IoT Check List Example Process

How to engage with security

Document revision: 1.0
Date: 25/08/2017
Status: Final
Authors: Paul Ritchie

Secarma Limited. 1 Archway, Birley Fields, Manchester, England, M15 5QJ.
Company Registration Number: 04217114. VAT Number: 775714400.

CONTENTS

1 INTRODUCTION

This document shows an example process to follow when working through the IoT CheckList. We assume that if you are reading this that you have a product you are considering developing and that you are looking to engage with Security as soon as possible. Following this process will allow you to capture the "Attack Surface" (parts which may be exploitable) of your device.

There is additional information about the IoT Checklist which sets context surrounding this which is available at this blog post:

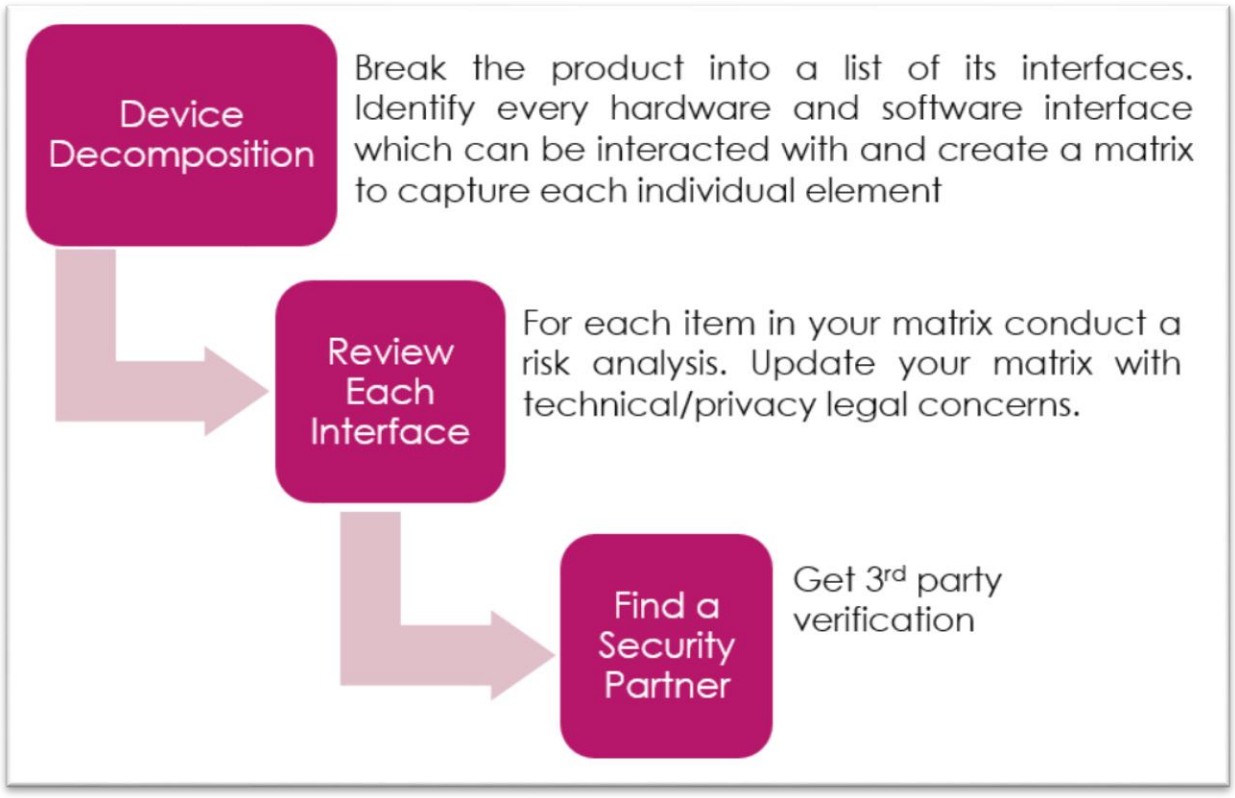
- https://www.secarma.co.uk/internet-of-things-iot-security-checklist/

The post covers various risks and provides high level advice that should be followed.

1.1 Process

There is a recommended three step process as outlined below:

Figure 1 – Process Chart



This document goes into more detail providing advice on how to do each of these.

If the first two steps are daunting or you just prefer being walked through it all. Then you can choose to park everything and simply go straight to finding a security partner.

The following steps create an example spreadsheet which is available at the URL below:

- https://github.com/SecarmaLabs/IoTChecklist/blob/master/examples/Example-Device_Decomposition_Matrix.xlsx

This has five sheets inside which match up to how the spreadsheet should look after each action was taken. Between this document that you are reading and the example XLSX you should have enough information to tackle your own analysis.

1.2 Device Decomposition

By the end of this step you will have created a spreadsheet (who doesn't love a spreadsheet?) which tracks all parts of your device that can be attacked. In effect, this is enumerating the "attack surface". Essentially this is exactly what an attacker will be doing (though most won't make spreadsheets).

To demonstrate how to do this Secarma have created a fictional product. Think of the following as the box description for an Internet enabled radio:

DAB/FM/MW Radio
Wi-Fi Connected
Internet Radio
Colour Display
Spotify Connect
MP3/WMA/FLAC/AAC playback via DLNA and USB
Infrared remote control
3-way speaker
High gloss black finish
Listen to stations from around the world
Play your music from your computer
Wired Ethernet
120 stations pre-set
Aux in socket for MP3 playback
Headphone socket
AC Adaptor

These are the features of the device which are being put forward as a product description. This is what consumers are looking at when choosing the device. If nothing else it gives us a starting point.

Open the blank device decomposition spreadsheet available from here:

- https://github.com/SecarmaLabs/IoTChecklist/blob/master/Blank-Device_Decomposition_Matrix.xlsx

Write into that a list of all features that the radio has one row at a time. You should have this:

Figure 2 – After Step One

Interface Name	Summary	Technical Concerns	Privacy/Legal Concerns
DAB/FM/MW Radio			
Wi-Fi Connected			
Internet Radio			
Colour Display			
Spotify Connect			
MP3/WMA/FLAC/AAC playback via DLNA and USB			
Infrared remote control			
3 way speaker			
High gloss black finish			
Listen to stations from around the world			
Play your music collection from your computer			
Wired Ethernet			
120 station preset			
Aux in socket for MP3 playback			
Headphone socket			
AC Adaptor			

If you are looking at the completed spreadsheet this appears as the “Features on the Box” sheet.

At this point discuss each row or research to see if there are potential technical and/or privacy/legal concerns. There are two simple rules:

- If something is an “input” or if it talks to another device in some way you are going to say yes that is a technical concern.
- If something handles personal information it is going to have a privacy/legal concern.

You may need to research each item yourself to find if anyone has ever exploited a technical concern. For example, while the “DAB/FM/MW” feature is an input it may have never been exploited before so it is a low priority.

1.2.1 Prune the unnecessary rows

If the line is totally irrelevant to the security of the device, then simply remove it. In our example, these are:

- Colour Display – shows a picture, is not a touch screen so not an input point.
- 3 way speaker – is not a target.
- High gloss black finish – not a target.
- Listen to stations from around the world – duplicate of “internet radio”.
- 120 station preset – not a target.
- Aux in socket for MP3 playback – not a target (we assume no software on the radio interacts over Aux).
- Headphone socket – not a target.
- AC Adaptor – not a target.

At the end of pruning you should have arrived at the following list:

Figure 3 -After Pruning

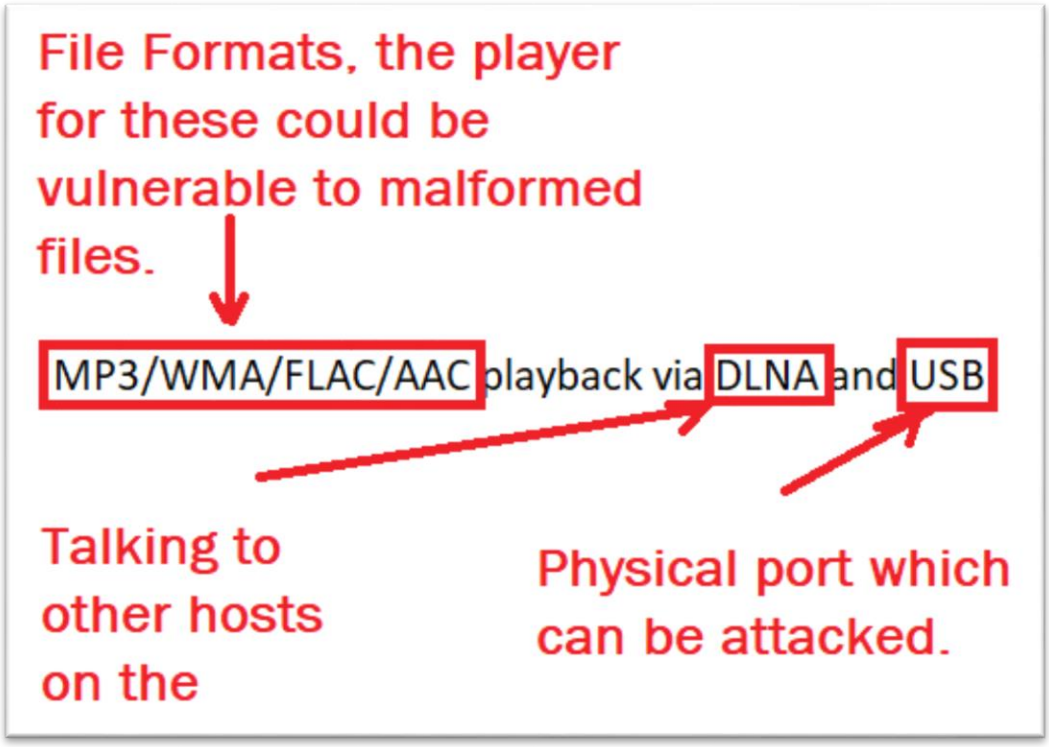
Interface Name	Summary	Technical Concerns	Privacy/Legal Concerns
DAB/FM/MW Radio		Y	
Wi-Fi Connected		Y	Y
Internet Radio		Y	Y
Spotify Connect		Y	Y
MP3/WMA/FLAC/AAC playback		Y	
DLNA		Y	
USB		Y	
Infrared remote control		Y	
Play your music collection from your computer		Y	
Wired Ethernet		Y	

In the completed spreadsheet, this appears as the After-Pruning" sheet.

1.2.2 Expansion for Specificity

One of our rows is not specific enough so we should expand that to create more rows. The following shows

Figure 4 – Expanding row for specificity



As can be seen the attacker has a lot of options from that one row. We need to add DLNA and USB as separate items to get specific.

After expansion, we now have the list as shown below:

Figure 5 – After Expansion

Interface Name	Summary	Technical Concerns	Privacy/Legal Concerns
DAB/FM/MW Radio		Y	
Wi-Fi Connected		Y	Y
Internet Radio		Y	Y
Spotify Connect		Y	Y
MP3/WMA/FLAC/AAC playback		Y	
DLNA		Y	
USB		Y	
Infrared remote control		Y	
Play your music collection from your computer		Y	
Wired Ethernet		Y	

If you are reading the completed spreadsheet, this appears as the “After-Expansion” sheet.

1.2.3 Discuss Additional Items

We are complete with our task at this point if literally every feature was described in the product details. This is not true so at this point you need to discuss any additional items to add. As a minimum for this example Secarma are going to add three rows:

- **Web API** - The radio exposes an API to allow mobile applications to remotely control it and to alter settings on the device. This runs a REST based web service over HTTP on TCP port 80.
- **Web UI** - There is a user interface which runs on the same HTTP service as the API.
- **Hardware Level** -The hardware choices and how things are connected can have a tangible impact on security. Researchers are dismantling devices and looking for weaknesses.

The hardware level can be broken down into individual chips and memory blocks etc. As our radio is fictional we have not got design diagrams Secarma are saying simply “hardware level”.

The following shows the spreadsheet after adding these items:

Figure 6 – After Additional Items

Interface Name	Summary	Technical Concerns	Privacy/Legal Concerns
DAB/FM/MW Radio		Y	
Wi-Fi Connected		Y	Y
Internet Radio		Y	Y
Spotify Connect		Y	Y
MP3/WMA/FLAC/AAC playback		Y	
DLNA		Y	
USB		Y	
Infrared remote control		Y	
Play your music collection from your computer		Y	
Wired Ethernet		Y	
Web API		Y	
Web UI		Y	
Hardware Level		Y	

We have highlighted the new rows in green.

If you are reading the completed spreadsheet, this appears as the “After-Additional-Items” sheet.

1.3 Review Each Interface

At this point you have created a matrix of the potentially exploitable parts. You have also identified things that would have either a technical or privacy/legal concern. Congratulations you have defined your attack surface!

Now the challenging work starts. For each row in the spreadsheet, follow the list of information gathering steps:

1) **Known exploits** – Search online for known exploits and attacks. Create a summary in your spreadsheet which covers the potential exploits. If possible estimate the ease of attack and likelihood.
2) **Best Practices** – Search for relevant best practices. If you are using a form of embedded Linux then find relevant lockdown guides and the same for each configured service.
    a. There are various benchmarks from CIS (https://www.cisecurity.org/cis-benchmarks/) which are useful starting points. They provide best practice guidelines for operating systems as well as a number of services like Apache, MySQL etc.
    b. If CIS does not have a guide then you may have to consult vendor documentation or look for alternative sources.
3) **Apply Best Practices** – Configure things in-line with best practices. Test that these configurations still allow your device to operate as intended.
4) **Prioritise** – Based on all your understanding of the threats faced you should now add a column to your spreadsheet to mark testing priorities. For example, we have gone with a rating system from 1-5 where 1 is “must test” and 5 is “if we had infinite budget and time let’s look at this”. Pick a system that works for you and apply it.

By the end of your review you should have a final spreadsheet shown below:

Figure 7 – Completed Decomposition Matrix

Interface Name	Summary	Technical Concerns	Privacy/Legal Concerns	Priority
DAB/FM/MW Radio	If the embedded system did something with data received over radio frequncies then this could be an exploitable input. Radio station name might have an overflow if someone sends a long enough string? Unlikely but you	Y		5
Wi-Fi Connected	This device becomes part of someones network. We would need to test how it does that. Does it store network passwords securely? Can the device be decommissioned	Y	Y	1
Internet Radio	It is connected to the Internet. How does it access stations? Is this over plain-text HTTP? Does this Internet connectivity allow the device to download updates?	Y	Y	1
Spotify Connect	Allowing mobile applications to control the radio's player remotely. Has a discovery protocol. It starts a networked service on the LAN to do this. Feasible	Y	Y	2
MP3/WMA/FLAC/AAC playback	The media player libraries on the device may have flaws which can be exploited by crafted files.	Y		2
DLNA	Specifies how devices share media over a network. Sounds like it is potentially vulnerable same way as spotify connect.	Y		2
USB	connected.	Y		2
Infrared remote control	IR can be recorded and replayed easily where an attacker has access to the legitimate remote control.	Y		5
Play your music collection from yo	Depending on how this is achieved we may have real problems. If you configure SMB credentials on the radio to do this then you are collecting sensitive information. Regardless we are interfacing with a computer on the network which makes this an input	Y		1
Wired Ethernet	Same risks as Wi-Fi really. A machine connected to the same network can attemt to attack the radio.	Y		
Web API	The radio exposes an API to allow mobile applications to remotely control it and to alter settings on the device. This runs a REST based web service over HTTP on TCP port 80.	Y		1
Web UI	There is a user interface which runs on the same HTTP service as the API.	Y		1
Hardware Level	The hardware choices and how things are connected can have a tangible impact on security. Researchers are dismantling devices and looking for weaknesses.	Y		1

This can serve as your “Risk Matrix”.

This appears as the “Completed” sheet within the example spreadsheet.

1.4 Find a Security Partner

So far you will have found out lots of information on your own unless you chose to find a partner sooner. At this point we are recommending that you find some 3rd party with security experience to verify your work and offer advice.

The reason for this is simple: your day job is not security.

You are also no doubt close to the project and are probably working long hours throwing yourself into it. What a partner provides is a fresh set of eyes with a narrow focus on security. They will have fewer assumptions and can spot gaps more easily. They may be aware of better “best practices” or of newer research. It is their job to know this.

Obviously Secarma are ready, willing and able to be that partner for you. However, you should find someone you are comfortable with, and follow all your relevant procurement policies.

Things that you should look for in a partner are:

- Able to understand your business and product.
- Able to explain new concepts clearly.
- Able to deliver within project deadlines reliably.
- People who are as excited about delivering security consultancy, as you are about your products.

At Secarma we aim to not just deliver results, but to behave as if we have a stake in your business. This idea was set by the co-founders and has been passed on via the company handbook since 2001. We look for these features at interview.

If you are seeking to engage with a security provider and you have already completed your decomposition process and have assembled your risk matrix? Then you are making it much easier to engage with a security provider. The scoping process is essentially all but complete and everyone you speak to should be capable of accurate quotations as a result.

Ultimately that ease of engagement will benefit you as the costs of consultancy will reduce accordingly.