

Before the  
FEDERAL COMMUNICATIONS COMMISSION  
Washington, DC 20554

In the Matter of	)	
	)	
Amendment of Part 0, 1, 2, 15 and 18 of the	)	ET Docket No. 15-170
Commission’s Rules regarding Authorization	)	
Of Radio frequency Equipment	)	
	)	
Request for the Allowance of Optional	)	RM-11673
Electronic Labeling for Wireless Devices	)	

**COMMENT of SUSAN SONS**

**To the Commission:**

**Executive Summary**

The rulemaking, as proposed, threatens to exacerbate the already deplorable state of wirelessly-networked device security, posing a direct threat to computer networks, vehicles, and medical devices with wireless capability, and by extension to any network that those networks may communicate with.

**Table of Contents**

1. Introduction of the Author
2. Current State of Wireless Network Device Firmware
3. Cybersecurity Benefits of Independent Research and Development
4. Impact on Wireless Network Devices’ Spectrum Usage
5. Conclusion
6. Thanks

## **1. Introduction of the Author**

**Susan Sons** serves as a Senior Systems Analyst at Indiana University's Center for Applied Cybersecurity Research (CACR), where she works as part of the NSF-funded Center for Trustworthy Scientific Cyberinfrastructure (CTSC) to secure the information assets of NSF-funded scientific facilities and projects, and contributes to computer security efforts in operations of the DHS-funded Software Assurance Marketplace (SWAMP) project. She recently led a project to secure the reference implementation of the Network Time Protocol which resulted in a re-implementation of the heretofore insecure and largely unmaintained critical software infrastructure which is undergoing continued testing and improvement for the benefit of the entire internet. Susan is an Amateur General Class radio operator with the call sign KC9PUA.

## **2. Current State of Wireless Network Device Firmware**

Wireless network devices -- that is, devices with radio components that are able to connect to computer networks or directly to other computer systems -- have become nearly ubiquitous in home, commercial, scientific, defense, and governmental settings. Many of these devices are blurring the line between what has traditionally been considered a software defined radio and general purpose computing devices. These devices are frequently in use in general IT infrastructure, scientifically essential, and life-critical applications due to the growing dependence of federal agencies (e.g. NSF, DOD, DOE, DHS) and the commercial sector on COTS (Commercial Off-The-Shelf) devices.

COTS wireless network devices are one of the most common entry points for cyberattacks into computer networks, due to the poor quality of their firmware and the difficulty in updating said firmware to close security holes. Device manufacturers have not done an adequate job of preventing attacks to network infrastructure<sup>1,2</sup>. The situation is so bad that someone developed and released a worm (a self-propagating computer program) that infects vulnerable routers in order to secure them against easily-exploited vulnerabilities in their manufacturers' firmware<sup>3</sup>!

Fortunately for users and network owners alike, a variety of community efforts make more secure firmware available for many common wireless network devices, and provide these improvements to the world under Open Source licenses to ensure their wide distribution. In the face of widespread security problems in manufacturers' firmware<sup>4</sup>, many of us in the security world are encouraging device owners to install such Open Source firmware in order to protect their devices. Routers are rare in the Internet

---

<sup>1</sup> <http://www.cnet.com/news/asus-router-vulnerabilities-go-unfixed-despite-reports/>

<sup>2</sup> <http://www.itbusinessedge.com/blogs/data-security/router-vulnerability-highlights-iot-security-risks.html>

<sup>3</sup> <http://www.symantec.com/connect/blogs/there-internet-things-vigilante-out-there>

<sup>4</sup> <http://www.cnet.com/news/top-wi-fi-routers-easy-to-hack-says-study/>

of Things (IoT) in that they usually can be upgraded with third-party firmware, allowing for the replacement of buggy and insecure<sup>5</sup> firmware from the manufacturer. Unfortunately, many manufacturers don't choose to undertake fixing such shortcomings themselves: "Hacking routers is an ideal way...to maintain a persistent hold on network traffic because the systems aren't updated with new software very often or patched in the way that Windows and Linux systems are."<sup>6</sup>.

### **3. Cybersecurity Benefits of Independent Research and Development**

The ability of users to install third-party firmware on their wireless network devices is essential to independent research and development efforts that benefit the whole internet. Placing restrictions on this ability would have a chilling effect on research and development essential to the wireless network device industry.

Manufacturers of wireless network devices rarely support (i.e. provide security fixes for) those devices for more than a few months to two years after the manufacturing date. Often, these devices are still being sold to consumers long after the manufacturers have stopped providing what few security improvements they provide in the first place. By installing third-party firmware, users can fix vulnerabilities through which a malicious third party could attack the device or other devices near or connected to it, including causing the device to operate outside the appropriate power, frequency, and modulation type in ways that would interfere with other devices and services.

The manufacturers who do make an effort to secure their wireless network devices often do so by leveraging software advances made by independent researchers<sup>7,8</sup>. For example, Buffalo Routers ship with the open source DD-WRT firmware<sup>9</sup>. Some Netgear devices now ship with a modified version of the open source OpenWRT firmware installed by the manufacturer. Using open source firmware in this way allows Netgear to push out security fixes produced by the OpenWRT development team, which is less effort for Netgear than writing a fix for each known problem themselves. This is possible only due to the ability of OpenWRT community members to access and test their open source firmware on Netgear's devices. It is unknown exactly how big a negative impact removal of the independent R&D pipeline would have on manufacturers' ability to ship usable, let alone secure, firmware on wireless network devices.

---

5

<http://www.computerworld.com/article/2476543/cybercrime-hacking/researchers-find-about-25-security-vulnerabilities-per-internet-of-things-device.html>

<sup>6</sup> <http://www.wired.com/2013/09/nsa-router-hacking/>

<sup>7</sup> <http://betanews.com/2015/10/07/linksys-linux-wrt1900acs-router-open-source/>

<sup>8</sup> [http://www.phoronix.com/scan.php?page=news\\_item&px=google-onhub-router](http://www.phoronix.com/scan.php?page=news_item&px=google-onhub-router)

<sup>9</sup> <http://www.cnet.com/news/buffalo-releases-dd-wrt-based-wi-fi-routers/>

#### **4. Impact on Wireless Network Devices' Spectrum Usage**

Independent research and development enabled by usage of third-party firmware on COTS also helps to manage the spectrum usage of wireless network devices. The Bufferbloat Project<sup>10</sup> in particular solved technical issues that were causing congestion and other problems that slowed down internet connections around the world. The Bufferbloat Project produced FQ\_CODEL, a protocol for governing the flow of packets across a network, which is now standard on many wireless network devices, including in many manufacturers' router firmware. Independent researchers from this project are now focused on the MakeWifiFast<sup>11</sup> initiative, yet another technical research project that promises to improve network performance *without* increasing the spectrum needs of wireless networks. Like Bufferbloat, MakeWifiFast will only work if independent researchers can test firmware on commodity hardware. This research and development is essential to the evolution of secure and efficient wireless network technology without untenable increases in wireless spectrum usage.

#### **5. Conclusion**

The proposed rulemaking limiting the access of third parties and use of third party firmware will have serious negative consequences for the security of all computer networks and devices with wireless networking capabilities, by preventing independent research and development efforts that are essential to securing these devices. By removing the proposed rules regarding measures to prevent consumers from replacing manufacturers' software and/or firmware with their own, the FCC would instead enable these vital research and development activities to continue.

#### **6. Thanks**

Special thanks to CACR staff members Ryan Kiser, Vineeta Sangaraju, and Von Welch for their help in drafting and editing these comments.

*Susan E. Sons*

*U.S. Citizen*

*Senior Systems Analyst, Center for Applied Cybersecurity Research  
Indiana University*

---

<sup>10</sup> <http://bufferbloat.net>

<sup>11</sup> [https://docs.google.com/document/d/1Se36svYE1Uzpppe1HWnEyat\\_sAGghB3kE285LElJBW4/edit?usp=sharing](https://docs.google.com/document/d/1Se36svYE1Uzpppe1HWnEyat_sAGghB3kE285LElJBW4/edit?usp=sharing)