FLORIDA TECH
FLORIDA'S STEM UNIVERSITY™

Department of Computer Science

CSE 4820: Wireless and Mobile Security

13. Software Defined Radios

Dr. Abdullah Aydeger
Location: Harris Inst #310
Email: aaydeger@fit.edu

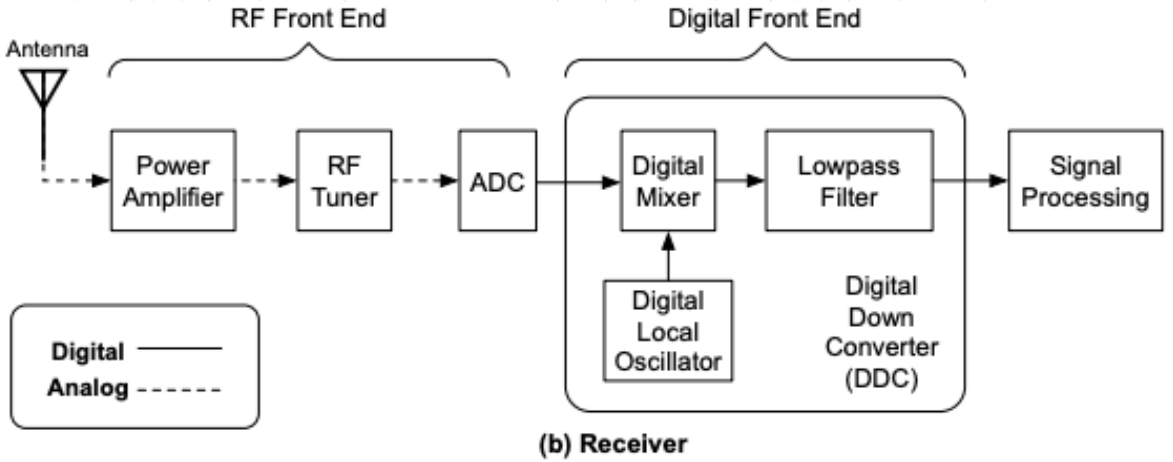
Outline

SDR

Software Defined Radios

- The process of reverse engineering a radio signal to understand elements such as frequency, modulation, encoding, and protocol in order to intercept or replicate the signal
  - For ex. replace sound waves with radio waves
    - By using special 'radio soundcard', you can receive and transmit arbitrary signals
- Has redefined wireless hacking
  - Instead of being limited by black box radios, unfettered access to RF
    - Access to Radio modules/protocols that were obscured

SDR Architecture



- Three main parts:
  - Radio Frequency (RF) amplifier, the tuner, and the Analog-to-Digital Converter (ADC)
- RF amplifier is responsible for boosting weak signals
- Tuner; select portion of radio spectrum to analyze
  - Like tuning on an old radio
- ADC; sampling (analog waveform to stream of digital numbers
- Antennas; isotropic (any direction) or directional

Choosing SDR

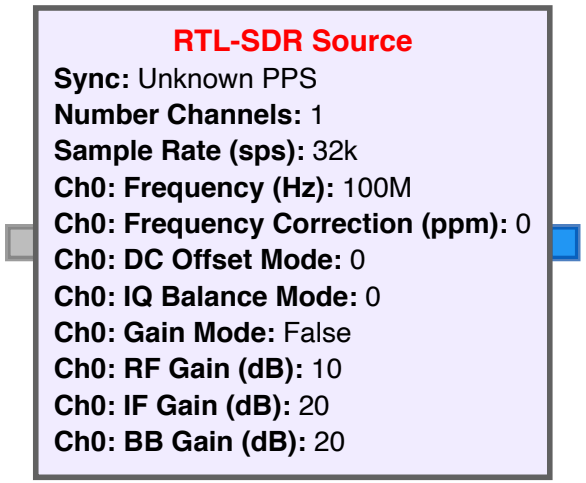
- Sample Rate/Bandwidth:
  - Maximum bandwidth you are able to view simultaneously
  - Measured in MSPS (Millions of samples per second)
  - For 802.11b/g, at least 20 MSPS, however 2 MSPS is fine for most
- Dynamic Range/ADC Resolution:
  - Similar to contrast ratio and dots-per-inch on TVs
  - Higher ADC lets you view loud and quiet signals together

Choosing SDR

- Transmit Capability:
  - Some SDRs are receive only
  - Full (transmit/receive at the same time) or half duplex
- Tuner Range
  - What frequencies you are able to receive

RTL-SDR

- Digital Video Tuner converted into SDR
- Receiver only
- Frequency Range: 50MHz to 1.7GHz
- ADC: 8 bits
- Popular among hobbyist due to low cost
- RTL-SDR Source block available in Gnuradio



https://amzn.to/321mYwB

HackRF

- Wide Band Software Defined Radio (SDR)
- Half-duplex transceiver
- Frequency Range: 10MHz to 6GHz, ADC: 8 bits
- Power: 30 mW - 1 mW (depending on band)
- Popular among researchers due to low cost
- Open sourced hardware

https://greatscottgadgets.com/hackrf/one/

Software: GNU Radio

- Gnuradio's modular design allows us to process and prepare signals to test methods of intercepting and replicating the signal
- Helpful blocks: hardware sinks/sources, file sink/sources, modulators, signal multipliers, signal sources, vector sources, variables, and QT Gui sinks

Software: Universal Radio Hacker

- Discussed in Pohl, Johannes, and Andreas Noack. "Universal radio hacker: a suite for analyzing and attacking stateful wireless protocols." 12th {USENIX} Workshop on Offensive Technologies ({WOOT} 18). 2018.
- Complete suite for wireless protocol investigations with native support for many common SDRs
- The URH allows easy demodulation of signals combined with an automatic detection of modulation parameters to identify the bits and bytes that fly over the air

https://github.com/jopohl/urh

Software: Universal Radio Hacker

- URH's protocol reverse-engineering:
  - You can either manually assign protocol fields and message types or
  - Let URH automatically infer protocol fields with a rule-based intelligence
- Finally, URH entails a fuzzing component aimed at stateless protocols and a simulation environment for stateful attacks
- Some examples of using URH to decode signals includes reversing: restaurant pagers, cloning car-key remotes, wireless keyboards, or intercepting weather signals

https://github.com/jopohl/urh

How to try this in wild?

- Finding a target
  - For ex., key fob, garage opener, wireless mouse, and RC car
- Device reconnaissance;
  - Figure out what frequency it uses
- Finding and capturing signal
- Replaying/changing

Device reconnaissance

- All RF devices subject to FCC (Federal Communications Commission) Certificate require registration with the FCC
- They are given an FCC ID
  - Usually it is printed somewhere on the device
- Looking up the FCC ID yields information about the RF signal to include the frequency

2 results were found that match the search criteria:
Grantee Code: B8Q Product Code: ACSCT

Displaying records 1 through 2 of 2.

View Form	Display Exhibits	Display Grant	Display Correspondence	Applicant Name	Address	City	State	Country	Zip Code	FCC ID	Application Purpose	Final Action Date	Lower Frequency In MHz	Upper Frequency In MHz
	Detail Summary			The Genie Company a Division of Overhead Door Corporation	1 Door Drive	Mt. Hope	TX	United States	44660	B8QACSCT	Original Equipment	01/08/1997	390.0	390.0

https://www.fcc.gov/oet/ea/fccid#:~:text=FCC%20ID%20numbers%20consists%20of,string%20representing%20the%20Grantee%2FApplicant.

FLORIDA TECH

FLORIDA'S STEM UNIVERSITY™

Thank you. Questions?

Dr. Abdullah Aydeger