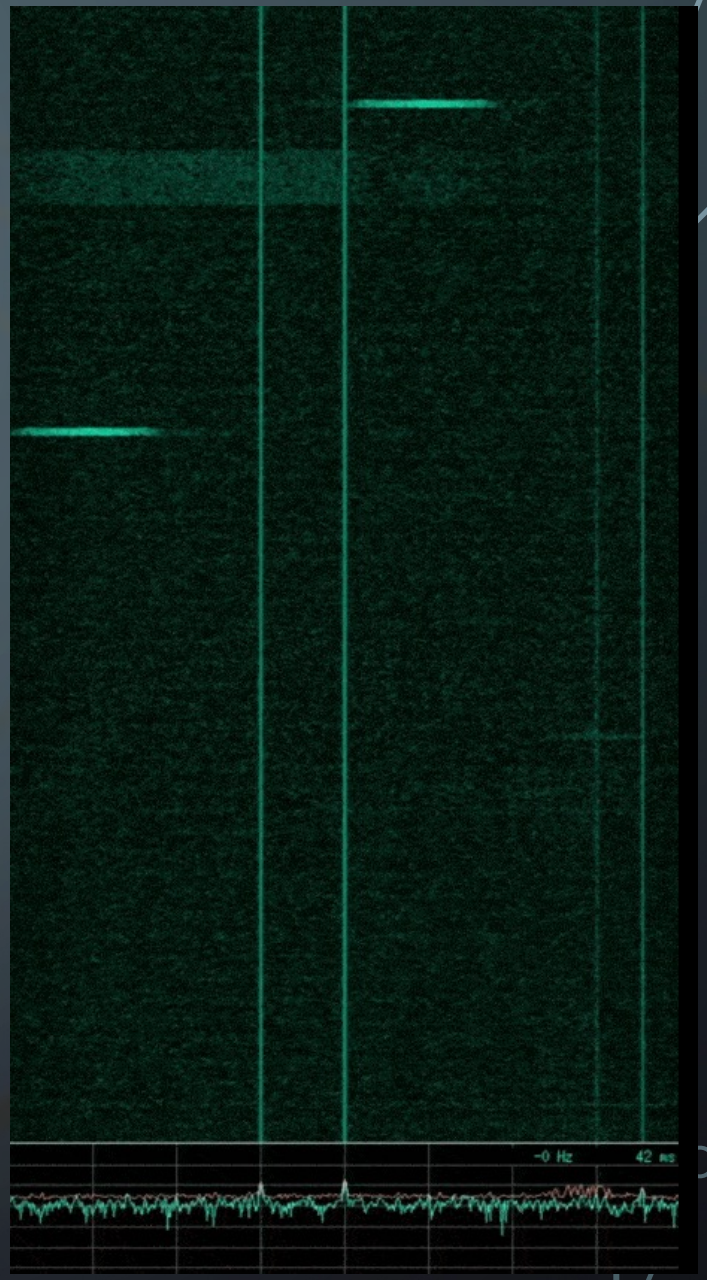
- 802.11 a/ac/g/n/b etc…
- 2.4 & 5 GHz band
- WEP
- WPA\WPA2
  - PSK
  - WPS
- WPA3



- Evolution of the Physical Layer

- Attacks
  - Evil-Twin
    - Evil-Portal
    - GTC downgrade
    - HTTPS downgrade
  - PMKID

- Security:
  Direct Sequence Spread Spectrum (DSSS)
  - Wide Frequency Set



https://www.elttam.com.au/blog/intro-sdr-and-rf-analysis/

TERMS

- AP – Access Point
- Client – device associated to AP via WiFi
- Monitor Mode – capable of sniffing WiFi traffic
- PSK – Pre-Shared Key
- Management Frames – used for deauthing attacks
- 4-way Handshake – EAPOL exchange needed for PSK
- PMKID – Primary Key ID

TOOLS

- Air-Crack Suite
- EAPHammer
- Kismet
- Alfa - AWUS036ACM

KISMET

Kismet - Mozilla Firefox

Kismet | New Tab

localhost:2501

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec

Kismet

Devices | Alerts | SSIDs | ADSB Live

Wi-Fi Access Points

Search:

Name	Type	Phy	Crypto	Signal	Channel	Data	Packets	Clients	BSSID	QBSS Chan Usage	QBSS Users
02:AA:A0:A4:48:20	Wi-Fi AP	IEEE802.11	WPA2-PSK	-87	44	0 B		0	02:AA:A0:A4:48:20	n/a	n/a
8E:6A:8D:5C:39:1A	Wi-Fi AP	IEEE802.11	WPA2-CCMP	-83	44	0 B		0	8E:6A:8D:5C:39:1A	12.94%	0
8E:6A:8D:5C:39:1B	Wi-Fi AP	IEEE802.11	WPA2-PSK	-83	44	0 B		0	8E:6A:8D:5C:39:1B	12.94%	1
8E:6A:8D:5C:39:18	Wi-Fi AP	IEEE802.11	WPA2-PSK	-83	44	0 B		0	8E:6A:8D:5C:39:18	12.94%	0
18:90:88:4F:C8:6B	Wi-Fi AP	IEEE802.11	Open	-88	40	0 B		0	18:90:88:4F:C8:6B	n/a	n/a
18:90:88:4F:C8:65	Wi-Fi AP	IEEE802.11	WPA3-SAE	-88	40	0 B		0	18:90:88:4F:C8:65	n/a	n/a
24:5A:4C:90:DF:45	Wi-Fi AP	IEEE802.11	WEP	-70	153	0 B		0	24:5A:4C:90:DF:45	7.843%	0
26:5A:4C:90:DF:44	Wi-Fi AP	IEEE802.11	WPA2-PSK	-59	11	0 B		0	26:5A:4C:90:DF:44	20.39%	0
26:5A:4C:A0:DF:45	Wi-Fi AP	IEEE802.11	WPA2-PSK	-70	153	0 B		0	26:5A:4C:A0:DF:45	7.843%	0
62:45:B7:FA:20:28	Wi-Fi AP	IEEE802.11	WEP	-83	36	0 B		0	62:45:B7:FA:20:28	n/a	n/a
A2:FF:70:06:1E:2E	Wi-Fi AP	IEEE802.11	WPA2-PSK	-82	157	0 B		0	A2:FF:70:06:1E:2E	7.451%	0

51 devices

Messages | Channels

```
Aug 15 2022 23:43:01  802.11 Wi-Fi device 8E:6A:8D:5C:39:19 advertising SSID 'XFINITY'
Aug 15 2022 23:43:01  802.11 Wi-Fi device 8E:6A:8D:5C:39:1F advertising SSID 'xfinitywifi'
Aug 15 2022 23:43:01  Detected new 802.11 Wi-Fi device B4:B6:86:9D:CC:68
Aug 15 2022 23:43:01  802.11 Wi-Fi device 8C:6A:8D:54:39:1D advertising SSID 'SCCGNET'
Aug 15 2022 23:43:01  Detected new 802.11 Wi-Fi device 20:1F:3B:89:8E:1E
Aug 15 2022 23:43:01  802.11 Wi-Fi device B6:53:D2:92:EA:F7 advertising SSID 'sieggsjh'
Aug 15 2022 23:42:48  Detected new 802.11 Wi-Fi device 9A:FC:8E:2A:7E:E2
Aug 15 2022 23:42:44  Detected new 802.11 Wi-Fi device 14:59:C0:91:8D:CF
```

Powered by many OSS components, see the **credits page**

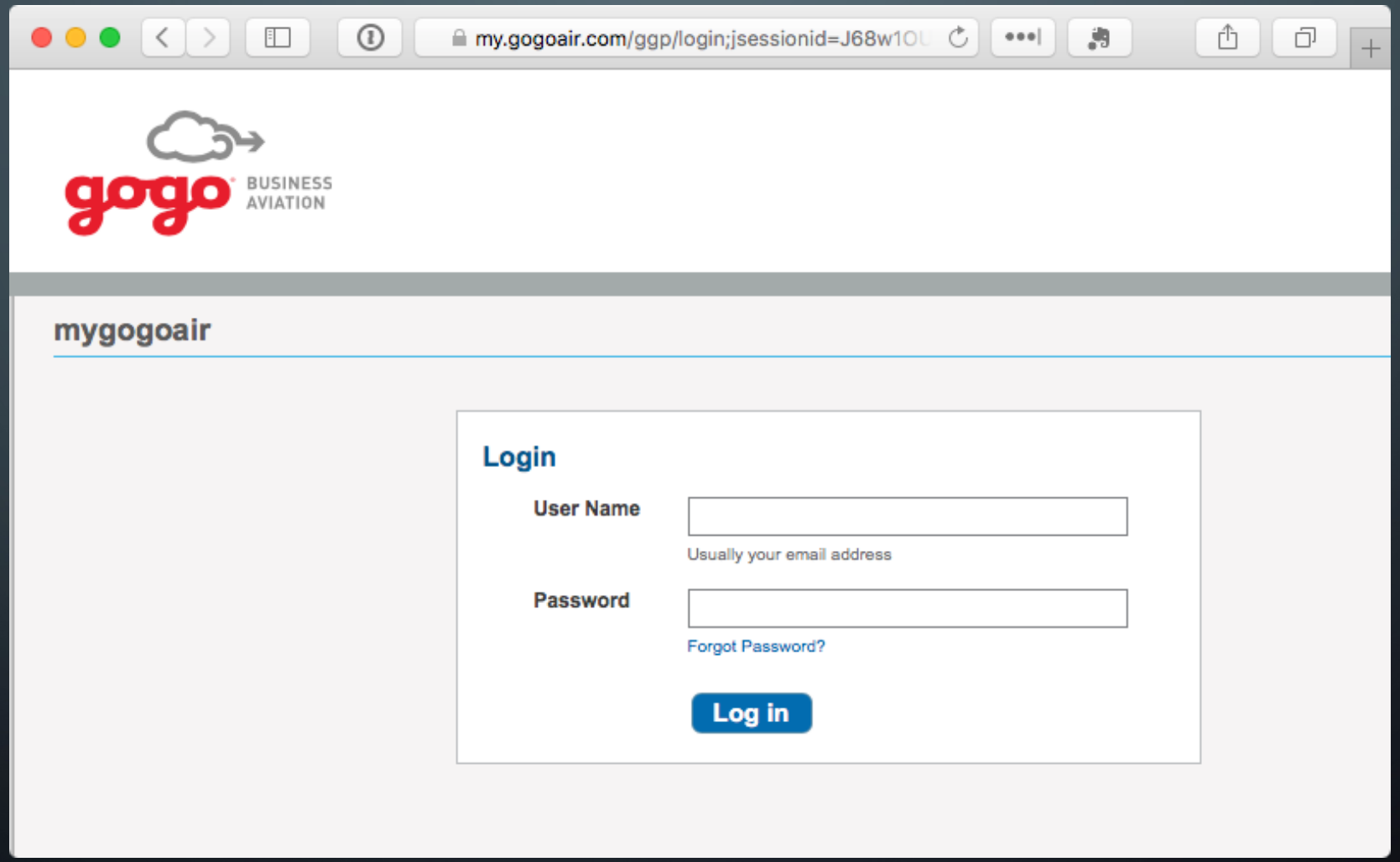
DEAUTHENTICATION / DISASSOCIATION

- Deauth
  - Uses Management Frames to tell target AP to break connection with associated client
- Disassociation
  - Management Frame to tell target client to break connection with AP
- These are active attacks
  - Forces a new 4-way handshake exchange
  - Sniff for EAPOL data

EVIL TWIN

- Spoof of legitimate AP
- Overpower legitimate AP with directional antenna and power amp

EVIL PORTAL


my.gogoair.com/ggp/login;jsessionid=J68w1O
gogo
BUSINESS
AVIATION
mygogoair
Login
User Name
Usually your email address
Password
Forgot Password?
Log in

PROBES, BAD KARMA, EVIL TWINS, AND EVIL PORTALS

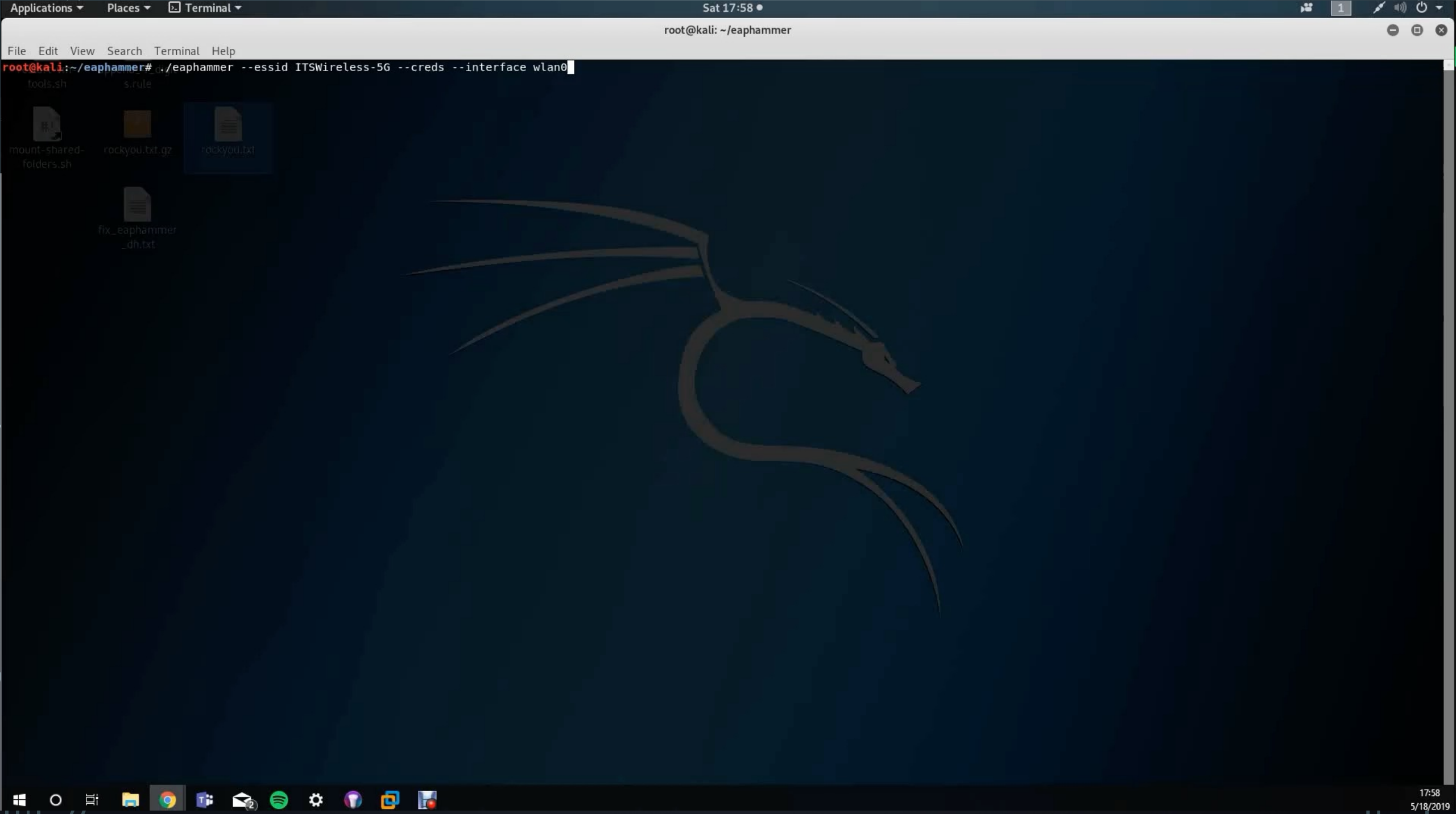
- MSCHAPv2 GTC Downgrade Attack
  - Targets devices that do not require certification validation
  - EAP-TLS and NTLMv2
  - Cleartext Passwords
- Karma
  - Replies to user AP probe requests

Applications Places Terminal Sat 17:58

root@kali: ~/eaphammer

File Edit View Search Terminal Help

```
root@kali:~/eaphammer# ./eaphammer --essid ITSWireless-5G --creds --interface wlan0
```



17:58
5/18/2019

BLUETOOTH LOW ENERGY

Bluetooth®

Ranges of Bluetooth devices by class

Class	Max. permitted power		Typ. range[2]
	(mW)	(dBm)	(m)
1	100	20	~100
1.5 (BT 5 Vol 6 Part A Sect 3)	10	10	~20
2	2.5	4	~10
3	1	0	~1
4	0.5	−3	~0.5

- 2.400 – 2.485 GHZ

- Bluetooth Classic -- “Old”
- Bluetooth Low Energy (BLE) -- “New”

- Vulnerabilities
  - Blueborne CVE-2017-0785
    - Phones, TV’s, Computers
  - CVE-2018-5383
    - Mobile Devices
    - ECC Validation issues during Diffie-Hellman exchange
  - CVE-2018-16986 & CVE-2018-16986
    - Buffer Overflow
    - Wireless Access Points
    - Bluetooth Maintenance Console Access
    - Malicious Firmware

HARALD “BLUETOOTH”

- King of Denmark and Norway
- United Nations
- Blueberries

HEDY LEMARR

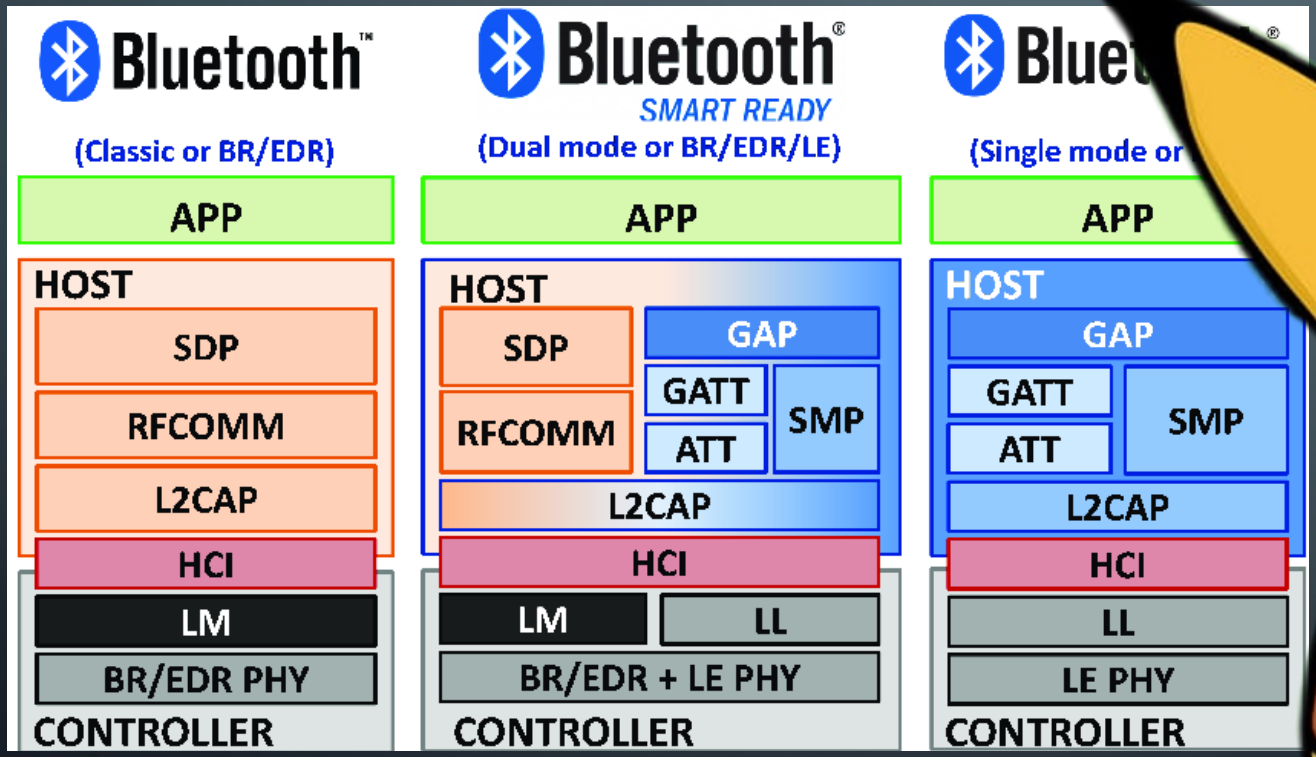
1914 - 2000

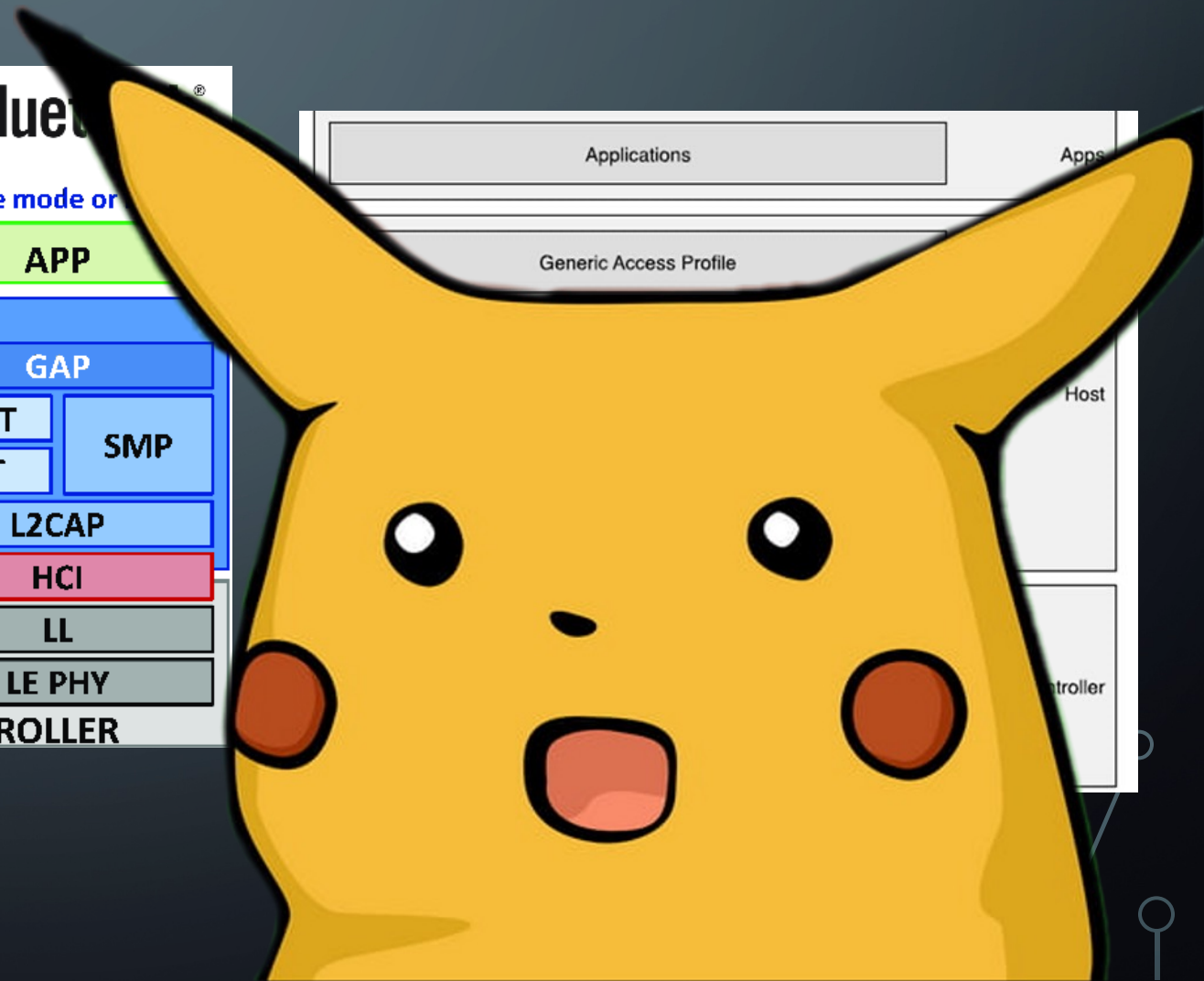
- Frequency Hopping Spread Spectrum (FHSS)
  - Anti- Jamming Method
- George Antheil
  - Pianist
- Radio Controlled Torpedoes
- Self playing piano
- Patent 1942

- Netflix
  - Bombshell: The Hedy Lemarr Story

BLUETOOTH PROTOCOL STACK

- Protocol Stack
- Service Discovery Protocol
  - UUID's



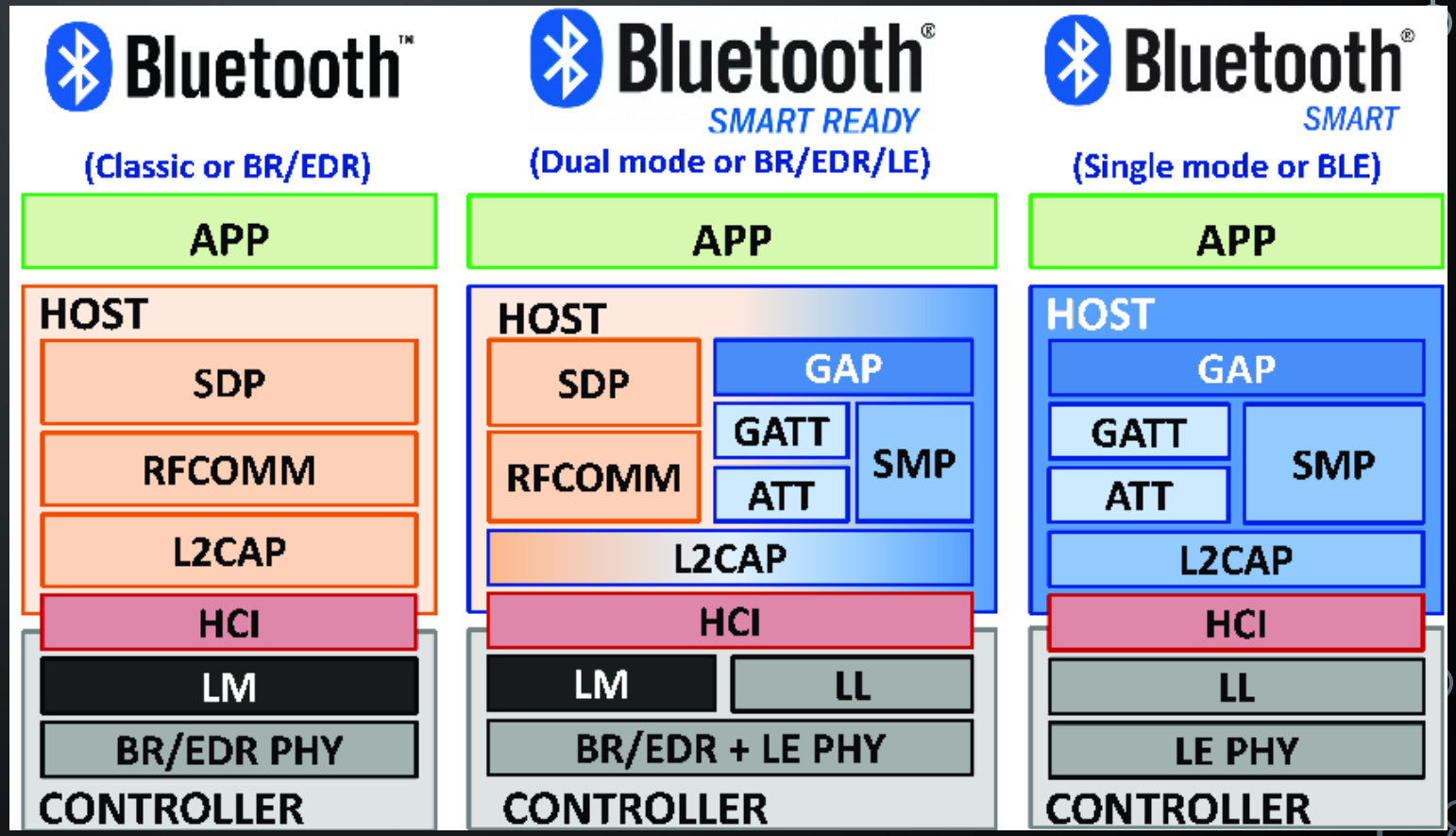


BASIC TERMS

- Devices:
  - Central
    - Connection Initiator
    - Controls timing and data exchange
  - Peripheral
    - Advertises
    - Accepts incoming connections

BLUETOOTH PROTOCOL STACK

- Generic Access Profile
  - Advertising and connections
- GATT Generic Attribute Profile
  - Profiles
  - Services
  - UUIDS
- ATT
  - Opcodes
- Security Management Profile
  - Controls Pairing and Bonding sessions



BLE SECURITY

- BLE 4.0 – Introduced Encrypted Sessions with 4.2
  - MITM
  - Eavesdropping
  - Authentication via Pairing/Bonding
- BLE 5.0
  - Strengthens “Just-Works” pairing by introducing nonce keying

BLE GATT

- Service – (Full UUID)
  - Characteristics – (Full UUID)
    - Properties – (Read/Write/Notify)
    - Descriptors –(Short UUID)
    - Value – The data that affects device operation
- Catalog of services on a device

GATT "HACKING"

- Abuse Read Privileges
  - Device Details – (iOS: Battery level, User name, OS version)
- Abuse Write Privileges
  - Simple GATT Value Examples
    - 0x08 – Write New Pin
    - 0x01 – Initialize OTA Firmware Update
    - 0x02 – Start Heating Cycle

TOOLS

- nRF Connect
- Nordic 52840 dongles
- UD100 Dongle

NRF CONNECT

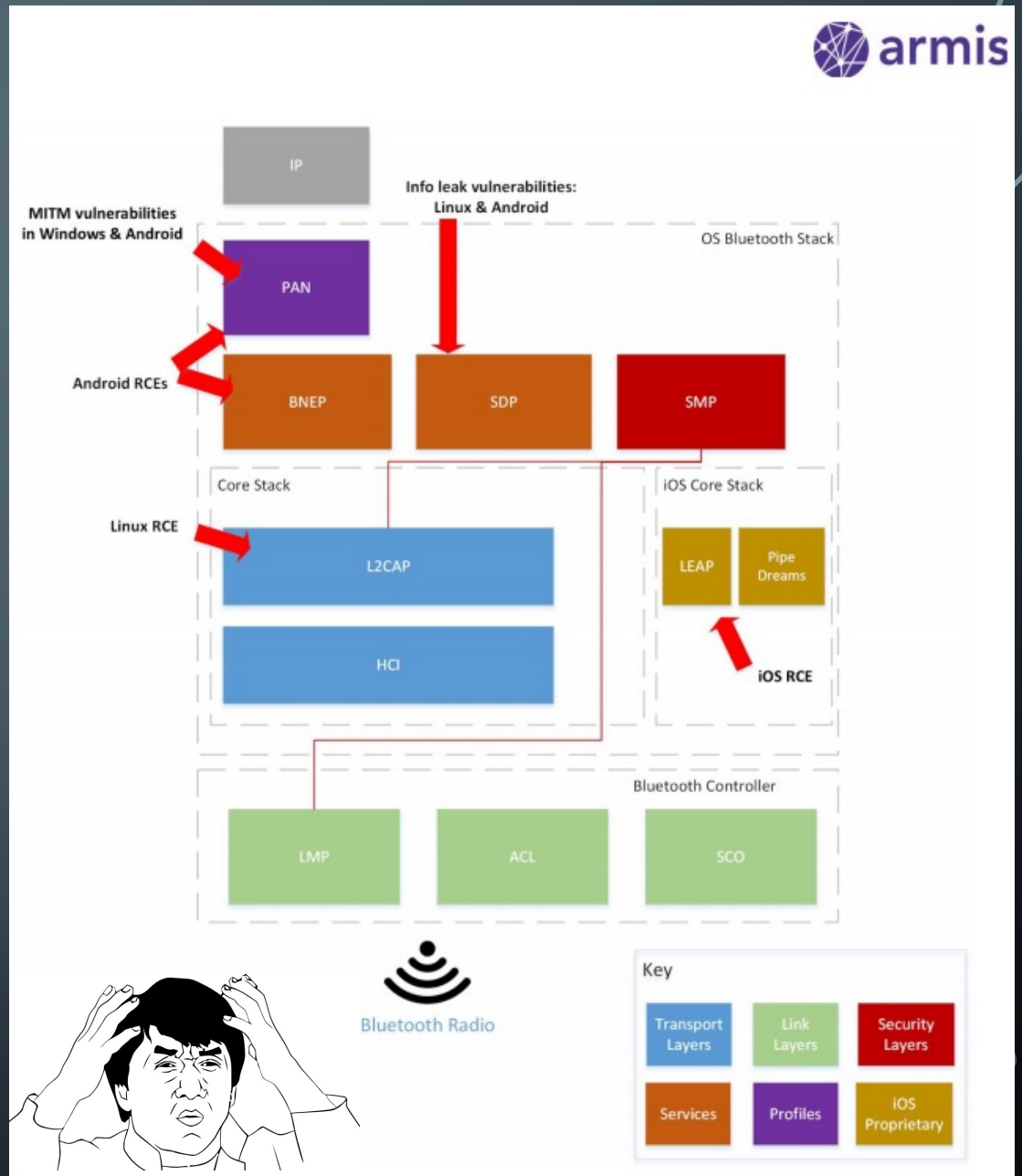
- Free application for iOS/Android/PC
- Intended for BLE debugging
- Great for BLE “Hacking”!
- Creates log files that can be exported
- Records Macro functions for basic scripting capabilities

BLUETOOTH VULNERABILITIES

- Blueborne
  - Armis, 2017
  - Windows, Android, iOS
  - https://www.armis.com/blueborne/
- Bleedingbit
  - Armis, 2018
  - Aruba, Cisco
  - https://www.armis.com/bleedingbit/
- SweynTooth
  - Feb 2020
  - Singapore University of Technology and Design
  - 12 vulnerabilities (Crash, Deadlock, Security Bypass)
  - 6+ Vendors

BLUEBORNE

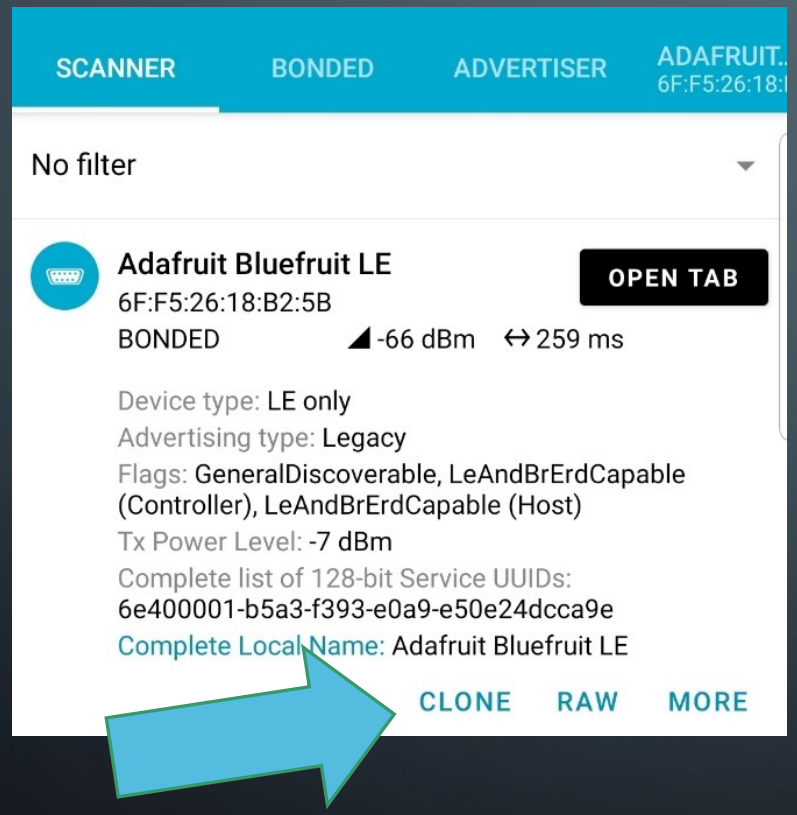
- PAN
- BNEP
  - Delivers packets on top of L2CAP
  - Used by PAN
  - Identifies protocols
- SDP
  - Device Services
  - UUID's
- L2CAP
  - Passes packets to HCI or Link Mangr/ ACL link
  - Multiplexing between layers
  - Packet Segmentation and reassembly
- LEAP

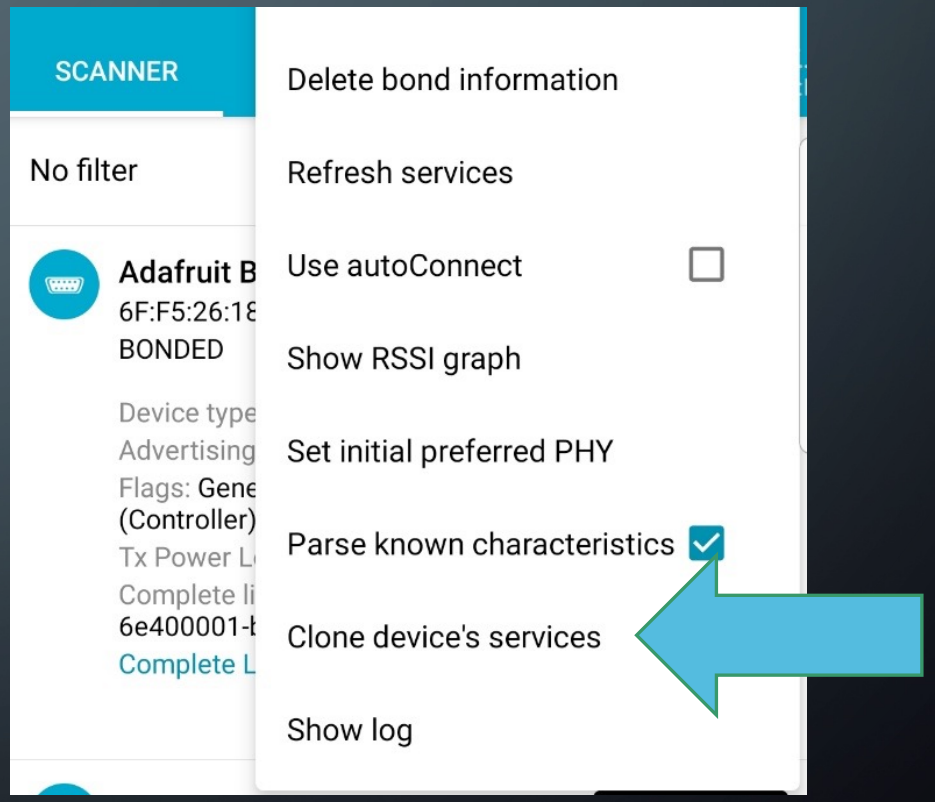


Basic blocks in the Bluetooth stack, indicating the location of various vulnerabilities

CLONING BLE SERVICES

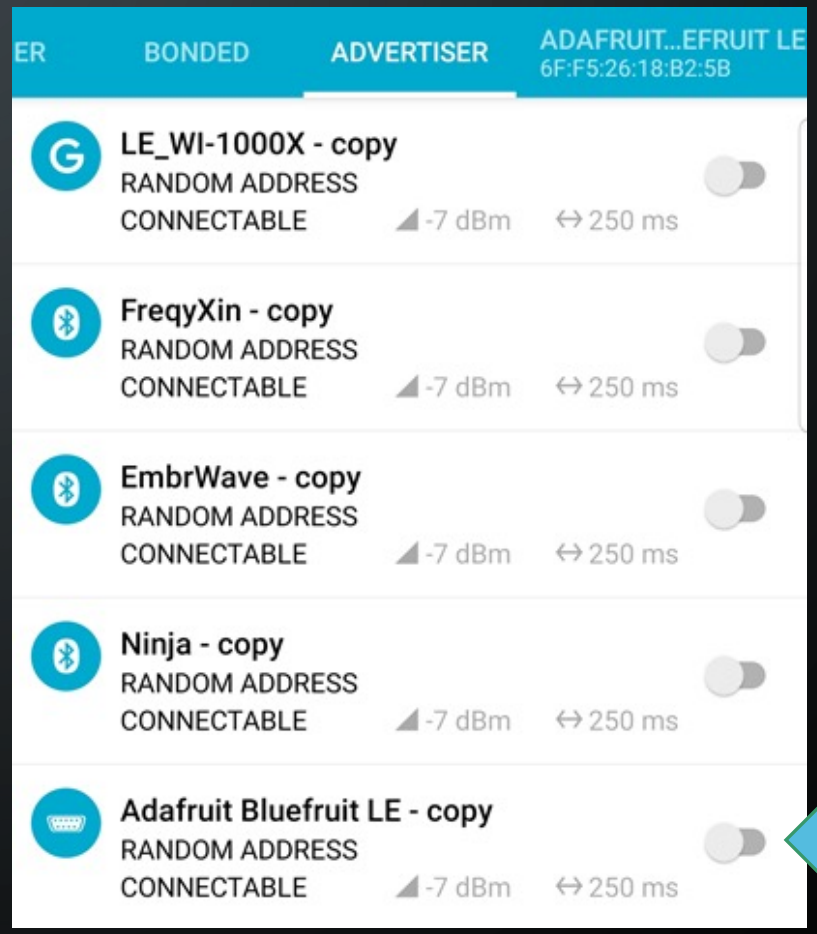
- Target: Adafruit Bluefruit LE
  - Spoofing BLE device to trick mobile application with nRF Connect





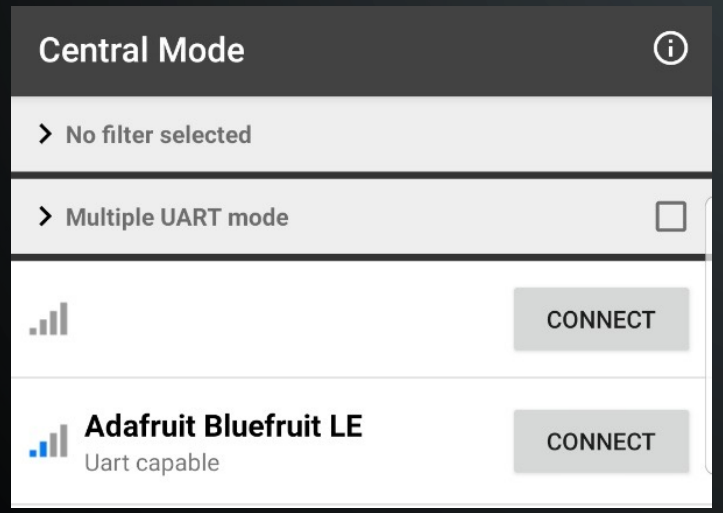
SPOOFING BLE DEVICE

- Use cloned device details
- Change device name
- Wait for connection

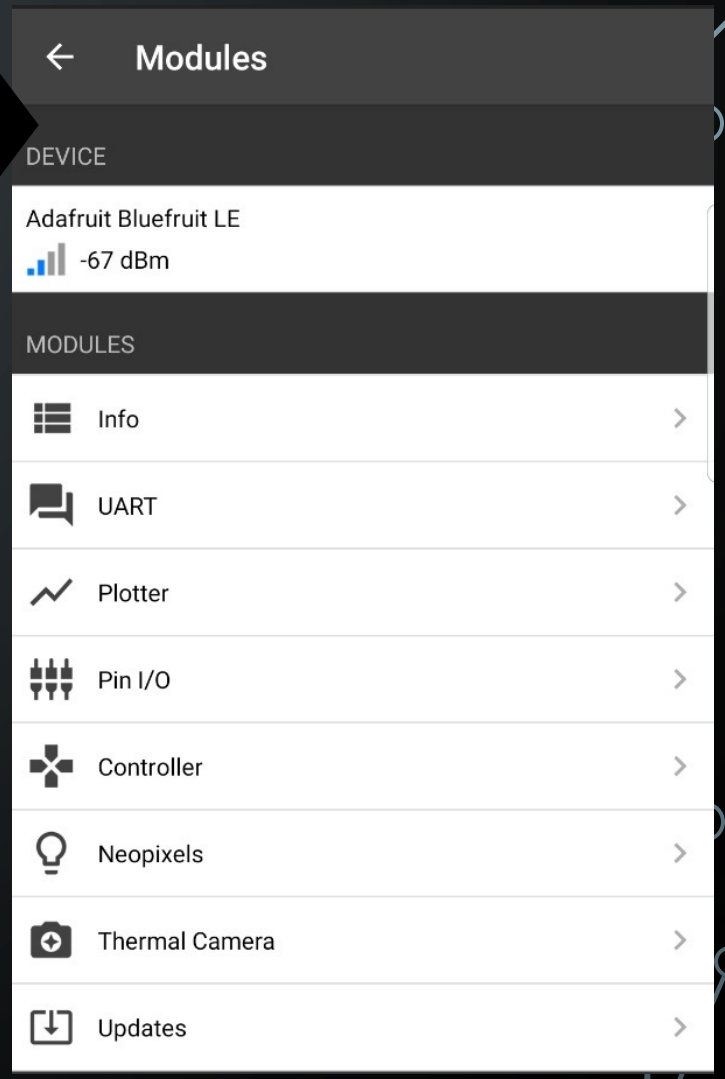


CONNECTION TO BLE SPOOF

- View from victim
  - Adafruit Bluefruit Connect App



Success!



BLUETOOTH DEMO

ZIGBEE

- Uses mesh topology
  - Designated “Coordinator” used to grant mesh network access
- Commonly utilized for static sensor installs
  - Building HVAC
  - Lighting
  - Wireless Sound System Configuration

KILLERBEE

- API-Mote
  - https://www.attify-store.com/products/apimote
- https://github.com/riverloopsec/killerbee

SOFTWARE DEFINED RADIO (SDR)

- RTL-SDR Dongle
- Universal Radio Hacker
- BladeRf A4
- Crazy Radio PA
  - MouseJack

MOUSEJACK

Freqy 🏳️‍🌈 ☠️
@FreqyXin

Not only did I work at place that started doing this, but they did so because I discovered they had about 6k vulnerable devices deployed in NA alone.

🖱️mousejack💋🖤

It's a fun story I should tell sometime. There was much anger.

> **Paul Crickard** @pcrickard · Sep 17
> Does anyone work at a place that inventories your keyboard and mouse?

7:26 PM · Sep 17, 2020 · Twitter for Android

MOUSEJACK

- Bastille Labs
- Targets 2.4Ghz Non-Bluetooth HID
- Logitech & Microsoft most greatly affected

HARDWARE

- Bitcraze -- CrazyRadio PA
- https://hackerwarehouse.com/product/crazyradio-pa/

JACKIT

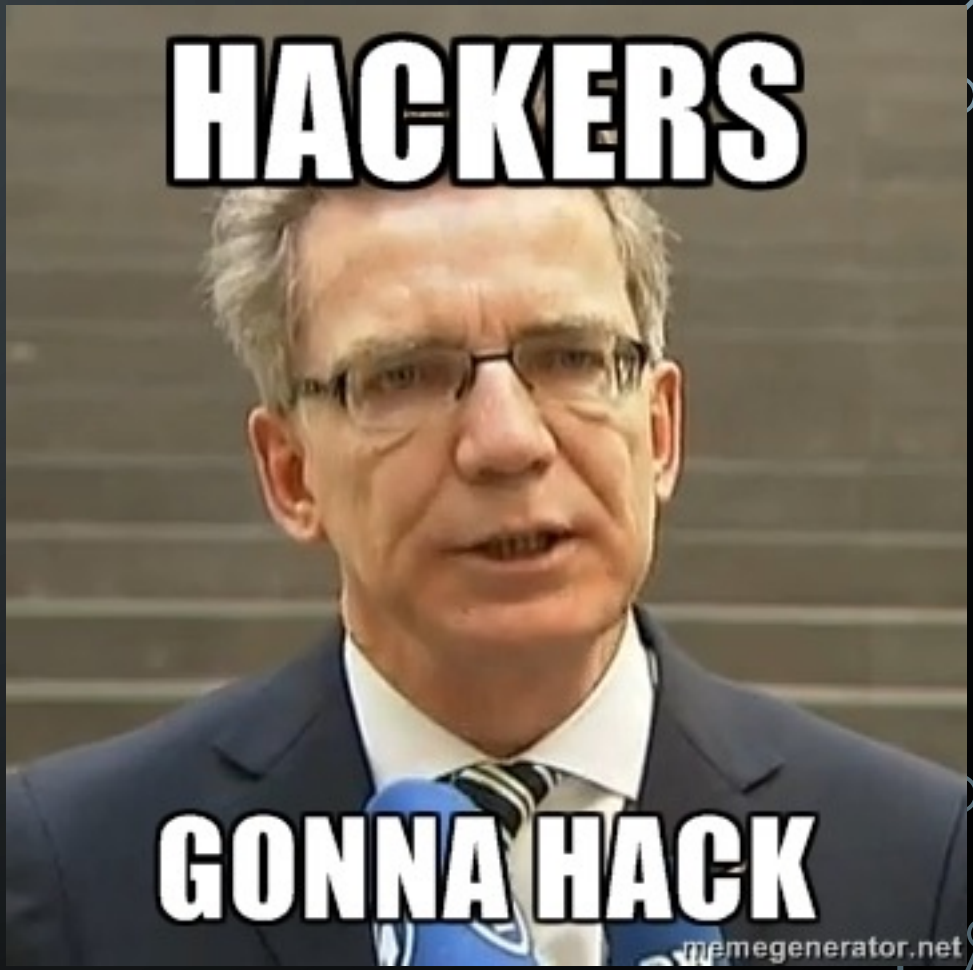
- https://github.com/insecurityofthings/jackit
- Scans for vulnerable devices
- Deliver Ducky script payloads to vulnerable devices

STORYTIME -- SUMMER 2018

- Junior Year – UW
- Previous BLE exploit Demo
- SOC Malware Analyst
- Large Digital Solutions Company

DISCOVERY

- Scanning with Crazy Radio
- ‘Issued’ Logitech Mouse
- Pwnd myself



Applications Places Terminal Sat 17:20

root@kali: ~/jackit

File Edit View Search Terminal Help

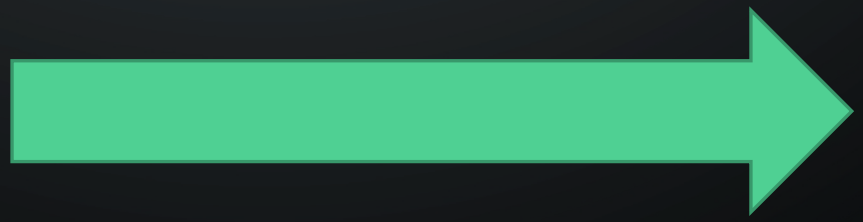
```
root@kali:~/jackit# jackit --script examples/nyan_troll_windows.txt
```

EXPLOITATION

- How often does your boss say, “prove it”, and then you hack them

CLEAN-UP & DETECTION

- MSDATP
  - Advanced Hunting
    - https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-atp/advanced-hunting-query-language
    - Org-Wide Registry Alert
    - 30-day log limit
    - PowerShell to dump USB HID Registry Keys
- Asset tracking




BURGER
3.95
OUR
EMADE
UPS

THE NUMBERS

- 6K+ Corp devices in North America
- Another 4K+ suspected world-wide

- Thousands of employee devices

- ~$100K in combined direct equipment loss

- 1 x multi-million dollar Cyber-Defense system

- 1 x $30 dongle

RFID

Band	Regulations	Range	Data speed
120–150 kHz (LF)	Unregulated	10 cm	Low
13.56 MHz (HF)	ISM band worldwide	10 cm–1 m	Low to moderate
433 MHz (UHF)	Short range devices	1–100 m	Moderate

Remarks
Animal identification, factory data collection
Smart cards (ISO/IEC 15693, ISO/IEC 14443 A, B). Non fully ISO compatible memory cards (Mifare Classic, iCLASS, Legic, Felica ...). Micro processor ISO compatible cards (Desfire EV1, Seos)
Defense applications, with active tags

NFC

- 13.56 MHz
- Smart Tags
- Key Fobs
- Pay Stations
- Mobile Tap Pay

COMMON RFID/NFC CARDS

- MiFare Classic/Ultralight/DES
  - 13.56 MHz
  - DES is currently uncracked
  - Ultralight cracking requires interaction with reader

- HID ProxCard II
  - 125 kHz
  - Little to no security

PROXMARK


Proxmark3
Iceman Collection
x
Proxgrind
HF_ANT_2.3uH±3%
Dual pocket ANT V6
Center Freq:13.56M
PROXGRIND