IN THIS ISSUE >>> #40

Main Article:

HackRF One

Secondary Article:

HackRF One Cont.

Bonus Materials:

Website Domain Change

Update Corner:

Website Updates

TOUCHPOINT
INTERNATIONAL DEVELOPMENT GROUP, INC
YOUR ONE STOP SHOP FOR TECHNICAL AND TACTICAL EQUIPMENT

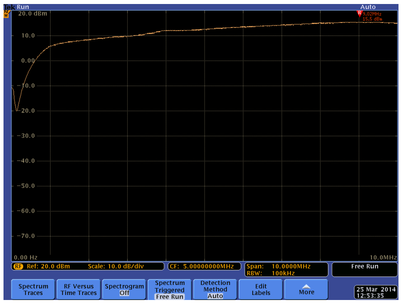
A Bi-Monthly Snapshot into Emerging Threats and Trends

Digital Update

HackRF One

Fun with Radio Frequency

The HackRF One is another device by Great Scott Gadgets designed to listen on almost the entire RF spectrum. Both the source code and the hardware are open source, so you can build your own and change its operating modes as you wish. This device has the ability to transmit or receive any radio frequency signals with the only real limitation being in the antenna you use. The stock antenna (the ANT 500 if the seller bundles the antenna) that we received with our HackRF One limits us to the 75 MHz to 1 GHz range, but it can currently operate more in the 1 MHz to 6 GHz range in half duplex, officially. As you try to tune lower than 1 MHz the quality drops off significantly, as the chart below shows. While it is do-able, the current model is not rated to go above or below the official range. The device takes an SMA connection for the antenna, so anything that fits that connection will work and will allow for a wider range or different ranges and farther distance than the stock antenna. The range on the stock antenna leaves a lot to be desired. It is a decent telescopic antenna, but you will definitely have to buy a new one and not rely on it being anything other than a starter antenna.



RF Ref: 20.0 dBm Scale: 10.0 dB/div
CF: 5.00000000MHz
Span: 10.0000MHz
RBW: 100kHz
25 Mar 2014
12:53:35

So what can we do with this device? With its ability to listen or transmit on almost any frequency, we have the ability to receive all kinds of different frequencies, such as Wi-Fi (2.4 GHz, 5 GHz), Bluetooth (2.4 GHz), FM Radio (88 to 108 MHz), Keyless Entry for cars (315 MHz, 433.92 MHz), Keyless Entry for buildings (13.56), garage doors (315 MHz), baby monitors (49 MHz, 902 MHz, 2.4 GHz), etc. There is no lack of frequencies we can listen to with this device.

CURRENT COURSES >>>

- *ESSR*
- *Wireless Analysis*
- *Basic Non-Standard Communications*
- *Advanced Non-Standard Communications*
- *Basic OSINT*
- *Advanced OSINT*
- *Identity Management*
- *NSC RasPi*
- *Data Protection*

CURRENT TOPICS >>>

After Second Bungle, IRS Suspends Equifax's "taxpayer identity" contract

-Arstechnica

White House wants to end Social Security numbers as a national ID

-Arstechnica

GOP rep moves to end use of Social Security numbers as credit bureau ID

-The Hill

T-Mobile says it will not stop claiming its network is faster than Verizon's

-The Verge

Beware of sketchy iOS popups that want your Apple ID

-Arstechnica

Microsoft Cortana Can Now Read Your Skype Messages to Make Chat Smarter

-The Hacker News

FBI Arrests A Cyberstalker After Shady "No-Logs" VPN Provider Shared User Logs

-The Hacker News

Kaspersky Russian Spying Rumors: Should You Use This Antivirus?

-Tom's Guide

Hyatt Hotels Suffers 2nd Card Breach in 2 Years

-KrebsonSecurity

EVENTS >>>

ToorCamp 2018

June 20-24 2018, San Juan, WA

Black Hat USA 2018

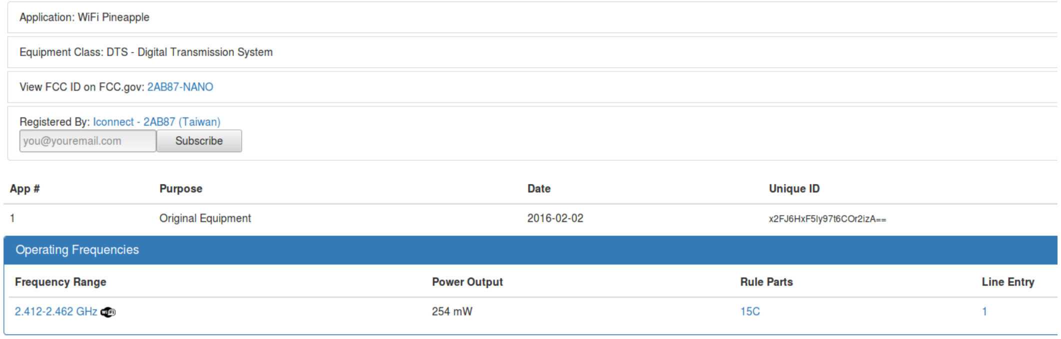
Aug 4-9 2018, Las Vegas, NV

DEF CON 26

Aug 9-12 2018, Las Vegas, NV

HackRF One Cont.

If a device transmits wirelessly, the manufacturer must register the device with the FCC. The FCC ID is printed somewhere on the device (normally on the back or under the battery). This is great in discovering what frequency a device operates on and what frequency you need to tune the HackRF One to listen to. This is obviously not true for devices that illegally broadcast wirelessly.



Application: WiFi Pineapple

Equipment Class: DTS - Digital Transmission System

View FCC ID on FCC.gov: 2AB87-NANO

Registered By: Iconnect - 2AB87 (Taiwan)

App #	Purpose	Date	Unique ID
1	Original Equipment	2016-02-02	x2FJ6HxF5ly97t6COr2izA==

Operating Frequencies

Frequency Range	Power Output	Rule Parts	Line Entry
2.412-2.462 GHz	254 mW	15C	1

You can look up a device's ID on the FCC website but, like all government sites, it's not designed with usability in mind. The best site we have found for lookups is: https://fccid.io. Even if you don't plan on listening in on a frequency, it may be a good idea to plug in your phone's ID to see what frequencies it can operate on.

Now that's just the receiving side. This device can also transmit signals on whatever frequency you choose. That means if you want to transmit your own tunes over the FM radio, or you want to transmit your voice over a walkie-talkie, this device makes it pretty simple. If we captured a signal from a garage door opener, we could re-transmit it over the same frequency to open the garage again. Cars are a little bit different but, apply the same concept and you could unlock a car by re-transmitting the unlock signal over the same frequency it was captured on, in most cases. This is known as a replay attack and it's very simple to do but, with the implementation of rolling codes, it's a bit more difficult. This can be easily bypassed by other means that are not going to be discussed in this newsletter. Another approach would be to analyze the signal and modify it for re-transmission. A good example of this is garage door openers. Most garage door openers use a finite number of codes in transmission to open the garage door. If you can find a pattern, you can broadcast all of the different code combinations until it opens the garage door. It may take a long time to broadcast all of the possible combinations, but eventually you're getting in.

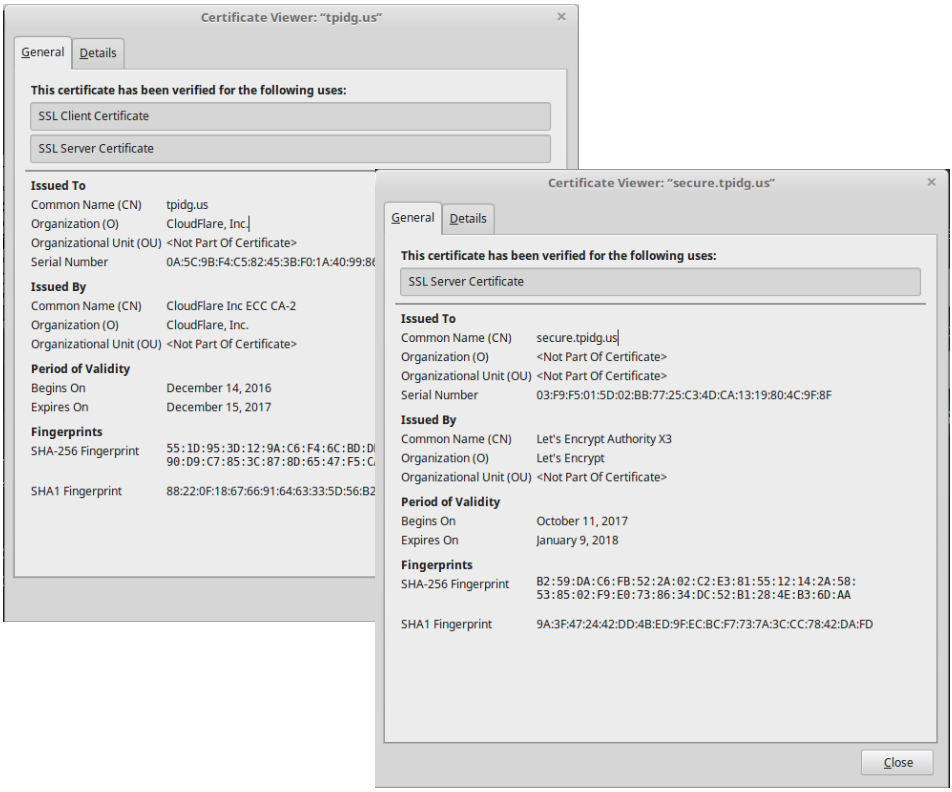
It should be noted that the FCC imposes strict regulations on the RF spectrum. Listening in on someone's private communications or broadcasting over an allocated frequency is completely illegal. If you don't know whether or not it is legal, don't do it.

Contact admin@tpidg.us for additional information on this device and how this device can be used in an operational capacity.

BONUS MATERIALS >>>

Domain Change for Login Section https://secure.tpidg.us

You may have noticed that the entire login section of our site moved to https://secure.tpidg.us. This was to further separate out the unauthorized sections of our site from the public side of the site. This also gives us the benefit of disabling Cloudflare on that part of the site. Due to the nature of how Cloudflare works, they have full access to all traffic that passes between our server and the visitor whether that be encrypted traffic or not. While we don't think Cloudflare is going to be doing anything malicious on purpose, there are benefits to having the login side be independent of Cloudflare. The main benefit is being able to use our own TLS certificate instead of using Cloudflare's TLS certificate. We used Let's Encrypt to generate our TLS certificate and this means that only we have access to encrypted traffic, not Cloudflare, not anyone else. We will cover Let's Encrypt in full detail in a future issue.



```
This certificate has been verified for the following uses:
SSL Client Certificate
SSL Server Certificate

Issued To
Common Name (CN)          tpidg.us
Organization (O)          CloudFlare, Inc.
Organizational Unit (OU)  <Not Part Of Certificate>
Serial Number             0A:5C:9B:F4:C5:82:45:3B:F0:1A:40:99:86

Issued By
Common Name (CN)          CloudFlare Inc ECC CA-2
Organization (O)          CloudFlare, Inc.
Organizational Unit (OU)  <Not Part Of Certificate>

Period of Validity
Begins On                 December 14, 2016
Expires On                December 15, 2017

Fingerprints
SHA-256 Fingerprint       55:1D:95:3D:12:9A:C6:F4:6C:BD:D
                          90:D9:C7:85:3C:87:8D:65:47:F5:C

SHA1 Fingerprint          88:22:0F:18:67:66:91:64:63:33:5D:56:B2
```

```
This certificate has been verified for the following uses:
SSL Server Certificate

Issued To
Common Name (CN)          secure.tpidg.us
Organization (O)          <Not Part Of Certificate>
Organizational Unit (OU)  <Not Part Of Certificate>
Serial Number             03:F9:F5:01:5D:02:BB:77:25:C3:4D:CA:13:19:80:4C:9F:8F

Issued By
Common Name (CN)          Let's Encrypt Authority X3
Organization (O)          Let's Encrypt
Organizational Unit (OU)  <Not Part Of Certificate>

Period of Validity
Begins On                 October 11, 2017
Expires On                January 9, 2018

Fingerprints
SHA-256 Fingerprint       B2:59:DA:C6:FB:52:2A:02:C2:E3:81:55:12:14:2A:58:
                          53:85:02:F9:E0:73:86:34:DC:52:B1:28:4E:B3:6D:AA

SHA1 Fingerprint          9A:3F:47:24:42:DD:4B:ED:9F:EC:BC:F7:73:7A:3C:CC:78:42:DA:FD
```

The clear separation also helps us to make clear what we do on each side of the site. A great example of this is we do use Google Analytics on the public side of the site to see how many visitors we get a day (if you use a script blocker, you aren't counted), but the private side of the site does not use Google Analytics. This has always been the case, but now we can provide a very clear distinction between the two. We do collect login logs, but that's about it. Nothing you do while you are logged in is tracked. So the real question is why even use Cloudflare? Cloudflare is a great service and there is no disputing that. TPIDG.US is hosted on a custom built server running from our office and having Cloudflare between the visitor and our server helps protect it from DDOS attacks and ensures 100% uptime. We don't have access to the multi-gigabit connection that Cloudflare does, so a DDOS attack would shut us down. This is great for the public facing site that everyone is allowed to access, but with all of the sensitive and proprietary content in the login section, we would prefer to eliminate as many variables as possible.

UPDATE CORNER >>>

Website Changes

Updates to https://www.tpidg.us for the month of October. For comments or suggestions send an email to admin@tpidg.us

Domain Change for Login Section of Website

- Changed domain of login side of the website. For full details, read the article to the left.

About Us

- Our about us page changed to reflect more current information including courses we have added or removed.

Login Side

- Added a projects page for current, past and future projects. Feel free to explore.
- Closed registration to the public. If you have an access code, you can still register. Otherwise, you will need to be approved by an admin.

Anything you would like us to add to our website?

Contact admin@tpidg.us

READER QUESTIONS >>>

Have a specific **question** you would like us to answer?

Have a suggestion for a **topic**?

Want to **contribute** to the digital update?

Let us know at digitalupdate@tpidg.us