SOFTWARE DEFINED RADIO: WITH EVEN MORE AWESOME

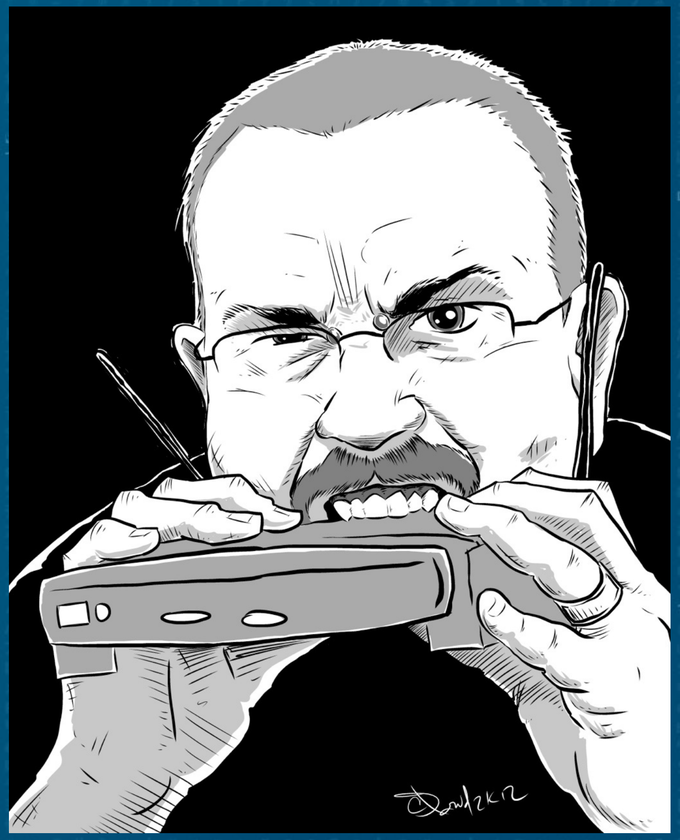
• LIVE WEBINAR 1/31/19 12PM PST •

LARRY PESCE, DIRECTOR OF RESEARCH

https://www.inguardians.com/webinars/

About Me

- Penetration Tester/Hardware Hacker aka Director of Research & Sr. Managing Consultant @ InGuardians
- SANS Instructor
- Paul's Security Weekly Podcast (silent) Founder and Host
- Extra class ham radio operator (KB1TNF)



Some Background

- Software Defined Radio (SDR) has become huge!
  - Highly recommended to look at for security and for fun
- Many platforms to choose from
- Many *projects* to choose from

SDR Platform Selection

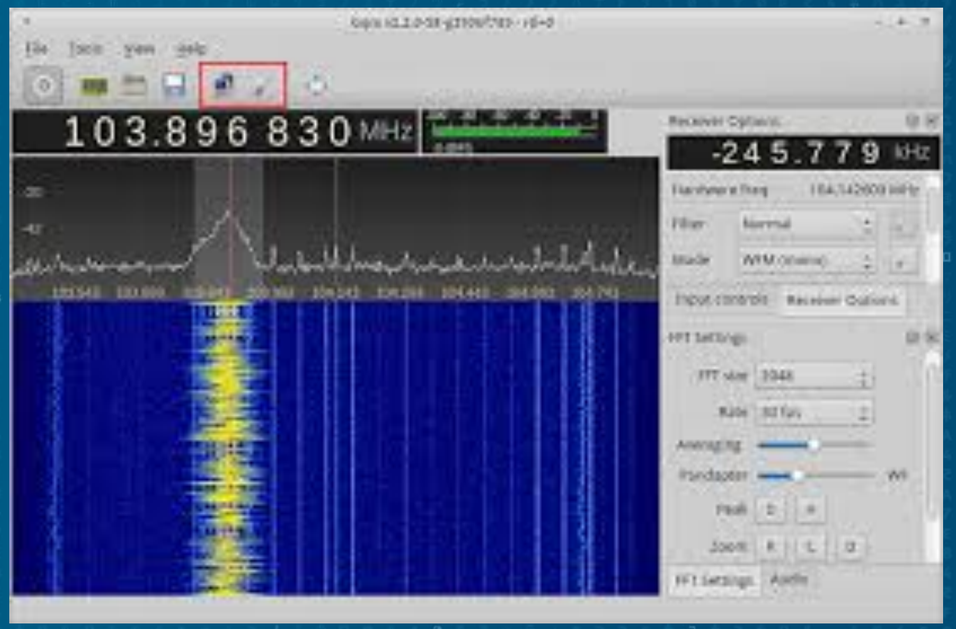
- Not all SDR platforms are created equal
- Some of my favorites include:
  - HackRF, $300, RX/TX, add ons
  - BladeRF, $375+, RX/TX
  - Ettus B200moini, $770* RX/TX
  - *RTL-SDR, $35 RX only*

RX is Fun

- I LOVE doing RX!
- Finding signals that I did not know was there…
- What do they do? What are they for?
- Often with unexpected results

Visualization

- GQRX is solid for initial discovery
- Lots of features and *visualization*
- Want to take it up a notch? Check out Web connected SDRs!
  - http://www.websdr.org
  - http://websdr.ewi.utwente.nl:8901
- How about “the Buzzer” (UVB-76) at 4625kHz
  - http://priyom.org/military-stations/russia/the-buzzer



DEMO

GQRX and WebSDR

openwebrx and KiwiSDR

- WebSDR is semi-closed source
- openwebrx is an open source alternative
  - Uses the RTL-SDR and a RasPi
  - Network connected, supports 4 users
  - Has some “issues”
    - https://github.com/faithanalog/openwebrx
- KiwiSDR reimplements openwebrx
  - Custom SDR, Beaglebone Green
  - Fixes the “issues”, $300 price tag

DEMO

OpenWebRX and KiwiSDR

rtl_433

- Utility 433 mHz ISM band receiver
- Many devices in use here!
- rtl_433 knows how to decode
  - More than 100 devices!
  - Some are more reliable than others
- Can also be used in “generic mode”
  - Saving and re-analysis of samples too
- You often find unexpected things…
  - …that make you ask all sorts of other questions!

```
Reading samples in async mode...
Tuned to 433910000 Hz.
*** signal_start = 2698807, signal_end = 2832099
signal_len = 133292,  pulses = 239
Iteration 1. t: 194    min: 98 (142)    max: 290 (97)    delta 41
Iteration 2. t: 194    min: 98 (142)    max: 290 (97)    delta 0
Pulse coding: Short pulse length 98 - Long pulse length 290

Short distance: 91, long distance: 276, packet distance: 2840

p_limit: 194
bitbuffer:: Number of rows: 10
[00] {25} 55 55 c0 00 : 01010101 01010101 11000000 0
[01] {25} 55 55 c0 00 : 01010101 01010101 11000000 0
[02] {25} 55 55 c0 00 : 01010101 01010101 11000000 0
[03] {25} 55 55 c0 00 : 01010101 01010101 11000000 0
[04] {25} 55 55 c0 00 : 01010101 01010101 11000000 0
[05] {25} 55 55 c0 00 : 01010101 01010101 11000000 0
[06] {25} 55 55 c0 00 : 01010101 01010101 11000000 0
[07] {25} 55 55 c0 00 : 01010101 01010101 11000000 0
[08] {25} 55 55 c0 00 : 01010101 01010101 11000000 0
[09] {14} 55 54 : 01010101 010101
```

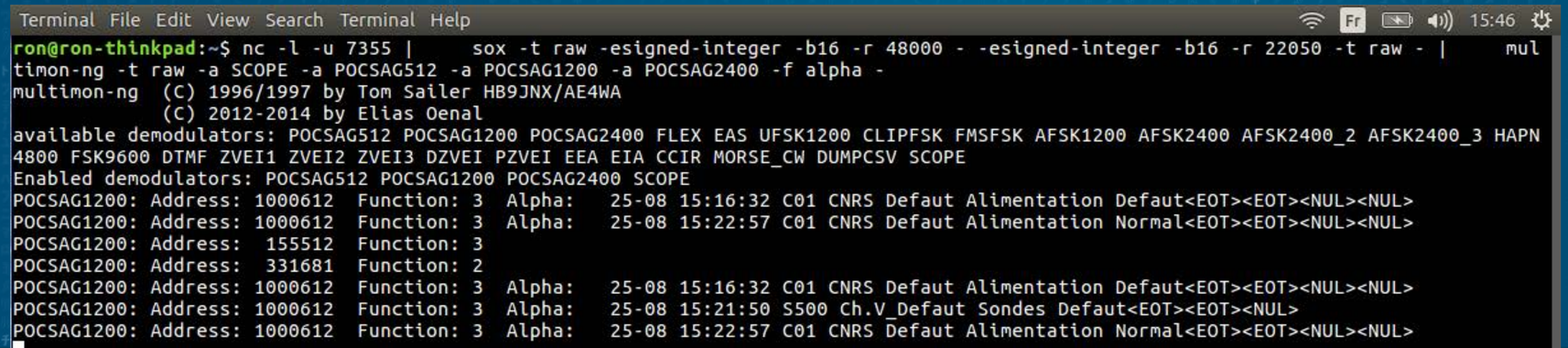
DEMO*

rtl_433

I’m not exactly sure what we’ll find here…

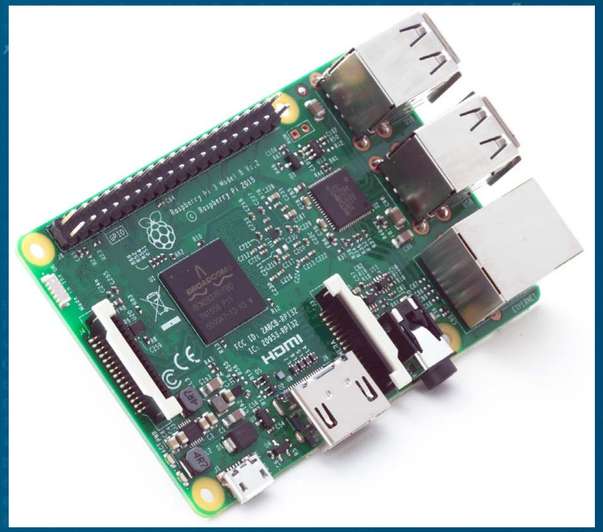
multimon-ng

- Not specifically for radio
- Helpful for post-processing audio signals
- Several formats for decoding
  - DTMF, Morse Code
  - POCSAG, FLEX quite interesting
- Can take raw audio as an in input via a pipe
- Now all we need is a signal, with rtl_fm, at say 929.010 mHz (or thereabouts)



RX only?

- Sure, it is a great way to get started, cheap!
- Want to transmit? Cool. How about:
  - PiFM - https://github.com/rm-hull/pifm
  - rpitx - https://github.com/F5OEO/rpitx
- Or, FL2K…
- rpitx2 is also amazing



rpitx2

- Rpitx uses the Raspi GPIO to transmit
  - Toggled at a high rate of speed to generate RF
- Add a short wire to increase range
- Updates to rpitx2 includes addition of RTL-SDR RX
  - Great for capture and replay based attacks
  - Easy, menu driven
- Not perfect, lots of harmonics
  - Not the best steward of radio

DEMO

rpitx2

FL2K

- Custom drivers for the FL2000 chipset
- Like Pi transmitters, toggles a GPIO pin for TX
- FL200 chips often found in inexpensive USB 3.0 to VGA adapters
  - Typically under $15
  - https://www.amazon.com/gp/product/B0773NQF2D
- Yes, it uses a VGA adapter to transmit RF signals…
  - Let that sink in for a bit

DEMO

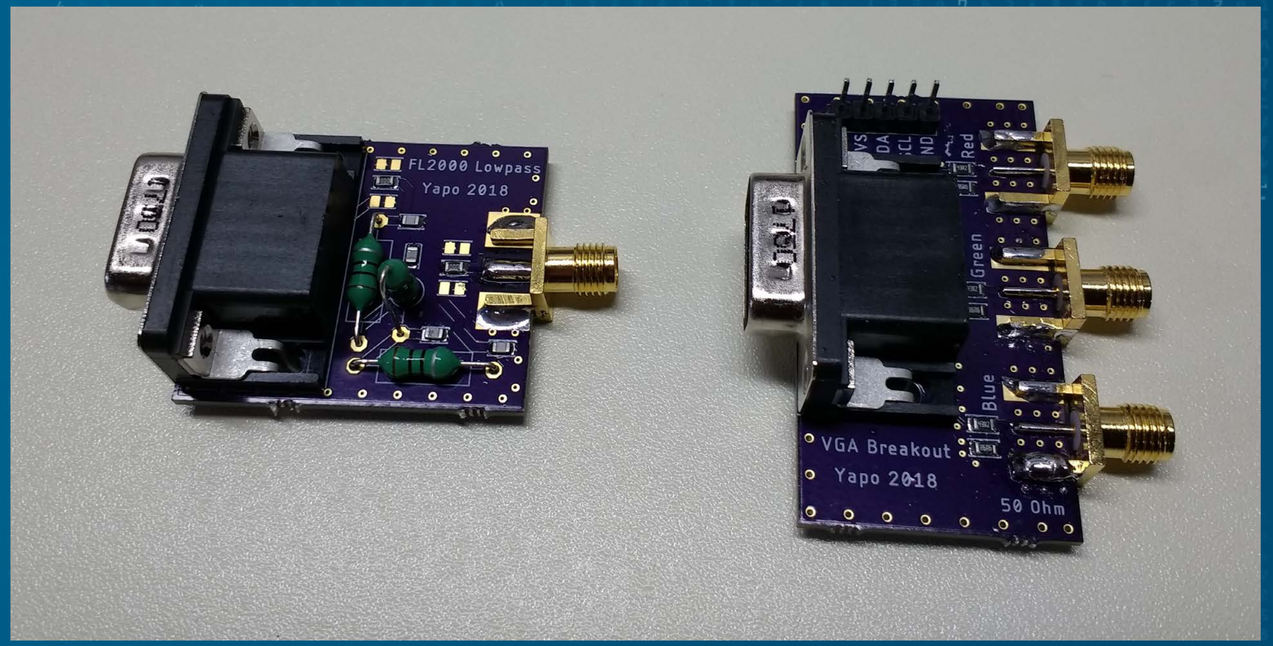
FL2K

Even More

- Using fl2k_fm we can send FM modulated signals…
- Using fl2k_file we can do much more
  - Spoofing GPS, UMTS, LTE, GSM
  - Creating DVB-T transmissions (Digital Video Broadcasting - Terrestrial)
  - Creating DAB (Digital Audio Broadcast)
- Think of the possibilities!
  - https://github.com/steve-m/fl2k-examples

Short Range

- FL2K, rpitx2 not robust RF wise
  - Lots of features
  - Harmonics
  - Lack of antenna
- FL2K has VGA adapters from Ted Yapo
  - Add better antennas
  - Add filtering
- Even tie to an amplifier



https://hackaday.io/project/21145

Why is this Important?

- We are going to continue to find more devices that can be repurposed for transmitters…
  - No longer something that is considered Nation State only capability
  - Check out Dragos Ruiu's latest works to scare your pants off
  - Vapor Trail, FL2K, riptx2…what's next?

http://www.vaportrail.io

No, really, what's next?

- What does this mean for data exfiltration?
- What does this mean for C&C?
- Knowing how to look, what to look for and thinking like an attacker will help us excel!
- Expanding our detection RF programs is not just the pipe dream of the paranoid

The one with the GPS

- We did a transmit with FM on FL2K
  - It wasn't very…robust
- FL2K is a hack!
- We can do better, especially with the extra FL2K capabilities, such as GPS
- Need to use better tools, such as the HackRF

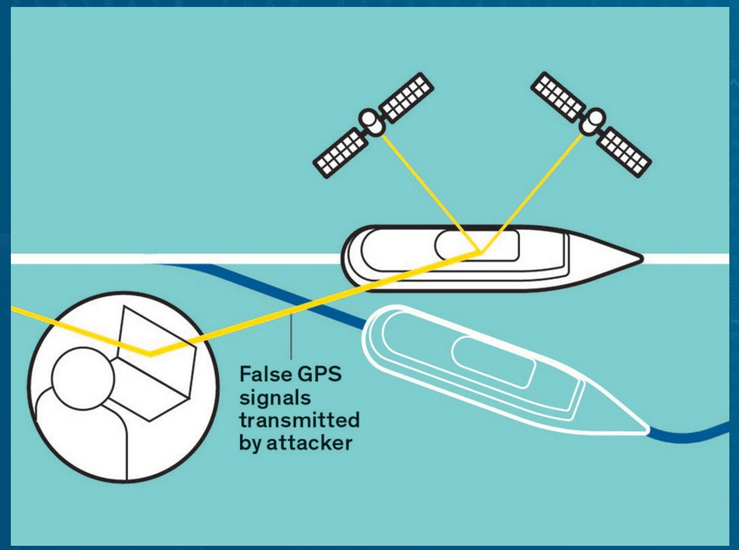
Some Background

- GPS, US funded satellite positioning system
- Original implementation in 1973
- TX only from satellite
- Location of receiver derived with Time + satellite position + math
  - Knowing accurate position of satellites important

Why Spoof GPS

Why Spoof GPS? (2)

- VIP attacks on cars
- VIC on shipping
- Anti-drone techniques



RF Tools

- Sure we can do this (unsuccessfuly?) with FL2K, but not at range
  - Stability, etc.
- Use of a HackRF is more reliable
  - It is meant to TX, and well
- Also BladeRF, ADALM Pluto, others

Software Tools

- gps-sdr-sim is the kick butt software to use!
  - https://github.com/osqzss/gps-sdr-sim
- Static position, path/trajectory spoofing
  - Static at command line
  - Path needs CSV, ECEF, or NMEA GGA stream
  - NMEA2UM, NMEA simulator
  - http://www.labsat.co.uk/index.php/en/free-gps-nmea-simulator-software

Simple Install

- Under Ubuntu 18.04, a few apt-get and git clone away
- Hard part is knowing where the satellites are for math!
  - The data is available, but obtuse filenames
- Need daily BRDC to calculate satellite location

Why is this Important?

- It has been my experience that there is a lasting effect
  - My test device did not updates time or location without intervention after 2 hours
- What do you use that is location based? Time based?
- Drones, Cars, Location base auth…
- Time based auth (TOTP)

https://zxsecuroty.co.nz/presentations/201607_Unrestcon-ZXSecurity_GPSSpoofing.pdf

Just Scratching the Surface

- There are so many more protocols and frequency ranges to explore
- Which of those are in our environment
  - …and which ones leak data?
  - …and which ones are a security risk, or could cause a compromise?
- SDR has opened up so much of the RF spectrum for analysis
- We haven't even touched on analyzing *unknown* signals!

Conclusions

- I hope I piqued your interest in SDR!
- We learned that
  - Analysis can be performed with inexpensive tools
  - Attacks can be performed with inexpensive tools
  - Much work has already been done
  - Attacks don’t always require lots of technical expertise
- We can spend more to do more
  - How deep does the rabbit hole go?

INGUARDIANS™

WEEKLY EXECUTIVE BRIEFING

Thanks!

larry@inguardians.com
@haxorthematrix