Federal Communications Commission
Office of Engineering and Technology
Laboratory Division

March 18, 2015

SOFTWARE SECURITY REQUIREMENTS FOR U-NII DEVICES

I. INTRODUCTION

On March 31, 2014, the Commission revised the rules in Part 15 that permits U-NII devices in the 5 GHz Band.[1] As part of that revision, the Commission required that all U-NII device software be secured to prevent its modification to ensure that the device operates as authorized thus reducing the potential for harmful interference to authorized users.[2] Although, the Commission refused to set specific security protocols, the methods used by manufacturers to implement the security requirements must be well documented in the application for equipment authorization. In this document, we provide general guidance on the type of information that should be submitted in the equipment authorization application.[3] The security description provided in the application must cover software security, configuration, and authentication protocols descriptions, as appropriate. This guidance applies to master and client devices. Special circumstances that apply only to client devices are also addressed.

II. SOFTWARE SECURITY DESCRIPTION GUIDE

An applicant must describe the overall security measures and systems that ensure that:

1. only properly authenticated software is loaded and operating the device; and
2. the device is not easily modified to operate with RF parameters outside of the authorization.

The description of the software must address the following questions in the operational description for the device and clearly demonstrate how the device meets the security requirements.[4] While the Commission did not adopt any specific standards, it is suggested that the manufacturers may consider applying existing industry standards for strong security and authentication.[5]

---

[1] *See Revision of Part 15 of the Commission's Rules to Permit Unlicensed National Information Infrastructure (U-NII) Devices in the 5 GHz Band, First Report and Order,* ET Docket No. 13-49 (2014) (1st R&O).

[2] For U-NII devices certified as SDR, see KDB Publication 442812 D01.

[3] All application purposes require the submission of a Software Security Description.

[4] An exhibit that is part of the Operational Description can be subject to confidentiality. Applicants may request that the software description, as part of the operational description exhibit type, be held confidential. If the software description is submitted as the software information exhibit, it is automatically held confidential.

[5] It is suggested that manufacturers follow existing security standards and definitions: X.800, RFC 2828, and IEEE 802.11i. Strong security implementations include the use of public key infrastructure (PKI) solutions and/or software downloads via mutually authenticated and secure connections with manufacturer network management systems (NMS). On the other hand, examples of weak security implementations include those that rely solely on the distribution of firmware in compiled binary form without any form authentication or verification between the device and entity sending the firmware. These implementations

(continued....)

This guide is not intended to be exhaustive and may be modified in the future. There may be follow-up questions based on the responses provide by the applicant for authorization.

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 authorization.[7]

(...continued from previous page)
are typically susceptible to device "flashing" with third-party firmware or software capable of operating the device outside of its authorization.

[6] *See*, for example, www.dd-wrt.com/

[7] Note that Certified transmitter modules must have sufficient level of security to ensure that when integrated into a permissible host the device parameters are not modified outside those approved in the grant of authorization. (*See*, KDB Publication 99639). This requirement includes any driver software that may be installed in the host, as well as, any third party software that may be permitted to control the module. A full description of the process for managing this should be included in the filing.

III. SOFTWARE CONFIGURATION DESCRIPTION GUIDE

In addition to the general security consideration, for devices which have "User Interfaces" (UI) to configure the device in a manner that may impact the operational parameter, the following questions shall be answered by the applicant and the information included in the operational description. The description must address if the device supports any of the country code configurations or peer-peer mode communications discussed in KDB 594280 Publication D01.[8]

SOFTWARE CONFIGURATION DESCRIPTION	
USER CONFIGURATION GUIDE	1. To whom is the UI accessible? (Professional installer, end user, other.)
	a) What parameters are viewable to the professional installer/end-user?[9]
	b) What parameters are accessible or modifiable by the professional installer?
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	c) What parameters are accessible or modifiable to by the end-user?
	(1) Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?
	(2) What controls exist that the user cannot operate the device outside its authorization in the U.S.?
	d) Is the country code factory set? Can it be changed in the UI?
	(1) If so, what controls exist to ensure that the device can only operate within its authorization in the U.S.?
	e) What are the default parameters when the device is restarted?
	2. Can the radio be configured in bridge or mesh mode? If yes, an attestation may be required. Further information is available in KDB Publication 905462 D02.
	3. For a device that can be configured as a master and client (with active or passive scanning), if this is user configurable, describe what controls exist, within the UI, to ensure compliance for each mode. If the device acts as a master in some bands and client in others, how is this configured to ensure compliance?
	4. For a device that can be configured as different types of access points, such as point-to-point or point-to-multipoint, and use different types of antennas, describe what controls exist to ensure compliance with applicable limits and the proper antenna is used for each mode of operation. (See Section 15.407(a))

[8] *See* KDB Publication 594280 D01Software Configuration Control for Devices. The document provides guidance for devices permitting device configurations and limitations on configuration parameters accessible to the third parties.

[9] The specific parameters of interest for this purpose are those that may impact the compliance of the device. These typically include frequency of operation, power settings, antenna types, DFS settings, receiver thresholds, or country code settings which indirectly programs the operational parameters.

CHANGE NOTICE

07/10/2014: 594280 D02 UNII Device Security v01 has been changed to 594280 D02 UNII Device Security v01r01. Changes made to items 3 and 4 in the Software Configuration Description table.

03/18/2015: 594280 D02 UNII Device Security v01r01 has been changed to 594280 D02 UNII Device Security v01r02. Changes made to questions in General Description and Third Party Access sections of the Software Security Description table.