

## Basic Checklist for IOT Device security testing

- 1) Wireless Security pen testing : The wireless technology like infrared receiver, BLE, 4G, LTE, Zigbee, LoRA, WiFi, MQTT, Bluetooth, Wi-Fi, NFC, Radio-frequency Identification (RFID), etc. like checking version used, what are the current vulnerabilities present how to overcome that?, any better



alternative available?

- 2) Encryption Security: SSL implementation over network to check its encryption standards, how data is sent via network? SSL or plane text? Is the current SSL weak? Or strong? How the device communicate with each other or to the main server? Also check the security of data which is stored, is it encrypted? Or does it require encryption or not?



- 3) Firmware Security: The device must verify the signature and then only it must initiate the upgrade process, or else anyone can create modified firmware and update the device and play with it. And also it must have the protection mechanism for the anti-Downgrade process of Firmware. Sometimes the attacker downgrade the firmware which is having known vulnerability and try to exploit it.

