RADIO FREQUENCY EXPLOITATION

FLETCHER DAVIS

WHO AM I?

- Senior at George Mason University
- Majoring in Cyber Security Engineering
- Gained experience in RF Security and Exploitation through previous internships, personal research, and school education

AGENDA

1. RF Technical Overview/Introduction
2. Methods of RF Exploitation
    1. Presentation on Replay Attack/Demo
    2. Presentation on Jamming/Demo
    3. Presentation on RollJam
    4. Presentation on MouseJack/Demo
3. Closing Remarks/Future of RF

WHAT ARE RADIO FREQUENCIES?

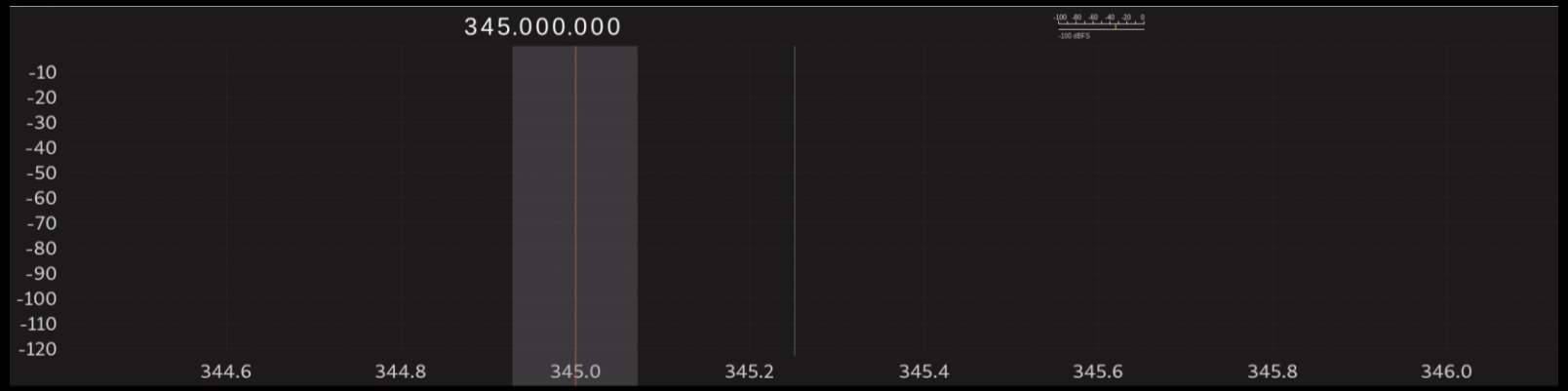
- The Radio Spectrum is comprised of radio waves between 3 kHz to 300 GHz
- Since Radio Signals are waves, they are periodic and have a frequency
- Higher the frequency → Smaller the wavelength → Shorter the distance
- Best-known for their use in wireless communication

Designation	Abbreviation	Frequencies	Wavelengths
Very Low Frequency	VLF	3 kHz - 30 kHz	100 km - 10 km
Low Frequency	LF	30 kHz - 300 kHz	10 km - 1 km
Medium Frequency	MF	300 kHz - 3 MHz	1 km - 100 m
High Frequency	HF	3 MHz - 30 MHz	100 m - 10 m
Very High Frequency	VHF	30 MHz - 300 MHz	10 m - 1 m
Ultra High Frequency	UHF	300 MHz - 3 GHz	1 m - 100 mm
Super High Frequency	SHF	3 GHz - 30 GHz	100 mm - 10 mm
Extremely High Frequency	EHF	30 GHz - 300 GHz	10 mm - 1 mm

SOFTWARE DEFINED RADIOS (SDR)

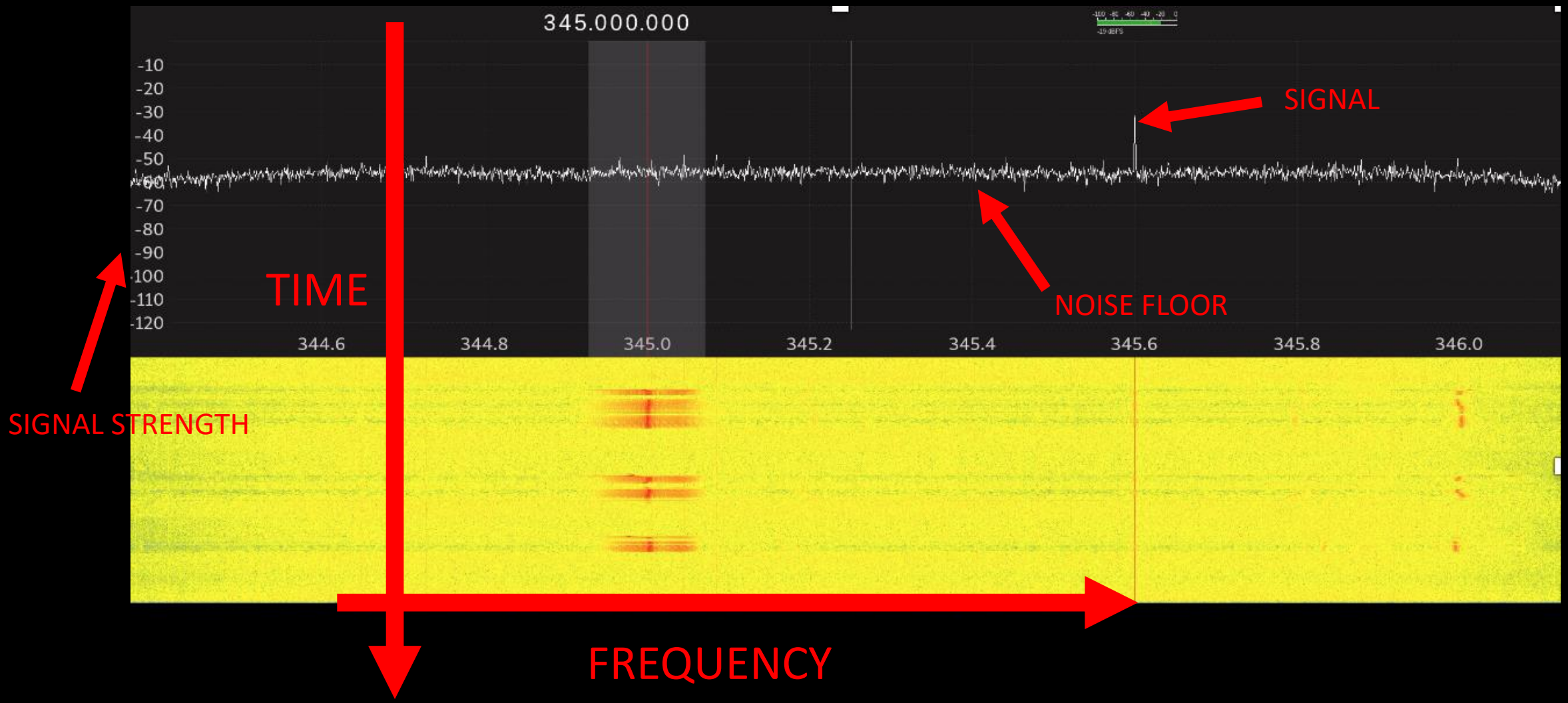
- A radio is any kind of device that wirelessly transmits or receives signals in the radio frequency spectrum
- A SDR is a radio where components that have been traditionally implemented in hardware are instead implemented by means of software on a personal computer or embedded system
- Hardware that can implemented in software are: mixers, filters, amplifiers, modulators/demodulators, and detectors

SPECTOGRAM/WATERFALL



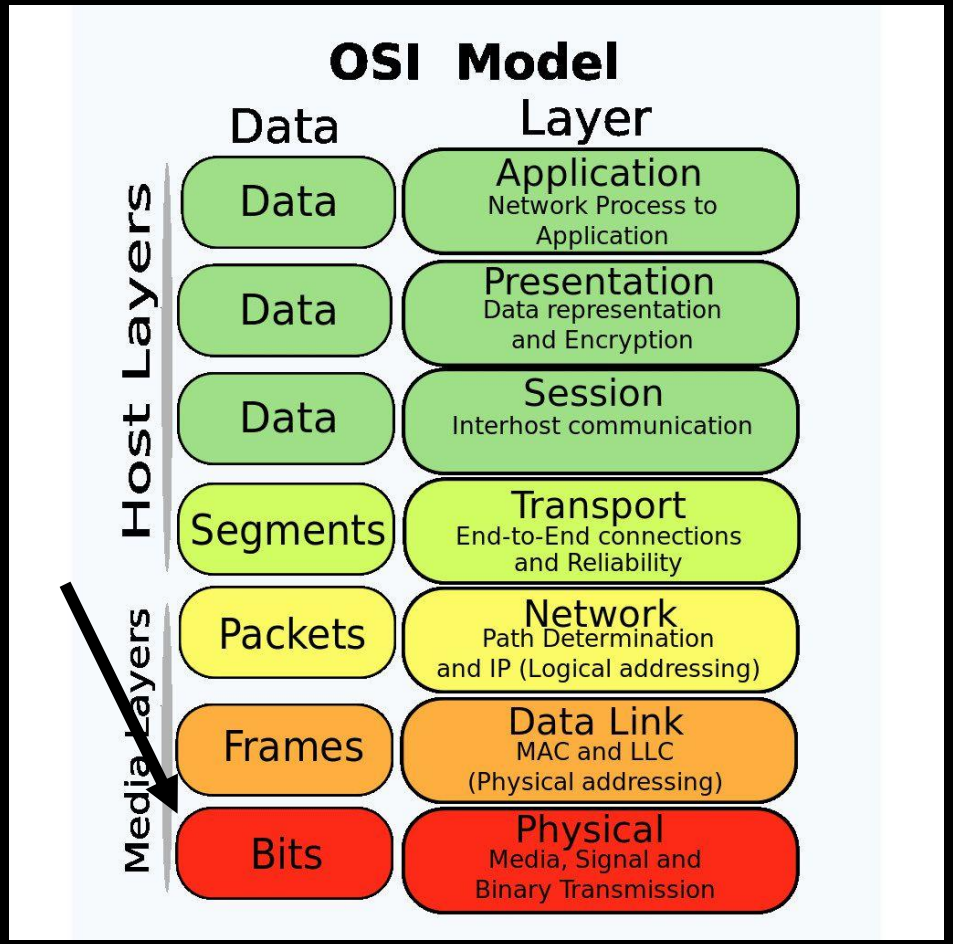
Windows: SDR#/CubicSDR

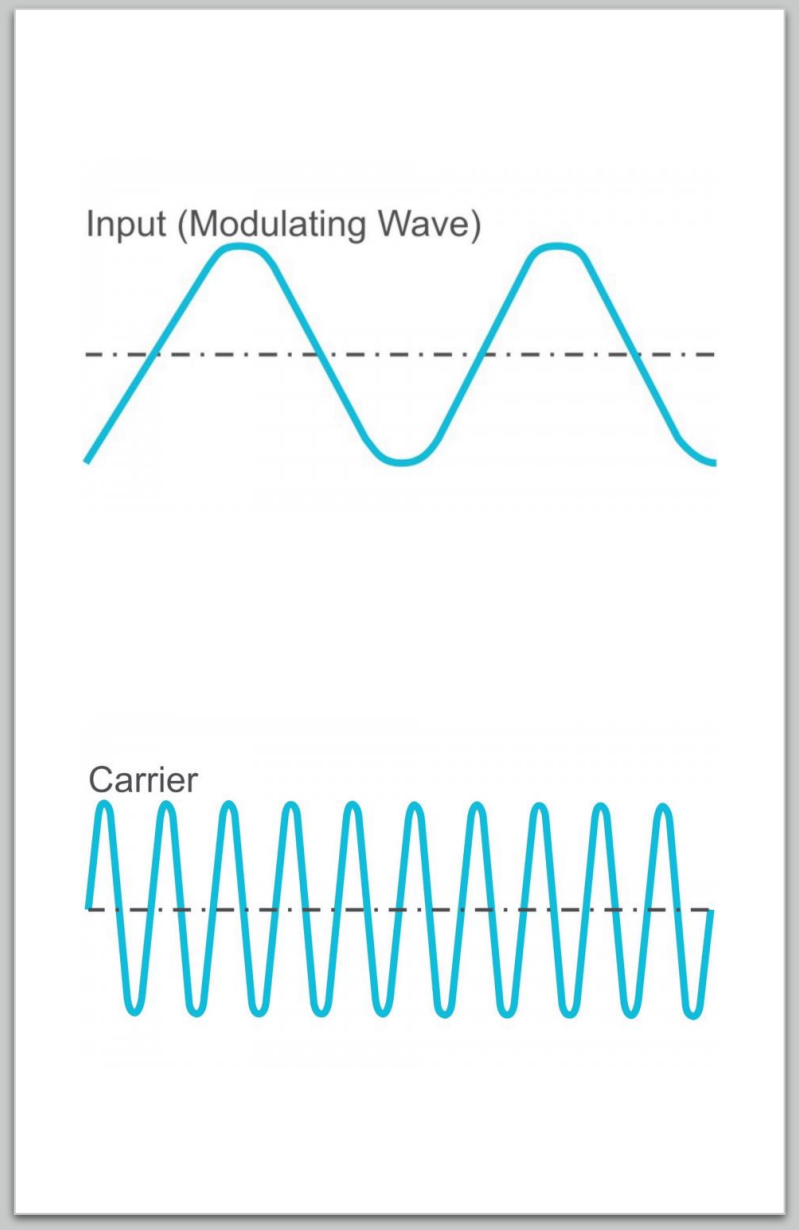
MacOS/Linux: GQRX



PHYSICAL LAYER

- Radio Frequencies are part of the Physical Layer of the OSI Model
- Lowest Layer in Communication Stack
- In Wireless Communication:
  - Bits (1's and 0's) are sent over an RF medium as patterns of energy



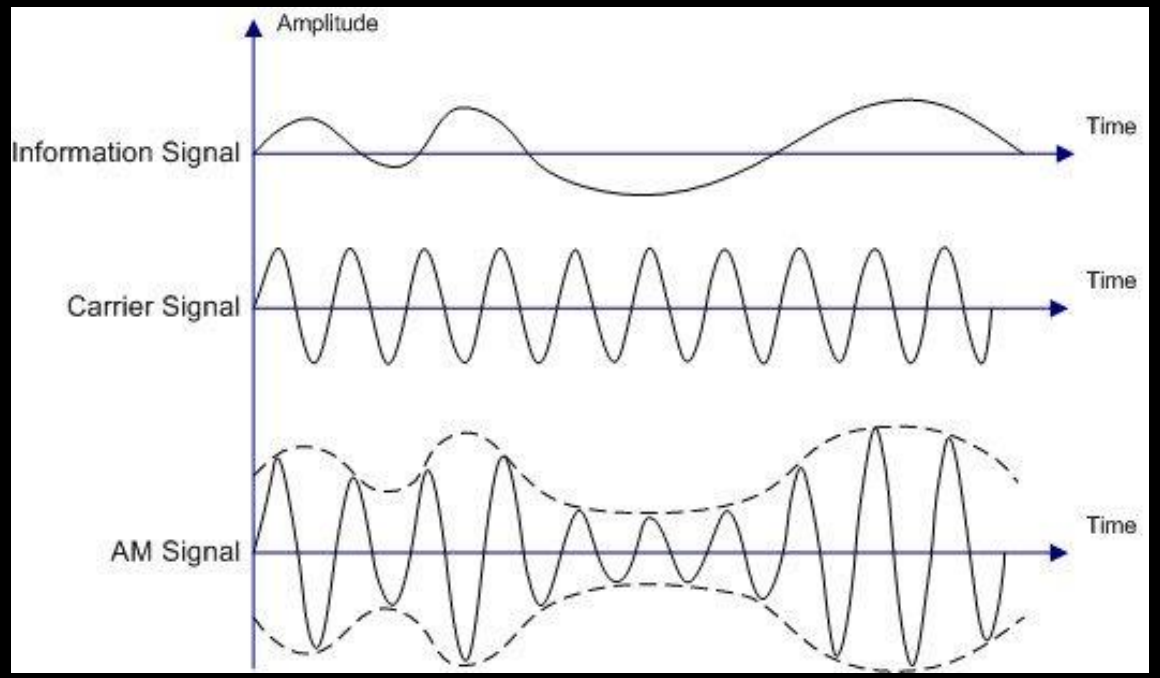


MODULATION

- A carrier wave is a pure wave of constant frequency, a bit like a sine wave.
- By itself it doesn't carry much information that we can relate to (such as speech or data)
- To include speech information or data information, another wave needs to be imposed, called an input signal.
  - This process of imposing an input signal onto a carrier wave is called modulation.

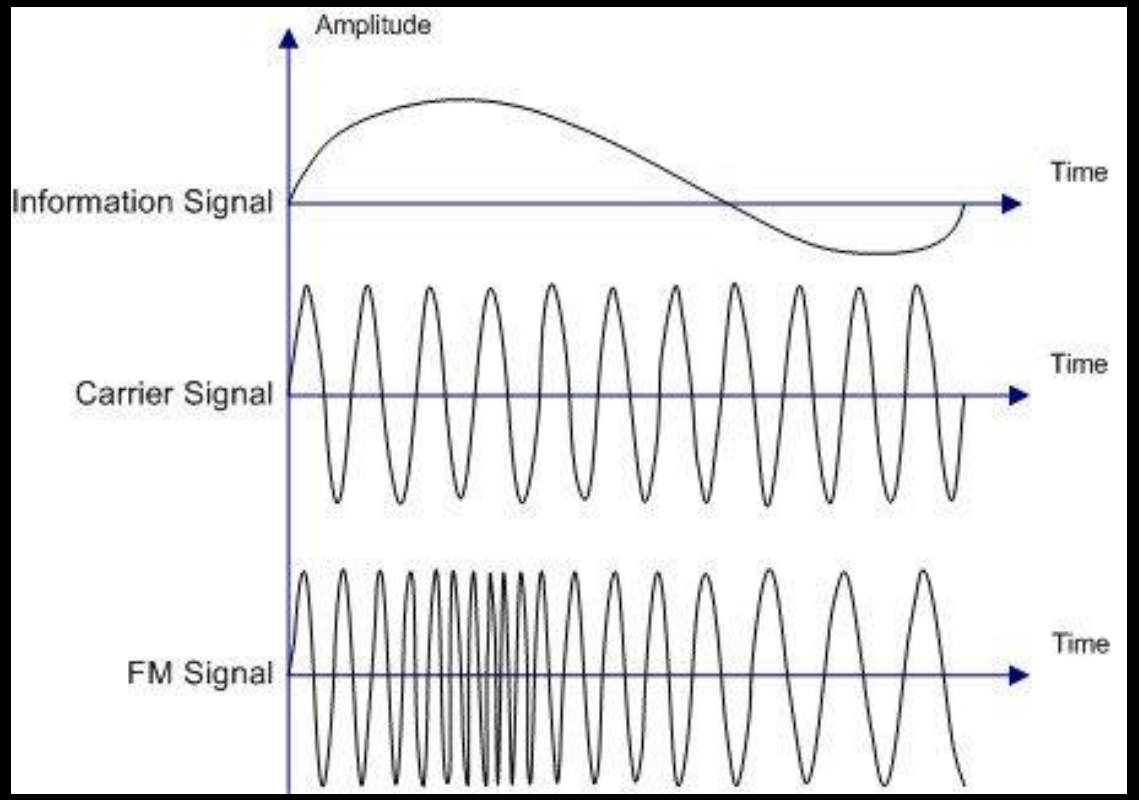
AMPLITUDE MODULATION (AM)

- The amplitude of the carrier wave is modified proportionally according to the amplitude of the input signal
- AM radios do not need complicated demodulators and costs were reduced
- Frequency Range: 535 to 1705 Kilohertz



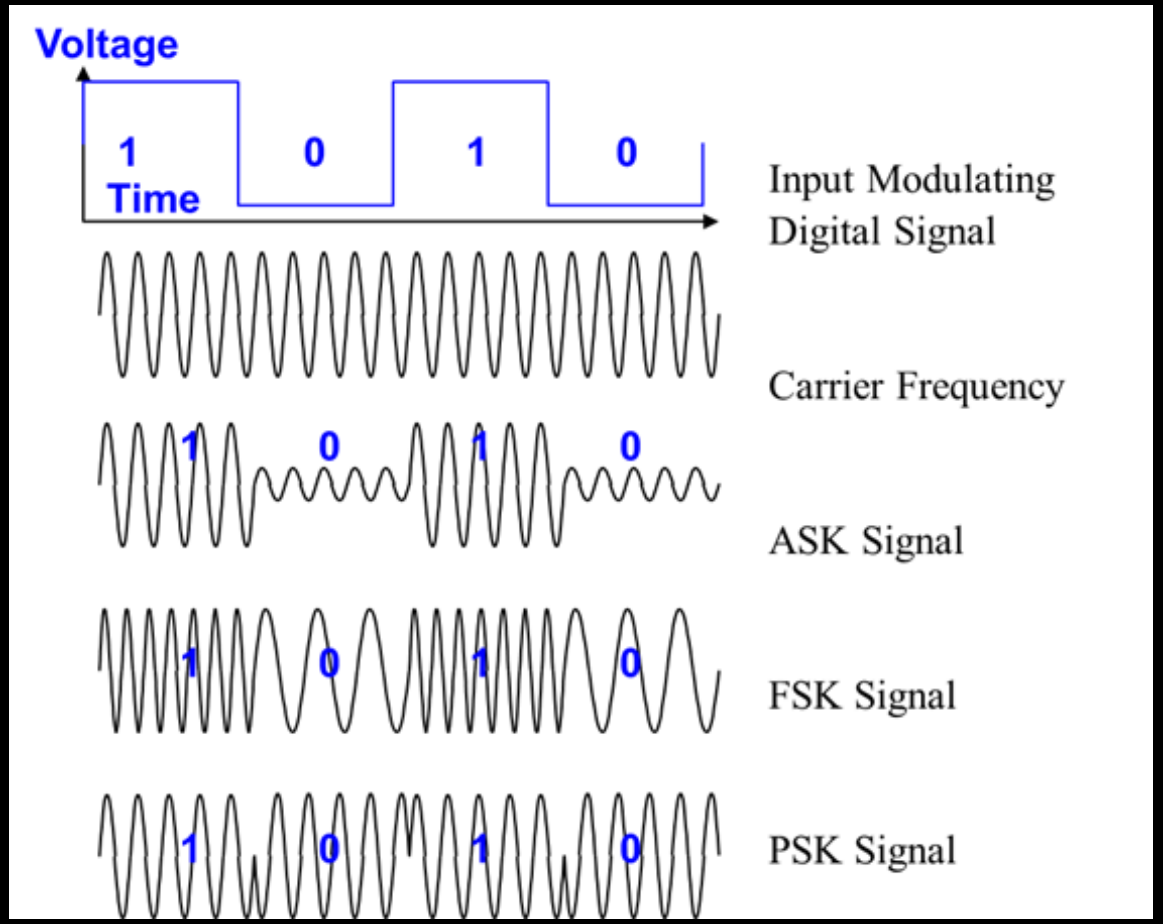
FREQUENCY MODULATION (FM)

- The instantaneous frequency of the carrier wave is altered according to the amplitude of the input signal.
- Demodulation process is more complicated than AM
- Frequency Range: 88-108 Megahertz



DIGITAL MODULATION

- Analog signal carrying digital data
- Data is sampled at some rate and then compressed and turned into a bit stream
  - A stream of 1s and 0s
- This bit stream is then created into a square wave which is then superimposed on the carrier.



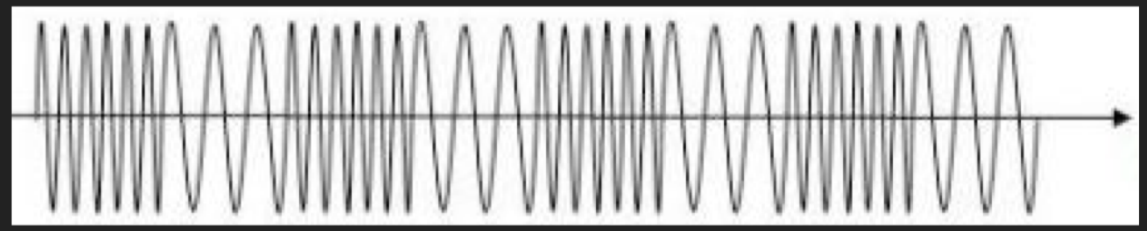
HOW TRANSMITTING WORKS

MAC Frame			
HW Addresses	Sequence Number	(other stuff)	Layer 3 Frame

Layer 2 (MAC)

PHY Frame						
Preamble	Start of Frame Delim.	PHY Header	+	MAC Frame	+	CRC

Modulation (Maps 1s and 0s to electrical phenomena)

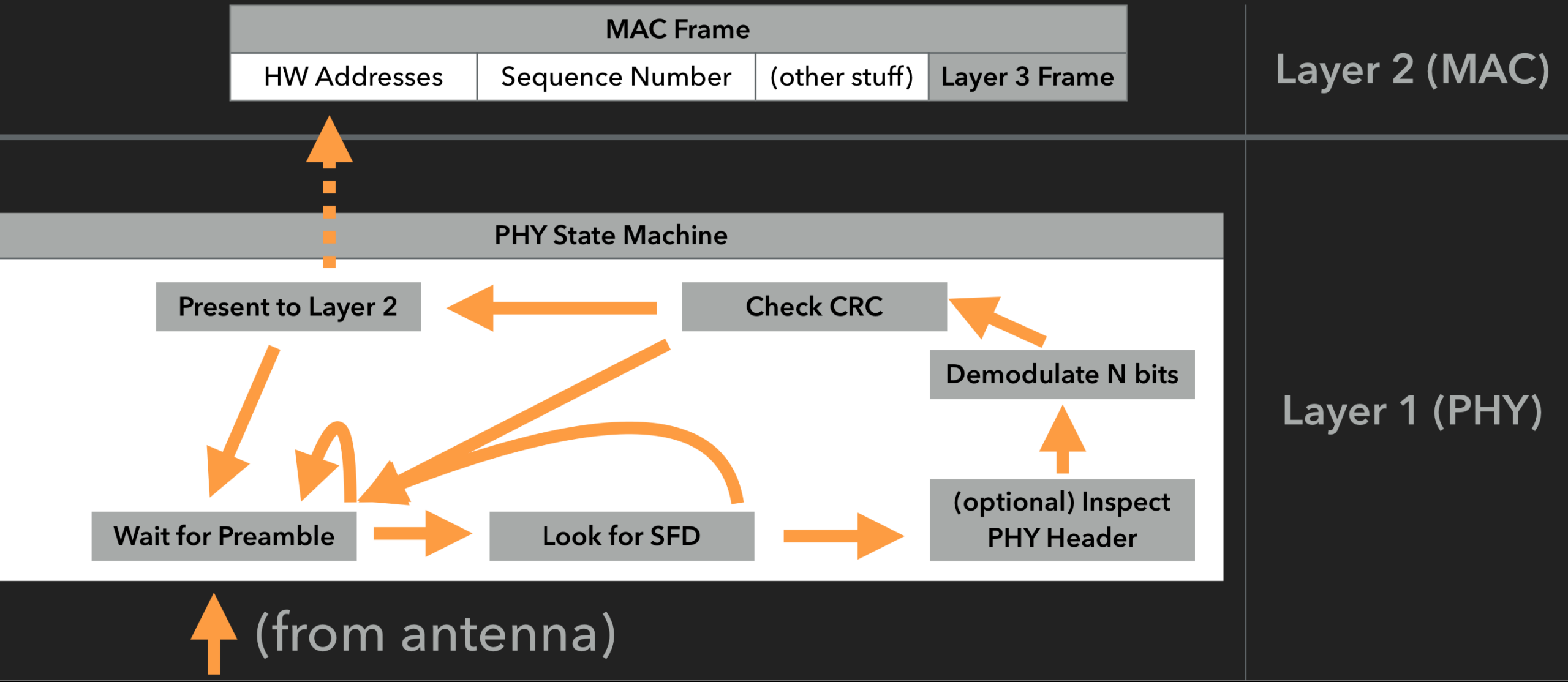


(to antenna)

Layer 1 (PHY)

Source: https://paper.seebug.org/papers/Security%20Conf/Defcon/2017/Matt%20Knight%20and%20Marc%20Newlin/DEFCON-25-Matt-Knight-and-Marc-Newlin-Radio-Exploitation.pdf

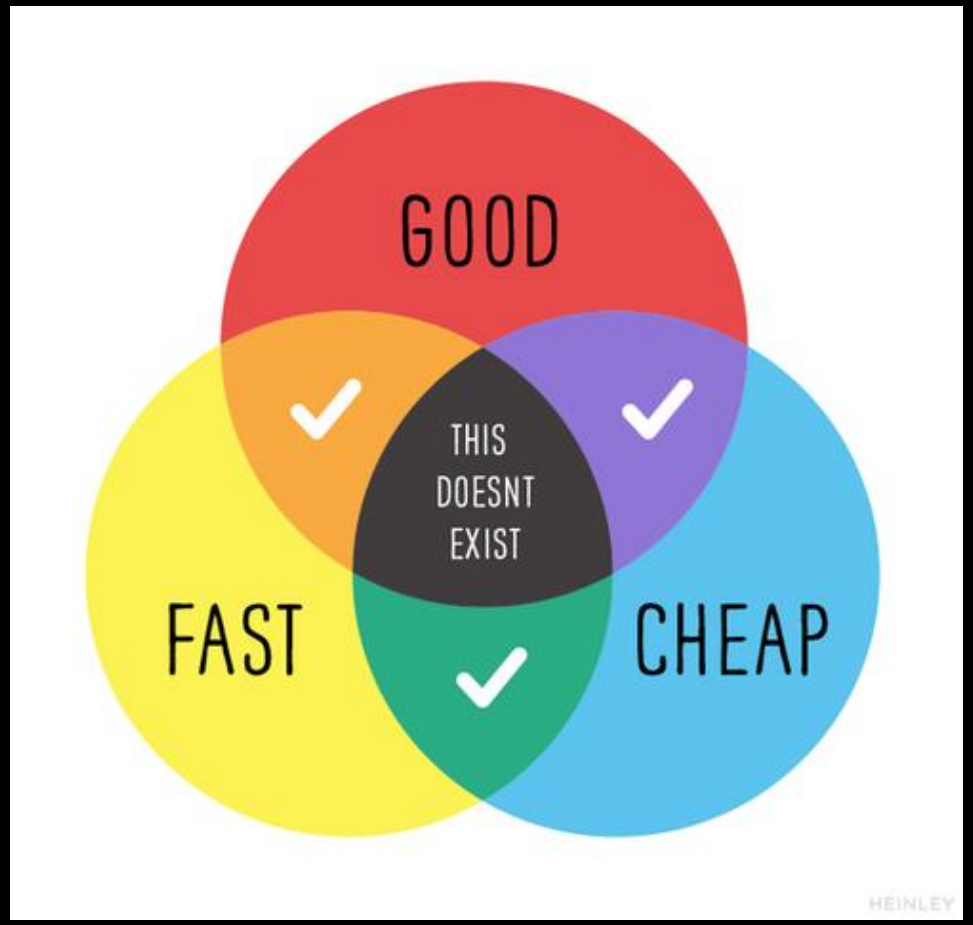
HOW RECEIVING WORKS



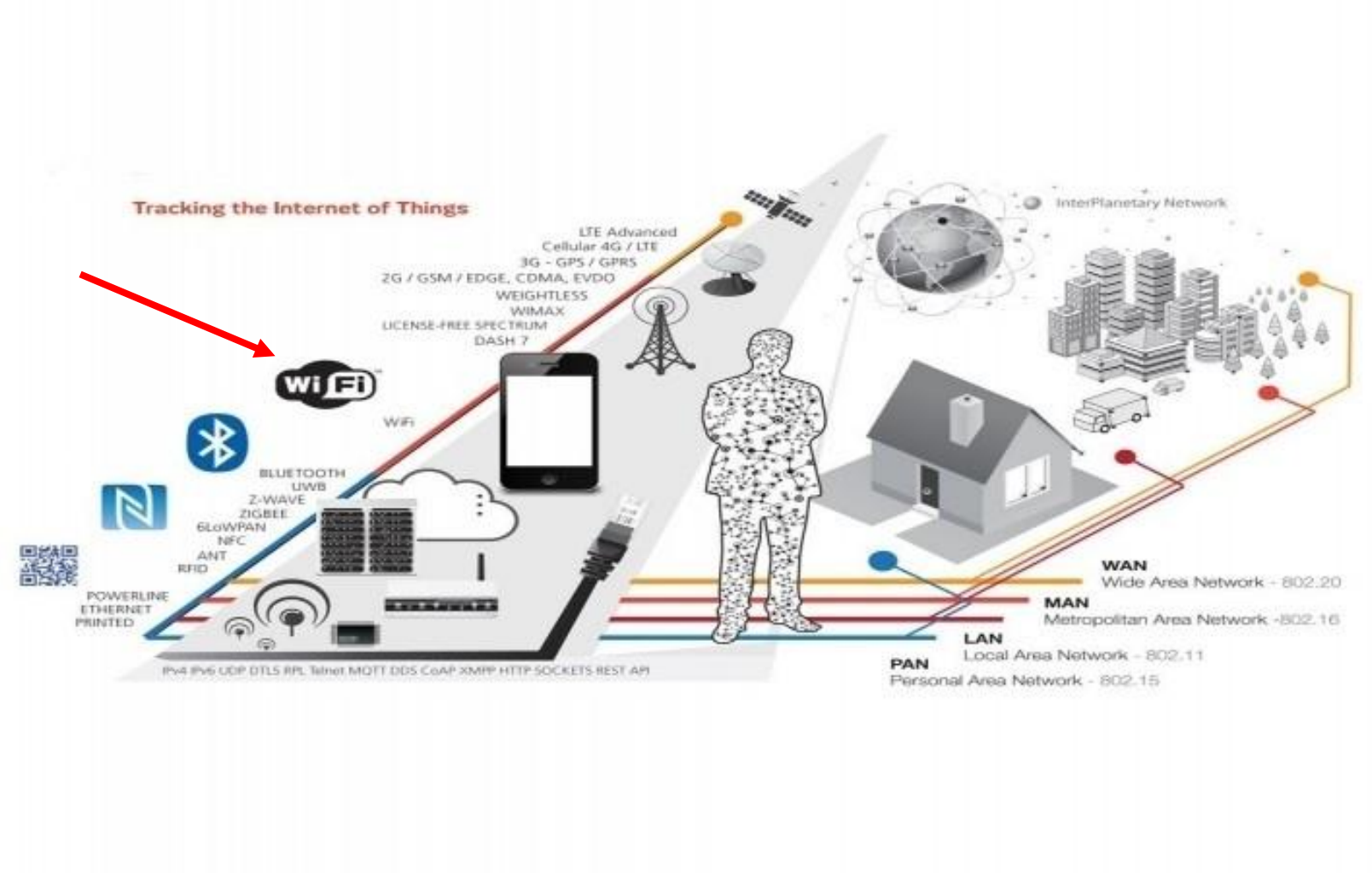
Source: https://paper.seebug.org/papers/Security%20Conf/Defcon/2017/Matt%20Knight%20and%20Marc%20Newlin/DEFCON-25-Matt-Knight-and-Marc-Newlin-Radio-Exploitation.pdf

WHY IS RF SECURITY SO IMPORTANT?

- Wireless Devices are everywhere!
  - Estimated 50 billion IOT devices by 2020
- Internet of Things
  - Connected Embedded Devices
  - Vulnerable by hardware/software constraints
- Hardware: Small, Inexpensive
  - Limits connectivity and encryption
- Software: Legacy Compatible, Easily Configurable
  - Difficult to update and secure



INTERNET OF THINGS



METHODS OF RF EXPLOITATION

REPLAY OVERVIEW

- An attacker captures transmission of interest that correlates with an action they wish to induce on a target and replays that transmission to induce that action
- Can be either raw IQ spectrum capture or a decoded packet payload
- Software Defined Radio replays the captured transmission

REPLAY COUNTERMEASURES

Replay attacks can be defeated by enforcing cryptographic authentication and freshness

Cryptographic authentication allows two endpoints to validate their authenticity

Freshness refers to tracking a sequence number within a message frame. When combined with cryptographic authentication, it makes replay attacks much harder to execute

REPLAY DEMO

JAMMING OVERVIEW

- An attackers transmits noise or conflicting traffic at the same frequency as a target with sufficient bandwidth and power
- Software Defined Radio sends arbitrary packets
- Denies legitimate network traffic/Disrupts network state
- Ex. Think it like someone yelling over you while you talk

JAMMING COUNTERMEASURES

From an attacker's perspective, jamming is self-defeating because it denies an attackers ability to monitor transmissions on a jammed network

Defenders can mitigate jamming with the implementation of a jam detection system or frequency hopping mechanism

Jamming detection systems compare the incoming radio signal with the expected signal strength and other signal factors

Frequency hopping mechanisms transmit radio signals by rapidly switching frequency channels using a pseudorandom sequence known by the transmitter and receiver

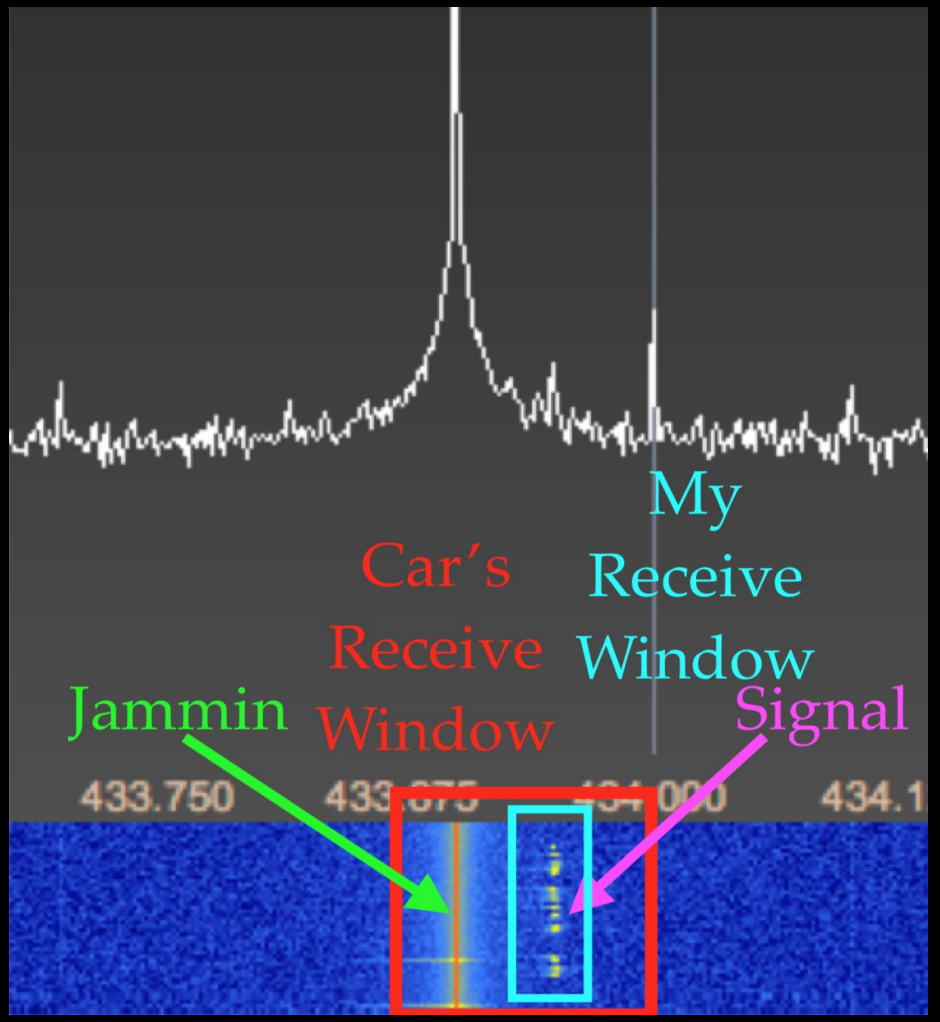

JAMMING DEMO

ROLLJAM OVERVIEW

- Rolling Code:
  - Pseudorandom Number Generator in Key and Car
  - Synced Seed + Counter → Increments after every press
- Hit Button → Key Sends Code
- Hit Button Again → Key Sends Next Code
- If an attacker were to replay the first code, the car would reject it because it has already been used
- Difficult to predict and prevents replay attacks

ROLLJAM OVERVIEW

- An attacker would jam at a slightly deviated frequency, then receive the key fob signal, filtering the jam
- Wait till the victim presses the key twice, then replay the first code
- Save the second code for later when the attacker wants to unlock the car



ROLLJAM COUNTERMEASURES

Encrypt/Hash the Key Fob signal

Use a Time-Based Algorithm

Implement a challenge/response via transceivers instead of one-way communication

Many key fobs are RX+TX, yet they only utilize one-way communication and lack encryption/time-based algorithms

ROLLJAM DEMO

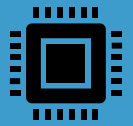

#CarTheft
Pandora

MOUSEJACK OVERVIEW

- MouseJack is a class of vulnerabilities that affects the vast majority of wireless, non-Bluetooth keyboards and mice.
- These peripherals are “connected” to a host computer wirelessly using a radio transceiver
- Mouse movements are usually sent unencrypted
- An attacker can launch an attack from up to 100 meters away, injecting keystrokes and ultimately taking control of a target computer

MOUSEJACK COUNTERMEASURES

There are two types of nR24L chips used by keyboards, mice, and dongles: one-time-programmable and flash memory



One-time-programmable devices can not be updated once they leave the factory and the only security mechanism is to unplug the device

Flash memory devices can be secured through firmware updates. It is recommended to install the update before using the device

MOUSEJACK DEMO

CONCLUSIONS

- As wireless devices continue to integrate into our digital lives and assume critical functions in society:
  - It is necessary device manufacturers/integrators consider the security risks that come with these devices
- Understanding wireless security and its vulnerabilities today allows us to secure communications for years to come

ACKNOWLEDGMENTS

Matt Knight and Marc Newlin

- Security Researchers @ Bastille
- Marc Newlin discovered the MouseJack vulnerability in 2016

Samy Kamkar

- Security Researcher
- Developed RollJam
- Got me interested in Radio Frequencies and RF Security

RESOURCES

- https://www.livescience.com/50399-radio-waves.html
- https://www.allaboutcircuits.com/textbook/radio-frequency-analysis-design/radio-frequency-modulation/the-many-types-of-rf-modulation-radio-frequency/
- https://conference.hitb.org/hitbsecconf2016ams/materials/D1%20COMMSEC%20-%20Marc%20Newlin%20-%20Applying%20Regulatory%20Data%20to%20IoT%20RF%20Reverse%20Engineering.pdf
- https://paper.seebug.org/papers/Security%20Conf/Defcon/2017/Matt%20Knight%20and%20Marc%20Newlin/DEFCON-25-Matt-Knight-and-Marc-Newlin-Radio-Exploitation.pdf
- https://samy.pl/defcon2015/2015-defcon.pdf
- https://www.bastille.net/research/vulnerabilities/mousejack

THANK YOU

https://github.com/IAmSecurity