### 433.900.000



www. water water the service of the

### SOFTWARE DEFINED RADIO: WITH EVEN MORE AWESOME • LIVE WEBINAR 1/31/19 12PM PST • LARRY PESCE, DIRECTOR OF RESEARCH

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



2 manual physical production of the second pro



### About Me

2

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





# 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

RX is Fun

5





### Visualization

6

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 





	○ 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0				
Posternollion       Posternollion			ニマロヨメリザチャラミカルドアルビムで、回来市市名を「マイルフヨレラロマリニミメチル市人市のの窓区へ、インド・ドラーンデザムスのフマニメがなら非凡二のマシスションティー・ドラーンデュロシリティ、レンチリのロラボザーの万字、ロンチャンションディーションディー		G

### 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

8



Image: Section in the section in the section in the section in the section is the section in the section in the section is the section in the section is th	こして ひとう F 1 2 0 0 7 7 7 7 1 7 7 7 7 7 7 7 7 7 7 7 7 7			
SCHOLESS STATES STATES THE STATES STA	「マロヨメリルテレブミホスドス1250880000000000000000000000000000000000		こうこうが、していたした。	Ope
		マーマンションののので、「「「「「「「「」」」」」」」」」」」」」」」」」」」」」」」」」」」		

### enWebRX and KiwiSDR



### rtl\_433

Utility 433 mHz ISM band receiver Reading samples in async mode... Tuned to 433910000 Hz. \*\*\* signal start = 2698807, signal end = 2832099 signal len = 133292, pulses = 239Many devices in use here! Iteration 1. t: 194 max: 290 (97) delta 41 min: 98 (142) Iteration 2. t: 194 max: 290 (97) min: 98 (142) delta 0 Pulse coding: Short pulse length 98 - Long pulse length 290 rtl 433 knows how to decode Short distance: 91, long distance: 276, packet distance: 2840 p limit: 194 More than 100 devices! bitbuffer:: Number of rows: 10 {25} 55 55 c0 00 : 01010101 01010101 11000000 0 {25} 55 55 c0 00 : 01010101 01010101 11000000 0 55 55 c0 00 : 01010101 01010101 11000000 0 {25} Some are more reliable than others {25} 55 55 c0 00 : 01010101 01010101 11000000 0 55 55 c0 00 : 01010101 01010101 11000000 0 55 55 c0 00 : 01010101 01010101 11000000 0 Can also be used in "generic mode" 55 c0 00 : 01010101 01010101 11000000 0 {25} 55 55 c0 00 : 01010101 01010101 11000000 0 {25} 55 55 c0 00 : 01010101 01010101 11000000 0  $\{14\}$  55 54 : 01010101 010101 Saving and re-analysis of samples too You often find unexpected things... • ...that make you ask all sorts of other questions!



	ファナススパフェマロコックテナススパフェアランテアレマテナススパフェアリーション		
<ul> <li>・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・</li></ul>			
************************************	C 1 2 2 3 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4		l'm not e

### rtl\_433 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)

Terminal File Edit View Search Terminal Help	
<pre>ron@ron-thinkpad:~\$ nc -l -u 7355   sox -t raw</pre>	-esigned-integer -b16 -r
timon-ng -t raw -a SCOPE -a POCSAG512 -a POCSAG120	0 -a POCSAG2400 -f alpha
multimon-ng (C) 1996/1997 by Tom Sailer HB9JNX/AE	4WA
(C) 2012-2014 by Elias Oenal	
available demodulators: POCSAG512 POCSAG1200 POCSA	G2400 FLEX EAS UFSK1200 C
4800 FSK9600 DTMF ZVEI1 ZVEI2 ZVEI3 DZVEI PZVEI EE	A EIA CCIR MORSE_CW DUMPC
Enabled demodulators: POCSAG512 POCSAG1200 POCSAG2	400 SCOPE
POCSAG1200: Address: 1000612 Function: 3 Alpha:	25-08 15:16:32 C01 CNRS
POCSAG1200: Address: 1000612 Function: 3 Alpha:	25-08 15:22:57 C01 CNRS
POCSAG1200: Address: 155512 Function: 3	
POCSAG1200: Address: 331681 Function: 2	
POCSAG1200: Address: 1000612 Function: 3 Alpha:	25-08 15:16:32 C01 CNRS
POCSAG1200: Address: 1000612 Function: 3 Alpha:	25-08 15:21:50 S500 Ch.
POCSAG1200: Address: 1000612 Function: 3 Alpha:	25-08 15:22:57 C01 CNRS

 - esigned-integer -b16 -r 22050 -t raw 48000

LIPFSK FMSFSK AFSK1200 AFSK2400 AFSK2400\_2 AFSK2400\_3 HAPN SV SCOPE

Defaut Alimentation Defaut<EOT><EOT><NUL><NUL> Defaut Alimentation Normal<EOT><EOT><NUL><NUL>

```
Defaut Alimentation Defaut<EOT><EOT><NUL><NUL>
V_Defaut Sondes Defaut<EOT><EOT><NUL>
Defaut Alimentation Normal<EOT><EOT><NUL><NUL>
```



### 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/F50E0/rpitx • Or, FL2K... rpitx2 is also amazing





### rpitx2

14

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 



INTROPERSE AND A CONSTRUCTION CONSTRUCTURES CONSTRU	- ちしゃらにいたりましたアワタノトツサナムスパフニマロヨメリルデレジを命馬におっている時やいし、ことににっているとなっクラノトツサナムスパフニマロヨメリルデレジを命馬におっていたいが、 しし ししにく やさおり スワタノトツテナ ユスパフヨレラロマリニ たメザル曲人 ふさホア にあい クラノロヨ ひえ デルマ ユトナニリ テレメ むこと バボス キバフョ におばし ユリミコ こメラ じニス グラノ	 「日おちことでするかがある」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」」	- 1977 クノナデトフェルククラルミメートリックにおけるとなるのクルビデュックドク - 1977		
		- 日おんだら、「その思想での心的で少えとグラナムスのスカレラ回マは、あって、「、」、「、」、これできるひをワタノレジトテルズのフロニメットプレスに回び、スキャッテス」と思ったとし、日子はそれでは、日子に ここに、「、そハフト」、ストラレメモリ、田子正子」やに出現二 いていしょう			





### 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 

16





INTERPORT       INTERPORT	- ショックロション・ション・ション・ション・ション・ション・ション・ション・ション・ション・					
18:10:10:10:10:10:10:10:10:10:10:10:10:10:		本へ兄の日のやちのワタユデノトスのフルビーホムドロシスビデルが大いたった日に日本のドロショムビデルがたで、この日の10、ホムドロショムビデルがた。この日の10、ロレホッムの日日には、日の日の日に、日の日	- ロマリニミメチル水人らさら了日おらさドロ・ニメチレヨルラロミリホへんぶんかく - ことチャリミヨさメラロニヤツラメは目の - こことまアツラエトネサー デストロツチュリ			





### 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 

18







### 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?

20

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

23



### Why Spoof GPS



24



### 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

27

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)

29

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**<sup>™</sup>

### WEEKLY EXECUTIVE BRIEFING

DNU

GUARDIN

ADVANCED

HH0000HHH0

Latest from the InfoSec world.

- Future events and trainings.
- We won't spam you!

https://www.inguardians.com/brief

.010101000000

## nanks

larry@inguardians.com @haxorthematrix

