

Overview

Submission in opposition of Federal Communications Commission (FCC) NPRM 15-170 and associated guidance documentation produced by the FCC.

Submitter Qualifications

Mr. Lara has been employed in the IT Security Field since late 2004 and current works as a Senior Systems Engineer of a value added re seller based out of San Diego, California which provides computer security solutions, services, and support.

Training

- Network Routing
- Network Security
- Computer Programming
- Data Loss Prevention
- Trained by (but not limited to) the following networks and security vendors
 - McAfee/Intel Security
 - Additionally includes by Ciphitrust and Secure Computing since acquired by Intel Security
 - Palo Alto Networks
 - Checkpoint
 - Cisco System

Personal Statements

All statements made in this submission are the personal opinions of Mr. Conrad Lara. No statement in this submission shall be taken to represent an official statement or endorsement by any organization.

Reasons for opposition

Ability to be handled by other means

Community Awareness Outreach

The FCC lists a total of 39 enforcement actions on its “Weather Radar Interference Enforcement” page¹ of the listed violations 17(43%) occurred in Puerto Rico 5 (12%) In Colorado with the remainder

¹ <https://www.fcc.gov/encyclopedia/weather-radar-interference-enforcement> Retrieved September 29th 2015 (Last Updated July 13th 2015)

spread among other facilities. Zero of these violations named a non corporate entity as a cause and point solely to commercial entity cause. The FCC could provide targeted outreach into those areas highest affected without the need to promulgate regulatory changes. Targeted education in the addition has ability to affect changes to deployments already completed while regulatory changes to newer produced hardware can only show results on newer production leaving a large window for potential ongoing issue.

Fine Assessment system

The FCC currently has it in its power in addition to the power to order the discontinuance of operating radios causing interference to assess fines under 47 CFR 1.80² including the ability to utilize upward adjusting criteria for “Ability to pay/relative disincentive” which can be utilized for larger companies to send a message to the industry, “Substantial economic gain” which can be used against corporations gaining financial from their actions and finally “Substantial harm” to increase the base fines due to risk of life and property that interference to a TWDR system incurs. Used in conjunction with outreach programs an effective level of cessation of interference will follow.

“Fencing” unlikely to be sustainable

RF “Fencing” or the attempt at locking down of the RF components is unlikely to be a long term method to secure the hardware in question.

Hardware Designs

Current models of “WIFI” hardware are available in two primary designs, either as a chip intended to be integrated with another processing device (such as when embedded in a device intended to extend an existing computer, commonly known as PCIE or USB add on devices) or as a System On Chip (SoC) where a processing unit that runs software is a part of (and potentially is actually built on the same silicon wafer) as the RF Components which then function in a similar manner as the self contained chips

Multiple Use of chips

Current major chip designs are designed to be used for multiple services. This multi use design allows the creating of a single base design that can be used by Part 15 Unlicensed users, Licensed Part 90 users, “WIMAX”, 4.9GHz Public Safety and other services either now in existence or to later created. Since these chips are intended to be used as a single source component across all sectors they can not forcefully be locked to a specific band range.

Failure of “fencing” via access control means to the chip

In order to secure add on chips via a “secure channel” some means of authentication would presumably be required, however since the authentication method would have to be present in all on board devices it can be obtained and later compromised rendering the method ineffective. Vendors have historically tried this in the past to secure their hardware for one reason or another. Tivo video records, Apple

² http://www.ecfr.gov/cgi-bin/text-idx?mc=true&node=se47.1.1_180&rgn=div8 Retrieved October 9th

iPhone's and iPad's are two very common product families that have been attempted to lock down by their manufactures and failed. To rely on such a method would likely leave the Commission in a spot worse than it is today, as to date open source projects have worked with adhering to regulatory requirements³. Should programmers in the open source community be forced to dedicate more time to bypass on board security measures a possibility exists that less time will be spent on enforcing regulatory compliance.

Affect on other services

As noted previously the hardware designed for these services is designed to be used across multiple services with small changes. By promulgating rules that force the restriction of the hardware could cause the lesser services, such as Public Safety (4.9GHz) and the Amateur Radio Service (Part 97) to sufferer from significantly increased costs, significantly fewer options, and potentially no options at all.

Amateur Radio Service (Part 97)

Restrictions to the ability to load firmware on modern wifi hardware will have a significant affect on the Amateur Radio Service.

Communications needs are changing, no longer is simple voice communications acceptable when the nation is in a state of emergency. Data communications with photo, video, conference audio, etc are vital to emergency services and served agencies providing services to the public in time of need.

Amateur Radio has been responding to this need, groups like the Amateur Radio Emergency Data Network (AREDN)⁴ are dependent upon the ability to readily obtain hardware in an affordable and efficient manner that can be utilized by licensed operators. Restrictions on the loading of firmware on the devices or the restriction to access the RF frequency components as permitted to licensed Part 97 operators will degrade the ability for these vital members of the disaster response to provide services to the public in time of need.

Increased costs to the Commission by needing to increase enforcement actions

Should Amateur Radio Operators be denied the ability to migrate WIFI devices to “clear” Part 97 frequency space outside the normal WIFI band than they will likely be forced to utilized frequency inside the WIFI space. As most devices operating in the WIFI bands are operating under Part 15 they are secondary to Part 97 operations. Amateur Radio Operators will therefor be forced to speak with local interference sources and attempt to convince them to either shield their signal or disable their signals all together. This could become quite costly for the Commission Enforcement division as the prevalence of WIFI devices could necessitate a constant presence in highly populated areas at a time when the Commission is attempting to scale back it enforcement office location count⁵

Risk to national security and national cyber defense

While the Commission has much need to enforce the appropriate and legal use of the radio spectrum so that the greatest number of Citizens can benefit from the use of limited RF spectrum in this case the Commission needs are also affected by the needs of the nation outside of the RF spectrum.

³ <https://wireless.wiki.kernel.org/en/developers/regulatory> Retreived October 9th

⁴ <http://www.aredn.org>

⁵ https://apps.fcc.gov/edocs_public/attachmatch/DOC-334393A1.pdf

Commercial wireless routers are often released, maintained for a short period of time, and then abandoned by their manufacturers as they move onto a newer product. Care must be taken however as Wireless Routers are multifunction computers that can be subject to infection.⁶⁷⁸⁹¹⁰ As manufacturers take time to issue patches or worse yet fail to patch older hardware at all, the United States will find itself in the position of ever increasing in frequency security risks posed by these insecure devices. Permitting without limitation 3rd party implementations allows more parties to provide security to growing number of vulnerable devices and protect national security.

Consultation with the Department of Homeland CyberSecurity division should be taken prior to the restriction of any operating software on wireless devices since third party software at this time fill a crucial need in protecting the national security.

Restriction on the development of emerging technology and degradation of radio frequency spectrum.

Restriction upon what software can be loaded onto a device would further restrict the evolution of the devices. While the FCC needs to be concerned with emissions standards the FCC does not need to concern itself with protocols that run atop those emissions. Restrictions upon the loading of software, that by its very need requires the ability to interact with the RF chips directly, will reduce the ability for the development of extensions of technology. Today Time Division Multiple Access (TDMA) is used in some closed single vendor implementations which can provide for significant improvement in the efficiency of the use of the RF spectrum as compared to the more common Carrier Sense Multiple Access (CSMA), by prohibiting the development of this and similar technology the Commission will be left in a position where spectrum could be much more efficiently utilized but the capability to do so has been denied by rule.

Inconsistent with recent Commission proceedings

The Commission recently backed the rights of consumers in its Net Neutrality proceedings with its issuing of the order for an Open Internet¹¹. Wireless devices are a vital part to an open internet, restrictions on what firmware can run atop and its ability to access the radio modems onboard locks the consumer into a position where they may no longer have a choice. The Commission found in its proceedings that providers either have or may consider interfering with internet traffic, having cut off this plane the next target would be consumer devices to enforce the restrictions at the 'edge' which can easily be done in locked down non modifiable devices. It is in the best interest of the Commission and the nation to continue to promote open access on any item that can or could connect to the global internet.

6 <http://arstechnica.com/security/2015/09/attackers-install-highly-stealthy-backdoors-in-cisco-routers/>

7 <http://www.pcworld.com/article/2985040/networking-hardware/malware-implants-on-cisco-routers-revealed-to-be-more-widespread.html>

8 <http://www.computerworld.com/article/2486032/malware-vulnerabilities/vulnerabilities-in-some-netgear-router-and-nas-products-open-door-to-remote-.html>

9 <http://www.welivesecurity.com/2014/02/17/mysterious-moon-worm-spreads-into-many-linksys-routers-and-hunts-new-victims/>

10 <https://threatpost.com/disclosed-netgear-router-vulnerability-under-attack/114960/>

11 https://apps.fcc.gov/edocs_public/attachmatch/FCC-15-24A1.pdf

Alternative Changes

In light of the above opposition I submit the following potential alternative/additional changes the Commission could adopt to reduce the concerns presented above.

Open Disclosure to increase compliance from third parties.

As noted previously the open source community does provide general compliance enforcement already and has shown no desire to violate these regulations. For as long as hardware has existed an end user could conceivably modify the device to perform in a manner not authorized. Legitimate users would utilize the devices in the manner intended. Current RF chips as noted above perform all the RF actions and only protocol related and frequency items are left to the operating systems in most cases. In many cases these designs are reversed engineers, only now are manufactures beginning to work with the open source community more frequently. Should the Commission wish to ensure the performance of the RF Spectrum the Commission could instead promulgate rules requiring manufactures to provide full open documentation on chip sets and deployments which would ensure open source deployments and 3rd party firmwares maintain the compliance levels the Commission has ordered.

Requirement to open hardware to licensed users

Should the Commission feel the need to restrict access for unlicensed users is so great as justify passing these regulations the Commission should promulgate rules requiring manufactures to provide open access to the software onboard these devices including to the RF to users whom are licensed to make changes, including but not limited to, the Amateur Radio Service (Part 97)

Sincerely,

/s/

Conrad Lara