Upon receiving a new product. Perform steps in order of reading. Text written in italics is purely for information.  
  
Turn on product, verify functionality.  
  
Inspect case, write down external anti-tamper (tamper-evident, tamper-resistant) measures and externally available ports and their probable purpose.   
  
*Tamper-evident measures are any measures that introduce a visible and permanent change when the device has been opened. The most self-evident example of this is removable or breakable seals on the device. The device can only be opened after these have been broken, and once broken they are very difficult to convincingly repair. This includes cases that are designed such that they can only be opened by damaging them irreparably. Tamper-resistant measures are any measures that make access to the circuit board difficult, usually by reinforcing the device. Security screws will not be counted among these, as for anyone serious these are no more an inconvenience as any other exotic screw head.*  
Disassemble case, expose the PCB, then reassemble case and turn on product, verify functionality, note changes.   
  
In case of no changes: No tamper detection mechanisms. If no detection, or resistance measures have been taken: **Security Hazard: Device vulnerable to tampering.** If there are no tamper-evidence measures taken then the problem is elevated to **Security Fail: Potentially unnoticed physical access.**

**Tool suggestion: Powertools(saw, drill)**

Disassemble case, write down labels to IC’s, attempt to obtain datasheets, and categorise based on function. For each IC also determine whether their pins can be probed or not (BAG-IC’s and IC’s with pins that are excessively small can generally not be properly interfaced with using flying probes.)  
**Tool suggestion: Magnifying glass**

|  |  |
| --- | --- |
| Mutable storage | Cryptography |
| Immutable storage | Wireless communication |
| Processor | DAC/ADC |
| Signal Processing | Sensor |
| Actuator | Unknown |
|  |  |

Identify ports on the PCB, write down probable purpose, if no probable purpose can be found, assume debug or testing purpose. Do the same for wireless devices. If necessary, attach a cable with one connector removed and analyse the wires using an oscilloscope.  
  
For any IC which has sufficiently large external pins, attempt to setup probes   
  
If there is a JTAG port, attempt to interface with the JTAG on the chip. Specifically attempt to use it against previously mentioned chips, particularly those mounted on Ball Array Grids, as those cannot be interfaced with using flying probes.

**Requested tools:   
Logic analyzer (atleast 8 pins) , e.g.:** [**https://www.adafruit.com/product/2512**](https://www.adafruit.com/product/2512) **Oscilloscope already available.  
JTAGulator: https://www.adafruit.com/product/1550**  
  
In the case of storage, wireless chips, attempt to interface with the chip using the pins. In the case of SPI or I²C connected chips, first attempt to discern the clock speed using an oscilloscope. Analyse the output of storage chips to determine the frequency of characers. Lack of frequency uniformity: **Security Fail: Accessible unecrypted or poorly encrypted data at rest***ECB encoding could lead to non-uniform code. This is insufficient to properly ensure that the data cannot be read, as one could simply correlate cyphertext to plaintext through Chosen Plaintext attacks.*In the case of processors and a lack of external immutable storage, attempt to ascertain the existence of in-processor immutable storage. If there is none, this implies that the firmware is located in mutable storage, and therefore: **Security Fail: Insecure Root of Trust** In the other extreme, where there is only immutable storage, the device necessarily cannot store updates. **Security Fail: No Update Mechanism**.   
  
*Immutable storage means that the storage is read-only, i.e. the contents of the storage device cannot be altered after the fact.*

Example sheets

|  |  |
| --- | --- |
| Tamper- | Description |
| Resistant | Unopenable case |
| Evident | Seal over screws |
| Detection | Outer case lined with traces. |
|  |  |
|  |  |
|  |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| Type | Label | Description |
| Mutable storage | 25SF081 | SPI-flash storage device |
| Wireless Comm | FU63427K | Wireless LAN chip |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |