FCC forced firmware lockdown - what now?

Simon Wunderlich

sw@simonwunderlich.de

May 4, 2016

WIRELESS
BATTLE
OF THE
MESH v9
PORTO

Structure of this discussion

- Introduction on FCC regulations, activities and reactions from industry and community
- Update on the EU status by Max Mehl (FSFE)
- Open discussion on technical and/or political solutions in the auditorium. Remote participation by William Lumpkins (IEEE).

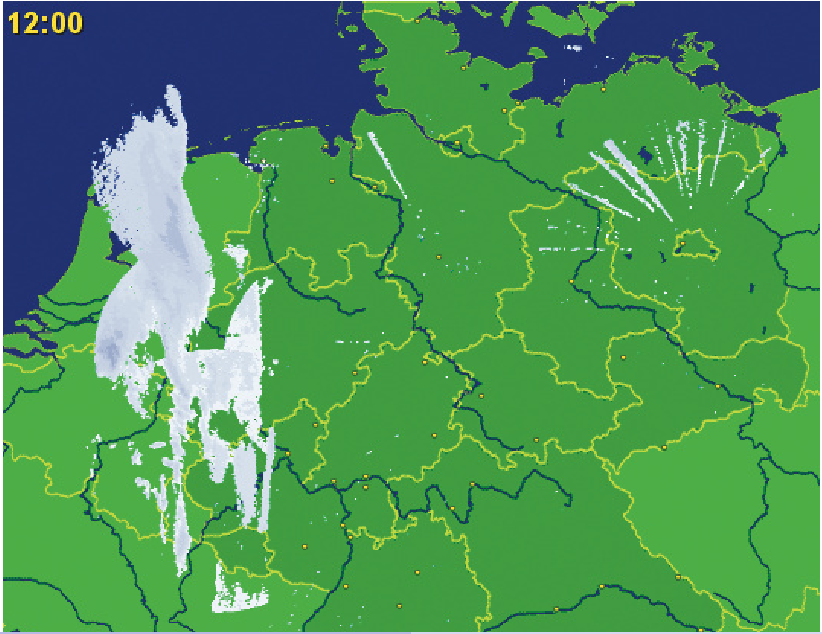
What happened?

- Every (radio emitting) device sold in the US must have FCC (Federal Communications Commission) approval
- According to new rules in the FCC, U-NII devices operating under Part 15C (operating on 5GHz) must implement ”device security” to prevent users to use ”illegal” radio parameters.
- There is a similar directive in Europe to be implemented: Directive 2014/53/EU, as well as Canada: RSS-247

What is the FCCs goal

- Prevent ”normal users” to use illegal channels (channels 12, 13, 14 on 2.4 GHz)
- Prevent using too high transmission power
- Prevent using DFS channels (5.3 - 5.7 GHz) without having DFS functionality
- make sure DFS is running near airports with Terminal-area Doppler Weather Radar (TDWR), which is primarily relevant for those operating a wifi router outside within a mile or so of 45 airports in the US (operate on 5.60-5.65 GHz).

Weather radar disturbance by WiFi APs



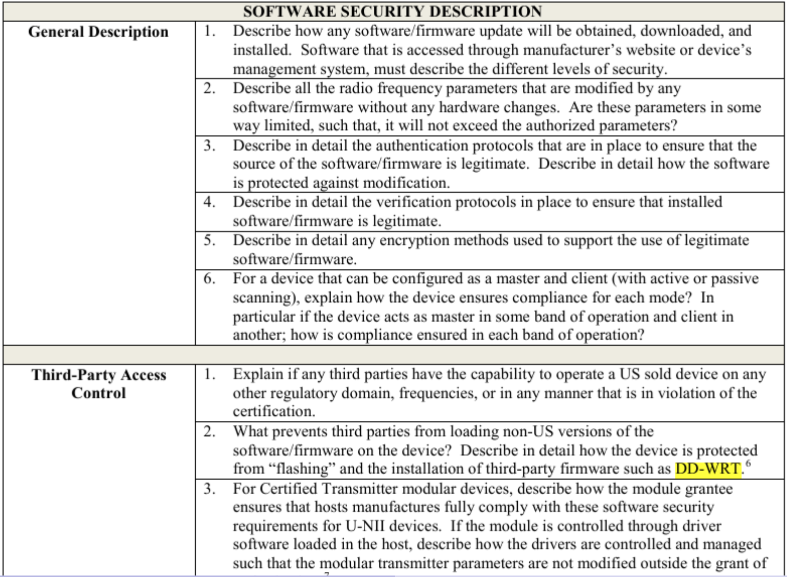
FCC rules (i)

- 15.407(i): Device Security. All U-NII devices must contain security features to protect against modification of software by unauthorized parties.
    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. 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 and must describe the methods in their application for equipment authorization.

FCC rules (ii)

- Manufacturers must take steps to ensure that DFS functionality cannot be disabled by the operator of the U-NII device.
- An applicant must describe the overall security measures and systems that ensure that only:
  1. Authenticated software is loaded and operating the device.
  2. The device is not easily modified to operate with RF parameters outside of the authorization.

Guidance Document / Questions (DD-WRT removed by now)



SOFTWARE SECURITY DESCRIPTION	
General Description	1. Describe how any software/firmware update will be obtained, downloaded, and installed. Software that is accessed through manufacturer's website or device's management system, must describe the different levels of security.
	2. Describe all the radio frequency parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited, such that, it will not exceed the authorized parameters?
	3. Describe in detail the authentication protocols that are in place to ensure that the source of the software/firmware is legitimate. Describe in detail how the software is protected against modification.
	4. Describe in detail the verification protocols in place to ensure that installed software/firmware is legitimate.
	5. Describe in detail any encryption methods used to support the use of legitimate software/firmware.
	6. For a device that can be configured as a master and client (with active or passive scanning), explain how the device ensures compliance for each mode? In particular if the device acts as master in some band of operation and client in another; how is compliance ensured in each band of operation?
Third-Party Access Control	1. Explain if any third parties have the capability to operate a US sold device on any other regulatory domain, frequencies, or in any manner that is in violation of the certification.
	2. 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 firmware such as DD-WRT.[6]
	3. For Certified Transmitter modular devices, describe how the module grantee ensures that hosts manufactures fully comply with these software security requirements for U-NII devices. If the module is controlled through driver software loaded in the host, describe how the drivers are controlled and managed such that the modular transmitter parameters are not modified outside the grant of

What is the problem with that?

- highly integrated SOC designs make it difficult to "lock" only the radio parameters
- If there is no possibility to lock the hardware (by eeprom, radio firmware, etc), manufacturers can only lock the whole router firmware
- locking router firmware is not desirable:
  - OpenWRT can't be used anymore (at least no self-compiled OpenWRT)
  - Security problems are kept open if vendors don't care (and most often, they don't)
  - New features and performance enhancements can't be implemented by tech-savvy users
  - Wireless communities and companies can't easily source devices anymore

Why do we care (in the EU or non-US markets)?

- US market for electronics is one of the biggest
- FCC regulations are adopted by other countries, and trade agreements exist to sell FCC approved devices in other countries as well
- If (asian) vendors start to lock down their hardware, not only the US market but also the EU market will be affected.
- This lock down already started, e.g. with TP-Link and Ubiquiti access points

What happened?

- 2014, June 2nd: FCC accepts test reports for updated rules for U-NII devices operating under Part 15C
- 2015, May 28: Canada (IC) adds security feature requirement (RSS-247)
- 2015, June 1st: stop approval of devices under the old rules (postponed to December?)
- 2016, February 17th: lockdown of TP-Link devices was reported
- 2016, June 1st: stop marketing under the old rules (i.e. no new devices can't be sold)
- 2016, June 13th: European countries need to implement directive 2014/53/EU by member states.
- 2017, June 13th: Devices in Europe must be certified according to the new regulations according to 2014/53/EU

Affected devices

- WiFi Access Points
- Other devices which use WiFi and can use Access Point Mode - Phones, Tablets with Cyanogenmod, etc

Political activities

- Battlemesh v8 workshop raised lots of awareness
- Over 3000 comments on FCC filing 15-170
- SaveWiFi iniative on libreplanet: `https://libreplanet.org/wiki/Save_WiFi`
- FSFE joint statement against Radio Lockdown in the EU
- Mailing lists at PRPL foundation and bufferbloat sites to discuss and organize countermeasures
- However, FCC rules haven't been changed, and are still in place

Technical workarounds and ideas

- Split radio and (linux) host system - e.g. minimal, signed radio firmwares? Anyone working with chip vendors?
- Use general purpose boards and PCI Express WiFi cards - more expensive
- Localize hardware for not affected markets - e.g. for South America, etc. This doesn't solve the problem for US and EU though

Workarounds ... really?

- Solving the "TWDR" problem with this regulations seems to be shooting with way (!) too big cannons on the sparrow
- Alternative: As before, check manually with a "radio van" and fine people. They know what they are doing, and they should be held responsible.
- How big is the problem? 10 cases in 7 years (according to Eric Schultz, need to check sources)
- all cases involved profit companies who misconfigured their routers, and could easily be avoided by UI changes.

Rarity (ripped from Eric Schultz' Slidedeck)

- Routers within a few miles of an airport...
- And running in the 5Ghz range...
- ... spefically covering 5.60 - 5.65 GHz
- And running on a DFS channel...
- And modified to ignore the DFS signal...
- And the antenna is outside...
- And the antenna is high enough to transmit and interfere with the radar beam...
- But not too high because the beam is actually only 0.3 degrees wide...
- And the TDWR radar has to be turned on...
- Which is only turned on when there's storm of a sufficient size.

Questions to discuss about

- Etherpad: `http://tinyurl.com/WBMFCC`
- What are your experiences with recently certified WiFi Hardware?
- How can we still keep OpenWRT on these devices?
- What can we suggest to Hardware vendors so that they keep their router firmware open for community?

Further readings

- PRPL foundation mailing list on the topic: `http://lists.prplfoundation.org/cgi-bin/mailman/listinfo/fcc`
- Bufferbloat FCC mailing list on the topic: `http://lists.redbarn.org/mailman/listinfo/bufferbloat-fcc-discuss`
- FCC U-NII update and further information: `https://apps.fcc.gov/oetcf/kdb/forms/FTSSearchResultPage.cfm?id=39498&switch=P`
- comments on the issue at FCC (closed by now): `http://apps.fcc.gov/ecfs/proceeding/view?name=15-170`
- Summaries on the EU Directive: `https://juliareda.eu/2015/10/dear-european-governments-dont-endanger-free-and-open-wifi-networks/`, `https://blog.tohojo.dk/2015/10/the-new-wifi-regulations-in-europe.html`
- FSFE information and statement: `https://fsfe.org/activities/radiodirective/`
- Great talk by Eric Schultz: `https://wwahammy.com/libreplanet-presentation-of-yes-the-fcc-might-ban-your-operating-system/`
- News coverage:
  - Hackaday: `http://hackaday.com/2016/02/26/fcc-locks-down-router-firmware/`
  - Wired: `http://www.wired.com/2016/03/way-go-fcc-now-manufacturers-locking-routers/`
  - IEEE magazine: `http://sci-hub.io/10.1109/MCE.2016.2516063` (not the original, no IEEE paywall, and note that I personally don't agree with quite a few points in that article)

Thank you!

- Thank you very much for your attention!