FCC Rules on FOSS and Software-Defined Radio

Software Freedom Law Center

July 6, 2007

1 Executive Summary

The Software Freedom Law Center (SFLC) has examined the Federal Communication Commission's (FCC) rules, which go into effect today, governing Software Defined Radio (SDR) devices and concluded that the rules do not restrict the activities of independent developers and distributors of Free and Open Source Software (FOSS) designed for use with SDR devices. While the FCC's position on FOSS is more conservative than is necessary, the FCC has given a qualified endorsement to the use of FOSS by SDR manufacturers by recognizing the benefits of using FOSS in wireless products. The FCC's SDR rules create an opportunity for wireless hardware manufacturers, the FOSS community, and the FCC to communicate openly and productively about the ability of public disclosure and open standards to strengthen the security and robustness of wireless devices.

2 Background

2.1 FCC SDR Rules

On March 11, 2005, the FCC released a set of rules outlining an alternative method for certification of devices whose radio frequency and power characteristics can be modified by software (such devices are designated Software Defined Radio devices).[1] The rules allow manufacturers who have certified under the new process to update the software on the devices without re-certifying the devices with the FCC.

The rules require any manufacturer certifying a device under the new process to take steps to prevent "unauthorized" changes to the software on the device that might alter its radio frequency and power parameters in a way that takes it out of compliance with the regulations known as FCC Part 15 regulations.[2] The specific technology implemented to accomplish this task is left to the manufacturers seeking certification, although the FCC suggests several possible mechanisms that can serve as such "security measures."[3]

---

[1] *See Report and Order* in ET Docket No. 03-108, 20 FCC Rcd 5486 (2005), ("*Cognitive Radio Report and Order*"). Summary available at `http://edocket.access.gpo.gov/2005/05-8808.htm`.

[2] *Cognitive Radio Report and Order* at 5488.

[3] *See Cognitive Radio Report and Order* at 5509.

In response to a petition from Cisco Systems, Inc., the FCC issued a Memorandum Opinion and Order on April 25, 2007, making two clarifications to the rules.[4] First, the FCC clarified the scope of the rules to require certification under the new process of any device that uses software to comply with the Part 15 regulations if such software is "designed or expected to be modified by a party other than the manufacturer."[5] Second, the FCC stated a position regarding the use of Free and Open Source Software (FOSS) on SDR devices. The FCC acknowledged the use of FOSS by device manufacturers and noted some of the advantages of FOSS for the industry. However, citing concerns regarding publishing information relating to security measures, the FCC stated that a SDR device which uses FOSS to build the "security measures" protecting the software against modification would face a "high burden" during the certification process "to demonstrate that it is sufficiently secure."[6]

2.2 Linux-based Wireless Devices

The FCC notes in its Memorandum Opinion and Order that the industry now commonly uses both the kernel named Linux and complete FOSS operating systems in wireless radio devices under its regulatory control. For example, many 802.11 wireless network routers use FOSS to provide a fully functional system, including network address translation (NAT), network firewalling, intranet web servers, and other network management features. Such functionality, which if licensed as individual proprietary components can be prohibitively expensive, is readily available with any FOSS operating system. Many manufacturers have therefore chosen to configure their devices with these FOSS systems rather than proprietary alternatives. In such a configuration, almost none of the FOSS on the device interacts directly with the FCC-regulated radio hardware. Typically, only small pieces of code either running as a Linux kernel module and/or as a wholly independent firmware on the chip itself actually constitute an SDR component whose modification would need to be limited by the "security measures" described in the FCC's rules. This white paper focuses primarily on these small components, but the reader should not lose sight of how much software on the standard FOSS-based FCC-regulated consumer devices remains far from the regulatory control of the FCC.

3 Legal Analysis

3.1 FCC Jurisdiction Does Not Extend to Independent Software Developers

The FCC is a statutory body with a grant of jurisdiction strictly defined by Congress.[7] First, it has the power to regulate "interstate and foreign communication by wire or radio."[8] This primary jurisdictional grant gives it wide latitude to make and enforce rules for broadcasters and telecommunication carriers. Second, it has ancillary jurisdiction to make rules and regulations necessary for carrying out its primary responsibilities.[9] This ancillary jurisdiction includes the power to make "reasonable regulations ... governing the interference potential of devices which in their operation are capable of emitting radio frequency energy."[10] It is much more narrowly constrained than the FCC's primary jurisdiction over broadcasters and carriers, because courts, fearful that the FCC's powers would become "unbounded" if it were allowed to make rules governing any activity or party that might have an effect on radio or wire transmissions, have precluded such a reading of the FCC's jurisdictional grant.[11] Thus, while the FCC's ancillary jurisdiction reasonably extends to

---

[4]ET Docket No. 03-108 (2007).

[5]*Memorandum Opinion and Order* at page 3, available at `http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-07-66A1.pdf` (quoting *Cognitive Radio Report and Order* at 5504; 47 C.F.R. §2.1).

[6]*See Memorandum Opinion and Order* at page 4.

[7]*Michigan v. EPA*, 268 F.3d 1075 (D.C. Cir. 2001); *Louisiana Pub. Srev. Comm'n v. FCC*, 476 U.S. 355 (1986).

[8]47 U.S.C. §152 (a).

[9]47 U.S.C. §154 (i).

[10]47 U.S.C. §302 (a).

[11]*FCC v. Midwest Video Corp.*, 440 U.S. 689 (1979).

regulating the marketing and sale of devices that create active radio interference, it does not extend to such activities as the construction of buildings that might interfere with radio signals.[12]

Similarly, the FCC's ancillary jurisdiction cannot reasonably extend to the development of software by parties uninvolved in the marketing or sale of radio devices. Congress did not contemplate the FCC as a generic technology regulatory agency, and courts have repeatedly limited the FCC's reach when it attempted to make rules outside of the realm of the distribution or marketing of equipment capable of wire or radio signal transmission.[13] Attempts by the FCC to regulate the activities of software developers not engaged in the importation or marketing of radio devices and not employed by telecommunication carriers are likely to be met with similar judicial restriction.

3.2 FCC Rules for SDR Device Certification Only Affect Radio Equipment Manufacturers

Even if the FCC did have the power to regulate independent software development, it has promulgated no rules governing such activity. Its new rules related to SDR are addressed to "manufacturers" of radio "equipment," modifying the rules for certification of such "hardware-based device[s]" prior to their "marketing or importation."[14] No other parties or activities are affected by the regulations. Thus, unless a given entity engages in the marketing or importation of hardware-based radio equipment, it is unaffected by these regulations.

3.3 FCC Rules Govern Equipment, Not Software

The FCC has promulgated the SDR rules as a modification to its existing regulations governing the certification for marketing and sale of devices that may interfere with radio transmissions.[15] These rules limit the ability to "manufacture, import, sell, offer for sale, or ship devices or home electronic equipment and systems, or use devices, which fail to comply with regulations promulgated pursuant to this section."[16]

Since software is a representation of a mathematical algorithm, it is not a "device", "home electronic equipment" or a "home electronic ... system."[17] Further, there is no precedent for applying the device certification rules to software except as installed as a component of a specific hardware device. Indeed, the FCC has explicitly limited the certification requirements to "hardware-based device[s]."[18] Both of these facts make it clear that the FCC rules do not apply to software by itself, but only to hardware-based devices.

---

[12]*Illinois Citizens Committee for Broadcasting v. FCC*, 467 F.2d 1397 (7th Cir. 1972).

[13]See *American Library Association v. FCC*, (D.C. Cir. 2005) (the FCC has no power to regulate television components unrelated to signal reception); *Illinois, supra*, 467 F.2d 1397 (the FCC lacks jurisdiction over objects that interfere with television transmissions).

[14]See *Cognitive Radio Report and Order* at 5505.

[15]See *Cognitive Radio Report and Order* at 5487. Codified at 47 C.F.R. §0.457, §2.1, §2.932, §2.944, §2.1033, §2.1043, and §15.202.

[16]47 U.S.C. §302.

[17]The only place where the FCC's rules or its enabling statute include software within the definition of any of these terms is in the context of regulating telecommunications carriers: the definition of "Telecommunications Equipment" in 47 U.S.C. §153 (45) states that the term "includes software integral to such equipment." This definition explicitly excludes "customer premises equipment." Thus, it applies only to equipment used by carriers, on the premises of the carriers, to provide telecommunications services. The careful limitation of this definition to carrier equipment is consistent with the FCC's broad jurisdiction over carriers' business practices, allowing the FCC to regulate software in this specific domain where Congress is unwilling to grant jurisdiction over software developed or used by other parties not under the FCC's direct jurisdiction. In addition, the explicit inclusion of "software integral to such equipment" in this definition implicitly excludes software from other uses of the term "equipment" in the statute. If Congress had intended the general term "equipment" to include software, it would have defined it accordingly, as it did in the limited case of "Telecommunications Equipment."

[18]See *Cognitive Radio Report and Order* at 5505.

3.4   FCC Rules Contemplate FOSS SDR Development without Restricting It

The FCC's Memorandum Opinion and Order clarifying its SDR certification rules acknowledges the use of "open source software" by SDR device manufacturers and notes the advantages FOSS provides to the industry. It declines to forbid or restrict the use of FOSS on SDR devices. However, it discourages use of FOSS in the "hardware and software security elements" of SDR devices by stating that systems "*wholly* dependent on open source elements" would have a "high burden" to demonstrate their security during the certification process.[19]

Nowhere do the rules restrict any party other than a manufacturer seeking certification for a device. Even in that case, they do not restrict the manufacturer's activities directly, but simply warn that the certification will be less likely to be granted if the manufacturer relies "*wholly*" on FOSS in building the device. The rules acknowledge the activities of the FOSS community in developing radio device software and, in keeping with the FCC's jurisdictional limitations, decline to formulate rules governing any participant in this activity except manufacturers seeking certification for their devices.

This reluctance on the part of the FCC to create regulations for technological development — beyond regulating the actual marketing of devices — is consistent with the FCC's position on experimental or specialized equipment. Such equipment is exempt from the certification requirements if it is not marketed to the public and is only used under controlled conditions.[20] It is allowed to be developed and distributed as long as it is used for such limited purposes. Thus, even entities who install and run software — FOSS or otherwise — on radio hardware devices for the purposes of testing, research or development are exempt from the new SDR certification rules as long as they abide by the other applicable FCC rules.

4   Policy Analysis

The FCC's rules on SDR device certification present two positive developments for FOSS deployment in the wireless technology space. First, the FCC permits the use of FOSS in all but a very narrowly constrained subsystem on a specific type of device. Second, the FCC has provided much greater regulatory clarity than has existed on this issue since the commencement of the SDR rulemaking process in 2003. This freedom to deploy FOSS and the clarity of the FCC's position allows hardware manufacturers and FOSS developers to openly collaborate on most parts of SDR device design, and it frees software developers from concerns that they might have to deal with legal issues related to the FCC.

Unfortunately, the FCC has not gone as far as it could in embracing and encouraging the use of FOSS by SDR device manufacturers. Its rules express reservations about the security of FOSS-based systems based on the notion that "making information on security measures publicly available could assist parties in determining ways to defeat them."[21] However, there is broad consensus among software security experts that public disclosure of security design actually results in more secure systems, especially when the system is subject to repeated, low-cost attacks by attackers who can share information freely among themselves.[22]

---

[19] *See Memorandum Opinion and Order* at page 4 (emphasis added).

[20] 47 C.F.R. Part 2.803.

[21] *Memorandum Opinion and Order* at page 4.

[22] *See* Swire, Peter P., *A Model for When Disclosure Helps Security: What is Different About Computer and Network Security?*, Journal on Telecommunications and High Technology Law, Vol. 2, 2004. Available at SSRN: http://ssrn.com/abstract=531782. Swire makes a technical, economic, and regulatory argument for different disclosure models maximizing security based on the nature of the system being designed. He finds that disclosure tends to result in higher security for systems like SDR consumer products that are exposed to multiple attackers who can share information with each other. Disclosure of security designs for such devices tends to benefit designers more than attackers, as the designers can learn from each other and improve their designs accordingly, offsetting the advantages the attackers already have in information-gathering and -sharing. *See also*, Schneier, Bruce, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World*, pp.119-128 (2003). Schneier deconstructs the myth that "security through obscurity" is an effective strategy, noting the brittleness of systems designed under that approach.

SDR devices used by consumers fit this description: the software on a cellphone or 802.11 card is exposed to virtually unlimited attack by anyone who purchases the device, and anything learned from such an attack can be communicated at low cost to fellow attackers. Design details disclosed by manufacturers, on the other hand, have tremendous benefits for other manufacturers' ability to spot security flaws, but they provide little benefit to attackers. These arguments are articulated in greater depth in a Petition for Reconsideration submitted to the FCC in June 2007 by the SDR Forum, a wireless industry consortium with a vested interest in the SDR rulemaking process.[23]

On a positive note, the FCC does signal in its Memorandum Opinion and Order that it is open to persuasion on the subject of FOSS-based security systems. It states that "manufacturers should not intentionally make the distinctive elements that implement that manufacturer's particular security measures in a software defined radio public, *if doing so would increase the risk that these security measures could be defeated or otherwise circumvented to allow operation of the radio in a manner that violates the FCC's rules.*"[24] This qualification suggests that the FCC is not committed to this proposition, as does the doubly qualified message that only devices "wholly" (not mostly, or partly) based on FOSS would face a "high" (not insurmountable) burden during certification. The FCC's refusal to categorically prohibit FOSS in any part of an SDR system reads as an invitation to the wireless device industry and the FOSS community to demonstrate the suitability of FOSS for the design of all software subsystems of SDR devices.

5   Conclusion

The SDR rules promulgated by the FCC represent a positive development for FOSS developers working in the wireless space. The rules allow FOSS developers not affiliated with device manufacturers to continue work on their software without restriction. They allow SDR manufacturers to employ FOSS for most of the functionality of their devices, and they leave open the possibility that a device using a purely FOSS-based software platform could also pass FCC certification if it managed to demonstrate the soundness of its security strategy. The rules should spur FOSS developers and hardware manufacturers to collaborate on design strategies that maximize the efficiency, robustness, and freedom inherent in the FOSS development process while ensuring that manufacturers satisfy the FCC's security mandate.

---

[23]*See* SDR Forum's *Petition for Reconsideration* in ET Docket No. 03-108 (2007). Available at `http://www.sdrforum.org/uploads/pub_439156SDRF-07-A-0012-V0_0_0_Response_to_MOO.pdf`.

[24]*See Memorandum Opinion and Order* at page 4 (emphasis added).