  
unless otherwise referred things are based off [1]  
  
Hardware issues found:  
  
The boot code should immutable, that is, be stored on ROM or on inaccessible flash so that it can be seen as a root of trust, from which a secure boot is possible in case of a security breach.  
  
Sensors on an IoT device can be vulnerable, either by controlling their sensing environment, or by directly tampering the sensors. This can lead to (partially) known plaintext attacks, or in extreme cases data execution attacks.  
  
Any data stored on the device should never be left unencrypted (especially keys and user information). Check the storage devices.  
  
Check for unnecessary ports! Any debug or test ports need to be fused off, and network ports need to be closed if not in use!  
  
Anything that is easily removed has to be considered vulnerable to replacement  
  
Logs need to be stored in a non-removable way!

Check boundary scan for sensitive information (CIPHER KEY!) [2]  
  
Firmware issies found:

Malware infecting the firmware can cause loss of control of the device, which can lead to APT or a botnet infection like Mirai.

Check for exploits.  
  
The device NEEDS to be patchable. I don’t care if we don’t find anything.  
  
Just because we don’t understand your security, doesn’t mean your device is secure. Put in something proven and you shouldn’t have to hide what you did.  
  
Firmware updates need to be VALIDATED.   
  
Privileged code and data needs to be isolated from the pieces that don’t need access to them. Privilege should never be higher than necessary.  
  
The update/control server authentication needs to be checked.

Reference:

[1] J. Kruse-brandao, J. L. Garcia, and M. Edwards, *Baseline Security Recommendations for IoT*, no. November. 2017.

[2] A. Cui, Y. Luo, H. Li, and G. Qu, “Why current secure scan designs fail and how to fix them?,” *Integr. VLSI J.*, vol. 56, no. October 2016, pp. 105–114, 2017.