Toyota Material Handling Manufacturing Sweden AB

FCC Software Security Description for 'DHU4'

Table of Contents

1 Introduction

This document describes the security measures taken by Toyota Material Handling Manufacturing Sweden (TMHMS) to ensure that no unwanted changes are introduced in the software images loaded onto trucks using our product 'DHU4'. Especially relating to the WiFi radio module settings, to make sure that we conform to the testing and tuning performed for FCC certification of the WiFi radio module, the FC20 module from Quectel.

2 Detailed description

2.1 Model Name

The model being certified is model 'DHU4' which has an external antenna, Smarteq P/N 550237.

2.2 Files involved

The binary parameter files for the FC20 Bluetooth/WiFi module are received from Quectel and contains the parameters set up during certification testing. The specific files are:

- bdwlan30.bin – Contains the WiFi radio parameters
- tfbtnv11.bin – Contains the Bluetooth radio parameters

These files contain the tuning parameters controlling the FC20 radios. TMHMS will not be modifying or customizing the contents of this file after certification. The files are stored in the TMHMS repositories in Azure DevOps (ADO), only accessible by TMHMS developers or developers contracted by TMHMS.

As a firmware image is built for the DHU4 device, the resulting firmware image is signed by TMHMS's private keys that are not available except in the pipelines in ADO. Not even developers have direct access to the keys.

2.3 Building a firmware image

Any official builds must be made using our ADO pipelines, set up for that purpose. Only these pipelines have access to the secret data necessary to properly sign a firmware image so that it will be accepted by a DHU4 device. The private key is stored in a Azure Key Vault and only available inside the build agent running the ADO pipelines through the environment and is never stored to a file or logged anywhere.

2.4 Downloading a firmware image

When we download a firmware update, containing the parameter files for the Bluetooth/WiFi module, we will check the downloaded contents' signatures against TMHMS's public keys, corresponding to the private keys mentioned above, and will not proceed with installation or booting the new firmware if they do not match.

2.5 Using the settings files on device

2.5.1 Booting

As the device tries to boot a newly installed firmware, the high assurance boot (HAB) feature of the CPU will be utilized to make sure that any kernel and root file system that has not been correctly signed by TMH/TMHMS private keys cannot be booted.

This means that if a root file system is modified after download or install, the digest of the new file system will no longer match that of the decrypted signature, and the device will refuse to boot it.

Since this root file system contains the parameter files for the WiFi module, they too are unmodified as compared to the files that we built into our firmware images, if the check passes.

2.5.2 Loading the parameter files

After all the boot steps have been verified against the public keys, the new kernel is booted and the root file system mounted. The root file system is of type squashfs, which can only be mounted read-only, and hence, cannot be modified while the system is running. When the kernel boots, it will load the parameter file to the FC20 module from the root file system, knowing that it will still be unmodified from the file that was built into the root file system image that we built and signed in our official build pipelines.

2.5.3 On device summary

The HAB is a hardware assisted feature of the silicon that runs the DHU4 device and allows verification of software signatures against key hashes burned into fuses as the DHU4/DHUnx devices are manufactured. In the different steps of the boot process, each next step is verified in a chain leading back to this burned in root of trust, providing a strong guarantee that no piece of software that is modified without our consent should be able to run on the device, especially until the Linux kernel and kernel drivers have been loaded.

3 Answers to questionnaire in FCC KBD 594280

3.1 General Description, question #1

Question: "Describe how any software/firmware updates for elements than can affect the device's RF parameters will be obtained, downloaded, validated and installed. For software that is accessed through manufacturer's website or device's management system, describe the different levels of security as appropriate"

Answer: See §2 in this document.

3.2 General Description, question #2

Question: "Describe the RF parameters that are modified by any software/firmware without any hardware changes. Are these parameters in some way limited such that any other software/firmware changes will not allow the device to exceed the authorized RF characteristics?"

Answer: See §2 in this document.

3.3 General Description, question #3

Question: "Describe in detail the authentication protocols that are in place to ensure that the source of the RF-related software/firmware is valid. Describe in detail how the RF-related software is protected against modification"

Answer: The rootfs containing the software and settings for the radio is digitally signed, using RSA-4096 encryption of a SHA-256 hash, when we build it. At boot the kernel will verify the signature of the rootfs. This verifies that the rootfs is unmodified as compared to what be built and released. At runtime, the rootfs is mounted read-only and cannot be modified while the system is running. See §2.5 in this document. The signing keys are only available to the build agent while running the pipeline, as described in §2.3 in this document.

3.4 General Description, question #4

Question: "Describe in detail any encryption methods used to support the use of legitimate RF-related software/firmware"

Answer: We use the HAB feature of NXP's hardware for signing and verifying official Toyota software. Four RSA-4096 super root key (SRK) pairs are created which are used to sign the image signing key(s), which are also RSA-4096. At any given time only one SRK is actively used and an SRK can be permanently revoked if not trusted anymore. A root of trust for the four SRKs is established by burning the SHA-256 hash of the public key of each pair into dedicated NXP processor HAB fuses and the device is locked. From this point the NXP boot ROM will only accept signed boot images using a signing key which in turn is signed by the active SRK key and which in turn is trusted via the SRK hash in fuses.

A signed image contains the certificates of all keys, SRK, image signing key and the signature itself. To authenticate an image the NXP HAB (ROM code) is invoked which ensures a proper certificate chain and that the signature is correct. At power on it is the ROM that loads the first stage bootloader and invokes HAB to check this image. The first stage bootloader in turn loads the

second phase bootloader and invokes HAB to check this image. The second stage bootloader then loads the Linux kernel image and invokes HAB to check this image.

The root file system itself is read-only, signed and verified using Linux dm-verity functionality. The basis for dm-verity is a key-pair of which the public key itself is stored along with the Linux kernel image and similarly verified by the second stage bootloader before invoking the kernel. The authentication of this read only file system is then handled by the Linux kernel which as explained also has been authenticated.

Thus, all software in the root file system, including the radio driver, firmware and configuration, is unmodified, genuine Toyota software as released by us.

If at any step in the described chain a signature is incorrect, the device halts and refuses to proceed booting.

3.5 General Description, question #5

Question: "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?"

Answer: The module will be configured as a client and the software and configuration is secured against modification as described in §3.4 above.

3.6 Third-Party Access Control, question #1

Question: "Explain if any third parties have the capability to operate a U.S.-sold device on any other regulatory domain, frequencies, or in any manner that may allow the device to operate in violation of the device's authorization if activated in the U.S"

Answer: There is no access for third parties to change the frequencies, regulatory domain or other radio parameters.

3.7 Third-Party Access Control, question #2

Question: "Describe, if the device permits third-party software or firmware installation, what mechanisms are provided by the manufacturer to permit integration of such functions while ensuring that the RF parameters of the device cannot be operated outside its authorization for operation in the U.S. In the description include what controls and/or agreements are in place with providers of third-party functionality to ensure the devices' underlying RF parameters are unchanged and how the manufacturer verifies the functionality"

Answer: There is no access for third parties to install firmware on the device.

3.8 Third-Party Access Control, question #3

Question: "For Certified Transmitter modular devices, describe how the module grantee ensures that host manufacturers 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 RF parameters are not modified outside the grant of authorization."

Answer: The module has no logic of its own and is fully controlled through the device driver loaded in the host device. This driver is verified as unchanged as described in the answer to §3.4 and is not modifiable by third parties.

3.9 User Configuration Guide, questions

"Describe the user configurations permitted through the UI. If different levels of access are permitted for professional installers, system integrators or end-users, describe the differences"

Answer: The device is intended for machine to machine communication and has no UI.

3.9.1 User Configuration Guide, question #1a

Question: "What parameters are viewable and configurable by different parties?"

Answer: The device is intended for machine to machine communication and has no UI.

3.9.2 User Configuration Guide, question #1b

Question: "What parameters are accessible or modifiable by the professional installer or system integrators?"

Answer: See §2 in this document.

3.9.3 User Configuration Guide, question #1b1

Question: "Are the parameters in some way limited, so that the installers will not enter parameters that exceed those authorized?"

Answer: The user can never change any RF calibration files. See also §2 in this document.

3.9.4 User Configuration Guide, question #1b2

Question: "What controls exist that the user cannot operate the device outside its authorization in the U.S.?"

Answer: The system integrator is always a trained Toyota technician.

3.9.5 User Configuration Guide, question #1c

Question: "What parameters are accessible or modifiable by the end-user?"

Answer: The user can never change any RF calibration files. See also §2 in this document.

3.9.6 User Configuration Guide, question #1c1

Question: "Are the parameters in some way limited, so that the user or installers will not enter parameters that exceed those authorized"

Answer: The user can never change any RF calibration files. See also §2 in this document.

3.9.7 User Configuration Guide, question #1c2

Question: "What controls exist so that the user cannot operate the device outside its authorization in the U.S.?"

Answer: The device is intended for machine to machine communication and has no UI.

3.9.8 User Configuration Guide, question #1d

Question: "Is the country code factory set? Can it be changed in the UI?"

Answer: Yes, it is factory set and cannot be changed in the user interface

3.9.9 User Configuration Guide, question #1d1

Question: "If it can be changed, what controls exist to ensure that the device can only operate within its authorization in the U.S.?"

Answer: N/A.

3.10 User Configuration Guide, question #1e

Question: "What are the default parameters when the device is restarted?"

Answer: WiFi is turned off at boot until appropriate drivers have been loaded and settings have been read, as set in the factory or by a trained technician.

3.11 User Configuration Guide, question #2

Question: "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."

Answer: The device does not support using the radio in bridge or mesh mode.

3.12 User Configuration Guide, question #3

Question: "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?"

Answer: The device has no UI.

3.13 User Configuration Guide, question #4

Question: "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."

Answer: The device will always be used with the provided antenna.