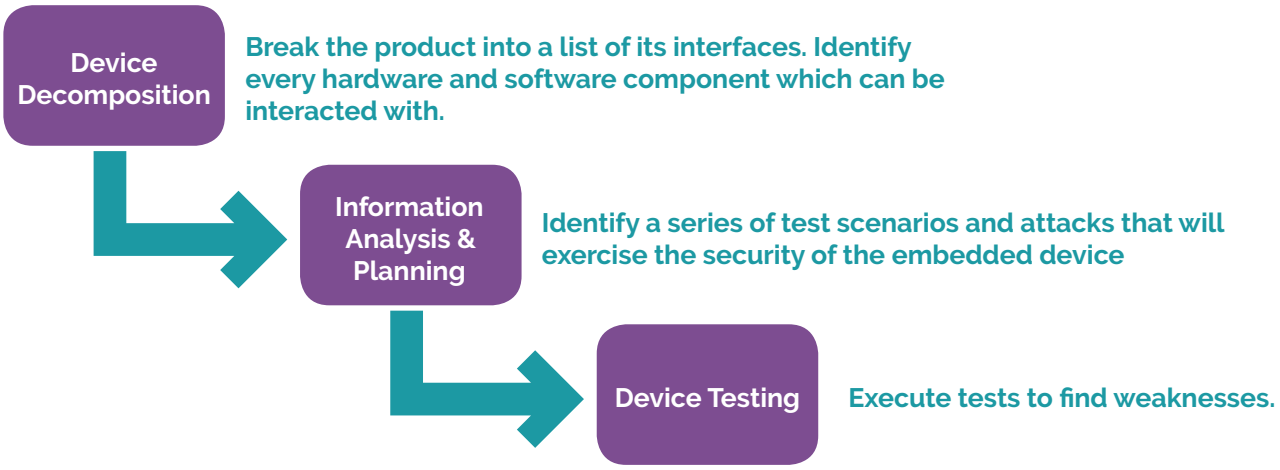
Our methodology

The following shows our process at a high-level before we present some specific steps which are generally included:



This follows time-worn practices within penetration testing in general: enumerate, identify attack surface, then exploit.

Documentation Review	Hardware Review	Software Review
Many parts of our freely available IoT Checklist can be covered by looking at the user manual. We would look for signs such as: › Fixed passwords (static across every device instance) › Firmware Update Mechanism › Decommissioning Advice for Consumers	Give us a device and we will dismantle it (in the same manner an attacker would). We would then: › Enumerate components and research them › Look for header PINs we can connect to › Attempt UART/JTAG or other data extraction techniques › Find any weaknesses from manufacturing techniques	Generally, it is possible to extract the firmware from either the device itself using techniques listed above, or by visiting a vendor's website. Whatever software is powering a device, Secarma would recommend assuming that the source code is available to attackers. On that basis, we are happy to: › Conduct a Black-Box application assessment of administration services. › Conduct a Code Review with source being provided

The risks are great. With personal data and IP stored on connected devices, attackers have the very real potential to completely shut down an organisation – making IoT product reviews critical to product development plan.