Honeywell

Honeywell International Inc
Honeywell Scanning and Mobility
9680 Old Bailes Road
Fort Mill, SC 29707 USA

February, 03, 2015

Software Security Description

As specified in FCC KDB 594280 D02 U-NII Device Security v01r01, 2014-07-10,and as requested per FCC KDB 905462 D03 Client Without DFS New Rules v01r01

Grantee: Honeywell International Inc.

Device: Dolphin 75eL0N Handheld Computer

Description: Containing WLAN IEEE 802.11a,b,g,n,a,ac (UNII acc. to new FCC rules), Bluetooth, NFC

FCC IDs: HD5-75EL0N, HD5-75EL00

IC IDs: 1693B-75EL0N, 1693B-75EL00

Q1: Describe how ~~m~~any software/firmware update will be obtained, downloaded and installed.

A1: The software/firmware will be released on official company support site. Only customers with authenticated account can access it. After getting the software/firmware, customers will have to put it on a SD card, insert it to the device and then make the device enter recovery mode. Then the device will find the update package and do installing itself.

Q2: 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 parameter?

A2: The software can only modify channel frequency to be scanned. Any invalid or illegal channel frequency will be filtered by the driver. So the driver will make sure the parameters are compliant with regulatory limitations

Q3: Are there any authentication protocols in place to ensure that the source of the software/firmware is legitimate? If so, describe in details. If not, describe how the software is secured from modification.

A3: The source code is stored on authenticated servers and only developers with authenticated account can access the code.

Q4: Are there any verification protocols in place to ensure that the software/firmware is legitimate? If so, describe in details.

A4: The software/firmware will be signed with our certificate. If the software is modified by hackers, it will have illegal signing and the system will not recognize it.

Q5: Describe, if any, encryption method used.

A: WPA/WPA2-PSK, WPA/WPA2-EAP

Q6: 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 bands of operation and client in another; how is compliance ensured in each band of operation?

A6**:** The device is a client according to FCC part 15.202. The device does passive scanning for all 5G bands channels.
The device does active scanning for all 2.4G. Active scanning on channels 12,13,14 is disabled. The user can select per menu option if the device will mark the channel active when detected beacon/probe response from that channel. The device will not answer on channels 12, 13, 14 no matter how the user configures it.

Q7: How are unauthorized software/firmware changes prevented?

A7: The source code is disallowed to access without authorized accounts.

- **Q7.1: Is it possible for thirds parties to load device drivers that could modify the RF parameters, country of operation, or other parameters which impact device compliance? If so, describe procedures to ensure that only approved drivers are loaded.**
- A7.1: No. Third-party's software will not have legal signature. The device will not load the software without valid signature.

- **Q7.2: 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?**

- A7.2: US sold device is only the version that is FCC certified. This version of device complies with FCC regulation by driver hard coding and can't be changed in any manner. The EU/CE versions won't have FCC label info on the device and will not sell in the US.

- **Q7.3: What prevents third parties from loading non-US versions of the software/firmware on the device?**

- A7.3: The US version identity is stored in device's EEPROM. Third parties don't have permission to modify the data in EEPROM in released version. They don't have the tool either.

Q8: To whom the UI accessible? (Professional Installer, end user, other.): End user

- **Q8.1: What parameters are viewable to the professional installer/ end user?**
- A8.1: Network SSID, Security Type, User name, Password
- **Q8.2: What parameters are accessible, or modifiable to the professional installer?**
- A8.2**:** Network SSID, Security Type, User name, Password
  - **Q8.2.1: Are the parameters in some way limited so that the installer will not enter parameters that exceed those authorized?**
  - A8.2.1: Network will not be connected if they input wrong parameters.
  - **Q8.2.2: What controls exist that the user cannot operate the device outside its authorization in the US?**
  - A8.2.2: The driver filters illegal parameters.
- **Q8.3: What configuration options are available to the end user?**
- A8.3: Network Profile
  - **Q8.3.1: Are the parameters in some way limited so that the installer will not enter parameters that exceed those authorized?**
  - A8.3.1: Network will not be connected if they input wrong parameters
  - Q8.3.2: **What controls exist that the user cannot operate the device outside its authorization in the US?**
  - **A8.3.2:** The driver filters illegal parameters.
- **Q8.4: Is the country code factory set? Can it be changed in the UI?**
- A8**.**4: Country code is factory set, and cannot be changed in the UI**.**
- **Q8.5: What are the default parameters when the device is restarted?**
- AQ8.5: The previously configured network profiles including network SSID, security parameters are stored when the device is restarted. The FCC compliance configuration is guaranteed by hard code in the driver. Users can’t change the FCC related configuration.

Q9: Can the radio be configured in bridge, or mesh mode? No.

Michael Robinson

Michael Robinson
Phone: 315.554.6387
Email: michael.robinson3@honeywell.com