Yes, the FCC might ban your operating system

(but that’s not the real problem)

Eric Schultz

Who am I?

- Independent software engineer and open source consultant

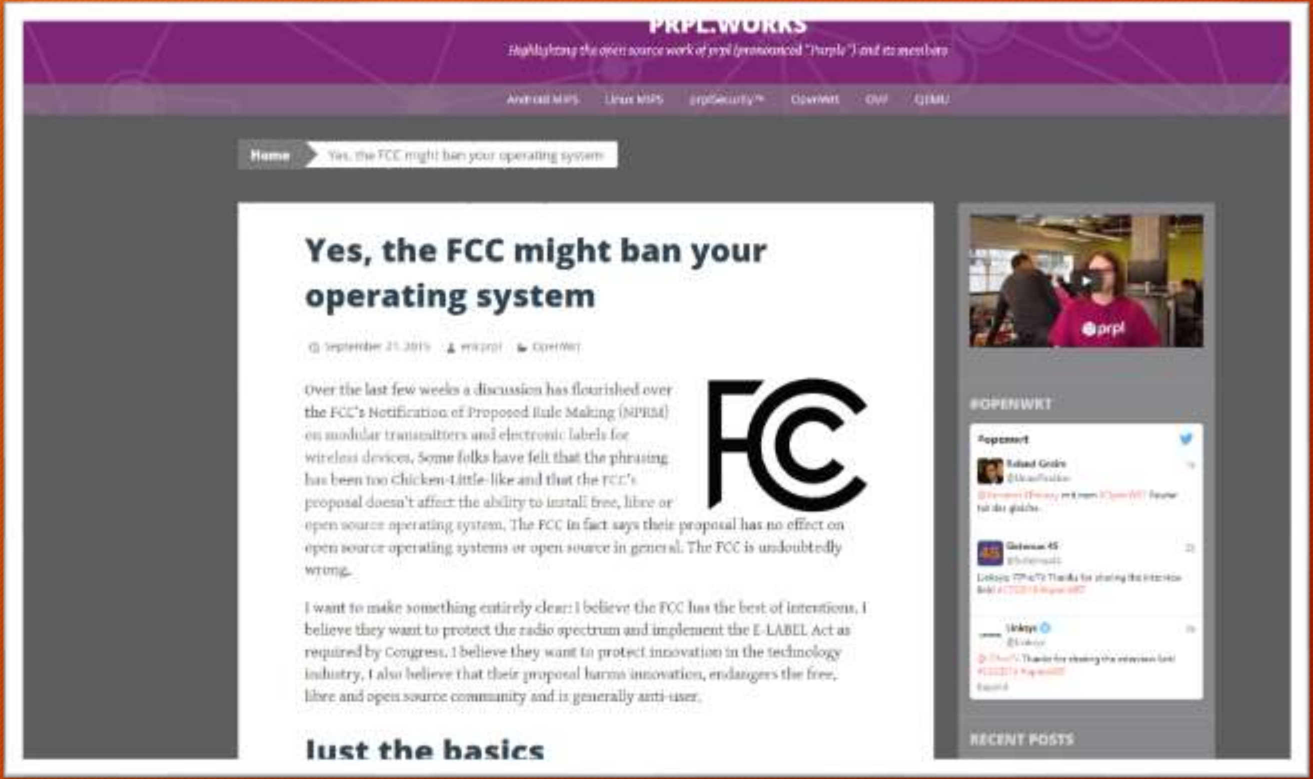
prpl

AgGateway

OUTERCURVE FOUNDATION

Microsoft

Introduction


PRPL.WORKS
Highlighting the open source work of prpl (pronounced "Purple") and its members
Android MIPS
Linux MIPS
prplSecurity™
OpenWrt
OVP
QEMU
Home
Yes, the FCC might ban your operating system
#OPENWRT
RECENT POSTS

Yes, the FCC might ban your operating system

September 21, 2015 · ericprpl · OpenWrt

Over the last few weeks a discussion has flourished over the FCC's Notification of Proposed Rule Making (NPRM) on modular transmitters and electronic labels for wireless devices. Some folks have felt that the phrasing has been too Chicken-Little-like and that the FCC's proposal doesn't affect the ability to install free, libre or open source operating system. The FCC in fact says their proposal has no effect on open source operating systems or open source in general. The FCC is undoubtedly wrong.

I want to make something entirely clear: I believe the FCC has the best of intentions. I believe they want to protect the radio spectrum and implement the E-LABEL Act as required by Congress. I believe they want to protect innovation in the technology industry. I also believe that their proposal harms innovation, endangers the free, libre and open source community and is generally anti-user.

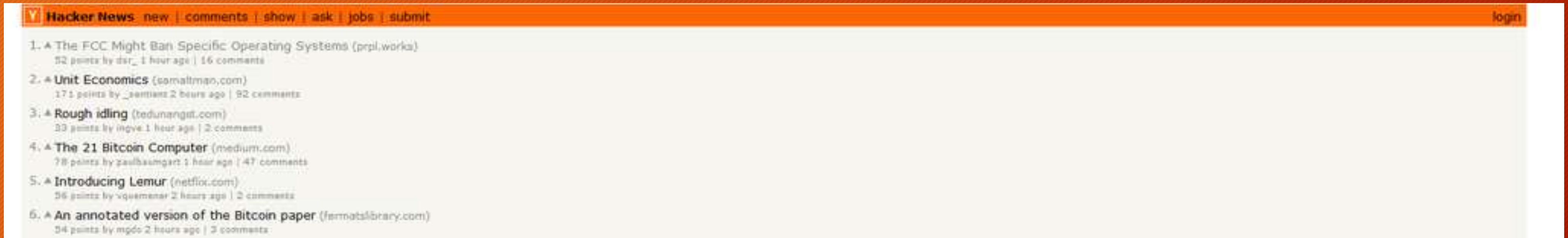
Just the basics

Introduction

Y Hacker News new | comments | show | ask | jobs | submit login

1. ▲ The 21 Bitcoin Computer (medium.com)
   67 points by paulbaumgart 1 hour ago | 31 comments
2. ▲ Unit Economics (samaltman.com)
   183 points by _sentient 2 hours ago | 86 comments
3. ▲ The FCC Might Ban Specific Operating Systems (prpl.works)
   37 points by dar_ 1 hour ago | 12 comments
4. ▲ Rough idling (tedunangst.com)
   26 points by ingve 54 minutes ago | 1 comment
5. ▲ Introducing Lemur (netflix.com)
   49 points by vquemener 1 hour ago | 1 comment
6. ▲ An annotated version of the Bitcoin paper (fermatslibrary.com)

Introduction



1. ▲ The FCC Might Ban Specific Operating Systems (prpl.works)
   52 points by dsr_ 1 hour ago | 16 comments
2. ▲ Unit Economics (samaltman.com)
   171 points by _sentient 2 hours ago | 92 comments
3. ▲ Rough idling (tedunangst.com)
   33 points by ingve 1 hour ago | 2 comments
4. ▲ The 21 Bitcoin Computer (medium.com)
   78 points by paulbaumgart 1 hour ago | 47 comments
5. ▲ Introducing Lemur (netflix.com)
   56 points by vquemener 2 hours ago | 2 comments
6. ▲ An annotated version of the Bitcoin paper (fermatslibrary.com)
   54 points by mgdo 2 hours ago | 3 comments

HOW MANY COMMENTS?!

- NPRM had around 4000 comments, with very few in favor
- Opposed by FSF, OSI, SFC, Google, Boeing, research labs, ARRL, OpenWrt, DD-Wrt, Mozilla, ThinkPenguin, Linux Torvalds, Vint Cerf, doctors, servicemembers, hams, developers and more

Concerned about two FCC rules/proposals

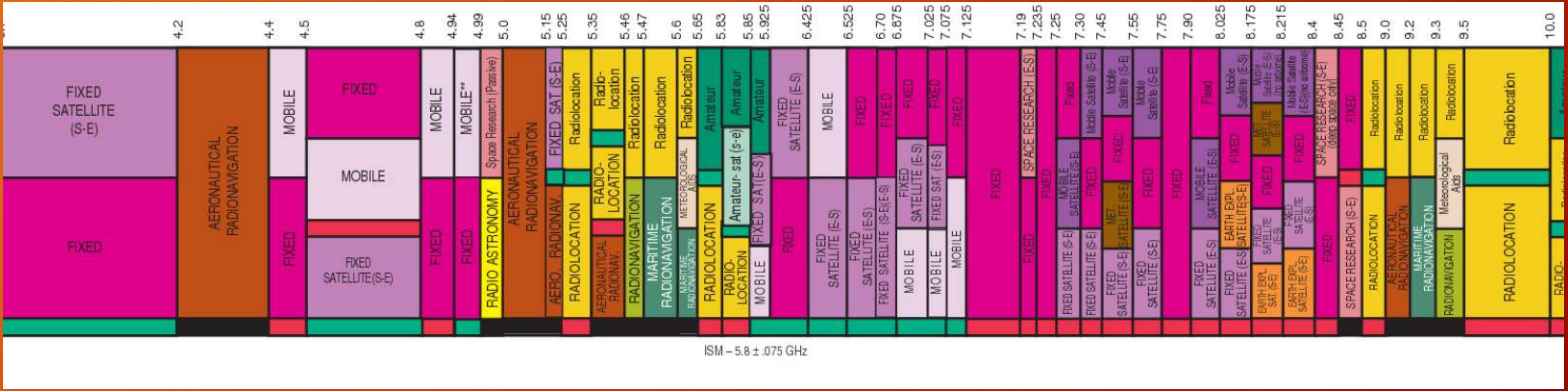
1. U-NII rules
2. NPRM on ELABEL Act and Modular Transmitters

Background on the FCC

What the FCC does with radios

- Regulate radiospectrum users

Radio spectrum map



Radio spectrum is a finite resource!

- We can’t expand the radio spectrum
- Also, different parts of spectrum have different use cases
- Lower frequency (generally) has a better ability to penetrate structures travel longer distances at lower power
- Example: 2.4Ghz versus 60 Ghz

Spectrum split into three categories

- No one may use
- Everyone may appropriately use
- Licensed parties may appropriately use

Licensed parties

- Different classes of users
- Amateur radio operators, commercial operators (radio, TV, mobile phone), armed forces, safety personnel, air traffic control
- Each user must meet some sort of requirement to be licensed

Appropriate use?

- Depends on user and frequency
- Includes regulation of frequency, power output, modulation technique

Why power matters

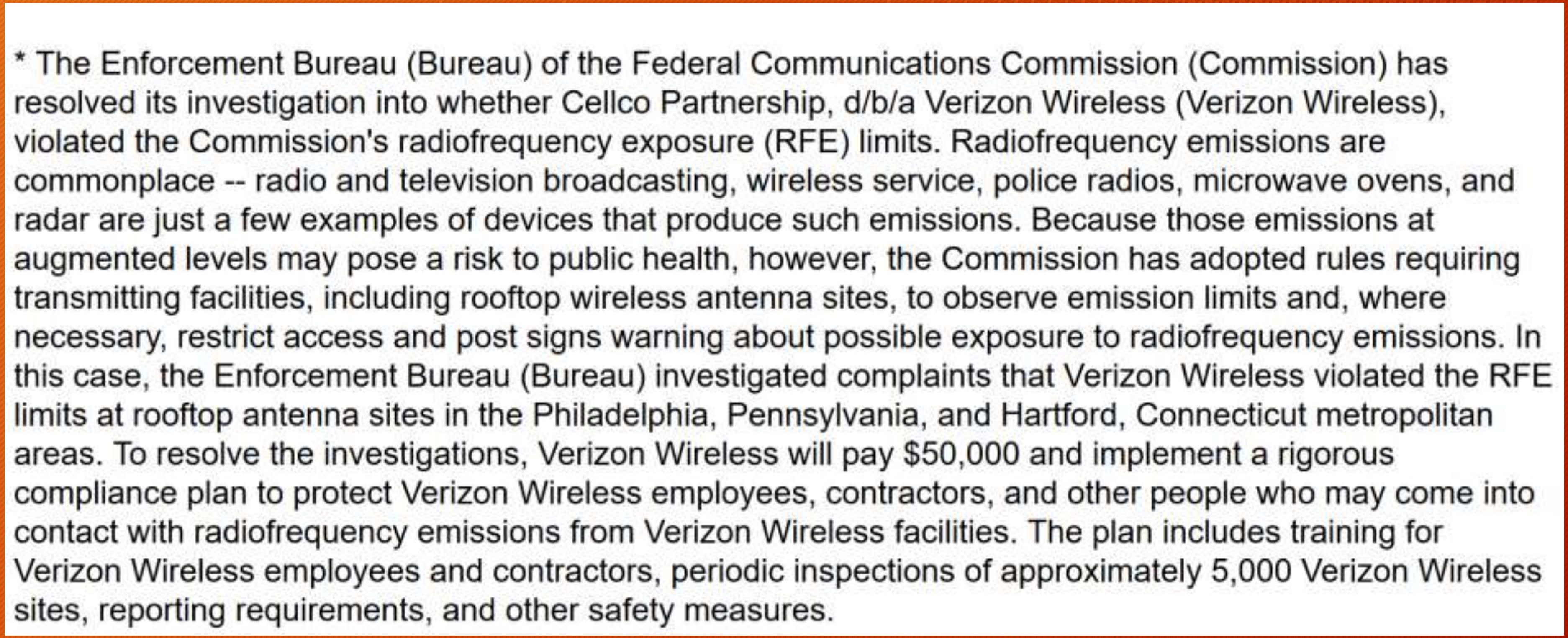
- It’s a spectrum sharing technique

One more side of appropriate use: Primary and secondary users

- What if two groups need the same slice of spectrum?
- What if one is “more important” that than the other?

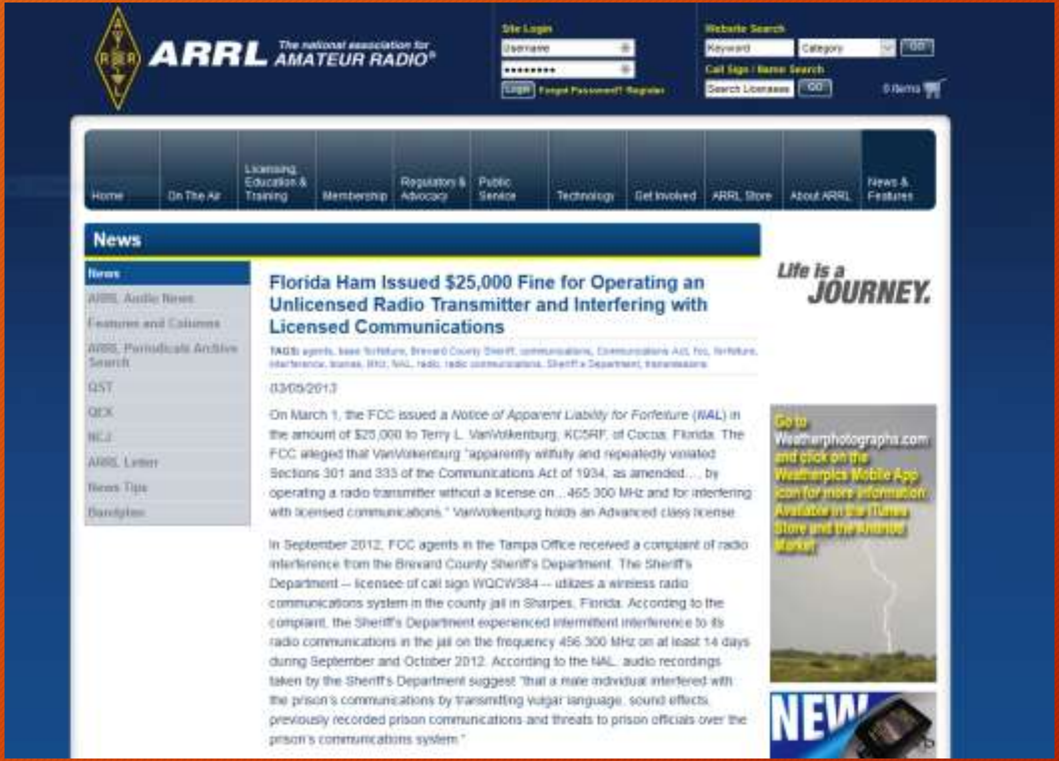
- Solution: Share same spectrum but secondary users MUST defer to needs of primary users

The fines for inappropriate usage



* The Enforcement Bureau (Bureau) of the Federal Communications Commission (Commission) has resolved its investigation into whether Cellco Partnership, d/b/a Verizon Wireless (Verizon Wireless), violated the Commission's radiofrequency exposure (RFE) limits. Radiofrequency emissions are commonplace -- radio and television broadcasting, wireless service, police radios, microwave ovens, and radar are just a few examples of devices that produce such emissions. Because those emissions at augmented levels may pose a risk to public health, however, the Commission has adopted rules requiring transmitting facilities, including rooftop wireless antenna sites, to observe emission limits and, where necessary, restrict access and post signs warning about possible exposure to radiofrequency emissions. In this case, the Enforcement Bureau (Bureau) investigated complaints that Verizon Wireless violated the RFE limits at rooftop antenna sites in the Philadelphia, Pennsylvania, and Hartford, Connecticut metropolitan areas. To resolve the investigations, Verizon Wireless will pay $50,000 and implement a rigorous compliance plan to protect Verizon Wireless employees, contractors, and other people who may come into contact with radiofrequency emissions from Verizon Wireless facilities. The plan includes training for Verizon Wireless employees and contractors, periodic inspections of approximately 5,000 Verizon Wireless sites, reporting requirements, and other safety measures.

The fines for inappropriate usage



Florida Ham Issued $25,000 Fine for Operating an Unlicensed Radio Transmitter and Interfering with Licensed Communications

TAGS: agents, base forfeiture, Brevard County Sheriff, communications, Communications Act, fcc, forfeiture, interference, license, MHz, NAL, radio, radio communications, Sheriff's Department, transmissions

03/05/2013

On March 1, the FCC issued a *Notice of Apparent Liability for Forfeiture* (NAL) in the amount of $25,000 to Terry L. VanVolkenburg, KC5RF, of Cocoa, Florida. The FCC alleged that VanVolkenburg "apparently willfully and repeatedly violated Sections 301 and 333 of the Communications Act of 1934, as amended . . . by operating a radio transmitter without a license on . . 465.300 MHz and for interfering with licensed communications." VanVolkenburg holds an Advanced class license.

In September 2012, FCC agents in the Tampa Office received a complaint of radio interference from the Brevard County Sheriff's Department. The Sheriff's Department -- licensee of call sign WQCW384 -- utilizes a wireless radio communications system in the county jail in Sharpes, Florida. According to the complaint, the Sheriff's Department experienced intermittent interference to its radio communications in the jail on the frequency 456.300 MHz on at least 14 days during September and October 2012. According to the NAL, audio recordings taken by the Sheriff's Department suggest "that a male individual interfered with the prison's communications by transmitting vulgar language, sound effects, previously recorded prison communications and threats to prison officials over the prison's communications system."

Important notes

- Unintentional violation IS illegal and can be punished
- Intentional or negligent violations will not be looked upon kindly

- If a user learns their transmission is interfering with others, they MUST stop the interference immediately.

What the FCC does with radios

- Regulate radiospectrum users
- Regulate marketed devices

Why devices?

- Devices can behave badly and cause interference
- If users are responsible, we don’t want users breaking the law
- Manufacturers are required to use accepted best-practices for engineering and I’m sure they occasionally do

Devices are regulated by use-case

- Part 15 devices (unlicensed devices) have different requirements than Part 97 (amateur radio devices)

Device

- I’ve never found a definition
- Not just the hardware portion of radio
- But not ALL of the software on the hardware

- Implied to be the radio hardware and the software which can control the radio parameters

So how much software “controls the radio parameters”?

- Depends on the particular device
- Where is the last barrier that can override all radio control decisions?

How the Linux Wifi Regulatory Works

- The Linux Kernel has a regulatory subsystem
- Takes care of managing the regulatory domain, including legal requirements on power, frequency, DFS
  - i.e. if you’re set to the US domain, requests to the driver to not use DFS on DFS-only frequencies would be denied by the kernel
- Provides a highly audited, reusable implementation for wireless drivers
- Not every driver uses it but it’s the recommended design

So where does the device end?

- Includes the (radio) firmware in almost all cases
- Includes driver in most cases
- If your driver does not have an internal regulatory system and uses the kernel implementation, the device ends INSIDE the kernel.

U-NII Rules

The large scale lock-down begins in 2014

- FCC approves new rules to restrict the modification of U-NII devices
- U-NII = Unlicensed National Infrastructure Initiative = 5Ghz
- 15.407(i): “All U-NII devices must contain security features to protect against modification of software by unauthorized parties.”

But wait, there’s more…

(1) “Manufacturers must implement security features in any digitally modulated devices capable of operating in any of the U-NII bands, so that third parties are not able to reprogram the device to operate outside the parameters for which the device was certified. **The software must prevent the user** from operating the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved for the device. (FCC then gives examples of ways manufacturers can do this, including **electronic signatures** on software)

But wait, there’s more…

(2)“Manufacturers must take steps to ensure that DFS functionality cannot be disabled by the operator of the U-NII device.”

Oh there’s even more

- From the instructions for hardware manufacturers to comply:

  “What prevents third parties from loading non-US versions of the software/firmware on the device? Describe in detail how the device is protected from “flashing” and the installation of third-party [images] such as DD-WRT.”

Why 2014?

- Until then, the only Wifi running on 5Ghz was 802.11a and the alternate band for 802.11n

- Now, 802.11ac is THE standard for high speed wifi

802.11ac

- It ONLY runs on 5Ghz (2.4Ghz is just too congested)
- The channel sizes are MUCH larger (from 20mhz to as much as 160mhz)
- 5Ghz was previously used for 11a and as an 11n alternative frequency

- Sadly, something else is ALSO there…

Terminal Doppler Weather Radar

- High-precision weather radar
- Used at about 50 of the busiest airports in the country and in more around the world
- In the middle of the 5Ghz band (but differs slightly across country)

- So how does the FCC manage this? Dynamic Frequency Selection

Dynamic Frequency Selection

- DFS was required for operators and for manufacturers since early in the last decade
- Anytime an unlicensed 5Ghz Wifi device is on a shared frequency, it listens for a special signal from a TDWR
- If it hears it, the device negotiates a new frequency with clients and switches to the new frequency
- As a backup, 5Ghz wifi routers may only be operated inside a building

FCC Logic?

- If we can’t restrict 5Ghz wifi to indoors anymore
- And we want to make sure people turn off DFS near airports
- Then LOCK DOWN ALL THE THINGS!!!!!

This must be a huge problem for the FCC, right?

- No, not really
- About 10 cases over 7 years
- All involved for profit companies (AT&T, for example) who were breaking the law
- Most could have been avoided by simple UI changes to manufacturer and third-party router firmware to eliminate unintentional violations
- NONE were due to individuals

Problem Number 2

- NPRM on the ELABEL Act and Modular Transmitters (and SDRs and a ton more)
- NPRM=Notice for Proposed Rulemaking

Definitions

- Modular Transmitters: approved transmitters that can be added to hardware without requiring approval of the whole device
  - An Add-on
- ELABEL Act: act of Congress to allow electronic FCC labels instead of physical ones

Problems in the NPRM (Application for grant of certification)

2.1033.(4)(i)“For devices including modular transmitters which are software defined radios and use software to control the radio or other parameters subject to the Commission’s rules, the description must include details of the equipment’s capabilities for software modification and upgradeability, including all frequency bands, power levels, modulation types, or other modes of operation for which the device is designed to operate, whether or not the device will be initially marketed with all modes enabled. The description must state which parties will be authorized to make software changes (e.g., the grantee, wireless service providers, other authorized parties) and the software controls that are provided to prevent unauthorized parties from enabling different modes of operation. Manufacturers must describe the methods used in the device to secure the software in their application for equipment authorization and must include a high level operational description or flow diagram of the software that controls the radio frequency operating parameters. The applicant must provide an attestation that only permissible modes of operation may be selected by a user.”

Problems in the NPRM (Certified modular transmitters)

2.1042.(8)(e) “Manufacturers of any radio including certified modular transmitters which includes a software defined radio must take steps to ensure that only software that has been approved with a particular radio can be loaded into that radio. The software must not allow the installers or end-user to operate the transmitter with operating frequencies, output power, modulation types or other radio frequency parameters outside those that were approved. Manufacturers may use means including, but not limited to the use of a private network that allows only authenticated users to download software, electronic signatures in software or coding in hardware that is decoded by software to verify that new software can be legally loaded into a device to meet these requirements.”

Software defined radio?

- Radio logic could be done in software
- Allows more complex algorithms for reliable transceiving (handles beamforming or even DFS)
- Hardware could be sold in a wider range of use-cases with just changes in software
- A broader range of people could innovate and experiment

History of Software Defined Radios

- Towards the end of the last decade, the FCC saw SDRs and were horrified
- Instead of educating and enforcing laws, they wanted to avoid needing to came up with a “better” plan:
  - FCC would verify that SDR software doesn’t violate rules
  - Signing all SDR software with an FCC key
  - Require hardware to only run FCC signed software
- This was not a popular plan.

Plan two

- Tell people to secure SDRs but don’t say how
  - FCC said it was possible for open source software to be used for securing but it would have a high burden
- Separate approvals for SDRs and non-SDRs (although the devices aren’t technically that different)
  - SDRs had more difficult approval policies but were slightly more flexible in abilities
- The few that exist are niche products for hams
- SDRs don’t seem that secured (but I haven’t investigated much)
  - Possibly due to FCC being worried about the lack of a market

So why are we talking about SDRs in the NPRM?

- FCC admits in the NPRM that the SDR market is doomed and approval is too difficult
- Eliminate SDR distinction
- And apparently make a bunch of other devices meet some of the SDR requirements.
- …which were too difficult and didn’t succeed in the market.

ELABEL Act

- Allow manufacturers to show the certificate of conformance on a display instead of a piece of paper
- Rule proposal reads:

  > "(d) The necessary label information must be programmed by the responsible party and must be secured in such a manner that third-parties cannot modify it."

FCC Response

A little caught off guard

- Spokesperson said the policy didn’t affect open source operating systems
- Confidential “high ranking FCC official” said they felt there was a way to comply and protect open source
    - Apparently 4000 people disagree?

First blog post

- Julius Knapp, Chief of Office of Engineering and Technology
  - “Securing RF Devices Amid Changing Technology”
- We don’t tell you HOW to secure the radio or that you can’t use FLOSS images but you have to secure the radio
- We’re not opposed to open source as long as you secure the radio

Second blog post

- “Clearing the Air on Wi-Fi Software Updates”
- We’re going to work with stakeholders!
- We changed the U-NII guidance to not mention DD-Wrt
- Sounds warm and fuzzy but same result

I haz a mad

- I responded to this on my blog wwahammy.com
- Asked 17 questions that the FCC should have clear answers to before moving forward. They have no responded.

The “workarounds” suck

- Lockdown the entire device or
- Run the radio firmware on a co-processor where root can’t touch it (like cell phones)

- Both of these are unacceptable and should be condemned

What’s the problem with lockdown?

- Takes control away from users and puts manufacturers completely in charge
  - Lack of updates
  - Security holes
  - Unintentional violation by the user due to bad hardware
  - Functionality limits (bad mesh networking)

What’s the problem with lockdown?

- Takes control away from users and puts manufacturers completely in charge
- Ignores that different users have different privileges
  - Hams
  - Public safety personnel

What’s the problem with lockdown?

- Takes control away from users and puts manufacturers completely in charge
- Ignores that different users have different privileges
- Ends low-cost wireless radio research
  - Research labs
  - FLOSS community members (finding bugs in radio firmware, reducing power usage)

What’s the problem with lockdown?

- Takes control away from users and puts manufacturers completely in charge
- Ignores that different users have different privileges
- Ends low-cost wireless radio research
- Prevents the use of devices across some borders
  - Servicemembers
  - Business folks

Why are they doing this?!

- Reduces enforcement costs
- May want to sell part of the spectrum and need way to enforce
- Don’t trust individuals, the FLOSS community or non-companies
- Like high-tech solutions to social problems
- Want the regulatory world before SDRs

What I think the solution is

- Work with manufacturers to make sure modification of radio parameters REQUIRES reflashing
- Work with free software community to make sure default UI’s aren’t dangerous
- Require the release of radio firmware source code
- Hams should work more on protecting the spectrum for all
- Collaborative campaign to discourage inappropriate usage
- Fair, firm punishment to those who break the rules, particularly if they endanger others or do it for profit
- Create better tools for the community to find and discourage law-breakers (Cory Doctorow proposal)
- End the forcing of people and devices into regulatory boxes

Questions (and discussion)

wwahammy.com

eric@wwahammy.com

@wwahammy